

Log Tank Service

User Guide

Issue 01
Date 2025-02-21



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.

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

Trademarks and Permissions



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

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

Notice

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

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

Huawei Cloud Computing Technologies Co., Ltd.

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

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

Contents

1 Granting LTS Permissions to IAM Users.....	1
2 Purchasing LTS Resource Packages.....	3
3 Log Management.....	7
3.1 Overview.....	7
3.2 Managing Log Groups.....	7
3.3 Managing Log Streams.....	11
3.4 Viewing Log Management.....	14
3.5 Setting Multi-Account Log Aggregation.....	18
4 Log Ingestion.....	21
4.1 Overview.....	21
4.2 Using ICAgent to Collect Logs.....	23
4.2.1 Overview.....	23
4.2.2 Installing ICAgent (Intra-Region Hosts).....	24
4.2.3 Installing ICAgent (Extra-Region Hosts).....	30
4.2.4 Managing ICAgent.....	39
4.2.5 Managing Host Groups.....	47
4.2.6 Ingesting BMS Text Logs to LTS.....	54
4.2.7 Ingesting CCE Application Logs to LTS.....	62
4.2.8 Ingesting ECS Text Logs to LTS.....	76
4.2.9 Ingesting ServiceStage Containerized Application Logs to LTS.....	84
4.2.10 Ingesting ServiceStage Cloud Host Logs to LTS.....	93
4.2.11 Ingesting Self-Built Kubernetes Application Logs to LTS.....	101
4.2.12 Setting ICAgent Structuring Parsing Rules.....	115
4.3 Ingesting Cloud Service Logs to LTS.....	135
4.3.1 Overview.....	135
4.3.2 Ingesting AOM Logs to LTS.....	139
4.3.3 Ingesting APIG Logs to LTS.....	139
4.3.4 Ingesting CBH Logs to LTS.....	140
4.3.5 Ingesting CFW Logs to LTS.....	140
4.3.6 Ingesting CTS Logs to LTS.....	140
4.3.7 Ingesting DDS Logs to LTS.....	141
4.3.8 Ingesting DMS for Kafka Logs to LTS.....	141

4.3.9 Ingesting DRS Logs to LTS.....	141
4.3.10 Ingesting GaussDB(DWS) Logs to LTS.....	142
4.3.11 Ingesting ELB Logs to LTS.....	142
4.3.12 Ingesting Enterprise Router Logs to LTS.....	143
4.3.13 Ingesting FunctionGraph Logs to LTS.....	143
4.3.14 Ingesting GaussDB Logs to LTS.....	143
4.3.15 Ingesting GES Logs to LTS.....	143
4.3.16 Ingesting TaurusDB Logs to LTS.....	143
4.3.17 Ingesting GeminiDB Logs to LTS.....	143
4.3.18 Ingesting GeminiDB Mongo Logs to LTS.....	143
4.3.19 Ingesting GeminiDB Cassandra Logs to LTS.....	143
4.3.20 Ingesting IoTDA Logs to LTS.....	144
4.3.21 Ingesting ModelArts Logs to LTS.....	144
4.3.22 Ingesting MRS Logs to LTS.....	144
4.3.23 Ingesting RDS for MySQL Logs to LTS.....	144
4.3.24 Ingesting RDS for PostgreSQL Logs to LTS.....	144
4.3.25 Ingesting RDS for SQL Server Logs to LTS.....	144
4.3.26 Ingesting ROMA Connect Logs to LTS.....	144
4.3.27 Ingesting SMN Logs to LTS.....	144
4.3.28 Ingesting SecMaster Logs to LTS.....	144
4.3.29 Ingesting OBS Files to LTS (Beta).....	145
4.3.30 Ingesting VPC Logs to LTS.....	149
4.3.31 Ingesting WAF Logs to LTS.....	150
4.4 Using APIs to Ingest Logs to LTS.....	150
4.4.1 Collecting Logs Using APIs.....	150
4.4.2 API for Reporting Logs.....	152
4.4.3 API for Reporting High-Precision Logs.....	157
4.5 Ingesting Logs to LTS Across IAM Accounts.....	163
4.6 Using Kafka to Report Logs to LTS.....	167
4.7 Using Flume to Report Logs to LTS.....	172
5 Log Search and Analysis.....	183
5.1 Overview.....	183
5.2 Setting Cloud Structuring Parsing.....	183
5.2.1 Overview.....	183
5.2.2 Setting Cloud Structuring Parsing.....	185
5.2.3 Setting Structured and Tag Fields.....	191
5.2.4 Setting Custom Log Time.....	192
5.2.5 Setting a Structuring Template.....	195
5.3 Setting Indexes.....	198
5.4 Searching Logs.....	214
5.4.1 Accessing the Log Search Page.....	215
5.4.2 Using LTS Search Syntax.....	222

5.4.3 Creating an LTS Quick Analysis Task.....	233
5.4.4 Saving Conditions for Quick Search.....	234
5.5 Viewing Real-Time Logs.....	237
5.6 Analyzing Logs in LTS.....	238
5.7 SQL Analysis Syntax.....	240
5.7.1 Overview.....	240
5.7.2 Aggregate Function.....	244
5.7.3 Period-over-Period Functions.....	245
5.7.4 JSON Function.....	248
5.7.5 IP Functions.....	249
5.7.6 Mathematical Functions.....	251
5.7.7 Time Functions.....	255
5.7.8 Extrema Function.....	262
5.7.9 String Functions.....	262
5.7.10 SPLIT Functions.....	266
5.7.11 Comparison Operators.....	268
5.7.12 IP Functions.....	269
5.7.13 Reduction Functions.....	271
5.7.14 Other Functions.....	272
5.7.15 JOIN Clause.....	273
5.7.16 SQL Query Example.....	274
6 Log Visualization.....	276
6.1 Overview.....	276
6.2 Visualizing Logs in Statistical Charts.....	277
6.2.1 Statistical Charts.....	277
6.2.2 Table.....	278
6.2.3 Bar Chart.....	280
6.2.4 Line Chart.....	282
6.2.5 Pie Chart.....	284
6.2.6 Number Chart.....	288
6.2.7 Digital Line Chart.....	289
6.2.8 Map.....	290
6.2.9 Funnel Chart.....	292
6.3 Visualizing Logs in Dashboards.....	293
6.3.1 Creating a Dashboard.....	293
6.3.2 Adding a Dashboard Filter.....	299
6.3.3 Dashboard Templates.....	301
6.3.3.1 APIG Dashboard Templates.....	301
6.3.3.2 CCE Dashboard Templates.....	306
6.3.3.3 CDN Dashboard Templates.....	317
6.3.3.4 CFW Dashboard Templates.....	321
6.3.3.5 CSE Dashboard Templates.....	325

6.3.3.6 DCS Dashboard Template.....	330
6.3.3.7 DDS Dashboard Template.....	331
6.3.3.8 DMS Dashboard Template.....	332
6.3.3.9 DSL Dashboard Template.....	332
6.3.3.10 ER Dashboard Template.....	334
6.3.3.11 METRIC Dashboard Template.....	335
6.3.3.12 Nginx Dashboard Templates.....	336
6.3.3.13 VPC Dashboard Template.....	342
6.3.3.14 WAF Dashboard Templates.....	343
7 Log Alarms.....	349
7.1 Overview.....	349
7.2 Configuring Log Alarm Rules.....	350
7.3 Configuring Log Alarm Action Rules.....	363
7.3.1 Creating a Message Template on the LTS Console.....	363
7.3.2 Creating an Alarm Action Rule.....	370
7.4 Viewing Alarms in LTS.....	372
8 Log Transfer.....	374
8.1 Overview.....	374
8.2 Transferring Logs to OBS.....	375
8.3 Transferring Logs to DIS.....	383
8.4 Transferring Logs to DMS.....	386
8.5 Transferring Logs to DWS.....	390
9 Log Processing.....	394
9.1 Processing Logs with SQL Scheduled Jobs.....	394
9.2 Processing Logs with FunctionGraph Function Templates.....	398
9.3 Generating Metrics from Logs (Beta).....	399
10 Configuration Center.....	402
10.1 Setting LTS Log Collection Quota and Usage Alarms.....	402
10.2 Configuring Log Content Delimiters.....	404
10.3 Setting ICAgent Collection.....	407
11 Querying Real-Time LTS Traces.....	408

1 Granting LTS Permissions to IAM Users

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

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

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

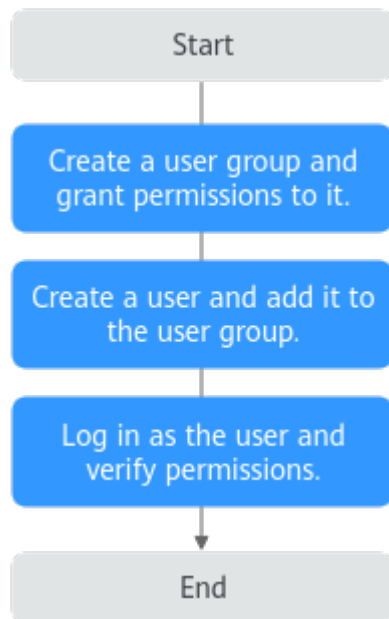
[Figure 1-1](#) shows the process flow of role/policy-based authorization.

Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in [Permissions](#) for LTS.

Process Flow

Figure 1-1 Process of granting LTS permissions



1. Log in to the IAM console. Create a user group on the IAM console and assign the **LTS FullAccess** permissions to the group. For details, see [Creating a User Group and Assigning Permissions](#).

NOTE

If you select the **LTS FullAccess** permissions, the **Tenant Guest** policy that the permission depends on is automatically selected. You also need to grant the **Tenant Administrator** policy for the global service project to the user group.

2. Create a user on the IAM console and add the user to the user group created in [1](#). For details, see [Creating an IAM User](#).
3. Log in to the LTS console as the created user, switch to the authorized region, and verify your permissions by performing operations on the console. For details, see [Logging In as an IAM User](#).

2 Purchasing LTS Resource Packages

LTS offers pay-per-use resource packages for scenarios with stable usage to save costs. During fee settlement, usage is deducted from these packages first. For more billing information, see [Price Calculator](#).

Usage Rules

- Resources used after your resource packages expire are pay-per-use.
- Usage beyond the package quota is pay-per-use.
- The billing cycle of a resource package starts from the effective time you set and ends at 23:59:59 on the same day when the package expires.
- After a resource package expires, its remaining quota will be automatically cleared. For more information, see [How Will My Resource Packages Be Used To Pay for Cloud Services?](#)

Purchasing LTS Resource Packages

Step 1 Log in to the [LTS console](#).

Step 2 On the **Log Management** page, click **Buy Package**.

Step 3 On the **Buy Package** page, set parameters by referring to [Table 2-1](#) or [Table 2-2](#).

 **NOTE**

Cold storage packages are available only to whitelisted users. To use them, you need to enable intelligent cold storage by referring to [Managing Log Streams](#) and [submit a service ticket](#).

Table 2-1 Parameters shown when you select Recommended for Bill As

Parameter	Description
Region	Region where LTS is located. You are advised to select the same region as that of the service application system.
Bill As	Select Recommended .
Package Type	(Whitelist function) You can select read/write traffic, index traffic, standard storage, and cold storage packages.

Parameter	Description
Specification	100 GB is selected by default.
Quantity	Number of resource packages. The value ranges from 1 to 3,000.
Description	<p>The storage space is determined by the selected quantity. For example, if you purchase two resource packages, the storage volume is 100 GB x 2 = 200 GB.</p> <p>NOTE</p> <ul style="list-style-type: none"> On the LTS resource package purchase page, the unit of storage volume is GB-month. In the Billing Center, it is GB-hour. For example, if you purchase a 100 GB storage package (100 GB-month) on LTS, the total storage volume displayed on the resource package page of Billing Center is 72,000 GB, that is, 100 GB x 1 x 24 hours x 30 days = 72,000 GB-hour. If you purchase only one 100 GB read/write traffic package, the total volume is displayed as 100 GB on the resource package page of Billing Center. If you purchase only one 100 GB index traffic package, the total capacity is displayed as 100 GB on the resource package page of Billing Center.
Duration	Select the usage duration (by month or year) of the resource package.
Valid	<ul style="list-style-type: none"> Immediately: Once the payment is complete, the package takes effect immediately and the usage is deducted preferentially from the package. At set time: Set the time when the resource package takes effect, for example, Jul 11, 2023 10:30:00. <p>NOTE If you select a time that is not on the hour, for example, Jul 11, 2023 10:30:00, the system starts deducting the usage from the resource package from the next hour, that is, 11:00:00 on July 13, 2023.</p>
For	<ul style="list-style-type: none"> All enterprise projects: The package can be used by all enterprise projects. Specific enterprise project: The package can be used only by a specified enterprise project. <p>NOTE If Enterprise Project Management Service (EPS) is not enabled, this parameter is unavailable. For details, see Enabling the Enterprise Project Function.</p>

Table 2-2 Parameters shown when you select Calculated for Bill As

Parameter	Description
Region	Region where LTS is located. You are advised to select the same region as that of the service application system.

Parameter	Description
Bill As	<p>Calculated: The usage of read/write traffic, index traffic, standard storage, and cold storage packages is calculated based on the volume of new logs per day (GB/day or TB/day), log retention (days), and standard log retention (days). (Cold storage packages are available only to whitelisted users. You need to set Standard Log Retention (days) only after cold storage is enabled.)</p> <p>Read/write traffic packages and index traffic packages are related to the volume of new logs per day. Standard storage packages and cold storage packages are related to the volume of new logs per day, log retention duration, and standard log retention (days).</p>
Calculation Results	<p>For example, if the volume of new logs per day is 10 GB, the log retention duration is 30 days, the standard retention duration is 7 days, and the default specification (100 GB) is selected for each package, the calculation result for one month is as follows. If TB/day is selected, convert TB to GB.</p> <div data-bbox="703 954 1342 1261" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p>Bill As</p> <p>Recommended Calculated</p> <p>Raw Log Size <input type="text" value="10"/> GB/day</p> <p>Log Retention (days) <input type="text" value="30"/></p> <p>Standard Log Retention (days) <input type="text" value="7"/></p> <hr/> <p>Calculation Results</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;"> <p>● Read/Write ... 100GB * 1</p> <p>● Standard storage 100GB * 1</p> </div> <div style="text-align: center;"> <p>● Index traffic 100GB * 3</p> <p>● Cold Storage 100GB * 3</p> </div> </div> </div> <ul style="list-style-type: none"> For read/write traffic packages: The read/write traffic has a compression ratio of 1:5. The required traffic is $(10 \text{ GB} \times 30 \text{ days})/5 = 60 \text{ GB}$, which is less than 100 GB. Therefore, only one package is required. For index traffic packages: $(10 \text{ GB} \times 30 \text{ days})/100 \text{ GB} = 3$. Therefore, three packages are required. For standard storage packages: The total volume is $10 \text{ GB} \times 7 \text{ days} = 70 \text{ GB}$, which is less than 100 GB. Therefore, only one package is required. For cold storage packages: The cold storage duration is $30 - 7 = 23 \text{ days}$. The number of required packages is $(10 \text{ GB} \times 23 \text{ days})/100 \text{ GB} = 2.3$, which is rounded up to 3. Therefore, three packages are required.
Duration	<p>Select the usage duration (by month or year) of the resource package.</p>

Parameter	Description
Valid	<ul style="list-style-type: none"> • Immediately: Once the payment is complete, the package takes effect immediately and the usage is deducted preferentially from the package. • At set time: Set the time when the resource package takes effect, for example, Jul 11, 2023 10:30:00. <p>NOTE If you select a time that is not on the hour, for example, Jul 11, 2023 10:30:00, the system starts deducting the usage from the resource package from the next hour, that is, 11:00:00 on July 13, 2023.</p>
For	<ul style="list-style-type: none"> • All enterprise projects: The package can be used by all enterprise projects. • Specific enterprise project: The package can be used only by a specified enterprise project. <p>NOTE If Enterprise Project Management Service (EPS) is not enabled, this parameter is unavailable. For details, see Enabling the Enterprise Project Function.</p>

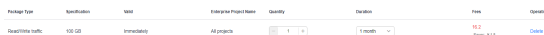
Step 4 Click **Add to List**.

Step 5 Confirm the parameter settings, and click **Buy Now**.

Step 6 On the purchase details page, adjust the quantity and duration as required and click **Pay Now**.

 **NOTE**

A maximum of 5,000 resource packages can be purchased in an order.



Step 7 On the LTS purchase page, select a payment method and click **Pay**. After the payment is complete, you can return to the LTS console.

Step 8 In the upper part of the **Resource Packages** card, click **Purchased** to view information about the purchased packages. For details, see [Resource Packages](#).

----End

3 Log Management

3.1 Overview

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

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

1. Create a log group. For details, see [Managing Log Groups](#).
2. Create a log stream. For details, see [Managing Log Streams](#).
3. Aggregate log groups and streams of multiple accounts for centralized management. For details, see [Setting Multi-Account Log Aggregation](#).
4. On the **Log Management** page, view resource statistics, and the **My Favorites**, **My Favorites(Local Cache)**, and **Recently Visited** lists. For details, see [Viewing Log Management](#).

3.2 Managing Log Groups

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

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

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

Prerequisites

If the IAM users under your account want to use LTS, you need to grant them the permissions required. For details, see [Granting LTS Permissions to IAM Users](#).

Creating a Log Group

Step 1 Log in to the [LTS console](#).

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

Step 3 On the displayed page, set log group parameters by referring to [Table 3-1](#).

Table 3-1 Log group parameters

Parameter	Description
Log Group Name	<ul style="list-style-type: none"> Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period. Collected logs are sent to log streams of the corresponding log groups. If there are too many logs to collect, separate logs into different log groups based on log types, and name log groups in an easily identifiable way.
Enterprise Project Name	<p>Select an enterprise project. You can click View Enterprise Projects to view all enterprise projects.</p> <p>Enterprise projects allow you to manage cloud resources and users by project.</p> <p>NOTE</p> <ul style="list-style-type: none"> An enterprise project can be used only after it is enabled. For details, see Enabling the Enterprise Project Function. Then, resources of this enterprise project can be removed. For details, see Removing Resources from an Enterprise Project.
Log Retention (Days)	<p>Specify the log retention duration for the log group, that is, how many days the logs will be stored in LTS after being reported to LTS.</p> <p>By default, logs are retained for 30 days (customizable for 1 to 365 days).</p> <p>LTS periodically deletes logs based on the configured log retention duration. For example, if you set the duration to 30 days, LTS retains the reported logs for 30 days and then deletes them.</p> <p>NOTE</p> <ul style="list-style-type: none"> Currently, logs of whitelisted users can be retained for 1,095 days. If necessary, submit a service ticket. Creating log groups is free of charge. You are charged based on the log volume. For details, see Price Calculator.

Parameter	Description
Tag	<p>Tag the log group as required. Click Add Tags, enter a tag key and value, and enable Apply to Log Stream.</p> <ul style="list-style-type: none">• To add more tags, repeat this step. A maximum of 20 tags can be added.• To delete a tag, click Delete in the Operation column of the tag.• A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters.• A tag key must be unique.• If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag. <p>NOTE If your organization has configured tag policies for LTS, add tags to log groups, log streams, log ingestion rules, and host groups based on the tag policies. If a tag does not comply with the tag policies, the log group, log stream, ingestion rule, and host group creation may fail. Contact your administrator to learn more about tag policies. For details about tag policies, see Overview of a Tag Policy. For details about tag management, see Managing Tags.</p>
Remark	Enter remarks. The value contains up to 1,024 characters.

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

- In the log group list, you can view information such as the log group name, tags, and log streams.
- Click the log group name to access the log stream details page.
- When multiple log groups are created concurrently, there may be a limit exceeding error.

----End

Modifying a Log Group

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

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

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

Step 3 Click **OK**.

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

----End

Deleting a Log Group

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

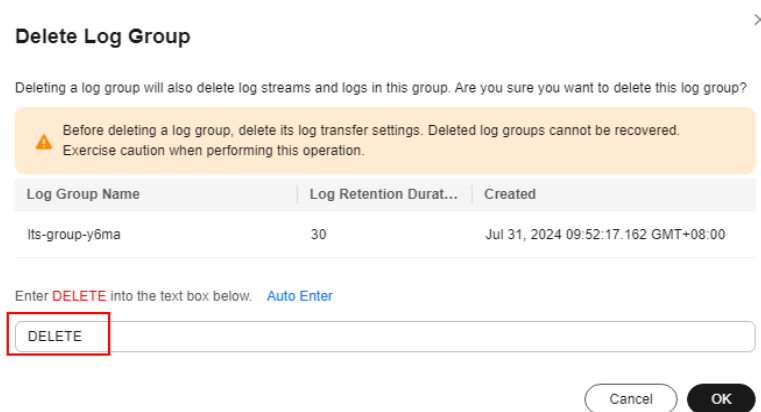
NOTE

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

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

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

Figure 3-1 Deleting a log group



----End

Searching Log Groups/Streams


In the log group list, you can set the following filter criteria:

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

Other Operations

- To check the details of a log group, including the log group name, ID, and creation time, go to the log group list and click **More > Details** in the **Operation** column of the desired log group.
- If you have enabled ICAgent diagnosis by referring to [Setting ICAgent Collection](#), you can click **More > ICAgent Collect Diagnosis** in the

Operation column of the target log group to check its ICAgent's exceptions, overall status, and collection monitoring.

- To download all displayed information about a log group to the local PC, click  next to the search box.

3.3 Managing Log Streams

LTS manages logs by log stream. Collected logs of different types are classified and stored in different log streams for easier log management. If there are a large number of logs, you can create multiple log streams and name them for quick log search. For example, you can sort operation logs and access logs into different log streams, making it easier to find specific logs when you need them. You can add tags to log streams to help O&M personnel manage services.


A maximum of 100 log streams can be created in a log group. If you cannot create a log stream, delete unnecessary log streams before creating new ones, or create log streams in another log group.

Prerequisites

You have created a log group.

Creating a Log Stream

Step 1 Log in to the [LTS console](#). The **Log Management** page is displayed by default.

Step 2 Click  on the left of the target log group.

Step 3 Click **Create Log Stream**. On the displayed page, set log stream parameters by referring to [Table 3-2](#).

NOTE

If your organization has configured tag policies for LTS, add tags to log groups, log streams, log ingestion rules, and host groups based on the tag policies. If a tag does not comply with the tag policies, the log group, log stream, ingestion rule, and host group creation may fail. Contact your administrator to learn more about tag policies. For details about tag policies, see [Overview of a Tag Policy](#). For details about tag management, see [Managing Tags](#).

Table 3-2 Log stream parameters

Parameter	Description
Log Group Name	The name of the target log group is displayed by default.
Log Stream Name	Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period.

Parameter	Description
Enterprise Project Name	<p>Select the required enterprise project. The default value is default. You can click View Enterprise Projects to view all enterprise projects.</p> <p>NOTE</p> <ul style="list-style-type: none"> • An enterprise project can be used only after it is enabled. For details, see Enabling the Enterprise Project Function. • Then, resources of this enterprise project can be removed. For details, see Removing Resources from an Enterprise Project.
Log Storage	<p>If this function is disabled, Log Retention (Days) cannot be enabled.</p> <ul style="list-style-type: none"> • If enabled, logs will be stored in the search engine and all log functions are available. • If disabled, logs will not be stored to LTS. This saves on index traffic and storage costs, but disables log search, analysis, alarm, consumption, and processing. You will only be allowed to use metric generation and log transfer functions.
Log Retention (Days)	<p>Specify the log retention duration for the log stream, that is, how many days the logs will be stored in LTS after being reported to LTS.</p> <p>By default, logs are retained for 30 days (customizable for 1 to 365 days).</p> <ul style="list-style-type: none"> • If you enable Log Retention (Days) for the log stream, logs are retained for the duration set for the log stream. • If you disable Log Retention (Days) for the log stream, logs are retained for the duration set for the log group.
Tag	<p>You can tag log streams as required. Click Add Tags and enter a tag key and tag value.</p> <p>NOTE</p> <ul style="list-style-type: none"> • To add more tags, repeat this step. A maximum of 20 tags can be added. • To delete a tag, click Delete in the Operation column of the tag. • A tag key can contain up to 128 characters, and a tag value can contain up to 255 characters. • A tag key must be unique. • If a tag is used by a transfer task, you need to modify the task configuration after deleting the tag.
Anonymous Write	<p>Anonymous write is disabled by default. Only logs reported by Android, iOS, applets, and browsers can be written anonymously. To use this function, submit a service ticket to add your account to the whitelist.</p> <p>If anonymous write is enabled for a log stream, no valid authentication is required, which may lead to the generation of dirty data.</p>

Parameter	Description
Remark	Enter remarks. The value contains up to 1,024 characters.

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

 **NOTE**

- You can view the log stream billing status. For details, see [Price Calculator](#).
- The function of reporting SDRs by log stream is in Friendly User Test (FUT). You can [submit a service ticket](#) to enable it.

----End

Modifying a Log Stream

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

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

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

 **NOTE**

- If you disable **Log Retention (Days)**, the log stream will inherit the log retention setting of the log group.
- If you enable **Log Retention (Days)**, you can set the log retention duration specifically for the log stream.
- The logs that exceed the retention period will be automatically deleted. You can transfer logs to OBS buckets for long-term storage.
- Currently, only whitelisted users can [submit service tickets](#) to apply for extending the log retention period to 1,095 days. A test is required to evaluate whether the underlying resources in your regions support 1,095-day retention.

Step 3 Click **OK**.

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

----End

Deleting a Log Stream

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

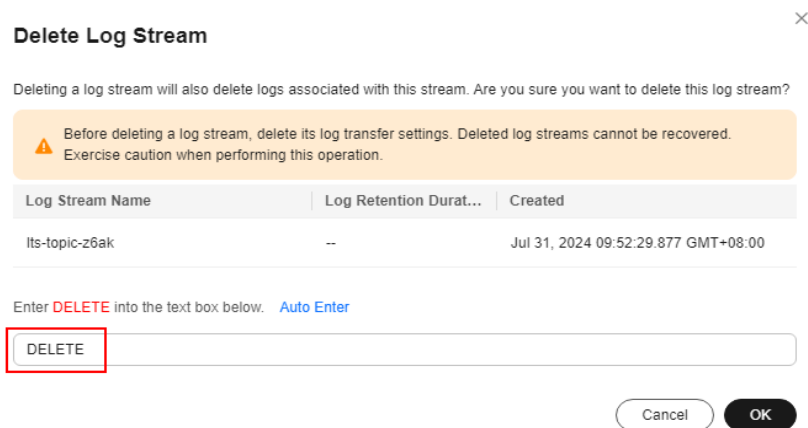
 NOTE

- 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.

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

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

Figure 3-2 Deleting a log stream



----End

Other Operations

- Adding a log stream to favorites
Click **More > Edit** in the **Operation** column of a log stream. On the displayed dialog box, enable **My Favorites** and/or **My Favorites(Local Cache)**. The stream is then displayed in the **My Favorites/My Favorites(Local Cache)** list.
- Viewing details
Click **More > Details** in the **Operation** column of a log stream to view its details, including its name, ID, and creation time.
- Collection diagnosis: If you have enabled ICAgent diagnosis by referring to [Setting ICAgent Collection](#), you can click **More > ICAgent Collect Diagnosis** in the **Operation** column of the target log stream to check its ICAgent's exceptions, overall status, and collection monitoring.

3.4 Viewing Log Management

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

Resource Statistics

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

- Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.
- Step 2** Under **Overview**, click **Details** in the upper right corner of the **Statistics** area to access the resource statistics details page.
- Step 3** Select a time range as required. By default, resource statistics display log resource data of one week (from now).

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

NOTE

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

Step 4 View the resource statistics.

- **Read/Write:** LTS charges for the amount of compressed log data read from and written to LTS. Generally, the log compression ratio is 5:1.
- **Index Traffic - Standard:** Raw logs are full-text indexed (delimited) by default for log search. When logs are written to databases, traffic fees are charged at a time.
- **Standard Storage Volume:** Space used for storing compressed logs, indexes, and copies is billed. The space is roughly the size of the raw logs.


NOTE

Standard storage statistics indicate the latest total storage volume within a specified time range.

- **Raw Log Traffic:** size of raw logs.
- **Basic Transfer Traffic:** traffic for transferring logs to OBS, DMS, and DIS. Such transfers do not require field mapping and consume less computing power. This parameter is displayed only when log transfer billing is enabled.
- **Advanced Transfer Traffic:** traffic for transferring logs to DWS and DLI. Such transfers require field mapping and consume more computing power. This parameter is displayed only when log transfer billing is enabled.

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

- For a new log group or log stream, resource statistics will be collected in at least one hour.

- Click the name of one of the top 100 log groups to query its log stream resource statistics.
- Click  to download the resource statistics of the log groups and streams.


 **NOTE**

The downloaded files are in **.CSV** format.

----End

Alarm Statistics and Latest Alarms

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

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

Log Applications

LTS provides multiple log applications under **Overview** on the **Log Management** page. These log applications are out-of-the-box dashboard templates for quick log analysis.

- **ELB Log Center**: Elastic Load Balance (ELB) logs can be ingested to LTS and displayed in the ELB dashboard templates.
- **APIG Log Center**: API Gateway (APIG) logs can be ingested to LTS and displayed in the APIG dashboard templates. For details, see [APIG Dashboard Templates](#).
- **VPC Flow Log Center**: Virtual Private Cloud (VPC) logs can be ingested to LTS and displayed in the VPC dashboard templates. For details, see [VPC Dashboard Template](#).
- **CFW Log Center**: Cloud Firewall (CFW) logs can be ingested to LTS and displayed in the CFW dashboard templates. For details, see [CFW Dashboard Templates](#).
- **CTS Log Center**: Cloud Trace Service (CTS) logs can be ingested to LTS but cannot be displayed in the CTS dashboard templates. For details, see [Ingesting CTS Logs to LTS](#).
- **Multi-Account Log Center**: Log streams of multiple accounts can be copied to a specified account for central storage and analysis of logs from those accounts. For details, see [Setting Multi-Account Log Aggregation](#).

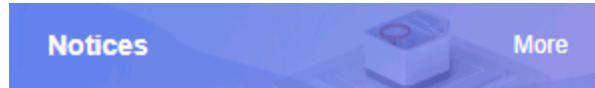
Log Groups

Log groups and log streams are listed in **Log Groups**. For more information, see [Managing Log Groups](#) and [Managing Log Streams](#).

Notices

This area displays the new functions and news of LTS.

To view more function descriptions, click [More](#).



Multiple characters are supported for character separation. **NEW**

Apr 30, 2023

Alarm rules can be edited in batches and temporarily closed. **NEW**

Mar 30, 2023

Self-built K8s log ingestion **NEW**

Feb 28, 2023

My Favorites/My Favorites (Local Cache)


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

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

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

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

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

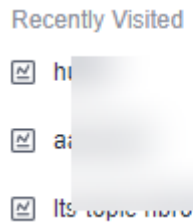
- Step 1** In the **Log Groups** list, click  on the left of log group **lts-test**.
- Step 2** Click **More > Edit** in the **Operation** column of the target log stream. On the displayed dialog box, enable **My Favorites** and/or **My Favorites(Local Cache)** and click **OK**.
- Step 3** After the log stream is added to favorites, it is displayed in **My Favorites/My Favorites(Local Cache)** on the right.

----End

Recently Visited

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

Figure 3-3 Recently visited



FAQ

This area displays frequently asked questions. To view more, click [More](#).

Video Introduction

There are video tutorials covering LTS functions, ECS text log ingestion, CCE application log ingestion, and ICAgent installation.

3.5 Setting Multi-Account Log Aggregation

The multi-account log center allows you to copy log streams of multiple accounts to a specified account to centrally store and analyze logs across accounts. This meets the requirements in scenarios such as security compliance and centralized analysis.

NOTE

Currently, this function is available only in regions CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, CN South-Guangzhou, LA-Sao Paulo1, CN North-Beijing4, CN Southwest-Guiyang1, LA-Santiago, and AF-Cairo. To use this function in other regions, [submit a service ticket](#).

Background

- Corporate groups often use Landing Zone, a multi-account solution that allows business departments to use different accounts, to enhance security by isolating permissions and resources.
- Their security compliance departments expect to collect logs centrally, and aggregate key logs of different accounts of each business department into one log account for centralized storage and analysis to meet the security compliance audit requirements of different countries and regions.
- To meet operations analysis requirements, their operations departments may also expect to aggregate key logs of different accounts of each business department into one log account for centralized storage and analysis, to facilitate unified big data processing and visual display.

Solution

- The Organizations service helps you govern multiple accounts within your organization. It enables you to consolidate multiple Huawei Cloud accounts into an organization that you create and centrally manage these accounts. You can use Service Control Policies (SCPs) to control the maximum available permissions for all accounts in your organization. This helps you better meet the service security and compliance requirements of your business.
- LTS provides the multi-account log center based on Organizations. You can log in to Organizations using the management account and specify a member account in your organization as the delegated administrator account of the trusted service LTS, and then go to the LTS console to copy the log streams of another member account to the management or delegated administrator account. In this way, logs of multiple accounts are aggregated into one account.
- The target log groups or streams are generated by copying the source log groups or streams from a member account to the management or delegated administrator account. Therefore, they do not interfere with the source log groups or streams of the member account. You can configure transfer, consumption, and processing tasks for them separately.

Prerequisites

- An organization has been created. For details, see [Creating an Organization](#).
- LTS has been set as a trusted service. For details, see [Enabling or Disabling a Trusted Service](#).
- The management or delegated administrator account has been granted the read-only permission on the Organizations service. For details about delegated account operations, see [Specifying, Viewing, or Removing a Delegated Administrator](#). For details about how to grant permissions, see [Creating an IAM User and Granting Organizations Permissions](#).

Setting a Multi-Account Log Aggregation Task

Step 1 Log in to the console using the management or delegated administrator account and choose **Log Tank Service** in the navigation pane. The **Log Management** page is displayed.

Step 2 Click **Multi-Account Log Center** under **Log Applications**.

Step 3 On the displayed page, enable **Log receiving status**, select a member account on the left, and select its source log groups or streams on the right. You can also customize the names of the target log groups or streams.

NOTE

- To stop using multi-account log aggregation, simply disable **Log receiving status**. In this case, all aggregation settings become invalid, and logs in the source log streams stop being aggregated to the target log streams.
- The number of log streams to be created cannot exceed the limit. For details, see the constraints described in [Basic Resources](#).

Step 4 Click **OK**. It takes about 5 minutes to create the aggregation settings for the account. Refresh the page later to view the settings.

 **NOTE**

- By default, a target log stream is initialized using the index and structuring configurations of the log stream of the source account. After the aggregation is configured, subsequent index and structuring configuration changes of the source will not be synchronized to the target.
- Deleting the log groups or streams of the source account does not affect their target equivalents.
- After you deselect a log group or stream in **Aggregation Settings** and click **OK**, its logs will not be aggregated to the target log group or stream.

----End

4 Log Ingestion

4.1 Overview

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

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

NOTE

Before configuring log ingestion, ensure that ICAgent collection is enabled by referring to [Setting LTS Log Collection Quota and Usage Alarms](#).

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

Data Sources

[Table 4-1](#) lists the sources of logs that can be reported to LTS.

Table 4-1 Data sources

Type	Scenario	Ingestion Method
Application	Program output	Ingesting CCE Application Logs to LTS
	Access logs	Ingesting WAF Logs to LTS

Type	Scenario	Ingestion Method
OS	Linux	<ul style="list-style-type: none"> Installing ICAgent (Intra-Region Hosts) Installing ICAgent (Extra-Region Hosts)
	Windows	
	Docker files	
	Docker output	
Database	MySQL	<ul style="list-style-type: none"> Ingesting TaurusDB Logs to LTS Ingesting RDS for MySQL Logs to LTS
	SQL Server	Ingesting RDS for SQL Server Logs to LTS
	PostgreSQL	Ingesting RDS for PostgreSQL Logs to LTS
	GaussDB	Ingesting GaussDB(DWS) Logs to LTS
	GeminiDB	<ul style="list-style-type: none"> Ingesting GeminiDB Logs to LTS Ingesting GeminiDB Mongo Logs to LTS Ingesting GeminiDB Cassandra Logs to LTS
Standard protocol	HTTP polling	Using Kafka to Report Logs to LTS
	Syslog	Using Kafka to Report Logs to LTS
	Kafka	Using Kafka to Report Logs to LTS
Third party	Logstash	Using Kafka to Report Logs to LTS
	Flume	Using Kafka to Report Logs to LTS
	Beats	Using Kafka to Report Logs to LTS
Cloud service	Logs of Huawei Cloud services, such as ECS and CCE	Ingesting Cloud Service Logs to LTS

4.2 Using ICAgent to Collect Logs

4.2.1 Overview

You can use ICAgent to collect logs to LTS. When creating a log ingestion task, you can customize collection configurations, such as parsing, whitelist, and blacklist rules, and raw log uploading settings. An ICAgent collection configuration defines the process of collecting logs of the same type from a server, parsing them, and sending them to a specified log stream.

ICAgent Collection Principles

Once ICAgent is installed, LTS listens to the corresponding log files in real time. After receiving a collection configuration delivered by the LTS console, ICAgent periodically parses the configuration, obtains the collection path, matches the path on the node, monitors the corresponding files of the node, and detects the file changes through polling and inotify mechanisms.

Upon detecting a file change, ICAgent reads the file content, divides the content into blocks, and sends the blocks to the processing module for log processing, such as single-line, multi-line, structuring, splitting, and tagging. Then, ICAgent submits the processed task to the sending task pool to report the task to LTS.

ICAgent Installation

To collect host metrics, container metrics, node logs, container logs, and standard output logs from hosts, you need to install ICAgent on the hosts.

For details, see [Installing ICAgent \(Intra-Region Hosts\)](#) and [Installing ICAgent \(Extra-Region Hosts\)](#).

NOTE

- An intra-region host is in the same region as the LTS console, for example, both in CN-Hong Kong.
- An extra-region host is in a different region than the LTS console or provided by a third party.

Advantages

- Collecting log data in non-intrusive mode as log files: You do not need to modify application code, and log collection does not affect application running.
- Handling various exceptions during log collection: Security measures such as proactive retry and local cache are taken when a network or server exception occurs.
- Centralized management: After installing ICAgent, you only need to set configurations such as host groups and ICAgent collection on the LTS console.
- Comprehensive self-protection mechanisms: ICAgent is designed with strict limitations and protective measures regarding CPU, memory, and network

usage, to minimize its impact on the performance of other services sharing the same server.

ICAgent Structuring Parsing Rules

Before configuring log ingestion, get to know the structuring parsing rules of ICAgent collection to facilitate your operations. LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream. For details, see [Setting ICAgent Structuring Parsing Rules](#).

4.2.2 Installing ICAgent (Intra-Region Hosts)

An intra-region host is in the same region as your LTS console, for example, both in CN North-Beijing4. To use LTS to collect logs (such as host metrics, container metrics, node logs, container logs, and standard output logs) from intra-region hosts, you need to install ICAgent on the hosts. ICAgent is a log collection tool for LTS. It runs on hosts where logs need to be collected.

Prerequisites

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

ICAgent Installation Constraints

- Linux: ICAgent can only be installed on hosts running [supported Linux OSs](#).
- Windows: ICAgent can only be installed on hosts running the following 64-bit Windows OSs:

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

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

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

NOTE

ICAgent installed on Windows hosts cannot be upgraded or uninstalled on the **Host Management** page. To use a newer ICAgent version, uninstall the original one and then install the newer version. To uninstall ICAgent, go to the `\ICProbeAgent\bin\manual\win` directory where the ICAgent installation package was decompressed, and double-click the script named `uninstall.bat`. When message **ICAgent uninstall success** is displayed, the uninstallation is successful.

Installation Methods

There are two methods to install ICAgent.

Table 4-2 Installation methods

Method	Scenario
Initial installation	<p>You can use this method to install ICAgent on a host that has no ICAgent installed.</p> <p>Run the ps -aux grep icagent command on the host to check whether there is an ICAgent process. If no, the ICAgent has not been installed.</p> <ul style="list-style-type: none"> • Initial Installation (Linux) • Initial Installation (Windows)
Inherited installation (supported only for Linux hosts)	<p>When ICAgent has already been installed on one host but needs to be installed on multiple hosts, you can use this method.</p> <ul style="list-style-type: none"> • Inherited Installation (Linux) • Batch Inherited Installation (Linux)



Initial Installation (Linux)

Step 1 If you set **Installation Mode** to **Create an agency**, you need to create an IAM agency in advance.

1. Log in to the IAM console.
2. In the navigation pane, choose **Agencies**.
3. Click **Create Agency** in the upper right corner to create an agency by referring to [Cloud Service Agency](#). Set the parameters as follows:
 - a. **Agency Type**: Select **Cloud service**.
 - b. **Cloud Service**: Select **Elastic Cloud Server (ECS) and Bare Metal Server (BMS)**.
 - c. **Validity Period**: Select **Unlimited**.
 - d. **Permissions**: Select both **LTS Administrator** and **APM Administrator**. The authorization takes effect 15 to 30 minutes later.
 - e. **Scope**: Select **Region-specific projects**.
4. After the agency is created, make its settings take effect.
 - a. Log in to the ECS console.
 - b. Click the ECS where ICAgent is to be installed. The ECS details page is displayed.

 **NOTE**

You can set an agency when purchasing an ECS server: Click **Buy ECS** on the ECS console. In the **Advanced Settings** area, select an agency from the **Agency** drop-down list. Set other parameters and click **Submit**.

- c. In the **Management Information** area, click  next to **Agency**, select the created agency, and click  for the agency to take effect. For more information about agencies, see [Account Delegation](#).

Step 2 Log in to the management console and choose **Management & Deployment > Log Tank Service**.

Step 3 Choose **Host Management > Hosts** in the navigation pane.

Step 4 Click **Install ICAgent** in the upper right corner.

 **NOTE**

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

Table 4-3 Installing ICAgent

Parameter	Description	Example
Host	<p>Intra-region hosts is selected by default. Check whether the host whose logs need to be collected is in or out of the region.</p> <p>NOTE</p> <ul style="list-style-type: none"> An intra-region host is in the same region as the LTS console, for example, both in CN-Hong Kong. An extra-region host is not in the same region as the LTS console, for example, a host in another Huawei Cloud region or provided by a third party. 	-
OS	<p>Linux is selected by default.</p>	-
Installation Mode	<ul style="list-style-type: none"> If you select Obtain AK/SK, you need to obtain the AK/SK in advance. An AK is used together with an SK to sign requests cryptographically, ensuring that the requests are secret, complete, and correct. For details, see How Do I Obtain an Access Key (AK/SK)? <p>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.</p> <ul style="list-style-type: none"> If you select Create an agency, you do not need to obtain and enter the AK/SK. ICAgent automatically obtains the AK/SK during agency creation. For details, see Step 1. 	-

Step 5 On the **Install ICAgent** page, click **Copy Command** to copy the ICAgent installation command.

Step 6 Perform the following steps based on site requirements (a Huawei Cloud ECS is used as an example). For details, see [Logging In to a Linux ECS Using VNC](#).

1. Log in to the ECS console.
2. Click **Remote Login** in the **Operation** column of the target ECS where ICAgent is to be installed.

3. In the **Logging In to a Linux ECS** dialog box, click **Log In** in the **Other Login Modes** area.
4. On the displayed page, enter username **root** and the password set during ECS purchase.
5. After logging in to the ECS, run the following command to install ICAgent:
 - If you select **Obtain AK/SK for Installation Mode**, run the ICAgent installation command and enter the obtained AK/SK as prompted. (If you have manually replaced the AK/SK when copying the command, the system will not prompt you to enter the AK/SK.)
 - If you select **Create an agency for Installation Mode**, run the ICAgent installation command. You do not need to enter the AK/SK since ICAgent automatically obtains it.
6. When message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host.

Figure 4-1 Installation command output

```
ecs-test-diy login: root
Password:
Last failed login: Wed Jul 18 09:57:56 CST 2024 on tty1
There were 2 failed login attempts since the last successful login.

Welcome to Huawei Cloud Service

[root@ecs-test-diy ~]# s
install.sh > auto agent i
Enter the AK:
JK05
Enter the SK:
para1 is empty
2024-07-18 10:08:44 [INFO] : start to install ICAgent.
2024-07-18 10:08:44 [INFO] : begin to download install package from iagent-c
2024-07-18 10:08:46 [INFO] : check sha256 success,start
2024-07-18 10:08:47 [INFO] : download success.
2024-07-18 10:08:47 [INFO] : start install package.
Start install ICAgent...
Screen
Start
change syslog port to 20891
serviceRestart
no cronTab for root
starting ICAgent
ICAgent install success.
```

- Step 7** Choose **Host Management > Hosts** in the navigation pane of the LTS console and check whether the ICAgent status is **Running**.

Figure 4-2 Hosts


-----End

Initial Installation (Windows)

- Step 1** Click **Install ICAgent** in the upper right corner.
- Step 2** Set **Host** to **Intra-region hosts**.
- Step 3** Set **OS** to **Windows**.
- Step 4** You can download it to the local PC by clicking the name of the package or visiting the download URL.
- Step 5** Save the ICAgent installation package to a directory on the target host, for example, **C:\ICAgent**, and decompress the package.

- Step 6** Obtain an AK/SK pair. For details, see [How Do I Obtain an Access Key \(AK/SK\)?](#)
- Step 7** On the **Install ICAgent** page, click **Copy Command** to copy the ICAgent installation command to the local PC and replace the AK/SK in the command with the obtained one.
- Step 8** Open the Command Prompt, go to the directory where the ICAgent installation package is decompressed, and run the copied command.

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

 **NOTE**

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

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

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

----End

Inherited Installation (Linux)

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

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

```
bash /opt/oss/servicemgr/ICAgent/bin/remotelInstall/remote_install.sh -ip x.x.x.x
```
2. Enter the password for user **root** of the host when prompted.

 NOTE

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

Batch Inherited Installation (Linux)

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

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

Prerequisites

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

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

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

 NOTE

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

Procedure

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

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

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

```
batch install begin  
Please input default passwd:
```

```
send cmd to 192.168.0.109
send cmd to 192.168.0.39
2 tasks running, please wait...
2 tasks running, please wait...
2 tasks running, please wait...
End of install agent: 192.168.0.39
End of install agent: 192.168.0.109
All hosts install icagent finish.
```

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

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

4.2.3 Installing ICAgent (Extra-Region Hosts)

An extra-region host refers to a host located outside the current Huawei Cloud region or a non-Huawei Cloud host. This category includes hosts in self-built Internet Data Centers (IDCs), those provided by third parties, and those in other Huawei Cloud regions. To collect logs from extra-region hosts to LTS, ensure that the hosts can communicate with LTS located in the current Huawei Cloud region, and then install ICAgent on the hosts. ICAgent is a log collection tool for LTS. It runs on hosts where logs need to be collected.

Extra-region hosts use two types of network channels to report logs to LTS:

- **Public network:** An extra-region host connected to the public network can communicate with and report logs to LTS in the current Huawei Cloud region through the public network. However, for security reasons, private lines are usually preferred in actual production environments.

NOTE

If you select **Public network** when installing ICAgent on an extra-region host, ensure that the region support log reporting via public networks.

- **Private line:** Extra-region hosts connect to LTS in the current Huawei Cloud region through a jump server or VPCEP, offering greater security and stability. In this scenario, extra-region hosts cannot communicate with LTS in the current region by default, and ICAgent installed on these hosts cannot directly access the network segment used by the Huawei Cloud management plane to report logs. Therefore, you need to configure a network connection solution to use a jump server or VPCEP to connect to the LTS backend and forward data to LTS.
 - **Jump server:** functions as a data forwarder and forwards the data collected by ICAgent from extra-region hosts to LTS. This solution is suitable for tests or scenarios with low log traffic. VPCEP is recommended for scenarios with high log traffic.
 - **VPCEP:** provides convenient and secure channels to connect to LTS in the current region, enabling resources in the VPC to access VPCEP without the need for EIPs. This solution reduces the risks of data transmission on public networks and improves the transmission security and efficiency.

Prerequisites

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

Installation Methods

There are two methods to install ICAgent.

Table 4-4 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 Choose **Host Management** > **Hosts** in the navigation pane.

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

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

Step 4 Set **Network Connectivity**. For extra-region hosts to report logs to LTS in the current region, you are advised to select **Private line** for higher stability and reliability.

- If you select **Public network**, start from [Step 6](#).
- If you select **Private line**, start from [Step 5](#).

Step 5 Set **LTS Backend Connection**. If you select **Private line** in the previous step, the extra-region host cannot communicate with LTS in the current region by default, and ICAgent installed on the host cannot directly access the network segment used by the Huawei Cloud management plane to report logs. Therefore, you need to configure a network connection solution to use a jump server or VPCEP to connect to the LTS.

- If you set **LTS Backend Connection** to **VPCEP**:

Configure a VPCEP domain name. With the assistance of Huawei Cloud network engineers, configure DNS domain name resolution rules in other regions to resolve VPCEP domain names to specified IP addresses. Then, copy the command as prompted on the **Install ICAgent** page.

```
ping {VPCEP domain name}
```

Run this command on the host you want to collect logs from. If the ping command succeeds, the network configuration is correct. Proceed to [Step 6](#).

- If you set **LTS Backend Connection** to **Jump server**:

a. Create a Linux ECS as a jump server.

Log in to the ECS console and create a Linux ECS. For details, see [Purchasing an ECS](#). If you have an ECS that meets the requirements for use as a jump server, skip this step.

 NOTE

- The minimum specifications for the ECS are 1 vCPU and 1 GB of memory. The recommended specifications are 2 vCPUs and 4 GB of memory. You are advised to use an image of **CentOS 6.5 64bit** or later version.
 - If the jump server communicates with the extra-region host over the public network, an EIP must be enabled. Conversely, when it uses a VPC peering connection, an EIP is not required.
 - The region of the jump server must be the same as the current region of LTS.
- b. Add security group rules for the jump server and enable the corresponding inbound ports to ensure data connectivity between the extra-region hosts and the jump server.
- i. Log in to the ECS console, check the ECS list, and locate the ECS that you created as the jump server.
 - ii. Click its name to go to the ECS details page. Click the security group name to access the security group details page.
 - iii. Click the **Inbound Rules** tab and click **Add Rule**. Set the ports by referring to [Table 4-5](#). Set other parameters based on your network requirements. For details, see [Adding a Security Group Rule](#).

Table 4-5 Security group rule

Ac tio n	Prot ocol	Port	Description
All ow	TCP	8149,8102,8923,3020 0,30201,80	Ports used by ICAgent to send data to the jump server, ensuring data connectivity between hosts in other regions and the jump server.

- c. Return to the ECS list, locate the ECS created in [Step 5.a](#), and view its private IP address and EIP (available if an EIP has been enabled).
- d. Go back to the LTS console. On the **Install ICAgent** page, enter the obtained private IP address of the jump server to generate its SSH tunneling command.

 NOTE

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

- e. On the **Install ICAgent** page, click **Copy Command** to copy the SSH tunneling command.

```
ssh -f -N -L {Private IP address of the jump server}:8149:{LTS reporting IP address}:8149 -L {Private IP address of the jump server}:8102:{LTS reporting IP address}:8102 -L {Private IP address of the jump server}:8923:{LTS reporting IP address}:8923 -L {Private IP address of the jump server}:30200:{LTS reporting IP address}:30200 -L {Private IP address of the jump server}:30201:{LTS reporting IP address}:30201 -L {Private IP address of the jump server}:80:icagent-{Region}://{OBS domain name}:80 {Private IP address of the jump server}
```

- f. Log in to the jump server as user **root** and run the copied SSH tunneling command.

- g. Run the `netstat -lnp | grep ssh` command to check whether the corresponding TCP ports are being listened to. If the command output similar to [Figure 4-3](#) is returned, the ports are open.

Figure 4-3 Open TCP ports

```
root@ecs-debc-qff-tiaobanji ~]# netstat -lnp | grep ssh
tcp        0      0 192.168.0.79:8102    0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:80     0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:8149   0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN      1772/sshd
tcp        0      0 192.168.0.79:30200  0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:30201  0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:8923   0.0.0.0:*           LISTEN      1994/sshd
tcp6       0      0 :::22               :::*                 LISTEN      1772/sshd
```

NOTE

If the jump server powers off and restarts, run the `netstat -lnp | grep ssh` command again.

- h. On the **Install ICAGENT** page, enter the DC and the connection IP address of the jump server.
- **DC:** Specify a name for the data center of the host so it is easier to find the host. Enter up to 64 characters. Use only digits, letters, hyphens (-), and underscores (_).
 - **Connection IP:** If the jump server communicates with the extra-region host via EIP connection, enter the EIP of the jump server. Conversely, when using a VPC peering connection, enter the internal IP address (private IP address) of the VPC where the jump server locates. For the EIP and private IP address, see [Step 5.c](#).

Step 6 Obtain an AK/SK. For details, see [How Do I Obtain an Access Key \(AK/SK\)?](#) On the **Install ICAGENT** page, copy the ICAGENT installation command and replace the AK/SK in the command with the obtained one.

Step 7 Log in to the extra-region host as user **root** (by using a remote login tool such as PuTTY) and run the copied command.

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

NOTE

If the installation fails, uninstall ICAGENT and reinstall it. If the reinstallation fails, contact technical support.

----End

Initial Installation (Windows)

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

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

Step 3 Set **Host** to **Extra-region hosts**.

Step 4 Set **OS** to **Windows**.

Step 5 Set **Network Connectivity**. Extra-region hosts report logs to LTS via a public network or a private line. The latter is recommended for higher stability and reliability.

- If you select **Public network**, start from [Step 7](#).
- If you select **Private line**, start from [Step 6](#).

Step 6 Set **LTS Backend Connection**. If you select **Private line** in the previous step, the extra-region host cannot communicate with LTS in the current region by default, and ICAgent installed on the host cannot directly access the network segment used by the Huawei Cloud management plane to report logs. Therefore, you need to configure a network connection solution to use a jump server or VPCEP to connect to the LTS.

- If you set **LTS Backend Connection** to **VPCEP**:

Configure a VPCEP domain name. With the assistance of Huawei Cloud network engineers, configure DNS domain name resolution rules in other regions to resolve VPCEP domain names to specified IP addresses. Then, copy the command as prompted on the **Install ICAgent** page.

```
ping {VPCEP domain name}
```

Run this command on the host you want to collect logs from. If the ping command succeeds, the network configuration is correct. Proceed to [Step 7](#).

- If you set **LTS Backend Connection** to **Jump server**:

a. Create a Linux ECS as a jump server.

Log in to the ECS console and create a Linux ECS. For details, see [Purchasing an ECS](#). If you have an ECS that meets the requirements for use as a jump server, skip this step.

 **NOTE**

- The minimum specifications for the ECS are 1 vCPU and 1 GB of memory. The recommended specifications are 2 vCPUs and 4 GB of memory. You are advised to use an image of **CentOS 6.5 64bit** or later version.
 - If the jump server communicates with the extra-region host over the public network, an EIP must be enabled. Conversely, when it uses a VPC peering connection, an EIP is not required.
 - The region of the jump server must be the same as the current region of LTS.
- b. Add security group rules for the jump server and enable the corresponding inbound ports to ensure data connectivity between the extra-region hosts and the jump server.
- Log in to the ECS console, check the ECS list, and locate the ECS that you created as the jump server.
 - Click its name to go to the ECS details page. Click the security group name to access the security group details page.
 - Click the **Inbound Rules** tab and click **Add Rule**. Set the ports by referring to [Table 4-6](#). Set other parameters based on your network requirements. For details, see [Adding a Security Group Rule](#).

Table 4-6 Security group rule

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

- c. Return to the ECS list, locate the ECS created in [Step 6.a](#), and view its private IP address and EIP (available if an EIP has been enabled).
- d. Go back to the LTS console. On the **Install ICAgent** page, enter the obtained private IP address of the jump server to generate its SSH tunneling command.

NOTE

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

- e. On the **Install ICAgent** page, click **Copy Command** to copy the SSH tunneling command.


```
ssh -f -N -L {Private IP address of the jump server}:8149:{LTS reporting IP address}:8149 -L {Private IP address of the jump server}:8102:{LTS reporting IP address}:8102 -L {Private IP address of the jump server}:8923:{LTS reporting IP address}:8923 -L {Private IP address of the jump server}:30200:{LTS reporting IP address}:30200 -L {Private IP address of the jump server}:30201:{LTS reporting IP address}:30201 -L {Private IP address of the jump server}:80:icagent-{Region}:[OBS domain name]:80 {Private IP address of the jump server}
```
- f. Log in to the jump server as user **root** and run the copied SSH tunneling command.
- g. Run the **netstat -lnp | grep ssh** command to check whether the corresponding TCP ports are being listened to. If the command output similar to [Figure 4-4](#) is returned, the ports are open.

Figure 4-4 Open TCP ports

```
root@ecs-debc-qff-tiaobanji ~# netstat -lnp | grep ssh
tcp        0      0 192.168.0.79:8102    0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:80     0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:8149   0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 0.0.0.0:22          0.0.0.0:*           LISTEN      1772/sshd
tcp        0      0 192.168.0.79:30200  0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:30201  0.0.0.0:*           LISTEN      1994/sshd
tcp        0      0 192.168.0.79:8923   0.0.0.0:*           LISTEN      1994/sshd
tcp6       0      0 :::22               :::*                LISTEN      1772/sshd
```

NOTE

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

Step 7 Click the link on the **Install ICAgent** page to download the ICAgent installation package.

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

Step 9 Obtain an AK/SK and save it to replace the AK/SK in the installation command. For details, see [How Do I Obtain an Access Key \(AK/SK\)?](#)

If you set **LTS Backend Connection** to **Jump Server**, you also need to set **Connection IP**.

Connection IP: If the jump server communicates with the extra-region host via EIP connection, enter the EIP of the jump server. Conversely, when using a VPC peering connection, enter the internal IP address (private IP address) of the VPC where the jump server locates. For the EIP and private IP address, see [Step 6.c](#).

Step 10 On the **Install ICAgent** page, click **Copy Command** to copy the ICAgent installation command.

Step 11 Log in to the Windows host, open the Command Prompt, go to the directory where the ICAgent installation package is decompressed, and run the ICAgent installation command.

If the message **Service icagent installed successfully** is displayed, the installation is successful. You can then choose **Host Management > Hosts** in the navigation pane of the LTS console to check the ICAgent status.

 **NOTE**

If the installation fails, uninstall ICAgent and reinstall it. If the reinstallation fails, contact technical support.

----End

Creating Multiple Jump Servers for Load Balancing Using ELB

A single jump server may encounter a single point of failure (SPOF), potentially leading to O&M instability. To mitigate this, you can create multiple jump servers and use ELB to distribute traffic among them, enhancing access reliability.

Step 1 Create a Linux ECS as a jump server.

Log in to the ECS console and create a Linux ECS. For details, see [Purchasing an ECS](#). If you have an ECS that meets the requirements for use as a jump server, skip this step.

 **NOTE**

- The minimum specifications for the ECS are 1 vCPU and 1 GB of memory. The recommended specifications are 2 vCPUs and 4 GB of memory. You are advised to use an image of **CentOS 6.5 64bit** or later version.
- If the jump server communicates with the extra-region host over the public network, an EIP must be enabled. Conversely, when it uses a VPC peering connection, an EIP is not required.
- The region of the jump server must be the same as the current region of LTS.

Step 2 Add security group rules for the jump server and enable the corresponding inbound ports to ensure data connectivity between the extra-region hosts and the jump server.

1. Log in to the ECS console, check the ECS list, and locate the ECS that you created as the jump server.

2. Click its name to go to the ECS details page. Click the security group name to access the security group details page.
3. Click the **Inbound Rules** tab and click **Add Rule**. Set the ports by referring to [Table 4-7](#). Set other parameters based on your network requirements. For details, see [Adding a Security Group Rule](#).

Table 4-7 Security group rule

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

Step 3 Return to the ECS list, locate the ECS created in [Step 1](#), and view its private IP address and EIP (available if an EIP has been enabled).

Step 4 Log in to the LTS console. In the navigation pane, choose **Host Management > Hosts**. Click **Install ICAgent**. On the displayed page, enter the private IP address of the jump server to generate the SSH tunneling command.

 **NOTE**

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

Step 5 On the **Install ICAgent** page, click **Copy Command** to copy the SSH tunneling command.

```
ssh -f -N -L {Private IP address of the jump server}:8149:{LTS reporting IP address}:8149 -L {Private IP address of the jump server}:8102:{LTS reporting IP address}:8102 -L {Private IP address of the jump server}:8923:{LTS reporting IP address}:8923 -L {Private IP address of the jump server}:30200:{LTS reporting IP address}:30200 -L {Private IP address of the jump server}:30201:{LTS reporting IP address}:30201 -L {Private IP address of the jump server}:80:icagent-{Region}.{OBS domain name}:80 {Private IP address of the jump server}
```

Step 6 Log in to the jump server as user **root** and run the copied SSH tunneling command.

Step 7 Repeat the preceding steps to create multiple jump servers. Add them to the same VPC by selecting the same VPC for **Network** during their creation.

Step 8 Log in to the ELB console and create a load balancer. For details, see [Creating a Dedicated Load Balancer](#). When creating the load balancer, you should:

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

Step 9 Add listeners for TCP ports 30200, 30201, 8149, 8923, 8102, and 80. For details, see [Adding a TCP Listener](#).

Step 10 Create a backend server group and add all jump servers in the group. For details, see [Adding Backend Servers](#).

- Step 11** Return to the LTS console. On the **Install ICAgent** page, enter the EIP of the load balancer in **Connection IP**, copy the installation command, and run it on the extra-region host.

----End

Inherited Installation (Linux)

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

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

```
bash /opt/oss/servicemgr/ICAgent/bin/remotelInstall/remote_install.sh -ip x.x.x.x
```
2. Enter the password for user **root** of the host when prompted.

NOTE

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

Batch Inherited Installation (Linux)

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

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

Prerequisites

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

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

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

NOTE

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

Procedure

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

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

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

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

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

2. After the installation is complete, choose **Host Management > Hosts** in the navigation pane to view the host status. For details, see [Checking the ICAgent Status](#).

4.2.4 Managing ICAgent

After ICAgent is installed, you can [upgrade](#) and [uninstall](#) it, and [view its status](#) and [version](#).

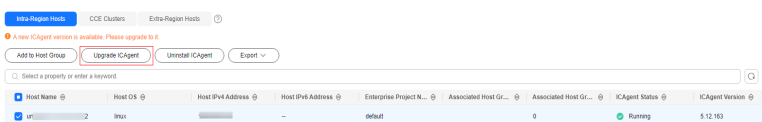
Upgrading ICAgent

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.

For Windows hosts, you must uninstall ICAgent before installing a new version.

- Step 1** Log in to the management console and choose **Management & Deployment > Log Tank Service**.
- Step 2** Choose **Host Management > Hosts** in the navigation pane.
- Step 3** Select **Intra-Region Hosts** or **Extra-Region Hosts**. When the system prompts you that a new ICAgent version is available, select one or more check boxes of hosts where ICAgent is to be upgraded, and click **Upgrade ICAgent**.

Figure 4-5 Upgrading ICAgent on an intra-region host



- Step 4** Click the **CCE Cluster** tab. Search for and select the cluster whose ICAgent is to be upgraded, and click **Upgrade ICAgent**.
- If there are no CCE clusters available, **Output to AOM** is unavailable.
 - To disable the function of exporting container standards to AOM, you need to have ICAgent 5.12.133 or later.
 - If you create a CCE cluster for the first time, ICAgent will be installed on hosts in the cluster by default, and logs will be reported to AOM. **Output to AOM** is enabled by default. To report logs to LTS, disable **Output to AOM** before upgrading ICAgent. You are advised to choose **Log Ingestion > Cloud Service > Cloud Container Engine (CCE)** to collect container data and output it to LTS instead of AOM.
 - CCE cluster ID (ClusterID): Each cluster has a fixed ID.
 - When ICAgent is upgraded, LTS creates log groups and host groups for your CCE cluster. The name of the log group and host group is **k8s-log-{ClusterID}**. You can create an ingestion configuration (**Cloud Services > Cloud Container Engine (CCE)**) to add logs of the current CCE cluster to the log group.
 - If the hosts of a cluster have no ICAgent installed or outdated ICAgent installed, click **Upgrade ICAgent** to install or upgrade ICAgent on all hosts in the cluster.

Figure 4-6 Upgrading ICAgent on a CCE cluster



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

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

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

----End

Uninstalling ICAgent

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

NOTE

Only ICAgent installed on Linux hosts can be uninstalled from the **Host Management** page of the LTS console. To uninstall ICAgent from a Windows host, go to **\ICProbeAgent\bin\manual\win** in the directory where the ICAgent installation package was decompressed, and double-click the script named **uninstall.bat**. If message **ICAgent uninstall success** is displayed, the uninstallation is successful.

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

You can uninstall ICAgent using either of the following methods:

- Uninstalling ICAgent on the console: applies to the scenario where ICAgent has been successfully installed.
 - a. Choose **Host Management > Hosts** in the navigation pane.
 - b. Select one or more hosts where ICAgent is to be uninstalled and click **Uninstall ICAgent**.
 - c. In the displayed dialog box, click **OK**.
The uninstallation begins. This process takes about a minute.
The hosts with ICAgent uninstalled will be removed from the host list.

 **NOTE**

To reinstall ICAgent, wait for 5 minutes after it is uninstalled. Otherwise, the ICAgent may be automatically uninstalled again.

- Logging in to the host to uninstall ICAgent: applies to the scenario where ICAgent fails to be installed.
 - a. Log in to a host where ICAgent is to be uninstalled as user **root**.
 - b. Run the following command:

```
bash /opt/oss/servicemgr/ICAgent/bin/manual/uninstall.sh
```

If the message **ICAgent uninstall success** is displayed, the uninstallation has completed.
- Remotely uninstalling ICAgent: applies to the scenario where the ICAgent has been successfully installed and needs to be remotely uninstalled.
You can uninstall ICAgent on one host remotely from another host.
 - a. Run the following command on the host where ICAgent has been installed. *x.x.x.x* indicates the IP address of the host you want to uninstall ICAgent from.

```
bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -ip x.x.x.x
```
 - b. Enter the password for user **root** of the host when prompted.

 **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.
 - If the message **ICAgent uninstall success** is displayed, the uninstallation has completed.
- Batch uninstalling ICAgent: applies to the scenario where the ICAgent has been installed and needs to be uninstalled in batches.
If ICAgent has been installed on a host and the ICAgent installation package **ICProbeAgent.tar.gz** is in the **/opt/ICAgent/** directory of the host, you can use this method to uninstall ICAgent from multiple hosts at once.

 **NOTE**

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

Prerequisites

The IP addresses and passwords of all hosts to uninstall ICAgent have been collected, sorted in the **iplist.cfg** file, and uploaded to the **/opt/ICAgent/**

directory on the host that has ICAgent installed. Each IP address and password in the **iplist.cfg** file must be separated by a space. Examples:

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

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

 **NOTE**

- The **iplist.cfg** file contains sensitive information. You are advised to clear it after using it.
 - If all hosts share a password, list only IP addresses in the **iplist.cfg** file and enter the password manually during execution. If one of the hosts uses a different password, type the password behind its IP address.
- a. Run the following command on the host that has ICAgent installed:
- ```
bash /opt/oss/servicemgr/ICAgent/bin/remoteUninstall/remote_uninstall.sh -
batchModeConfig /opt/ICAgent/iplist.cfg
```

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

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

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

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

## Checking the ICAgent Status

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

**Table 4-8** ICAgent statuses

| Status              | Description                                                      |
|---------------------|------------------------------------------------------------------|
| Running             | ICAgent is running properly.                                     |
| Uninstalled         | ICAgent is not installed.                                        |
| Installing          | ICAgent is being installed. This process takes about one minute. |
| Installation failed | ICAgent installation failed.                                     |
| Upgrading           | ICAgent is being upgraded. This process takes about one minute.  |



| Status               | Description                                                                                                       |
|----------------------|-------------------------------------------------------------------------------------------------------------------|
| Upgrade failed       | ICAgent upgrade failed.                                                                                           |
| Offline              | ICAgent is abnormal because the 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.                  |

## Checking the ICAgent Version Description

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

**Table 4-9** ICAgent version description

| Version | Description                                                                                                                                                                          | Released   |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 7.1.17  | Optimized the log collection process to adjust the size of transmitted blocks.                                                                                                       | 2025-01-03 |
| 7.1.14  | <ul style="list-style-type: none"> <li>Optimized the log collection process.</li> <li>Updated to persistently save signature information during log collection.</li> </ul>           | 2024-12-25 |
| 7.1.12  | Solved the issue where, in some scenarios, CPU usage increased due to timer leakage caused by the Go version.                                                                        | 2024-12-15 |
| 7.1.6   | <ul style="list-style-type: none"> <li>Enabled logs to report image names.</li> <li>Optimized the log collection process.</li> <li>Upgraded ICAgent's base image version.</li> </ul> | 2024-11-21 |
| 7.1.5   | Solved the issue that logs continued to be collected after all configurations in a project are deleted or disabled.                                                                  | 2024-11-21 |
| 7.1.3   | Optimized the httpclient component's performance in log sending.                                                                                                                     | 2024-11-02 |
| 7.1.1   | Optimized the ICAgent architecture and unified the Agents of AOM 1.0 and AOM 2.0.                                                                                                    | 2024-10-26 |

| Version  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Released   |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 5.12.233 | <ul style="list-style-type: none"> <li>Optimized the structuring performance for container logs.</li> <li>Solved the issue that error diagnosis occasionally failed to be reported in CCE scenarios.</li> <li>Solved the issue that inactive files failed to be collected in VM scenarios.</li> </ul>                                                                                                                                                                                       | 2024-10-17 |
| 5.12.232 | <ul style="list-style-type: none"> <li>Replaced the JSON library used for parsing standard output logs with the sonic library to reduce the CPU usage.</li> <li>Solved the issue of log transmission timeouts when using LTS.</li> </ul>                                                                                                                                                                                                                                                    | 2024-10-14 |
| 5.12.231 | <ul style="list-style-type: none"> <li>Solved the issue that ICAgent restarted under the following conditions: Standard output was collected by LTS; there were no log ingestion rules defined in LTS; and a container was created in CCE and standard output logs were printed.</li> <li>Solved the issue where <b>hisfile</b> in the cursor file was incorrectly recognized as a directory.</li> <li>Solved the issue where the incremental collection switch was ineffective.</li> </ul> | 2024-10-11 |
| 5.12.230 | <ul style="list-style-type: none"> <li>Solved the issue where periodic cursor refresh was not functioning.</li> <li>Solved the issue where the cursor could not be reset after the <b>base</b> file was wrapped since the wrapping file could not be found.</li> <li>Solved the issue of high CPU usage caused by file signature.</li> </ul>                                                                                                                                                | 2024-10-09 |
| 5.12.224 | Cleared all <b>export HISTSIZE=0</b> entries (if any) from the <b>.bashrc</b> file in the ECS upgrade scenario.                                                                                                                                                                                                                                                                                                                                                                             | 2024-09-27 |
| 5.12.218 | <ul style="list-style-type: none"> <li>Supported GBK encoding in the logs reported by ICAgent.</li> <li>Enabled ICAgent to collect the same log files repeatedly.</li> </ul>                                                                                                                                                                                                                                                                                                                | 2024-09-26 |
| 5.12.185 | <ul style="list-style-type: none"> <li>Fixed the invalid blacklist path in the VM log configuration.</li> <li>Optimized the collection of containerd standard output logs.</li> </ul>                                                                                                                                                                                                                                                                                                       | 2024-05-20 |

| Version  | Description                                                                                                                                                                                                                                                                                                       | Released   |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 5.12.184 | <ul style="list-style-type: none"> <li>Solved the issue of being unable to exclude wrapped files when container logs were collected.</li> <li>Changed the number of concurrent collection coroutines of node log collection to 32.</li> </ul>                                                                     | 2024-05-16 |
| 5.12.183 | Optimized the wrapping files in the standard output of containerd nodes.                                                                                                                                                                                                                                          | 2024-05-11 |
| 5.12.182 | Solved the syslog switch issue.                                                                                                                                                                                                                                                                                   | 2024-04-28 |
| 5.12.181 | <ul style="list-style-type: none"> <li>Solved the ICAgent authentication failure on self-built Kubernetes clusters.</li> <li>Solved the log truncation issue.</li> <li>Solved the issue that some files were not collected because wrapped files could not be found when the log rate was high.</li> </ul>        | 2024-04-25 |
| 5.12.177 | Solved the infinite loop issue of wrapping.                                                                                                                                                                                                                                                                       | 2024-03-28 |
| 5.12.176 | <ul style="list-style-type: none"> <li>Optimized .zip streaming parsing: Check whether transferred files are complete.</li> <li>Specified the maximum number of connections to each PodLB host.</li> </ul>                                                                                                        | 2024-03-18 |
| 5.12.175 | Solved the collection performance bottleneck issue of structured logs.                                                                                                                                                                                                                                            | 2024-03-13 |
| 5.12.172 | Optimized the supported wrapping mode.                                                                                                                                                                                                                                                                            | 2024-02-28 |
| 5.12.171 | Solved the JSON parsing issue (not deleting escape characters) of standard output logs of Docker nodes.                                                                                                                                                                                                           | 2024-01-31 |
| 5.12.170 | <ul style="list-style-type: none"> <li>Supported incremental collection of host, container, and standard output logs.</li> <li>Resolved the host GPU metric disconnection issue.</li> </ul>                                                                                                                       | 2024-01-29 |
| 5.12.166 | <ul style="list-style-type: none"> <li>Solved the high memory usage issue of the standard output log collection plug-in.</li> <li>Solved the issue that the VM log collection plug-in repeatedly collected wrapped files.</li> <li>Added the log group and log stream information to the cursor files.</li> </ul> | 2023-12-27 |
| 5.12.165 | Added the function of obtaining the initial agent ID from the configuration file. If the agent ID does not meet the verification requirements, the randomly generated UUID is used.                                                                                                                               | 2023-12-21 |

| Version  | Description                                                                                                                                                                                                                                                    | Released   |
|----------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 5.12.163 | Supported ICAgent installation using the UniAgent plug-in.                                                                                                                                                                                                     | 2023-12-13 |
| 5.12.159 | <ul style="list-style-type: none"><li>Solved the leakage issue of the standard output log collection coroutine.</li><li>Solved the issue that standard output wrapping logs could not be collected after standard output logs were collected to AOM.</li></ul> | 2023-11-27 |
| 5.12.158 | Solved the issue that memory leakage of container metrics caused ICAgent restart when the metric switch was turned off.                                                                                                                                        | 2023-11-08 |
| 5.12.157 | <ul style="list-style-type: none"><li>Container log ingestion to LTS: supported Docker driver Device Mapper.</li><li>Solved the issue that ICAgent restarted due to too many VM logs (fast transferring) and sharp increase of memory usage.</li></ul>         | 2023-11-06 |
| 5.12.156 | Solved the issue of obtaining the installation package from OBS and changed the protocol from HTTP to HTTPS.                                                                                                                                                   | 2023-11-01 |
| 5.12.154 | Supported log structuring.                                                                                                                                                                                                                                     | 2023-10-31 |
| 5.12.153 | Released version 7.                                                                                                                                                                                                                                            | 2023-10-19 |
| 5.12.150 | <ul style="list-style-type: none"><li>Resolved the cluster name and ID not-set issues.</li><li>Supported CCE clusters of v1.27.</li></ul>                                                                                                                      | 2023-10-17 |
| 5.12.149 | Supported mounting wrapping.                                                                                                                                                                                                                                   | 2023-10-12 |
| 5.12.148 | Solved the high CPU usage issue in the multi-GPU scenario.                                                                                                                                                                                                     | 2023-08-30 |
| 5.12.147 | Solved the issue that log transfer function could not be restarted and the host GPU metric adaptation issue.                                                                                                                                                   | 2023-08-17 |
| 5.12.142 | Supported the collection of container GPU metrics of CCE clusters of v1.25 or later.                                                                                                                                                                           | 2023-06-13 |
| 5.12.139 | Solved the issue of a large number of TIME_WAIT TCP connections when LTS logs are reported.                                                                                                                                                                    | 2023-04-25 |
| 5.12.135 | <ul style="list-style-type: none"><li>Solved the 0% CPU usage issue.</li><li>Solved the missing container network metrics of containerd nodes in CCE v1.23 clusters.</li><li>Supported collection of disk partition metrics of EulerOS 2.5.</li></ul>          | 2023-02-08 |

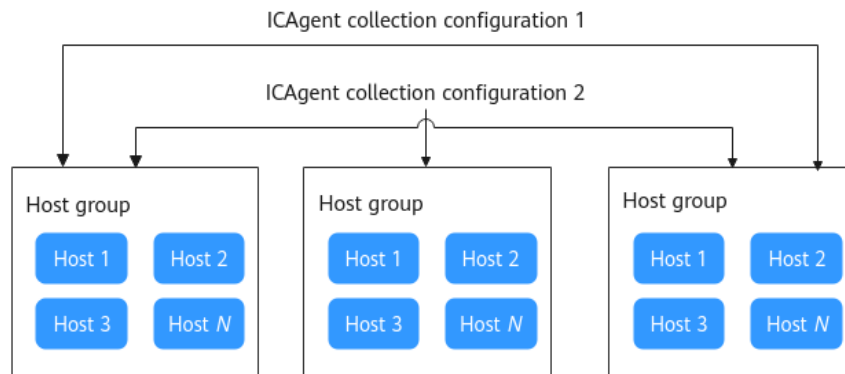
| Version  | Description                                                                                                                                                                                                                                                                                                                                                                           | Released   |
|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------|
| 5.12.133 | Supported multi-line collection of container standard output logs.                                                                                                                                                                                                                                                                                                                    | 2022-12-17 |
| 5.12.130 | Supported direct ingestion of CCE logs to LTS.                                                                                                                                                                                                                                                                                                                                        | 2022-11-04 |
| 5.12.120 | <ul style="list-style-type: none"><li>Added a metric: maximum number of process handles.</li><li>Supported changing of the LTS PodLB domain name.</li></ul>                                                                                                                                                                                                                           | 2022-08-28 |
| 5.12.111 | Added thread metrics and fixed the issue that the LVS disk partition metrics fail to be obtained.                                                                                                                                                                                                                                                                                     | 2022-06-09 |
| 5.12.100 | <ul style="list-style-type: none"><li>Added two metrics: used memory working set and memory working set usage.</li><li>Supported container log tagging with <b>stderr.log</b> or <b>stdout.log</b> during collection.</li><li>Added the <b>Pod_ip</b> tag for container log reporting.</li><li>Supported double asterisks (**) for matching files in the current directory.</li></ul> | 2022-01-15 |
| 5.12.98  | Supported LTS log collection blacklists and changed the source of container metrics to <b>working_set</b> .                                                                                                                                                                                                                                                                           | 2021-09-29 |
| 5.12.96  | Supported discovery of more types of cloud resources.                                                                                                                                                                                                                                                                                                                                 | 2021-09-22 |
| 5.12.90  | Updated the GPU metric source.                                                                                                                                                                                                                                                                                                                                                        | 2021-07-15 |
| 5.12.87  | Supported more types of disks.                                                                                                                                                                                                                                                                                                                                                        | 2021-03-30 |
| 5.12.75  | Adapted to secure containers.                                                                                                                                                                                                                                                                                                                                                         | 2021-03-09 |

## 4.2.5 Managing Host Groups

Host groups allow you to configure host log ingestion efficiently. You can add multiple hosts to a host group and associate the host group with log ingestion configurations. The ingestion configurations will then be applied to all the hosts in the host group. For details, see [Figure 4-7](#).

- 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.

**Figure 4-7** Host groups



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

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

**NOTE**

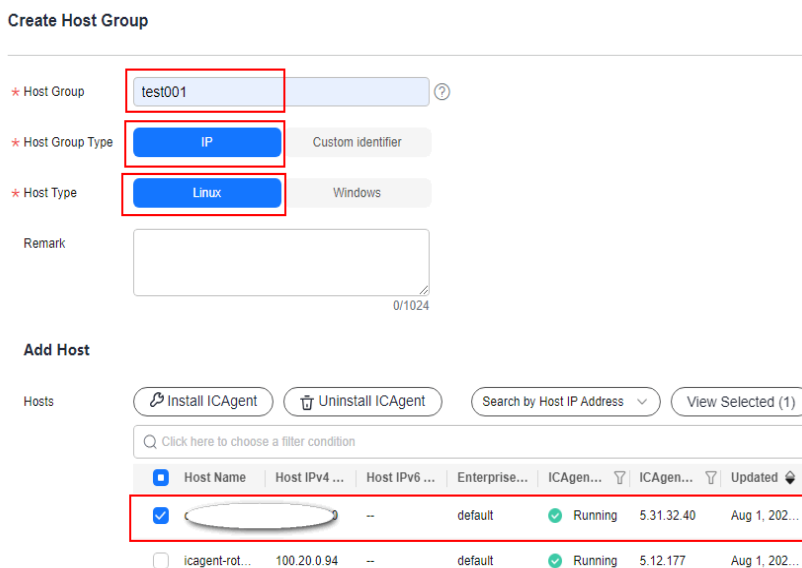
Host groups with custom identifiers are suitable for the following scenarios:

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

## Creating a Host Group (IP Address)

- Step 1** Log in to the management console and choose **Management & Deployment > Log Tank Service**.
- Step 2** Choose **Host Management > Host Groups** in the navigation pane.
- Step 3** Click **Create Host Group** in the upper right corner.
- Step 4** In the displayed slide-out panel, enter a host group name, select **IP** for **Host Group Type**, and select a host OS (**Linux** or **Windows**).

**Figure 4-8** Creating an IP address host group




- Step 5** In the host list, select one or more hosts to add to the group and click **OK**.
- You can filter hosts by host name or host IP address. You can also click **Search by Host IP Address** and enter multiple host IP addresses in the displayed search box to search for matches.
  - If your desired hosts are not in the list, click **Install ICAgent**. On the displayed page, install ICAgent on the hosts as prompted. For details, see [Installing ICAgent \(Intra-Region Hosts\)](#) or [Installing ICAgent \(Extra-Region Hosts\)](#).

----End

## Creating a Host Group (Custom Identifier)

To create a host group of the custom identifier type, you need to plan the hosts to be identified in advance.

- Step 1** Click **Create Host Group** in the upper right corner.
- Step 2** In the displayed slide-out panel, enter a host group name, select **Custom Identifier** for **Host Group Type**, and select a host OS (**Linux** or **Windows**).

- Step 3** Enter a custom identifier. You can also click  **Add** to enter more.

### NOTE

Up to 10 custom identifiers can be added.

- Step 4** Click **OK**. After the host group is created, go to **5** to add hosts to it.
- Step 5** Perform the following operations to create the **custom\_tag** file to save host tags:
- Log in to the host and run the **cd /opt/cloud** command. If the system indicates that the **/opt/cloud** directory does not exist, run the **mkdir /opt/cloud/** command to create it. If the **/opt/cloud** directory already exists, navigate to it and run the **mkdir lts** command to create the **lts** directory in it.

2. Run the **chmod 750 lts** command to modify the permission on the **lts** directory.
3. Run the **touch custom\_tag** command in the **lts** directory to create the **custom\_tag** file.
4. Run the **chmod 640 custom\_tag;vi custom\_tag** command to modify the **custom\_tag** permission and open the file.
5. Press **i** to enter the insert mode, enter a custom identifier, press **Esc**, enter **:wq!**, save the modification and exit.
6. Use either of the following methods to add a host to the custom identifier host group:

**Table 4-10** Methods

| Type       | Method 1 (Recommended)                                                                                                                                                                                                                                                                                                                                                            | Method 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Linux host | View the host's identifier in the <b>custom_tag</b> file of the <b>/opt/cloud/lts</b> directory on the host. Then, add the identifier to the host group to include the host within it. For example, if the <b>custom_tag</b> file in the <b>/opt/cloud/lts</b> directory shows the host's identifier as <b>test1</b> , simply add <b>test1</b> to the group's custom identifiers. | <ul style="list-style-type: none"> <li>- Add the host group's custom identifier to the <b>custom_tag</b> file in the <b>/opt/cloud/lts</b> directory on the host to include the host within the host group. For example, if the group's custom identifier is <b>test</b>, enter <b>test</b> into the <b>custom_tag</b> file.</li> <li>- If the group has multiple custom identifiers, simply enter any one of them into the <b>custom_tag</b> file of the <b>/opt/cloud/lts</b> directory on the host.</li> </ul> |



| Type         | Method 1 (Recommended)                                                                                                                                                                                                                                                                                                                                                                | Method 2                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Windows host | View the host's identifier in the <b>custom_tag</b> file of the <b>C:\opt\cloud\lts</b> directory on the host. Then, add the identifier to the host group to include the host within it. For example, if the <b>custom_tag</b> file in the <b>C:\opt\cloud\lts</b> directory shows the host's identifier as <b>test1</b> , simply add <b>test1</b> to the group's custom identifiers. | <ul style="list-style-type: none"> <li>- Add the host group's custom identifier to the <b>custom_tag</b> file in the <b>C:\opt\cloud\lts</b> directory on the host to include the host within the host group. For example, if the group's custom identifier is <b>test</b>, enter <b>test</b> into the <b>custom_tag</b> file.</li> <li>- If the group has multiple custom identifiers, simply enter any one of them into the <b>custom_tag</b> file of the <b>C:\opt\cloud\lts</b> directory on the host.</li> </ul> |





----End



## Modifying a Host Group

You can change the name of a host group, add hosts to or remove hosts from a host group, or associate a host group with log ingestion configurations. For details, see [Table 4-11](#).

**Table 4-11** Operations on host groups

| Operation                  | Procedure                                                                                                                                                                                                                                                                                                                                                          |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Changing a host group name | <ol style="list-style-type: none"> <li>1. Go to the <b>Host Groups</b> page.</li> <li>2. In the host group list, click the modification button in the <b>Operation</b> column of the target host group.</li> <li>3. On the displayed dialog box, modify the information such as the host group name and custom identifier.</li> <li>4. Click <b>OK</b>.</li> </ol> |

| Operation                         | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Adding hosts to a host group      | <p><b>Method 1:</b></p> <ol style="list-style-type: none"> <li>In the host group list, click  in the row containing the target host group whose type is <b>IP</b>.</li> <li>Click <b>Add Host</b>.</li> <li>In the displayed slide-out panel, all hosts that are not in the host group and run the selected OS type are displayed. Select the hosts to be added to the host group. <ul style="list-style-type: none"> <li>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.</li> <li>If your desired hosts are not in the list, click <b>Install ICAgent</b>. On the displayed page, install ICAgent on the hosts as prompted. For details, see <a href="#">Installing ICAgent</a>.</li> </ul> </li> <li>Click <b>OK</b>.</li> </ol> <p><b>Method 2:</b></p> <ol style="list-style-type: none"> <li>Choose <b>Host Management &gt; Hosts</b> in the navigation pane.</li> <li>In the host list, select the target hosts and click <b>Add to Host Group</b>.</li> <li>In the displayed slide-out panel, select the target host group.</li> <li>Click <b>OK</b>.</li> </ol> |
| Removing a host from a host group | <ol style="list-style-type: none"> <li>In the host group list, click  in the row containing the target host group.</li> <li>In the host list, click <b>Remove</b> in the <b>Operation</b> column of the row containing the host to be removed.</li> <li>In the displayed dialog box, click <b>OK</b>.</li> </ol> <p><b>NOTE</b><br/>This operation is not supported for hosts in the custom identifier host group.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Uninstalling ICAgent from a host  | <ol style="list-style-type: none"> <li>In the host group list, click  in the row containing the target host group.</li> <li>In the host list, click <b>Uninstall ICAgent</b> in the <b>Operation</b> column of the row containing the target host.</li> <li>In the displayed dialog box, click <b>OK</b> to uninstall ICAgent from the host and remove the host from the host group.</li> </ol> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>This operation is not supported for hosts in the custom identifier host group.</li> <li>If the host has also been added to other host groups, it will be removed from those groups as well.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |

| Operation                                                          | Procedure                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Removing hosts from a host group                                   | <ol style="list-style-type: none"> <li>1. In the host group list, click  in the row containing the target host group.</li> <li>2. In the host list, select the target hosts and click the <b>Remove</b> button above the list.</li> <li>3. Click <b>OK</b>.</li> </ol>                                                                                                                                                           |
| Associating a host group with an ingestion configuration           | <ol style="list-style-type: none"> <li>1. In the host group list, click  in the row containing the target host group.</li> <li>2. Click the <b>Associated Ingestion Configuration</b> tab.</li> <li>3. Click <b>Associate</b>.</li> <li>4. In the displayed slide-out panel, select the target ingestion configuration.</li> <li>5. Click <b>OK</b>. The associated ingestion configuration is displayed in the list.</li> </ol> |
| Disassociating a host group from an ingestion configuration        | <ol style="list-style-type: none"> <li>1. On the <b>Associated Ingestion Configuration</b> tab, click <b>Disassociate</b> in the <b>Operation</b> column of the row containing the target ingestion configuration.</li> <li>2. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                                        |
| Disassociating a host group from multiple ingestion configurations | <ol style="list-style-type: none"> <li>1. On the <b>Associated Ingestion Configuration</b> tab, select the target ingestion configurations and click the <b>Disassociate</b> button above the list.</li> <li>2. Click <b>OK</b>.</li> </ol>                                                                                                                                                                                                                                                                       |
| Copying a host group ID                                            | Hover your cursor over a host group name to copy the host group ID.                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Exporting host information                                         | <ol style="list-style-type: none"> <li>1. On the <b>Hosts</b> page, switch to the <b>Intra-Region Hosts</b>, <b>CCE Cluster</b>, or <b>Extra-Region Hosts</b> tab and select the desired hosts.</li> <li>2. Click <b>Export</b> to export the information of the selected hosts to the local PC.</li> </ol>                                                                                                                                                                                                       |

## Deleting Host Groups

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

**Step 2** Delete a host group:

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

**Step 3** Delete host groups in batches:

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

----End

## 4.2.6 Ingesting BMS Text Logs to LTS

A Bare Metal Server (BMS) features both the scalability of VMs and high performance of physical servers. It provides dedicated servers on the cloud, delivering the performance and security required by core databases, critical applications, high-performance computing (HPC), and big data.

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

Perform the following steps to complete the ingestion configuration:

1. [Step 1: Select a Log Stream](#)
2. [Step 2: \(Optional\) Select a Host Group](#)
3. [Step 3: Configure the Collection](#)
4. [Step 4: Configure Indexing](#)
5. [Step 5: Complete the Ingestion Configuration](#)

To collect logs from multiple scenarios, [set multiple ingestion configurations in a batch](#).


### Prerequisites

ICAgent has been **installed** and **added** to the host group. You have enabled **ICAgent Diagnosis** to view exceptions, overall status, and collection status of ICAgent. For details, see [Setting ICAgent Collection](#).

### Step 1: Select a Log Stream

1. Log in to the [LTS console](#).
2. Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **BMS (Bare Metal Server)**.

Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > BMS (Bare Metal Server)** on the displayed page.

Alternatively, choose **Log Management** in the navigation pane and click the target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and click **Ingest Log**. In the displayed dialog box, click **BMS (Bare Metal Server)**.

3. Select a log group from the **Log Group** drop-down list. If there is no desired log group, click **Create Log Group**. For details, see [Managing Log Groups](#).
4. Select a log stream from the **Log Stream** drop-down list. If there is no desired log stream, click **Create Log Stream**. For details, see [Managing Log Streams](#).
5. Click **Next: (Optional) Select Host Group**.

## Step 2: (Optional) Select a Host Group

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

### NOTE

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

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

## Step 3: Configure the Collection

After selecting host groups, configure the collection as follows:

### NOTE

- Ensure that sensitive information is not collected.
  - If a collection path of a host has been configured in AOM, do not configure the path in LTS.
  - If log files were last modified more than 12 hours earlier than the time when the path is added, the files are not collected.
  - LTS cannot collect logs of PostgreSQL (database) instances.
1. **Collection Configuration Name:** Enter 1 to 64 characters. Only letters, digits, hyphens (-), underscores (\_), and periods (.) are allowed. Do not start with a period or underscore, or end with a period.

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

### 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. Import the old configuration or create one as required.
2. **Collection Paths:** Add one or more host paths. LTS will collect logs from these paths. The rules for setting collection paths are as follows:

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

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

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

 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 Web Application Firewall (WAF) and configure the path again.

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

```
/var/logs/1/a.log
/var/logs/2/a.log
```
  - Example 2: **/var/logs/service-\*/a.log** will match files as follows:
 

```
/var/logs/service-1/a.log
/var/logs/service-2/a.log
```
  - Example 3: **/var/logs/service/a\*.log** will match files as follows:
 

```
/var/logs/service/a1.log
/var/logs/service/a2.log
```
- If the collection path is set to a file name, the corresponding file is collected. Only text files can be collected.
  - **Add Custom Wrapping Rule:** ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping.

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

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

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

After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see [Checking the ICAgent Version Description](#).

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

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

Blacklist filters can be exact matches or wildcard pattern matches. For details, see [Collection Paths](#).

 **NOTE**

- If you blacklist a file or directory that has been set as a collection path in the previous step, the blacklist settings will be used and the file or files in the directory will be filtered out.
  - If a log has been added to the blacklist, it cannot be collected even if you create a log ingestion task. You can collect it again only after you delete the collection path from the blacklist.
  - If you specify a directory, all files in the directory are filtered out, but log files in the folders in the directory cannot be filtered out.
5. **Collect Windows Event Logs:** To collect logs from Windows hosts, enable this option and set the following parameters.

**Table 4-12** Parameters for collecting windows event logs

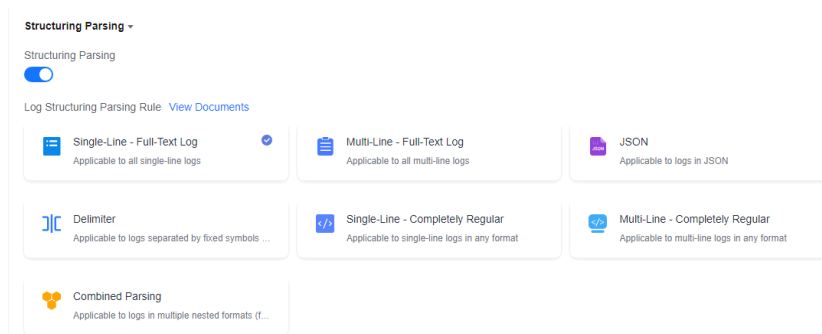
| Parameter                    | Description                                                                                                                                                                                                                                                        |
|------------------------------|--------------------------------------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

6. Enable structuring parsing. For details, see [Setting ICAgent Structuring Parsing Rules](#).

LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream.

If you have configured cloud structuring parsing, delete its configurations before configuring ICAgent structuring parsing.

Figure 4-9 ICAgent structuring parsing configuration



7. Set other configurations.

Table 4-13 Other configurations

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Directory Depth  | The maximum directory depth is 20 levels.<br>Collection paths can use double asterisks (**) for multi-layer fuzzy match. Specify the maximum directory depth in the text box. For example, if your log path is <b>/var/logs/department/app/a.log</b> and your collection path is <b>/var/logs/**/a.log</b> , logs will not be collected when this parameter is set to <b>1</b> , but will be collected when this parameter is set to <b>2</b> or a larger number.                                                                   |
| Split Logs           | <ul style="list-style-type: none"> <li>If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs.</li> <li>If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.</li> </ul> |
| Collect Binary Files | LTS can collect binary files.<br>Run the <b>file -i File_name</b> command to view the file type. <b>charset=binary</b> indicates that a log file is a binary file.<br>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.<br>If this option is disabled, binary log files will not be collected.                                                                                                                                 |
| Log File Code        | The log file encoding format can be UTF-8 or GBK (not available to Windows).<br>UTF-8 encoding is a variable-length encoding mode and represents Unicode character sets. GBK, an acronym for Chinese Internal Code Extension Specification, is a Chinese character encoding standard that extends both the ASCII and GB2312 encoding systems.                                                                                                                                                                                       |



| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Collection Policy | <p>Select incremental or full collection.</p> <ul style="list-style-type: none"> <li>● <b>Incremental:</b> When collecting a new file, ICAgent reads the file from the end of the file.</li> <li>● <b>All:</b> When collecting a new file, ICAgent reads the file from the beginning of the file.</li> </ul>                                                                                                                                                                                               |
| Custom Metadata   | <ul style="list-style-type: none"> <li>● If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields.</li> <li>● If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs.<br/><b>Built-in Fields:</b> Select built-in fields as required.<br/><b>Custom Key-Value Pairs:</b> Click <b>Add</b> and set a key and value.</li> </ul> |

8. Configure the log format and time by referring to [Table 4-14](#).

**Table 4-14** Log collection settings

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Format | <ul style="list-style-type: none"> <li>● <b>Single-line:</b> Each log line is displayed as a single log event.</li> <li>● <b>Multi-line:</b> Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.</li> </ul>                                                                                                                                                                                                                                     |
| Log Time   | <p><b>System time:</b> log collection time by default. It is displayed at the beginning of each log event.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● Log collection time is the time when logs are collected and sent by ICAgent to LTS.</li> <li>● Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second.</li> <li>● Restriction on log collection time: Logs are collected within 24 hours before and after the system time.</li> </ul> |

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p><b>Time wildcard:</b> You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event.</p> <ul style="list-style-type: none"> <li>• If the time format in a log event is <b>2019-01-01 23:59:59.011</b>, the time wildcard should be set to <b>YYYY-MM-DD hh:mm:ss.SSS</b>.</li> <li>• If the time format in a log event is <b>19-1-1 23:59:59.011</b>, the time wildcard should be set to <b>YY-M-D hh:mm:ss.SSS</b>.</li> </ul> <p><b>NOTE</b><br/>If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p><b>Example:</b></p> <pre> YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:spm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)                     </pre> |
| Log Segmentation      | <p>This parameter needs to be specified if the <b>Log Format</b> is set to <b>Multi-line</b>. <b>By generation time</b> indicates that a time wildcard is used to detect log boundaries, whereas <b>By regular expression</b> indicates that a regular expression is used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| By regular expression | <p>You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select <b>Multi-line</b> for <b>Log Format</b> and <b>By regular expression</b> for <b>Log Segmentation</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

 **NOTE**

The time wildcard and regular expression will look for the specified pattern right from the beginning of each log line. If no match is found, the system time, which may be different from the time in the log event, is used. In general cases, you are advised to select **Single-line** for **Log Format** and **System time** for **Log Time**.

9. Click **Next: Index Settings**.

## Step 4: Configure Indexing

1. (Optional) Configure indexing. For details, see [Setting Indexes](#).
2. Click **Submit**.



## Step 5: Complete the Ingestion Configuration

The created ingestion configuration will be displayed.

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

### NOTE

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

- To stop log collection of an ingestion configuration, toggle off  in the **Status** column to disable the configuration. To restart log collection, toggle on  in the **Status** column.

### NOTE

Disabling an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. Exercise caution when performing this operation.

- Click **More > ICAgent Collect Diagnosis** in the **Operation** column of the ingestion configuration to monitor the exceptions, overall status, and collection status of ICAgent.

## Setting Multiple Ingestion Configurations in a Batch

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

- Step 1** On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see [Table 4-15](#).

**Table 4-15** Adding configurations in batches

| Type           | Parameter             | Description                                                                                                                                                                                                                                                           |
|----------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic Settings | Ingestion Type        | Choose <b>BMS (Bare Metal Server)</b> .                                                                                                                                                                                                                               |
|                | Configurations to Add | Enter the number of ingestion configurations in the text box and click <b>Add</b> .<br><br>A maximum of 100 ingestion configurations can be added, including the one already exists under <b>Ingestion Settings</b> by default. Therefore, you can add up to 99 more. |

| Type               | Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ingestion Settings | Configuration List | <ol style="list-style-type: none"> <li>1. The ingestion configurations are displayed on the left. You can add up to 99 more configurations.</li> <li>2. The ingestion configuration details are displayed on the right. Set them by referring to <b>Step 3: Configure the Collection</b>.</li> <li>3. After an ingestion configuration is complete, you can click <b>Apply to Other Configurations</b> to copy its settings to other configurations.</li> </ol> |

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

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

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

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. If you toggle off the switch in the **Status** column of an ingestion configuration, logs will not be collected for this configuration.
- Select multiple existing ingestion configurations and click **Delete**.

----End

## 4.2.7 Ingesting CCE Application Logs to LTS

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

After ingesting CCE logs to LTS, you can centrally manage and analyze them and visualize log reports on the LTS console. This helps you better monitor and manage containerized application running, promptly detect container issues, and improve container performance and reliability.

Perform the following steps to complete the ingestion configuration:

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

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

## Prerequisites

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

### NOTE


- If you use AOM 2.0 for the first time, authorize it by referring to [Subscribing to AOM 2.0](#). Then, log in to the AOM 2.0 console, grant AOM 2.0 the permission to access data of cloud services, such as LTS and CCE, by referring to [Cloud Service Authorization](#).
- On the **Hosts** page, select **CCE Clusters**, select the target cluster in the search box, and click **Upgrade ICAgent**. For details, see [Upgrading ICAgent](#).
- You have disabled **Output to AOM**.
- You have enabled **ICAgent Diagnosis** to view exceptions, overall status, and collection status of ICAgent. For details, see [Setting ICAgent Collection](#).

## Constraints

- CCE cluster nodes whose container engine is Docker are supported. For details, see [Cloud Container Engine \(CCE\)](#).
- CCE cluster nodes whose container engine is Containerd are supported. You must be using ICAgent 5.12.130 or later.
- CCE Turbo clusters are supported. You must be using ICAgent 5.12.130 or later.
- To collect container log directories mounted to host directories to LTS, you must configure the node file path.
- Constraints on the Docker storage driver: Currently, container file log collection supports only the overlay2 storage driver. devicemapper cannot be used as the storage driver. Run the following command to check the storage driver type:  

```
docker info | grep "Storage Driver"
```
- If you select **Fixed log stream** for log ingestion, ensure that you have created a CCE cluster.

## Step 1: Select a Log Stream

1. Log in to the [LTS console](#).
2. Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **CCE (Cloud Container Engine)**.  
Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > CCE (Cloud Container Engine)**.  
Alternatively, choose **Log Management** in the navigation pane and click the target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and click **Ingest Log**. In the displayed dialog box, click **CCE (Cloud Container Engine)**.
3. Choose a collection mode between **Fixed log stream** (recommended) and **Custom log stream**.

**Table 4-16** Collection modes

| Collection Mode   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fixed log stream  | <ul style="list-style-type: none"> <li>• Advantages: All logs are collected to one log stream. You can view them by namespace, workload, or container name.</li> <li>• Disadvantages:<br/>Since logs of different structures are collected into the same stream, log structuring and SQL visual analysis are unavailable.<br/><br/>Since each stream has a limited write rate of 100 MB/s, there may be performance bottlenecks in heavy traffic.</li> </ul> |
| Custom log stream | <ul style="list-style-type: none"> <li>• Advantages:<br/>Since logs of different structures are collected to different streams, log structuring and SQL visual analysis are available.<br/><br/>Since the cumulative write rate of multiple streams is not limited, there are no performance bottlenecks in heavy traffic.</li> <li>• Disadvantage: Logs cannot be viewed by namespace, workload, or container name.</li> </ul>                              |

- If you set **Collect** to **Fixed log stream**, perform the following steps:  
Logs will be collected to a fixed log stream. The default log streams for a CCE cluster are **stdout-*{ClusterID}*** for standard output/errors, **hostfile-*{ClusterID}*** for node files, **event-*{ClusterID}*** for Kubernetes events, and **containerfile-*{ClusterID}*** for container files. Log streams are automatically named with a cluster ID. For example, if the cluster ID is **Cluster01**, the standard output/error log stream is **stdout-Cluster01**.  
Log streams that can be created for a CCE cluster are **stdout-*{ClusterID}*** for standard output/errors, **hostfile-*{ClusterID}*** for node files, **event-*{ClusterID}*** for Kubernetes events, and **containerfile-*{ClusterID}*** for container files. If one of them has been created in a log group, the log stream will no longer be created in the same log group or other log groups.
  - i. Select a cluster from the **CCE Cluster** drop-down list.
  - ii. The default log group is **k8s-log-*ClusterID***. For example, if the cluster ID is **c7f3f4a5-bcb8-11ed-a4ec-0255ac100b07**, the default log group will be **k8s-log-c7f3f4a5-bcb8-11ed-a4ec-0255ac100b07**.

 **NOTE**

If there is no such group, the system displays the following message: This log group does not exist and will be automatically created to start collecting logs.

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

- If you set **Collect** to **Custom log stream**, perform the following steps:
  - i. Select a cluster from the **CCE Cluster** drop-down list.
  - ii. Select a log group from the **Log Group** drop-down list. If there are no desired log groups, click **Create Log Group** to create one.
  - iii. Select a log stream from the **Log Stream** drop-down list. If there are no desired log streams, click **Create Log Stream** to create one.
  - iv. Click **Next: Check Dependencies**.

## Step 2: Check Dependencies

The system automatically checks the following items:

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

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

### NOTE

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

## Step 3: (Optional) Select a Host Group

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

### NOTE

- The host group to which the cluster belongs is selected by default. You can also select host groups as required.
  - For a host group of CCE clusters, its custom identifier must be in the format of **k8s-log-Cluster ID**.
  - You can also skip this step, but the collection configuration will not take effect. You are advised to select a host group during the first ingestion configuration. If you skip this step, follow either of the following ways to configure host groups after the ingestion configuration is complete:
    - Choose **Host Management > Host Groups** in the navigation pane and associate host groups with ingestion configurations.
    - Choose **Log Ingestion > Ingestion Management** in the navigation pane. In the ingestion configuration list, click **Modify** in the **Operation** column. On the page displayed, select required host groups.
2. Click **Next: Configurations**.

## Step 4: Configure the Collection

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

1. **Collection Configuration Name:** Enter 1 to 64 characters. Only letters, digits, hyphens (-), underscores (\_), and periods (.) are allowed. Do not start with a period or underscore, or end with a period.
2. **Data Source:** Select a data source type and configure it. For details, see [Table 4-17](#).

 **NOTE**

If multiple hosts are configured to collect logs from the mounted network disks or shared storage devices at the same time, duplicate logs will be collected.

**Table 4-17** Data source parameters

| Parameter                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Container standard output | <p>Collects stderr and stdout logs of a specified container in the cluster.</p> <p><b>NOTE</b><br/>The standard output of the matched container is collected to the specified log stream. Standard output to AOM stops.</p> <ul style="list-style-type: none"> <li>• <b>Output to AOM:</b> ICAgent has been installed on hosts in the cluster and collects container standard output to AOM only. This function is enabled by default. To collect container standard output to LTS, disable this function.</li> <li>• Either <b>Container Standard Output (stdout)</b> or <b>Container Standard Error (stderr)</b> must be enabled.</li> <li>• If you enable <b>Container Standard Error (stderr)</b>, select your collection destination path: <b>Collect standard output and standard error to different files (stdout.log and stderr.log)</b> or <b>Collect standard output and standard error to the same file (stdout.log)</b>.</li> <li>• <b>Allow Repeated File Collection</b> (not available to Windows)<br/>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.<br/>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</li> </ul> |



| Parameter      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Container file | <p>Collects file logs of a specified container in the cluster.</p> <ul style="list-style-type: none"> <li> <b>Add Collection Path:</b> Add one or more host paths. LTS will collect logs from these paths. For more examples, see <a href="#">Collection Paths</a>. </li> </ul> <p><b>NOTE</b><br/>If a container mount path has been configured for the CCE cluster workload, the paths added for this field are invalid. The collection paths take effect only after the mount path is deleted.</p> <ul style="list-style-type: none"> <li> <b>Add Custom Wrapping Rule:</b> ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping.<br/>The built-in rules are <i>{basename}{connector}{wrapping identifier}.{suffix}</i> and <i>{basename}.{suffix}{connector}{wrapping identifier}</i>. Connectors can be hyphens (-), periods (.), or underscores (_), wrapping identifiers can contain only non-letter characters, and the suffix can contain only letters.<br/>A custom wrapping rule consists of <i>{basename}</i> and the feature regular expression of the wrapped file. Example: If your log file name is <b>test.out.log</b> and the names after wrapping are <b>test.2024-01-01.0.out.log</b> and <b>test.2024-01-01.1.out.log</b>, configure the collection path to <b>/opt/*.log</b>, and add a custom wrapping rule: <i>{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log</i>. </li> <li> <b>Allow Repeated File Collection</b> (not available to Windows)<br/>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.<br/>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams. </li> <li> <b>Set Collection Filters:</b> Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out. </li> </ul> |

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node file        | <p>Collects files of a specified node in a cluster.</p> <ul style="list-style-type: none"> <li>• <b>Add Collection Path:</b> Add one or more host paths. LTS will collect logs from these paths. For more examples, see <a href="#">Collection Paths</a>.</li> <li>• <b>Add Custom Wrapping Rule:</b> ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping.<br/>The built-in rules are <i>{basename}{connector}{wrapping identifier}.{suffix}</i> and <i>{basename}.{suffix}{connector}{wrapping identifier}</i>. Connectors can be hyphens (-), periods (.), or underscores (_), wrapping identifiers can contain only non-letter characters, and the suffix can contain only letters.<br/>A custom wrapping rule consists of <i>{basename}</i> and the feature regular expression of the wrapped file. Example: If your log file name is <b>test.out.log</b> and the names after wrapping are <b>test.2024-01-01.0.out.log</b> and <b>test.2024-01-01.1.out.log</b>, configure the collection path to <b>/opt/*.log</b>, and add a custom wrapping rule: <i>{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log</i>.</li> <li>• <b>Allow Repeated File Collection</b> (not available to Windows)<br/>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.<br/>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</li> <li>• <b>Set Collection Filters:</b> Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.</li> </ul> |
| Kubernetes event | <p>Collects event logs of the Kubernetes cluster.</p> <p>Kubernetes events of a Kubernetes cluster can be collected to only one log stream.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

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

 **NOTE**

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

**Table 4-18** Kubernetes matching rules

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

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

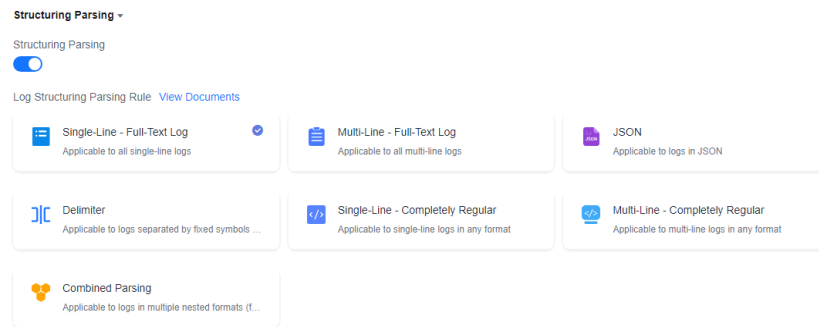
| Parameter                      | Description                                                                                                                                                                                                                                                              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

4. Enable structuring parsing. For details, see [Setting ICAgent Structuring Parsing Rules](#).

LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream.

If you have configured cloud structuring parsing, delete its configurations before configuring ICAgent structuring parsing.

**Figure 4-10** ICAgent structuring parsing configuration



5. Set other configurations.

**Table 4-19** Other configurations

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Directory Depth  | The maximum directory depth is 20 levels.<br>Collection paths can use double asterisks (**) for multi-layer fuzzy match. Specify the maximum directory depth in the text box. For example, if your log path is <b>/var/logs/department/app/a.log</b> and your collection path is <b>/var/logs/**/a.log</b> , logs will not be collected when this parameter is set to <b>1</b> , but will be collected when this parameter is set to <b>2</b> or a larger number.                                                                       |
| Split Logs           | <ul style="list-style-type: none"> <li>• If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs.</li> <li>• If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.</li> </ul> |
| Collect Binary Files | LTS can collect binary files.<br>Run the <b>file -i File_name</b> command to view the file type. <b>charset=binary</b> indicates that a log file is a binary file.<br>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.<br>If this option is disabled, binary log files will not be collected.                                                                                                                                     |

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log File Code     | The log file encoding format can be UTF-8 or GBK (not available to Windows).<br>UTF-8 encoding is a variable-length encoding mode and represents Unicode character sets. GBK, an acronym for Chinese Internal Code Extension Specification, is a Chinese character encoding standard that extends both the ASCII and GB2312 encoding systems.                                                                                                                                                              |
| Collection Policy | Select incremental or full collection. <ul style="list-style-type: none"> <li>● <b>Incremental:</b> When collecting a new file, ICAgent reads the file from the end of the file.</li> <li>● <b>All:</b> When collecting a new file, ICAgent reads the file from the beginning of the file.</li> </ul>                                                                                                                                                                                                      |
| Custom Metadata   | <ul style="list-style-type: none"> <li>● If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields.</li> <li>● If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs.<br/><b>Built-in Fields:</b> Select built-in fields as required.<br/><b>Custom Key-Value Pairs:</b> Click <b>Add</b> and set a key and value.</li> </ul> |

6. Configure the log format and time by referring to [Table 4-20](#).

 **NOTE**

The following functions are no longer recommended. Use [structuring parsing](#) instead.

**Table 4-20** Log collection settings

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Format | <ul style="list-style-type: none"> <li>● <b>Single-line:</b> Each log line is displayed as a single log event.</li> <li>● <b>Multi-line:</b> Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.</li> </ul>                                                                                                                                                                                                                                     |
| Log Time   | <p><b>System time:</b> log collection time by default. It is displayed at the beginning of each log event.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● Log collection time is the time when logs are collected and sent by ICAgent to LTS.</li> <li>● Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second.</li> <li>● Restriction on log collection time: Logs are collected within 24 hours before and after the system time.</li> </ul> |

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p><b>Time wildcard:</b> You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event.</p> <ul style="list-style-type: none"> <li>• If the time format in a log event is <b>2019-01-01 23:59:59.011</b>, the time wildcard should be set to <b>YYYY-MM-DD hh:mm:ss.SSS</b>.</li> <li>• If the time format in a log event is <b>19-1-1 23:59:59.011</b>, the time wildcard should be set to <b>YY-M-D hh:mm:ss.SSS</b>.</li> </ul> <p><b>NOTE</b><br/>If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p><b>Example:</b></p> <pre> YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)                     </pre> |
| Log Segmentation      | <p>This parameter needs to be specified if the <b>Log Format</b> is set to <b>Multi-line</b>. <b>By generation time</b> indicates that a time wildcard is used to detect log boundaries, whereas <b>By regular expression</b> indicates that a regular expression is used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| By regular expression | <p>You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select <b>Multi-line</b> for <b>Log Format</b> and <b>By regular expression</b> for <b>Log Segmentation</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

 **NOTE**

The time wildcard and regular expression will look for the specified pattern right from the beginning of each log line. If no match is found, the system time, which may be different from the time in the log event, is used. In general cases, you are advised to select **Single-line** for **Log Format** and **System time** for **Log Time**.

7. Click **Next: Index Settings**.



## Step 5: Configure Indexing

1. (Optional) Configure indexing. For details, see [Setting Indexes](#).
2. Click **Submit**.



## Step 6: Complete the Ingestion Configuration

The created ingestion configuration will be displayed.

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

### NOTE

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

- To stop log collection of an ingestion configuration, toggle off  in the **Status** column to disable the configuration. To restart log collection, toggle on  in the **Status** column.

### NOTE

Disabling an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. Exercise caution when performing this operation.

- Click **More > ICAgent Collect Diagnosis** in the **Operation** column of the ingestion configuration to monitor the exceptions, overall status, and collection status of ICAgent.

## Setting Multiple Ingestion Configurations in a Batch

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

- Step 1** On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see [Table 4-21](#).

**Table 4-21** Adding configurations in batches

| Type           | Parameter      | Description                                  |
|----------------|----------------|----------------------------------------------|
| Basic Settings | Ingestion Type | Select <b>CCE (Cloud Container Engine)</b> . |

| Type               | Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | Configurations to Add | Enter the number of ingestion configurations in the text box and click <b>Add</b> .<br><br>A maximum of 100 ingestion configurations can be added, including the one already exists under <b>Ingestion Settings</b> by default. Therefore, you can add up to 99 more.                                                                                                                                                                                           |
| Ingestion Settings | Configuration List    | <ol style="list-style-type: none"> <li>1. The ingestion configurations are displayed on the left. You can add up to 99 more configurations.</li> <li>2. The ingestion configuration details are displayed on the right. Set them by referring to <b>Step 4: Configure the Collection</b>.</li> <li>3. After an ingestion configuration is complete, you can click <b>Apply to Other Configurations</b> to copy its settings to other configurations.</li> </ol> |

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

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

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

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. If you toggle off the switch in the **Status** column of an ingestion configuration, logs will not be collected for this configuration.
- Select multiple existing ingestion configurations and click **Delete**.

----End

## 4.2.8 Ingesting ECS Text Logs to LTS

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

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

Perform the following steps to complete the ingestion configuration:


1. [Step 1: Select a Log Stream](#)
2. [Step 2: \(Optional\) Select a Host Group](#)
3. [Step 3: Configure the Collection](#)
4. [Step 4: Configure Indexing](#)
5. [Step 5: Complete the Ingestion Configuration](#)

To collect logs from multiple scenarios, [set multiple ingestion configurations in a batch](#).

## Prerequisites

ICAgent has been [installed](#) and [added](#) to the host group. You have enabled **ICAgent Diagnosis** to view exceptions, overall status, and collection status of ICAgent. For details, see [Setting ICAgent Collection](#).

## Step 1: Select a Log Stream

1. Log in to the [LTS console](#).
2. Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **ECS (Elastic Cloud Server)**.  
Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > ECS (Elastic Cloud Server)**.  
Alternatively, choose **Log Management** in the navigation pane and click the target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and click **Ingest Log**. In the displayed dialog box, click **ECS (Elastic Cloud Server)**.
3. Select a log group from the **Log Group** drop-down list. If there is no desired log group, click **Create Log Group**. For details, see [Managing Log Groups](#).
4. Select a log stream from the **Log Stream** drop-down list. If there is no desired log stream, click **Create Log Stream**. For details, see [Managing Log Streams](#).
5. Click **Next: (Optional) Select Host Group**.

## Step 2: (Optional) Select a Host Group

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

### NOTE

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

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

## Step 3: Configure the Collection

After selecting host groups, configure the collection as follows:

 NOTE

- Ensure that sensitive information is not collected.
- If a collection path of a host has been configured in AOM, do not configure the path in LTS.
- When configuring log ingestion, you can select multiple host groups and add multiple hosts to a host group. Therefore, you can control log ingestion by setting paths of different hosts and selecting multiple host groups.
- If log files were last modified more than 12 hours earlier than the time when the path is added, the files are not collected.
- LTS cannot collect logs of PostgreSQL (database) instances.

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

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

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

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

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

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

 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 Web Application Firewall (WAF) and configure the path again.

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

`/var/logs/1/a.log`

`/var/logs/2/a.log`

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

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

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

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

`/var/logs/service/a1.log`

`/var/logs/service/a2.log`

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

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

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

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

After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see [Checking the ICAgent Version Description](#).

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

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

Blacklist filters can be exact matches or wildcard pattern matches. For details, see [Collection Paths](#).

#### NOTE

- If you blacklist a file or directory that has been set as a collection path in the previous step, the blacklist settings will be used and the file or files in the directory will be filtered out.
  - If a log has been added to the blacklist, it cannot be collected even if you create a log ingestion task. You can collect it again only after you delete the collection path from the blacklist.
  - If you specify a directory, all files in the directory are filtered out, but log files in the folders in the directory cannot be filtered out.
- ### 5. Collect Windows Event Logs: To collect logs from Windows hosts, enable this option and set the following parameters.

**Table 4-22** Parameters for collecting windows event logs

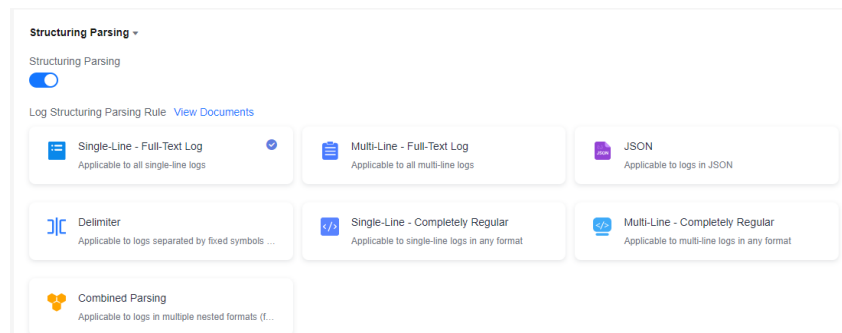
| Parameter                    | Description                                                                                                                                                                                                                                                        |
|------------------------------|--------------------------------------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

6. Enable structuring parsing. For details, see [Setting ICAgent Structuring Parsing Rules](#).

LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream.

If you have configured cloud structuring parsing, delete its configurations before configuring ICAgent structuring parsing.

**Figure 4-11** ICAgent structuring parsing configuration



7. Set other configurations.

**Table 4-23** Other configurations

| Parameter           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Directory Depth | The maximum directory depth is 20 levels.<br>Collection paths can use double asterisks ( <b>**</b> ) for multi-layer fuzzy match. Specify the maximum directory depth in the text box. For example, if your log path is <b>/var/logs/department/app/a.log</b> and your collection path is <b>/var/logs/**/a.log</b> , logs will not be collected when this parameter is set to <b>1</b> , but will be collected when this parameter is set to <b>2</b> or a larger number. |

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Split Logs           | <ul style="list-style-type: none"> <li>If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs.</li> <li>If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.</li> </ul>                        |
| Collect Binary Files | <p>LTS can collect binary files.</p> <p>Run the <b>file -i <i>File_name</i></b> command to view the file type. <b>charset=binary</b> indicates that a log file is a binary file.</p> <p>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.</p> <p>If this option is disabled, binary log files will not be collected.</p>                                                                                                                              |
| Log File Code        | <p>The log file encoding format can be UTF-8 or GBK (not available to Windows).</p> <p>UTF-8 encoding is a variable-length encoding mode and represents Unicode character sets. GBK, an acronym for Chinese Internal Code Extension Specification, is a Chinese character encoding standard that extends both the ASCII and GB2312 encoding systems.</p>                                                                                                                                                                                                   |
| Collection Policy    | <p>Select incremental or full collection.</p> <ul style="list-style-type: none"> <li><b>Incremental:</b> When collecting a new file, ICAgent reads the file from the end of the file.</li> <li><b>All:</b> When collecting a new file, ICAgent reads the file from the beginning of the file.</li> </ul>                                                                                                                                                                                                                                                   |
| Custom Metadata      | <ul style="list-style-type: none"> <li>If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields.</li> <li>If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs. <ul style="list-style-type: none"> <li><b>Built-in Fields:</b> Select built-in fields as required.</li> <li><b>Custom Key-Value Pairs:</b> Click <b>Add</b> and set a key and value.</li> </ul> </li> </ul> |

- Configure the log format and time by referring to [Table 4-24](#).

**Table 4-24** Log collection settings

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Format       | <ul style="list-style-type: none"> <li>• <b>Single-line:</b> Each log line is displayed as a single log event.</li> <li>• <b>Multi-line:</b> Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Log Time         | <p><b>System time:</b> log collection time by default. It is displayed at the beginning of each log event.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Log collection time is the time when logs are collected and sent by ICAgent to LTS.</li> <li>• Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second.</li> <li>• Restriction on log collection time: Logs are collected within 24 hours before and after the system time.</li> </ul> <p><b>Time wildcard:</b> You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event.</p> <ul style="list-style-type: none"> <li>• If the time format in a log event is <b>2019-01-01 23:59:59.011</b>, the time wildcard should be set to <b>YYYY-MM-DD hh:mm:ss.SSS</b>.</li> <li>• If the time format in a log event is <b>19-1-1 23:59:59.011</b>, the time wildcard should be set to <b>YY-M-D hh:mm:ss.SSS</b>.</li> </ul> <p><b>NOTE</b><br/>If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p><b>Example:</b></p> <pre> YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00) </pre> |
| Log Segmentation | <p>This parameter needs to be specified if the <b>Log Format</b> is set to <b>Multi-line</b>. <b>By generation time</b> indicates that a time wildcard is used to detect log boundaries, whereas <b>By regular expression</b> indicates that a regular expression is used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



| Parameter             | Description                                                                                                                                                                                                                                                           |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| By regular expression | You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select <b>Multi-line</b> for <b>Log Format</b> and <b>By regular expression</b> for <b>Log Segmentation</b> . |

 **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**.

9. Click **Next: Index Settings**.

### Step 4: Configure Indexing

1. (Optional) Configure indexing. For details, see [Setting Indexes](#).
2. Click **Submit**.



### Step 5: Complete the Ingestion Configuration

The created ingestion configuration will be displayed.

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

 **NOTE**

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

- To stop log collection of an ingestion configuration, toggle off  in the **Status** column to disable the configuration. To restart log collection, toggle on  in the **Status** column.

 **NOTE**

Disabling an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. Exercise caution when performing this operation.

- Click **More > ICAgent Collect Diagnosis** in the **Operation** column of the ingestion configuration to monitor the exceptions, overall status, and collection status of ICAgent.

## Setting Multiple Ingestion Configurations in a Batch

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

- Step 1** On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see [Table 4-25](#).

**Table 4-25** Adding configurations in batches

| Type               | Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic Settings     | Ingestion Type        | Select <b>ECS (Elastic Cloud Server)</b> .                                                                                                                                                                                                                                                                                                                                                                                                                      |
|                    | Configurations to Add | Enter the number of ingestion configurations in the text box and click <b>Add</b> .<br><br>A maximum of 100 ingestion configurations can be added, including the one already exists under <b>Ingestion Settings</b> by default. Therefore, you can add up to 99 more.                                                                                                                                                                                           |
| Ingestion Settings | Configuration List    | <ol style="list-style-type: none"> <li>The ingestion configurations are displayed on the left. You can add up to 99 more configurations.</li> <li>The ingestion configuration details are displayed on the right. Set them by referring to <a href="#">Step 3: Configure the Collection</a>.</li> <li>After an ingestion configuration is complete, you can click <b>Apply to Other Configurations</b> to copy its settings to other configurations.</li> </ol> |

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

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

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

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. If you toggle off the switch in the **Status** column of an ingestion configuration, logs will not be collected for this configuration.
- Select multiple existing ingestion configurations and click **Delete**.

----End

### 4.2.9 Ingesting ServiceStage Containerized Application Logs to LTS

LTS collects log data from containerized applications of ServiceStage. 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.

Perform the following steps to complete the ingestion configuration:

1. [Step 1: Select a Log Stream](#)
2. [Step 2: Check Dependencies](#)
3. [Step 3: \(Optional\) Select a Host Group](#)
4. [Step 4: Configure the Collection](#)
5. [Step 5: Configure Indexing](#)
6. [Step 6: Complete the Ingestion Configuration](#)

To collect logs from multiple scenarios, [set multiple ingestion configurations in a batch](#).

#### NOTE

Currently, this function is available only to whitelisted users. To use it, [submit a service ticket](#).

## Prerequisites

- ICAgent has been installed and added to the host group.
- A ServiceStage application has been created. For details, see [Creating an Application](#).
- A ServiceStage environment has been created. For details, see [Creating an Environment](#).
- A ServiceStage component has been created. For details, see [Creating and Deploying a Component](#).
- You have enabled **ICAgent Diagnosis** to view exceptions, overall status, and collection status of ICAgent. For details, see [Setting ICAgent Collection](#).

## Constraints


- CCE cluster nodes whose container engine is Docker are supported.
- CCE cluster nodes whose container engine is Containerd are supported. You must be using ICAgent 5.12.130 or later.
- To collect container log directories mounted to host directories to LTS, you must configure the node file path.
- Constraints on the Docker storage driver: Currently, container file log collection supports only the overlay2 storage driver. devicemapper cannot be used as the storage driver. Run the following command to check the storage driver type:

```
docker info | grep "Storage Driver"
```

## Step 1: Select a Log Stream

1. Log in to the [LTS console](#).
2. Choose **Log Ingestion** > **Ingestion Center** in the navigation pane. Then, click **ServiceStage - Containerized Application Logs** under **Self-Built software**.

Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > ServiceStage - Containerized Application Logs**.

Alternatively, choose **Log Management** in the navigation pane and click the target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and click **Ingest Log**. In the displayed dialog box, click **ServiceStage - Containerized Application Logs** under **Self-Built software**.

3. In the **Select Log Stream** step, set the following parameters:
  - a. Select a ServiceStage application and ServiceStage environment.
  - b. Select a log group from the **Log Group** drop-down list. If there are no desired log groups, click **Create Log Group** to create one.
  - c. Select a log stream from the **Log Stream** drop-down list. If there are no desired log streams, click **Create Log Stream** to create one.
4. Click **Next: Check Dependencies**.

## Step 2: Check Dependencies

1. The system automatically checks whether there is a host group with the custom identifier **k8s-log-Application ID**.  
If not, click **Auto Correct**.

### NOTE

- **Auto Correct:** Configure dependencies with one click.
  - **Check Again:** Recheck dependencies.
2. Click **Next: (Optional) Select Host Group**.

## Step 3: (Optional) Select a Host Group

1. In the host group list, the host group to which the cluster belongs is selected by default. You can also select host groups as required.
2. Click **Next: Configurations**.

## Step 4: Configure the Collection

When you configure ServiceStage containerized application log ingestion, the collection configuration details are as follows.

1. **Collection Configuration Name:** Enter 1 to 64 characters. Only letters, digits, hyphens (-), underscores (\_), and periods (.) are allowed. Do not start with a period or underscore, or end with a period.
2. **Data Source:** Select a data source type and configure it. The following data source types are supported: container standard output, container file path, node file path, and K8s event.

**Table 4-26** Collection configuration parameters

| Type                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Container standard output | <p>Collects stderr and stdout logs of a specified container in the cluster. Either <b>Container Standard Output (stdout)</b> or <b>Container Standard Error (stderr)</b> must be enabled.</p> <ul style="list-style-type: none"> <li>• If you enable <b>Container Standard Error (stderr)</b>, select your collection destination path: <b>Collect standard output and standard error to different files (stdout.log and stderr.log)</b> or <b>Collect standard output and standard error to the same file (stdout.log)</b>.</li> <li>• The standard output of the matched container is collected to the specified log stream. Standard output to AOM stops.</li> <li>• <b>Allow Repeated File Collection</b> (not available to Windows)<br/>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.<br/>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</li> </ul>                           |
| Container file            | <p>Collects file logs of a specified container in the cluster.</p> <ul style="list-style-type: none"> <li>• <b>Collection Paths:</b> Add one or more host paths. LTS will collect logs from these paths. For details, see <a href="#">2</a>.</li> </ul> <p><b>NOTE</b><br/>If a container mount path has been configured for the CCE cluster workload, the paths added for this field are invalid. The collection paths take effect only after the mount path is deleted.</p> <ul style="list-style-type: none"> <li>• <b>Allow Repeated File Collection</b> (not available to Windows)<br/>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.<br/>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</li> <li>• <b>Set Collection Filters:</b> Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.</li> </ul> |

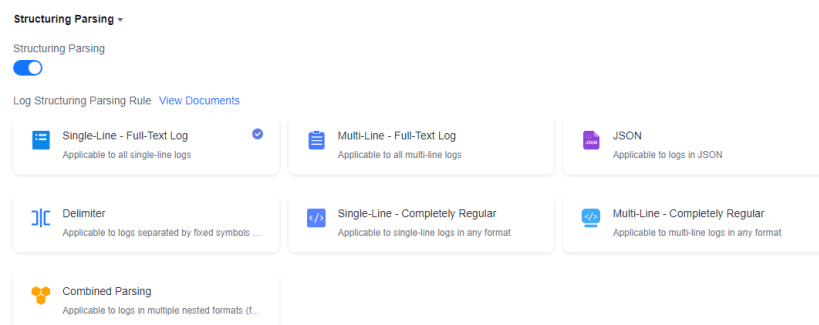
| Type             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node file        | <p>Collects files of a specified node in a cluster.</p> <ul style="list-style-type: none"> <li>● <b>Collection Paths:</b> Add one or more host paths. LTS will collect logs from these paths.</li> <li>● <b>Allow Repeated File Collection</b> (not available to Windows)<br/>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.</li> </ul> <p>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</p> <ul style="list-style-type: none"> <li>● <b>Set Collection Filters:</b> Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.</li> </ul> |
| Kubernetes event | <p>Collects event logs of the Kubernetes cluster. You do not need to set parameters. Only ICAgent 5.12.150 or later is supported.</p> <p><b>NOTE</b><br/>Kubernetes events of a Kubernetes cluster can be collected to only one log stream.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

3. If you select **Container standard output** or **Container file** as the data source type, set the ServiceStage matching rule by selecting the corresponding component from the drop-down list.
4. Enable structuring parsing. For details, see [Setting ICAgent Structuring Parsing Rules](#).

LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream.

If you have configured cloud structuring parsing, delete its configurations before configuring ICAgent structuring parsing.

**Figure 4-12** ICAgent structuring parsing configuration



5. Set other configurations.

**Table 4-27** Other configurations

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Directory Depth  | <p>The maximum directory depth is 20 levels.</p> <p>Collection paths can use double asterisks (**) for multi-layer fuzzy match. Specify the maximum directory depth in the text box. For example, if your log path is <b>/var/logs/department/app/a.log</b> and your collection path is <b>/var/logs/**/a.log</b>, logs will not be collected when this parameter is set to <b>1</b>, but will be collected when this parameter is set to <b>2</b> or a larger number.</p>                                                              |
| Split Logs           | <ul style="list-style-type: none"> <li>• If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs.</li> <li>• If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.</li> </ul> |
| Collect Binary Files | <p>LTS can collect binary files.</p> <p>Run the <b>file -i File_name</b> command to view the file type. <b>charset=binary</b> indicates that a log file is a binary file.</p> <p>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.</p> <p>If this option is disabled, binary log files will not be collected.</p>                                                                                                                  |
| Log File Code        | <p>The log file encoding format can be UTF-8 or GBK (not available to Windows).</p> <p>UTF-8 encoding is a variable-length encoding mode and represents Unicode character sets. GBK, an acronym for Chinese Internal Code Extension Specification, is a Chinese character encoding standard that extends both the ASCII and GB2312 encoding systems.</p>                                                                                                                                                                                |
| Collection Policy    | <p>Select incremental or full collection.</p> <ul style="list-style-type: none"> <li>• <b>Incremental:</b> When collecting a new file, ICAgent reads the file from the end of the file.</li> <li>• <b>All:</b> When collecting a new file, ICAgent reads the file from the beginning of the file.</li> </ul>                                                                                                                                                                                                                            |

| Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Custom Metadata | <ul style="list-style-type: none"> <li>If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields.</li> <li>If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs.<br/><b>Built-in Fields:</b> Select built-in fields as required.<br/><b>Custom Key-Value Pairs:</b> Click <b>Add</b> and set a key and value.</li> </ul> |

6. Configure the log format and time by referring to [Table 4-28](#).

**Table 4-28** Log collection settings

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Format | <ul style="list-style-type: none"> <li><b>Single-line:</b> Each log line is displayed as a single log event.</li> <li><b>Multi-line:</b> Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.</li> </ul>                                                                                                                                                                                                                                   |
| Log Time   | <p><b>System time:</b> log collection time by default. It is displayed at the beginning of each log event.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Log collection time is the time when logs are collected and sent by ICAgent to LTS.</li> <li>Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second.</li> <li>Restriction on log collection time: Logs are collected within 24 hours before and after the system time.</li> </ul> |



| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p><b>Time wildcard:</b> You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event.</p> <ul style="list-style-type: none"> <li>• If the time format in a log event is <b>2019-01-01 23:59:59.011</b>, the time wildcard should be set to <b>YYYY-MM-DD hh:mm:ss.SSS</b>.</li> <li>• If the time format in a log event is <b>19-1-1 23:59:59.011</b>, the time wildcard should be set to <b>YY-M-D hh:mm:ss.SSS</b>.</li> </ul> <p><b>NOTE</b><br/>If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p><b>Example:</b></p> <pre> YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)                     </pre> |
| Log Segmentation      | <p>This parameter needs to be specified if the <b>Log Format</b> is set to <b>Multi-line</b>. <b>By generation time</b> indicates that a time wildcard is used to detect log boundaries, whereas <b>By regular expression</b> indicates that a regular expression is used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| By regular expression | <p>You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select <b>Multi-line</b> for <b>Log Format</b> and <b>By regular expression</b> for <b>Log Segmentation</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

7. Click **Next: Index Settings**.

## Step 5: Configure Indexing

1. (Optional) Configure indexing. For details, see [Setting Indexes](#).
2. Click **Submit**.

## Step 6: Complete the Ingestion Configuration



The created ingestion configuration will be displayed.

- Click its name to view its details.

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

 **NOTE**

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

- To stop log collection of an ingestion configuration, toggle off  in the **Status** column to disable the configuration. To restart log collection, toggle on  in the **Status** column.

 **NOTE**

Disabling an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. Exercise caution when performing this operation.

- Click **More > ICAgent Collect Diagnosis** in the **Operation** column of the ingestion configuration to monitor the exceptions, overall status, and collection status of ICAgent.

## Setting Multiple Ingestion Configurations in a Batch

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

- Step 1** On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see [Table 4-29](#).

**Table 4-29** Adding configurations in batches

| Type           | Parameter             | Description                                                                                                                                                                                                                                                       |
|----------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic Settings | Ingestion Type        | Select <b>ServiceStage - Containerized Application Logs</b> .                                                                                                                                                                                                     |
|                | Configurations to Add | Enter the number of ingestion configurations in the text box and click <b>Add</b> .<br>A maximum of 100 ingestion configurations can be added, including the one already exists under <b>Ingestion Settings</b> by default. Therefore, you can add up to 99 more. |

| Type               | Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ingestion Settings | Configuration List | <ol style="list-style-type: none"> <li>1. The ingestion configurations are displayed on the left. You can add up to 99 more configurations.</li> <li>2. The ingestion configuration details are displayed on the right. Set them by referring to <a href="#">Step 4: Configure the Collection</a>.</li> <li>3. After an ingestion configuration is complete, you can click <b>Apply to Other Configurations</b> to copy its settings to other configurations.</li> </ol> |

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

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

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

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. If you toggle off the switch in the **Status** column of an ingestion configuration, logs will not be collected for this configuration.
- Select multiple existing ingestion configurations and click **Delete**.

----End

## 4.2.10 Ingesting ServiceStage Cloud Host Logs to LTS

LTS collects log data from cloud hosts of ServiceStage. 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.

Perform the following steps to complete the ingestion configuration:

1. [Step 1: Select a Log Stream](#)
2. [Step 2: \(Optional\) Select a Host Group](#)
3. [Step 3: Configure the Collection](#)
4. [Step 4: Configure Indexing](#)
5. [Step 5: Complete the Ingestion Configuration](#)

To collect logs from multiple scenarios, [set multiple ingestion configurations in a batch](#).


### NOTE

Currently, this function is available only to whitelisted users. To use it, [submit a service ticket](#).

## Prerequisites

- ICAgent has been installed and added to the host group.
- A ServiceStage application has been created. For details, see [Creating an Application](#).
- A ServiceStage environment has been created. For details, see [Creating an Environment](#).
- A ServiceStage component has been created. For details, see [Creating and Deploying a Component](#).
- You have enabled **ICAgent Diagnosis** to view exceptions, overall status, and collection status of ICAgent. For details, see [Setting ICAgent Collection](#).

## Step 1: Select a Log Stream

1. Log in to the [LTS console](#).
2. Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **ServiceStage - Cloud Host Logs**.  
Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > ServiceStage - Cloud Host Logs**.  
Alternatively, choose **Log Management** in the navigation pane and click the target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and click **Ingest Log**. In the displayed dialog box, click **ServiceStage - Cloud Host Logs**.
3. In the **Select Log Stream** step, set the following parameters:
  - a. Select a ServiceStage application and ServiceStage environment.
  - b. Select a log group from the **Log Group** drop-down list. If there are no desired log groups, click **Create Log Group** to create one.
  - c. Select a log stream from the **Log Stream** drop-down list. If there are no desired log streams, click **Create Log Stream** to create one.
4. Click **Next: (Optional) Select Host Group**.

## Step 2: (Optional) Select a Host Group

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

### NOTE

You can skip this step and configure host groups after the ingestion configuration is complete. There are two ways to do this:

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

## Step 3: Configure the Collection

Perform the following steps to configure the collection:

1. **Collection Configuration Name:** Enter 1 to 64 characters. Only letters, digits, hyphens (-), underscores (\_), and periods (.) are allowed. Do not start with a period or underscore, or end with a period.
2. **Collection Paths:** Add one or more host paths. LTS will collect logs from these paths. The rules for setting collection paths are as follows:

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

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

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

### 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 WAF and configure the path again.

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

```
/var/logs/1/a.log
/var/logs/2/a.log
```
  - Example 2: **/var/logs/service-\*/a.log** will match files as follows:  

```
/var/logs/service-1/a.log
/var/logs/service-2/a.log
```
  - Example 3: **/var/logs/service/a\*.log** will match files as follows:  

```
/var/logs/service/a1.log
/var/logs/service/a2.log
```
- If the collection path is set to a file name, the corresponding file is collected. Only text files can be collected.
3. **Allow Repeated File Collection** (not available to Windows)  
After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see [Checking the ICAgent Version Description](#).

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

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

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

**Table 4-30** Parameters for collecting windows event logs

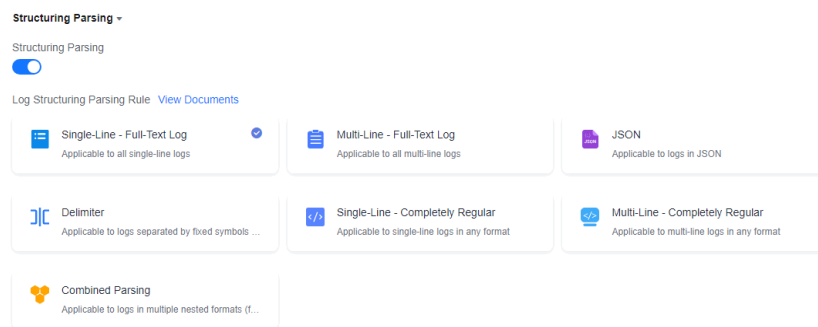
| Parameter                    | Description                                                                                                                                                                                                                                                        |
|------------------------------|--------------------------------------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

6. Set the ServiceStage matching rule by selecting the corresponding component.
7. Enable structuring parsing. For details, see [Setting ICAgent Structuring Parsing Rules](#).

LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream.

If you have configured cloud structuring parsing, delete its configurations before configuring ICAgent structuring parsing.

**Figure 4-13** ICAgent structuring parsing configuration



8. Set other configurations.

**Table 4-31** Other configurations

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Directory Depth  | The maximum directory depth is 20 levels.<br>Collection paths can use double asterisks (**) for multi-layer fuzzy match. Specify the maximum directory depth in the text box. For example, if your log path is <b>/var/logs/department/app/a.log</b> and your collection path is <b>/var/logs/**/a.log</b> , logs will not be collected when this parameter is set to <b>1</b> , but will be collected when this parameter is set to <b>2</b> or a larger number.                                                                   |
| Split Logs           | <ul style="list-style-type: none"> <li>If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs.</li> <li>If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.</li> </ul> |
| Collect Binary Files | LTS can collect binary files.<br>Run the <b>file -i File_name</b> command to view the file type. <b>charset=binary</b> indicates that a log file is a binary file.<br>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.<br>If this option is disabled, binary log files will not be collected.                                                                                                                                 |
| Log File Code        | The log file encoding format can be UTF-8 or GBK (not available to Windows).<br>UTF-8 encoding is a variable-length encoding mode and represents Unicode character sets. GBK, an acronym for Chinese Internal Code Extension Specification, is a Chinese character encoding standard that extends both the ASCII and GB2312 encoding systems.                                                                                                                                                                                       |

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Collection Policy | <p>Select incremental or full collection.</p> <ul style="list-style-type: none"> <li>● <b>Incremental:</b> When collecting a new file, ICAgent reads the file from the end of the file.</li> <li>● <b>All:</b> When collecting a new file, ICAgent reads the file from the beginning of the file.</li> </ul>                                                                                                                                                                                               |
| Custom Metadata   | <ul style="list-style-type: none"> <li>● If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields.</li> <li>● If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs.<br/><b>Built-in Fields:</b> Select built-in fields as required.<br/><b>Custom Key-Value Pairs:</b> Click <b>Add</b> and set a key and value.</li> </ul> |

9. Configure the log format and time by referring to [Table 4-32](#).

**Table 4-32** Log collection settings

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Format | <ul style="list-style-type: none"> <li>● <b>Single-line:</b> Each log line is displayed as a single log event.</li> <li>● <b>Multi-line:</b> Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.</li> </ul>                                                                                                                                                                                                                                     |
| Log Time   | <p><b>System time:</b> log collection time by default. It is displayed at the beginning of each log event.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● Log collection time is the time when logs are collected and sent by ICAgent to LTS.</li> <li>● Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second.</li> <li>● Restriction on log collection time: Logs are collected within 24 hours before and after the system time.</li> </ul> |



| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p><b>Time wildcard:</b> You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event.</p> <ul style="list-style-type: none"> <li>If the time format in a log event is <b>2019-01-01 23:59:59.011</b>, the time wildcard should be set to <b>YYYY-MM-DD hh:mm:ss.SSS</b>.</li> <li>If the time format in a log event is <b>19-1-1 23:59:59.011</b>, the time wildcard should be set to <b>YY-M-D hh:mm:ss.SSS</b>.</li> </ul> <p><b>NOTE</b><br/>If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p><b>Example:</b></p> <pre> YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)                     </pre> |
| Log Segmentation      | This parameter needs to be specified if the <b>Log Format</b> is set to <b>Multi-line</b> . <b>By generation time</b> indicates that a time wildcard is used to detect log boundaries, whereas <b>By regular expression</b> indicates that a regular expression is used.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| By regular expression | You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select <b>Multi-line</b> for <b>Log Format</b> and <b>By regular expression</b> for <b>Log Segmentation</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |

10. Click **Next: Index Settings**.

## Step 4: Configure Indexing

- (Optional) Configure indexing. For details, see [Setting Indexes](#).
- Click **Submit**.

## Step 5: Complete the Ingestion Configuration



The created ingestion configuration will be displayed.

- Click its name to view its details.
- Click **Modify** in the **Operation** column to modify the ingestion configuration.
- Click **Configure Tag** in the **Operation** column to add a tag.

- Click **More > Copy** in the **Operation** column to copy the ingestion configuration.
- Click **More > Delete** in the **Operation** column to delete the ingestion configuration.

 **NOTE**

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

- To stop log collection of an ingestion configuration, toggle off  in the **Status** column to disable the configuration. To restart log collection, toggle on  in the **Status** column.

 **NOTE**

Disabling an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. Exercise caution when performing this operation.

- Click **More > ICAgent Collect Diagnosis** in the **Operation** column of the ingestion configuration to monitor the exceptions, overall status, and collection status of ICAgent.

## Setting Multiple Ingestion Configurations in a Batch

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

- Step 1** On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see [Table 4-33](#).

**Table 4-33** Adding configurations in batches

| Type           | Parameter             | Description                                                                                                                                                                                                                                                       |
|----------------|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic Settings | Ingestion Type        | Select <b>ServiceStage - Cloud Host Logs</b> .                                                                                                                                                                                                                    |
|                | Configurations to Add | Enter the number of ingestion configurations in the text box and click <b>Add</b> .<br>A maximum of 100 ingestion configurations can be added, including the one already exists under <b>Ingestion Settings</b> by default. Therefore, you can add up to 99 more. |

| Type               | Parameter          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------|--------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ingestion Settings | Configuration List | <ol style="list-style-type: none"> <li>1. The ingestion configurations are displayed on the left. You can add up to 99 more configurations.</li> <li>2. The ingestion configuration details are displayed on the right. Set them by referring to <a href="#">Step 3: Configure the Collection</a>.</li> <li>3. After an ingestion configuration is complete, you can click <b>Apply to Other Configurations</b> to copy its settings to other configurations.</li> </ol> |

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

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

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

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. If you toggle off the switch in the **Status** column of an ingestion configuration, logs will not be collected for this configuration.
- Select multiple existing ingestion configurations and click **Delete**.

----End

## 4.2.11 Ingesting Self-Built Kubernetes Application Logs to LTS

Kubernetes is an open-source container orchestration engine. It provides automatic deployment, large-scale scalability, and containerized application management. LTS can store and analyze application logs of services and nodes reported from Kubernetes clusters.

Perform the following steps to complete the ingestion configuration:

1. [Step 1: Select a Log Stream](#)
2. [Step 2: Check Dependencies](#)
3. [Step 3: Install the Log Collection Component](#)
4. [Step 4: \(Optional\) Select a Host Group](#)
5. [Step 5: Configure the Collection](#)
6. [Step 6: Configure Indexing](#)
7. [Step 7: Complete the Ingestion Configuration](#)

To collect logs from multiple scenarios, [set multiple ingestion configurations in a batch](#).

### Prerequisites

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


- Ensure that kubectl has been configured for the Kubernetes cluster.
- You have enabled **ICAgent Diagnosis** to view exceptions, overall status, and collection status of ICAgent. For details, see [Setting ICAgent Collection](#).

## Step 1: Select a Log Stream

1. Log in to the [LTS console](#).
2. Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **Self-built K8s - Application Logs**.

Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > Self-built K8s - Application Logs**.

Alternatively, choose **Log Management** in the navigation pane and click the

target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and click **Ingest Log**. In the displayed dialog box, click **Self-built K8s - Application Logs**.

3. Choose a collection mode between **Fixed log stream** (recommended) and **Custom log stream**.

**Table 4-34** Collection modes

| Collection Mode   | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Fixed log stream  | <ul style="list-style-type: none"> <li>• Advantage: Logs of the same type are stored in the same stream for easy search.</li> <li>• Disadvantages:<br/>Since logs of different structures are collected into the same stream, log structuring and SQL visual analysis are unavailable.<br/>Since each stream has a limited write rate of 100 MB/s, there may be performance bottlenecks in heavy traffic.</li> </ul> |
| Custom log stream | <ul style="list-style-type: none"> <li>• Advantages:<br/>Since logs of different structures are collected to different streams, log structuring and SQL visual analysis are available.<br/>Since the cumulative write rate of multiple streams is not limited, there are no performance bottlenecks in heavy traffic.</li> <li>• Disadvantage: Complex management of a large number of log streams</li> </ul>        |

- If you set **Collect** to **Fixed log stream**, perform the following steps:  
Logs will be collected to a fixed log stream. The default log streams for a kubernetes cluster are **stdout-*{ClusterID}*** for standard output/errors, **hostfile-*{ClusterID}*** for node files, **event-*{ClusterID}*** for Kubernetes events, and **containerfile-*{ClusterID}*** for container files. Log streams are

automatically named with a cluster ID. For example, if the cluster ID is **Cluster01**, the standard output/error log stream is **stdout-Cluster01**.

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

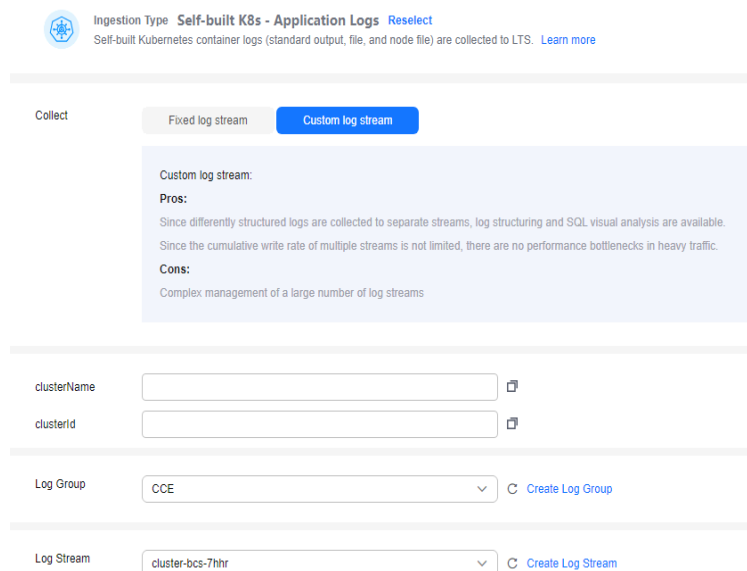
- i. Select **Fixed log stream** for **Collect**.
- ii. Enter the cluster name and ID.
- iii. Select a log group.

 **NOTE**

If there is no such group, the system displays the following message: This log group does not exist and will be automatically created to start collecting logs.

- iv. Click **Next: Check Dependencies**.
- If you set **Collect** to **Custom log stream**, perform the following steps:
- i. Select **Custom log stream**.
  - ii. Enter the cluster name and ID.
  - iii. Select a log group from the **Log Group** drop-down list. If there are no desired log groups, click **Create Log Group** to create one.
  - iv. Select a log stream from the **Log Stream** drop-down list. If there are no desired log streams, click **Create Log Stream** to create one.

**Figure 4-14** Custom log stream



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

## Step 2: Check Dependencies

1. The system automatically checks whether the following are met:

- There is a host group with the custom identifier **k8s-log-ClusterID**.
- There is a log group named **k8s-log-ClusterID**. The log retention period and description of the log group can be modified. If **Fixed log stream** is selected, this item is checked.
- The recommended log stream exists. The log retention period and description of the log stream can be modified. If **Fixed log stream** is selected, this item is checked.

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

 **NOTE**

- **Auto Correct:** a one-click option to finish the previous settings.
  - **Check Again:** Recheck dependencies.
2. Click **Next: Install ICAgent**.

### Step 3: Install the Log Collection Component

On any host in the Kubernetes cluster, perform the following steps:

1. Obtain the ICAgent installation package.
  - a. Obtain the ICAgent installation package (based on your actual information).  
`wget https://icagent-{regionId}.{obsDomainName}/ICAgent_linux/icagentK8s-5.5.1.2.tar.gz`
  - b. Decompress the ICAgent installation package.  
`tar -xvzf icagentK8s-5.5.1.2.tar.gz`
  - c. Go to the directory.  
`cd icagentK8s`
  - d. Generate installation commands:  
Select the region of ingested logs.  
Select the project ID of the ingesting account.  
For **Kubernetes Cluster**, select **Intra-Region**.
2. Install ICAgent.
  - a. Copy the ICAgent installation command. You must replace the AK/SK with the obtained one. Manually replace it when copying the command, or replace it as prompted when running the command.  
To prevent your AK/SK from being disclosed, select **Turn off command history to prevent the AK/SK from being stored** to disable historical record collection.

**Figure 4-15** Installing ICAgent

Procedure

Step 1: Copy the ICAgent installation command.

Turn off command history to prevent the AK/SK from being stored.

Installation command generated:

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

If the message **ICAgent install success** is displayed, the installation is successful. Then check the ICAgent status in the host list.

3. Click **ICAgent Already Installed**.

#### Step 4: (Optional) Select a Host Group

1. In the host group list, the host group to which the cluster belongs is selected by default. You can also select host groups as required.
2. Click **Next: Configurations**.

#### Step 5: Configure the Collection

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

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

**Table 4-35** Collection configuration parameters

| Type                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Container standard output | <p>Collects stderr and stdout logs of a specified container in the cluster.</p> <p>Collects stderr and stdout logs of a specified container in the cluster. Either <b>Container Standard Output (stdout)</b> or <b>Container Standard Error (stderr)</b> must be enabled.</p> <ul style="list-style-type: none"> <li>• If you enable <b>Container Standard Error (stderr)</b>, select your collection destination path: <b>Collect standard output and standard error to different files (stdout.log and stderr.log)</b> or <b>Collect standard output and standard error to the same file (stdout.log)</b>.</li> <li>• The standard output of the matched container is collected to the specified log stream. Standard output to AOM stops.</li> <li>• <b>Allow Repeated File Collection</b> (not available to Windows) After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.</li> </ul> <p>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</p> |

| Type           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Container file | <p>Collects file logs of a specified container path in a cluster.</p> <ul style="list-style-type: none"> <li> <b>Collection Paths:</b> Add one or more host paths. LTS will collect logs from these paths.           <p><b>NOTE</b><br/>If a container mount path has been configured for the CCE cluster workload, the paths added for this field are invalid. The collection paths take effect only after the mount path is deleted.</p> </li> <li> <b>Add Custom Wrapping Rule:</b> ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping.           <p>The built-in rules are <i>{basename}{connector}{wrapping identifier}.{suffix}</i> and <i>{basename}.{suffix}{connector}{wrapping identifier}</i>. Connectors can be hyphens (-), periods (.), or underscores (_), wrapping identifiers can contain only non-letter characters, and the suffix can contain only letters.</p> <p>A custom wrapping rule consists of <i>{basename}</i> and the feature regular expression of the wrapped file. Example: If your log file name is <b>test.out.log</b> and the names after wrapping are <b>test.2024-01-01.0.out.log</b> and <b>test.2024-01-01.1.out.log</b>, configure the collection path to <b>/opt/*.log</b>, and add a custom wrapping rule: <i>{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log</i>.</p> </li> <li> <b>Allow Repeated File Collection</b> (not available to Windows)           <p>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.</p> <p>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</p> </li> <li> <b>Set Collection Filters:</b> Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.           </li> </ul> |



| Type             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Node file        | <p>Collects files of a specified node path in a cluster.</p> <ul style="list-style-type: none"> <li>● <b>Collection Paths:</b> Add one or more host paths. LTS will collect logs from these paths.</li> <li>● <b>Add Custom Wrapping Rule:</b> ICAgent determines whether a file is wrapped based on the file name rule. If your wrapping rule does not comply with the built-in rules, you can add a custom wrap rule to prevent log loss during repeated collection and wrapping.<br/>The built-in rules are <i>{basename}{connector}{wrapping identifier}.{suffix}</i> and <i>{basename}.{suffix}{connector}{wrapping identifier}</i>. Connectors can be hyphens (-), periods (.), or underscores (_), wrapping identifiers can contain only non-letter characters, and the suffix can contain only letters.<br/>A custom wrapping rule consists of <i>{basename}</i> and the feature regular expression of the wrapped file. Example: If your log file name is <b>test.out.log</b> and the names after wrapping are <b>test.2024-01-01.0.out.log</b> and <b>test.2024-01-01.1.out.log</b>, configure the collection path to <b>/opt/*.log</b>, and add a custom wrapping rule: <i>{basename}\.\d{4}-\d{2}-\d{2}\.\d{1}.out.log</i>.</li> <li>● <b>Allow Repeated File Collection</b> (not available to Windows)<br/>After you enable this function, one host log file can be collected to multiple log streams. This function is available only to certain ICAgent versions. For details, see <a href="#">Checking the ICAgent Version Description</a>.<br/>After you disable this function, each collection path must be unique. That is, the same log file in the same host cannot be collected to different log streams.</li> <li>● <b>Set Collection Filters:</b> Blacklisted directories or files will not be collected. If you specify a directory, all files in the directory are filtered out.</li> </ul> |
| Kubernetes event | <p>Collects event logs of the Kubernetes cluster. You do not need to configure this parameter. Only ICAgent 5.12.150 or later is supported.</p> <p><b>NOTE</b><br/>Kubernetes events of a Kubernetes cluster can be collected to only one log stream.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

3. Set kubernetes matching rules only when the data source type is set to **Container standard output** or **Container file**.

 **NOTE**

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

**Table 4-36** Kubernetes matching rules

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

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

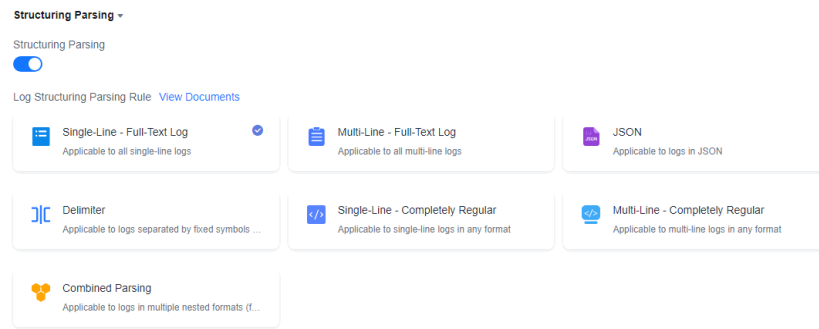
| Parameter                      | Description                                                                                                                                                                                                                                                              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

4. Enable structuring parsing. For details, see [Setting ICAgent Structuring Parsing Rules](#).

LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream.

If you have configured cloud structuring parsing, delete its configurations before configuring ICAgent structuring parsing.

**Figure 4-16** ICAgent structuring parsing configuration



5. Set other configurations.

**Table 4-37** Other configurations

| Parameter            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Directory Depth  | The maximum directory depth is 20 levels.<br>Collection paths can use double asterisks (**) for multi-layer fuzzy match. Specify the maximum directory depth in the text box. For example, if your log path is <b>/var/logs/department/app/a.log</b> and your collection path is <b>/var/logs/**/a.log</b> , logs will not be collected when this parameter is set to <b>1</b> , but will be collected when this parameter is set to <b>2</b> or a larger number.                                                                       |
| Split Logs           | <ul style="list-style-type: none"> <li>• If log splitting is enabled, logs exceeding the specified size will be split into multiple logs for collection. Specify the size in the range from 500 KB to 1,024 KB. For example, if you set the size to 500 KB, a 600 KB log will be split into a 500 KB log and a 100 KB log. This restriction is applicable to single-line logs only, not multi-line logs.</li> <li>• If log splitting is disabled, when a log exceeds 500 KB, the extra part will be truncated and discarded.</li> </ul> |
| Collect Binary Files | LTS can collect binary files.<br>Run the <b>file -i File_name</b> command to view the file type. <b>charset=binary</b> indicates that a log file is a binary file.<br>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.<br>If this option is disabled, binary log files will not be collected.                                                                                                                                     |

| Parameter         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log File Code     | <p>The log file encoding format can be UTF-8 or GBK (not available to Windows).</p> <p>UTF-8 encoding is a variable-length encoding mode and represents Unicode character sets. GBK, an acronym for Chinese Internal Code Extension Specification, is a Chinese character encoding standard that extends both the ASCII and GB2312 encoding systems.</p>                                                                                                                                                   |
| Collection Policy | <p>Select incremental or full collection.</p> <ul style="list-style-type: none"> <li>● <b>Incremental:</b> When collecting a new file, ICAgent reads the file from the end of the file.</li> <li>● <b>All:</b> When collecting a new file, ICAgent reads the file from the beginning of the file.</li> </ul>                                                                                                                                                                                               |
| Custom Metadata   | <ul style="list-style-type: none"> <li>● If this option is disabled, ICAgent will report logs to LTS based on the default system fields. You do not need to and cannot configure the fields.</li> <li>● If this option is enabled, ICAgent will report logs based on your selected built-in fields and fields created with custom key-value pairs.<br/><b>Built-in Fields:</b> Select built-in fields as required.<br/><b>Custom Key-Value Pairs:</b> Click <b>Add</b> and set a key and value.</li> </ul> |

6. Configure the log format and time by referring to [Table 4-38](#).

**Table 4-38** Log collection settings

| Parameter  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Log Format | <ul style="list-style-type: none"> <li>● <b>Single-line:</b> Each log line is displayed as a single log event.</li> <li>● <b>Multi-line:</b> Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.</li> </ul>                                                                                                                                                                                                                                     |
| Log Time   | <p><b>System time:</b> log collection time by default. It is displayed at the beginning of each log event.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● Log collection time is the time when logs are collected and sent by ICAgent to LTS.</li> <li>● Log printing time is the time when logs are printed. ICAgent collects and sends logs to LTS with an interval of 1 second.</li> <li>● Restriction on log collection time: Logs are collected within 24 hours before and after the system time.</li> </ul> |

| Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | <p><b>Time wildcard:</b> You can set a time wildcard so that ICAgent will look for the log printing time as the beginning of a log event.</p> <ul style="list-style-type: none"> <li>• If the time format in a log event is <b>2019-01-01 23:59:59.011</b>, the time wildcard should be set to <b>YYYY-MM-DD hh:mm:ss.SSS</b>.</li> <li>• If the time format in a log event is <b>19-1-1 23:59:59.011</b>, the time wildcard should be set to <b>YY-M-D hh:mm:ss.SSS</b>.</li> </ul> <p><b>NOTE</b><br/>If a log event does not contain year information, ICAgent regards it as printed in the current year.</p> <p><b>Example:</b></p> <pre> YY - year (19) YYYY - year (2019) M - month (1) MM - month (01) D - day (1) DD - day (01) hh - hours (23) mm - minutes (59) ss - seconds (59) SSS - millisecond (999) hpm - hours (03PM) h:mmpm - hours:minutes (03:04PM) h:mm:sspm - hours:minutes:seconds (03:04:05PM) hh:mm:ss ZZZZ (16:05:06 +0100) hh:mm:ss ZZZ (16:05:06 CET) hh:mm:ss ZZ (16:05:06 +01:00)                     </pre> |
| Log Segmentation      | <p>This parameter needs to be specified if the <b>Log Format</b> is set to <b>Multi-line</b>. <b>By generation time</b> indicates that a time wildcard is used to detect log boundaries, whereas <b>By regular expression</b> indicates that a regular expression is used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| By regular expression | <p>You can set a regular expression to look for a specific pattern to indicate the beginning of a log event. This parameter needs to be specified when you select <b>Multi-line</b> for <b>Log Format</b> and <b>By regular expression</b> for <b>Log Segmentation</b>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

 **NOTE**

The time wildcard and regular expression will look for the specified pattern right from the beginning of each log line. If no match is found, the system time, which may be different from the time in the log event, is used. In general cases, you are advised to select **Single-line** for **Log Format** and **System time** for **Log Time**.

7. Click **Next: Index Settings**.

## Step 6: Configure Indexing

1. (Optional) Configure indexing. For details, see [Setting Indexes](#).
2. Click **Submit**.



## Step 7: Complete the Ingestion Configuration

The created ingestion configuration will be displayed.

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

### NOTE

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

- To stop log collection of an ingestion configuration, toggle off  in the **Status** column to disable the configuration. To restart log collection, toggle on  in the **Status** column.

### NOTE

Disabling an ingestion configuration may lead to log collection failures, potentially resulting in service exceptions related to user logs. Exercise caution when performing this operation.

- Click **More > ICAgent Collect Diagnosis** in the **Operation** column of the ingestion configuration to monitor the exceptions, overall status, and collection status of ICAgent.

## Setting Multiple Ingestion Configurations in a Batch

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

- Step 1** On the **Ingestion Management** page, click **Batch Ingest** to go to the details page. For details, see [Table 4-39](#).

**Table 4-39** Adding configurations in batches

| Type           | Parameter      | Description                                       |
|----------------|----------------|---------------------------------------------------|
| Basic Settings | Ingestion Type | Select <b>Self-built K8s - Application Logs</b> . |



| Type               | Parameter             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                    | Configurations to Add | Enter the number of ingestion configurations in the text box and click <b>Add</b> .<br><br>A maximum of 100 ingestion configurations can be added, including the one already exists under <b>Ingestion Settings</b> by default. Therefore, you can add up to 99 more.                                                                                                                                                                                           |
| Ingestion Settings | Configuration List    | <ol style="list-style-type: none"> <li>1. The ingestion configurations are displayed on the left. You can add up to 99 more configurations.</li> <li>2. The ingestion configuration details are displayed on the right. Set them by referring to <b>Step 5: Configure the Collection</b>.</li> <li>3. After an ingestion configuration is complete, you can click <b>Apply to Other Configurations</b> to copy its settings to other configurations.</li> </ol> |

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

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

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

- Select multiple existing ingestion configurations and click **Edit**. On the displayed page, select an ingestion type to modify the corresponding ingestion configurations.
- Select multiple existing ingestion configurations and click **Enable** or **Disable**. If you toggle off the switch in the **Status** column of an ingestion configuration, logs will not be collected for this configuration.
- Select multiple existing ingestion configurations and click **Delete**.

----End

## 4.2.12 Setting ICAgent Structuring Parsing Rules

You can use ICAgent to collect logs to LTS. When creating a log ingestion task, you can customize collection policies, such as parsing, whitelist, and blacklist rules, and raw log uploading settings. An ICAgent collection configuration defines the process of collecting logs of the same type from a server, parsing them, and sending them to a specified log stream.

### Advantages

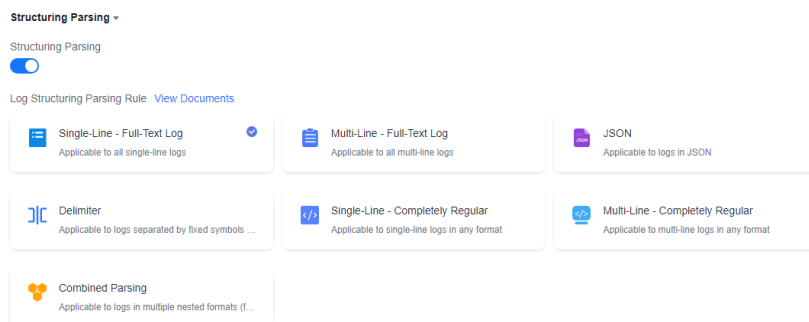
- Collecting log data in non-intrusive mode as log files: You do not need to modify application code, and log collection does not affect application running.
- Handling various exceptions during log collection: Security measures such as proactive retry and local cache are taken when a network or server exception occurs.
- Centralized management: After installing ICAgent, you only need to set configurations such as host groups and ICAgent collection on the LTS console.

- Comprehensive self-protection mechanisms: ICAgent is designed with strict limitations and protective measures regarding CPU, memory, and network usage, to minimize its impact on the performance of other services sharing the same server.

Before configuring log ingestion, get to know the structuring parsing rules of ICAgent collection to facilitate your operations. LTS enables combined parsing, allowing you to create different structuring parsing rules for each collection configuration of a log stream.

LTS supports the following log structuring parsing rules:

- **Single-Line - Full-Text Log**: Each log line is displayed as a single log event.
- **Multi-Line - Full-Text Log**: Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.
- **JSON**: splits JSON logs into key-value pairs.
- **Delimiter**: applicable to logs separated by fixed symbols (such as spaces, commas, and colons).
- **Single-Line - Completely Regular**: uses a regular expression to extract fields from single-line logs in any format. After entering a regular expression, click **Verify** to verify it.
- **Multi-Line - Completely Regular**: uses a regular expression to extract fields from multi-line logs in any format. The regular expression of the first line can be automatically generated or manually entered. After entering a regular expression, click **Verify** to verify it.
- **Combined Parsing**: applicable to logs in multiple nested formats, for example, JSON logs with delimiters. For logs with complex structures and requiring multiple parsing modes, you can use this mode. It allows you to input code of JSON format on the console to define the pipeline logic for log parsing. You can add one or more plug-in processing configurations. ICAgent executes the configurations one by one based on the specified sequence.



 **NOTE**

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

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


### Single-Line - Full-Text Log

If you want to display each line of log data as a single log on the LTS page, select **Single-Line**.

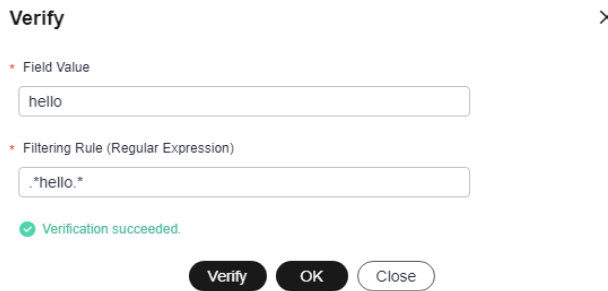
1. Select **Single-Line - Full-Text Log**.
2. Enable **Log Filtering** (disabled by default) as required and add a maximum of 20 whitelist or blacklist rules.


**Figure 4-17** Log filtering rules



- Add a whitelist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a matching criterion, collecting and reporting only logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). In single-line and multi-line full-text modes, **content** is used as the key name *{key}* of the full text by default. The relationship between multiple filtering rules is **OR**. For example, to collect log events containing **hello** from the log source file, set the filtering rule to **.\*hello.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

**Figure 4-18** Verification

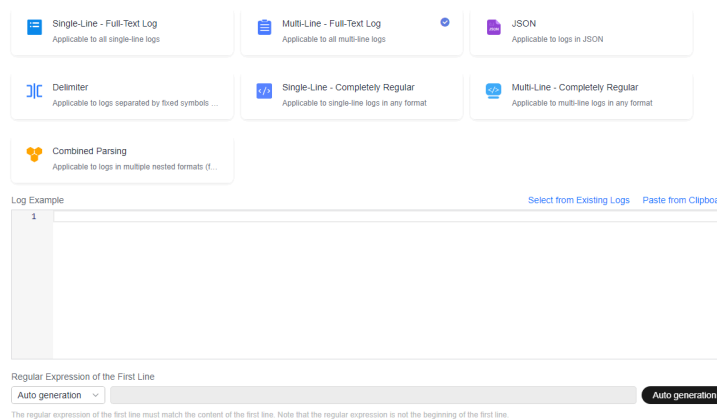


- Add a blacklist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a discarding criterion, discarding logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). In single-line and multi-line full-text modes, **content** is used as the key name *{key}* of the full text by default. The relationship between multiple filtering rules is **OR**. For example, if you do not want to collect log events containing **test** from the log source file, set the filtering rule to **.\*test.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

## Multi-Line - Full-Text Log

Multiple lines of exception log events can be displayed as a single log event. This is helpful when you check logs to locate problems.

1. Select **Multi-Line - Full-Text Log**.
2. Select a log example from existing logs or paste it from the clipboard.
  - Click **Select from Existing Logs**, select a log event, and click **OK**. You can select different time ranges to filter logs.
  - Click **Paste from Clipboard** to paste the copied log content to the **Log Example** box.



3. A regular expression can be automatically generated or manually entered under **Regular Expression of the First Line**. The regular expression of the first line must match the entire first line, not just the beginning of the first line.


**Figure 4-19** Regular expression of the first line



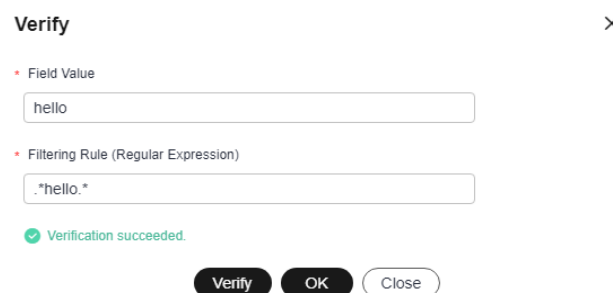
4. Enable **Log Filtering** (disabled by default) as required and add a maximum of 20 whitelist or blacklist rules.


**Figure 4-20** Log filtering rules



- Add a whitelist rule (available only when **Log Filtering** is enabled). You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a matching criterion, collecting and reporting only logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). In single-line and multi-line full-text modes, **content** is used as the key name *{key}* of the full text by default. The relationship between multiple filtering rules is **OR**. For example, to collect log events containing **hello** from the log source file, set the filtering rule to **.\*hello.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

**Figure 4-21** Verification



- Add a blacklist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a discarding criterion, discarding logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). In single-line and multi-line full-text modes, **content** is used as the key name *{key}* of the full text by default. The relationship between multiple filtering rules is **OR**. For example, if you do not want to collect log events containing **test** from the log source file, set the filtering rule to **.\*test.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.


## JSON

This option is applicable to JSON logs and splits them into key-value pairs.

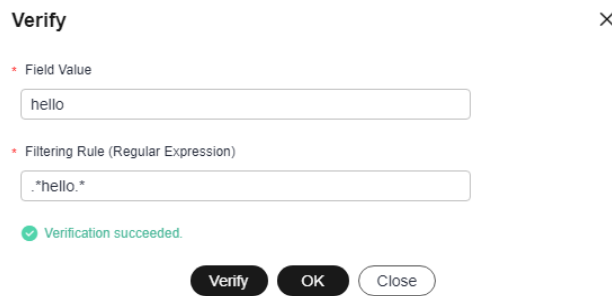
1. Choose **JSON**.
2. Enable **Log Filtering** (disabled by default) as required and add a maximum of 20 whitelist or blacklist rules.


**Figure 4-22** Log filtering rules



- Add a whitelist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a matching criterion, collecting and reporting only logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, to collect log events containing **hello** from the log source file, set the filtering rule to **.\*hello.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

**Figure 4-23** Verification



- Add a blacklist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a discarding criterion, discarding logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, if you do not want to collect log events containing **test** from the log source file, set the filtering rule to **.\*test.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

3. **Raw Log Upload:**

After this function is enabled, raw logs are uploaded to LTS as the value of the **content** field.

4. **Upload Parsing Failure Log:**

After this function is enabled, raw logs are uploaded to LTS as the value of the **\_content\_parse\_fail\_** field.

5. **Custom Time:**

Enabling this lets you specify a field as the log time. Otherwise, the time set during ingestion configuration is used.

6. **JSON Parsing Layers:** Add 1 to 4 JSON parsing layers. The value must be an integer and is **1** by default.

This function expands the fields of a JSON log. For example, for raw log `{"key1":{"key2":"value"}}`, if you choose to parse it into 1 layer, the log will become `{"key1":{"key2":"value"}}`; if you choose to parse it into 2 layers, the log will become `{"key1.key2":"value"}`.

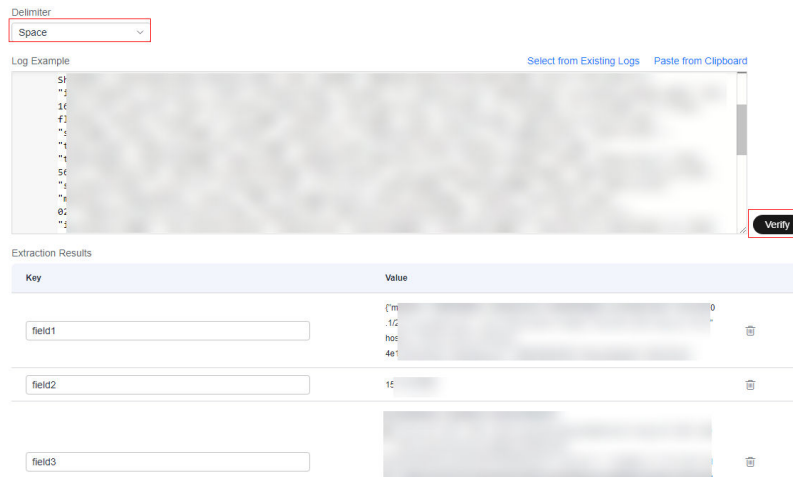
## Delimiter

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

1. Select a delimiter.
2. Select or customize a delimiter.
3. Select a log example from existing logs or paste it from the clipboard, click **Verify**, and view the results under **Extraction Results**.

- Click **Select from Existing Logs**, select a log event, and click **OK**. You can select different time ranges to filter logs.
- Click **Paste from Clipboard** to paste the copied log content to the **Log Example** box.


Figure 4-24 Delimiter



4. Enable **Log Filtering** (disabled by default) as required and add a maximum of 20 whitelist or blacklist rules.

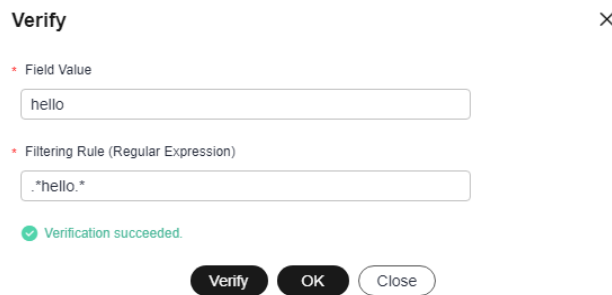
Figure 4-25 Log filtering rules




- Add a whitelist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a matching criterion, collecting and reporting only logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, to collect log events containing **hello** from the log source file, set the filtering rule to **.\*hello.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.



**Figure 4-26** Verification



- Add a blacklist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a discarding criterion, discarding logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, if you do not want to collect log events containing **test** from the log source file, set the filtering rule to **.\*test.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.
- 5. **Raw Log Upload:**  
After this function is enabled, raw logs are uploaded to LTS as the value of the **content** field.
- 6. **Upload Parsing Failure Log:**  
After this function is enabled, raw logs are uploaded to LTS as the value of the **\_content\_parse\_fail\_** field.
- 7. **Custom Time:**  
Enabling this lets you specify a field as the log time. Otherwise, the time set during ingestion configuration is used.

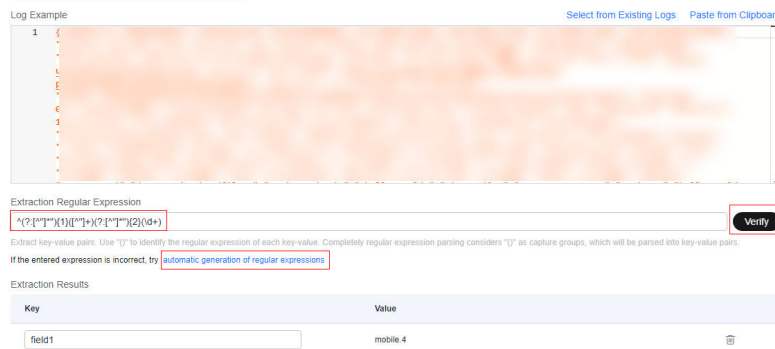
## Single-Line - Completely Regular

This option is applicable to single-line logs in any format and uses a regular expression to extract fields.

1. Select **Single-Line - Completely Regular**.
2. Select a log example from existing logs or paste it from the clipboard.
  - Click **Select from Existing Logs**, select a log event, and click **OK**. You can select different time ranges to filter logs.
  - Click **Paste from Clipboard** to paste the copied log content to the **Log Example** box.
3. Enter a regular expression for extracting the log under **Extraction Regular Expression**, click **Verify**, and view the results under **Extraction Results**.

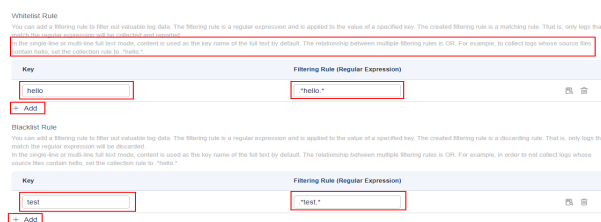
Alternatively, click **automatic generation of regular expressions**. In the displayed dialog box, extract fields based on the log example, enter the key, and click **OK** to automatically generate a regular expression. Then, click **OK**.


**Figure 4-27** Extracting a regular expression



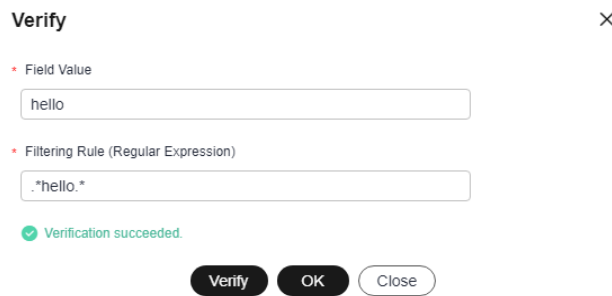
4. Enable **Log Filtering** (disabled by default) as required and add a maximum of 20 whitelist or blacklist rules.


**Figure 4-28** Log filtering rules



- Add a whitelist rule (available only when **Log Filtering** is enabled). You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a matching criterion, collecting and reporting only logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, to collect log events containing **hello** from the log source file, set the filtering rule to **\*hello.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

**Figure 4-29** Verification



- Add a blacklist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a discarding criterion, discarding logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, if you do not want to collect log events containing **test** from the log source file, set the filtering rule to **.\*test.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

5. **Raw Log Upload:**

After this function is enabled, raw logs are uploaded to LTS as the value of the **content** field.

6. **Upload Parsing Failure Log:**

After this function is enabled, raw logs are uploaded to LTS as the value of the **\_content\_parse\_fail\_** field.

7. **Custom Time:**

Enabling this lets you specify a field as the log time. Otherwise, the time set during ingestion configuration is used.

## Multi-Line - Completely Regular

This option is applicable to multi-line logs in any format and uses a regular expression to extract fields.

1. Select **Multi-Line - Completely Regular**.
2. Select a log example from existing logs or paste it from the clipboard.
  - Click **Select from Existing Logs**, select a log event, and click **OK**. You can select different time ranges to filter logs.
  - Click **Paste from Clipboard** to paste the copied log content to the **Log Example** box.
3. A regular expression can be automatically generated or manually entered under **Regular Expression of the First Line**. The regular expression of the first line must match the entire first line, not just the beginning of the first line.

**NOTE**

The regular expression of the first line is used to identify the beginning of a multi-line log. Example:

```
2024-10-11 10:59:07.000 a.log:1 level:warn
no.1 log
2024-10-11 10:59:17.000 a.log:2 level:warn
no.2 log
```

Complete lines:

```
2024-10-11 10:59:07.000 a.log:1 level:warn
no.1 log
```

First line:

```
2024-10-11 10:59:07.000 a.log:1 level:warn
```

Example of the regular expression of the first line: `^\(d+-\d+-\d+\s+\d+:\d+:\d+\.\d+\)`. The date in each first line is unique. Therefore, the regular expression in the first line can be generated based on the date.

4. Enter a regular expression for extracting the log under **Extraction Regular Expression**, click **Verify**, and view the results under **Extraction Results**.

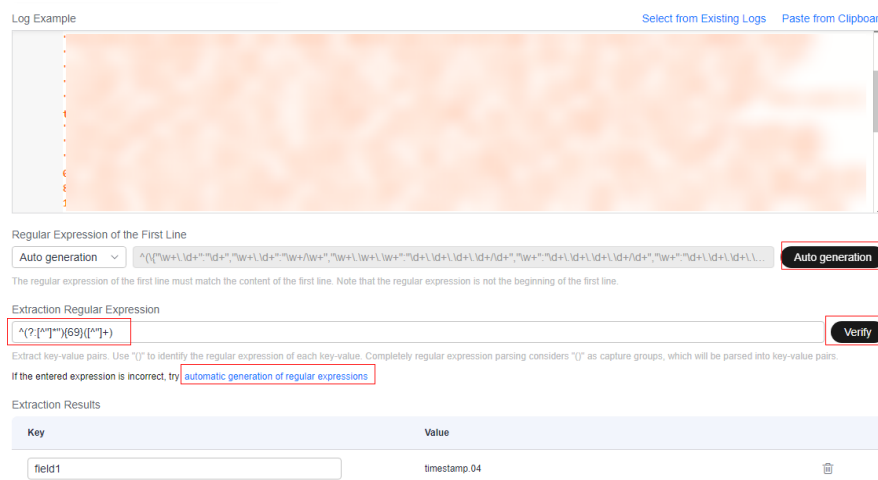
Alternatively, click **automatic generation of regular expressions**. In the displayed dialog box, extract fields based on the log example, enter the key, and click **OK** to automatically generate a regular expression. Then, click **OK**.

**NOTE**

The extraction result is the execution result of the extraction regular expression instead of the first line regular expression. To check the execution result of the first line regular expression, go to the target log stream.

If you enter an incorrect regular expression for **Regular Expression of the First Line**, you cannot view the reported log stream data.


**Figure 4-30** Setting a regular expression



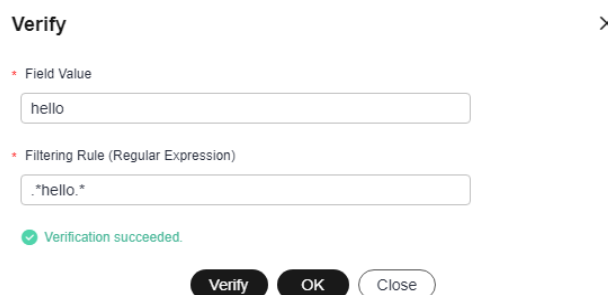
5. Enable **Log Filtering** (disabled by default) as required and add a maximum of 20 whitelist or blacklist rules.


**Figure 4-31** Log filtering rules



- Add a whitelist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a matching criterion, collecting and reporting only logs that match the specified regular expression.
  - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, to collect log events containing **hello** from the log source file, set the filtering rule to **.\*hello.\***.
  - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.

**Figure 4-32** Verification



- Add a blacklist rule (available only when **Log Filtering** is enabled).  
You can add filtering rules to retain valuable log data by applying regular expressions to the values of specified keys. A filtering rule acts as a discarding criterion, discarding logs that match the specified regular expression.
    - i. Click **Add** and enter a key and filtering rule (regular expression). A key is a log field name. The relationship between multiple filtering rules is **OR**. For example, if you do not want to collect log events containing **test** from the log source file, set the filtering rule to **.\*test.\***.
    - ii. Click  in the **Operation** column, enter a field value, and click **Verify** to verify the rule.
6. **Raw Log Upload:**  
After this function is enabled, raw logs are uploaded to LTS as the value of the **content** field.

7. **Upload Parsing Failure Log:**  
After this function is enabled, raw logs are uploaded to LTS as the value of the `_content_parse_fail_` field.
8. **Custom Time:**  
Enabling this lets you specify a field as the log time. Otherwise, the time set during ingestion configuration is used.

## Combined Parsing

This option is applicable to logs in multiple nested formats, for example, JSON logs with delimiters. You can customize parsing rules based on the syntax.

1. Select **Combined Parsing**.
2. Select a log example from existing logs or paste it from the clipboard and enter the configuration content under **Plug-in Settings**.
3. Customize the settings based on the log content by referring to the following plug-in syntaxes.
  - processor\_regex

**Table 4-40** Regular expression extraction

| Parameter            | Type    | Description                                                            |
|----------------------|---------|------------------------------------------------------------------------|
| source_key           | string  | Original field name.                                                   |
| regex                | string  | <b>()</b> in a regular expression indicates the field to be extracted. |
| keys                 | string  | Field name for the extracted content.                                  |
| keep_source          | boolean | Whether to retain the original field.                                  |
| keep_source_if_parse | boolean | Whether to retain the original field when a parsing error occurs.      |

- processor\_split\_string

**Table 4-41** Parsing using delimiters

| Parameter  | Type   | Description                           |
|------------|--------|---------------------------------------|
| source_key | string | Original field name.                  |
| split_sep  | string | Delimiter string.                     |
| keys       | string | Field name for the extracted content. |

| Parameter                  | Type                     | Description                                                                                                                    |
|----------------------------|--------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| keep_source                | boolean                  | Whether to retain the original field in the parsed log.                                                                        |
| split_type                 | char/special_char/string | Delimiter type. The options are <b>char</b> (single character), <b>special_char</b> (invisible character), and <b>string</b> . |
| keep_source_if_parse_error | boolean                  | Whether to retain the original field when a parsing error occurs.                                                              |

- processor\_split\_key\_value

**Table 4-42** Key-value pair segmentation

| Parameter        | Type    | Description                                                                                |
|------------------|---------|--------------------------------------------------------------------------------------------|
| source_key       | string  | Original field name.                                                                       |
| split_sep        | string  | Delimiter between key-value pairs. The default value is the tab character (\t).            |
| expand_connector | string  | Delimiter between the key and value in a key-value pair. The default value is a colon (:). |
| keep_source      | boolean | Whether to retain the original field in the parsed log.                                    |

- processor\_add\_fields

**Table 4-43** Adding a field

| Parameter | Type        | Description                                                                                                            |
|-----------|-------------|------------------------------------------------------------------------------------------------------------------------|
| fields    | json/object | Name and value of the field to be added. The field is in key-value pair format. Multiple key-value pairs can be added. |

- processor\_drop

**Table 4-44** Discarded fields

| Parameter | Type   | Description               |
|-----------|--------|---------------------------|
| drop_keys | string | List of discarded fields. |

- processor\_rename

**Table 4-45** Renaming a field

| Parameter   | Type   | Description    |
|-------------|--------|----------------|
| source_keys | string | Original name. |
| destkeys    | string | New name.      |

- processor\_json

**Table 4-46** JSON expansion and extraction

| Parameter                  | Type    | Description                                                                                                                                             |
|----------------------------|---------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| source_key                 | string  | Original field name.                                                                                                                                    |
| keep_source                | string  | Whether to retain the original field in the parsed log.                                                                                                 |
| expand_depth               | int     | JSON expansion depth. The default value <b>0</b> indicates that the depth is not limited. Other numbers, such as <b>1</b> , indicate the current level. |
| expand_connector           | string  | Connector for expanding JSON. The default value is an underscore ( <code>_</code> ).                                                                    |
| prefix                     | string  | Prefix added to a field name when JSON is expanded.                                                                                                     |
| keep_source_if_parse_error | boolean | Whether to retain the original field when a parsing error occurs.                                                                                       |

- processor\_filter\_regex

**Table 4-47** Filters

| Parameter | Type        | Description                                                                                    |
|-----------|-------------|------------------------------------------------------------------------------------------------|
| include   | json/object | The key indicates the log field, and the value indicates the regular expression to be matched. |
| exclude   | json/object | The key indicates the log field, and the value indicates the regular expression to be matched. |

- processor\_gotime



**Table 4-48** Extraction time

| Parameter       | Type    | Description                                                                                                                  |
|-----------------|---------|------------------------------------------------------------------------------------------------------------------------------|
| source_key      | string  | Original field name.                                                                                                         |
| source_format   | string  | Original time format.                                                                                                        |
| source_location | int     | Original time zone. If the value is empty, it indicates the time zone of the host or container where the logtail is located. |
| dest_key        | string  | Target field after parsing.                                                                                                  |
| dest_format     | string  | Time format after parsing.                                                                                                   |
| dest_location   | int     | Time zone after parsing. If this parameter is left blank, the time zone of the local host is used.                           |
| set_time        | boolean | Whether to set the parsed time as the log time.                                                                              |
| keep_source     | boolean | Whether to retain the original field in the parsed log.                                                                      |

4. Example:

```
[
 {
 "type": "processor_regex",
 "detail": {
 "source_key": "content",
 "regex": "*",
 "keys": [
 "key1",
 "key2"
],
 "multi_line_regex": "*",
 "keep_source": true,
 "keep_source_if_parse_error": true
 }
 },
 {
 "type": "processor_split_string",
 "detail": {
 "split_sep": ".",
 "split_type": ".",
 "split_keys": [
 "key1",
 "key2"
],
 "source_key": "context",
 "keep_source": true,
 "keep_source_if_parse_error": true
 }
 },
 {
 "type": "processor_add_fields",
 "detail": {
 "fields": [
 {
 "key1": "value1"
 }
]
 }
 }
]
```

```

 },
 {
 "key2": "value2"
 }
]
}
},
{
 "type": "processor_drop",
 "detail": {
 "drop_keys": [
 "key1",
 "key2"
]
 }
},
{
 "type": "processor_rename",
 "detail": {
 "source_key": [
 "skey1",
 "skey2"
],
 "dest_keys": [
 "dkey1",
 "dkey2"
]
 }
},
{
 "type": "processor_json",
 "detail": {
 "source_key": "context",
 "expand_depth": 4,
 "expand_connector": "_",
 "prefix": "prefix",
 "keep_source": true,
 "keep_source_if_parse_error": true
 }
},
{
 "type": "processor_gotime",
 "detail": {
 "source_key": "skey",
 "source_format": "ydm",
 "source_location": 8,
 "dest_key": "dkey",
 "dest_format": "ydm",
 "dest_location": 8,
 "set_time": true,
 "keep_source": true,
 "keep_source_if_parse_error": true
 }
},
{
 "type": "processor_filter_regex",
 "detail": {
 "include": {
 "ikey1": "*",
 "ikey2": "*"
 },
 "exclude": {
 "ekey1": "*",
 "ekey1": "*"
 }
 }
}
]

```


## Custom Time

Enable **Custom Time** and set parameters by referring to [Table 4-49](#).

 **NOTE**

- If the time format is incorrect or the specified field does not exist, the log time is the time set during ingestion configuration.
- The time field needs to be verified again when operations such as field name modification, field deletion, and field type modification are performed on structuring parsing.

**Table 4-49** Parameter configuration

| Parameter                  | Description                                                                                                                                                                                                                                             | Example             |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| Key Name of the Time Field | Name of an extracted field. You can select an extracted field from the drop-down list. The field is of the <b>string</b> or <b>long</b> type.                                                                                                           | test                |
| Field Value                | Value of an extracted field. After a <b>Key</b> is selected, the <b>Value</b> is automatically filled in.<br><b>NOTE</b><br>The value of the field must be within 24 hours earlier or later than the current time.                                      | 2023-07-19 12:12:00 |
| Time Format                | For details, see <a href="#">Common Log Time Formats</a> .                                                                                                                                                                                              | yyyy-MM-dd HH:mm:ss |
| Operation                  | Click the verification icon (  ). If message <b>The time format is successfully matched with the time field value.</b> is displayed, the verification is successful. | -                   |

## Common Log Time Formats

[Table 4-50](#) lists common log time formats.

 **NOTE**

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

**Table 4-50** Time formats

| Format | Description            | Example |
|--------|------------------------|---------|
| EEE    | Abbreviation for Week. | Fri     |

| Format                      | Description                                                                                  | Example                     |
|-----------------------------|----------------------------------------------------------------------------------------------|-----------------------------|
| EEEE                        | Full name for Week.                                                                          | Friday                      |
| MMM                         | Abbreviation for Month.                                                                      | Jan                         |
| MMMM                        | Full name for Month.                                                                         | January                     |
| dd                          | Number of the day in a month, ranging from 01 to 31 (decimal).                               | 07, 31                      |
| HH                          | Hour, in 24-hour format.                                                                     | 22                          |
| hh                          | Hour, in 12-hour format.                                                                     | 11                          |
| MM                          | Number of the month, ranging from 01 to 12 (decimal).                                        | 08                          |
| mm                          | Number of the minute, ranging from 00 to 59 (decimal).                                       | 59                          |
| a                           | AM or PM                                                                                     | AM, PM                      |
| hh:mm:ss a                  | Time in the 12-hour format.                                                                  | 11:59:59 AM                 |
| HH:mm                       | Hour and minute format.                                                                      | 23:59                       |
| ss                          | Number of the second, ranging from 00 to 59 (decimal).                                       | 59                          |
| yy                          | Year without century, ranging from 00 to 99 (decimal).                                       | 04, 98                      |
| yyyy                        | Year (decimal).                                                                              | 2004, 1998                  |
| d                           | Number of the day in a month, ranging from 1 to 31 (decimal).                                | 7, 31                       |
| DDD                         | Number of the day in a year, ranging from 001 to 366 (decimal).                              | 365                         |
| u                           | Number of the day in a week, ranging from 1 to 7 (decimal). The value 1 indicates Monday.    | 2                           |
| w                           | Number of the week in a year. Sunday is the start of a week. The value ranges from 00 to 53. | 23                          |
| W                           | Number of the week in a month, ranging from 0 to 5.                                          | 2                           |
| U                           | Number of the day in a week, ranging from 0 to 6 (decimal). The value 0 indicates Sunday.    | 5                           |
| EEE MMM dd<br>HH:mm:ss yyyy | Standard date and time.                                                                      | Tue Nov 20 14:12:58<br>2020 |

| Format             | Description                 | Example         |
|--------------------|-----------------------------|-----------------|
| EEE MMM dd<br>YYYY | Standard date without time. | Tue Nov 20 2020 |
| HH:mm:ss           | Standard time without date. | 11:59:59        |
| %s                 | UNIX Timestamp.             | 147618725       |

## 4.3 Ingesting Cloud Service Logs to LTS

### 4.3.1 Overview

LTS collects log data of many Huawei Cloud services, such as compute, storage, security, and database services. You can use LTS to search for cloud service logs by keyword, analyze operation data, and monitor the running status and alarms. The following table lists the cloud service logs that can be collected by LTS.

**Table 4-51** Cloud service logs collected by LTS

| Service Abbreviation | Cloud Service                     | Log Type                   | Document                                       | Dashboard                                                                                                                                         |
|----------------------|-----------------------------------|----------------------------|------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| AOM                  | Application Operations Management | All logs                   | <a href="#">Ingesting AOM Logs to LTS</a>      | -                                                                                                                                                 |
| APIG                 | API Gateway                       | Gateway access logs (APIG) | <a href="#">Ingesting APIG Logs to LTS</a>     | <ul style="list-style-type: none"> <li>• APIG Monitoring Center</li> <li>• APIG Access Center</li> <li>• APIG Monitoring by the Second</li> </ul> |
| BMS                  | Bare Metal Server                 | All logs                   | <a href="#">Ingesting BMS Text Logs to LTS</a> | -                                                                                                                                                 |
| CBH                  | Cloud Bastion Host                | Operation logs             | <a href="#">Ingesting CBH Logs to LTS</a>      | -                                                                                                                                                 |

| Service Abbreviation | Cloud Service                         | Log Type                                                                                                                   | Document                                              | Dashboard            |
|----------------------|---------------------------------------|----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|----------------------|
| CCE                  | Cloud Container Engine                | <ul style="list-style-type: none"> <li>User application logs</li> <li>CCE management plane logs</li> </ul>                 | <a href="#">Ingesting CCE Application Logs to LTS</a> | -                    |
| CFW                  | Cloud Firewall                        | <ul style="list-style-type: none"> <li>Attack logs (CFW)</li> <li>Access logs (CFW)</li> <li>Traffic logs (CFW)</li> </ul> | <a href="#">Ingesting CFW Logs to LTS</a>             | -                    |
| CTS                  | Cloud Trace Service                   | Cloud service management plane operation logs                                                                              | <a href="#">Ingesting CTS Logs to LTS</a>             | -                    |
| DDS                  | Document Database Service             | <ul style="list-style-type: none"> <li>DDS audit logs</li> <li>DDS error logs</li> <li>DDS slow query logs</li> </ul>      | <a href="#">Ingesting DDS Logs to LTS</a>             | DDS Audit Log Center |
| DMS                  | Distributed Message Service for Kafka | DMS rebalancing logs                                                                                                       | <a href="#">Ingesting DMS for Kafka Logs to LTS</a>   | -                    |
| DRS                  | Data Replication Service              | Access logs                                                                                                                | <a href="#">Ingesting DRS Logs to LTS</a>             | -                    |
| DWS                  | Data Warehouse Service                | <ul style="list-style-type: none"> <li>CN logs</li> <li>DN logs</li> <li>OS messages logs</li> <li>Audit logs</li> </ul>   | <a href="#">Ingesting GaussDB(DWS) Logs to LTS</a>    | -                    |
| ECS                  | Elastic Cloud Server                  | All logs (text logs collected by ICAgent)                                                                                  | <a href="#">Ingesting ECS Text Logs to LTS</a>        | -                    |

| Service Abbreviation | Cloud Service        | Log Type                                                                                                            | Document                                                 | Dashboard                                                                                                                                |
|----------------------|----------------------|---------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| ELB                  | Elastic Load Balance | Layer-7 access logs (ELB)                                                                                           | <a href="#">Ingesting ELB Logs to LTS</a>                | <ul style="list-style-type: none"> <li>ELB Monitoring Center</li> <li>ELB Access Center</li> <li>ELB Monitoring by the Second</li> </ul> |
| ER                   | Enterprise Router    | All ER logs                                                                                                         | <a href="#">Ingesting Enterprise Router Logs to LTS</a>  | -                                                                                                                                        |
| Function Graph       | FunctionGraph        | Function execution logs                                                                                             | <a href="#">Ingesting FunctionGraph Logs to LTS</a>      | -                                                                                                                                        |
| GaussDB              | GaussDB              | GAUSSV5 audit logs                                                                                                  | <a href="#">Ingesting GaussDB Logs to LTS</a>            | -                                                                                                                                        |
| GES                  | Graph Engine Service | Audit logs                                                                                                          | <a href="#">Ingesting GES Logs to LTS</a>                | -                                                                                                                                        |
| GaussDB for MySQL    | GaussDB(for MySQL)   | <ul style="list-style-type: none"> <li>GAUSSDB_MYSQL error logs</li> <li>GAUSSDB_MYSQL slow query logs</li> </ul>   | <a href="#">Ingesting TaurusDB Logs to LTS</a>           | -                                                                                                                                        |
| GeminiDB Redis       | GeminiDB Redis       | GeminiDB Redis slow query logs                                                                                      | <a href="#">Ingesting GeminiDB Logs to LTS</a>           | -                                                                                                                                        |
| GeminiDB Mongo       | GeminiDB Mongo       | <ul style="list-style-type: none"> <li>GeminiDB Mongo error logs</li> <li>GeminiDB Mongo slow query logs</li> </ul> | <a href="#">Ingesting GeminiDB Mongo Logs to LTS</a>     | -                                                                                                                                        |
| GeminiDB Cassandra   | GeminiDB Cassandra   | GeminiDB Cassandra slow query logs                                                                                  | <a href="#">Ingesting GeminiDB Cassandra Logs to LTS</a> | -                                                                                                                                        |

| Service Abbreviation | Cloud Service               | Log Type                                                                                                    | Document                                                                     | Dashboard |
|----------------------|-----------------------------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------|-----------|
| IoTDA                | IoT Device Access           | Device operation logs                                                                                       | <a href="#">Ingesting IoTDA Logs to LTS</a>                                  | -         |
| ModelArts            | ModelArts                   | Operation logs                                                                                              | <a href="#">Ingesting ModelArts Logs to LTS</a>                              | -         |
| MRS                  | MapReduce Service           | All logs (text logs collected by ICAgent)                                                                   | <a href="#">Ingesting MRS Logs to LTS</a>                                    | -         |
| RDS for MySQL        | RDS for MySQL               | <ul style="list-style-type: none"> <li>MySQL error logs</li> <li>MySQL slow query logs</li> </ul>           | <a href="#">Ingesting RDS for MySQL Logs to LTS</a>                          | -         |
| RDS for PostgreSQL   | RDS for PostgreSQL          | <ul style="list-style-type: none"> <li>PostgreSQL error logs</li> <li>POSTGRESQL slow query logs</li> </ul> | <a href="#">Ingesting RDS for PostgreSQL Logs to LTS</a>                     | -         |
| RDS for SQL Server   | RDS for SQL Server          | SQLServer error logs                                                                                        | <a href="#">Ingesting RDS for SQL Server Logs to LTS</a>                     | -         |
| ROMA Connect         | ROMA Connect                | Gateway access logs                                                                                         | <a href="#">Ingesting ROMA Connect Logs to LTS</a>                           | -         |
| SMN                  | Simple Message Notification | SMN messaging logs                                                                                          | <a href="#">Ingesting SMN Logs to LTS</a>                                    | -         |
| SecMaster            | SecMaster                   | All logs                                                                                                    | <a href="#">Ingesting SecMaster Logs to LTS</a>                              | -         |
| ServiceStage         | ServiceStage                | ServiceStage containerized application logs                                                                 | <a href="#">Ingesting ServiceStage Containerized Application Logs to LTS</a> | -         |
| ServiceStage         | ServiceStage                | ServiceStage cloud host logs                                                                                | <a href="#">Ingesting ServiceStage Cloud Host Logs to LTS</a>                | -         |



| Service Abbreviation | Cloud Service            | Log Type                                                                            | Document                                  | Dashboard     |
|----------------------|--------------------------|-------------------------------------------------------------------------------------|-------------------------------------------|---------------|
| VPC                  | Virtual Private Cloud    | VPC flow logs                                                                       | <a href="#">Ingesting VPC Logs to LTS</a> | VPC Flow Logs |
| WAF                  | Web Application Firewall | <ul style="list-style-type: none"><li>• Attack logs</li><li>• Access logs</li></ul> | <a href="#">Ingesting WAF Logs to LTS</a> | -             |

### 4.3.2 Ingesting AOM Logs to LTS

LTS can collect logs from AOM.

For details, see [Accessing LTS](#).

### 4.3.3 Ingesting APIG Logs to LTS

LTS can collect logs from APIG.

#### Prerequisites

You have created and used an API gateway of Huawei Cloud.

#### Configuring APIG Log Ingestion in LTS

Perform the following operations to configure APIG log ingestion:

**Step 1** Log in to the [LTS console](#).

**Step 2** Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **APIG (API Gateway)**.

**Step 3** Select a log stream.

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

**Step 4** Click **Configure APIG** to configure APIG on the APIG console. For details, see [Viewing API Call Logs](#).

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

**Table 4-52** Log stream parameters

| Parameter                            | Description                                                                                                                                                                                                                                                               |
|--------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Structure and Index             | If this function is enabled, the structuring for the log stream is based on the APIG system template, and the indexing enables quick analysis for all parsed APIG fields. Enabling structuring and indexing is required for SQL analysis of APIG logs with visual charts. |
| Auto Add Tag<br>log_type=apig_access | If this option is enabled, the tag <b>log_type=apig_access</b> is automatically added to the log stream, and the APIG dashboard template can then match this log stream.                                                                                                  |
| Auto Create Chart                    | If this option is enabled, an APIG dashboard is automatically created for the log stream.                                                                                                                                                                                 |

**Step 6** Click **Submit**.

----End

### 4.3.4 Ingesting CBH Logs to LTS

LTS can collect logs from CBH.

For details, see [Configuring LTS](#).

### 4.3.5 Ingesting CFW Logs to LTS

LTS can collect logs from CFW. It also enables real-time, efficient, and secure analysis and processing of a vast volume of collected logs.

For details, see [Configuring Logs](#).

### 4.3.6 Ingesting CTS Logs to LTS

LTS can collect logs from CTS.

#### Prerequisites

You have purchased and used a Huawei Cloud CTS instance.

#### Configuring CTS Log Ingestion in LTS

Perform the following operations to configure CTS log ingestion:

##### NOTE

CTS logs ingested to LTS are retained on the LTS console for 30 days by default. You can specify a log retention period ranging from 1 to 365 days when creating a log group. For details, see [Managing Log Groups](#).

**Step 1** Log in to the [LTS console](#).

**Step 2** Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **CTS (Cloud Trace Service)**.

**Step 3** Select a log stream.

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

**Step 4** Click **Configure CTS**. For details about the procedure and parameter settings, see the [Cloud Trace Service User Guide](#).

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

**Table 4-53** Log stream parameters

| Parameter                | Description                                                                                                                                                                                                                                                            |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Structure and Index | If this function is enabled, the structuring for the log stream is based on the CTS system template, and the indexing enables quick analysis for all parsed CTS fields. Enabling structuring and indexing is required for SQL analysis of CTS logs with visual charts. |

**Step 6** Click **Submit**.

----End

## 4.3.7 Ingesting DDS Logs to LTS

LTS can collect logs from DDS.

For details, see [Log Reporting](#).

## 4.3.8 Ingesting DMS for Kafka Logs to LTS

LTS can collect logs from DMS for Kafka. Rebalancing logs record rebalancing details, including the time, reason, and triggering client of rebalancing. They are stored and can be queried in LTS.

For details, see [Viewing Kafka Rebalancing Logs](#).

## 4.3.9 Ingesting DRS Logs to LTS

LTS can collect logs from DRS. After log ingestion is configured, all newly generated logs of DRS instances (including real-time migration, backup migration, real-time synchronization, real-time disaster recovery, and recording and playback instances) are uploaded to LTS for management.

For details, see [Log Reporting](#).

### 4.3.10 Ingesting GaussDB(DWS) Logs to LTS

LTS can collect logs from GaussDB(DWS).

For details, see [Cluster Log Management](#).

### 4.3.11 Ingesting ELB Logs to LTS

LTS can collect logs from ELB.

#### Prerequisites

You have created and used a Huawei Cloud load balancer.

#### Constraints

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

#### Configuring ELB Log Ingestion

Perform the following operations to configure ELB log ingestion:

**Step 1** Log in to the [LTS console](#).

**Step 2** Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **ELB (Elastic Load Balance)**.

**Step 3** Select a log stream.

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

**Step 4** Click **Configure ELB**. For details, see [Access Logging](#).

**Step 5** Configure a log stream.

**Table 4-54** Log stream parameters

| Parameter                                  | Description                                                                                                                                                                                                                                                            |
|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Structure and Index                   | If this function is enabled, the structuring for the log stream is based on the ELB system template, and the indexing enables quick analysis for all parsed ELB fields. Enabling structuring and indexing is required for SQL analysis of ELB logs with visual charts. |
| Auto Add Tag<br>log_type=elb_7layer_access | If this option is enabled, the tag <b>log_type=elb_7layer_access</b> is automatically added to the log stream, and the ELB dashboard template can then match this log stream.                                                                                          |

| Parameter         | Description                                                                              |
|-------------------|------------------------------------------------------------------------------------------|
| Auto Create Chart | If this option is enabled, an ELB dashboard is automatically created for the log stream. |

**Step 6** Click **Submit**.

----End

### 4.3.12 Ingesting Enterprise Router Logs to LTS

LTS can collect logs from Enterprise Router.

For details, see [Creating a Flow Log](#).

### 4.3.13 Ingesting FunctionGraph Logs to LTS

LTS can collect logs from FunctionGraph.

For details, see [Managing Function Logs](#).

### 4.3.14 Ingesting GaussDB Logs to LTS

LTS can collect logs from GaussDB.

For details, see [Interconnecting with LTS and Querying Database Audit Logs](#).

### 4.3.15 Ingesting GES Logs to LTS

LTS can collect logs from GES.

For details, see [Creating a Graph Without Using a Template](#).

### 4.3.16 Ingesting TaurusDB Logs to LTS

LTS can collect logs from TaurusDB.

For details, see [Configuring Log Reporting](#).

### 4.3.17 Ingesting GeminiDB Logs to LTS

LTS can collect logs from GeminiDB. If you enable log reporting for your GeminiDB Redis instance, new logs generated for the instance will be uploaded to LTS for management.

For details, see [Enabling or Disabling Log Reporting](#).

### 4.3.18 Ingesting GeminiDB Mongo Logs to LTS

LTS can collect logs from GeminiDB Mongo.

For details, see [Enabling or Disabling Log Reporting](#).

### 4.3.19 Ingesting GeminiDB Cassandra Logs to LTS

LTS can collect logs from GeminiDB Cassandra.

To use this function, [submit a service ticket](#) to GeminiDB.

### 4.3.20 Ingesting IoTDA Logs to LTS

LTS can collect logs from IoTDA.

For details, see [Viewing Run Logs](#).

### 4.3.21 Ingesting ModelArts Logs to LTS

LTS can collect logs from the AI development platform ModelArts.

For details, see [Deploying as a Real-Time Service](#).

### 4.3.22 Ingesting MRS Logs to LTS

LTS can collect logs from MRS.

For details, see [How Do I Interconnect MRS with LTS?](#)

### 4.3.23 Ingesting RDS for MySQL Logs to LTS

LTS can collect logs from RDS for MySQL.

For details, see [Log Reporting](#).

### 4.3.24 Ingesting RDS for PostgreSQL Logs to LTS

LTS can collect logs from RDS for PostgreSQL.

For details, see [Log Reporting](#).

### 4.3.25 Ingesting RDS for SQL Server Logs to LTS

LTS can collect logs from RDS for SQL Server.

For details, see [Log Management](#).

### 4.3.26 Ingesting ROMA Connect Logs to LTS

LTS can collect logs from ROMA Connect.

For details, see [Viewing API Call Logs](#).

### 4.3.27 Ingesting SMN Logs to LTS

LTS can collect logs from SMN.

For details, see [Logs](#).

### 4.3.28 Ingesting SecMaster Logs to LTS

LTS can collect logs from SecMaster.

For details, see [Creating a Data Delivery](#).

## 4.3.29 Ingesting OBS Files to LTS (Beta)

Files in OBS buckets can be imported to LTS at a time or periodically. Then, you can search for, analyze, and process these files. Files in encrypted buckets cannot be imported to LTS. To import such files, delete the buckets' encryption configurations first. For details, see [Deleting the Encryption Configuration of a Bucket](#).


This function is available only for whitelisted users in regions CN North-Beijing4 and CN South-Guangzhou. To use it, [submit a service ticket](#).

### Importing Files in a Single OBS Bucket to LTS

**Step 1** Log in to the [LTS console](#).

**Step 2** Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **OBS (Object Storage Service)**.

Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > OBS (Object Storage Service)**.

Alternatively, choose **Log Management** in the navigation pane and click the target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and click **Ingest Log**. In the displayed dialog box, click **OBS (Object Storage Service)**.

**Step 3** Select a log group from the **Log Group** drop-down list. If there is no desired log group, click **Create Log Group**. For details, see [Managing Log Groups](#).

**Step 4** Select a log stream from the **Log Stream** drop-down list. If there is no desired log stream, click **Create Log Stream**. For details, see [Managing Log Streams](#).

**Step 5** Click **Next: Configurations**.

**Step 6** On the **Configurations** page, set parameters by referring to [Table 4-55](#).



**Table 4-55** Configuring the collection

| Type           | Parameter                     | Description                                                                                                                                                                                                                                                                       |
|----------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Basic Settings | Collection Configuration Name | Enter a name containing 1 to 64 characters. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed. It cannot start with a period or underscore, or end with a period.                                                                                   |
|                | Task Monitoring               | This function is enabled by default.<br>It logs task execution statuses to log stream <b>lts-system/lts-obs2lts-statistics</b> , allowing you to view OBS file import data on LTS's <b>Task Monitoring Center</b> and configure alarm rules to promptly detect any import issues. |

| Type                          | Parameter                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------|---------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| OBS Data Source Configuration | OBS Bucket                            | Select the OBS bucket from which log files are imported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                               | Folder Prefix                         | Enter the prefix ( <b>your_prefix/</b> ) or the full path ( <b>your_prefix/file.gz</b> ) of the OBS files to be imported. Only original files whose size less than 5 GB can be imported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|                               | Regular Expression for File Filtering | <p>Enter a regular expression for filtering files, so that only files with names matching the regular expression will be imported. If no regular expression is specified, files are not filtered.</p> <p><b>NOTE</b></p> <p>Assume that there are files <b>aab</b> and <b>aba</b> in the directory:</p> <ul style="list-style-type: none"> <li>• To match only file <b>aab</b>, use regular expression <b>aab</b>, <b>aa</b>, <b>^aab</b>, or <b>aa</b>.</li> <li>• To match only file <b>aba</b>, use regular expression <b>aba</b>, <b>^aba</b>, or <b>^ab</b>. Do not use <b>ab</b>, which will also match <b>aab</b>.</li> <li>• To match both <b>aab</b> and <b>aba</b>, use regular expression <b>ab</b> or <b>a.*</b>.</li> <li>• If there are regular keywords, they must be escaped. For example, <b>{}</b> must be escaped to <b>\{\}</b>.</li> </ul> |
|                               | Compressed Format                     | Auto check, non-compression, and gzip/zip/snappy compression are supported. If you select <b>ZIP</b> , only zip packages containing a single file without any folders are supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



| Type                      | Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------------------------|-----------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                           | Import Interval | <ul style="list-style-type: none"> <li>● <b>One-off:</b> LTS imports files only once and does not detect new files.</li> <li>● <b>Custom interval:</b> LTS automatically detects new files and imports them at a fixed interval. If you enable <b>Restore Archived Files</b>, OBS files in the Archive storage class can be restored. This option must be enabled for Archive files. Restoring Archive files takes some time (an expedited restore of Archive files takes 1 to 5 minutes). For details, see <a href="#">Object Restore Option and Time Required</a>. Clicking <b>Preview</b> in the lower right corner for the first time may time out. Try clicking <b>Preview</b> again.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- If a periodic task starts its first scan of files on OBS, the range of the last modification time of the files is (First run time of the period - Fixed interval time, First run time of the period]. For example, if the periodic task starts for the first time at 12:00:00 and the fixed time interval configured for the OBS import task is 10 minutes, then the last modification time of the OBS files scanned for the first time will be within the interval (11:50:00, 12:00:00]. The second period runs at 12:10:00, so the last modification time of the files scanned will be within the interval (12:00:00, 12:10:00].</li> <li>- If a one-off task fails to process a file, it will not parse or report any other scanned files to LTS.</li> <li>- If a custom-interval task is disabled and then enabled again, the monitoring data continuity can be retained for up to one day.</li> <li>- If a custom-interval task fails to process files in an interval, it will not parse or report any other files scanned during that interval to LTS.</li> </ul> |
| Data Format Configuration | Log File Code   | <p>The log file encoding format can be UTF-8 or GBK. UTF-8 encoding is a variable-length encoding mode and represents Unicode character sets. GBK, an acronym for Chinese Internal Code Extension Specification, is a Chinese character encoding standard that extends both the ASCII and GB2312 encoding systems.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |

| Type | Parameter       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      | Extraction Mode | <p>Select an extraction mode based on the log type. A maximum of 1 MB of an OBS log will be extracted. Any excess will be truncated and discarded.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• If a single-line log exceeds 1 MB, the excess of that line will be truncated and discarded.</li> <li>• If a block in a multi-line log exceeds 1 MB, the excess of that block will be truncated and discarded.</li> <li>• Logs in ORC and JSON formats are parsed as single-line logs. If a single line exceeds 1 MB, the log will be discarded.</li> </ul> <ul style="list-style-type: none"> <li>• <b>Single-line - full-text:</b> collects the full text of single-line logs without structuring parsing. To perform structuring parsing on logs, complete OBS file import and then configure structuring parsing by referring to <a href="#">Setting Cloud Structuring Parsing</a>.</li> <li>• <b>Multi-line - full-text:</b> collects the full text of multi-line logs (such as stack logs) without structuring parsing. To perform structuring parsing on logs, complete OBS file import and then configure structuring parsing by referring to <a href="#">Setting Cloud Structuring Parsing</a>.</li> <li>• <b>ORC:</b> collects logs in ORC format. If <b>Custom Time</b> is disabled, the time when logs are collected is used as the log time. If <b>Custom Time</b> is enabled, you can specify a field to set the log time. Set the time field key name, value, and time format, and click  to verify your settings. <b>If the imported data is written to the Cluster Switch System (CSS), LTS does not support you to set a time two days ago for ORC logs. For details about the custom time format, see <a href="#">Patterns for Formatting and Parsing</a> on the Oracle official website.</b></li> <li>• <b>JSON:</b> collects logs in JSON format. If <b>Custom Time</b> is disabled, the time when logs are collected is used as the log time. If <b>Custom Time</b> is enabled, you can specify a field to set the log time. Set the time field key name, value, and time format, and click  to verify your settings. <b>If the imported data is written to the CSS, LTS does not support you to set a time two days ago for JSON logs. For details about the custom time format, see <a href="#">Patterns for Formatting and Parsing</a> on the Oracle official website.</b></li> </ul> |

| Type | Parameter | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|------|-----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|      |           | Set 1 to 4 JSON parsing layers. The value must be an integer and is 1 by default. This function expands the fields of a JSON log. For example, for raw log <code>{"key1":{"key2":"value"}}</code> , if you choose to parse it into 1 layer, the log will become <code>{"key1":{"key2":"value"}}</code> ; if you choose to parse it into 2 layers, the log will become <code>{"key1.key2":"value"}</code> . |

**Step 7** After the setting is complete, click **Preview** in the lower right corner. The preview function scans and returns only the first 10 lines of the first file that meets the conditions.

**Step 8** Check the result preview in the lower part. If the result is correct, click **Submit**.

**Step 9** The created ingestion configuration will be displayed. During closed beta testing, up to 10 OBS ingestion configurations can be created.

- Click its name to view its details.
- Click **Modify** in the **Operation** column to modify the ingestion configuration. Ingestion configurations whose import interval is **One-off** cannot be modified.
- Click **Configure Tag** in the **Operation** column to add a tag.
- Click **Copy** in the **Operation** column to copy the ingestion configuration.
- Click **Delete** in the **Operation** column to delete the ingestion configuration.

 **NOTE**

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

- Click the log stream in the **Log Stream** column to go to its details page. Then you can search for and analyze logs ingested to LTS. For details, see [Log Search and Analysis](#).

----End

### 4.3.30 Ingesting VPC Logs to LTS

LTS can collect logs from VPC.

#### Prerequisites

You have purchased and used a Huawei Cloud VPC.

#### Constraints

For details about the supported ECSs, see [VPC Flow Log Overview](#).

#### Configuring VPC Log Ingestion

Perform the following operations to configure VPC log ingestion:

- Step 1** Log in to the [LTS console](#).
- Step 2** Choose **Log Ingestion > Ingestion Center** in the navigation pane and click **VPC (Virtual Private Cloud)**.
- Step 3** Select a log stream.
1. Select a log group from the **Log Group** drop-down list. If there are no desired log groups, click **Create Log Group** to create one.
  2. Select a log stream from the **Log Stream** drop-down list. If there are no desired log streams, click **Create Log Stream** to create one.
  3. Click **Next: Configure VPC**.
- Step 4** Click **Configure VPC**. For details, see [Creating a VPC Flow Log](#).
- Step 5** Click **Next: Configure Log Stream**.

**Table 4-56** Log stream parameters

| Parameter                         | Description                                                                                                                                                                                                                                                            |
|-----------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Auto Structure and Index          | If this function is enabled, the structuring for the log stream is based on the VPC system template, and the indexing enables quick analysis for all parsed VPC fields. Enabling structuring and indexing is required for SQL analysis of VPC logs with visual charts. |
| Auto Add Tag<br>log_type=vpc_flow | If this option is enabled, the tag <b>log_type=vpc_flow</b> is automatically added to the log stream, and the VPC dashboard template can then match this log stream.                                                                                                   |
| Auto Create Chart                 | If this option is enabled, a VPC dashboard is automatically created for the log stream.                                                                                                                                                                                |

- Step 6** Click **Submit**.

----End

### 4.3.31 Ingesting WAF Logs to LTS

LTS can collect logs from WAF.

For details, see [Using LTS to Log WAF Activities](#).

## 4.4 Using APIs to Ingest Logs to LTS

### 4.4.1 Collecting Logs Using APIs

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

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

**Table 4-57** Scenarios

| Name                                        | Log Time                                                                                                                                                                                   | Example                                                                                                                                                                                                                                                                                                                                                                                                | Scenario                                                                                                          |
|---------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| <p><b>Reporting Logs</b></p>                | <p>When invoking the API to upload a batch of logs, you can specify an initial time with log_time_ns field.</p> <p>Time of each log can be calculated with log_time_ns+sequence count.</p> | <pre data-bbox="895 342 1184 622"> {   "log_time_ns":   "1586850540000000000",   "contents": [     "log1",     "log2"   ],   "labels": {     "user_tag": "string"   } } </pre> <p>When reported to LTS:</p> <p>The time of log1 is <b>158685054000000000</b>.</p> <p>The time of log2 is <b>158685054000000001</b>.</p>                                                                                | <p>The logs are generated in sequence at similar time.</p>                                                        |
| <p><b>Reporting High-Precision Logs</b></p> | <p>When you invoke the API to upload a batch of logs, the log_time_ns field must be used to specify the log time for each log.</p>                                                         | <pre data-bbox="895 936 1184 1417"> {   "contents":[     {       "log_time_ns":"15868505400000000",       "log":"log3"     },     {       "log_time_ns":"15868505400000008",       "log":"log4"     }   ],   "labels":{"     "user_tag":"string"   } } </pre> <p>When reported to LTS:</p> <p>The time of log3 is <b>158685054000000000</b>.</p> <p>The time of log4 is <b>158685054000000008</b>.</p> | <p>The uploaded logs are generated out of order at different times. Each log needs to have its own timestamp.</p> |

**Table 4-58** Access IP address

| Region            | Access IP address |
|-------------------|-------------------|
| CN North-Beijing1 | 100.125.57.101    |

| Region                            | Access IP address |
|-----------------------------------|-------------------|
| CN North-Beijing2                 | 100.125.6.108     |
| CN North-Beijing4                 | 100.125.12.150    |
| CN East-Shanghai1                 | 100.125.11.177    |
| CN East-Shanghai2                 | 100.125.140.102   |
| CN South-Guangzhou                | 100.125.158.115   |
| CN Southwest-Guiyang1             | 100.125.0.27      |
| CN South-Guangzhou-InvitationOnly | 100.125.4.30      |
| AP-Singapore                      | 100.125.4.58      |

**NOTE**

You can obtain the access IP address from the command displayed on the ICAgent installation page of the LTS console. For details, see [Installing ICAgent \(Intra-Region Hosts\)](#).

## 4.4.2 API for Reporting Logs

### Function

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

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

**NOTE**

For details about the constraints on log reporting, see [Log Read/Write Constraints](#).

### URI

POST /v2/{project\_id}/lts/groups/{log\_group\_id}/streams/{log\_stream\_id}/tenant/contents

**Table 4-59** URI parameters

| Parameter     | Mandatory | Type   | Description                                                                                                                                                                                                                                                                               |
|---------------|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| project_id    | Yes       | String | Project ID. For details about how to obtain it, see <a href="#">Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</a> .<br>No default value.<br>Value length: 32 characters                                                                                           |
| log_group_id  | Yes       | String | Log group ID. For details about how to obtain it, see <a href="#">Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</a> .<br>No default value.<br>Value length: 36 characters                                                                                         |
| log_stream_id | Yes       | String | Log stream ID. For details about how to obtain it, see <a href="#">Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</a> .<br>No default value.<br>Value length: 36 characters<br><b>NOTE</b><br>A write rate exceeding 100 MB/s per log stream may cause log losses. |

## Request Parameters

**Table 4-60** Request header parameters

| Parameter    | Mandatory | Type   | Description                                                                                                                                                                                                                         |
|--------------|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | Yes       | String | Indicates the user token obtained from IAM. For details about how to obtain a user token, see <a href="#">Obtaining a User Token</a> .<br>No default value.<br>Minimum length: 1,000 characters<br>Maximum length: 2,000 characters |

| Parameter    | Mandatory | Type   | Description                                                                                                                                          |
|--------------|-----------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content-Type | Yes       | String | Set this parameter to <b>application/json;charset=UTF-8</b> .<br>No default value.<br>Minimum length: 30 characters<br>Maximum length: 30 characters |

**Table 4-61** Request body parameters

| Parameter         | Mandatory | Type            | Description                                                                                                                                                                                                                                      |
|-------------------|-----------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| log_time_ns       | Yes       | Long            | Time when log data is reported (UTC time in nanoseconds).<br><b>NOTE</b><br>Logs reported to LTS through APIs are retained for two days (from the log reporting time to the current time). Logs reported more than two days ago will be deleted. |
| contents          | Yes       | Array of String | Indicates the log content.                                                                                                                                                                                                                       |
| labels            | Yes       | Object          | Custom labels.<br><b>NOTE</b><br>Do not set field names to <b>built-in reserved fields</b> . Otherwise, problems such as duplicate field names and inaccurate query may occur.                                                                   |
| tenant_project_id | No        | String          | Project ID. For details about how to obtain it, see <b>Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</b> .                                                                                                               |

## Response Parameters

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



**Table 4-62** Response body parameters

| Parameter    | Type   | Description                                                                                                                  |
|--------------|--------|------------------------------------------------------------------------------------------------------------------------------|
| errorCode    | String | Indicates the error code.<br>Example value:<br><ul style="list-style-type: none"> <li>• SVCSTG.ALS.200.200</li> </ul>        |
| errorMessage | String | Indicates the response description.<br>Example value:<br><ul style="list-style-type: none"> <li>• Report success.</li> </ul> |
| result       | String | Response result.                                                                                                             |

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

**Table 4-63** Response body parameters

| Parameter    | Type   | Description                                                                                                                                                                                      |
|--------------|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| errorCode    | String | Indicates the error code.<br>Example value:<br><ul style="list-style-type: none"> <li>• SVCSTG.ALS.200.201</li> <li>• SVCSTG.ALS.200.210</li> </ul>                                              |
| errorMessage | String | Indicates the error description.<br>Example value:<br><ul style="list-style-type: none"> <li>• Request conditions must be json format.</li> <li>• projectid xxx log's quota has full.</li> </ul> |
| result       | String | Response result.                                                                                                                                                                                 |

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

**Table 4-64** Response body parameters

| Parameter    | Type   | Description                                                                                                                      |
|--------------|--------|----------------------------------------------------------------------------------------------------------------------------------|
| errorCode    | String | Indicates the error code.<br>Example value:<br><ul style="list-style-type: none"> <li>• SVCSTG.ALS.403.105</li> </ul>            |
| errorMessage | String | Indicates the error description.<br>Example value:<br><ul style="list-style-type: none"> <li>• Project id is invalid.</li> </ul> |
| result       | String | Response result.                                                                                                                 |

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

**Table 4-65** Response body parameters

| Parameter    | Type   | Description                                                                                                            |
|--------------|--------|------------------------------------------------------------------------------------------------------------------------|
| errorCode    | String | Indicates the error code.<br>Example value:<br><ul style="list-style-type: none"> <li>LTS.200500</li> </ul>            |
| errorMessage | String | Indicates the error description.<br>Example value:<br><ul style="list-style-type: none"> <li>Internal error</li> </ul> |
| result       | String | Response result.                                                                                                       |

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

**Table 4-66** Response body parameter

| Parameter | Type   | Description                           |
|-----------|--------|---------------------------------------|
| result    | String | The requested service is unavailable. |

## Example Request

```
POST https://{access_IP_address:8102}/v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents
{
 "log_time_ns": 1586850540000000000,
 "contents": [
 "Fri Feb 1 07:48:04 UTC 2019 0\n",
 "Sat Apri 18 16:04:04 UTC 2019"
],
 "labels": {
 "user_tag": "string"
 }
}
```

## Example Response

Example response with status code **200**:

Logs are reported.

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

Example response with status code **401**:

The authentication information is incorrect or invalid.

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

## Status Code

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

## 4.4.3 API for Reporting High-Precision Logs

### Function

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

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

#### NOTE

Each log event will carry a nanosecond-level timestamp when it is reported. When you view logs on the LTS console, the log events are sorted by timestamp. For details about the constraints on log reporting, see [Log Read/Write Constraints](#).

### URI

POST /v2/{project\_id}/lts/groups/{log\_group\_id}/streams/{log\_stream\_id}/tenant/contents/high-accuracy

**Table 4-67** URI parameters

| Parameter     | Mandatory | Type   | Description                                                                                                                                                                                                                                                                               |
|---------------|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| project_id    | Yes       | String | Project ID. For details about how to obtain it, see <a href="#">Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</a> .<br>No default value.<br>Value length: 32 characters                                                                                           |
| log_group_id  | Yes       | String | Log group ID. For details about how to obtain it, see <a href="#">Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</a> .<br>No default value.<br>Value length: 36 characters                                                                                         |
| log_stream_id | Yes       | String | Log stream ID. For details about how to obtain it, see <a href="#">Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</a> .<br>No default value.<br>Value length: 36 characters<br><b>NOTE</b><br>A write rate exceeding 100 MB/s per log stream may cause log losses. |

## Request Parameters

**Table 4-68** Request header parameters

| Parameter    | Mandatory | Type   | Description                                                                                                                                                                                                                         |
|--------------|-----------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| X-Auth-Token | Yes       | String | Indicates the user token obtained from IAM. For details about how to obtain a user token, see <a href="#">Obtaining a User Token</a> .<br>No default value.<br>Minimum length: 1,000 characters<br>Maximum length: 2,000 characters |

| Parameter        | Mandatory | Type   | Description                                                                                                                                                                        |
|------------------|-----------|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Content-Type     | Yes       | String | Set this parameter to <b>application/json;charset=UTF-8</b> .<br>No default value.<br>Minimum length: 30 characters<br>Maximum length: 30 characters                               |
| Content-Encoding | No        | String | Log compression format.<br>Example value: <ul style="list-style-type: none"> <li>• <b>GZIP</b></li> <li>• <b>SNAPPY</b></li> <li>• <b>gzip</b></li> <li>• <b>snappy</b></li> </ul> |

**Table 4-69** Request body parameters

| Parameter         | Mandatory | Type                                 | Description                                                                                                                                                                             |
|-------------------|-----------|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| contents          | Yes       | Array of <a href="#">LogContents</a> | Indicates a list of log events that carry reporting timestamps.                                                                                                                         |
| labels            | Yes       | Object                               | Custom labels.<br><b>NOTE</b><br>Do not set field names to <a href="#">built-in reserved fields</a> . Otherwise, problems such as duplicate field names and inaccurate query may occur. |
| tenant_project_id | No        | String                               | Project ID. For details about how to obtain it, see <a href="#">Obtaining the Account ID, Project ID, Log Group ID, and Log Stream ID</a> .                                             |

**Table 4-70** LogContents

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

## Response Parameters

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

**Table 4-71** Response body parameters

| Parameter    | Type   | Description                                                                                                                  |
|--------------|--------|------------------------------------------------------------------------------------------------------------------------------|
| errorCode    | String | Indicates the error code.<br>Example value:<br><ul style="list-style-type: none"> <li>• SVCSTG.ALS.200.200</li> </ul>        |
| errorMessage | String | Indicates the response description.<br>Example value:<br><ul style="list-style-type: none"> <li>• Report success.</li> </ul> |
| result       | String | Response result.                                                                                                             |

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

**Table 4-72** Response body parameters

| Parameter | Type   | Description                                                                                                                                         |
|-----------|--------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| errorCode | String | Indicates the error code.<br>Example value:<br><ul style="list-style-type: none"> <li>• SVCSTG.ALS.200.201</li> <li>• SVCSTG.ALS.200.210</li> </ul> |

| Parameter    | Type   | Description                                                                                                                                                                               |
|--------------|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| errorMessage | String | Indicates the error description.<br>Example value: <ul style="list-style-type: none"> <li>Request conditions must be json format.</li> <li>projectid xxx log's quota has full.</li> </ul> |
| result       | String | Response result.                                                                                                                                                                          |

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

**Table 4-73** Response body parameters

| Parameter    | Type   | Description                                                                                                                 |
|--------------|--------|-----------------------------------------------------------------------------------------------------------------------------|
| errorCode    | String | Indicates the error code.<br>Example value: <ul style="list-style-type: none"> <li>SVCSTG.ALS.403.105</li> </ul>            |
| errorMessage | String | Indicates the error description.<br>Example value: <ul style="list-style-type: none"> <li>Project id is invalid.</li> </ul> |
| result       | String | Response result.                                                                                                            |

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

**Table 4-74** Response body parameters

| Parameter    | Type   | Description                                                                                                         |
|--------------|--------|---------------------------------------------------------------------------------------------------------------------|
| errorCode    | String | Indicates the error code.<br>Example value: <ul style="list-style-type: none"> <li>LTS.200500</li> </ul>            |
| errorMessage | String | Indicates the error description.<br>Example value: <ul style="list-style-type: none"> <li>Internal error</li> </ul> |
| result       | String | Response result.                                                                                                    |

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

**Table 4-75** Response body parameter

| Parameter | Type   | Description                           |
|-----------|--------|---------------------------------------|
| result    | String | The requested service is unavailable. |

## Example Request

```
POST https://{access_IP_address:8102}/v2/{project_id}/lts/groups/{log_group_id}/streams/{log_stream_id}/tenant/contents/high-accuracy
{
 "contents": [
 {
 "log_time_ns": 1586850540000000000,
 "log": "Fri Feb 15 15:48:04 UTC 2019"
 },
 {
 "log_time_ns": 1586850540000000001,
 "log": "Sat Apri 18 16:04:04 UTC 2019"
 }
],
 "labels": {
 "user_tag": "string"
 }
}
```

## Example Response

Example response with status code **200**:

Logs are reported.

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

Example response with status code **401**:

The authentication information is incorrect or invalid.

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

## Status Code

| Status Code | Description                                                                                             |
|-------------|---------------------------------------------------------------------------------------------------------|
| 200         | The request has succeeded.                                                                              |
| 400         | The request is invalid. Modify the request based on the description in <b>error_msg</b> before a retry. |
| 401         | The authentication information is incorrect or invalid.                                                 |



| Status Code | Description                           |
|-------------|---------------------------------------|
| 500         | An internal error occurred.           |
| 503         | The requested service is unavailable. |

## 4.5 Ingesting Logs to LTS Across IAM Accounts

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

### NOTE

After you configure cross-account ingestion, if account A deletes the agency from IAM, LTS cannot detect the deletion and the cross-account ingestion still takes effect. If the cross-account ingestion configuration is no longer used, notify account B to delete it.

### Prerequisites

An agency relationship has been created.

### Constraints

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


### Setting Cross-Account Ingestion

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

**Step 1** Log in to the [LTS console](#).

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

Alternatively, choose **Log Ingestion > Ingestion Management** in the navigation pane, and click **Ingest Log > Cross-Account Ingestion - Log Stream Mapping**.

Alternatively, choose **Log Management** in the navigation pane and click the target log stream to access its details page. Click  in the upper right corner. On the displayed page, click the **Log Ingestion** tab and **Ingest Log**. In the displayed dialog box, click **Cross-Account Ingestion - Log Stream Mapping**.

**Step 3** Select an agency.

Set parameters by referring to [Table 4-76](#) and click **Next: Log Stream Mapping**.

**Table 4-76** Agency parameters

| Parameter              | Description                                                                                                                                                                                |
|------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Agency Name            | Enter the name of the agency created in IAM by the delegator. A delegator account can <b>create an agency</b> to delegate resource management permissions to another Huawei Cloud account. |
| Delegator Account Name | Enter the delegator account name to verify the delegation.                                                                                                                                 |

 **NOTE**

- The delegator account and the delegated account must be different tenants.
- The delegated account must be assigned the **Agent Operator** role to verify the agency when using the LTS agency function.

**Step 4** Map log streams.

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

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

**Table 4-77** Parameters of automatic ingestion rule configuration

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

 **NOTE**

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

c. Click **Preview**.

 **NOTE**

1. There are two types of preview results:
  - **A new target log stream will be created:** A target log group or log stream will be created in the delegated account.
  - **An existing target log stream will be ingested:** The target log group or log stream already exists in the delegated account.
2. Preview error messages are as follows:
  - Source log stream *xxx* has been configured as the target log stream.
  - Target log stream *xxx* has been configured as the source log stream.
  - Target log stream *xxx* already exists in another log group.
  - Target log stream *xxx* exists in different target log groups.
  - Duplicate rule names.
  - The source log stream *xxx* is already mapped.
  - The number of log groups has reached the upper limit. Select an existing log group.

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

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

● **Manual configuration**

- a. On the **Log Stream Mapping** page, click **Add Rule**. Set the rule by referring to [Table 4-78](#).

**Table 4-78** Parameters

| Parameter          |                   | Description                                                                                                                                                                                                                                |
|--------------------|-------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Rule Name          |                   | The default value is <b>rule_xxx</b> . You can also specify a name as needed.<br>Can contain only letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot start with a period or underscore, or end with a period. |
| Delegat or Account | Source Log Group  | Log group of the delegator account. Select an existing log group.                                                                                                                                                                          |
|                    | Source Log Stream | Log stream of the delegator account. Select an existing log stream.                                                                                                                                                                        |

| Parameter         |                   | Description                                                                                               |
|-------------------|-------------------|-----------------------------------------------------------------------------------------------------------|
| Delegated Account | Target Log Group  | Log group of the delegator account. You can select an existing log group or enter a name to create one.   |
|                   | Target Log Stream | Log stream of the delegated account. You can select an existing log stream or enter a name to create one. |

b. Click **Preview**.

 **NOTE**

1. There are two types of preview results:
  - **A new target log stream will be created:** A target log group or log stream will be created in the delegated account.
  - **An existing target log stream will be ingested:** The target log group or log stream already exists in the delegated account.
2. There are five types of preview errors:
  - Source log stream *xxx* has been configured as the target log stream.
  - Target log stream *xxx* has been configured as the source log stream.
  - Target log stream *xxx* already exists in another log group.
  - Target log stream *xxx* exists in different target log groups.
  - Duplicate rule names.
  - The source log stream *xxx* is already mapped.
  - The number of log groups or log streams exceeds the upper limit.

If any of the preceding error messages is displayed, delete the corresponding ingestion rule of the log stream.
- c. After the preview is complete, click **Submit** and wait until the log ingestion task is created.

**Step 5** Complete the ingestion configuration.

 **NOTE**

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

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

----End

## 4.6 Using Kafka to Report Logs to LTS

You can use various Kafka Producer SDKs or collection tools that support the Kafka protocol to report logs to LTS. This function applies to the following scenarios:

- **Scenario 1:** If you have built a system based on open-source tools, such as Logstash, simply modify the configuration file to enable log reporting to LTS.
- **Scenario 2:** If you want to use Kafka Producer SDKs to collect and report logs, you do not need to install ICAgent.

### NOTE

Currently, this function is available only in regions CN North-Beijing4, CN South-Guangzhou, CN East-Shanghai1, CN East-Shanghai2, and AP-Singapore. To use it in other regions, [submit a service ticket](#).

### Prerequisites

- You have registered an account and enabled LTS.
- You have obtained the ID of the region where LTS is deployed.
- **You have obtained the AK/SK of your account.**
- You have obtained a project ID of your Huawei Cloud account. For details, see [API Credentials](#) in *My Credentials*.
- You have obtained the IDs of the target log group and stream in LTS.
- Currently, this function is available only for reporting ECSs logs over intranets.

### Constraints

- Currently, this function is available only on intranets. The port number must be 9095. You can set the IP address as required.
- The supported Kafka protocol versions are 1.0.X, 2.X.X, and 3.X.X.
- The supported compression modes are gzip, snappy, and lz4.
- The Kafka authentication mode is SASL\_PLAINTEXT.
- The **ACKS** parameter of the Kafka protocol must be set to 0.

### Configuration

- To use the Kafka protocol to report logs, set the following common parameters:

**Table 4-79** Common parameters

| Parameter   | Description                    | Type   |
|-------------|--------------------------------|--------|
| projectId   | Project ID of the user account | String |
| logGroupId  | LTS log group ID               | String |
| logStreamId | LTS log stream ID              | String |

| Parameter    | Description                              | Type   |
|--------------|------------------------------------------|--------|
| regionName   | Region where the LTS service is deployed | String |
| accessKey    | AK of the user account                   | String |
| accessSecret | SK of the user account                   | String |

- To use Kafka to report logs, you also need to set the following parameters:

**Table 4-80** Configuration parameters

| Parameter        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Connecti on type | <b>SASL_PLAINTEXT</b> is supported.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| hosts            | IP address and port number of Kafka. The format is <code>lts-kafka.\${regionName}.\${external_global_domain_name}:9095</code> or <code>lts-access.\${regionName}.\${external_global_domain_name}:9095</code> . Set the IP address based on the site requirements and set the port number to 9095. For details, see <a href="#">Obtaining Parameters</a> . For example, the value of <b>hosts</b> for the CN North-Beijing4 region is <code>lts-kafka.cn-north-4.myhuaweicloud.com:9095</code> . |
| topic            | Kafka topic name. The format is <code>_\${log group ID}_\${log stream ID}</code> , in which the LTS log group and stream IDs are connected by an underscore (_).                                                                                                                                                                                                                                                                                                                                |
| username         | Username for accessing Kafka. Set this parameter to the project ID of the user account.                                                                                                                                                                                                                                                                                                                                                                                                         |
| password         | Password for accessing Kafka. The format is <code>_\${accessKey}#\${accessSecret}</code> , in which the AK and SK of the user account are connected by a number sign (#).                                                                                                                                                                                                                                                                                                                       |
| headers          | When customizing the <b>label</b> field, you need to configure <b>headers</b> .<br>Add a header with the key <b>LTS_LOG_TYPE</b> and the value <b>FORMAT</b> to <b>headers</b> . The reported logs must be standardized logs that meet the format requirement.                                                                                                                                                                                                                                  |

- `_${message}` log format  
Logs must comply with this format only when a header whose key is **LTS\_LOG\_TYPE** and value is **FORMAT** is added to **headers**.

**Table 4-81** Log parameters

| Parameter         | Mandatory | Type            | Description                                                                                                                                                                                                                                                                                                                                      |
|-------------------|-----------|-----------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| tenant_project_id | Yes       | String          | Project ID of the user account                                                                                                                                                                                                                                                                                                                   |
| tenant_group_id   | Yes       | String          | LTS log group ID                                                                                                                                                                                                                                                                                                                                 |
| tenant_stream_id  | Yes       | String          | LTS log stream ID                                                                                                                                                                                                                                                                                                                                |
| log_time_ns       | Yes       | Long            | Log collection time (UTC time, in nanoseconds)<br><br><b>NOTE</b><br>The interval between the log collection time and current time must be less than the log retention duration. Otherwise, reported logs will be cleared. For example, if the log retention duration is seven days, the log collection time must be within the last seven days. |
| contents          | Yes       | Array of String | Log content                                                                                                                                                                                                                                                                                                                                      |
| labels            | Yes       | Object          | Custom labels<br><br><b>NOTE</b><br>Avoid using the name of a <b>built-in reserved field</b> as a field name to prevent issues like duplicate names and query inaccuracies.                                                                                                                                                                      |

## Log Example

```
{
 "tenant_project_id": "${projectId}",
 "tenant_group_id": "${logGroupId}",
 "tenant_stream_id": "${logStreamId}",
 "log_time_ns": "XXXXXXXXXXXXXXXXXXXX",
 "contents": [
 "This is a log 1",
 "This is a log 2"
],
 "labels": {
 "type": "kafka"
 }
}
```

## Calling Example

1. The following uses FileBeat as an example to describe how to configure parameters for calling by Beat series software.

```
output.kafka:
 hosts: ["${ip}:${port}"]
 partition.round_robin:
```

```

reachable_only: false
username: "${projectId}"
password: "${accessKey}#${accessSecret}"
topic: "${logGroupId}_${logStreamId}"
sasl.mechanism: "PLAIN"
security.protocol: "SASL_PLAINTEXT"
acks: "0"
compression: gzip

```

2. When Logstash is used to report logs:

```

input {
 stdin {}
}
output {
 kafka {
 # Configure an address.
 bootstrap_servers => "${ip}:${port}"
 # Configure a topic.
 topic_id => "${logGroupId}_${logStreamId}"
 # Configure a message acknowledgment mechanism.
 acks => "0"
 # Configure a compression mode.
 compression_type => "gzip"
 # Configure an authentication mode.
 security_protocol => "SASL_PLAINTEXT"
 sasl_mechanism => "PLAIN"
 # Username: projectId; Password: accessKey#accessSecret
 sasl_jaas_config => "org.apache.kafka.common.security.plain.PlainLoginModule required username='${projectId}' password='${accessKey}#${accessSecret}';"
 }
}

```

3. When Flume is used to report logs:

```

#Name
a1.sources = r1
a1.channels = c1
a1.sinks = k1
#Source
a1.sources.r1.type = TAILDIR
a1.sources.r1.channels = c1
a1.sources.r1.filegroups = f1
a1.sources.r1.filegroups.f1 = /tmp/test.txt
a1.sources.r1.fileHeader = true
a1.sources.r1.maxBatchCount = 1000
#Channel
a1.channels.c1.type = memory
a1.channels.c1.capacity = 10000
a1.channels.c1.transactionCapacity = 100
#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";
#Bind
a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1

```

## SDK Calling Examples

1. Java SDK calling example:

Maven dependency (take Kafka protocol 2.7.1 as an example):

```

<dependencies>
 <dependency>

```



```
<groupId>org.apache.kafka</groupId>
<artifactId>kafka-clients</artifactId>
<version>2.7.1</version>
</dependency>
</dependencies>
```

### Sample code:

```
package org.example;
import org.apache.kafka.clients.producer.KafkaProducer;
import org.apache.kafka.clients.producer.Producer;
import org.apache.kafka.clients.producer.ProducerRecord;
import java.util.Properties;
public class ProducerDemo {
 public static void main(String[] args) {
 Properties props = new Properties();
 // Configure an address.
 props.put("bootstrap.servers", "${ip}:${port}");
 // Configure a message acknowledgment mechanism.
 props.put("acks", "0");
 // Configure an authentication mode.
 props.put("security.protocol", "SASL_PLAINTEXT");
 props.put("sasl.mechanism", "PLAIN");
 // Username: projectId; Password: accessKey#accessSecret
 props.put("sasl.jaas.config",
 "org.apache.kafka.common.security.plain.PlainLoginModule required username='${projectId}'
 password='${accessKey}#${accessSecret}");
 // Configure a compression mode.
 props.put("compression.type", "${compress_type}");
 props.put("key.serializer", "org.apache.kafka.common.serialization.StringSerializer");
 props.put("value.serializer", "org.apache.kafka.common.serialization.StringSerializer");
 // 1. Create a producer object.
 Producer<String, String> producer = new KafkaProducer<>(props);
 // 2. Call the send method.
 for (int i = 0; i < 1; i++) {
 ProducerRecord record = new ProducerRecord<>("${logGroupId}_${logStreamId}", "${message}");
 // Configure recordHeader.
 // record.headers().add(new RecordHeader("LTS_LOG_TYPE", "FORMAT".getBytes()));
 producer.send(record);
 }
 // 3. Close the producer.
 producer.close();
 }
}
```

## 2. Python SDK calling example:

```
from kafka import KafkaProducer
producer = KafkaProducer(
 # Configure an address.
 bootstrap_servers="${ip}:${port}",
 # Configure a message acknowledgment mechanism.
 acks="0",
 # Configure a compression mode.
 compression_type="${compression_type}"
 # Configure an authentication mode.
 sasl_mechanism="PLAIN",
 security_protocol="SASL_PLAINTEXT",
 # Username: projectId; Password: accessKey#accessSecret
 sasl_plain_username="${projectId}",
 sasl_plain_password="${accessKey}#${accessSecret}"
)
print('start producer')
for i in range(0, 3):
 data = bytes("${message}", encoding="utf-8")
 future = producer.send("${logGroupId}_${logStreamId}", data)
 result = future.get(timeout=10)
 print(result)
print('end producer')
```

## Error Description

If there is an invalid or mismatched parameter, an error message will be displayed.

**Table 4-82** Error description

| Error Message                    | Cause                                                                                                                                                                                                                                                                                   |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TopicAuthorizationException      | The <b>projectId</b> (project ID), <b>accessKey</b> (AK), and <b>accessSecret</b> (SK) parameters are invalid or mismatched.                                                                                                                                                            |
| UnknownTopicOrPartitionException | The <b>logGroupId</b> (log group ID) and <b>logStreamId</b> (log stream ID) parameters are invalid or mismatched.                                                                                                                                                                       |
| InvalidRecordException           | This error occurs only when the <b>headers</b> parameter is configured to report standardized logs.<br>The log format is incorrect, or the settings of <b>projectId</b> , <b>logGroupId</b> , and <b>logStreamId</b> in the log are inconsistent with those of the external parameters. |

## Obtaining Parameters

**Table 4-83** Regions

| Region             | RegionName                                 |
|--------------------|--------------------------------------------|
| CN North-Beijing4  | lts-kafka.cn-north-4.myhuaweicloud.com     |
| CN East-Shanghai1  | lts-access.cn-east-3.myhuaweicloud.com     |
| CN East-Shanghai2  | lts-kafka.cn-east-2.myhuaweicloud.com      |
| CN South-Guangzhou | lts-access.cn-south-1.myhuaweicloud.com    |
| AP-Singapore       | lts-kafka.ap-southeast-3.myhuaweicloud.com |

## 4.7 Using Flume to Report Logs to LTS

Flume is a reliable, high-availability, and distributed system for collecting, aggregating, and transporting massive logs. It allows you to customize various data senders in a log system for better data collection. Flume can also process data simply and write data to various data receivers.

You can collect logs using Flume and report logs using the Kafka protocol supported by LTS. The following are some common data collection scenarios:

1. [Using Flume to Collect Text Logs to LTS](#)
2. [Using Flume to Collect Database Table Data to LTS](#)
3. [Using Flume to Collect Logs Transmitted with the Syslog Protocol to LTS](#)
4. [Using Flume to Collect Logs Transmitted with the TCP/UDP Protocol to LTS](#)
5. [Using Flume to Collect Device Management Data Reported with the SNMP Protocol to LTS](#)
6. [Using Default Interceptors to Process Logs](#)
7. [Using a Custom Interceptor to Process Logs](#)
8. [Enriching Logs with External Data Sources and Reporting the Logs to LTS](#)

## Prerequisites

- The Java Development Kit (JDK) has been installed on the host.
- Flume has been installed and the JDK path has been configured in the Flume configuration file.

## Using Flume to Collect Text Logs to LTS

You can add the **conf** file to use Flume to collect text logs and report them to LTS by referring to the following example. For details about the following parameters, see [Using Kafka to Report Logs to LTS](#).

```
#Named
a1.sources = r1
a1.channels = c1
a1.sinks = k1

#Source
a1.sources.r1.type = TAILDIR
a1.sources.r1.channels = c1
a1.sources.r1.filegroups = f1
a1.sources.r1.filegroups.f1 = /tmp/test.txt
a1.sources.r1.fileHeader = true
a1.sources.r1.maxBatchCount = 1000

#Channel
a1.channels.c1.type = memory
a1.channels.c1.capacity = 10000
a1.channels.c1.transactionCapacity = 100

#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

#Bind
a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

## Using Flume to Collect Database Table Data to LTS

You can use Flume to collect database table data and report it to LTS to monitor table data changes. For details about the following parameters, see [Using Kafka to Report Logs to LTS](#).

**Step 1** Download the [flume-ng-sql-source](#) plug-in and compress it into a JAR package named **flume-ng-sql-source.jar**. Before packaging, ensure that the version of flume-ng-core in the POM file is the same as that of Flume to be installed. Then, place the JAR package in the **lib** directory in the Flume package installation path, for example, **FLUME\_HOME/lib**. Replace **FLUME\_HOME** with the actual installation path.

**Step 2** Add the MySQL driver to the **FLUME\_HOME/lib** directory.

1. Download the MySQL driver package.  
`wget https://dev.mysql.com/get/Downloads/Connector-J/mysql-connector-java-5.1.35.tar.gz`
2. Decompress the driver package and compress it into a JAR package.  
`tar xzf mysql-connector-java-5.1.35.tar.gz`
3. Place the JAR package in the **FLUME\_HOME/lib/** directory.  
`cp mysql-connector-java-5.1.35-bin.jar FLUME_HOME/lib/`

**Step 3** Add the **conf** file for collecting MySQL data.

```
a1 indicates the agent name.
source indicates the input source of a1.
channels indicates a buffer.
sinks indicates the output destination of a1. In this example, Kafka is used.
a1.channels = c1
a1.sources = r1
a1.sinks = k1

#source
a1.sources.r1.type = org.keedio.flume.source.SQLSource
Connect to MySQL: Replace {mysql_host} with the IP address of your VM and {database_name} with the
database name. You can run the ifconfig or ip addr command to obtain the IP address.
Add ?useUnicode=true&characterEncoding=utf-8&useSSL=false to the URL. Otherwise, the connection
may fail.
a1.sources.r1.hibernate.connection.url = jdbc:mysql://{mysql_host}:3306/{database_name}?
useUnicode=true&characterEncoding=utf-8&useSSL=false
Hibernate Database connection properties
MySQL account, which generally is root.
a1.sources.r1.hibernate.connection.user = root
Enter your MySQL password.
a1.sources.r1.hibernate.connection.password = xxxxxxxx
a1.sources.r1.hibernate.connection.autocommit = true
MySQL driver.
a1.sources.r1.hibernate.dialect = org.hibernate.dialect.MySQL5Dialect
a1.sources.r1.hibernate.connection.driver_class = com.mysql.jdbc.Driver
Store the status file.
a1.sources.r1.status.file.path = FLUME_HOME/bin
a1.sources.r1.status.file.name = sqlSource.status
Custom query
Replace {table_name} with the name of the data table to be collected. You can also use the following
method:
a1.sources.r1.custom.query = select * from {table_name}

#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
```

```
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 10000
a1.channels.c1.transactionCapacity = 10000
a1.channels.c1.byteCapacityBufferPercentage = 20
a1.channels.c1.byteCapacity = 800000
```

**Step 4** After being started, Flume collects table data from the database to LTS.

----End

## Using Flume to Collect Logs Transmitted with the Syslog Protocol to LTS

Syslog is a protocol used to transmit log messages on an IP network. Flume collects logs transmitted using syslog and reports them to LTS. For details about the following parameters, see [Using Kafka to Report Logs to LTS](#).

- To receive UDP logs, add the **conf** file for collecting logs transmitted using syslog. Example:

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type=syslogudp
host_port indicates the port number of the syslog server.
a1.sources.r1.port = {host_port}
host_ip indicates the IP address of the syslog server.
a1.sources.r1.host = {host_ip}
a1.sources.r1.channels = c1

a1.channels.c1.type = memory

#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";
a1.sinks.k1.channel = c1
```

- To receive TCP logs, add the **conf** file for collecting logs transmitted using syslog. Example:

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type=syslogtcp
host_port indicates the port number of the syslog server.
a1.sources.r1.port = {host_port}
host_ip indicates the IP address of the syslog server.
a1.sources.r1.host = {host_ip}
a1.sources.r1.channels = c1

a1.channels.c1.type = memory

#Sink
a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
```

```
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";
a1.sinks.k1.channel = c1
```

## Using Flume to Collect Logs Transmitted with the TCP/UDP Protocol to LTS

You can use Flume to collect logs transmitted with the TCP/UDP protocol and report them to LTS. For details about the following parameters, see [Using Kafka to Report Logs to LTS](#).

- To collect TCP port logs, add the **conf** file of the collection port. Example:

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type = netcat
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = {host_port}

a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

- To collect UDP port logs, add the **conf** file of the collection port. Example:

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type = netcatudp
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = {host_port}

a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

## Using Flume to Collect Device Management Data Reported with the SNMP Protocol to LTS

You can use Flume to collect device management data reported with SNMP and send the data to LTS. For details about the following parameters, see [Using Kafka to Report Logs to LTS](#).

- Listen to port number 161 of the SNMP communication by adding the **conf** file for receiving SNMP logs. Example:

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type = netcatudp
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = 161

a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

- Listen to port number 162 of SNMP trap communication by adding the **conf** file for receiving SNMP logs. Example:

```
a1.sources = r1
a1.sinks = k1
a1.channels = c1

a1.sources.r1.type = netcatudp
a1.sources.r1.bind = 0.0.0.0
a1.sources.r1.port = 162

a1.sinks.k1.type = org.apache.flume.sink.kafka.KafkaSink
a1.sinks.k1.kafka.topic = ${logGroupId}_${logStreamId}
a1.sinks.k1.kafka.bootstrap.servers = ${ip}:${port}
a1.sinks.k1.kafka.producer.acks = 0
a1.sinks.k1.kafka.producer.security.protocol = SASL_PLAINTEXT
a1.sinks.k1.kafka.producer.sasl.mechanism = PLAIN
a1.sinks.k1.kafka.producer.compression.type = gzip
a1.sinks.k1.kafka.producer.sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule
required username="${projectId}" password="${accessKey}#${accessSecret}";

a1.channels.c1.type = memory
a1.channels.c1.capacity = 1000
a1.channels.c1.transactionCapacity = 100

a1.sources.r1.channels = c1
a1.sinks.k1.channel = c1
```

## Using Default Interceptors to Process Logs

In Flume, an interceptor is a simple pluggable component between a source and channels. Before a source writes received events to channels, the interceptor can convert or delete the events. Each interceptor processes only the events received by a given source.

- **Timestamp interceptor**

This interceptor inserts a timestamp into Flume event headers. If no interceptor is used, Flume receives only messages. To configure the connection between a source and a timestamp interceptor, set **type** to **timestamp** and the class name full path **preserveExisting** to **false**. You can also set **preserveExisting** to **true**, indicating the value of the timestamp header will not be replaced if the header already exists in the event. Configuration example:

```
a1.sources.r1.interceptors = timestamp
a1.sources.r1.interceptors.timestamp.type=timestamp
a1.sources.r1.interceptors.timestamp.preserveExisting=false
```

- **Regex filtering interceptor**

This interceptor filters out unnecessary logs during collection or selectively collects logs that meet a specified regular expression. Set **type** to **REGEX\_FILTER**. If you set **excludeEvents** to **false**, events that match a specified regular expression are collected. If you set **excludeEvents** to **true**, matched events are deleted and unmatched events are collected. Example configuration for connecting a source to a regex filtering interceptor:

```
a1.sources.r1.interceptors = regex
a1.sources.r1.interceptors.regex.type=REGEX_FILTER
a1.sources.r1.interceptors.regex.regex=(today)|(Monday)
a1.sources.r1.interceptors.regex.excludeEvents=false
```

In this way, the configured interceptor collects only the logs containing **today** or **Monday** in the log messages.

- **Search and replace interceptor**

This interceptor provides a simple string-based search and replacement function based on Java regular expressions. Configuration example:

```
Interceptor alias
a1.sources.r1.interceptors = search-replace
Interceptor type. The value must be search_replace.
a1.sources.r1.interceptors.search-replace.type = search_replace

Delete characters from the event body and match the event content based on a specified regular
expression.
a1.sources.r1.interceptors.search-replace.searchPattern = today
Replace the matched event content.
a1.sources.r1.interceptors.search-replace.replaceString = yesterday
Set a character set. The default value is utf8.
a1.sources.r1.interceptors.search-replace.charset = utf8
```

## Using a Custom Interceptor to Process Logs

The following uses Java as an example to describe how to customize an interceptor in Flume. **FLUME\_HOME** specifies where Flume is installed. It is **/tools/flume** in this example and needs to be replaced with the actual Flume installation directory.

**Step 1** Create a Maven project and introduce the Flume dependency.



Ensure that the dependency matches the Flume version in the target cluster.

```
<dependencies>
 <dependency>
 <groupId>org.apache.flume</groupId>
 <artifactId>flume-ng-core</artifactId>
 <version>1.10.1</version>
 <scope>provided</scope>
 </dependency>
</dependencies>
```

The dependency does not need to be packaged into the final JAR package. Therefore, set the scope to **provided**.

**Step 2** Create a class to implement the **Interceptor** interface and related methods.

- **initialize()** method: initializes the interceptor, reads configuration information, and establishes connections.
- **intercept(Event event)** method: intercepts and processes a single event, and receives an event object as input and returns a modified event object.
- **intercept(List<Event> list)** method: processes events in a batch, and intercepts and processes the event list.
- **close ()** method: closes the interceptor, releases the resources, and closes the connections.

```
import org.apache.flume.Event;
import org.apache.flume.interceptor.Interceptor;

import java.nio.charset.StandardCharsets;
import java.util.ArrayList;
import java.util.List;

public class TestInterceptor implements Interceptor {
 @Override
 public void initialize() {
 }
 @Override
 public Event intercept(Event event) {
 // Obtain event data.
 String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
 // Check whether the event data contains a specified string.
 if (eventData.contains("hello")) {
 // If an event contains the specified string, the event is excluded and null is returned.
 return null;
 }
 return event;
 }
 @Override
 public List<Event> intercept(List<Event> events) {
 // Create a new list to store the processed events.
 List<Event> interceptedEvents = new ArrayList<>();
 for (Event event : events) {
 Event interceptedEvent = intercept(event);
 if (interceptedEvent != null) {
 interceptedEvents.add(interceptedEvent);
 }
 }
 return interceptedEvents;
 }
 @Override
 public void close() {
```

```
}
}
```

**Step 3** Build an interceptor. The creation and configuration of an interceptor is usually implemented in Builder mode. The complete code is as follows:

```
import org.apache.flume.Context;
import org.apache.flume.Event;
import org.apache.flume.interceptor.Interceptor;

import java.nio.charset.StandardCharsets;
import java.util.ArrayList;
import java.util.List;

public class TestInterceptor implements Interceptor {
 @Override
 public void initialize() {
 }
 @Override
 public Event intercept(Event event) {
 // Obtain event data.
 String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
 // Check whether the event data contains a specified string.
 if (eventData.contains("hello")) {
 // If an event contains the specified string, the event is excluded and null is returned.
 return null;
 }
 return event;
 }
 @Override
 public List<Event> intercept(List<Event> events) {
 List<Event> interceptedEvents = new ArrayList<>();
 for (Event event : events) {
 Event interceptedEvent = intercept(event);
 if (interceptedEvent != null) {
 interceptedEvents.add(interceptedEvent);
 }
 }
 return interceptedEvents;
 }
 @Override
 public void close() {
 }

 // Build an interceptor.
 public static class Builder implements Interceptor.Builder {
 @Override
 public void configure(Context context) {
 }
 @Override
 public Interceptor build() {
 return new TestInterceptor();
 }
 }
}
```

**Step 4** Convert the interceptor to a JAR package and upload it to the **lib** folder in your Flume installation directory.

**Step 5** Compile the configuration file and configure the custom interceptor in it.

When configuring the full class name of the interceptor, note that the format is *Full class name of the interceptor*\$Builder.

```
Configuration of the interceptor.
#Definition of the interceptor.
a1.sources.r1.interceptors = i1
Full class name of the interceptor.
a1.sources.r1.interceptors.i1.type = TestInterceptor$Builder
```

## Step 6 Run Flume.

----End

KV parsing logs: Strings are separated by spaces and converted into strings of the Map type.

```
public class TestInterceptor implements Interceptor {
 @Override
 public void initialize() {
 }

 @Override
 public Event intercept(Event event) {
 // Obtain event data.
 String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
 Map<String, Object> splitMap = new HashMap<>();
 String[] splitList = eventData.split(" ");
 for (int i = 0; i < splitList.length; i++) {
 splitMap.put("field" + i, splitList[i].trim());
 }
 eventData.setBody(splitMap.toString().getBytes(StandardCharsets.UTF_8));
 return event;
 }

 @Override
 public List<Event> intercept(List<Event> events) {
 List<Event> interceptedEvents = new ArrayList<>();
 for (Event event : events) {
 Event interceptedEvent = intercept(event);
 if (interceptedEvent != null) {
 interceptedEvents.add(interceptedEvent);
 }
 }
 return interceptedEvents;
 }

 @Override
 public void close() {
 }
}
```

## Enriching Logs with External Data Sources and Reporting the Logs to LTS

An event is the basic unit for Flume to transmit data from a source to a destination. An event consists of a header and a body. The header stores certain attributes of the event in the K-V structure, and the body stores the data in the byte array format.

If an external data source is available and you want to enrich the log content, such as modifying or deleting log content, or adding fields, add the content changes to the event's body so that Flume can report them to LTS. The following example shows how to use Java to extend the log content. For details about the following parameters, see [Using Kafka to Report Logs to LTS](#).

```
import com.alibaba.fastjson.JSONObject;
```

```
import org.apache.flume.Context;
import org.apache.flume.Event;
import org.apache.flume.interceptor.Interceptor;

import java.nio.charset.StandardCharsets;
import java.util.ArrayList;
import java.util.List;

public class TestInterceptor implements Interceptor {
 @Override
 public void initialize() {
 }

 @Override
 public Event intercept(Event event) {
 // Obtain the event data, convert the original data into JSON strings, and add extra fields.
 String eventData = new String(event.getBody(), StandardCharsets.UTF_8);
 JSONObject object = new JSONObject();
 object.put("content", eventData);
 object.put("workLoadType", "RelipcaSet");
 eventData = object.toJSONString();
 eventData.setBody(eventData.getBytes(StandardCharsets.UTF_8));
 return event;
 }

 @Override
 public List<Event> intercept(List<Event> events) {
 List<Event> interceptedEvents = new ArrayList<>();
 for (Event event : events) {
 Event interceptedEvent = intercept(event);
 if (interceptedEvent != null) {
 interceptedEvents.add(interceptedEvent);
 }
 }
 return interceptedEvents;
 }

 @Override
 public void close() {
 }
}
```

# 5 Log Search and Analysis

---

## 5.1 Overview

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

- To facilitate search and analysis, configure structuring and indexing for the reported logs first to ensure the log length and format meet the requirements. For details, see [Setting Cloud Structuring Parsing](#) and [Setting Indexes](#).
- After structuring the logs, use LTS [search syntax](#) to set search criteria for higher efficiency. For details, see [Searching Logs](#).
- LTS uses [SQL analysis syntax](#) to analyze structured log fields and visualizes query and analysis results in charts. For details, see [Analyzing Logs in LTS](#).

## 5.2 Setting Cloud Structuring Parsing

### 5.2.1 Overview

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. You can then use SQL syntax to query and analyze the structured logs.

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

## Parsing Modes

LTS offers both cloud-based and ICAgent-based structuring parsing modes. However, a log stream can only be configured with one parsing mode. For example, if you have configured cloud structuring parsing for a log stream, delete the existing parsing configuration before configuring ICAgent structuring parsing. For details, see [Figure 5-1](#).

If you have not configured structuring parsing when configuring log ingestion, you can configure ICAgent or cloud configuring parsing for the target log stream separately.

- ICAgent structuring parsing is performed on the collection side and supports combined parsing of plug-ins. You can set multiple collection configurations with different structuring parsing rules for a single log stream. This parsing mode is recommended. For details, see [Setting ICAgent Structuring Parsing Rules](#).
- Leveraging the computing power of LTS servers, cloud structuring parsing structures logs in log streams using various log extraction methods. In the future, it will incur log processing traffic fees based on the log volume.

**Figure 5-1** Different parsing modes



## Precautions

- Log structuring is performed on a per-log-stream basis.
- Log structuring is recommended when most logs in a log stream share a similar pattern.

- After the structuring configuration is modified, the modification takes effect only for newly written log data.

## 5.2.2 Setting Cloud Structuring Parsing

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

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

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

### NOTE

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**.

## Constraints

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

## Cloud Structuring Parsing

**Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.



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

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

 NOTE

- If **Raw Log Save** is enabled, raw logs will be stored in LTS as the value of the **content** field. The **content** field is also counted in both resource statistics and charging.
- If **Upload Parsing Failure Log** is enabled, raw logs will be uploaded to LTS as the value of the **\_content\_parse\_fail\_** field.
- **Regular Expressions**: Extract fields using regular expressions.
- **JSON**: Extract key-value pairs from JSON log events.
- **Delimiter**: Extract fields using delimiters (such as commas or spaces).
- **Nginx**: Customize the format of access logs by using the **log\_format** command.
- **Structuring Template**: Extract fields using a custom or system template.

**Step 4** Modify or delete the configured structuring configuration.

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

 NOTE

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

----End

## Regular Expressions

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

**Step 1** Select a typical log event as the sample.

- Click **Select from Existing Logs**, select a log event, and click **OK**. You can select different time ranges to filter logs.
- Click **Paste from Clipboard** to paste the copied log content to the sample log box.

 NOTE

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

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

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



- **Auto generate:** Select the log content you want to extract as a field in the sample log event. In the dialog box displayed, set the field name. The name must start with a letter and contain only letters and digits. Then click **Add**.
- **Manually enter:** Enter a regular expression in the text box and click **Extract Field**. A regular expression may contain multiple capturing groups, which group strings with parentheses. There are three types of capturing groups:
  - (*exp*): Capturing groups are numbered by counting their opening parentheses from left to right. The numbering starts with 1.
  - (?<*name*>*exp*): named capturing group. It captures text that matches *exp* into the group *name*. The group name must start with a letter and contain only letters and digits. A group is recalled by group name or number.
  - (?:*exp*): non-capturing group. It captures text that matches *exp*, but it is not named or numbered and cannot be recalled.

#### NOTE

- Delimiters split log content into multiple words. Select a portion between two adjacent delimiters as a field. Default delimiters: ;'";=()[]{}@&<>/:\\?\\n\\t\\r and spaces.
- When you select **manually enter**, the regular expression can contain up to 5000 characters. You do not have to name capturing groups when writing the regular expression. When you click **Extract Field**, those unnamed groups will be named as **field1**, **field2**, **field3**, and so on.

**Step 3** Specify a field as the log time. For details, see [Setting Custom Log Time](#).

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

----End

## JSON

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

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

#### NOTE

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

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

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

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

Enter the log event in the text box.

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

#### NOTE

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

Check and edit the fields if needed. For details about rules for configuring extracted fields, see [Setting Structured Fields](#).

**Step 3** Specify a field as the log time. For details, see [Setting Custom Log Time](#).

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

----End

## Delimiter

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

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

#### NOTE

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

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

**Step 2** Select or customize a delimiter.

#### NOTE

- For invisible characters, enter hexadecimal characters starting with 0x. The length ranges from 0 to 4 characters. There are 32 invisible characters in total.
- For custom characters, enter 1 to 10 characters, each as an independent delimiter.
- For a custom string, enter 1 to 30 characters as one whole delimiter.

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

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

Enter the log event in the text box.

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

 **NOTE**

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

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

Check and edit the fields if needed. For details about rules for configuring extracted fields, see [Setting Structured Fields](#).

**Step 4** Specify a field as the log time. For details, see [Setting Custom Log Time](#).

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

----End

## Nginx

You can customize the format of access logs by the **log\_format** command.

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

 **NOTE**

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

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

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

 **NOTE**

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

Log format

- Default Nginx log format:

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

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

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

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

Enter the log event in the text box.

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

Configure the following Nginx log format in step 2:

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

 **NOTE**

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

Check and edit the fields if needed. For details about rules for configuring extracted fields, see [Setting Structured Fields](#).

**Step 4** Specify a field as the log time. For details, see [Setting Custom Log Time](#).

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

----End

## Structuring Template

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

For details, see [Setting a Structuring Template](#).

## 5.2.3 Setting Structured and Tag Fields

### Setting Structured Fields

You can set extracted fields after cloud structuring. For details, see [Table 5-1](#).

**Table 5-1** Rules for configuring structured fields

Template Name	Field Name	Field Type Can Be Changed	Field Can Be Deleted
Regular expressions (auto generate)	User-defined. The name must start with a letter and contain only letters and digits.	Yes	Yes
Regular expressions (manually enter)	<ul style="list-style-type: none"> <li>User-defined.</li> <li>Default names such as <b>field1</b>, <b>field2</b>, and <b>field3</b> will be used.</li> </ul>	Yes	Yes
JSON	Names are set automatically, but you can set aliases for fields.	Yes	Yes
Delimiter	Default names such as <b>field1</b> , <b>field2</b> , <b>field3</b> are used. You can modify these names.	Yes	Yes
Nginx	Names are set based on Nginx configuration, but you can set aliases for fields.	Yes	Yes
Custom templates	User-defined.	Yes	Yes

#### NOTE

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

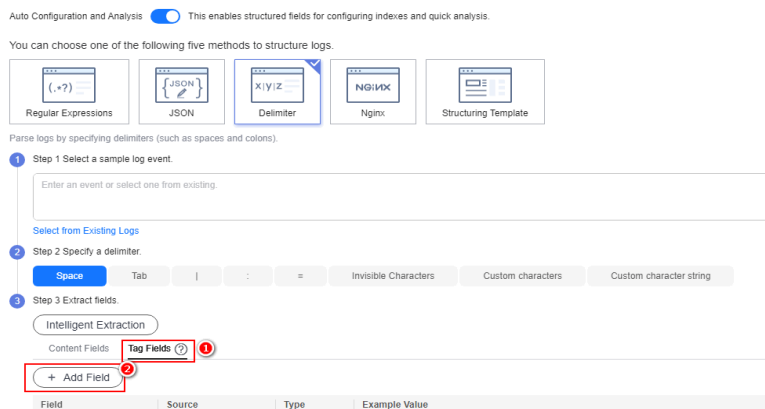
- Can contain only letters, digits, hyphens (-), underscores (\_), and periods (.).
- Cannot start with a period (.) or underscore (\_) or end with a period (.)
- Can contain 1 to 64 characters.

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

**Figure 5-2** Adding a tag field



**Step 2** In the **Field** column, enter a name for 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 3** To add more fields, click **Add Field**.

**Step 4** Click **Save**.

**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

## 5.2.4 Setting Custom Log Time

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

### Enabling Custom Log Time

**Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.

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

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

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

 NOTE

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

**Table 5-2** Parameter configuration

Parameter	Description	Example
Key	Name of an extracted field. You can select an extracted field from the drop-down list. The field is of the <b>string</b> or <b>long</b> type.	test
Value	Value of an extracted field. After a <b>Key</b> is selected, the <b>Value</b> is automatically filled in.	2022-07-19 12:12:00
Format	For details, see <a href="#">Common Log Time Formats</a> .	yyyy-MM-dd HH:mm:ss
Operation	Click <b>Verify</b> . If the message <b>The time format is successfully matched with the time field value.</b> is displayed, the verification is successful.	-

----End

## Common Log Time Formats

[Table 5-3](#) lists common log time formats.

 NOTE

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

**Table 5-3** Time formats

Format	Description	Example
EEE	Abbreviation for Week.	Fri
EEEE	Full name for Week.	Friday
MMM	Abbreviation for Month.	Jan
MMMM	Full name for Month.	January
dd	Number of the day in a month, ranging from 01 to 31 (decimal).	07, 31
HH	Hour, in 24-hour format.	22

Format	Description	Example
hh	Hour, in 12-hour format.	11
MM	Number of the month, ranging from 01 to 12 (decimal).	08
mm	Number of the minute, ranging from 00 to 59 (decimal).	59
a	AM or PM	AM, PM
hh:mm:ss a	Time in the 12-hour format.	11:59:59 AM
HH:mm	Hour and minute format.	23:59
ss	Number of the second, ranging from 00 to 59 (decimal).	59
yy	Year without century, ranging from 00 to 99 (decimal).	04, 98
yyyy	Year (decimal).	2004, 1998
d	Number of the day in a month, ranging from 1 to 31 (decimal).	7, 31
DDD	Number of the day in a year, ranging from 001 to 366 (decimal).	365
u	Number of the day in a week, ranging from 1 to 7 (decimal). The value 1 indicates Monday.	2
w	Number of the week in a year. Sunday is the start of a week. The value ranges from 00 to 53.	23
W	Number of the week in a month, ranging from 0 to 5.	2
U	Number of the day in a week, ranging from 0 to 6 (decimal). The value 0 indicates Sunday.	5
EEE MMM dd HH:mm:ss yyyy	Standard date and time.	Tue Nov 20 14:12:58 2020
EEE MMM dd yyyy	Standard date without time.	Tue Nov 20 2020
HH:mm:ss	Standard time without date.	11:59:59
%s	UNIX Timestamp.	147618725



## Examples

**Table 5-4** lists common time standards, examples, and expressions.

**Table 5-4** Examples

Example	Time Expression	Time Standard
2022-07-14T19:57:36+08:00	yyyy-MM-dd'T'HH:mm:ssXXX	Custom
1548752136	%s	Custom
27/Jan/2022:15:56:44	dd/MMM/yyyy:HH:mm:ss	Custom
2022-08-15 17:53:23+08	yyyy-MM-dd HH:mm:ssX	Custom
2022-08-05T08:24:15.536+0000	yyyy-MM-dd'T'HH:mm:ss.SSSZ	Custom
2022-08-20T10:04:03.204000Z	yyyy-MM-dd'T'HH:mm:ss.SSSZ	Custom
2022-08-22T06:52:08Z	yyyy-MM-dd'T'HH:mm:ssZ	Custom
2022-07-24T10:06:41.000	yyyy-MM-dd'T'HH:mm:ss.SSS	Custom
Monday, 02-Jan-06 15:04:05 MST	EEEE, dd-MMM-yy HH:mm:ss Z	RFC850
Mon, 02 Jan 2006 15:04:05 MST	EEE, dd MMM yyyy HH:mm:ss Z	RFC1123
02 Jan 06 15:04 MST	dd MMM yy HH:mm Z	RFC822
02 Jan 06 15:04 -0700	dd MMM yy HH:mm Z	RFC822Z
2023-01-02T15:04:05Z07:00	yyyy-MM-dd'T'HH:mm:ssZ	RFC3339
2022-12-11 15:05:07	yyyy-MM-dd HH:mm:ss	Custom

## 5.2.5 Setting a Structuring Template

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

### System Templates

You can choose from multiple system templates, but cannot modify the field types in them or delete the fields. For details, see [Table 5-5](#).

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

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

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

 **NOTE**

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

**Table 5-5** System template fields

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

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

Template Name	Field Name	Field Type Can Be Changed	Field Can Be Deleted
CCE audit logs	Defined by CCE.	No	No
CCE event logs	Defined by CCE.	No	No
CCE NGINX-INGRESS logs	Defined by CCE.	No	No -
GeminiDB Redis audit logs	Defined by GeminiDB Redis.	No	No
Influx slow query logs	Defined by Influx.	No	No
METRIC system logs	Defined by the monitoring log fields filtered by the metric generation task.	No	No
Microgateway	Defined by Microgateway.	No	No
GeminiDB Mongo audit logs	Defined by GeminiDB Mongo.	No	No

**Step 4** Click **Save**.

----End

## Custom Templates

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

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

## 5.3 Setting Indexes

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

## Index Types

LTS supports full-text and field indexes. For details, see [Table 5-6](#).

**Table 5-6** Index types

Index Type	Description
Index Whole Text	<p>LTS splits all field values of an entire log into multiple words when this function is enabled.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>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.</li> <li>System reserved fields are not included in full-text indexes. You need to use index fields (Key:Value) to search for them. For details, see <a href="#">System Reserved Fields</a>.</li> </ul>
Index Fields	<p>Query logs by specified field names and values (Key:Value).</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>LTS creates index fields for certain system reserved fields by default. For details, see <a href="#">System Reserved Fields</a>.</li> <li>If an index field is configured for a field, the delimiter of the field value is subject to the index field configuration.</li> <li>The quick analysis column in structuring settings has been removed. To use quick analysis, configure index fields and enable quick analysis for the required fields.</li> </ul> <p>Here are two examples:</p> <ul style="list-style-type: none"> <li>In the log example, the level and status index fields are configured. The level field is of the <b>string</b> type, the field value is error, and a delimiter is configured. The status field is of the <b>long</b> type, and no delimiter needs to be configured. You can use level:error to search for all logs whose level value is error.</li> <li>In the log example, LTS creates indexes for system reserved fields such as <b>hostName</b>, <b>hostIP</b>, and <b>pathFile</b> by default.</li> </ul>

## Precautions

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

- Before the field index function is available, fields supported by SQL analysis come from structured parsing on the cloud. After the field index function is available, fields supported by SQL analysis come from the field index as long as the field index is configured. Therefore, modifying the field index may affect the query results in the existing visualized charts, dashboards, SQL alarms, scheduled SQL statements, and Grafana ingestion. Exercise caution when performing this operation.

## Configuring Full-Text Indexing

**Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.

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

**Step 3** On the log stream details page, click  in the upper right corner. On the page displayed, click the **Index Settings** tab.

**Step 4** Set index parameters by referring to [Table 5-7](#). **Index Whole Text** is enabled by default.

### NOTE

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

**Table 5-7** Custom full-text indexing parameters

Parameter	Description
Index Whole Text	If <b>Index Whole Text</b> is enabled, a full-text index is created.
Case-Sensitive	Indicates whether letters are case-sensitive during query. <ul style="list-style-type: none"> <li>• If this function is enabled, the query result is case-sensitive. For example, if the example log contains <b>Know</b>, you can query the log only with <b>Know</b>.</li> <li>• If this function is disabled, the query result is case-insensitive. For example, if the example log contains <b>Know</b>, you can also query the log with <b>KNOW</b> or <b>know</b>.</li> </ul>

Parameter	Description
Include Chinese	<p>Indicates whether to distinguish between Chinese and English during query.</p> <ul style="list-style-type: none"> <li>• 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.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>- Unigram segmentation is to split a Chinese string into Chinese characters.</li> <li>- The advantage of unigram segmentation is efficient word segmentation of massive logs, and other Chinese segmentation methods have great impact on the write speed.</li> <li>- If <b>Include Chinese</b> is enabled, unigram segmentation is used for Chinese characters (each Chinese character is segmented separately). To obtain more accurate search results, use phrases with the syntax <i>"phrase to be searched for"</i>.</li> </ul> <ul style="list-style-type: none"> <li>• After this function is disabled, all content is split based on delimiters.</li> </ul> <p>For example, assume that the log content is: <b>error,400,I Know TodayIsMonday.</b></p> <ul style="list-style-type: none"> <li>• After this function is disabled, the English content is split based on delimiters. The log is split into <b>error</b>, <b>400</b>, <b>I</b>, <b>Know</b>, and <b>TodayIsMonday</b>. You can search for the log by <b>error</b> or <b>TodayIsMonday</b>.</li> <li>• After this function is enabled, the background analyzer of LTS splits the log into <b>error</b>, <b>400</b>, <b>I</b>, <b>Know</b>, <b>Today</b>, <b>Is</b>, and <b>Monday</b>. You can search for the log by <b>error</b> or <b>Today</b>.</li> </ul>

Parameter	Description
Delimiters	<p>Splits the log content into multiple words based on the specified delimiters. If the default settings cannot meet your requirements, you can customize delimiters. All ASCII codes can be defined as delimiters.</p> <p>If you leave <b>Delimiters</b> blank, the field value is regarded as a whole. You can search for logs only through a complete string or by fuzzy match.</p> <p>Click <b>Preview</b> to see the effect.</p> <p>For example, assume that the log content is: <b>error,400,I Know TodayIsMonday.</b></p> <ul style="list-style-type: none"> <li>• If no delimiter is set, the entire log is regarded as a string <b>error,400,I Know TodayIsMonday</b>. You can search for the log only by the complete string <b>error,400,I Know TodayIsMonday</b> or by fuzzy match <b>error,400,I K*</b>.</li> <li>• If the delimiter is set to a comma (,), the raw log is split into: <b>error, 400,</b> and <b>I Know TodayIsMonday</b>. You can search for the log by fuzzy or exact match, for example, <b>error, 400, I Kn*</b>, and <b>TodayIs*</b>.</li> <li>• If the delimiters are set to a comma (,) and space, the raw log is split into: <b>error, 400, I, Know, TodayIsMonday</b>. You can search for the log by fuzzy or exact match, for example, <b>Know,</b> and <b>TodayIs*</b>.</li> </ul>
ASCII Delimiters	<p>Click <b>Add ASCII Delimiter</b> and enter the ASCII value by referring to <a href="#">ASCII Table</a>.</p>

**Step 5** Click **OK**.

----End

## Configuring Index Fields

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

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

**Step 2** Click **Add Field** under **Index Fields** to configure field indexing. For details, see [Table 5-8](#).

### NOTE

- The indexing parameters take effect only for the current field.
- Index fields that do not exist in log content are invalid.
- For details about system fields, see [System Reserved Fields](#).
- Automatically configuring field indexes: Click **Auto Configure**. LTS generates field indexes based on the first log event in the preview or common system




reserved fields (such as **hostIP**, **hostName**, and **pathFile**). You can add or delete fields as required.

- Configuring field indexes in batches: Select fields and click **Batch Configure**.

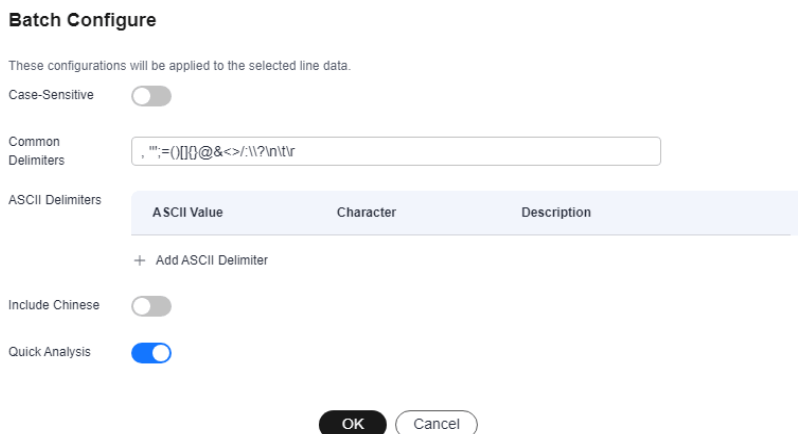
**Table 5-8** Custom index field parameters

Parameter	Description
Field	<p>Log field name, such as <b>level</b> in the example log.</p> <p>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 (__).</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Double underscores (__) are used in built-in reserved fields that are not displayed to users in LTS. Avoid using them in custom log field names, as this will prevent the configuration of field index names.</li> <li>• LTS creates index fields for certain system reserved fields by default. For details, see <a href="#">System Reserved Fields</a>.</li> <li>• For system fields, <b>system</b> is displayed next to their names.</li> </ul>
Action	<p>Displays the field status, including new, not modified, modified, and deleted. After the index field is changed, click <b>Compare</b> to view the differences between the original and modified configurations.</p> <ul style="list-style-type: none"> <li>• New fields cannot be modified.</li> <li>• When you modify the settings of <b>Type</b>, <b>Case-Sensitive</b>, <b>Common Delimiters</b>, <b>ASCII Delimiters</b>, <b>Include Chinese</b>, or <b>Quick Analysis</b>, the system compares the modified settings with the original settings and changes the action to modified.</li> <li>• After you click <b>OK</b>, the fields whose action is deleted are not saved.</li> </ul>
Type	<ul style="list-style-type: none"> <li>• Data type of the log field value. The options are <b>string</b>, <b>long</b>, <b>json</b>, and <b>float</b>.</li> </ul> <p><b>NOTE</b></p> <p>The JSON type takes effect only for ICAgent structuring parsing and does not take effect for cloud structuring parsing.</p> <ul style="list-style-type: none"> <li>• Fields of long and float types do not support <b>Case-Sensitivity</b>, <b>Include Chinese</b> and <b>Delimiters</b>.</li> </ul>
Case-Sensitive	<p>Indicates whether letters are case-sensitive during query.</p> <ul style="list-style-type: none"> <li>• If this function is enabled, the query result is case-sensitive. For example, if the <b>message</b> field in the example log contains <b>Know</b>, you can query the log only with <b>message:Know</b>.</li> <li>• If this function is disabled, the query result is case-insensitive. For example, if the <b>message</b> field in the example log contains <b>Know</b>, you can also query the log with <b>message:KNOW</b> or <b>message:know</b>.</li> </ul>

Parameter	Description
Common Delimiters	<p>Splits the log content into multiple words based on the specified delimiters. If the default settings cannot meet your requirements, you can customize delimiters. All ASCII codes can be defined as delimiters.</p> <p>If you leave <b>Delimiters</b> blank, the field value is regarded as a whole. You can search for logs only through a complete string or by fuzzy match.</p> <p>For example, the content of the <b>message</b> field in the example log is <b>I Know TodayIsMonday</b>.</p> <ul style="list-style-type: none"> <li>• If no delimiter is set, the entire log is regarded as a string <b>I Know TodayIsMonday</b>. You can search for the log only by the complete string <b>message:I Know TodayIsMonday</b> or by fuzzy search <b>message:I Know TodayIs*</b>.</li> <li>• If the delimiter is set to a space, the raw log is split into: <b>I, Know,</b> and <b>TodayIsMonday</b>. You can find the log by fuzzy search or exact words, for example, <b>message:Know,</b> or <b>message: TodayIsMonday</b>.</li> </ul>
ASCII Delimiters	<p>Click <b>Add ASCII Delimiter</b> and enter the ASCII value by referring to <a href="#">ASCII Table</a>.</p>

Parameter	Description
Include Chinese	<p>Indicates whether to distinguish between Chinese and English during query.</p> <ul style="list-style-type: none"> <li>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.</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Unigram segmentation is to split a Chinese string into Chinese characters.</li> <li>The advantage of unigram segmentation is efficient word segmentation of massive logs, and other Chinese segmentation methods have great impact on the write speed.</li> <li>If <b>Include Chinese</b> is enabled, unigram segmentation is used for Chinese characters (each Chinese character is segmented separately). To obtain more accurate search results, use phrases with the syntax <i>#"phrase to be searched for"</i>.</li> </ul> <ul style="list-style-type: none"> <li>After this function is disabled, all content is split based on delimiters.</li> </ul> <p>For example, the content of the <b>message</b> field in the example log is <b>I Know TodayIsMonday</b>.</p> <ul style="list-style-type: none"> <li>After this function is disabled, the English content is split based on delimiters. The log is split into <b>I</b>, <b>Know</b>, and <b>TodayIsMonday</b>. You can search for the log by <b>message:Know</b> or <b>message:TodayIsMonday</b>.</li> <li>After this function is enabled, the background analyzer of LTS splits the log into <b>I</b>, <b>Know</b>, <b>Today</b>, <b>Is</b>, and <b>Monday</b>. You can search for the log by <b>message:Know</b> or <b>message:Today</b>.</li> </ul>
Quick Analysis	<p>By default, this option is enabled, indicating that this field will be sampled and collected. For details, see <a href="#">Creating an LTS Quick Analysis Task</a>.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>The principle of quick analysis is to collect statistics on 100,000 logs that match the search criteria, not all logs.</li> <li>The maximum length of a field for quick analysis is 2000 bytes.</li> <li>The quick analysis field area displays the first 100 records.</li> </ul>
Operation	<p>Click  to delete the target field.</p>

**Figure 5-3** Batch configuration



**Step 3** Click **OK**.

----End

## System Reserved Fields

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

### NOTE

- When using APIs to write log data or add ICAgent configurations, avoid using the same field names as reserved field names to prevent issues such as duplicate field names and incorrect queries.
- LTS adds system reserved fields to log data at no cost. However, your usage of these fields will be billed on a pay-per-use basis. Enabling the index function for these fields will also generate a small amount of index traffic and storage fees. For more information, see [Price Calculator](#).
- A custom log field must not contain double underscores (\_\_) in its name. If it does, indexing cannot be configured for the field.

**Table 5-9** System reserved field description

Field	Data Format	Index and Statistics Settings	Description
collectTime	Integer, Unix timestamp (ms)	Index setting: After indexing is enabled, a field index is created for <b>collectTime</b> by default. The index data type is long. Enter <b>collectTime : xxx</b> during the query.	Indicates the time when logs are collected by ICAgent. Example: <b>"collectTime":"1681896081334"</b> indicates 2023-04-19 17:21:21 when converted into standard time.

Field	Data Format	Index and Statistics Settings	Description
<code>__time__</code>	Integer, Unix timestamp (ms)	Index setting: After indexing is enabled, a field index is created for <b>time</b> by default. The index data type is long. This field cannot be queried.	<p>Log time refers to the time when a log is displayed on the console.</p> <p>In the example, "<code>__time__</code>":"1681896081334" is 2023-04-19 17:21:21 when converted into standard time.</p> <p>By default, the collection time is used as the log time. You can also customize the log time.</p>
<code>lineNum</code>	Integer	Index setting: After indexing is enabled, a field index is created for <b>lineNum</b> by default. The index data type is long.	<p>Line number (offset), which is used to sort logs.</p> <p>Non-high-precision logs are generated based on the value of <b>collectTime</b>. The default value is <b>collectTime * 1000000 + 1</b>. For high-precision logs, the value is the nanosecond value reported by users.</p> <p>Example: "<code>lineNum</code>":"1681896081333991900"</p>
<code>category</code>	String	Index setting: After indexing is enabled, a field index is created for <b>category</b> by default. The index data type is string, and the delimiters are empty. Enter <b>category</b> : <i>xxx</i> during the query.	<p>Log type, indicating the source of the log.</p> <p>Example: The field value of logs collected by ICAgent is <b>LTS</b>, and that of logs reported by a cloud service such as DCS is <b>DCS</b>.</p>

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

Field	Data Format	Index and Statistics Settings	Description
serviceID	String	Index setting: After indexing is enabled, a field index is created for <b>serviceID</b> by default. The index data type is string, and the delimiters are empty. Enter <b>serviceID: xxx</b> during the query.	Workload ID in the Kubernetes scenario. Example: <b>"serviceID":"cf5b453xxxad61d4c483b50da3fad5ad"</b>
podName	String	Index setting: After indexing is enabled, a field index is created for <b>podName</b> by default. The index data type is string, and the delimiters are empty. Enter <b>podName: xxx</b> during the query.	Pod name in the Kubernetes scenario. Example: <b>"podName":"alertmanager-alertmanager-0"</b>
podIp	String	Index setting: After indexing is enabled, a field index is created for <b>podIp</b> by default. The index data type is string, and the delimiters are empty. Enter <b>podIp: xxx</b> during the query.	Pod IP address in the Kubernetes scenario. Example: <b>"podIp":"10.0.0.145"</b>
containerName	String	Index setting: After indexing is enabled, a field index is created for <b>containerName</b> by default. The index data type is string, and the delimiters are empty. Enter <b>containerName: xxx</b> during the query.	Container name used in the Kubernetes scenario. Example: <b>"containerName":"config-reloader"</b>

Field	Data Format	Index and Statistics Settings	Description
hostName	String	Index setting: After this function is enabled, a field index is created for <b>hostName</b> by default. The index data type is string, and the delimiters are empty. Enter <code>hostName: xxx</code> during the query.	Indicates the host name where ICAgent resides.  Such as <code>"hostName": "epstest-xx518"</code> in the example.
hostId	String	Index setting: After this function is enabled, a field index is created for <b>hostId</b> by default. The index data type is string, and the delimiters are empty. Enter <code>hostId: xxx</code> during the query.	Indicates the host ID where ICAgent resides. The ID is generated by ICAgent. Such as <code>"hostId": "318c02fe-xxxx-4c91-b5bb-6923513b6c34"</code> in the example.
hostIP	String	Index setting: After this function is enabled, a field index is created for <b>hostIP</b> by default. The index data type is string, and the delimiters are empty. Enter <code>hostIP: xxx</code> during the query.	Host IP address where the log collector resides (applicable to IPv4 scenario)  Such as <code>"hostIP": "192.168.0.31"</code> in the example.
hostIPv6	String	Index setting: After this function is enabled, a field index is created for <b>hostIPv6</b> by default. The index data type is string, and the delimiters are empty. Enter <code>hostIPv6: xxx</code> during the query.	Host IP address where the log collector resides (applicable to IPv6 scenario)  Such as <code>"hostIPv6": ""</code> in the example.



Field	Data Format	Index and Statistics Settings	Description
pathFile	String	Index setting: After this function is enabled, a field index is created for <b>pathFile</b> by default. The index data type is string, and the delimiters are empty. Enter pathFile: xxx during the query.	File path is the path of the collected log file.  Such as "pathFile": "stdout.log" in the example.
content	String	Index setting: After <b>Index Whole Text</b> is enabled, the delimiters defined in <b>Index Whole Text</b> are used to delimit the value of the <b>content</b> field. The <b>content</b> field cannot be configured in the field index.	Original log content. Example: <b>"content": "level=error ts=2023-04-19T09:21:21.333895559Z"</b>
__receive_time__	Integer, Unix timestamp (ms)	Index setting: After this function is enabled, a field index is created for <b>__receive_time__</b> by default. The index data type is long.	Time when a log is reported to the server, which is same as the time when the LTS collector receives the log.
__client_time__	Integer, Unix timestamp (ms)	Index setting: After indexing is enabled, a field index is created for <b>__client_time__</b> by default. The index data type is long.	Time when the client reports a device log.

Field	Data Format	Index and Statistics Settings	Description
_content_parse_fail_	String	Index setting: After indexing is enabled, a field index is created for <b>_content_parse_fail_</b> by default. The index data type is string, and the default delimiter is used. Enter <b>_content_parse_fail_ : xxx</b> during the query.	Content of the log that fails to be parsed.
__time	Integer, Unix timestamp (ms)	The <b>__time</b> field cannot be configured in the field index.	N/A
logContent	String	The <b>logContent</b> field cannot be configured in the field index.	N/A
logContentSize	Integer	The <b>logContentSize</b> field cannot be configured in the field index.	N/A
logIndexSize	Integer	The <b>logIndexSize</b> field cannot be configured in the field index.	N/A
groupName	String	The <b>groupName</b> field cannot be configured in the field index.	N/A
logStream	String	The <b>logStream</b> field cannot be configured in the field index.	N/A

## ASCII Table

Table 5-10 ASCII table

AS CII Val ue	Character	ASC II Val ue	Character	AS CII Val ue	Character	AS CII Val ue	Character
0	NUL (Null)	32	Space	64	@	96	`
1	SOH (Start of heading)	33	!	65	A	97	a
2	STX (Start of text)	34	"	66	B	98	b
3	ETX (End of text)	35	#	67	C	99	c
4	EOT (End of transmission)	36	\$	68	D	100	d
5	ENQ (Enquiry)	37	%	69	E	101	e
6	ACK (Acknowledge)	38	&	70	F	102	f
7	BEL (Bell)	39	'	71	G	103	g
8	BS (Backspace)	40	(	72	H	104	h
9	HT (Horizontal tab)	41	)	73	I	105	i
10	LF (Line feed)	42	*	74	J	106	j
11	VT (Vertical tab)	43	+	75	K	107	k
12	FF (Form feed)	44	,	76	L	108	l
13	CR (Carriage return)	45	-	77	M	109	m
14	SO (Shift out)	46	.	78	N	110	n
15	SI (Shift in)	47	/	79	O	111	o
16	DLE (Data link escape)	48	0	80	P	112	p

AS CII Value	Character	ASC II Value	Character	AS CII Value	Character	AS CII Value	Character
17	DC1 (Device control 1)	49	1	81	Q	113	q
18	DC2 (Device control 2)	50	2	82	R	114	r
19	DC3 (Device control 3)	51	3	83	S	115	s
20	DC4 (Device control 4)	52	4	84	T	116	t
21	NAK (Negative acknowledge)	53	5	85	U	117	u
22	SYN (Synchronous idle)	54	6	86	V	118	v
23	ETB (End of transmission block)	55	7	87	W	119	w
24	CAN (Cancel)	56	8	88	X	120	x
25	EM (End of medium)	57	9	89	Y	121	y
26	SUB (Substitute)	58	:	90	Z	122	z
27	ESC (Escape)	59	;	91	[	123	{
28	FS (File separator)	60	<	92	\	124	
29	GS (Group separator)	61	=	93	]	125	}
30	RS (Record separator)	62	>	94	^	126	~
31	US (Unit separator)	63	?	95	_	127	DEL (Delete)

## 5.4 Searching Logs

## 5.4.1 Accessing the Log Search Page

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

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

### Searching Logs

**Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.

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

**Step 3** You can select a time range above the search box to view log data accordingly.

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

#### NOTE

- **From now:** queries log data generated in a time range that ends with the current time, such as the previous 1, 5, or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from now, the charts on the dashboard display the log data that is generated from 18:20:31 to 19:20:31.
- **From last:** queries log data generated in a time range that ends with the current time, such as the previous 1 or 15 minutes. For example, if the current time is 19:20:31 and **1 hour** is selected as the relative time from last, the charts on the dashboard display the log data that is generated from 18:00:00 to 19:00:00.
- **Specified:** queries log data that is generated in a specified time range. The time range can be up to three months for common users and six months for whitelisted users. If necessary, [submit a service ticket](#) to extend the time range to six months.

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

- In the search area, click the search box, enter a keyword or select a field or keyword from the drop-down list, and click **Search**.

#### NOTE

- System reserved fields include **appName**, **category**, **clusterId**, **clusterName**, and **collectTime**. By default, the fields are displayed in simplified mode, and **hostIP**, **hostName**, and **pathFile** are displayed at the beginning. For more system reserved fields, see [Setting Indexes](#).
- The structured fields are displayed in **key:value** format.
- If there is too much content in the log search box, the content can be automatically wrapped and displayed in multiple lines.
- The height of the search box can be fixed.
- 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**.
- Click a field for which quick analysis has been enabled to add it to the search box. For details about how to enable quick analysis, see [Creating an LTS Quick Analysis Task](#).

 **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.

**Step 5** On the **Log Search** tab page, perform the following operations. For more operations, see [Common Log Search Operations](#).

1. Under **Log Statistics**, view the bar chart showing the log quantity in different time segments. The scale of the log quantity is displayed on the left.

 **NOTE**


If the embedding function is used, you can collapse or expand the log quantity statistics chart. For parameters of embedding LTS, see [LTS Address](#).

2. In the log content area, hover the cursor over a field and click the log content in blue. You can search for logs by copying, adding to query, adding to query (interactive mode), creating query, excluding from query (interactive mode), hiding, and excluding from query.
3. In the log content area, you can select a list or raw log to display its log content.

 **NOTE**

The log highlighting mechanism works as follows: Once a log meets the search criteria, the system identifies the log's strings that match these criteria and applies highlight tags to the matching sections, making them visibly highlighted on the page. However, when the query criteria are complex, particularly involving OR relationships, content that does not actually match the criteria may also be highlighted on the page.

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

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

----End

## Interactive Mode

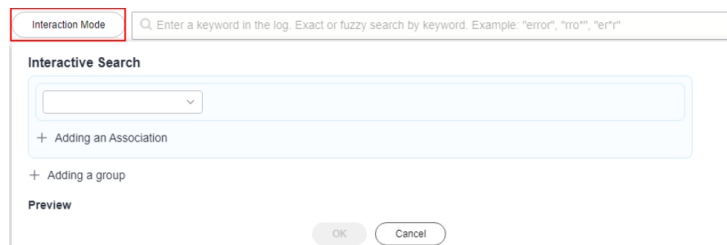
Before using the interactive mode function, ensure that logs are properly reported and structured, and indexing have been configured. For details, see [Setting Cloud Structuring Parsing](#) and [Setting Indexes](#).

Interactive search generates simple search statements, allowing you to set search criteria and specify query filter rules on the LTS console to filter log records. For

more functions or nested queries, enter SQL statements manually. For details, see [SQL Analysis Syntax](#).

**Step 1** Click **Interaction Mode** in front of the search box to access the interactive search page.

**Figure 5-4** Interactive Mode



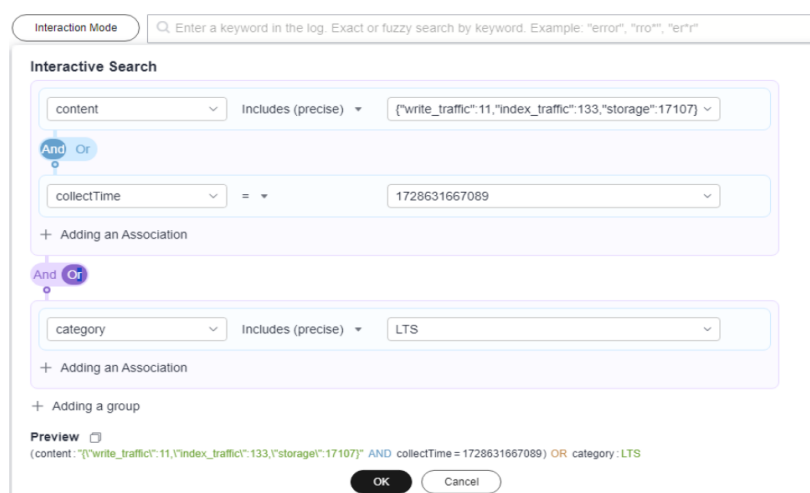
**Step 2** Select the log search field and criteria from the drop-down list. The corresponding values of the field will be displayed in the search box. Add associations or groups to customize your search mode.

- The drop-down list displays index fields, structured fields, and **system reserved fields**.
- **AND** indicates that all conditions must be met.
- **OR** indicates that only one of the conditions needs to be met.

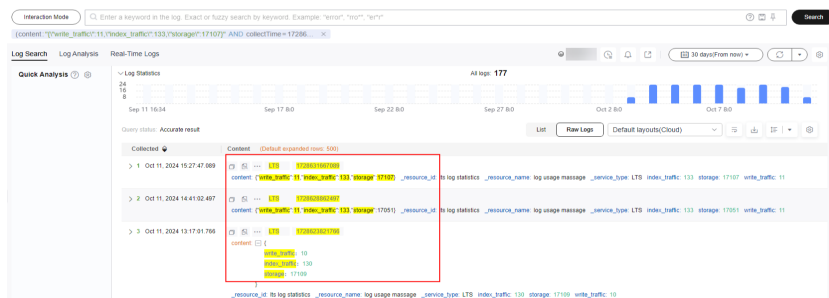
For example, you can select fields such as **content**, **collectTime**, and **category** and set different conditions. Then you can preview the search statement at any time and modify the search conditions with ease.

(The following figure is for reference only.)

(content:"{"write\_traffic":11,"index\_traffic":133,"storage":17107}" AND collectTime=1728631667089) OR category:LTS



**Step 3** After setting the parameters, click **OK**. LTS searches for logs based on your search statement and displays the search results on the **Log Search** tab page. (The following figure is for reference only.)










----End








## Common Log Search Operations







In the log content display area, you can share and download logs, and view context. For details, see [Table 5-11](#).

**Table 5-11** Common operations

Operation	Description
Creating quick search	Click  to create a quick search.
Viewing dashboards	Click  to view the dashboards you created.
Adding alarm rules	Click  and <a href="#">create an alarm rule</a> on the displayed page.
Sharing logs	Click  to copy the link of the current log search page to share the logs that you have searched.
Refreshing logs	You can click  to refresh logs in two modes: manual refresh and automatic refresh. <ul style="list-style-type: none"> <li>Manual refresh: Select <b>Refresh Now</b> from the drop-down list.</li> <li>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.</li> </ul>
Copying logs	Click  to copy the log content.
Viewing context of a log	Click  to view the log context. <b>NOTE</b> You can select <b>Simple View</b> to view the log context. You can also download the context.




Operation	Description
More operations	<p>Click  to access the log details page of the time segment and view more log information.</p> <ul style="list-style-type: none"> <li>On the <b>Extended Fields</b> tab page, view field names and values. You can also click buttons in the <b>Operation</b> column to add a field to or exclude a field from a query, set whether a field exists or does not exist, or set whether a field is hidden.</li> <li>On the <b>JSON Format</b> tab page, view the JSON format of logs.</li> <li>On the <b>Context Logs</b> tab page, you can set the number of lines to be queried and filtered fields. You can also download logs and enable the summary mode.</li> </ul>
Unfold/Fold	<p>Click  to display all the log content. Click  to fold the log content.</p> <p><b>NOTE</b> <b>Unfold</b> is enabled by default.</p>
Downloading logs	<p>This function is available only to whitelisted users. To enable it, <a href="#">submit a service ticket</a>.</p> <p>Click . On the displayed page, click <b>Direct Download and Transfer and Download</b> (this option is available only after one-off transfer is enabled).</p> <ul style="list-style-type: none"> <li><b>Direct Download:</b> Download log files to the local PC. Up to 20 million logs can be downloaded at a time for a whitelisted user. A non-whitelisted user can download up to 5,000 logs at a time. Select <b>.csv</b> or <b>.txt</b> from the drop-down list and click <b>Download</b> to export logs to the local PC.</li> <li><b>Transfer and Download</b> (available only to whitelisted users): Download log files through OBS transfer tasks. Up to 20 million logs can be downloaded at a time. Click <b>Transfer</b> to access the <b>Configure Log Transfer</b> page. For details, see <a href="#">Transferring Logs to OBS</a>.</li> <li>Hover your cursor over  and click <b>View Download History</b>. On the displayed page, view, download, and delete log download records.</li> </ul>
Hiding/Expanding all	<p>Click  to set the number of lines displayed in the log content. Click  to hide the log content.</p> <p><b>NOTE</b> By default, logs are not collapsed, and two lines of logs are shown after collapsing. You can display up to six lines.</p>

Operation	Description
JSON	<p>Move the cursor over , click <b>JSON</b>, and set JSON formatting.</p> <p><b>NOTE</b> Formatting is enabled by default. The default number of expanded levels is 2. If a log contains multiple backslashes, the first backslash will be lost when the log is displayed in JSON format because it will be processed as an escape character during JSON parsing.</p> <ul style="list-style-type: none"> <li>• Formatting enabled: Set the default number of expanded levels. Maximum value: <b>10</b>.</li> <li>• Formatting disabled: JSON logs will not be formatted for display.</li> </ul>
Collapse configuration	<p>Move the cursor over , click <b>Log Collapse</b>, and set the maximum characters to display in a log.</p> <p>If the number of characters in a log exceeds the maximum, the extra characters will be hidden. Click <b>Expand</b> to view all.</p> <p><b>NOTE</b> Logs are collapsed by default, with a default character limit of 400.</p>
Log time display	<p>Move the cursor over  and click <b>Log time display</b>. On the page that is displayed, set whether to display milliseconds and whether to display the time zone.</p> <p><b>NOTE</b> By default, the function of displaying milliseconds is enabled.</p>
Virtual Scrolling	<p>Move the cursor over  and click <b>Virtual Scrolling</b>. On the page that is displayed, set whether to enable virtual scrolling and enter the buffer size.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Virtual scrolling eliminates or minimizes frame and page freezing for better user experience.</li> <li>• Data is re-rendered during the process. This may affect smoothness.</li> <li>• The buffer size determines the amount of data that can be loaded simultaneously. The larger the buffer, the more data loaded simultaneously, but the worse the scrolling performance.</li> </ul>
Invisible fields (  )	<p>This list displays the invisible fields configured in the layout settings.</p> <ul style="list-style-type: none"> <li>• The  button is unavailable for log streams without layout settings configured.</li> <li>• If the log content is <b>CONFIG_FILE</b> and layout settings are not configured, the default invisible fields include <b>appName</b>, <b>clusterId</b>, <b>clusterName</b>, <b>containerName</b>, <b>hostIPv6</b>, <b>NameSpace</b>, <b>podName</b>, and <b>serviceID</b>.</li> </ul>

## Cross-stream Search (Available to Whitelisted Users)

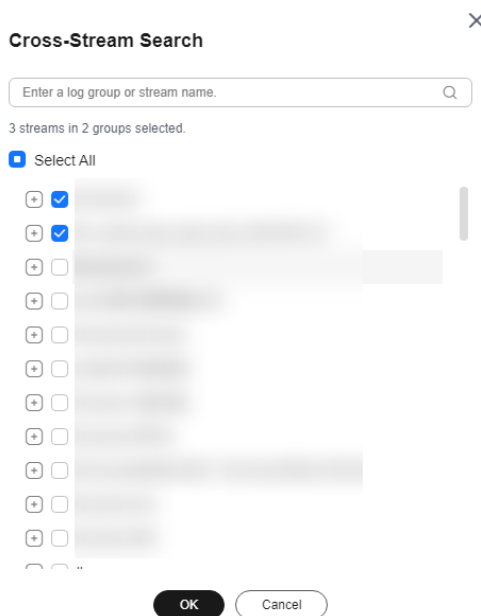
Currently, this function is available only to whitelisted users. To enable it, [submit a service ticket](#).

On the log stream details page, you can search for logs across log streams. This means you can search for logs in other log streams without exiting the current log search page.

**Step 1** On the log stream details page, click  .




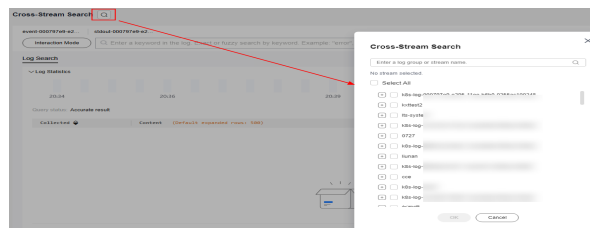
**Step 2** On the displayed page, select one or more target log streams.



**Step 3** Click **OK**.

**Step 4** On the target log stream details page displayed, search for logs by referring to [Using LTS Search Syntax](#).

To change the log stream, click  next to **Cross-Stream Search** in the upper left corner and select another log stream.



**Step 5** After the search is complete, click **Exit** in the upper right corner to return to the current log stream search page.

- If the target log streams for cross-stream search use different delimiters, the log keywords in different streams will be highlighted differently.
- Up to 50 log streams can be searched at a time.
- Only raw logs can be searched. SQL statements cannot be used for statistical analysis.
- You can select log streams across log groups, but not across regions.
- If you select multiple log streams with different index configurations for cross-stream search, for example, indexing **Key1** in stream A but not in stream B, searches for **Key1:xxx** will only return logs from stream A. Address the issue according to the error message and retry the log search.

----End

## 5.4.2 Using LTS Search Syntax

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

To quickly understand and use the search syntax, you are advised to learn [Search Modes](#), [Phrase Search](#), [Operators](#), and [Search Statement Examples](#).

### 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` and spaces.
- 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**.
- For details about how to handle common log search syntax issues and errors, see [How Do I Solve Log Search Issues?](#)

## Search Modes

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

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

**Table 5-12** Search modes

Search Mode	Description	Example
By full text	<p>LTS splits an entire log into multiple keywords when full-text index is set.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• <b>content</b> is a built-in field corresponding to the original log text. The search statement <b>GET</b> is equivalent to <b>content:GET</b>. By default, the original log content is matched.</li> <li>• By default, multiple keywords are connected through <b>AND</b>. The search statement <b>GET POST</b> is equivalent to <b>GET and POST</b>.</li> </ul>	<ul style="list-style-type: none"> <li>• GET POST</li> <li>• GET and POST</li> <li>• content:GET and content:POST</li> </ul> <p>The preceding search statements have the same function, indicating that logs containing both GET and POST are searched.</p>
By field	<p>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.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• The <b>value</b> parameter cannot be empty. You can use the <b>key: ""</b> statement to search for logs with empty field values.</li> <li>• When field search is used together with the <b>not</b> operator, logs that do not contain this field are matched.</li> </ul>	<ul style="list-style-type: none"> <li>• <b>request_time&gt;60 and request_method:po*</b> indicates that the system searches for logs in which the value of <b>request_time</b> is greater than 60 and the value of <b>request_method</b> starts with <b>po</b>.</li> <li>• <b>request_method: ""</b> indicates that logs in which the value of <b>request_method</b> is empty are searched.</li> <li>• <b>not request_method:GET</b> indicates that logs that do not contain the <b>request_method</b> field and whose <b>request_method</b> value is not <b>GET</b> are searched.</li> </ul>

Search Mode	Description	Example
By exact match	<p>Use exact words for search. LTS searches with word segmentation, which does not define the sequence of keywords.</p> <p><b>NOTE</b> If the search statement is <b>abc def</b>, all logs that contain both <b>abc</b> and <b>def</b> are matched, for example, logs <b>abc def</b> and <b>def abc</b>. To ensure the sequence of keywords, use <b>Phrase Search #"</b>abc def<b>".</b></p>	<ul style="list-style-type: none"> <li>● <b>GET POST</b> indicates that logs containing both <b>GET</b> and <b>POST</b> are searched.</li> <li>● <b>request_method:GET</b> indicates that logs in which the value of <b>request_method</b> contains <b>GET</b> are searched.</li> <li>● <b>#"/var/log"</b> indicates that logs containing phrase <b>/var/log</b> are searched.</li> </ul>
By fuzzy match	<p>Specify a keyword in the search statement and add a wildcard, that is, an asterisk (*) or a question mark (?), to the middle or end of the keyword. LTS searches all logs for 100 words that meet the search criteria and returns logs that contain the words. The more precise the specified word is, the more accurate the search results are.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>● The asterisk (*) indicates that multiple characters are matched, and the question mark (?) indicates that one character is matched.</li> <li>● When an asterisk (*) and a question mark (?) are used as delimiters, fuzzy search is not supported since the question mark is a default delimiter. To perform a fuzzy search, remove the question mark from delimiters.</li> <li>● Words cannot start with an asterisk (*) or a question mark (?).</li> <li>● Long and float data does not support fuzzy search using asterisks (*) or question marks (?).</li> <li>● If the fuzzy condition prefix is short and more than 100 words meet the criteria, the search results will be inaccurate.</li> </ul>	<ul style="list-style-type: none"> <li>● <b>GE*</b> indicates that the system searches for words starting with <b>GE</b> in all logs and returns logs containing these words.</li> <li>● <b>request_method:GE*</b> indicates that the system searches for <b>request_method</b> values starting with <b>GE</b> in all logs and returns logs containing these words.</li> </ul>

Search Mode	Description	Example
By scope	<p>The long and float data supports range search.</p> <ul style="list-style-type: none"> <li>Method 1: Use operators such as = (equal to) &gt; (greater than) &lt; (less than) operators to search for logs.</li> <li>Method 2: Use the in operator to search for logs. The open/closed interval can be modified.</li> </ul> <p><b>NOTE</b> The string fields do not support range query.</p>	<ul style="list-style-type: none"> <li>request_time&gt;=60 indicates that the system searches for logs whose request_time value is greater than or equal to 60.</li> <li>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.</li> </ul>
By phrase	<p>Phrase search is used to fully match target phrases in logs to ensure the sequence in which keywords appear.</p> <p><b>NOTE</b> Fuzzy search is not supported for phrase search.</p>	<p><b>#"abc def"</b> indicates that the system searches all logs for the logs that contain the target phrase abc def.</p>

- Delimiters

LTS splits the log content into multiple words based on delimiters. Default delimiters include `,";=()[]{}@&<>/:\|?\\n\t\r` and spaces.

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

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

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

- Keyword sequence

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

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

- Chinese search

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

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

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

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

- Invalid keyword

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

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

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

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

## Phrase Search

Phrase search precisely matches target phrases. For example, the search statement **#"abc def"** searches all logs containing both **abc** and **def** in that specific sequence, with **abc** preceding **def**. For details about the differences between phrase search and keyword search, see [Table 5-13](#).

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

**Table 5-13** Differences between two search modes

Search Mode	Description	Example
By phrase	Distinguishes the sequence of keywords and is used to accurately match target phrases, making the search result more accurate.	Assume that your log stream contains the following two raw logs: <ul style="list-style-type: none"> <li>• Raw log 1: <b>this service is lts</b></li> <li>• Raw log 2: <b>lts is service</b></li> </ul> If you search for <b>#"is lts"</b> or <b>#"lts is"</b> , each query matches one log.



Search Mode	Description	Example
By keyword	Does not distinguish the sequence of keywords. The keyword is matched based on the search logic.	<p>Assume that your log stream contains the following two raw logs:</p> <ul style="list-style-type: none"> <li>Raw log 1: <b>this service is lts</b></li> <li>Raw log 2: <b>lts is service</b></li> </ul> <p>If you search for <b>is lts</b> or <b>lts is</b>, each query matches two logs.</p>

The constraints are as follows:

- Fuzzy search cannot be used together with phrase search.  
The asterisk (\*) and question mark (?) in phrase search are regarded as common characters. Therefore, phrase search does not support fuzzy search and can be used to search for the asterisk (\*) and question mark (?) in logs.
- Phrase search does not support search by delimiter.  
For example, in the search statement **#"var/log"**, / is a delimiter. The search statement is equivalent to **#"var log"**, and is used to search for logs containing the target phrase **var log**. Similarly, search statements such as **#"var:log"** and **#"var;log"** are used to search for logs that contain the target phrase **var log**.
- Phrase search is recommended for search in Chinese.  
By default, unary word segmentation is used for Chinese characters. Each Chinese character is segmented separately. During the search, logs that contain each Chinese character in the search statement are matched, which is similar to fuzzy search. When more accurate results are required, phrase search is recommended.

## Operators

For details about operators supported by the search statements, see [Table 5-14](#).

### NOTE

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

**Table 5-14** Operators

Operator	Description	Example
and	<p>If there is no syntax keyword between multiple keywords, the <b>and</b> relationship is used by default.</p> <p><b>NOTE</b> When <b>and</b> is used as an operator, use a space before and after it. For example, <b>1 and 2</b> indicates that logs containing both <b>1</b> and <b>2</b> are searched, and <b>1and2</b> indicates that logs containing <b>1and2</b> are searched.</p>	<b>GET 200</b> is equivalent to <b>GET and 200</b> .
AND	<b>AND</b> operator, equivalent to <b>and</b> .	GET AND 200
&&	<p><b>AND</b> operator.</p> <p><b>NOTE</b> When <b>&amp;&amp;</b> is used as an operator, spaces are not necessary. For example, <b>1 &amp;&amp; 2</b> is equivalent to <b>1&amp;&amp;2</b>, indicating that logs containing both <b>1</b> and <b>2</b> are searched.</p>	1&&2
or	<p><b>or</b> operator.</p> <p><b>NOTE</b> When <b>or</b> is used as an operator, use a space before and after it.</p>	request_method:GET or status:200
OR	<b>OR</b> operator, equivalent to <b>or</b> .	request_method:GET OR status:200
	<b>OR</b> operator. When <b>  </b> is used as an operator, spaces are not necessary.	request_method:GET    status:200
not	<p><b>not</b> operator.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>When <b>not</b> is used as an operator, use a space before and after it.</li> <li>When field search is used together with the not operator, logs that do not contain this field are matched.</li> </ul>	request_method:GET not status:200, not status:200
( )	Specifies fields that should be matched with higher priority.	(request_method:GET or request_method:POST) and status:200

Operator	Description	Example
:	Searches for a specified field (key:value). <b>NOTE</b> Use double quotation marks (") to enclose a field name (key) or value that contains reserved characters, such as spaces and colons (:). Examples: <ul style="list-style-type: none"> <li>• "request method":GET</li> <li>• message:"This is a log"</li> <li>• time:"09:00:00"</li> <li>• ipv6:"2024:AC8:2ac::d09"</li> </ul>	request_method:GET
""	Encloses a syntax keyword to convert it into common characters. For example, "and" means searching for logs that contain this word. The word <b>and</b> here is not an operator.	request_method:"GET"
\	Escapes double quotation marks ("). The escaped quotation marks indicate the symbol itself.	To search for <b>instance_id:nginx"01"</b> , use <b>instance_id:nginx\"01\"</b> .
*	An asterisk is a wildcard that matches zero, single, or multiple characters. <b>NOTE</b> Put * in the middle or at the end of a keyword.	request_method:P*T
?	A question mark matches a single character. <b>NOTE</b> Put ? in the middle or at the end of a keyword.	<b>request_method:P?T</b> can match <b>PUT</b> but cannot match <b>POST</b> .
>	Searches logs in which the value of a field is greater than a specified value.	request_time>100
>=	Searches logs in which the value of a field is greater than or equal to a specified value.	request_time>=100
<	Searches logs in which the value of a field is less than a specified value.	request_time<100
<=	Searches logs in which the value of a field is less than or equal to a specified value.	request_time<=100

Operator	Description	Example
=	Searches logs in which the value of a field is equal to a specified value, applying only to float or long fields. For fields of this type, the equal sign (=) and colon (:) have the same function.	<b>request_time=100</b> is equivalent to <b>request_time:100</b> .
in	Searches for logs whose field values are in a specified range. Brackets indicate a closed interval, and parentheses indicate an open interval. Numbers are separated with spaces. <b>NOTE</b> Enter <b>in</b> in lowercase. When it is used as an operator, use a space before and after it.	<ul style="list-style-type: none"> <li>request_time in [100 200]</li> <li>request_time in (100 200]</li> </ul>
#""	Searches for logs that contain the target phrase, ensuring the sequence of keywords. <b>NOTE</b> The asterisk (*) and question mark (?) in phrase search are regarded as common characters. Therefore, phrase search does not support fuzzy search and can be used to search for the asterisk (*) and question mark (?) in logs.	request_method:#"GET POST"

## Search Statement Examples

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

**Figure 5-5** Log sample

```
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
content: {
 request_method: POST
 request_uri: /authui/login
 request_time: 56
 request_length: 3718
 status: 200
 x-language: zh-cn
 date: Mon, 17 Apr 2023 00:33:48 GMT
 content-type: application/json
 content-encoding: gzip
 scheme: https
 sec-ch-ua-mobile: ?0
 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/113.0.0.0 Safari/537.36
 week: 20230417
}
content-encoding: gzip
content-type: application/json
date: Mon, 17 Apr 2023 00:33:48 GMT
request_length: 3718
request_method: POST
request_time: 56
request_uri: /authui/login
scheme: https
sec-ch-ua-mobile: ?0
status: 200
week: 20230417
x-language: zh-cn
```

**Table 5-15** Search statement examples

Search Requirement	Search Statement
Logs of POST requests whose status code is 200	request_method:POST and status=200
Logs of successful GET or POST requests (status codes 200 to 299)	(request_method:POST or request_method:GET) and status in [200 299]
Logs of failed GET or POST requests	(request_method:POST or request_method:GET) not status in [200 299]
Logs of non-GET requests	not request_method:GET
Logs of successful GET request and request time is less than 60 seconds	request_method:GET and status in [200 299] not request_time>=60
Logs whose request time is 60 seconds.	<ul style="list-style-type: none"> <li>request_time:60</li> <li>request_time=60</li> </ul>
Logs of requests whose time is greater than or equal to 60 seconds and less than 200 seconds	<ul style="list-style-type: none"> <li>request_time&gt;=60 and request_time&lt;200</li> <li>request_time in [60 200)</li> </ul>
Logs that contain and	content:"and" <b>NOTE</b> Double quotation marks are used to enclose <b>and</b> . In this case, <b>and</b> is a common string, not an operator.

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

For more complex search examples, see [Table 5-16](#).

**Table 5-16** Fuzzy search

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

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

- If this parameter is left blank, the value of this field is considered as a whole. In this case, when you use **User-Agent:Chrome** to search for logs, no log can be found.
- When the delimiter is set to `, "" ; = ( ) [ ] { } ? @ & < > / : \ n \ t \ r`, the value of this field is split into **Mozilla, 5.0, Windows, NT, 10.0, Win64, x64, AppleWebKit, 537.36, KHTML, like, Gecko, Chrome, 113.0.0.0, Safari, and 537.36**.

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

**Table 5-17** Delimiter-based search

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

### 5.4.3 Creating an LTS Quick Analysis Task

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

 **NOTE**

- Supports analysis on first 100,000 logs.  
The purpose of quick analysis is to quickly return the distribution and change trend of field values. It does not analyze all data, but only samples.
- Logs can be filtered by query time and criteria for analysis.  
Quick analysis is to analyze the logs queried by query statements. When the number of queried logs is 0, no result is displayed for quick analysis.
- Quick analysis can be used to generate query statements.  
You can click an analysis result to automatically generate a query statement, query logs, and generate a new quick analysis.
- The maximum length of a field for quick analysis is 2 KB.
- The distribution statistics in quick analysis field area displays the first 100 records.
- If quick analysis is not enabled within the analysis time range, a field does not exist, or a field value is null, the analysis result of the field is **null**.
  - When you click **null** to add a string field to the search box, *Field: "null"OR NOT Field: \** will be displayed.
  - When you click **null** to add a float or long field to the search box, **NOT Field: \*** will be displayed.
  - If quick analysis is not enabled, the column-store data used for analysis is not stored, and the analysis result is **null**. In this case, log search is meaningless and no log may be matched.

## Prerequisites


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

## Creating a Quick Analysis Task

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





**Step 1** Log in to the **LTS console**. The **Log Management** page is displayed by default.

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

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

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

### NOTE

-  indicates a field of the **string** type.
-  indicates a field of the **float** type.
-  indicates a field of the **long** type.
- The maximum length of a field for quick analysis is 2000 bytes.
- The quick analysis field area displays the first 100 records.
- The number of sampled fields are displayed.
- Click  to view the chart generated. For fields of the string type, the field distribution and intelligent aggregation timeline can be displayed. For fields of the long and float type, only the intelligent aggregation timeline can be displayed. Click the chart to view details.
- Click the field distribution or intelligent aggregation time line, the visualization page is displayed and the corresponding SQL query statement is generated. In this way, the distribution and change trend of field values are displayed more intuitively. For details, see [Analyzing Logs in LTS](#).

----End

## Secondary Analysis

The quick analysis supports secondary analysis of **float** and **long** fields.

Click **Max**, **Min**, **Avg**, and **Sum** under the target field to quickly collect the maximum, minimum, average, and sum values.

### 5.4.4 Saving Conditions for Quick Search


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



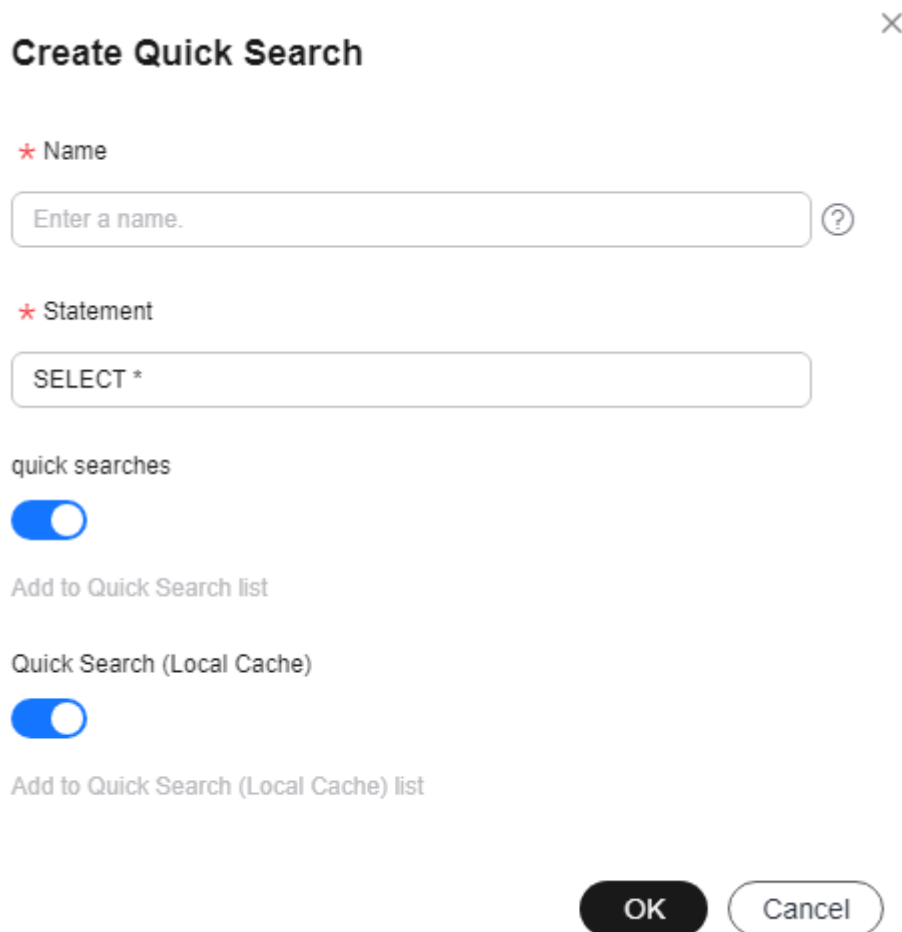
## Saving Conditions for Quick Search

**Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.

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

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

**Figure 5-6** Creating quick search



**Create Quick Search** ×

★ Name

Enter a name. ?

★ Statement

SELECT \*

quick searches

Add to Quick Search list

Quick Search (Local Cache)

Add to Quick Search (Local Cache) list

**OK** **Cancel**

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


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

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

----End

## Viewing Context of a Log

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

- Step 1** On the **Log Search** tab page of the log details page, click  to view the context. Details of several logs generated before and after the log are displayed.
- Step 2** On the displayed page, check the log context. For details, see [Table 5-18](#).

**Table 5-18** Introduction to log context viewing

Feature	Description
Search Rows	Select the number of lines of logs to be queried as required.
Highlighting	Enter a string to be highlighted and press <b>Enter</b> .
Filter	Enter a string to be filtered and press <b>Enter</b> . When both <b>Highlighting</b> and <b>Filter</b> are configured, the filtered string can also be highlighted.
Fields	The default field for viewing log context is <b>content</b> . Click <b>Fields</b> to view the context of other fields.
Prev	View half the number of <b>Search Rows</b> leading to the current position. For example, if <b>Search Rows</b> is set to 100 and you click <b>Prev</b> , 50 rows prior to the current position are displayed. In this case, the current line number is <b>-50</b> . If you click <b>Prev</b> again, the line number will become <b>-100, -150, -200</b> , and so on.
Current	Current log position. When <b>Prev</b> or <b>Update</b> is set, you can click <b>Current</b> to return to the position where the context starts (when the line number is 0).
Update	View half the number of <b>Search Rows</b> following the current position. For example, if <b>Search Rows</b> is set to 100 and you click <b>Update</b> , 50 rows following the current position are displayed. In this case, the current line number is 50. If you click <b>Update</b> again, the line number will become <b>100, 150, 200</b> , and so on.
Summary Mode	<ul style="list-style-type: none"> <li>• If this mode is enabled, only the line number and content are displayed.</li> <li>• If this mode is disabled, log details are displayed.</li> </ul>
Download	Only content in the <b>content</b> field can be downloaded to the local PC.

----End

## 5.5 Viewing Real-Time Logs

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

- When real-time logs exceed 1 MB in size but are fewer than 2,000 in total, LTS clears the initial 500 KB of logs, retaining only the most recent 500 KB.
- When real-time logs do not exceed 1 MB in size but exceed 2,000 in number, LTS clears the first 1,000 logs, retaining the latest 1,000.

### NOTE

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.

### Prerequisites

- You have created log groups and log streams.
- You have performed operations provided in [Installing ICAgent \(Intra-Region Hosts\)](#).
- You have configured log collection rules.

### Viewing Real-Time Logs

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

**Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.

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

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

### NOTE

Filter host and K8s logs by source.

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

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

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

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

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

----End

## 5.6 Analyzing Logs in LTS

After you structure logs, wait 1 to 2 minutes and then you can query and analyze the structured logs using SQL statements and visualize the query results.

### NOTE

Currently, this function is available to all users in regions CN South-Guangzhou, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN-Hong Kong, CN Southwest-Guiyang1, AP-Singapore, and CN North-Beijing1. It is also available to whitelisted users in regions CN South-Shenzhen, AP-Bangkok, ME-Riyadh, and AP-Jakarta.

### Prerequisites

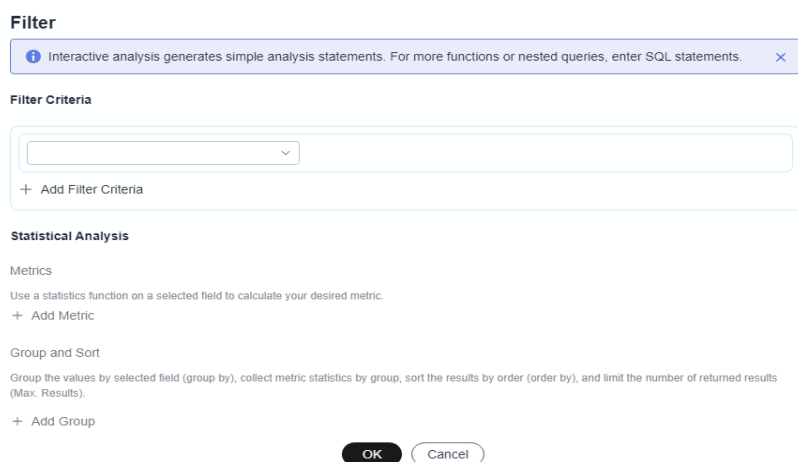
- Logs have been collected.
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

### NOTE

If a structured field shares a name with one of the reserved fields for SQL such as **time**, **select**, and **where**, or its name contains hyphens (-), underscores (\_), and periods (.), you need to double-quote the field during SQL query.

### Analyzing Logs

- Step 1** Log in to the [LTS console](#). The **Log Management** page is displayed by default.
- Step 2** Click the target log group or stream. The log stream details page is displayed.
- Step 3** Click the **Log Analysis** tab.
- Step 4** This tab page provides interactive analysis. You can use simple analysis statements to query visualized data and configure visualized charts. You can also set filters, add metrics and groups, and enable sorting for data analysis.



The screenshot shows a 'Filter' dialog box with the following sections:

- Filter**: A header with a blue information icon and a close button. Below it is a text box containing the message: "Interactive analysis generates simple analysis statements. For more functions or nested queries, enter SQL statements."
- Filter Criteria**: A section with a dropdown menu and a "+ Add Filter Criteria" button.
- Statistical Analysis**: A section with a "Metrics" sub-section. It includes a text box: "Use a statistics function on a selected field to calculate your desired metric." and a "+ Add Metric" button.
- Group and Sort**: A section with a text box: "Group the values by selected field (group by), collect metric statistics by group, sort the results by order (order by), and limit the number of returned results (Max. Results)." and a "+ Add Group" button.


At the bottom of the dialog are "OK" and "Cancel" buttons.

**Step 5** Select a time range, enter a SQL statement by referring to [SQL Analysis Syntax](#), and click **Search**. The search results will be displayed in various charts in the lower part.

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

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

 **NOTE**

- SQL query constraints are as follows:
  1. A maximum of 100,000 records can be returned for each query.
  2. If there are more than 100,000 aggregation results, they may be inaccurate.
- There are some constraints when you use a string in a WHERE clause.
  1. The value should be enclosed by single quotation marks (') for exact match, and by single or double quotation marks (") for fuzzy search. If the key shares a name with one of the SQL reserved fields, enclose the key with double quotation marks (").
  2. Recommended formats: WHERE "Key"= 'Value' and WHERE "Key" like ' %Value%'
- There are no constraints on **float** and **long** types in WHERE clauses. However, you are still advised to use the formats described above to avoid query exceptions caused by keyword conflicts.
- You can drag the log search box to adjust its height.
- After entering the search syntax, you can click  to set the formatting SQL statement and reverse formatting SQL statement to optimize the search statement and improve the search efficiency.

**Step 6** If the number of logs generated within the specified time range exceeds 1 billion, iterative query is triggered so you can view all logs in multiple queries. The message **Query status: Results are accurate** is displayed.

Query status: Results are accurate.

**Step 7** Select a chart to present the query result. For details, see [Visualizing Logs in Statistical Charts](#).


**Step 8** You can perform the following operations on the query result:

- Click **Create**. In the displayed **Create Chart** dialog box, set **Chart Name** and enable **Add to Dashboard** as required, and click **OK** to save the visual chart.
- Click **Save**. In the displayed **Save Chart** dialog box, set **Chart Name** and enable **Add to Dashboard** as required, and click **OK** to save the visual chart. Select a chart and click **Save**, to modify the chart.

- Click **Save As**. In the displayed dialog box, set **Chart Name** and enable **Add to Dashboard** as required, and click **OK** to copy the existing visual chart.

 **NOTE**

You must save a chart before saving it as a visual chart.

- Click **Download** to download the visual data of the current SQL query result. The file is in .csv format.
- Click . In the displayed **Create Alarm Rule** dialog box, configure **SQL alarm rules** for the selected visual chart.

 **NOTE**

You can create an alarm rule only after saving the chart.

- Click **Show Chart** to expand the visual charts of the current log stream. Click **Show Chart** again to collapse the visual charts of the current log stream.

----End

## 5.7 SQL Analysis Syntax

### 5.7.1 Overview

Structured Query Language (SQL) is a programming language used to control database access and manage data in databases. LTS SQL provides statements for querying structured data in log streams. In this document, SQL refers to LTS SQL.

SQL consists of commands and functions that are used to manage databases and database objects. When using this language, comply with the rules for using expressions and texts. In addition to SQL syntax reference, this document also provides information about expressions, functions, and operators. Basic SQL query statements are as follows.

 **NOTE**

Currently, this function is available to all users in regions CN South-Guangzhou, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN-Hong Kong, CN Southwest-Guiyang1, AP-Singapore, and CN North-Beijing1. It is also available to whitelisted users in regions CN South-Shenzhen, AP-Bangkok, ME-Riyadh, and AP-Jakarta.

### Syntax

```
SELECT [ALL | DISTINCT] { * | exprs }
FROM { <subquery>}
[WHERE where_condition]
[GROUP BY [col_name_list]
[HAVING expr]
[ORDER BY expr [ASC | DESC], expr [ASC | DESC], ...]
[LIMIT limit]
[OFFSET offset]
```

### Data Types

**Table 5-19** lists the data types supported by SQL query. If the data type of the current field needs to be changed, it will be converted. For example, a field of the

**string** type is converted to the **long** type. After the data type of a field is converted, the default value is displayed. For example, if the data of the **string** type is converted to the data of the **long** type, the default value **0** of the **long** type is displayed. Similarly, when a null value is converted to a non-null value, the default value is used. For example, when a null value of the **string** type is converted to a number, the default value **0** is returned.

 **NOTE**

In the SQL syntax, characters must be enclosed in single quotation marks ('). Fields or table names are not enclosed or are enclosed with double quotation marks ("). For example, 'msg' indicates the character string msg, and msg or "msg" indicates the structured msg field.

**Table 5-19** Data types supported in SQL queries

Native Data Type	Default Value	Description
STRING	""	Native <b>string</b> type
FLOAT	0.0	Native <b>float</b> type
LONG	0	Native <b>long</b> type

## Query Statements

**Table 5-20** SQL query statements

Statement	Description	Example
DISTINCT	Only distinct values are returned.	SELECT DISTINCT visitCount
FROM	Indicates the source data set of the queried data. It can be the structured data of the current log stream or a subset of this data. If FROM is not specified, the structured data of the current log stream is queried by default. If the data source to be queried is a subset, you need to compile a subquery statement.	SELECT visitCount
WHERE	Specifies the filter criteria. Arithmetic operators, relational operators, and logical operators are supported. You can enter the filtering condition in <b>where_condition</b> .	SELECT visitCount WHERE visitCount > 0

Statement	Description	Example
GROUP BY	Specifies the grouping field. Single-field grouping and multi-field grouping are supported. You can enter the structured field list in <b>col_name_list</b> .	SELECT host, count(*) AS pv WHERE visitCount > 0 GROUP BY host
HAVING	Used only with GROUP BY. This statement specifies the structured field used to filter the GROUP BY results.	SELECT host, count(*) AS pv GROUP BY host HAVING pv > 10
ORDER BY	Fields that follow must be used for GROUP BY. The query results of GROUP BY can be sorted by any structured field.	SELECT host, count(*) AS pv GROUP BY host ORDER BY pv
ASC/DESC	ASC (default) sorts from the lowest value to the highest value. DESC sorts from the highest value to the lowest value.	SELECT host, count(*) AS pv GROUP BY host ORDER BY pv DESC
LIMIT	Limits the number of structured logs returned in the query result. A maximum of 100,000 structured logs can be returned for each query. <b>NOTE</b> If the LIMIT statement is not used, the latest 100 records in the query result are returned by default.	SELECT host LIMIT 100

## Examples

**Table 5-21** Examples of common SQL query statements

Query Requirement	Query Statement
Standard query	SELECT "field" WHERE "field" = 'value'
Number of rows	SELECT count(*)
Column alias	SELECT count(*) AS "pv"
Deduplication	SELECT DISTINCT("field")
Pagination	SELECT "field" LIMIT 100
Sorting	SELECT "__time" ORDER BY "__time"
Grouping	SELECT "field" GROUP BY "field"



Query Requirement	Query Statement
Statistics by group	SELECT "field",count(*) GROUP BY "field"
Fuzzy search	SELECT "field" LIKE 'value%'
Sum	SELECT sum("field")
Maximum value	SELECT max("field")
Minimum value	SELECT min("field")
Average value	SELECT avg("field")
SQL nested subquery	SELECT sum(pv) FROM (SELECT "field",count(*) AS "pv" GROUP BY "field")
HAVING clause filtering	SELECT "field",count(*) AS "pv" GROUP BY "field" HAVING "pv" > 10
Query containing GET and POST requests	SELECT * WHERE "request_method" IN ('GET', 'POST')
Query without GET and POST requests	SELECT * WHERE "request_method" NOT IN ('GET', 'POST')
Logs of non-GET requests	SELECT * WHERE "request_method" != 'GET'
Logs of successful GET request with the 200 status code and request time is less than 60 seconds	SELECT * WHERE "request_method" = 'GET' AND "request_time" < 60
Logs of requests whose time is greater than or equal to 60 seconds and less than 200 seconds	SELECT * WHERE "request_time" >=60 and "request_time" < 200
Logs of GET or POST requests	SELECT * WHERE "request_method" = 'GET' OR "request_method" = 'POST'

The following reference statements contain all basic query syntax and are constructed based on structured logs of Elastic Load Balance (ELB).

```
SELECT url AS Url, host AS Host, failure_rate AS FailureRate,
CONCAT(CAST(access_count AS varchar), ' times') AS "All",
CONCAT(CAST(rsp_200_count AS varchar), ' times') AS "COUNT_200"
FROM (SELECT
CONCAT(host, CASE WHEN STRPOS(router_request_uri, '?') = 0 THEN router_request_uri ELSE
SUBSTR(router_request_uri, 1, 1) END) AS url,
host,count(1) AS access_count,
SUM(CASE WHEN status = 200 THEN 1 ELSE 0 END) AS "rsp_200_count",
(CASE WHEN COUNT(1) < 30 THEN 0 ELSE round(SUM(CASE WHEN status >= 400 THEN 1 ELSE 0 END) *
```

```
100.0 / COUNT(1, 2) END) AS failure_rate
WHERE host NOT IN ('monitor-new.olayc.cn')
GROUP BY host,router_request_uri
HAVING router_request_uri NOT IN ('/robots.txt', '/null', '/undefined')
)
ORDER BY FailureRate DESC
LIMIT 100
```

## 5.7.2 Aggregate Function

Aggregate functions collect statistics on specified columns of structured logs and return a single value. They are often used with the SELECT and GROUP BY clauses. [Table 5-22](#) lists the aggregate functions supported by LTS.

Pay attention to the following points when using aggregate functions:

- Aggregate functions can be used in the SELECT clause of any query. You can use the syntax such as AGG(expr) FILTER(WHERE whereExpr) to filter columns before aggregation. The aggregate function aggregates only the columns that meet the filter criteria.
- In the same SQL query statement, the result of the corresponding aggregate function varies according to the filter criteria.
- Only COUNT function can be used with DISTINCT function.
- Aggregation operations are not performed in a fixed order. When an SQL statement that contains multiple aggregate functions is executed for query, and the order for executing the functions affects the operation result, the results obtained from different queries may be inconsistent.
- If the data to be aggregated is of the **float** type, the aggregation results may be inconsistent if you perform the same query for multiple times. If you want to obtain the same result from executing the same query, you are advised to use the ROUND function.

### Syntax

```
SELECT COUNT(fieldname1)
```

## Aggregate Function Statements

**Table 5-22** Aggregate function statements

Statement	Description	Example
COUNT(*)	Counts the number of rows.	SELECT COUNT(*)
COUNT(DISTINCT expr)	Counts the number of rows of a field after deduplication. The field value can be a character string or number. The returned value is an estimated value (with a default 2.3% standard error).	SELECT COUNT(DISTINCT host)
SUM(expr)	Returns the sum of the numbers.	SELECT SUM(visitCount)

Statement	Description	Example
MIN(expr)	Returns the minimum number.	SELECT MIN(visitCount)
MAX(expr)	Returns the maximum number.	SELECT MAX(visitCount)
AVG(expr)	Returns the average value.	SELECT AVG(visitCount)
EARLIEST(expr)	The expression must be of the numeric type. The earliest value of <b>expr</b> , which is the first queried value, is returned.	SELECT EARLIEST(visitCount)
LATEST(expr)	The expression must be of the numeric type. The latest value of <b>expr</b> , which is the last queried value, is returned.	SELECT LATEST(visitCount)

### 5.7.3 Period-over-Period Functions

This section describes the basic syntax and examples of period-over-period functions.

#### compare Function

This function is used to compare the calculation result in the current period with that in a previous period (*n* seconds ago).

##### Syntax

- This syntax is used to compare the calculation result in the current period with that *n* seconds ago.  
`compare(x,n)`
- This syntax is used to compare the calculation result in the current period with that *n1*, *n2*, and *n3* seconds ago.  
`compare(x, n1, n2, n3...)`

##### Description

**Table 5-23** Parameters of the year-on-year function

Parameter	Description
x	Name of the target column. The value is of the <b>double</b> or <b>long</b> type.
n	Time window (in seconds). For example, <b>3600</b> means 1 hour, <b>86400</b> means 1 day, <b>604800</b> means 1 week, and <b>31622400</b> means 1 year.

##### Returned Data Type

JSON array. The format is [*Current calculation result, Calculation result  $n$  seconds ago, Ratio of the current calculation result to that  $n$  seconds ago*].

### Example

This example calculates the ratio of the number of visits in the same period of the current hour to that in the same period of the previous day.

1. Set the query and analysis time range to 1 hour (full hour), and run the following query and analysis statements: In the preceding command, **86400** indicates the current time minus **86400** seconds (one day).

```
SELECT
compare(PV, 86400)
FROM (SELECT count(*) AS PV)
```

2. Query and analysis results.

**Figure 5-7** Query and analysis results

EXPR\$0
[5994.0,6000.0,0.999]

### NOTE

- **5994.0** indicates the number of website visits in the current hour (for example, from 2021-01-02 00:00:00 to 2021-01-02 01:00:00).
  - **6000.0** indicates the number of website visits in the same period of the previous day, for example, from 2021-01-01 00:00:00 to 2021-01-01 01:00:00.
  - **0.999** indicates the ratio of the number of website visits in the current hour to that in the same period of the previous day.
3. Query and analysis results displayed in columns.

```
SELECT
diff[1] as "today",
diff[2] as "yesterday",
diff[3] as "ratio"
FROM(SELECT compare(pv, 86400) AS diff FROM (SELECT count(*) AS pv))
```

**Figure 5-8** Query and analysis results

today	yesterday	ratio
5993	6029	0.99402887

## ts\_compare Function

This function is used to compare the calculation result in the current period with that  $n$  seconds ago.

### NOTE

The `ts_compare` function must be grouped by time column (GROUP BY).

### Syntax

- This function is used to compare the calculation result in the current period with that  $n$  seconds ago.  
`ts_compare(x, n)`
- This function is used to compare the calculation result in the current period with that  $n1$ ,  $n2$ , and  $n3$  seconds ago.

ts\_compare(x, n1, n2, n3...)

### Description

**Table 5-24** Parameters of the period-over-period function

Parameter	Description
x	The value is of the <b>double</b> or <b>long</b> type.
n	Time window (in seconds). For example, <b>3600</b> (1 hour), <b>86400</b> (1 day), <b>604800</b> (1 week), and <b>31622400</b> (1 year).

### Returned Data Type

JSON array. The format is [*Current calculation result, Calculation result n seconds ago, Ratio of the current calculation result to that n seconds ago, UNIX timestamp n seconds ago*].

### Example

This example compares the number of website visits in the 3 hours of today with that in the 3 hours of the previous day.

Set the query and analysis time range to 3 hours of the current day and run the following statements: In the preceding command, **86400** indicates that the current time minus **86400** seconds (one day), and **date\_trunc('hour', \_\_time)** indicates that the **date\_trunc** function is used to truncate the input timestamp to the hour.

- Query and analysis statements

```
SELECT
 t_time,
 ts_compare(PV, 86400) AS data
FROM(
 SELECT
 date_trunc('hour', __time) AS t_time,
 count(*) AS PV
 GROUP BY
 t_time
 ORDER BY
 t_time
)
GROUP BY
 t_time
```

- Query and analysis results

t_time	data
2021-10-26T06:00:00.000Z	[159.0,224.0,0.7098214285714286,1.6351416E9]
2021-10-26T07:00:00.000Z	[100.0,148.0,0.6756756756756757,1.6351452E9]
2021-10-26T08:00:00.000Z	[100.0,100.0,1.0, 1.6016544E9, 1.6351488E9]

## 5.7.4 JSON Function

### Description

JSON functions are used to parse JSON objects or JSON arrays and extract values from them.

### Syntax

```
SELECT json_extract(Results, '$.[0].EndTime')
```

### JSON Function Statements

**Table 5-25** JSON function statements

Statement	Description	Example	Returned Value Type
json_extrac t	Extracts a set of JSON values (object or array) from a JSON object or JSON array.	json_extract(x, json_path)	Data of <b>string</b> type in JSON format
json_extrac t_scalar	Extracts a set of scalar values (string, integer, or Boolean) from a JSON object or JSON array. If the specified JSON path is not a scalar, null is returned.	json_extract_scal ar(x,json_path)	<b>varchar</b> type

### Examples

- **json\_extract function**

Obtain the value of the **EndTime** field in the **Results** field.

- a. Example field

```
Results:[{"EndTime":1626314520},{"FireResult":2}]
```

- b. Query and analysis statement

```
SELECT json_extract(Results, '$.[0].EndTime')
```

- c. Query and analysis result

**Table 5-26** Query and analysis results

EXPR\$0
1626314520

- **json\_extract\_scalar function**

Obtain the values of the **RawResultCount** field from the **Results** field, convert these values to **bigint** type, and sum them up.

- a. Example field

```
Results:[{"EndTime":1626314520},{"RawResultCount":1}]
```

- b. Query and analysis statement  
`SELECT sum(cast(json_extract_scalar(Results,'$.[1].RawResultCount') AS bigint) )`
- c. Query and analysis result

**Table 5-27** Query and analysis result

<b>EXPR\$0</b>
1546

## 5.7.5 IP Functions

### Constraints

The relationships between IP addresses and regions provided by LTS are from third-party libraries. The data is updated periodically (about half a year) and may not reflect the correct relationships. LTS will be optimized to update the libraries more frequently to provide better experience.

**A maximum of 5 million data records can be queried using the aggregate query of an IP function. Exceeding this limit will cause the query to time out.**

### Description

IP functions identify the country, state/province, city, and network carrier to which a target IP address belongs.

### Syntax

```
SELECT count(*) AS PV, ip_to_province(client_ip) AS province GROUP BY province
```

### IP Function Statements

**Table 5-28** IP function statements

Statement	Description	Example
ip_to_province	Identifies the state/province where an IP address is located.	ip_to_province(x)
ip_to_country	Identifies the country/region where an IP address is located.	ip_to_country(x)
ip_to_city	Identifies the city where an IP address is located.	ip_to_city(x)
ip_to_provider	Identifies the network carrier of an IP address.	ip_to_provider(x)

Statement	Description	Example
ip_to_geo	Returns the longitude and latitude of an IP address.	ip_to_geo(x)

## Examples

- **ip\_to\_province**

Obtains the top 3 states/provinces with the most requests.

- a. Query and analysis statement

```
SELECT count(*) AS PV, ip_to_province(client_ip) AS province GROUP BY province ORDER BY PV desc LIMIT 3
```

- b. Query and analysis result

**Table 5-29** Query and analysis result

PV	province
101	Guangdong
83	Shanghai
78	Shandong

- **ip\_to\_country**

Obtains the top 3 countries or regions with the most requests.

- a. Query and analysis statement

```
SELECT count(*) AS PV, ip_to_country(client_ip) AS county GROUP BY country ORDER BY PV desc LIMIT 3
```

- b. Query and analysis result

**Table 5-30** Query and analysis result

PV	country
100	China
76	United States
55	Canada

- **ip\_to\_city**

Obtains the top 3 cities with the most requests.

- a. Query and analysis statement

```
SELECT count(*) AS PV, ip_to_city(client_ip) AS city GROUP BY city ORDER BY PV desc LIMIT 3
```

- b. Query and analysis result



**Table 5-31** Query and analysis result

PV	city
109	Guangzhou
89	Shanghai
23	Xi'an

- **ip\_to\_provider**

Obtains the top 3 carriers with the most requests.

- a. Query and analysis statement

```
SELECT count(*) AS PV, ip_to_provider(client_ip) AS provider GROUP BY provider ORDER BY PV desc LIMIT 3
```

- b. Query and analysis result

**Table 5-32** Query and analysis result

PV	provider
115	Telecom
65	att.com
44	Unicom

- **ip\_to\_geo**

Returns the longitude and latitude of an IP address.

- a. Query and analysis statement

```
SELECT count(*) AS PV, ip_to_geo (client_ip) AS geo GROUP BY province ORDER BY PV desc LIMIT 3
```

- b. Query and analysis result

**Table 5-33**

PV	geo
101	*, *
83	47.369013, -68.326674
78	32.715891, -117.161588

## 5.7.6 Mathematical Functions

### Description

Mathematical functions are one type of scalar functions. They support only numeric fields and can be used to round values, obtain absolute values, and perform modulo operations. For details, see [Table 5-34](#).

In mathematical operations, if the operands involved in an expression are all integers, SQL uses integer operations. Otherwise, SQL switches to floating-point operations. You can force the switch by converting one of the operands to **float** type, and the runtime SQL extends the 32-bit floats in most expressions to 64-bit floats.

## Syntax

```
SELECT ABS(fieldname1) AS fieldname1_abs
```

## Mathematical Function Statements

**Table 5-34** Mathematical function statements

Statement	Description	Example
ABS(expr)	Returns the absolute value.	SELECT ABS(fieldname1)
CEIL(expr)	Rounds up to the nearest integer.	SELECT CEIL(fieldname1)
FLOOR(expr)	Rounds down to the nearest integer.	SELECT FLOOR(fieldname1)
TRUNCATE(expr, digits)	Truncates <b>expr</b> to a specified <b>digits</b> . If the number is negative, many positions to the left of the decimal point are truncated. If not specified, the number is zero by default.	SELECT TRUNCATE(fieldname1, 2)

Statement	Description	Example
ROUND(expr, digits)	Rounds <i>expr</i> to a specified number of decimal places. The result is of the same type as that of <i>expr</i> . <i>expr</i> can be an integer or a floating point number, but <i>digits</i> must be an integer. If <b>digits</b> is not specified, the default value <b>0</b> is used. If <b>digits</b> is a negative number, the value of <b>expr</b> is rounded off. If <b>expr</b> is a non-numeric value, it will be converted to 0. If <b>expr</b> is an infinite number, it is converted to a number with a finite number of digits of the closest <b>double</b> type.	SELECT ROUND(fieldname1, 2)
x + y	Addition.	SELECT fieldname1 + fieldname2
x - y	Subtraction.	SELECT fieldname1 - fieldname2
x * y	Multiplication.	SELECT fieldname1 * fieldname2
x / y	Division.	SELECT fieldname1 / fieldname2
MOD(x, y)	Modulo.	SELECT MOD(fieldname1, fieldname2)
LN(expr)	Logarithm (base: <b>e</b> ).	SELECT ln(expr)
LOG10(expr)	Logarithm (base <b>10</b> ).	SELECT LOG10(expr)
POWER(expr,power)	Power of <b>expr</b> .	SELECT POWER(expr ,2)
SQRT(expr)	Square root of <b>expr</b> .	SELECT SQRT(expr)
SIN(expr)	Sine.	SELECT SIN(expr)
COS(expr)	Cosine.	SELECT COS(expr)
TAN(expr)	Tangent.	SELECT TAN(expr)
COT(expr)	Cotangent.	SELECT COT(expr)
ASIN(expr)	Arcsine.	SELECT ASIN(expr)

Statement	Description	Example
ACOS(expr)	Arc cosine.	SELECT ACOS(expr)
ATAN(expr)	Inverse tangent.	SELECT ATAN(expr)

## Examples

### ACOS(expr)

Calculates the arccosine of a parameter value.  $y = \arccos x$ , where  $x$  is within  $[-1,1]$ .

1. Example field  
x:0.5
2. Query and analysis statement  

```
select ACOS(x)
```
3. Query and analysis result

**Table 5-35** Query and analysis result

x	EXPR\$1
0.5	1.0471975511965979

### ATAN(expr) function

Calculates the arctangent of a parameter value.  $y = \arctan x$ , where  $x$  is R.

1. Example field  
x:0.5
2. Query and analysis statement  

```
select ATAN(X)
```
3. Query and analysis result

**Table 5-36** Query and analysis result

x	EXPR\$1
0.5	1.0471975511965979

### ATAN2(expr)

Returns the angle  $\theta$  from rectangular coordinates  $(x, y)$  to polar coordinates  $(r, \theta)$ .

1. Example field  
x:3; y:4
2. Query and analysis statement  

```
SELECT x , y, ATAN2(x,y)
```
3. Query and analysis result

**Table 5-37** Query and analysis result

x	y	EXPR\$0
3	4	0.6435011087932844

## 5.7.7 Time Functions

### Description

Time functions can be used with **\_\_time**. Any column stored as a millisecond timestamp can use the **MILLIS\_TO\_TIMESTAMP** function, or any column stored as a string timestamp can use the **TIME\_PARSE** function. By default, the UTC time is used for time operations. You can change the time zone by setting the **timezone** parameter to the name of another time zone (for example, **Asia/Shanghai**) or to an offset (for example, **+08:00**).

### Syntax

Statement	Description	Example
CURRENT_DATE	Current date in the connected time zone.	SELECT CURRENT_DATE
CURRENT_TIMESTAMP	Current timestamp in the connected time zone.	SELECT CURRENT_TIMESTAMP
DATE_TRUNC(<unit>,<expr>)	Truncates the timestamp and returns it as a new timestamp.	SELECT DATE_TRUNC('minute',__time)

Statement	Description	Example
<p>TIME_FORMAT(&lt;expr&gt;,&lt;pattern&gt;,&lt;timezone&gt;))</p>	<p>Parses a character string into a timestamp using the specified pattern or ISO 8601 (for example, 2000-01-02T03:04:05Z ). <b>timezone</b> (if specified) should be a time zone name (such as <b>America/Los_Angeles</b>) or an offset (such as <b>+08:00</b>), and will be used as the time zone of the string that does not include a time zone offset. The mode and time zone must be literal. If a character string cannot be parsed as a timestamp, null is returned.</p>	<pre>SELECT TIME_FORMAT(__time,'yy-MM-dd HH:mm:ss','+08:00')</pre>
<p>TIME_PARSE(&lt;expr&gt;,&lt;pattern&gt;,&lt;timezone&gt;)</p>	<p>Parses a character string into a timestamp using the specified pattern or ISO 8601 (for example, 2000-01-02T03:04:05Z ). <b>timezone</b> (if specified) should be a time zone name (such as <b>America/Los_Angeles</b>) or an offset (such as <b>+08:00</b>), and will be used as the time zone of the string that does not include a time zone offset. The mode and time zone must be literal. If a character string cannot be parsed as a timestamp, null is returned.</p>	<pre>SELECT TIME_PARSE("timestamp ",'yyyy-MM-dd HH:mm:ss','+08:00')</pre>

Statement	Description	Example
MILLIS_TO_TIMESTAMP(expr)	Converts the timestamp to the time format.	SELECT MILLIS_TO_TIMESTAMP(expr)
TIMESTAMP_TO_MILLIS(expr)	Converts the time to the timestamp format.	SELECT TIMESTAMP_TO_MILLIS(expr)
EXTRACT(<extract_unit>FROM expr)	Extracts the time part from <b>expr</b> and returns it as a number.	SELECT EXTRACT(MINUTE FROM __time)
TIMESTAMPDIFF(<unit>,<expr1>,<expr2>)	Returns the unit between <b>expr1</b> and <b>expr2</b> .	SELECT TIMESTAMPDIFF (minute, expr1, expr2)
TIME_SERIES	Completes the missing data in the query time window.	TIME_SERIES(__time, period, time_format, [padding_value],<timezone>)

## TIME\_SERIES

The TIME\_SERIES function is used to supplement the missing data in the query time window.

### NOTE

- This function must be used together with ORDER BY and must be the first parameter of ORDER BY.
- The OFFSET statement cannot be used in the query statement.
- The TIME\_SERIES function cannot be used as a subquery.

### Syntax

```
time_series(__time, period, time_format, [padding_value], <timezone>)
```

### Parameter description

Table 5-38

Parameter	Description
__time	Time sequence.
period	Time window size (ISO 8601 standard). For example, <b>P1M</b> (1 month), <b>P1D</b> (1 day), <b>PT1H</b> (1 hour), <b>PT1M</b> (1 minute), and <b>PT1S</b> (1 second).
time_format	Time format of the returned result. (For details, see <a href="#">Joda DateTimeFormat</a> .)

Parameter	Description
padding_value	Supplemented content. Options: <ul style="list-style-type: none"> <li>● <b>0</b> or <b>zero</b>: By default, the missing value is set to <b>0</b>.</li> <li>● <b>null</b>: The missing value is set to null.</li> <li>● <b>last</b>: The missing value is set to the value corresponding to the previous time point.</li> <li>● <b>next</b>: The missing value is set to the value corresponding to the next time point.</li> <li>● <b>avg</b>: The missing value is set to the average value of two adjacent time points.</li> </ul>
timezone	Time zone, for example, UTC+08:00 (Beijing).

### Returned Data Type

The value is of the **bigint** type.

### Example

Supplement data based on the time granularity of a day, set the missing value to **0**, and add a time zone.

- Query and analysis statement  

```
select time_series(_time, 'P1D', 'yyyy-MM-dd HH:mm:ss', '0', '+08:00') as t_time, count(*) as num
group by t_time order by t_time
```
- Query and analysis results

t_time	num
2021-10-01 08:00:00	5
2021-10-02 08:00:00	0
2021-10-03 08:00:00	0
2021-10-04 08:00:00	21
2021-10-05 08:00:00	17
2021-10-06 08:00:00	0
2021-10-07 08:00:00	34

## CURRENT\_DATE/CURRENT\_TIMESTAMP

**CURRENT\_DATE** returns the ISO 8601 time (UTC time) of 00:00 on the current day. This function can be used to calculate timestamps.

**CURRENT\_TIMESTAMP** returns the ISO 8601 time (UTC time) of the current time. This function can be used to calculate timestamps.



1. Example field  
\_\_time: 2023-02-14T02:35:56.706Z
2. Query and analysis statement  
select \_\_time,CURRENT\_DATE, CURRENT\_TIMESTAMP,CURRENT\_TIMESTAMP
3. Query and analysis result

**Table 5-39** Query and analysis result

__time	CURRENT_DATE	CURRENT_TIMESTAMP
2023-02-14T02:35:56.706Z	2023-02-14T00:00:00.000Z	2023-02-14T14:35:57.000Z

## DATE\_TRUNC (<unit>, <timestamp\_expr>)

Truncates <timestamp\_expr> to the precision specified in <unit>, fills in 0, and returns the value as a new timestamp. The unit is case-insensitive, and can be milliseconds, second, minute, hour, day, week, month, quarter, year, decade, century, or millennium.

1. Example field  
\_\_time: 2023-02-14T02:35:56.706Z
2. Query and analysis statement  
SELECT \_\_time,DATE\_TRUNC('minute', \_\_time),DATE\_TRUNC('day', \_\_time),DATE\_TRUNC('year', \_\_time)
3. Query and analysis result

**Table 5-40** Query and analysis result

__time	EXPR\$1	EXPR\$2	EXPR\$3
2023-02-14T02:35:56.706Z	2023-02-15T08:50:00.000Z	2023-02-15T00:00:00.000Z	2023-01-01T00:00:00.000Z

## TIME\_PARSE(<string\_expr>, [<pattern>, [<timezone>]])/ TIME\_FORMAT(<timestamp\_expr>, [<pattern>, [<timezone>]])

Parses the given character string <timestamp\_expr> into a timestamp according to the custom <pattern> parameter and **Joda DateTimeFormat** mode. If <pattern> is not specified, the character string is parsed according to ISO 8601 by default. <timezone> is optional.

Parses the given timestamp <timestamp\_expr> into a character string according to the custom <pattern> parameter and **Joda DateTimeFormat** mode. If <pattern> is not specified, the timestamp is parsed according to ISO 8601 by default. <timezone> is optional.

1. Example field  
\_\_time: 2023-02-16T07:38:25.306Z  
start\_time:2023-02-14 02:35:56

2. Query and analysis statement  
SELECT \_\_time,TIME\_PARSE(start\_time,'yyyy-MM-dd HH:mm:ss'),TIME\_FORMAT(\_\_time,'yyyy-MM-dd HH:mm:ss')
3. Query and analysis result

**Table 5-41** Query and analysis result

__time	EXPR\$1	EXPR\$2
2023-02-16T07:38:25.306Z	2023-02-14T02:35:56.000Z	2023-02-16 07:38:25

### MILLIS\_TO\_TIMESTAMP(millis\_expr)/ TIMESTAMP\_TO\_MILLIS(timestamp\_expr)

MILLIS\_TO\_TIMESTAMP converts a number of milliseconds into a timestamp in ISO 8601 format. The converted parameter can be used to calculate timestamps. TIMESTAMP\_TO\_MILLIS converts a timestamp to a number of milliseconds.

1. Example field  
\_\_time: 2023-02-16T07:54:15.106Z,start\_time: 1676534055106
2. Query and analysis statement  
SELECT \_\_time,MILLIS\_TO\_TIMESTAMP(start\_time),TIMESTAMP\_TO\_MILLIS(\_\_time)
3. Query and analysis result

**Table 5-42** Query and analysis result

__time	EXPR\$1	EXPR\$2
2023-02-16T07:54:15.106Z	2023-02-16T07:54:05.000Z	1676534055106

### TIME\_EXTRACT(<timestamp\_expr>,[<unit>],[<timezone>])/EXTRACT(<unit> FROM timestamp\_expr)

TIME\_EXTRACT extracts time from **timestamp\_expr** and returns it as a number. The unit can be EPOCH (Unix time in seconds since the epoch), SECOND (second of the current minute), MINUTE (minute of the current hour), HOUR (hour of the current day), DAY (day of the current month), DOW (day of the current week), DOY (day of the current year), WEEK (week of the current year), MONTH (month of the current year), QUARTER (quarter of the current year), or YEAR (current year). <timezone> is optional. EXTRACT is short for TIME\_EXTRACT.

1. Example field  
\_\_time: 2023-02-16T07:54:15.106Z,start\_time: 1676534055106
2. Query and analysis statement  
SELECT \_\_time,MILLIS\_TO\_TIMESTAMP(start\_time),TIMESTAMP\_TO\_MILLIS(\_\_time)
3. Query and analysis result

**Table 5-43** Query and analysis result

<b>__time</b>	<b>EXPR\$1</b>	<b>EXPR\$2</b>
2023-02-16T07:54:15.106Z	2023-02-16T07:54:05.000Z	1676534055106

## Reference Information

- **Unit**

<b>unit</b>	<b>Description</b>
second	Second
minute	Minute
hour	Hour
day	Day
week	Week
month	Month
quarter	Quarter
year	Year

- **extract\_unit**

<b>extract_unit</b>	<b>Description</b>
SECOND	Second
MINUTE	Minute
HOUR	Hour
DAY	Day of a month
DOW	Day of a week
DOY	Day of a year
WEEK	Week of a year
MONTH	Month
QUARTER	Quarter
YEAR	Year

## 5.7.8 Extrema Function

### Description

Extrema functions return the maximum or minimum value after evaluating zero or more specified fields. For details, see [Table 5-44](#).

Pay attention to the following points when using the extrema functions:

- If no field is set, null is returned. Fields must be able to be converted to common data types.
- If all fields are null, null is returned. If only some fields are null, these fields will be ignored.
- If a field contains both numbers and strings, the function compares them as strings.
- If all columns are integers, the function compares them as **long** values.
- If all fields are numbers and at least one is a **float** value, the function compares them as **float** values.

### Syntax

```
SELECT GREATEST(fieldname1,fieldname2) AS the_greatest_field
```

### Extrema Function Statements

**Table 5-44** Extrema function statements

Statement	Description	Example
GREATEST([expr1, ...])	Returns the maximum value among zero or multiple fields.	SELECT GREATEST(fieldname1,fieldname2)
LEAST([expr1, ...])	Returns the minimum value among zero or multiple fields.	SELECT LEAST(fieldname1,fieldname2)

## 5.7.9 String Functions

### Description

SQL provides the string function for concatenating strings and converting between uppercase and lowercase letters. For details, see [Table 5-45](#).

#### NOTE

In the SQL syntax, characters must be enclosed in single quotation marks ('). Fields or table names are not enclosed or are enclosed with double quotation marks ("). For example, 'msg' indicates the character string **msg**, and **msg** or "**msg**" indicates the structured **msg** field.

## Syntax

```
SELECT (fieldname1 || fieldname2) AS fieldname1_fieldname2
```

## String Function Statements

**Table 5-45** String function statements

Statement	Description	Example
CONCAT(expr1, expr2...)	Concatenates all listed strings.	SELECT str1, str2, str3, CONCAT(str1, str2, str3) WHERE str1 IS NOT NULL
TEXTCAT(expr, expr)	Concatenates two strings.	SELECT str1, str2, TEXTCAT(str1, str2) WHERE str1 IS NOT NULL
STRING_FORMAT(pattern[, args...])	Formats strings based on the Java string format.	SELECT str1, STRING_FORMAT(str1, '%s') WHERE str1 IS NOT NULL
LENGTH(expr)	Returns the length of a string, which is the number of UTF-16 characters in the string.	SELECT LENGTH(str1) WHERE str1 IS NOT NULL
LOWER(expr)	Converts a string into lowercase letters.	SELECT LOWER(str1) WHERE str1 IS NOT NULL
POSITION(string1 IN string2 [FROM fromIndex])	Returns the index of the position where <b>string1</b> appears in <b>string2</b> for the first time. The search starts from the specified index. If no index is specified, the search starts from <b>index1</b> . If <b>string1</b> does not exist in <b>string2</b> , <b>0</b> is returned.	SELECT POSITION(str1 IN str2 FROM 5)
REGEXP_EXTRACT(expr, pattern, [index])	Extracts a string that matches a specified regular expression in <i>expr</i> . The index starts from 1. If no match is found, null is returned. If no index is specified or the index is 0, the first matched substring is returned. For exact match, add a caret (^) before the regular expression and a dollar sign (\$) after the regular expression.	SELECT REGEXP_EXTRACT(str1, '[A-Za-z]+://[A-Za-z0-9.-]+/(^[^ ]*)', 5)

Statement	Description	Example
REGEXP_LIKE(expr, pattern)	Checks whether a string matches a specified regular expression. For exact match, add a caret (^) before the regular expression and a dollar sign (\$) after the regular expression. The usage of this function is similar to that of the LIKE statement. The difference is that the LIKE statement searches for content with a specified pattern.	SELECT REGEXP_LIKE(str1, '\.(jpg jpeg png gif)\$')
REPLACE(expr, pattern, replacement)	Uses <b>replacement</b> to replace the substring same as <b>pattern</b> in <b>expr</b> .	SELECT REPLACE(expr,pattern, replacement)
STRPOS(string1, string2)	Returns the index of the position where <b>string2</b> appears in <b>string1</b> for the first time. The search starts from <b>index1</b> . If no result is found, <b>0</b> is returned.	SELECT STRPOS(str1, str2) WHERE str1 IS NOT NULL AND str2 IS NOT NULL
SUBSTRING(expr, index, [length])	Subtracts a string. <i>length</i> indicates how many UTF-16 characters will be extracted.	SELECT SUBSTRING(str1, 3, 10) WHERE str1 IS NOT NULL
RIGHT(expr, [length])	Truncates a specified length from the right to the left of a string.	SELECT RIGHT(str1, 5) WHERE str1 IS NOT NULL
LEFT(expr, [length])	Truncates a specified length from the left to the right of a string.	SELECT LEFT(str1, 5) WHERE str1 IS NOT NULL
SUBSTR(expr, index, [length])	Same as SUBSTRING.	SELECT SUBSTR(str1, 3, 10) WHERE str1 IS NOT NULL
UPPER(expr)	Converts a string into uppercase letters.	SELECT UPPER(str1) WHERE str1 IS NOT NULL
REVERSE(expr)	Reverses the character string.	SELECT REVERSE(str1) WHERE str1 IS NOT NULL

Statement	Description	Example
LPAD(expr, length, chars)	Adds specified characters to the left of a string until the string reaches the specified length. If the specified length is less than the actual string length, the string is truncated based on the specified length. If the string or the specified character is null, null is returned. If the specified character is empty, no padding is performed. Characters may be deleted if necessary.	SELECT LPAD(str1, 50, 'testStr') WHERE str1 IS NOT NULL
RPAD(expr, length, chars)	Adds specified characters to the right of a string until the string reaches the specified length. If the specified length is less than the actual string length, the string is truncated based on the specified length. If the string or the specified character is null, null is returned. If the specified character is empty, no padding is performed. Characters may be deleted if necessary.	SELECT RPAD(str1, 50, 'testStr') WHERE str1 IS NOT NULL
CONTAINS_STRING(<expr>, str)	Checks whether <b>expr</b> contains the <b>str</b> string.	SELECT CONTAINS_STRING(log_level, 'warn')
ICONTAINS_STRING(<expr>, str)	Checks whether <b>expr</b> contains the <b>str</b> string. The string is not case sensitive.	SELECT ICONTAINS_STRING(log_level, 'WARN')

## Examples

### REPEAT

REPEAT(expr, [N]) repeats **expr** for N times.

1. Example field  
field4:is
2. Query and analysis statement  
select field4, REPEAT(field4, 3)
3. Query and analysis result

**Table 5-46** Query and analysis result

field4	EXPR\$1
ls	isis

## 5.7.10 SPLIT Functions

### Description

SPLIT functions split a character string using a delimiter, and return the substrings.

### Syntax

```
SELECT split_to_map(x, delimiter01, delimiter02)
```

### SPLIT Function Statements

State ment	Description	Example	Parameter
split	Splits a character string using a delimiter and returns the substrings.	split(x, delimiter,[limit])	<ul style="list-style-type: none"> <li>• <b>x</b>: varchar parameter value.</li> <li>• <b>delimiter</b>: delimiter.</li> <li>• <b>limit</b>: an integer greater than 0, specifying the maximum number into which the character string can be split.</li> </ul>
split_part	Splits a character string using a specified delimiter and returns the indexed content.	split_part(x, delimiter, part)	<ul style="list-style-type: none"> <li>• <b>x</b>: varchar parameter value.</li> <li>• <b>delimiter</b>: delimiter.</li> <li>• <b>part</b>: index of the field to return.</li> </ul>
split_to_map	Splits a character string using the first delimiter, and then splits the string again using the other delimiter.	split_to_map(x, delimiter01, delimiter02)	<ul style="list-style-type: none"> <li>• <b>x</b>: varchar parameter value.</li> <li>• <b>delimiter01</b>: delimiter 1.</li> <li>• <b>delimiter02</b>: delimiter 2.</li> </ul>



## Examples

- **split**

Splits a target character string according to a specified string. **limit** specifies the maximum number of words to split into. If this parameter is not specified, all words are split by default.

- a. Example field

Id: dc1dab7e-b045-4e77-bda4-914d083d1bf7

- b. Query and analysis statement

```
SELECT split(Id,'-'), split(Id,'-',2)
```

- c. Query and analysis result

**Table 5-47** Query and analysis result of the split function

EXPR\$0	EXPR\$1
["dc1dab7e","b045","4e77","bda4","914d083d1bf7"]	["dc1dab7e","b045-4e77-bda4-914d083d1bf7"]

- **split\_part**

Splits a character string and returns the indexed content. The index starts from 0. If it is negative or greater than the number of substrings, an empty string is returned.

- a. Example field

Id: dc1dab7e-b045-4e77-bda4-914d083d1bf7

- b. Query and analysis statement

```
SELECT split_part(Id,'-',1)
```

- c. Query and analysis result

**Table 5-48** Query and analysis result of the split\_part function

EXPR\$0
b045

- **split\_to\_map**

Splits a character string using the first delimiter, and then splits the string again using the other delimiter. The result is displayed in format `{"KEY1":"VALUE1","KEY2":"VALUE2"}`. If a value cannot be split again, it is left blank.

- a. Example field

**Request:** request\_id:"e3ac4b70c7d244f080d434e300d8065a";  
request\_time: "1674965051000"

- b. Query and analysis statement

```
SELECT split_to_map(Request,';',':')
```

- c. Query and analysis result

**Table 5-49** Query and analysis result of the split\_to\_map function

EXPR\$0
{"request_id ":"e3ac4b70c7d244f080d434e300d8065a", "request_time":"1674965051000"}

## 5.7.11 Comparison Operators

### Description

Comparison operators are used to compare two values and return **true** or **false**. Values of the numeric type and contents of the string type can be compared. For example, comparison operators can be used to check whether the numeric field *num1* < *num2* is true and whether *str1* of the string type exists in string *strs*. For details, see [Table 5-50](#).

### Syntax

```
SELECT fieldname1 WHERE fieldname1 > fieldname2
```

### Comparison Operator Statements

**Table 5-50** Comparison operator statements

Statement	Description	Example
<code>x = y</code>	Equal to	<code>SELECT num1 &lt; num2</code>
<code>x &lt;&gt; y</code>	Not equal to	<code>SELECT num1 &lt;&gt; num2</code>
<code>x &gt; y</code>	Greater than	<code>SELECT num1 &gt; num2</code>
<code>x &gt;= y</code>	Greater than or equal to	<code>SELECT num1 &gt;= num2</code>
<code>x &lt; y</code>	Less than	<code>SELECT num1 &lt; num2</code>
<code>x &lt;= y</code>	Less than or equal to	<code>SELECT num1 &lt;= num2</code>
<code>x BETWEEN y AND z</code>	Equivalent to <b>x &gt;= y AND x &lt;= z</b>	<code>SELECT num1 BETWEEN num2 AND num3</code>
<code>x NOT BETWEEN y AND z</code>	Equivalent to <b>x &lt; y OR x &gt; z</b>	<code>SELECT num1 NOT BETWEEN num2 AND num3</code>

Statement	Description	Example
x LIKE pattern	Returns <b>true</b> if x matches the SQL LIKE mode.	SELECT str1 LIKE '*'
x NOT LIKE pattern	Returns <b>true</b> if x does not match the SQL LIKE mode.	SELECT str1 NOT LIKE '*'
x IS NULL	Returns <b>true</b> if x is null or an empty string.	SELECT str1 IS NULL
x IS NOT NULL	Returns <b>true</b> if x is neither null nor an empty string.	SELECT str1 IS NOT NULL
x IN (values)	If x is one of the listed values, <b>true</b> is returned.	SELECT str1 IN ('testStr1', 'testStr2')
x NOT IN (values)	If x is not listed, <b>true</b> is returned.	SELECT str1 NOT IN ('testStr1', 'testStr2')
x IN (subquery)	Returns <b>true</b> if x is returned through a specified subquery.	SELECT str1 WHERE str2 IN (SELECT DISTINCT str2 LIMIT 100)
x NOT IN (subquery)	If x is not returned through the specified subquery, <b>true</b> is returned.	SELECT str1 NOT IN (SELECT str2 LIMIT 100)

## 5.7.12 IP Functions

### Description

The IPv4 function can use an IPv4 address in dotted decimal notation (example: **192.168.0.1**) or an IP address in integer format (example: **3232235521**). The **subnet** parameter is an IPv4 subnet in CIDR notation (example: **192.168.0.0/16**).

## IP Function Statements

Statement	Description	Example
IPV4_MATCH(address,subnet)	If <b>subnet</b> belongs to <b>address</b> , <b>true</b> is returned. Otherwise, <b>false</b> is returned. If <b>address</b> is not a valid IPv4 address, <b>false</b> is returned. This function is more efficient if <b>address</b> is an integer rather than a string.	SELECT IPV4_MATCH (address,subnet)
IPV4_PARSE(address)	Parses <b>address</b> into an integer IPv4 address. If <b>address</b> is a valid IPv4 address, it can be parsed. If <b>address</b> is not a valid IPv4 address, <b>null</b> is returned.	SELECT IPV4_PARSE(address)
IPV4_STRINGIFY(address)	Converts an integer <b>address</b> into an IPv4 address in dotted notation. If <b>address</b> is a valid integer IPv4 address, it can be parsed. If <b>address</b> is not an IPv4 address, <b>null</b> is returned.	SELECT IPV4_STRINGIFY(address)

## Examples

### IPV4\_MATCH(address, subnet)

If **address** belongs to **subnet**, **true** is returned. Otherwise, **false** is returned. If **address** is not a valid IPv4 address, **false** is returned. This function is more efficient if **address** is an integer rather than a string.

1. Example field  
Ipv4: 192.168.1.18
2. Query and analysis statement  

```
select IPV4,IPV4_MATCH(Ipv4, '192.168.0.0/16')
```
3. Query and analysis result

**Table 5-51** Query and analysis result

IPV4	EXPR\$1
192.168.1.18	true

### IPV4\_PARSE(address)/IPV4\_STRINGIFY(address)

Parses **address** into an integer IPv4 address. If **address** is a valid IPv4 address, it can be parsed. If **address** is not a valid IPv4 address, **null** is returned.

1. Example field  
Ipv4: 192.168.0.1  
Num: 3232235521
2. Query and analysis statement  

```
select IPV4_PARSE(Ipv4), IPV4_STRINGIFY(Num)
```
3. Query and analysis result

**Table 5-52** Query and analysis result

EXPR\$0	EXPR\$1
-1062731775	192.168.0.1

## 5.7.13 Reduction Functions

### Description

Reduction functions operate on zero or a list of expressions and return a single expression. If no expression is passed as a parameter, the result is **NULL**. All expressions must be converted to public data types.

- If all parameters are **NULL**, the result is **NULL**. Otherwise, **NULL** parameters are ignored.
- If all parameters contain both numbers and strings, they are interpreted as strings.
- If all parameters are integers, they are interpreted as long integers.
- If all parameters are numeric and at least one of them is double, all parameters are interpreted as double.

### Syntax

```
GREATEST([expr1, ...]) / LEAST([expr1, ...])
```

## Examples

### GREATEST([expr1, ...])/LEAST([expr1, ...])

The GREATEST function returns the maximum value in zero or a list of expressions.

The LEAST function returns the minimum value in zero or a list of expressions.

1. Example field  
Num: 11785730
2. Query and analysis statement  

```
select Num,GREATEST("Num"/10,(select count(1))),LEAST("Num"/10,(select count(1)))
```
3. Query and analysis result

**Table 5-53** Query and analysis result of reduction functions

Num	EXPR\$1	EXPR\$2
11785730	1178573	1

## 5.7.14 Other Functions

### Description

SQL functions also support some conversion types and logical operations such as CASE and WHEN. For details, see [Table 5-54](#).

### Syntax

```
SELECT CAST(fieldname1 AS VARCHAR) AS fieldname1_str
```

### Other Function Statements

**Table 5-54** Other function statements

Keyword	Description	Example
CAST(value AS TYPE)	Converts the data type. Data types can be converted only to <b>varchar</b> or <b>float</b> .	SELECT fieldname1, CAST(fieldname1 AS VARCHAR)
CASE WHEN boolean_expr1 THEN result1 \[ WHEN boolean_expr2 THEN result2 ... \] \[ ELSE resultN \] END	Simple CASE function.	SELECT CASE WHEN httpStatus = 200 THEN 1 ELSE 0 END
NULLIF(value1, value2)	If <i>value1</i> is equal to <i>value2</i> , null is returned. Otherwise, <i>value1</i> is returned.	SELECT fieldname1, fieldname2, NULLIF(fieldname1, fieldname2)

Keyword	Description	Example
NVL(expr,expr-for-null)	If <b>expr</b> is null or an empty string, this function returns <b>expr-for-null</b> .	SELECT NVL(str1, 'expr-for-null')

## 5.7.15 JOIN Clause

The JOIN clause queries data in two or more tables. This section describes how to use the JOIN clause.

### Syntax

```
select key
from t1
LEFT|RIGHT|INNER JOIN t2
on t1.key=t2.key
```

Currently, LTS supports LEFT JOIN, RIGHT JOIN, and INNER JOIN.

**Table 5-55**

JOIN Mode	Description
LEFT JOIN	Join the right table (t2) based on the result of the left table (t1). <b>NOTE</b> If the table name contains only digits, add double quotation marks to the table name to convert it into a string. For example, if the table name is <b>123</b> , enter " <b>123</b> " in the JOIN statement.
RIGHT JOIN	Join the left table (t1) based on the result of the right table (t2). <b>NOTE</b> If the table name contains only digits, add double quotation marks to the table name to convert it into a string. For example, if the table name is <b>123</b> , enter " <b>123</b> " in the JOIN statement.
INNER JOIN	Intersection data of the results (elb1 and elb2) of two tables

### Examples

There are two tables. **access** indicates the host ingestion metrics, including path, latency, and status code. **host** indicates the host metrics, including CPU and memory. You can use JOIN to associate ingestion and host metrics and view different dimensions of metrics of the same host.

- **LEFT JOIN**

a. Query statements

```
SELECT
 "access"._time,
 "access".host_ip,
 "access".cost,
 "host".cpu,
 "host".memory
FROM
 log "access"
 LEFT JOIN (select memory,cpu,host_ip from log) host ON "access".host_ip = "host".host_ip
```

b. 60 data records returned

- **RIGHT JOIN**

a. Query statements

```
SELECT
 "access"._time,
 "host".host_ip,
 "access".cost,
 "host".cpu,
 "host".memory
FROM
 log "access"
 RIGHT JOIN (select memory,cpu,host_ip from log) host ON "access".host_ip = "host".host_ip
```

b. 60 data records returned

- **INNER JOIN**

a. Query statements

```
SELECT
 "access"._time,
 "host".host_ip,
 "access".cost,
 "host".cpu,
 "host".memory
FROM
 log "access"
 INNER JOIN (select memory,cpu,host_ip from log) host ON "access".host_ip = "host".host_ip
```


b. 45 data records returned

## 5.7.16 SQL Query Example

This section describes how to query ELB raw logs in LTS.

**Step 1** Log in to the LTS console, and click a log stream on the **Log Management** page to go to the log details page.

**Step 2** View logs on the **Raw Logs** tab page. The system obtains ELB raw logs.

**Step 3** Click  in the upper right corner. On the page that is displayed, select **Cloud Structuring Parsing**.

**Step 4** Select **Structuring Template**, and configure log structuring based on the ELB template. For other logs, you can select other structuring templates.

**Step 5** On the **Visualization** tab page, enter an SQL statement in the search box.

----End

## Display of Query Results

Table



The following statement queries the host, the number of logs of each **request\_uri**, the request body size in MB, and the ratios of 2xx, 3xx, 4xx, and 5xx responses. Then the results are displayed in a table, and sorted in descending order by the number of logs.

```
SELECT "router_request_uri" as "request_uri", "host", COUNT(*) as pv,
round(sum(body_bytes_sent) / 1024.0 , 5) as "body_bytes_sent(MB)",
round(sum(case when status >= 200 and status < 300 then 1 else 0 end) * 100.0 / COUNT(1), 6) as "2xx
ratio(%)",
round(sum(case when status >= 300 and status < 400 then 1 else 0 end) * 100.0 / count(1), 6) as "3xx
ratio(%)",
round(sum(case when status >= 400 and status < 500 then 1 else 0 end) * 100.0 / count(1), 6) as "4xx
ratio(%)",
round(sum(case when status >= 500 and status < 600 then 1 else 0 end) * 100.0 / count(1), 6) as "5xx
ratio(%)",
GROUP BY "host", "router_request_uri"
ORDER BY pv DESC
LIMIT 100
```

### Bar chart

The following statement queries the number of requests for each request URL and displays the results in a bar chart, with **request\_uri** set as the X axis and **pv** as the Y axis.

```
SELECT "router_request_uri" as "request_uri", "host", COUNT(*) as pv,
round(sum(body_bytes_sent) / 1024.0 , 5) as "body_bytes_sent(MB)",
round(sum(case when status >= 200 and status < 300 then 1 else 0 end) * 100.0 / COUNT(1), 6) as "2xx
ratio(%)",
round(sum(case when status >= 300 and status < 400 then 1 else 0 end) * 100.0 / count(1), 6) as "3xx
ratio(%)",
round(sum(case when status >= 400 and status < 500 then 1 else 0 end) * 100.0 / count(1), 6) as "4xx
ratio(%)",
round(sum(case when status >= 500 and status < 600 then 1 else 0 end) * 100.0 / count(1), 6) as "5xx
ratio(%)",
GROUP BY "host", "router_request_uri"
ORDER BY pv DESC
LIMIT 100
```

### Line chart

The following statement displays a line chart based on the query result, with **\_time\_** set as the X axis and **QPS** as the Y axis. The chart shows the queries per second (QPS) change at an interval of 5s in the query period.

```
select TIME_FORMAT(TIME_CEIL(TIME_PARSE(SUBSTRING(time_iso8601, 2, 25) , 'yyyy-MM-dd"'"HH:mm:ssZZ'), 'PT5S'), 'yyyy-MM-dd HH:mm:ss', '+08:00') AS _time_ , COUNT(*) as QPS from log group
by _time_
```

### Pie chart

The following statement queries the percentage of different values of status in the query period, and displays the results in a bar chart, with **Category** set to **status** and **Value** set to **rm**.

```
SELECT status, COUNT(1) AS rm GROUP BY status
```

### Number chart

The following statement queries the total number of normal requests in the last hour and displays the results in a number chart.

```
SELECT count(*) AS normalRequest WHERE status = 200
```

# 6 Log Visualization

## 6.1 Overview

LTS can analyze structured logs with [SQL query syntax](#) and display analysis results in various charts, catering to visualization needs of different O&M and operations analysis scenarios.

With more than 40 out-of-the-box dashboard templates and preset sample data that are easy to use and configure, LTS lowers the usage threshold and reduces repetitive development work. Cloud service logs ingested to LTS can be directly displayed in dashboard templates. This helps enterprises realize digital operations based on log data and facilitates digital transformation.

**Table 6-1** Visualization methods

Method	Description
Statistical charts	Statistical charts, such as tables, bar charts, and line charts, are rendered by LTS based on <a href="#">SQL query syntax</a> . For details, see <a href="#">Visualizing Logs in Statistical Charts</a> .
Dashboards	<ul style="list-style-type: none"><li>LTS provides dashboards for real-time data analysis. A dashboard consolidates and synchronously saves various statistical charts derived from SQL query and analysis. For details, see <a href="#">Visualizing Logs in Dashboards</a>.</li></ul>

### NOTE

Currently, this function is available to all users in regions CN South-Guangzhou, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN-Hong Kong, CN Southwest-Guiyang1, AP-Singapore, and CN North-Beijing1. It is also available to whitelisted users in regions CN South-Shenzhen, AP-Bangkok, ME-Riyadh, and AP-Jakarta.

## 6.2 Visualizing Logs in Statistical Charts

### 6.2.1 Statistical Charts

After logs are reported to LTS, you can search for key log data using [SQL analysis syntax](#) and view the results in charts. This helps you track log data trends effectively. You can also save chart analysis results to the dashboard for long-term monitoring.

#### Constraints

- Up to 100 charts can be created for a log stream.
- Up to 50 charts can be added to a dashboard.

#### Statistical Chart Types

Data in different scenarios can be displayed in table charts, bar charts, and line charts. For details, see [Table 6-2](#).

**Table 6-2** Chart types

Chart Type	Scenario
Table chart	A table chart is the most common way for data display. Data can be collected and compared through data structuring. This chart type is applicable to most scenarios.
Bar chart	A bar chart describes the classified data and intuitively compares the size of each classification item. This chart type is applicable to classified statistics, such as the number of occurrences of each error code type in the past day.
Line chart	A line chart requires the time sequence field to organize and aggregate metrics based on the time sequence. This chart type intuitively reflects the changes of metrics over time.
Pie chart	A pie chart shows the proportion of each category. The proportion of each category is measured by the sector size. This chart type is applicable to scenarios such as error code proportion analysis.
Number chart	A number chart describes a single metric. Generally, key metrics with business value are selected. This chart type is applicable to single-metric statistics such as daily, weekly, monthly PVs and UVs.
Digital line	A digital line chart combines a line chart and a number chart. The line chart displays data trends and changes, and the number chart displays key metrics. This chart type is applicable when trends and key data points need to be displayed at the same time.

Chart Type	Scenario
Map	A map displays the geographical location of data based on the location of a chart. Generally, a map displays the distribution of data in different geographical areas. This chart type is applicable to geographical location statistics, such as geographical distribution of attack IP addresses.
Funnel chart	A funnel chart is applicable to the service procedure with a single flow direction and a single path. The funnel chart collects statistics on each phase and uses a trapezoidal area to indicate the difference between the service volume of a phase and that of the previous phase.

## Operation Description

You can create and save a chart, or save a chart as another file. For details, see [Table 6-3](#).

**Table 6-3** Operation description

Operation	Description
Create	Selecting a chart type and saving the chart analysis result to the dashboard
Save	Saving the current visualized chart
Save As	Copying the existing visualized chart
Download	Downloading the chart analysis result to an Excel file
Show Chart	Expanding the visualized chart of the current log stream
Hide Chart	Hiding the visualized chart of the current log stream

## 6.2.2 Table

Table charts are one of the most common data display types and the most basic method for organizing and sorting data. By sorting data, you can quickly reference and analyze the data. By default, the data obtained through the query and analysis syntax is displayed in a table chart.

### Checking Tables

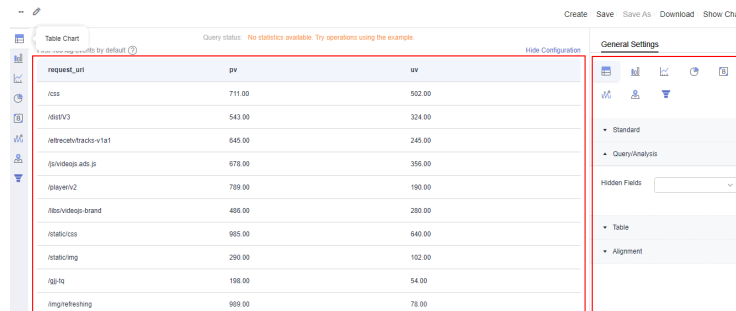
- Step 1** Log in to the LTS console.
- Step 2** In the navigation pane, choose **Log Management**.
- Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.

**Step 4** Choose **Log Analysis**.

**Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.

**Step 6** By default, the query results are displayed in a table below the log. Set parameters in the **General Settings** right pane by referring to [Table 6-4](#).

**Figure 6-1** Table chart



**Table 6-4** Table parameters

Type	Parameter	Description
Standard	Format	Displays the table chart data in the specified format.
	Unit	Specifies the unit of the data in the customized table chart.
	Decimal Places	Sets the number of decimal places to be displayed.
	Title Font Size	Sets the font size of the chart title.
Query/Analysis	Hidden Fields	Select a target field to hide it in the table chart.
Table	Records per Page	Number of data records displayed on each page.
	Display Total	Displays the total number of entries in the table.
Column	Alignment	Alignment mode of table data. The options are left alignment, right alignment, and center alignment.
	Filtering	After this function is enabled, you can search for data in the table column.
	Sorting	After this function is enabled, you can sort data in the table.

Type	Parameter	Description
	Font Size	Size of the table font. The value ranges from 12 px to 24 px.

----End

## 6.2.3 Bar Chart

A bar chart uses vertical or horizontal bars to compare values between categories. It shows the data of different categories and counts the number of elements in each category.

The bar chart provided by LTS consists of vertical bars and horizontal bars. The width of the rectangle block is fixed, and the height indicates the value. When multiple columns of data are mapped to the Y axis, the data is displayed in group columns.

By default, vertical bars are used. You can select either vertical or horizontal bars. A bar chart contains the following elements:

- X axis (horizontal axis)
- Y axis (vertical axis)
- Rectangular block
- Legend

### Checking Bar Charts

**Step 1** Log in to the LTS console.

**Step 2** In the navigation pane, choose **Log Management**.

**Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.

**Step 4** Choose **Log Analysis**.

**Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.


**Step 6** Click  to display the queried data in a bar chart. Set parameters in the **General Settings** right pane by referring to [Table 6-5](#).

Figure 6-2 Bar chart

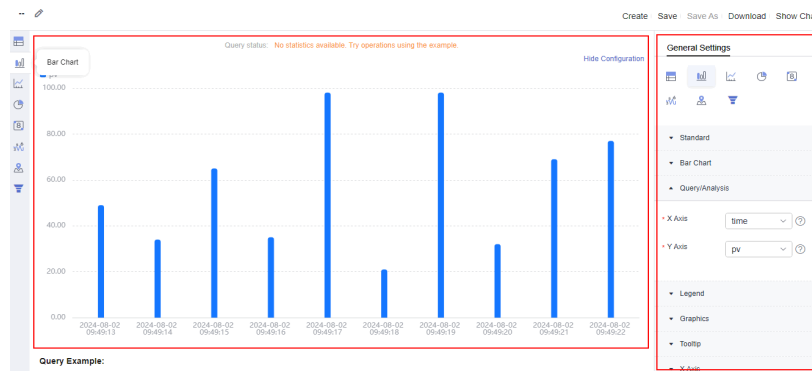


Table 6-5 Bar chart parameters

Type	Parameter	Description
Standard	Format	Displays the Y axis in the specified format.
	Unit	Customize the unit of the Y axis.
	Decimal Places	Sets the number of decimal places to be displayed.
	Title Font Size	Sets the font size of the chart title.
Bar Chart	Direction	Select <b>Bar chart</b> or <b>Horizontal bar chart</b> .
	Column Width	Sets the column width.
	Display Value	After this function is enabled, the value indicated by each bar is displayed.
	Font Size	Sets the font size of each bar.
	Stacked	After this function is enabled, the Y axis data is displayed in stack mode.
Query/ Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
Legend	Hide Legend	After this function is enabled, you can hide the legend and comparison results.
	Legend Position	Position of the legend in the chart. Select <b>Top</b> or <b>Right</b> .
	Comparison Value	Indicates whether to display the maximum value, minimum value, average value, and sum value. You can select multiple options.

Type	Parameter	Description
Graphics	Top Margin	Specifies the distance between the axis and the upper boundary of the graph.
	Bottom Margin	Specifies the distance between the axis and the lower boundary of the graph.
	Left Margin	Specifies the distance between the axis and the left boundary of the graph.
	Right Margin	Specifies the distance between the axis and the right boundary of the graph.
Tooltip	<b>None, Ascending, and Descending</b>	Dialog box configuration. When multiple Y-axis data records are selected, they can be sorted and displayed.
X Axis	Show	After this function is enabled, data on the X axis is displayed.
	X Axis Title	Title of the X axis.
Y Axis	Show	After this function is enabled, the Y axis data is displayed.
	Y Axis Title	Title of the Y axis.
	Position	Position of the Y axis. Select <b>Left</b> or <b>Right</b> .

----End

## 6.2.4 Line Chart

A line chart is used to analyze the data change trend in a certain period, which is reflected in the following aspects:

- Increment or decrement
- Increase/Decrease rate
- Regularity of increase/decrease (such as periodic change)
- Peak and valley values

Therefore, the line chart is the best choice for analyzing the data change trend over time. In addition, you can draw multiple lines to analyze the change trend of multiple groups of data in the same period, and then analyze the interaction and impact between data (such as in direct or inverse proportion).

### Checking Line Charts

**Step 1** Log in to the LTS console.


**Step 2** In the navigation pane, choose **Log Management**.

**Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.

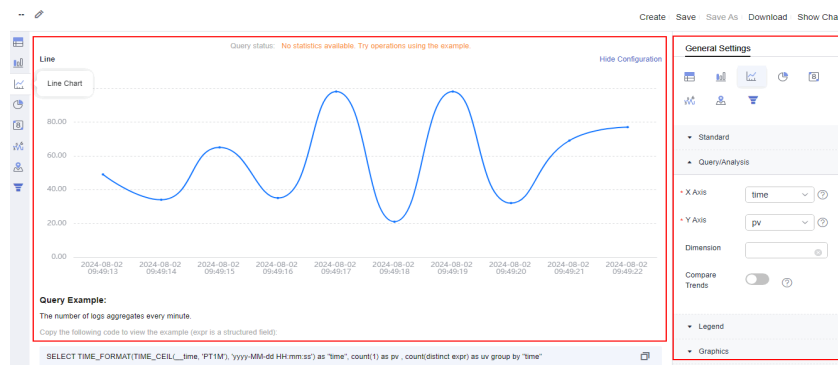


**Step 4** Choose **Log Analysis**.

**Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.

**Step 6** Click  to display the queried data in a line chart. Set parameters in the **General Settings** right pane by referring to [Table 6-6](#).

**Figure 6-3** Line chart



**Table 6-6** Line chart parameters

Type	Parameter	Description
Standard	Format	Select <b>K,Mil,Bil, 1,000,000</b> , or <b>Byte,KB,MB</b> from the drop-down list to specify the format of the Y axis.
	Unit	Customize the unit of the Y axis.
	Decimal Places	Sets the number of decimal places to be displayed.
	Title Font Size	Sets the font size of the chart title.
Query/ Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
	Dimension	Select a value from the drop-down list. Generally, it is an ordinal variable.
	Compare Trends	This function can be enabled when the X axis shows time data and <b>Dimension</b> is not specified.  After this function is enabled, set <b>Comparison</b> to a duration less than or equal to 24 hours. After the setting is complete, compare the data of the current time with the object time data.

Type	Parameter	Description
Legend	Hide Legend	After this function is enabled, you can hide the legend and comparison results.
	Legend Position	Select <b>Top</b> or <b>Right</b> .
	Comparison Value	Indicates whether to display the maximum value, minimum value, average value, and sum value. You can select multiple options.
Graphics	Line Shape	Line type. Select <b>Straight</b> or <b>Curved</b> .
	Line Width	Width of a polyline.
	Show Data Markers	Whether to display the connection points.
	Top Margin	Specifies the distance between the axis and the upper boundary of the graph.
	Bottom Margin	Specifies the distance between the axis and the lower boundary of the graph.
	Left Margin	Specifies the distance between the axis and the left boundary of the graph.
	Right Margin	Specifies the distance between the axis and the right boundary of the graph.
Tooltip	Sort By	Dialog box configuration. When multiple Y-axis data records are selected, they can be sorted and displayed.
X Axis	Show	After this function is enabled, data on the X axis is displayed.
	X Axis Title	Title of the X axis.
Y Axis	Show	After this function is enabled, the Y axis data is displayed.
	Y Axis Title	Title of the Y axis.
	Position	Position of the Y axis. Select <b>Left</b> or <b>Right</b> .

----End

## 6.2.5 Pie Chart

A pie chart shows the proportion of different categories. Different categories are compared by radian. A pie is divided into multiple sectors based on the proportion of each category. The entire pie indicates the total volume. Each sector indicates the proportion of the category to the total. The sum of all sectors is 100%. A pie chart contains the following elements:

- Sector
- Text percentage
- Legend

## Checking Pie Charts


**Step 1** Log in to the LTS console.

**Step 2** In the navigation pane, choose **Log Management**.

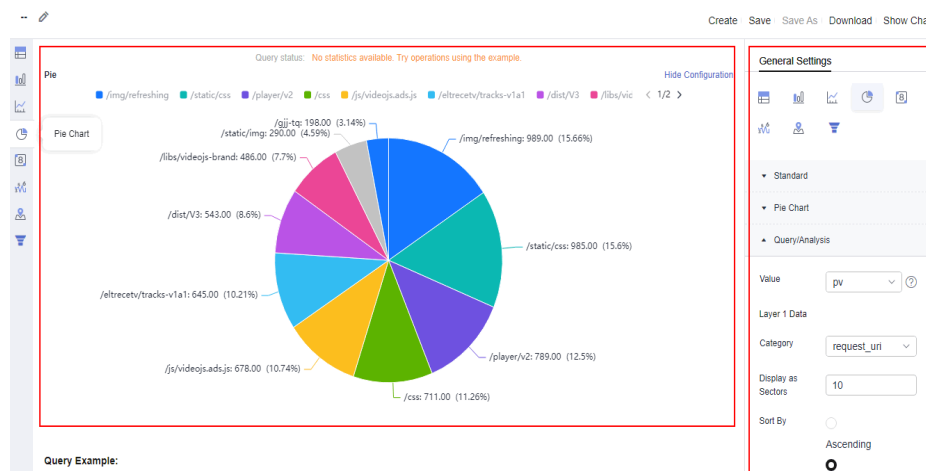
**Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.

**Step 4** Choose **Log Analysis**.

**Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.

**Step 6** Click  to display the queried data in a pie chart. Set parameters in the **General Settings** right pane by referring to [Table 6-7](#).

**Figure 6-4** Pie chart



**Table 6-7** Pie chart parameters

Type	Parameter	Description
Standard	Format	Select <b>K,Mil,Bil, 1,000,000</b> , or <b>Byte,KB,MB</b> from the drop-down list to specify the format of the Y axis.
	Unit	Customize the unit of the Y axis.
	Decimal Places	Sets the number of decimal places to be displayed.
	Title Font Size	Sets the font size of the chart title.

Type	Parameter	Description
Pie Chart	Pie Chart Type	<p>Includes pie, cyclic, and Coxcomb charts.</p> <ul style="list-style-type: none"> <li> <b>Pie</b>            A pie chart displays the percentage of each part in the whole. It divides a circle into different sectors. The area (or arc length and center angle) of each sector corresponds to the proportion of the data represented by the sector. In this way, the relationship between each part and the whole is intuitively displayed.         </li> <li> <b>Cyclic</b>            Essentially, a cyclic chart hollows out the center of a pie chart. Cyclic charts are better than pie charts in the following aspects:           <ul style="list-style-type: none"> <li>Cyclic charts display more information such as the total number.</li> <li>It is not intuitive to compare two pie charts directly. You can compare two cyclic charts by the cyclic bar length.</li> </ul> </li> <li> <b>Coxcomb</b>            A Coxcomb chart is not a cyclic chart in essence. Instead, it is a bar chart drawn in the polar coordinate system. Each category is evenly divided by an arc. The radius of the arc indicates the data size. Coxcomb charts are better than pie charts in the following aspects:           <ul style="list-style-type: none"> <li>A pie chart can contain a maximum of 10 categorized data records, while a Coxcomb chart can contain 10 to 30 data records.</li> <li>Because the radius and area are squared, a Coxcomb chart magnifies the difference between the values of each category. It is suitable for comparing the values of similar sizes.</li> <li>Due to the periodicity of a circle, a Coxcomb chart is also suitable for displaying data by time period, such as by week and month.</li> </ul> </li> </ul>
	Show Scale	After this function is enabled, text labels are displayed on the pie chart to describe data details, such as the value and name.
	Scale Text	This parameter can be set to <b>Category, Percent, Category: %</b> , or <b>Category: Value (%)</b> .


Type	Parameter	Description
	Label Position	After <b>Show Scale</b> is enabled, you can set this parameter to adjust the position of the label in the chart.
Query/ Analysis	Value	Specifies the value corresponding to the categorized data.
	Layer 1 Data	
	Category	Specifies the categorized data.
	Display as Sectors	Specifies the number of pie sectors to be displayed.
	Sort By	Specifies the ascending or descending order.
	Display Rest as Others	Specifies whether to display the data of other types as <b>Other</b> .
	Add Layer	Click <b>Add Layer</b> and set the data of the second layer. The data of each layer includes the category, display sectors, sorting mode, and displaying rest sectors as others.
Legend	Hide Legend	After this function is enabled, you can hide the legend and its content.
	Legend	Select <b>Value</b> or <b>Percent</b> , or both.
	Legend Position	Position of the legend in the chart. Select <b>Top</b> or <b>Right</b> .
Graphics	Outer Radius	Specifies the outer radius of the pie chart. The value ranges from 40 to 100.
	Inside Radius	Specifies the inside radius of the pie chart. The value ranges from 0 to 100.
	Top Margin	Specifies the distance between the axis and the upper boundary of the graph.
	Bottom Margin	Specifies the distance between the axis and the lower boundary of the graph.
	Left Margin	Specifies the distance between the axis and the left boundary of the graph.
	Right Margin	Specifies the distance between the axis and the right boundary of the graph.

----End

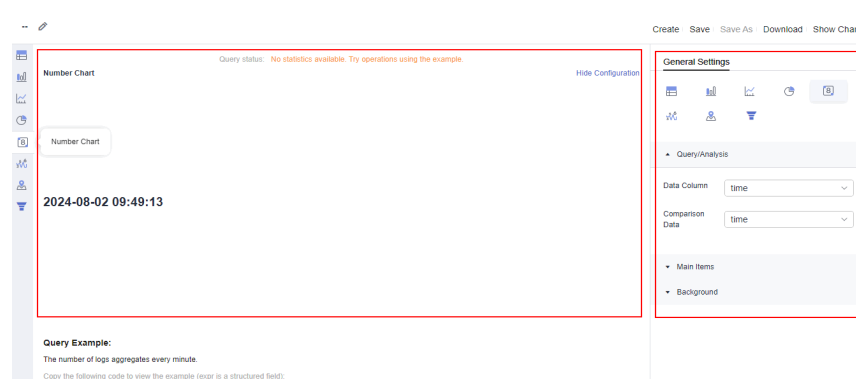
## 6.2.6 Number Chart

A number chart is usually used to represent a single data point or key metric. It can better display the relative size of information and data of the same type. The number chart is ideal for displaying key information and data that needs to be highlighted. It allows users to quickly and intuitively understand data trends and key metrics.

### Checking Number Charts

- Step 1** Log in to the LTS console.
- Step 2** In the navigation pane, choose **Log Management**.
- Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.
- Step 4** Choose **Log Analysis**.
- Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.
- Step 6** Click  to display the queried data in a number chart. Set parameters in the **General Settings** right pane by referring to [Table 6-8](#).

**Figure 6-5** Number chart



**Table 6-8** Number chart parameters

Type	Parameter	Description
Query/ Analysis	Data Column	Numeric or string data is supported.
	Comparison Data	Select a field to compare. The value of the field is displayed in the chart.
Main Items	Title Font Size	Sets the font size of the chart title.
	Format	Displays data in the specified format.
	Data Text Size	Font size of the displayed value. The value ranges from 12 px to 80 px.

Type	Parameter	Description
	Data Unit	Unit of the displayed value.
	Unit Text Size	Font size of the displayed value unit. The value ranges from 12 px to 50 px.
	Decimal Places	Sets the number of decimal places to be displayed.
	Add Comparison Data	After this function is enabled, the value of the field to compare is displayed.
	Comparison Formatting	Displays the data to compare in the specified format.
	Comparison Data Text Size	Font size of the value to compare. The value ranges from 12 px to 50 px.
	Comparison Data Unit	Unit to compare.
	Comparison Unit Text Size	Font size of the value unit to compare. The value ranges from 12 px to 50 px.
	Description	Description of the displayed value and comparison trend. The description is displayed below the value.
Background	Background	Background color of a chart, which can be dark or light.


----End

## 6.2.7 Digital Line Chart

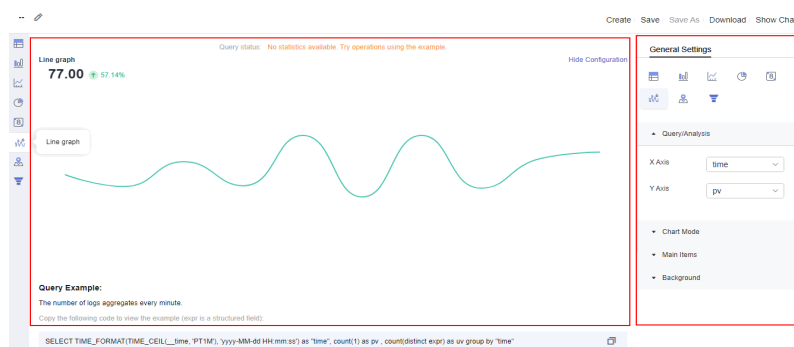
A digital line chart combines a line chart and a number chart to display the trend and key data points at the same time. This helps users better understand data and its change trend to make better service decisions.

### Checking Digital Line Charts

- Step 1** Log in to the LTS console.
- Step 2** In the navigation pane, choose **Log Management**.
- Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.
- Step 4** Choose **Log Analysis**.
- Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.

**Step 6** Click  to display the queried data in a digital line chart. Set parameters in the **General Settings** right pane by referring to [Table 6-9](#).

**Figure 6-6** Digital line chart



**Table 6-9** Digital line chart parameters

Type	Parameter	Description
Query/ Analysis	X Axis	Numeric or string data is supported.
	Y Axis	Numeric or string data is supported. You can select multiple data records.
Chart Mode	Line Shape	Line type. Select <b>Straight</b> or <b>Curved</b> .
Main Items	Title Font Size	Sets the font size of the chart title.
	Number Format	Displays data in the specified format.
	Data Text Size	Font size of the displayed value. The value ranges from 12 px to 80 px.
	Data Unit	Unit of the displayed value.
	Unit Text Size	Font size of the displayed value unit. The value ranges from 12 px to 50 px.
	Decimal Places	Sets the number of decimal places to be displayed.
Background	Background	Background color of a chart, which can be dark or light.

----End

## 6.2.8 Map

A map is used as the background to display geographic data in different colors and marks. Maps provided by LTS include the China map and the world map. After you use specific functions (**ip\_to\_province** for the China map and **ip\_to\_country** for the world map) in query and analysis statements, LTS displays analysis results on a map.



A map contains the following elements:

- Map canvas
- Color block

## Checking Maps


**Step 1** Log in to the LTS console.

**Step 2** In the navigation pane, choose **Log Management**.

**Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.

**Step 4** Choose **Log Analysis**.

**Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.

**Step 6** Click  to display the queried data in a map. Set parameters in the **General Settings** right pane by referring to [Table 6-10](#).

**Figure 6-7** Map



**Table 6-10** Map parameters


Parameter	Description
Map Type	Sets the region range displayed on the map, including the provincial map of China and the world map.
Province	If the map type is a provincial map of China, this field indicates a specific province, for example, Zhejiang province.
Country/Region	If the map type is a world map, the value of this field is a specific country, for example, China.
Data Column	Select the field whose value needs to be displayed.
Title Font Size	Sets the font size of the chart title.

----End

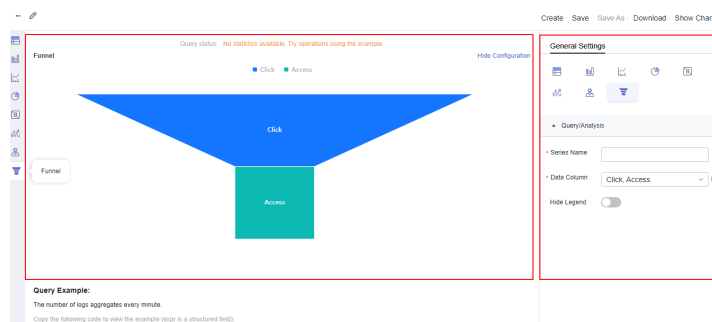
## 6.2.9 Funnel Chart

A funnel chart is applicable to unidirectional analysis of a single process with standard service procedure, long period, and many phases. By comparing service data in each phase of the procedure, you can intuitively find and describe the phase where a problem occurs and make decisions to solve the problem. The funnel chart uses a trapezoidal area to indicate the difference between the service volume of a phase and that of the previous phase.

### Checking Funnel Charts

- Step 1** Log in to the LTS console.
- Step 2** In the navigation pane, choose **Log Management**.
- Step 3** On the **Log Management** page, select the target log group and log stream. The log stream details page is displayed.
- Step 4** Choose **Log Analysis**.
- Step 5** Enter a query and analysis statement by referring to [SQL Analysis Syntax](#), set the time range, and click **Search**.
- Step 6** Click  to display the queried data in a funnel chart. Set parameters in the **General Settings** right pane by referring to [Table 6-11](#).

**Figure 6-8** Funnel chart



**Table 6-11** Funnel chart parameters

Parameter	Description
Series Name	Name of a funnel chart.
Data Column	Select a numeric field. The larger the value of a field, the higher the position of the field.
Hide Legend	After this function is enabled, you can hide the legend names above the funnel chart.

----End

## 6.3 Visualizing Logs in Dashboards

### 6.3.1 Creating a Dashboard

Dashboards serve as data visualization tools that summarize and display key performance metrics, important data, and analysis results. They offer a comprehensive overview of service or system statuses.

LTS provides various dashboard templates to visualize log data or retain statistical charts derived from queries and analyses.

#### NOTE

Currently, this function is available to all users in regions CN South-Guangzhou, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN-Hong Kong, CN Southwest-Guiyang1, AP-Singapore, and CN North-Beijing1. It is also available to whitelisted users in regions CN South-Shenzhen, AP-Bangkok, ME-Riyadh, and AP-Jakarta.

#### Prerequisites

- Logs have been collected.
- Logs have been structured. For details, see [Log Structuring](#).

#### Constraints

- Up to 100 dashboards can be created in an account.
- Up to 100 charts can be created for a log stream.
- Up to 50 charts can be added to a dashboard.

#### Creating a Dashboard

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Click . In the **Add Dashboard Group** dialog box, enter a group name.

#### NOTE

A group name can contain up to 64 characters, including letters, digits, hyphens (-), underscores (\_), and periods (.). Do not start or end with a period or underscore (\_).

**Step 3** Click **OK**. The group is created.

**Step 4** Click **Add Dashboard**. On the displayed page, set parameters by referring to [Table 6-12](#).

**Table 6-12** Parameters for creating a dashboard

Parameter	Description
Dashboard Name	<p>Enter a unique name to differentiate your dashboard from other dashboards in the log stream.</p> <p>The value can contain up to 255 characters and cannot start or end with a period (.). Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.</p>
Enterprise Project Name	<p>Select the required enterprise project. The default value is <b>default</b>. You can click <b>View Enterprise Projects</b> to view all enterprise projects.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• An enterprise project can be used only after it is enabled. For details, see <a href="#">Enabling the Enterprise Project Function</a>.</li> <li>• Then, resources of this enterprise project can be removed. For details, see <a href="#">Removing Resources from an Enterprise Project</a>.</li> </ul>
Add to Dashboard Group	<p>Add the created dashboard to a group for management.</p> <p>If this parameter is disabled, the created dashboard will be added to the system's default group.</p> <p>If this parameter is enabled, the created dashboard will be added to a group based on the group type you selected.</p> <ul style="list-style-type: none"> <li>• <b>Existing:</b> Select an existing dashboard group.</li> <li>• <b>Create:</b> Enter a dashboard group name to create one.</li> </ul>
Lite Mode	<p>Set whether to display the dashboard page in lite mode.</p> <ul style="list-style-type: none"> <li>• If you enable this mode, the buttons for editing and deleting the dashboard and adding filters will not be displayed on the dashboard.</li> <li>• If you disable this mode, the buttons for editing and deleting the dashboard and adding filters will be displayed on the dashboard.</li> </ul>
Add Chart	<p><b>Custom:</b> Select log streams' charts to add to the dashboard.</p> <ol style="list-style-type: none"> <li>1. Click <b>Add Chart</b> under <b>Custom</b>.</li> <li>2. Select one or more log streams, select one or more charts by clicking their check box ( <input type="checkbox"/> ), and click <b>OK</b>. On the dashboard details page displayed, adjust the charts as required and click <b>Save</b>.</li> <li>3. If there are no suitable charts or no charts at all in a log stream, click <b>Create Chart</b> to create one.</li> </ol>

Parameter	Description
	<p><b>Using Dashboard Templates:</b> You can select a custom template (extracted from a created dashboard) or a system template (LTS's built-in template, which cannot be modified).</p> <ol style="list-style-type: none"> <li>1. In the <b>Add Chart</b> area, click <b>Use Dashboard Templates</b>.</li> <li>2. Select a dashboard template and click <b>Next</b>. Select one or more log streams by clicking <input type="checkbox"/>, and click <b>OK</b>.</li> </ol>


**Step 5** The created dashboard will be displayed in the dashboard list.

- Click **Edit** in the **Operation** column of the dashboard to change the dashboard name and lite mode.
- Click **Move** in the **Operation** column of the dashboard to change the group.
- Click **Delete** in the **Operation** column of the dashboard to delete it.

----End

## Creating a Chart for a Dashboard

**Step 1** In the lower part of the dashboard directory, select a dashboard group and click the name of the target dashboard to access its details page.

**Step 2** Click  in the upper right corner. On the displayed page, select a log stream. Then click **Create Chart**.

**Step 3** On the **Add Chart** page displayed, click **Create**, set parameters by referring to [Table 6-13](#), and click **OK**.

**Table 6-13** Creating a chart

Parameter	Description
Chart Name	<p>Enter a unique name to differentiate your chart from other charts in the log stream.</p> <p>Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), spaces, brackets, and periods (.). Do not start or end with a period or space.</p>
SQL Statement	<ul style="list-style-type: none"> <li>• The default statement is <b>SELECT *</b>, which is used to query structured log data in the log stream.</li> <li>• For details about SQL statements, see <a href="#">SQL Analysis Syntax</a>.</li> </ul>
Chart Type	LTS provides various chart types, including tables, bar charts, and line charts.

Parameter	Description
Add to Dashboard	<ul style="list-style-type: none"> <li>If you enable this option, select one or more dashboards to add the chart to them.</li> <li>If you disable this option, the chart will not be displayed on any dashboard.</li> </ul>






**Step 4** Click **OK**.











----End









## Related Operations

After a dashboard is created, click the dashboard name to go to the details page. You can edit and remove its chart, and adjust chart positions. For details, see [Table 6-14](#).

**Table 6-14** Related operations

Operation	Description
Edit chart	Move the cursor to the upper right corner of a chart, click  , and select <b>Edit</b> from the drop-down list to edit the chart. For details, see <a href="#">Analyzing Logs in LTS</a> .
Remove chart	Move the cursor to the upper right corner of a chart, click  , select <b>Remove</b> from the drop-down list, and click <b>Save</b> .
Relocate chart	Move the cursor to a chart, drag the chart to the desired location on the dashboard, and click <b>Save</b> .
Resize chart	Move the cursor to the lower right corner of a chart, drag the corner to adjust the chart size, and click <b>Save</b> .
Modify filter	Move the cursor to the upper right corner of a filter, click  , and select <b>Modify</b> from the drop-down list. On the displayed page, edit the filter by referring to <a href="#">Adding a Filter</a> .
Copy filter	Move the cursor to the upper right corner of a filter, click  , and select <b>Copy</b> from the drop-down list. On the displayed page, click <b>OK</b> to copy the filter.
Delete filter	Move the cursor to the upper right corner of a filter, click  , and select <b>Delete</b> from the drop-down list. In the displayed <b>Delete Filter</b> dialog box, click <b>OK</b> to delete the filter.
Resize filter	Move the cursor to the lower right corner of a filter, drag the corner to adjust the filter size, and click <b>Save</b> .

Operation	Description
Enable auto refresh	Click  in the upper right corner, and enable auto refresh with a specified interval to refresh the data in all charts. The interval can be 1, 5, and 15 minutes.
Manually refresh	Select a dashboard and click  to manually refresh it.
View dashboard in full screen	Select a dashboard and click  to view the dashboard in full screen. In the full-screen mode, you can select <b>Stay Logged In</b> so that your account will not be logged out after a period of inactivity.
Exit full screen of dashboard	Move the cursor to the upper part of the screen and click  , or  , or press <b>Esc</b> on the keyboard.
View chart in full screen	Select a dashboard and click <b>Cancel</b> to exit the editing mode. Move the cursor to the upper right corner of a chart, click  , and select <b>Full Screen</b> from the drop-down list.
Exit full screen of chart	Move the cursor to the upper part of the screen and click  , or click  and select <b>Exit Full Screen</b> from the drop-down list, or press <b>Esc</b> on the keyboard.
Manually refresh chart	Select a dashboard, move the cursor to the upper right corner of a chart, click  , and select <b>Refresh</b> from the drop-down list. Alternatively, in full-screen mode, click  and select <b>Refresh</b> from the drop-down list.

Operation	Description
Set time range	<p>Select a dashboard and click the  1 hour(From now) ▾ drop-down list box before  .</p> <p>There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• <b>From now:</b> 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 <b>1 hour</b> 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.</li> <li>• <b>From last:</b> 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 <b>1 hour</b> 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.</li> <li>• <b>Specified:</b> queries log data that is generated in a specified time range.</li> </ul>
View chart details	<p>Select a dashboard, move the cursor to the upper right corner of a chart, click  , and select <b>View Details</b> from the drop-down list.</p>
Add alarm rules	<p>Select a dashboard, move the cursor to the upper right corner of a chart, click  , and select <b>Add Alarm Rule</b> from the drop-down list.</p>
Copy	<p>Select a dashboard, move the cursor to the upper right corner of a chart, click  , and select <b>Copy</b> from the drop-down list.</p>
Copy to other dashboards	<p>Select a dashboard, move the cursor to the upper right corner of a chart, click  , and select <b>Copy to Other Dashboards</b> from the drop-down list.</p>
Copy statement	<p>Select a dashboard, move the cursor to the upper right corner of a chart, click  , and select <b>Copy Statement</b> from the drop-down list.</p>
Export chart data	<p>Select a dashboard, move the cursor to the upper right corner of a chart, click  , and select <b>Export Chart Data</b> from the drop-down list.</p>



## 6.3.2 Adding a Dashboard Filter

Add filters to a dashboard so that you can filter data or replace data with variables.

Filters are used to modify query criteria for all statistical charts in a dashboard in batches. Each statistical chart is actually the results of a query and analysis statement.

- Filter type: Filter logs by log field key and value. To apply a filter, add it as a filtering condition before your query and analysis statement, and use **AND** or **NOT** to link the condition and statement. For example, *Key: Value AND [search query] | [SQL query]* indicates that logs containing *Key:Value* are searched for within the results of the original query and analysis statement. For this filter type, you can select or enter one or more values, which are connected by an **OR** relationship.
- Time series filter type: Labels and values are dynamically added for filtering. When adding a filter, you can add filter criteria, which are logically connected by AND.

### Prerequisites

- Logs have been collected.
- Charts have been added to a dashboard.
- A log structuring rule has been configured for the log stream. For details, see [Setting Cloud Structuring Parsing](#).


### Constraints

Up to 10 filters can be added for a dashboard.

### Adding a Filter

**Step 1** Log in to the LTS console, choose **Dashboards** in the navigation pane, and select a dashboard.

**Step 2** Click the dashboard name to go to the details page.


**Step 3** Click . On the **Filter** page, set the filter parameters by referring to [Adding a Dashboard Filter](#).

#### NOTE

Fields of the numeric type cannot be filtered.

**Table 6-15** Filter parameters

Parameter	Description
Filter Name	Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. It cannot start with a period or underscore, or end with a period.

Parameter	Description
Operator	Specify the relationship between filter criteria and chart query statements. The value can be <b>AND</b> (default) or <b>NOT</b> .
Key	The field to be filtered. Use only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore, end with a period, or use only digits.
Key Alias	Alias of the key, which is used to distinguish fields. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. It cannot start with a period or underscore, or end with a period.
Static Values	<p>Set the value corresponding to the key. You can click <b>Add</b> multiple times to add more values.</p> <p>Set the following parameters for adding a value:</p> <ul style="list-style-type: none"> <li>• <b>Value:</b> name of a value. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. It cannot start with a period or underscore, or end with a period.</li> <li>• <b>Alias:</b> alias of the value.</li> <li>• <b>Default Value:</b> If you enable this parameter, the value will be set as a default value for the key.</li> <li>• <b>Operation:</b> Click  to delete the value.</li> </ul>

Parameter	Description
Add Dynamic Value	<p>The dynamic values are the query results of the corresponding query and analysis statements. The query results change dynamically in different time ranges.</p> <ul style="list-style-type: none"> <li>• If <b>Add Dynamic Value</b> is disabled, the dynamic change of the query results cannot be set.</li> <li>• Enable this parameter to add a dynamic value for the key, displaying the dynamic changes of the query results. Set the following parameters: <ul style="list-style-type: none"> <li><b>Log Group:</b> Select the log group to be queried.</li> <li><b>Log stream:</b> Select the log stream to be queried.</li> <li><b>SQL Engine Version:</b> Select <b>Pipe character</b> or <b>Non-pipe character</b>. The default SQL query syntax of the pipe character version is <code>*   select *</code>, and that of the non-pipe character version is <code>select *</code>.</li> <li><b>Dynamic Value Source:</b> You can choose <b>fuzzy match</b> or <b>SQL query</b>.</li> <li><b>Fuzzy match:</b> Select structured fields configured for the current log stream.</li> <li><b>SQL query:</b> Enter a SQL query statement. Click <b>Search</b> to preview the dynamic value.</li> </ul> </li> </ul>

**Step 4** Click **OK**.

----End

## 6.3.3 Dashboard Templates

### 6.3.3.1 APIG Dashboard Templates

APIG is your fully managed API hosting service with high performance, availability, and security. With APIG, you can build, manage, and deploy APIs at any scale to package your capabilities and sell them at KooGallery. With just a few clicks, you can integrate your internal systems and selectively expose and monetize your service capabilities with minimal cost and risk. APIG helps you lower R&D costs and improve operational efficiency, freeing you to focus on your core business.

APIG dashboard templates support [Viewing APIG Access Center](#), [Viewing APIG Monitoring Center](#), and [Viewing APIG Monitoring by the Second](#).

#### Prerequisites

- Logs have been collected from APIG. For details, see [Ingesting APIG Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

## Viewing APIG Access Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **APIG dashboard templates** under **Dashboard Templates** and click **APIG access center** to view the chart details.

- Filter by requested domain name. The associated query and analysis statement is:  

```
select distinct(host)
```
- Filter by application ID. The associated query and analysis statement is:  

```
select distinct(app_id)
```
- **PV Distribution (Global)**. The associated query and analysis statement is:  

```
SELECT ip_to_country(my_remote_addr) as country,sum(ori_pv) as PV from (select my_remote_addr, count(1) as ori_pv group by my_remote_addr ORDER BY ori_pv desc LIMIT 10000) GROUP BY country HAVING country not in ('','Reserved address','*')
```
- **Average Latency Distribution (China)**. The associated query and analysis statement is:  

```
SELECT province,round(CASE WHEN "Average latency (ms)" > 0 THEN "Average latency (ms)" ELSE 0 END, 3) AS "Average latency (ms)"FROM (SELECT ip_to_province(my_remote_addr) as province,sum(rt)/sum(ori_pv) * 1000 AS "Average latency (ms)" from (select my_remote_addr, sum(request_time) as rt,count(1) as ori_pv group by my_remote_addr ORDER BY ori_pv desc LIMIT 10000) WHERE IP_TO_COUNTRY (my_remote_addr) = 'China' GROUP BY province) where province not in ('','Reserved address','*')
```
- **Average Latency Distribution (Global)**. The associated query and analysis statement is:  

```
SELECT country,round(CASE WHEN "Average latency (ms)" > 0 THEN "Average latency (ms)" ELSE 0 END, 2) AS "Average latency (ms)"FROM (SELECT ip_to_country(my_remote_addr) as country,sum(rt)/sum(ori_pv) * 1000 AS "Average latency (ms)" from (select my_remote_addr, sum(request_time) as rt,count(1) as ori_pv group by my_remote_addr ORDER BY ori_pv desc LIMIT 10000) GROUP BY country) where country not in ('','Reserved address','*')
```
- **PV/UV Today**. The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_ , 'yyyy-MM-dd HH:mm:ss') as _time_PV,UV FROM (select TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT600S') AS _time_ , count(1) as PV, APPROX_COUNT_DISTINCT(my_remote_addr) as UV from log WHERE __time <= CURRENT_TIMESTAMP and __time >= DATE_TRUNC('DAY',(CURRENT_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR group by _time_ order by _time_)
```
- **Top 10 Provinces by Visits**. The associated query and analysis statement is:  

```
select ip_to_province(my_remote_addr) as "province", sum(ori_pv) as "Visits" from(select my_remote_addr, count(1) as ori_pv group by my_remote_addr ORDER BY ori_pv desc LIMIT 10000)group by "province" HAVING "province" <> '-1' order by "Visits" desc limit 10
```
- **Top 10 Cities by Visits**. The associated query and analysis statement is:  

```
select ip_to_city(my_remote_addr) as "city", sum(ori_pv) as "Visits" from(select my_remote_addr, count(1) as ori_pv group by my_remote_addr ORDER BY ori_pv desc LIMIT 10000) group by "city" HAVING "city" <> '-1' order by "Visits" desc limit 10
```
- **Top 10 Hosts by Visits**. The associated query and analysis statement is:  

```
select host as "Host", count(1) as "PV" group by "Host" order by "PV" desc limit 10
```
- **Top 10 UserAgents by Visits**. The associated query and analysis statement is:  

```
select http_user_agent as "UserAgent", count(1) as "PV" group by "UserAgent" order by "PV" desc limit 10
```

- **Device Distribution by Type.** The associated query and analysis statement is:  

```
select case when regexp_like(lower(http_user_agent), 'iphone|ipod|android|ios') then 'Mobile' else 'PC' end as type , count(1) as total group by type
```
  - **Device Distribution by System.** The associated query and analysis statement is:  

```
select case when regexp_like(lower(http_user_agent), 'iphone|ipod|ios') then 'IOS' when regexp_like(lower(http_user_agent), 'android') then 'Android' else 'other' end as type , count(1) as total group by type HAVING type != 'other'
```
  - **TOP URL.** The associated query and analysis statement is:  

```
select router_uri , count(1) as pv, APPROX_COUNT_DISTINCT(my_remote_addr) as UV, round(sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1), 2) as "Access Success Rate" group by router_uri ORDER by pv desc
```
  - **Top IP Addresses by Visits.** The associated query and analysis statement is:  

```
select my_remote_addr as "Source IP Address",ip_to_country(my_remote_addr) as "Country/Region",ip_to_province(my_remote_addr) as "Province",ip_to_city(my_remote_addr) as "City",ip_to_provider(my_remote_addr) as "Carrier",count(1) as "PV" group by my_remote_addr ORDER by "PV" desc limit 100
```
- End

## Viewing APIG Monitoring Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **APIG dashboard templates** under **Dashboard Templates** and click **APIG monitoring center** to view the chart details.

- **Filter by requested domain name.** The associated query and analysis statement is:  

```
select distinct(host)
```
- **Filter by application ID.** The associated query and analysis statement is:  

```
select distinct(app_id)
```
- **PV.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_ , 'yyyy-MM-dd HH:mm:ss') as _time_ ,PV FROM (SELECT TIME_CEIL (TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'), 'PT300S') AS _time_ , count(1) AS PV FROM log GROUP BY _time_)
```
- **Request Success Rate.** The associated query and analysis statement is:  

```
select ROUND(sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1),2) as cnt
```
- **Average Latency.** The associated query and analysis statement is:  

```
select round(avg(request_time) * 1000, 3) as cnt
```
- **4xx Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "status" >= 400 and "status" < 500
```
- **404 Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "status" = 404
```
- **429 Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "status" = 429
```
- **504 Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "status" = 504
```
- **5xx Requests.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_ , 'yyyy-MM-dd HH:mm:ss') as _time_ ,cnt FROM (SELECT TIME_CEIL (TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'), 'PT300S') AS _time_ , count(1) AS cnt FROM log where "status" >= 500 GROUP BY _time_)
```
- **Status Code Distribution.** The associated query and analysis statement is:  

```
SELECT status, COUNT(1) AS rm GROUP BY status
```
- **UV.** The associated query and analysis statement is:

```
SELECT TIME_FORMAT(_time_, 'yyyy-MM-dd HH:mm:ss') as _time_UV FROM (select
TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT600S') AS _time_ ,
APPROX_COUNT_DISTINCT(my_remote_addr) as UV from log group by _time_)
```

- Traffic.** The associated query and analysis statement is:

```
select TIME_FORMAT(_time_,'yyyy-MM-dd HH:mm:ss') AS _time_,round(CASE WHEN "Inbound" > 0
THEN "Inbound" ELSE 0 END, 2) AS "Inbound",round(CASE WHEN "Outbound" > 0 THEN
"Outbound" ELSE 0 END, 2) AS "Outbound" FROM (SELECT TIME_CEIL(TIME_PARSE(time_local,
'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT600S') AS _time_,sum(request_length) / 1024.0 AS
"Inbound",sum(bytes_sent) / 1024.0 AS "Outbound" group by _time_)
```
- Access Failure Rate.** The associated query and analysis statement is:

```
SELECT TIME_FORMAT(_time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round(CASE WHEN "Failure rate"
> 0 THEN "Failure rate" ELSE 0 END, 2) AS "Failure rate",round(CASE WHEN "5xx Requests" > 0
THEN "5xx Requests" ELSE 0 END, 2) AS "5xx Requests" from (select
TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT600S') AS _time_,sum(case
when status >= 400 then 1 else 0 end) * 100.0 / count(1) as 'Failure rate' , sum(case when status
>=500 THEN 1 ELSE 0 END)*100.0/COUNT(1) as '5xx Requests' group by _time_)
```
- Latency.** The associated query and analysis statement is:

```
select TIME_FORMAT(_time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round(CASE WHEN "Avg." > 0
THEN "Avg." ELSE 0 END, 2) AS "Avg.",round(CASE WHEN "P50" > 0 THEN "P50" ELSE 0 END, 2)
AS "P50",round(CASE WHEN "P90" > 0 THEN "P90" ELSE 0 END, 2) AS "P90",round(CASE WHEN
"P99" > 0 THEN "P99" ELSE 0 END, 2) AS "P99",round(CASE WHEN "P9999" > 0 THEN "P9999" ELSE
0 END, 2) AS "P9999" from (select TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss
ZZ'),'PT600S') as _time_,avg(request_time) * 1000 as "Avg.", APPROX_QUANTILE_DS("request_time",
0.50)*1000 as "P50", APPROX_QUANTILE_DS("request_time", 0.90)*1000 as
"P90",APPROX_QUANTILE_DS("request_time", 0.99)*1000 as
"P99",APPROX_QUANTILE_DS("request_time", 0.9999)*1000 as 'P9999' group by _time_)
```
- Top Host Requests.** The associated query and analysis statement is:

```
SELECT "host", pv, uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate
(%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0
THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN
"Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN
"Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT
"host", count(1) AS pv, APPROX_COUNT_DISTINCT (my_remote_addr) AS uv, sum(CASE WHEN
"status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)",
avg(request_time) * 1000 AS "Average Latency (ms)", sum(request_length) / 1024.0 AS "Inbound
(KB)", sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "host" != " " GROUP BY "host")
ORDER BY pv DESC
```
- Top Host Latencies.** The associated query and analysis statement is:

```
SELECT "host", pv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate
(%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0
THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "P90
Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE
WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)"
FROM (SELECT "host", count(1) AS pv, sum(CASE WHEN "status" < 400 THEN 1 ELSE 0 END) *
100.0 / count(1) AS "Access Success Rate (%)", avg(request_time) * 1000 AS "Average Latency
(ms)",APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != " "
GROUP BY "host") ORDER BY "Average Latency (ms)" desc
```
- Top Host Failure Rates.** The associated query and analysis statement is:

```
SELECT "host", pv,round(CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)"
ELSE 0 END, 2) AS "Access Failure Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN
"Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "P90
Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE
WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)"
FROM (SELECT "host", count(1) AS pv, sum(CASE WHEN "status" >= 400 THEN 1 ELSE 0 END) *
100.0 / count(1) AS "Access Failure Rate (%)", avg(request_time) * 1000 AS "Average Latency
(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != " "
GROUP BY "host") ORDER BY "Access Failure Rate (%)" desc
```
- Top URL Requests.** The associated query and analysis statement is:

```
SELECT upstream_uri, pv,uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success
Rate (%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)"
> 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN
"Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN
"Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT
```

```
upstream_uri, count(1) AS pv, APPROX_COUNT_DISTINCT (my_remote_addr) AS uv, sum(CASE WHEN "status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)", avg(request_time) * 1000 AS "Average Latency (ms)", sum(request_length) / 1024.0 AS "Inbound (KB)", sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "host" != " " GROUP BY upstream_uri) ORDER BY pv desc
```

- **Top URL Failure Rates.** The associated query and analysis statement is:  
SELECT upstream\_uri, pv, round( CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)" ELSE 0 END, 2 ) AS "Access Failure Rate (%)", round( CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3 ) AS "Average Latency (ms)", round( CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3 ) AS "P90 Latency (ms)", round( CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3 ) AS "P99 Latency (ms)" FROM( SELECT upstream\_uri, count( 1 ) AS pv, sum( CASE WHEN "status" >= 400 THEN 1 ELSE 0 END ) \* 100.0 / count( 1 ) AS "Access Failure Rate (%)", avg( request\_time ) \* 1000 AS "Average Latency (ms)", APPROX\_QUANTILE\_DS(request\_time, 0.9) \* 1000 AS "P90 Latency (ms)", APPROX\_QUANTILE\_DS(request\_time, 0.99) \* 1000 AS "P99 Latency (ms)" WHERE "host" != " " GROUP BY upstream\_uri ) ORDER BY "Access Failure Rate (%)" desc
- **Top Backend Requests.** The associated query and analysis statement is:  
SELECT addr, pv, uv, round( CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)" ELSE 0 END, 2 ) AS "Access Success Rate (%)", round( CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3 ) AS "Average Latency (ms)", round( CASE WHEN "Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3 ) AS "Inbound (KB)", round( CASE WHEN "Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3 ) AS "Outbound (KB)" FROM ( SELECT my\_remote\_addr as addr, count( 1 ) AS pv, APPROX\_COUNT\_DISTINCT ( my\_remote\_addr ) AS uv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) \* 100.0 / count( 1 ) AS "Access Success Rate (%)", avg( request\_time ) \* 1000 AS "Average Latency (ms)", sum( request\_length ) / 1024.0 AS "Inbound (KB)", sum( bytes\_sent ) / 1024.0 AS "Outbound (KB)" WHERE "host" != " " GROUP BY addr having length(my\_remote\_addr) > 2) ORDER BY "pv" desc
- **Top Backend Latencies.** The associated query and analysis statement is:  
SELECT addr,pv,round( CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)" ELSE 0 END, 2 ) AS "Access Success Rate (%)",round( CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3 ) AS "Average Latency (ms)",round( CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3 ) AS "P90 Latency (ms)",round( CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3 ) AS "P99 Latency (ms)" FROM (SELECT my\_remote\_addr as addr,count( 1 ) AS pv,sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) \* 100.0 / count( 1 ) AS "Access Success Rate (%)",avg( request\_time ) \* 1000 AS "Average Latency (ms)",APPROX\_QUANTILE\_DS(request\_time, 0.9) \* 1000 AS "P90 Latency (ms)",APPROX\_QUANTILE\_DS(request\_time, 0.99) \* 1000 AS "P99 Latency (ms)" WHERE "host" != " " and "my\_remote\_addr" != '-' GROUP BY addr ) ORDER BY "Average Latency (ms)" desc
- **Top Backend Failure Rates.** The associated query and analysis statement is:  
SELECT addr, pv, round( CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)" ELSE 0 END, 2 ) AS "Access Failure Rate (%)", round( CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3 ) AS "Average Latency (ms)", round( CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3 ) AS "P90 Latency (ms)", round( CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3 ) AS "P99 Latency (ms)" FROM ( SELECT my\_remote\_addr as addr, count( 1 ) AS pv, sum( CASE WHEN "status" >= 400 THEN 1 ELSE 0 END ) \* 100.0 / count( 1 ) AS "Access Failure Rate (%)", avg( request\_time ) \* 1000 AS "Average Latency (ms)", APPROX\_QUANTILE\_DS(request\_time, 0.9) \* 1000 AS "P90 Latency (ms)", APPROX\_QUANTILE\_DS(request\_time, 0.99) \* 1000 AS "P99 Latency (ms)" WHERE "host" != " " and "my\_remote\_addr" != '-' GROUP BY addr) ORDER BY "Access Failure Rate (%)" desc
- **Top URL Latencies.** The associated query and analysis statement is:  
SELECT upstream\_uri, pv,round( CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)" ELSE 0 END, 2 ) AS "Access Success Rate (%)",round( CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3 ) AS "Average Latency (ms)",round( CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3 ) AS "P90 Latency (ms)",round( CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3 ) AS "P99 Latency (ms)" FROM (SELECT upstream\_uri, count( 1 ) AS pv, sum( CASE WHEN "status" < 400 THEN 1 ELSE 0 END ) \* 100.0 / count( 1 ) AS "Access Success Rate (%)", avg( request\_time ) \* 1000 AS "Average Latency (ms)", APPROX\_QUANTILE\_DS(request\_time, 0.9) \* 1000 AS "P90 Latency (ms)", APPROX\_QUANTILE\_DS(request\_time, 0.99) \* 1000 AS "P99 Latency (ms)" WHERE "host" != " " GROUP BY upstream\_uri ) ORDER BY "Average Latency (ms)" desc

----End

## Viewing APIG Monitoring by the Second

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **APIG dashboard templates** under **Dashboard Templates** and click **APIG monitoring by the second** to view the chart details.

- Filter by requested domain name. The associated query and analysis statement is:  

```
select distinct(host)
```
- Filter by application ID. The associated query and analysis statement is:  

```
select distinct(app_id)
```
- **QPS**. The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT1S'),'yyyy-MM-dd HH:mm:ss') AS __time_ , COUNT(*) as QPS from log group by __time_
```
- **Success Rate**. The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Success rate" > 0 THEN "Success rate" else 0 end,2) as "Success rate" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time, sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1) as 'Success rate' from log group by __time)
```
- **Latency**. The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Access latency" > 0 THEN "Access latency" else 0 end,2) as "Access latency",round(CASE WHEN "Upstream latency" > 0 THEN "Upstream latency" else 0 end,2) as "Upstream latency" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time, avg(request_time)* 1000 as 'Access latency',avg(upstream_response_time)* 1000 as 'Upstream latency' from log group by __time)
```
- **Traffic**. The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Incoming" > 0 THEN "Incoming" ELSE 0 END, 3) AS "Incoming",round(CASE WHEN "Outgoing body" > 0 THEN "Outgoing body" ELSE 0 END, 3) AS "Outgoing body" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'),'PT5S'),'yyyy-MM-dd HH:mm:ss') as __time , sum("request_length") / 1024.0 as "Incoming", sum("body_bytes_sent") / 1024.0 as "Outgoing body" group by __time)
```
- **Status Codes**. The associated query and analysis statement is:  

```
SELECT TIME_CEIL (TIME_PARSE (time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'), 'PT5S') AS "time", SUM(CASE WHEN "status" >= 200 AND "status" < 300 THEN 1 ELSE 0 END) AS "2XX", SUM(CASE WHEN "status" >= 300 AND "status" < 400 THEN 1 ELSE 0 END) AS "3XX", SUM(CASE WHEN "status" >= 400 AND "status" < 500 THEN 1 ELSE 0 END) AS "4XX", SUM(CASE WHEN "status" >= 500 AND "status" < 600 THEN 1 ELSE 0 END) AS "5XX", SUM(CASE WHEN "status" < 200 OR "status" >= 600 THEN 1 ELSE 0 END) AS "Other" FROM log WHERE TIME_PARSE (time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ') IS NOT NULL GROUP BY "time" ORDER BY "time" ASC LIMIT 100000
```
- **Backend Response Codes**. The associated query and analysis statement is:  

```
SELECT TIME_CEIL (TIME_PARSE (time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ'), 'PT5S') AS "time", SUM(CASE WHEN "upstream_status" >= 200 AND "upstream_status" < 300 THEN 1 ELSE 0 END) AS "2XX", SUM(CASE WHEN "upstream_status" >= 300 AND "upstream_status" < 400 THEN 1 ELSE 0 END) AS "3XX", SUM(CASE WHEN "upstream_status" >= 400 AND "upstream_status" < 500 THEN 1 ELSE 0 END) AS "4XX", SUM(CASE WHEN "upstream_status" >= 500 AND "upstream_status" < 600 THEN 1 ELSE 0 END) AS "5XX", SUM(CASE WHEN "upstream_status" < 200 OR "upstream_status" >= 600 THEN 1 ELSE 0 END) AS "Other" FROM log WHERE TIME_PARSE (time_local, 'dd/MMM/yyyy:HH:mm:ss ZZ') IS NOT NULL GROUP BY "time" ORDER BY "time" ASC LIMIT 100000
```

----End

### 6.3.3.2 CCE Dashboard Templates

CCE provides highly scalable, high-performance, enterprise-class Kubernetes clusters.

CCE dashboard templates support [Viewing CCE Logs: Node Operations](#), [Viewing CCE Logs Kubernetes Object Operations](#), [Viewing CCE Logs Kubernetes Event Queries](#), [Viewing CCE Logs Kubernetes Event Center](#), [Viewing CCE Logs](#)



## Aggregation Search, Viewing CCE Logs Account Operations, and Viewing CCE Audit Log Center.

### Prerequisites

- Logs have been collected from CCE. For details, see [Ingesting CCE Application Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

### Viewing CCE Logs: Node Operations

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CCE dashboard templates** under **Dashboard Templates** and click **CCE Logs: Node Operations** to view the chart details.

- Filter by node name. The associated query and analysis statement is:  

```
select distinct("objectRef.name")
```
- Filter by user. The associated query and analysis statement is:  

```
select distinct("user.username")
```
- Filter by status code. The associated query and analysis statement is:  

```
select distinct("responseStatus.code")
```
- Filter by operation type. The associated query and analysis statement is:  

```
select distinct("verb")
```
- **Node Quantity Trend.** The associated query and analysis statement is:  

```
SELECT time_series(TIME_PARSE(LEFT(requestReceivedTimestamp, 23),'yyyy-MM-dd"T"HH:mm:ss.SSS'), 'PT1H', 'yyyy-MM-dd HH', '0') as "dt", count(DISTINCT("objectRef.name")) as "Nodes" where "objectRef.resource" = 'nodes' and "objectRef.subresource" = 'status' and "verb" in ('update', 'patch') and "user.username" = 'system:node' group by "dt" order by "dt" desc limit 10000
```
- **Non-System User Operation Trend.** The associated query and analysis statement is:  

```
SELECT time_series(TIME_PARSE(LEFT(requestReceivedTimestamp, 23),'yyyy-MM-dd"T"HH:mm:ss.SSS'), 'PT1H', 'yyyy-MM-dd HH', '0') as "dt", count(*) as "Requests", "user.username" where "objectRef.resource" = 'nodes' and "user.username" not in ('kube-controller-manager','kube-apiserver-kubelet-client','apiserver') and "user.username" not like 'system:%' and "verb" in ('create','delete','update','patch') group by "dt", "user.username" order by "dt","Requests" desc limit 10000
```
- **create Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'create' group by "Status code"
```
- **delete Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'delete' group by "Status code"
```
- **patch Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'patch' group by "Status code"
```
- **update Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "objectRef.resource" = 'nodes' and "verb" = 'update' group by "Status code"
```
- **Node Blocking/Unblocking Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "requestObject" in ('{"spec":{"unschedulable":false}}','{"spec":{"unschedulable":true}}') group by "Status code"
```
- **Label Codes.** The associated query and analysis statement is:

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where
"objectRef.resource" = 'nodes' and "verb" in ('patch','update') and "requestObject" = 'labels' and
"requestObject" = 'metadata' group by "Status code"
```

- **Taint Codes.** The associated query and analysis statement is:  
select cast("responseStatus.code" as varchar) as "Status code", count(\*) as "count" where  
"objectRef.resource" = 'nodes' and "verb" in ('patch','update') and "requestObject" = 'taints' group by  
"Status code"
- **Eviction Codes.** The associated query and analysis statement is:  
select cast("responseStatus.code" as varchar) as "Status code", count(\*) as "count" where  
"objectRef.subresource" = 'eviction' and "objectRef.resource" = 'pods' and "verb" = 'create' group by  
"Status code"
- **Node Addition/Deletions.** The associated query and analysis statement is:  
select "auditID" AS "Audit ID", "objectRef.name" AS "Node", "verb" AS "Operation",  
"stageTimestamp" AS "Occurred", "user.username" AS "Operator", "responseStatus.code" AS "Status  
Code" where "objectRef.resource" = 'nodes' and "verb" in ('create','delete')
- **Taint Operations.** The associated query and analysis statement is:  
select "auditID" AS "Audit ID", "objectRef.name" AS "Node", "requestObject" AS "Taints",  
"requestReceivedTimestamp" AS "Occurred", "user.username" AS "Operator", "responseStatus.code"  
AS "Status Code" where "objectRef.resource" = 'nodes' and "verb" = 'patch' and "requestObject" =  
'taints'
- **Eviction Operations.** The associated query and analysis statement is:  
select "auditID" AS "Audit ID", "objectRef.name" AS "pod", "sourceIPs" AS "Source IP",  
"requestReceivedTimestamp" AS "Occurred", "user.username" AS "Operator", "responseStatus.code"  
AS "Status Code" where "objectRef.resource" = 'pods' and "verb" = 'create' and  
"objectRef.subresource" = 'eviction'
- **Label Operations.** The associated query and analysis statement is:  
select "auditID" AS "Audit ID", "objectRef.name" AS "Node", "requestObject" AS "Label",  
"requestReceivedTimestamp" AS "Occurred", "user.username" AS "Operator", "responseStatus.code"  
AS "Status Code" where "objectRef.resource" = 'nodes' and "verb" = 'patch' and "requestObject" =  
'labels'
- **Blocking Operations.** The associated query and analysis statement is:  
select "auditID" AS "Audit ID", "objectRef.name" AS "Node", "requestReceivedTimestamp" AS  
"Occurred", "user.username" AS "Operator", "responseStatus.code" AS "Status Code" where "verb" =  
'patch' and "objectRef.resource" = 'nodes' and "requestObject" = 'true' and "requestObject" =  
'unschedulable'
- **Unblocking Operations.** The associated query and analysis statement is:  
select "auditID" AS "Audit ID", "objectRef.name" AS "Node", "requestReceivedTimestamp" AS  
"Occurred", "user.username" AS "Operator", "responseStatus.code" AS "Status Code" where "verb" =  
'patch' and "objectRef.resource" = 'nodes' and "requestObject" not in ('true','taints','unschedulable')

----End

## Viewing CCE Logs Kubernetes Object Operations

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CCE dashboard templates** under **Dashboard Templates** and click **CCE Logs Kubernetes Object Operations** to view the chart details.

- Filter by namespace. The associated query and analysis statement is:  
select distinct("objectRef.namespace")
- Filter by operation type. The associated query and analysis statement is:  
select distinct("verb")
- Filter by status code. The associated query and analysis statement is:  
select distinct("responseStatus.code")
- Filter by resource object. The associated query and analysis statement is:  
select distinct("objectRef.name")
- Filter by resource type. The associated query and analysis statement is:  
select distinct("objectRef.resource")

- **Filter by user.** The associated query and analysis statement is:  

```
select distinct("user.username")
```
- **Major Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16),'T',' ') AS "dt", "verb" as "Operation Type",
count(*) as "count" where "verb" in ('create','delete','update','patch') and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "dt","Operation Type" order by "dt" limit 10000
```
- **Non-System User Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16),'T',' ') AS "dt", count(*) as "Requests
", "user.username" WHERE "user.username" not in ('kube-controller-manager','kube-apiserver-kubelet-
client','apiserver') and "user.username" not like 'system:%' and "verb" in
('create','delete','update','patch') and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','secrets',
'pvc') group by "dt", "user.username" limit 10000
```
- **create Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource type", count(*) as "count" where "verb" = 'create' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "objectRef.resource"
```
- **delete Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource Type", count(*) as "count" where "verb" = 'delete' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "objectRef.resource"
```
- **update Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource Type", count(*) as "count" where "verb" = 'update' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "objectRef.resource"
```
- **patch Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource Type", count(*) as "count" where "verb" = 'patch' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "objectRef.resource"
```
- **create Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'create' and "objectRef.resource"
in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "user.username"
```
- **delete Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'delete' and "objectRef.resource"
in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "user.username"
```
- **update Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'update' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "user.username"select "user.username" as "User", count(*)
as "count" where "verb" = 'update' and "objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "user.username"
```
- **patch Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'patch' and
"objectRef.resource" in
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','config
maps','persistentvolumeclaims') group by "user.username"
```
- **create Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "verb" =
'create' and "objectRef.resource" in
```

```
('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
```

- **delete Codes.** The associated query and analysis statement is:  
select cast("responseStatus.code" as varchar) as "Status code", count(\*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
- **update Codes.** The associated query and analysis statement is:  
select cast("responseStatus.code" as varchar) as "Status code", count(\*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
- **patch Codes.** The associated query and analysis statement is:  
select cast("responseStatus.code" as varchar) as "Status code", count(\*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
- **create Operation Trend.** The associated query and analysis statement is:  
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(\*) as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000
- **delete Operation Trend.** The associated query and analysis statement is:  
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(\*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000
- **update Operation Trend.** The associated query and analysis statement is:  
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(\*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000
- **patch Operation Trend.** The associated query and analysis statement is:  
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(\*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000

----End

## Viewing CCE Logs Kubernetes Event Queries

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CCE dashboard templates** under **Dashboard Templates** and click **CCE Logs Kubernetes Event Queries** to view the chart details.

- **Filter by namespace.** The associated query and analysis statement is:  
select distinct("objectRef.namespace")
- **Filter by operation type.** The associated query and analysis statement is:  
select distinct("verb")
- **Filter by status code.** The associated query and analysis statement is:  
select distinct("responseStatus.code")
- **Filter by resource object.** The associated query and analysis statement is:  
select distinct("objectRef.name")
- **Filter by resource type.** The associated query and analysis statement is:  
select distinct("objectRef.resource")
- **Filter by user.** The associated query and analysis statement is:  
select distinct("user.username")

- **Major Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16), 'T', ' ') AS "dt", "verb" as "Operation Type", count(*) as "count" where "verb" in ('create','delete','update','patch') and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "dt","Operation Type" order by "dt" limit 10000
```
- **Non-System User Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(requestReceivedTimestamp, 16), 'T', ' ') AS "dt", count(*) as "Requests", "user.username" WHERE "user.username" not in ('kube-controller-manager','kube-apiserver-kubelet-client','apiserver') and "user.username" not like 'system:%' and "verb" in ('create','delete','update','patch') and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','secrets','pvcs') group by "dt", "user.username" limit 10000
```
- **create Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource type", count(*) as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "objectRef.resource"
```
- **delete Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource Type", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "objectRef.resource"
```
- **update Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource Type", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "objectRef.resource"
```
- **patch Resources.** The associated query and analysis statement is:  

```
select "objectRef.resource" as "Resource Type", count(*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "objectRef.resource"
```
- **create Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "user.username"
```
- **delete Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "user.username"
```
- **update Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "user.username"select "user.username" as "User", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "user.username"
```
- **patch Users.** The associated query and analysis statement is:  

```
select "user.username" as "User", count(*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "user.username"
```
- **create Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
```

- **delete Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
```
- **update Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
```
- **patch Codes.** The associated query and analysis statement is:  

```
select cast("responseStatus.code" as varchar) as "Status code", count(*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by "responseStatus.code"
```
- **create Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(*) as "count" where "verb" = 'create' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000
```
- **delete Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(*) as "count" where "verb" = 'delete' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000
```
- **update Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(*) as "count" where "verb" = 'update' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000
```
- **patch Operation Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(*) as "count" where "verb" = 'patch' and "objectRef.resource" in ('deployments','statefulsets','cronjobs','daemonsets','jobs','pods','services','ingresses','configmaps','configmaps','persistentvolumeclaims') group by dt, "objectRef.resource" order by dt limit 10000
```

----End

## Viewing CCE Logs Kubernetes Event Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CCE dashboard templates** under **Dashboard Templates** and click **CCE Logs Kubernetes Event Center** to view the chart details.

- **Event Severity:** The options are **Warning** and **Normal**.
- **Filter by event type.** The associated query and analysis statement is:  

```
select distinct("name")
```
- **Filter by cluster ID.** The associated query and analysis statement is:  

```
select distinct("cluster_id")
```
- **Filter by namespace.** The associated query and analysis statement is:  

```
select distinct("namespace")
```
- **Filter by name.** The associated query and analysis statement is:  

```
select distinct("resource_name")
```
- **Contrack Full.** The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as "inc" from (select compare("total", 3600) as diff from(select count(1) as "total" from log where "name"='ContrackFull'))
```
- **Event Sync Error.** The associated query and analysis statement is:

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2) as "inc" from (select
compare("total", 3600) as diff from(select count(1) as "total" from log where "name"=
'NTPIDsDown'))
```

- **Insufficient Node PIDs.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name" in  
( 'PIDPressure','NodeHasPIDPressure' ) )
- **Insufficient Node FDs.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name"=  
'NodeHasFDPressure' )
- **Insufficient Node Disk Space.** The associated query and analysis statement  
is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name"=  
'NodeHasDiskPressure' )
- **Pod OOM.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "reason" in  
( 'OOMKilling','PodOOMKilling' ) )
- **DockerHung.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name"=  
'Failed' and  
"reason" = 'DockerHung' )
- **Node Restart.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name"=  
'NodeRebooted' )
- **Pull Image Failed.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name"=  
'Failed' and  
"reason" = 'ImagePullBackOff' )
- **Node OOM.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name" =  
'SystemOOM' )
- **Start Pod Failed.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100 , 2 ) as "inc" from (select  
compare( "total", 3600) as diff from( select count(1) as "total" from log where "name"=  
'Failed' and  
"resource\_kind" = 'Pod' and "reason" = 'ImagePullBackOff' )
- **Event Distribution.** The associated query and analysis statement is:  
select "type", count(\*) as "Events" group by "type"
- **Warning Event Trend.** The associated query and analysis statement is:  
select time\_series(\_\_time, 'PT1H', 'yyyy-MM-dd HH', '0') as "dt",count(1) as "count" from log where  
"type" = 'Warning' group by "dt" order by "dt"
- **Error Event Trend.** The associated query and analysis statement is:  
select time\_series(\_\_time, 'PT1H', 'yyyy-MM-dd HH', '0') as "dt",count(1) as "count" from log where  
"type" = 'Error' group by "dt" order by "dt"
- **Pod OOM Events.** The associated query and analysis statement is:  
select TIME\_FORMAT( \_\_time, 'yyyy-MM-dd HH:mm:ss', '+08:00') as "Time", "resource\_kind" as "Event  
Target", "name" as "Type", "resource\_name" as "Target Name", "reason" as "Details" from log where  
"name" in ( 'OOMKilling','PodOOMKilling' ) order by \_\_time desc limit 100
- **Pod Drive Event List.** The associated query and analysis statement is:  
select TIME\_FORMAT( \_\_time, 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as "Time", "resource\_kind" as  
"Event Target", "name" as "Type", "resource\_name" as "Target Name", "reason" as "Details" from log  
where "name" = 'NodeControllerEviction' order by \_\_time desc limit 100
- **Major Events.** The associated query and analysis statement is:

```
select TIME_FORMAT(__time, 'yyyy-MM-dd HH:mm:ss', '+08:00') as "Time", "type" as "Level",
"resource_kind" as "Event Target", "name" as "Type", "resource_name" as "Target Name", "reason" as
"Details" from log where "type" in ('Warning','Error') order by __time desc limit 100
```

----End

## Viewing CCE Logs Aggregation Search

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CCE dashboard templates** under **Dashboard Templates** and click **CCE Logs Aggregation Search** to view the chart details.

- Filter by namespace. The associated query and analysis statement is:  

```
select distinct("objectRef.namespace")
```
- Filter by user. The associated query and analysis statement is:  

```
select distinct("user.username")
```
- Filter by status code. The associated query and analysis statement is:  

```
select distinct("responseStatus.code")
```
- Filter by operation type. The associated query and analysis statement is:  

```
select distinct("verb")
```
- Filter by resource object. The associated query and analysis statement is:  

```
select distinct("objectRef.name")
```
- Filter by resource type. The associated query and analysis statement is:  

```
select distinct("objectRef.resource")
```
- Filter by request URL. The associated query and analysis statement is:  

```
select distinct("requestURI")
```
- Filter by userAgent. The associated query and analysis statement is:  

```
select distinct("userAgent")
```
- **User Distribution Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "user.username" as "User", count(*) as
"count" group by dt, "user.username" order by dt limit 10000
```
- **Namespace Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.namespace" as "Namespace",
count(*) as "count" group by dt, "objectRef.namespace" order by dt limit 10000
```
- **Operation Type Distribution Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.namespace" as "Namespace",
count(*) as "count" group by dt, "objectRef.namespace" order by dt limit 10000
```
- **Status Code Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, cast("responseStatus.code" as varchar) as
"Return code", count(*) as "count" group by dt, "Return code" order by dt limit 10000
```
- **Resource Type Trend.** The associated query and analysis statement is:  

```
SELECT REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type",
count(*) as "count" group by dt, "objectRef.resource" order by dt limit 10000 SELECT
REPLACE(LEFT(stageTimestamp, 16),'T',' ') AS dt, "objectRef.resource" as "Resource type", count(*) as
"count" group by dt, "objectRef.resource" order by dt limit 10000
```
- **Major Operations.** The associated query and analysis statement is:  

```
select "auditID" AS "Audit ID", "verb" AS "Operation Type", "requestReceivedTimestamp" AS
"Started", "stageTimestamp" AS "Ended", "user.username" AS "Operator", "sourceIPs" AS "Operation
Source", "userAgent", "objectRef.namespace" AS "Namespace", CONCAT(CONCAT("objectRef.resource",
"/"), "objectRef.subresource") AS "Operation Object", "objectRef.name" AS "Resource Name",
"responseStatus.code" AS "Return Code"
```

----End



## Viewing CCE Logs Account Operations

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CCE dashboard templates** under **Dashboard Templates** and click **CCE Logs Account Operations** to view the chart details.

- **Filter by username.** The associated query and analysis statement is:  
`select distinct("user.username")`
- **Filter by namespace.** The associated query and analysis statement is:  
`select distinct("objectRef.namespace")`
- **Filter by status code.** The associated query and analysis statement is:  
`select distinct("responseStatus.code")`
- **Resources Created.** The associated query and analysis statement is:  
`select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log where "verb" = 'create' ) )`
- **Resources Modified.** The associated query and analysis statement is:  
`select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(*) as "total" from log where "verb" in ('update','patch') ) )`
- **Resources Deleted.** The associated query and analysis statement is:  
`select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(*) as "total" from log where "verb" = 'delete' ) )`
- **Affected Namespaces.** The associated query and analysis statement is:  
`select case when "objectRef.namespace" is null then '_all_' else "objectRef.namespace" end as ns, count(1) as total group by ns limit 10000`
- **Deleted Resource.** The associated query and analysis statement is:  
`SELECT "objectRef.resource" as "resource", count(1) as "count" where "verb" = 'delete' group by "resource"`
- **Operation History.** The associated query and analysis statement is:  
`select case when "Operation" is null then 'None' else "Operation" end as "Operation", "Time", v from (select concat(CASE WHEN "objectRef.subresource" is null then "objectRef.resource" else "objectRef.subresource" end, '[', verb, ']') as "Operation", time_series(__time, 'PT1H', 'yyyy-MM-dd HH', '0') as "Time", count(1) as v from log where "verb" in ('create', 'patch', 'update', 'delete') group by "Operation", "Time" order by "Time" desc limit 10000 )`
- **Resource Operations.** The associated query and analysis statement is:  
`select CASE WHEN "objectRef.subresource" is null then "objectRef.resource" else "objectRef.subresource" end as "Resource", verb as "Operation", count(1) as total where "verb" in ('create','update','patch','delete') group by "Resource", "Operation" limit 10000`
- **Created Resources.** The associated query and analysis statement is:  
`SELECT "auditID" as "Event ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "Occurred", "requestURI" as "Resource", "objectRef.name" as "Resource Name", "responseStatus.code" as "Status Code", "sourceIPs" as "Source IP", "requestObject" as "Details" where "verb" = 'create' order by __time desc limit 1000`
- **Modified Resources.** The associated query and analysis statement is:  
`SELECT auditID as "Event ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "Occurred", "requestURI" as "Resource", "objectRef.name" as "Resource Name", "responseStatus.code" as "Status Code", "sourceIPs" as "Source IP", requestObject as "Details" where "verb" in ('update','patch') order by __time desc limit 1000`
- **Accessed Resources.** The associated query and analysis statement is:  
`SELECT auditID as "Event ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "Occurred", "requestURI" as "Resource", "objectRef.name" as "Resource Name", "responseStatus.code" as "Status Code", "sourceIPs" as "Source IP", requestObject as "Details" where "verb" in ('get','list') order by __time desc limit 1000`
- **Deleted Resources.** The associated query and analysis statement is:  
`SELECT auditID as "Event ID", time_format("__time",'yyyy-MM-dd HH:mm:ss') as "Occurred", "requestURI" as "Resource", "objectRef.name" as "Resource Name", "responseStatus.code" as "Status`

```
Code", "sourceIPs" as "Source IP", requestObject as "Details" where "verb" = 'delete' order by __time desc limit 1000
```

----End

## Viewing CCE Audit Log Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CCE dashboard templates** under **Dashboard Templates** and click **CCE Audit Log Center** to view the chart details.

- Filter by namespace. The associated query and analysis statement is:  

```
select distinct("objectRef.namespace")
```
- Filter by user. The associated query and analysis statement is:  

```
select distinct("user.username")
```
- Filter by operation type. The associated query and analysis statement is:  

```
select distinct("verb")
```
- Filter by status code. The associated query and analysis statement is:  

```
select distinct("responseStatus.code")
```
- Filter by resource object. The associated query and analysis statement is:  

```
select distinct("objectRef.name")
```
- Filter by resource type. The associated query and analysis statement is:  

```
select distinct("objectRef.resource")
```
- Filter by request URL. The associated query and analysis statement is:  

```
select distinct("requestURI")
```
- Filter by UserAgent. The associated query and analysis statement is:  

```
select distinct("userAgent")
```
- **Total Audit Records.** The associated query and analysis statement is:  

```
select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2) as "inc" from (select compare(total , 86400) as diff from(select count(1) as total from log))
```
- The query analysis statements associated with the **Number of Operators** chart are as follows:  

```
select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2) as "inc" from (select compare(total , 86400) as diff from(select count(distinct("user.username")) as total from log))
```
- **Active Nodes.** The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2) as "inc" from (select compare(total , 86400) as diff from(select count(DISTINCT "user.username") as total from log where "objectRef.resource" = 'nodes' and "objectRef.subresource" = 'status' and "verb" in ('update','put','patch') and "user.username" in ('node','system')))
```
- **Abnormal Visits.** The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2) as "inc" from (select compare(total , 86400) as diff from(select count(1) as total from log where "responseStatus.code" >= 400))
```
- **Sensitive Operations.** The associated query and analysis statement is:  

```
select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2) as "inc" from (select compare(total , 86400) as diff from(select count(1) as "total" from log where ("verb" = 'create' AND "objectRef.subresource" = 'exec') OR ("verb" = 'create' AND "objectRef.subresource" = 'attach' AND "objectRef.resource" = 'pods') OR ("objectRef.resource" = 'secrets' AND "verb" = 'get' AND ("user.username" != 'apiserver') AND ("user.username" not like 'system:node:%')) OR ("verb" = 'delete' AND ("user.username" not like 'system:node:%') AND ("user.username" not like 'system:serviceaccount:kube-system:%') AND ("user.username" != 'system:apiserver') AND ("user.username" != 'system:apiserve') AND ("user.username" != 'system:kube-scheduler') AND ("user.username" != 'system:kube-controller-manager'))))
```
- **Creation Operations.** The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2) as "inc" from (select compare(total , 86400) as diff from(select count(1) as total from log where verb = 'create'))
```

- **Update Operations.** The associated query and analysis statement is:  
`select diff[1] as "total" , round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log where verb in ('update','patch')) )`
- **Deletion Operations.** The associated query and analysis statement is:  
`select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100 , 2 ) as "inc" from (select compare( total , 86400) as diff from( select count(1) as total from log where verb = 'delete' ) )`
- **Operators.** The associated query and analysis statement is:  
`select "user.username" as "Username", count(*) as "count" group by "Username" order by "count" desc`
- **Namespaces.** The associated query and analysis statement is:  
`select "objectRef.namespace" as "Namespace", count(*) as "count" group by "Namespace"`
- **Resource Types.** The associated query and analysis statement is:  
`select "objectRef.resource" as "Resource type", count(*) as "count" group by "Resource type" order by "count" desc limit 20`
- **Operation Types.** The associated query and analysis statement is:  
`select verb as "Operation type", count(*) as "count" group by "Operation type" order by "count" desc`
- **Node Operations.** The associated query and analysis statement is:  
`select "verb" as "Operation type", count(*) as "count" where "objectRef.resource" = 'nodes' AND ("verb" in ('create','delete')) group by "Operation type" order by "count" desc`
- **Workload Operations.** The associated query and analysis statement is:  
`select "verb" as "Operation type", count(*) as "count" where "verb" in ('create', 'delete') and "objectRef.resource" in ('deployments','statefulsets','daemonsets','jobs','cronjobs') group by "Operation type" order by "count" desc`
- **Service/Ingress Operations.** The associated query and analysis statement is:  
`select "verb" as "Operation type", count(*) as "count" where "verb" in ('create', 'delete') and "objectRef.resource" in ('ingresses','services') group by "verb" order by "count" desc`
- **Major Operation Trend.** The associated query and analysis statement is:  
`SELECT REPLACE(LEFT("stageTimestamp", 16),'T',' ') AS "dt", "verb", count(*) as "count" where "verb" in ('create','delete','update','patch') group by "dt", "verb" order by "dt" limit 10000`
- **Non-System User Operation Trend.** The associated query and analysis statement is:  
`SELECT REPLACE(LEFT("stageTimestamp", 16),'T',' ') AS "dt", count(*) as "count", "user.username" as "Username" where "user.username" not in ('kube-controller-manager','kube-apiserver-kubelet-client','system','apiserver') group by "dt", "Username" order by "dt" limit 10000`

----End

### 6.3.3.3 CDN Dashboard Templates

CDN logs the requests to all domain names including those deleted. You can ingest these logs to LTS to analyze the access to your service resources in detail. If you have enabled the enterprise project function, log management is not available for deleted domain names.

CDN dashboard templates support [Viewing CDN Error Analysis](#), [Viewing CDN Basic Data](#), [Viewing CDN User Analysis](#), and [Viewing Popular CDN Resources](#).

#### Prerequisites

- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

#### Viewing CDN Error Analysis

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CDN dashboard templates** under **Dashboard Templates** and click **CDN Error Analysis** to view the chart details.

- **Top 5 Domain Name Errors.** The associated query and analysis statement is:  
select domain , count(\*) as c where http\_code > 400 group by domain order by c desc limit 5
- **Top 5 URI Errors.** The associated query and analysis statement is:  
select uri , count(\*) as c where http\_code > 400 group by uri order by c desc limit 5
- **Status Codes.** The associated query and analysis statement is:  
select http\_code , count(\*) as c where http\_code > 400 group by http\_code order by c desc
- **Errors by Carrier.** The associated query and analysis statement is:  
select ip\_to\_provider(client\_ip) as isp , count(\*) as c where http\_code > 400 group by isp having ip\_to\_provider(client\_ip) != "" order by c desc limit 10
- **Errors by Client.** The associated query and analysis statement is:  
select user\_agent as "Client version", count(\*) as "Errors" where http\_code > 400 group by user\_agent order by "Errors" desc limit 10
- **Errors by Province.** The associated query and analysis statement is:  
select ip\_to\_province(client\_ip) as province , count(\*) as c where http\_code > 400 and IP\_TO\_COUNTRY (client\_ip) = 'China' group by province order by c desc limit 50
- **4XX Errors.** The associated query and analysis statement is:

```
SELECT
 province AS "Province",
 isp AS "Carrier",
 c AS "Errors",
 round(c * 100.0 / sum(c), 2) AS "Rate (%)"
FROM
 (
 SELECT
 ip_to_province (client_ip) AS province,
 ip_to_provider (client_ip) AS isp,
 count(*) AS c
 FROM
 log
 WHERE
 http_code >= 400
 AND http_code < 500
 GROUP BY
 province,
 isp
 HAVING
 (
 ip_to_provider (client_ip)) != ""
 ORDER BY
 c DESC
)
GROUP BY
 province,
 isp,
 c
```

- **5XX Errors.** The associated query and analysis statement is:

```
SELECT
 province AS "Province",
 isp AS "Carrier",
 c AS "Errors",
 round(c * 100.0 / sum(c), 2) AS "Rate (%)"
FROM
 (
 SELECT
 ip_to_province (client_ip) AS province,
 ip_to_provider (client_ip) AS isp,
 count(*) AS c
 FROM
 log
 WHERE
 http_code >= 500
 GROUP BY
```

```

province,
isp
HAVING
(
ip_to_provider (client_ip)) != ""
ORDER BY
c DESC
)
GROUP BY
province,
isp,
c

```

- **Errors by Country.** The associated query and analysis statement is:  
select ip\_to\_country(client\_ip) as country , count(\*) as c where http\_code > 400 group by country order by c desc limit 50

----End

## Viewing CDN Basic Data

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CDN dashboard templates** under **Dashboard Templates** and click **CDN Basic Data** to view the chart details.

- **Cache Hit Ratio.** The associated query and analysis statement is:  
select round(diff[1],2) as Hit\_ratio, round(diff[2],2) as diff, round((diff[3]-1)\*100, 2) from (select compare(Hit\_ratio, 86400) as diff from (select sum(s) \* 100.0/count(\*) as Hit\_ratio from (select case when hit\_info = 'HIT' then 1 else 0 end as s from log)))
- **Download Speed.** The associated query and analysis statement is:  
select round(diff[1],2) as speed, round(diff[2],2) as diff, round((diff[3]-1)\*100, 2) from (select compare(speed, 86400) as diff from (select sum(response\_size) \* 1.0 /sum(response\_time) as speed from log ))
- **Status Codes.** The associated query and analysis statement is:  
select http\_code , count(\*) as c group by http\_code order by c desc
- **Latency Distribution.** The associated query and analysis statement is:  
select  
case when response\_time < 100 then '~100ms'  
when response\_time < 500 then '100~500ms'  
when response\_time < 1000 then '500ms~1s'  
when response\_time < 5000 then '1~5s'  
when response\_time < 6000 then '5~6s'  
when response\_time < 7000 then '6~7s'  
when response\_time < 8000 then '7~8s'  
when response\_time < 10000 then '8~10s'  
when response\_time < 15000 then '10~15s'  
else '15s~' end as latency ,  
count(\*) as cnt  
group by latency  
order by cnt
- **Request Bandwidth.** The associated query and analysis statement is:  
select TIME\_FORMAT (TIME\_FLOOR(\_\_time,'PT1M'), 'HH:mm', '+08:00') as thisdate,  
sum(response\_size) \* 8/1000000000.0 as "Bandwidth (Gbit/min)"  
group by TIME\_FLOOR(\_\_time,'PT1M')  
order by TIME\_FLOOR(\_\_time,'PT1M')
- **Visits and Users.** The associated query and analysis statement is:  
select TIME\_FORMAT (TIME\_FLOOR(\_\_time,'PT1M'), 'HH:mm', '+08:00') as thisdate,  
count(\*) as pv, APPROX\_COUNT\_DISTINCT(client\_ip) as uv group by TIME\_FLOOR(\_\_time,'PT1M')  
order by TIME\_FLOOR(\_\_time,'PT1M')
- **Average Latency.** The associated query and analysis statement is:  
select TIME\_FORMAT (TIME\_FLOOR(\_\_time,'PT1M'), 'HH:mm', '+08:00') as thisdate,  
avg(response\_time) as "Average Latency (ms)" group by TIME\_FLOOR(\_\_time,'PT1M') order by  
TIME\_FLOOR(\_\_time,'PT1M')

- **Request Hit Ratio.** The associated query and analysis statement is:

```
select
 TIME_FORMAT (TIME_FLOOR(m_time,'PT1M'), 'HH:mm', '+08:00') as thisdate ,
 sum(is_hit)*100.0/count(*) as hit_ratio
from (select TIME_FLOOR(_time,'PT1M') as m_time , case when hit_info = 'HIT'
then 1 else 0 end as is_hit from log) group by m_time order by m_time
```

----End

## Viewing CDN User Analysis

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CDN dashboard templates** under **Dashboard Templates** and click **CDN User Analysis** to view the chart details.

- **Visits.** The associated query and analysis statement is:

```
select diff[1] as pv,diff[2] as diff, round((diff[3]-1), 2) from (select compare(pv, 86400) as diff
from (select count(*) as pv from log))
```

- **Visitors.** The associated query and analysis statement is:

```
select diff[1] as uv, diff[2] as diff, round((diff[3]-1)*100, 2) from (select compare(uv , 86400) as diff
from (select APPROX_COUNT_DISTINCT(client_ip) as uv from log))
```

- **Visits by Client.** The associated query and analysis statement is:

```
select ua as "Client" , sum(c) as "Visits" from (select case when strpos(ua , 'iphone') > 1 then 'iphone'
when strpos(ua, 'ipad') > 1 then 'ipad' when strpos(ua, 'android') > 1 then 'android' when strpos(ua,
'windows') > 1 then 'windows' when strpos(ua , 'mac') > 1 then 'mac' when strpos(ua, 'linux') > 1
then 'linux' else ua end as ua , c from (select count(*) as c , lower(user_agent) as ua from log group
by ua order by c desc limit 2000)) group by "Client" order by "Visits" desc limit 100
```

- **Visits by Carrier.** The associated query and analysis statement is:

```
select ip_to_provider(client_ip) as isp ,count(*) as "Visits" group by isp order by "Visits" desc limit 100
```

- **Visits by Geography.** The associated query and analysis statement is:

```
select ip_to_province(client_ip) as province , count(*) as cnt where IP_TO_COUNTRY (client_ip) =
'China' group by province HAVING province not in ('Reserved address','') order by cnt desc limit 100
```

- **Top Valid Visitors.** The associated query and analysis statement is:

```
SELECT CASE WHEN ip_to_country(client_ip) = 'Shanghai' THEN concat(client_ip, ' (shanghai)')
WHEN ip_to_province(client_ip) = '' THEN concat(client_ip, ' (Unknown IP)') WHEN
ip_to_provider(client_ip) = 'Private IP' THEN concat(client_ip, ' (Private IP)') ELSE
concat(client_ip, ' (, ip_to_country(client_ip), '/', ip_to_province(client_ip), '/',
CASE WHEN ip_to_city(client_ip) = '-1' THEN 'Unknown city' ELSE ip_to_city(client_ip)
END, ' , ip_to_provider(client_ip), ')') END AS client, pv as "Total Visits", (pv -
success_count) as "Errors", round(CASE WHEN "throughput" > 0 THEN "throughput" ELSE 0 END,
1) AS "Total Downloads (GB)" from (select client_ip, count(*) as pv,
sum(response_size) / 1024.0 / 1024 / 1024.0 AS throughput, sum(CASE WHEN
http_code < 400 THEN 1 ELSE 0 END) AS success_count from log group by
client_ip order by success_count desc limit 100)
```

- **Top Visitors by Downloads.** The associated query and analysis statement is:

```
SELECT CASE WHEN ip_to_country(client_ip)='Shanghai' THEN concat(client_ip, ' (shanghai)') WHEN
ip_to_province(client_ip)='' THEN concat(client_ip, ' (Unknown IP)') WHEN
ip_to_provider(client_ip)='Private IP' THEN concat(client_ip, ' (Private IP)') ELSE concat(client_ip, ' (,
ip_to_country(client_ip), '/', ip_to_province(client_ip), '/', CASE WHEN ip_to_city(client_ip)='-1'
THEN 'Unknown city' ELSE ip_to_city(client_ip) END, ' ,ip_to_provider(client_ip), ')') END AS
client, pv as "Total Visits", error_count as "Errors", round(CASE WHEN "throughput" > 0
THEN "throughput" ELSE 0 END, 1) AS "Total Downloads (GB)" from (select client_ip ,
count(*) as pv, sum(response_size)/1024.0/1024/1024.0 AS throughput , sum(CASE WHEN
http_code > 400 THEN 1 ELSE 0 END) AS error_count from log group by client_ip order
by throughput desc limit 100)
```

----End

## Viewing Popular CDN Resources

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CDN dashboard templates** under **Dashboard Templates** and click **Popular CDN Resources** to view the chart details.

- **5 Most Visited Domain Names.** The associated query and analysis statement is:  

```
select domain ,count(*) as cnt group by domain order by cnt desc limit 5
```
- **5 Most Downloaded Domain Names.** The associated query and analysis statement is:  

```
select domain , sum(response_size) as "Total Downloads" group by domain order by "Total Downloads" desc limit 5
```
- **Popular Visits (URI).** The associated query and analysis statement is:  

```
select uri as URI, "Visits", "Visitors", round(CASE WHEN "Total Downloads (GB)" > 0 THEN "Total Downloads (GB)" ELSE 0 END, 2) AS "Total Downloads (GB)" from (select uri ,count(*) as "Visits" , APPROX_COUNT_DISTINCT(client_ip) as "Visitors", sum(response_size)/1024.0/1024.0/1024.0 as "Total Downloads (GB)" where http_code < 400 group by uri order by "Visits" desc limit 100)
```
- **Popular Visits (Source).** The associated query and analysis statement is:  

```
select refer_domain as "Referer",c as "Times",uv as "Users", round(c * 100.0 / sum(c), 2) as "Percentage" from (select refer_domain as refer_domain,count(*) as c,APPROX_COUNT_DISTINCT(client_ip) as uv from log where refer_domain != " group by refer_domain order by c desc limit 100) GROUP BY refer_domain, c, uv
```
- **Visits by Geography.** The associated query and analysis statement is:  

```
select ip_to_province(client_ip) as province , count(*) as cnt where IP_TO_COUNTRY (client_ip) = 'China' group by province HAVING province not in ('','Reserved address','*') order by cnt desc limit 1000
```
- **Download Speed by Geography.** The associated query and analysis statement is:  

```
select province, round(CASE WHEN "speed" > 0 THEN "speed" ELSE 0 END, 3) AS "speed" from (select ip_to_province(client_ip) as province , sum(response_size)* 1.0 /(sum(response_time)+1) as "speed" , count(*) as c where IP_TO_COUNTRY (client_ip) = 'China' group by province HAVING province not in ('','Reserved address','*') order by c desc limit 40)
```
- **Statistics by Province.** The associated query and analysis statement is:  

```
select ip_to_province(client_ip) as "Province" ,count(*) as "Visits", sum(response_size)/ 1024.0/1024.0/1024.0 as "Total Downloads (GB)" , sum(response_size) * 1.0 /sum(response_time) as "Download Speed (KB/s)" group by "Province" having ip_to_province(client_ip) != " order by "Total Downloads (GB)" desc limit 200
```
- **Carrier Traffic and Speed.** The associated query and analysis statement is:  

```
select ip_to_provider(client_ip) as isp , sum(response_size)* 1.0 /(sum(response_time)+1) as "Download Speed (KB/s)" , sum(response_size)/1024.0/1024.0/1024.0 as "Total Downloads (GB)", count(*) as c group by isp having ip_to_provider(client_ip) != " order by c desc limit 10
```
- **Statistics by Carrier.** The associated query and analysis statement is:  

```
select "Carrier", "Visits", round(CASE WHEN "Total Downloads (GB)" > 0 THEN "Total Downloads (GB)" ELSE 0 END, 2) AS "Total Downloads (GB)", round(CASE WHEN "Download Speed (KB/s)" > 0 THEN "Download Speed (KB/s)" ELSE 0 END, 2) AS "Download Speed (KB/s)" from (select ip_to_provider(client_ip) as "Carrier" ,count(*) as "Visits", sum(response_size)/ 1024.0/1024.0/1024.0 as "Total Downloads (GB)" , sum(response_size) * 1.0 /sum(response_time) as "Download Speed (KB/s)" group by "Carrier" having ip_to_provider(client_ip) != " and "Carrier" not in (*) order by "Total Downloads (GB)" desc limit 200)
```

----End

### 6.3.3.4 CFW Dashboard Templates

CFW is a next-generation cloud-native firewall. It protects Internet and VPC borders on the cloud by real-time intrusion detection and prevention, global unified access control, full traffic analysis, log audit, and tracing. CFW employs AI for intelligent defense, and can be elastically scaled to meet changing business

needs, helping you easily handle security threats. It allows you to view the risk levels, affected ports, matched rules, and attack event types of detected dangerous traffic in attack event logs. You can also view all traffic allowed or blocked in access control logs to better adjust access control policies.

CFW dashboard templates support [Viewing CFW Access Log Center](#), [Viewing CFW Traffic Log Center](#), and [Viewing CFW Attack Log Center](#).

## Prerequisites

- Logs have been collected from CFW. For details, see [Ingesting CFW Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

## Viewing CFW Access Log Center

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

**Step 2** In the **Log Applications** area, click **CFW Log Center** and choose **Go to the Dashboard**.

**Step 3** In the dashboard list, choose **CFW dashboard templates** under **Dashboard Templates** and click **CFW access log center** to view the chart details.

- The **Blockage Trends (Internet Access)** chart displays the blockage trend of Internet access. The associated query and analysis statement is:  

```
select time_series(MILLIS_TO_TIMESTAMP(hit_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time,COUNT(*) as frequency WHERE action='deny' AND direction='out2in' group by t_time order by t_time
```
- The **Blockage Trends (Server-Originated Access)** chart displays the blockage trend of server-originated access. The associated query and analysis statement is:  

```
select time_series(MILLIS_TO_TIMESTAMP(hit_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time,COUNT(*) as frequency WHERE action='deny' AND direction='in2out' group by t_time order by t_time
```
- The **5 Most Blocked Applications** chart displays the top 5 applications with the most Internet access blocks. The associated query and analysis statement is:  

```
SELECT app, COUNT(*) as frequency WHERE action='deny' AND direction='out2in' GROUP BY app ORDER BY frequency DESC LIMIT 5
```
- The **5 Most Blocked Destinations** chart displays the top 5 destinations with the most Internet access blocks. The associated query and analysis statement is:  

```
SELECT dst_ip, COUNT(*) as frequency WHERE action='deny' AND direction='out2in' GROUP BY dst_ip ORDER BY frequency DESC LIMIT 5
```
- The **5 Most Blocked Sources** chart displays the top 5 sources with the most Internet access blocks. The associated query and analysis statement is:  

```
SELECT src_ip, COUNT(*) as frequency WHERE action='deny' AND direction='out2in' GROUP BY src_ip ORDER BY frequency DESC LIMIT 5
```
- The **5 Most Blocked Applications (Server-Originated Access)** chart displays the top 5 applications with the most server-originated access blocks. The associated query and analysis statement is:  

```
SELECT app, COUNT(*) as frequency WHERE action='deny' AND direction='in2out' GROUP BY app ORDER BY frequency DESC LIMIT 5
```



- The **5 Most Blocked Destinations (Server-Originated Access)** chart displays the top 5 destinations with the most server-originated access blocks. The associated query and analysis statement is:  

```
SELECT dst_ip, COUNT(*) as frequency WHERE action='deny' AND direction='in2out' GROUP BY dst_ip ORDER BY frequency DESC LIMIT 5
```
- The **5 Most Blocked Sources (Server-Originated Access)** chart displays the top 5 sources with the most server-originated access blocks. The associated query and analysis statement is:  

```
SELECT src_ip, COUNT(*) as frequency WHERE action='deny' AND direction='in2out' GROUP BY src_ip ORDER BY frequency DESC LIMIT 5
```

----End

## Viewing CFW Traffic Log Center

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

**Step 2** In the **Log Applications** area, click **CFW Log Center** and choose **Go to the Dashboard**.

**Step 3** In the dashboard list, choose **CFW dashboard templates** under **Dashboard Templates** and click **CFW traffic log center** to view the chart details.

- The **Traffic Trends (Internet Access)** chart displays the traffic trend of Internet access. The associated query and analysis statement is:  

```
select time_series(MILLIS_TO_TIMESTAMP(start_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time, SUM(to_s_bytes) AS 'Inbound', SUM(to_c_bytes) AS 'Outbound' WHERE direction='out2in' group by t_time order by t_time
```
- The **Region Distribution of Inbound Internet Access (China)** chart displays the distribution of inbound Internet access by region in China. The associated query and analysis statement is:  

```
SELECT count(*) AS PV, ip_to_province(src_ip) AS province WHERE direction='out2in' and IP_TO_COUNTRY (src_ip) = 'China' GROUP BY province HAVING province not in ('Reserved address',*) ORDER BY PV DESC
```
- The **Region Distribution of Inbound Internet Access (Global)** chart displays the distribution of inbound Internet access by region in the world. The associated query and analysis statement is:  

```
SELECT count(*) AS PV, ip_to_country(src_ip) AS country WHERE direction='out2in' GROUP BY country HAVING country not in ('Reserved address',*) ORDER BY PV DESC
```
- The **Application Distribution of Internet Access** chart displays the application distribution of Internet access. The associated query and analysis statement is:  

```
SELECT app, COUNT(*) AS num WHERE direction='out2in' GROUP BY app ORDER BY num DESC
```
- The **Top 5 Source IP Addresses** chart displays the top 5 source IP addresses of Internet access. The associated query and analysis statement is:  

```
select src_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='out2in' GROUP BY src_ip ORDER BY sum_bytes DESC LIMIT 5
```
- The **Top 5 Destination IP Addresses** chart displays the top 5 destination IP addresses of Internet access. The associated query and analysis statement is:  

```
select dst_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='out2in' GROUP BY dst_ip ORDER BY sum_bytes DESC LIMIT 5
```
- The **Traffic Trends (Server-Originated Access)** chart displays the traffic trend of server-originated access. The associated query and analysis statement is:  

```
select time_series(MILLIS_TO_TIMESTAMP(start_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time, SUM(to_c_bytes) AS 'Inbound', SUM(to_s_bytes) AS 'Outbound' WHERE direction='in2out' group by t_time order by t_time
```

- The **Destination Region Distribution of Server Originated Access (China)** chart displays the destination region distribution of server-originated access in China. The associated query and analysis statement is:  

```
SELECT count(*) AS PV, ip_to_province(dst_ip) AS province WHERE direction='in2out' and IP_TO_COUNTRY (dst_ip) = 'China' GROUP BY province HAVING province not in ('Reserved address', '*') ORDER BY PV DESC
```
- The **Destination Region Distribution (Global)** chart displays the destination region distribution in the world. The associated query and analysis statement is:  

```
SELECT count(*) AS PV, ip_to_country(dst_ip) AS country WHERE direction='in2out' GROUP BY country HAVING country not in ('Reserved address', '*') ORDER BY PV DESC
```
- The **Application Distribution (Server-Originated Access)** chart displays the application distribution of server-originated access. The associated query and analysis statement is:  

```
SELECT app, COUNT(*) AS num WHERE direction='in2out' GROUP BY app ORDER BY num DESC
```
- The **Top 5 Source IP Addresses (Server-Originated Access)** chart displays the top 5 source IP addresses of server-originated access. The associated query and analysis statement is:  

```
select src_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='in2out' GROUP BY src_ip ORDER BY sum_bytes DESC LIMIT 5
```
- The **Top 5 Destination IP Addresses (Server-Originated Access)** chart displays the top 5 destination IP addresses of server-originated access. The associated query and analysis statement is:  

```
select dst_ip, SUM(bytes)/1024 as sum_bytes WHERE direction='in2out' GROUP BY dst_ip ORDER BY sum_bytes DESC LIMIT 5
```

----End

## Viewing CFW Attack Log Center

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

**Step 2** In the **Log Applications** area, click **CFW Log Center** and choose **Go to the Dashboard**.

**Step 3** In the dashboard list, choose **CFW dashboard templates** under **Dashboard Templates** and click **CFW attack log center** to view the chart details.

- **Attack Trends.** The associated query and analysis statement is:  

```
select time_series(MILLIS_TO_TIMESTAMP(event_time), 'PT1M', 'yyyy-MM-dd HH:mm:ss', '0') as t_time, count(*) as frequency group by t_time order by t_time
```
- **Sources (China).** The associated query and analysis statement is:  

```
SELECT count(*) as PV, ip_to_province(src_ip) as province WHERE IP_TO_COUNTRY (src_ip) = 'China' GROUP BY province HAVING province not in ('Reserved address', '*')
```
- **Sources (Global).** The associated query and analysis statement is:  

```
SELECT count(*) AS PV, ip_to_country(src_ip) AS country GROUP BY country HAVING country not in ('Reserved address', '*')
```
- **Types.** The associated query and analysis statement is:  

```
SELECT attack_type, COUNT(*) as num GROUP BY attack_type ORDER BY num
```
- **Top 5 Destinations.** The associated query and analysis statement is:  

```
SELECT dst_ip, COUNT(*) as frequency GROUP BY dst_ip ORDER BY frequency DESC LIMIT 5
```
- **Top 5 Sources.** The associated query and analysis statement is:  

```
SELECT src_ip, COUNT(*) as frequency GROUP BY src_ip ORDER BY frequency DESC LIMIT 5
```

----End

### 6.3.3.5 CSE Dashboard Templates

CSE is a cloud middleware used for microservice applications. You can also use it with other cloud services to quickly build a cloud-native microservice system for quick development and high-availability O&M of microservice applications.

CSE dashboard templates support [Viewing CSE Layer Access Center](#), [Viewing CSE Layer Monitoring Center](#), and [Viewing CSE Layer Monitoring in Seconds](#).

#### Prerequisites

- CSE logs have been collected to LTS.
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

#### Viewing CSE Layer Access Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CSE dashboard templates** under **Dashboard Templates** and click **CSE Layer Access Center** to view the chart details.

- **upstream\_host** allows you to filter upstream IP addresses. The associated query and analysis statement is:  

```
select distinct(upstream_host)
```
- **trace\_id** allows you to filter traces. The associated query and analysis statement is:  

```
select distinct(trace_id)
```
- **Day-over-day PV Change**. The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare("pv" , 86400) as diff from (select count(1) as "pv" from log))
```
- **Week-on-week PV Change**. The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare("pv" , 604800) as diff from (select count(1) as "pv" from log))
```
- **Day-over-day UV Change**. The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare("uv" , 86400) as diff from (select APPROX_COUNT_DISTINCT(authority) as "uv" from log))
```
- **Week-on-week UV Change**. The associated query and analysis statement is:  

```
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] * 100, 2) as inc from(select compare("uv" , 604800) as diff from (select APPROX_COUNT_DISTINCT(authority) as "uv" from log))
```
- **PV Distribution (China)**. The associated query and analysis statement is:  

```
select ip_to_province(authority) as province, sum(ori_pv) as pv from (select authority, count(1) as ori_pv group by authority ORDER BY ori_pv desc LIMIT 10000) where IP_TO_COUNTRY (authority) = 'China' group by province HAVING province not in ('','Reserved address','*')
```
- **PV Distribution (Global)**. The associated query and analysis statement is:  

```
SELECT ip_to_country(authority) as country,sum(ori_pv) as PV from (select authority, count(1) as ori_pv group by authority ORDER BY ori_pv desc LIMIT 10000) GROUP BY country HAVING country not in ('','Reserved address','*')
```
- **Average Latency Distribution (China)**. The associated query and analysis statement is:  

```
SELECT province,round(CASE WHEN "Average latency (ms)" > 0 THEN "Average latency (ms)" ELSE 0 END, 3) AS "Average latency (ms)" FROM (SELECT ip_to_province(authority) as province,sum(rt)/ sum(ori_pv) * 1000 AS "Average latency (ms)" from (select authority, sum(duration) as rt,count(1) as ori_pv group by authority ORDER BY ori_pv desc LIMIT 10000) WHERE IP_TO_COUNTRY (authority) = 'China' GROUP BY province) where province not in ('','Reserved address','*')
```
- **Average Latency Distribution (Global)**. The associated query and analysis statement is:

```
SELECT country,round(CASE WHEN "Average latency (ms)" > 0 THEN "Average latency (ms)" ELSE 0
END, 2) AS "Average latency (ms)" FROM (SELECT ip_to_country(authority) as country,sum(rt)/
sum(ori_pv) * 1000 AS "Average latency (ms)" from (select authority, sum(duration) as rt,count(1) as
ori_pv group by authority ORDER BY ori_pv desc LIMIT 10000) GROUP BY country) where country
not in ("Reserved address",*)
```

- **PV/UV Today.** The associated query and analysis statement is:  
SELECT TIME\_FORMAT( \_time\_, 'yyyy-MM-dd HH:mm:ss') as \_time\_,PV,UV FROM (select  
TIME\_CEIL(TIME\_PARSE(start\_time),'PT600S') AS \_time\_ , count(1) as PV,  
APPROX\_COUNT\_DISTINCT(authority) as UV from log WHERE \_\_time\_ <= CURRENT\_TIMESTAMP and  
\_\_time\_ >= DATE\_TRUNC( 'DAY',(CURRENT\_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR  
group by \_time\_ order by \_time\_)
- **Top 10 Provinces by Visits.** The associated query and analysis statement is:  
select ip\_to\_province(authority) as "province", sum(ori\_pv) as "Visits" from (select authority, count(1)  
as ori\_pv group by authority ORDER BY ori\_pv desc LIMIT 10000) group by "province" HAVING  
"province" <> '-1' order by "Visits" desc limit 10
- **Top 10 Cities by Visits.** The associated query and analysis statement is:  
select ip\_to\_city(authority) as "city", sum(ori\_pv) as "Visits" from (select authority, count(1) as ori\_pv  
group by authority ORDER BY ori\_pv desc LIMIT 10000) group by "city" HAVING "city" <> '-1' order  
by "Visits" desc limit 10
- **Top 10 Hosts by Visits.** The associated query and analysis statement is:  
select upstream\_host as "Host", count(1) as "PV" group by "Host" order by "PV" desc limit 10
- **Top 10 UserAgents by Visits.** The associated query and analysis statement is:  
select user\_agent as "UserAgent", count(1) as "PV" group by "UserAgent" order by "PV" desc limit 10
- **Device Distribution by Type.** The associated query and analysis statement is:  
select case when regexp\_like(lower(user\_agent), 'iphone|ipod|android|ios') then 'Mobile' else 'PC' end  
as type , count(1) as total group by type
- **Device Distribution by System.** The associated query and analysis statement  
is:  
select case when regexp\_like(lower(user\_agent), 'iphone|ipod|ios') then 'IOS' when  
regexp\_like(lower(user\_agent), 'android') then 'Android' else 'other' end as type , count(1) as total  
group by type HAVING type != 'other'
- **TOP URL.** The associated query and analysis statement is:  
select path , count(1) as pv, APPROX\_COUNT\_DISTINCT(authority) as UV, round(sum( case when  
response\_code < 400 then 1 else 0 end ) \* 100.0 / count(1), 2) as "Access Success Rate" group by  
path ORDER by pv desc
- **Top IP Addresses by Visits.** The associated query and analysis statement is:  
select authority as "Source IP Address",ip\_to\_country(authority) as "Country/  
Region",ip\_to\_province(authority) as "Province",ip\_to\_city(authority) as  
"City",ip\_to\_provider(authority) as "Carrier",count(1) as "PV" group by authority ORDER by "PV" desc  
limit 100

----End

## Viewing CSE Layer Monitoring Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CSE dashboard templates** under **Dashboard Templates** and click **CSE Layer Monitoring Center** to view the chart details.

- **upstream\_host** allows you to filter upstream IP addresses. The associated query and analysis statement is:  
select distinct(upstream\_host)
- **trace\_id** allows you to filter traces. The associated query and analysis statement is:  
select distinct(trace\_id)
- **PV.** The associated query and analysis statement is:  
SELECT TIME\_FORMAT( \_time\_, 'yyyy-MM-dd HH:mm:ss') as \_time\_,PV FROM ( SELECT TIME\_CEIL  
( TIME\_PARSE(start\_time), 'PT300S' ) AS \_time\_ , count( 1 ) AS PV FROM log GROUP BY \_time\_ )

- **Request Success Rate.** The associated query and analysis statement is:  

```
select ROUND(sum(case when response_code < 400 then 1 else 0 end) * 100.0 / count(1),2) as cnt
```
- **Average Latency.** The associated query and analysis statement is:  

```
select round(avg(duration) * 1000, 3) as cnt
```
- **4xx Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "response_code" >= 400 and "response_code" < 500
```
- **404 Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "response_code" = 404
```
- **429 Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "response_code" = 429
```
- **504 Requests.** The associated query and analysis statement is:  

```
SELECT COUNT(1) as cnt WHERE "response_code" = 504
```
- **5xx Requests.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_, 'yyyy-MM-dd HH:mm:ss') as _time_,cnt FROM (SELECT TIME_CEIL
(TIME_PARSE(start_time), 'PT300S') AS _time_, count(1) AS cnt FROM log where "response_code"
>= 500 GROUP BY _time_)
```
- **Status Code Distribution.** The associated query and analysis statement is:  

```
SELECT response_code, COUNT(1) AS rm GROUP BY response_code
```
- **UV.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_, 'yyyy-MM-dd HH:mm:ss') as _time_,UV FROM (select
TIME_CEIL(TIME_PARSE(start_time),'PT600S') AS _time_, APPROX_COUNT_DISTINCT(authority) as
UV from log group by _time_)
```
- **Traffic.** The associated query and analysis statement is:  

```
select TIME_FORMAT(_time_,'yyyy-MM-dd HH:mm:ss') AS _time_,round(CASE WHEN "Inbound" > 0
THEN "Inbound" ELSE 0 END, 2) AS "Inbound",round(CASE WHEN "Outbound" > 0 THEN
"Outbound" ELSE 0 END, 2) AS "Outbound" FROM (SELECT
TIME_CEIL(TIME_PARSE(start_time),'PT600S') AS _time_,sum(bytes_received) / 1024.0 AS
"Inbound",sum(bytes_sent) / 1024.0 AS "Outbound" group by _time_)
```
- **Access Failure Rate.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round(CASE WHEN "Failure rate"
> 0 THEN "Failure rate" ELSE 0 END, 2) AS "Failure rate",round(CASE WHEN "5xx ratio" > 0 THEN
"5xx ratio" ELSE 0 END, 2) AS "5xx ratio" from (select TIME_CEIL(TIME_PARSE(start_time),'PT600S')
AS _time_,sum(case when response_code >= 400 then 1 else 0 end) * 100.0 / count(1) as 'Failure
rate' , sum(case when response_code >=500 THEN 1 ELSE 0 END)*100.0/COUNT(1) as '5xx ratio'
group by _time_)
```
- **Latency.** The associated query and analysis statement is:  

```
select TIME_FORMAT(_time_, 'yyyy-MM-dd HH:mm:ss') as _time_,round(CASE WHEN "Avg" > 0
THEN "Avg" ELSE 0 END, 2) AS "Avg",round(CASE WHEN "P50" > 0 THEN "P50" ELSE 0 END, 2) AS
"P50",round(CASE WHEN "P90" > 0 THEN "P90" ELSE 0 END, 2) AS "P90",round(CASE WHEN "P99"
> 0 THEN "P99" ELSE 0 END, 2) AS "P99",round(CASE WHEN "P9999" > 0 THEN "P9999" ELSE 0
END, 2) AS "P9999" from (select TIME_CEIL(TIME_PARSE(start_time),'PT600S') as
time,avg(duration) * 1000 as "Avg", APPROX_QUANTILE_DS("duration", 0.50)*1000 as "P50",
APPROX_QUANTILE_DS("duration", 0.90)*1000 as "P90" ,APPROX_QUANTILE_DS("duration",
0.99)*1000 as 'P99',APPROX_QUANTILE_DS("duration", 0.9999)*1000 as 'P9999' group by _time_)
```
- **Top Host Requests.** The associated query and analysis statement is:  

```
SELECT "host", pv, uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate
(%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0
THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN
"Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN
"Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT
"host", count(1) AS pv, APPROX_COUNT_DISTINCT (my_remote_addr) AS uv, sum(CASE WHEN
"status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)",
avg(request_time) * 1000 AS "Average Latency (ms)", sum(request_length) / 1024.0 AS "Inbound
(KB)", sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "host" != " " GROUP BY "host")
ORDER BY pv DESC
```
- **Top Host Latencies.** The associated query and analysis statement is:  

```
SELECT "upstream_host", pv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access
Success Rate (%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average
Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)",
round(CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90
```

```
Latency (ms)", round(CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3)
AS "P99 Latency (ms)" FROM (SELECT "upstream_host", count(1) AS pv, sum(CASE WHEN
"response_code" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)",
avg(duration) * 1000 AS "Average Latency (ms)",APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS
"P90 Latency (ms)", APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99 Latency (ms)" WHERE
"upstream_host" != " GROUP BY "upstream_host") ORDER BY "Average Latency (ms)" desc
```

- Top Host Failure Rates.** The associated query and analysis statement is:

```
SELECT "upstream_host", pv,round(CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure
Rate (%)" ELSE 0 END, 2) AS "Access Failure Rate (%)", round(CASE WHEN "Average Latency (ms)"
> 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN
"P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)",
round(CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99
Latency (ms)" FROM (SELECT "upstream_host", count(1) AS pv, sum(CASE WHEN
"response_code" >= 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Failure Rate (%)",
avg(duration) * 1000 AS "Average Latency (ms)", APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS
"P90 Latency (ms)", APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99 Latency (ms)" WHERE
"upstream_host" != " GROUP BY "upstream_host") ORDER BY "Access Failure Rate (%)" desc
```
- Top URL Requests.** The associated query and analysis statement is:

```
SELECT path, pv,uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate
(%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0
THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN
"Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN
"Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT
path, count(1) AS pv, APPROX_COUNT_DISTINCT (authority) AS uv, sum(CASE WHEN
"response_code" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)",
avg(duration) * 1000 AS "Average Latency (ms)", sum(bytes_received) / 1024.0 AS "Inbound (KB)",
sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "upstream_host" != " GROUP BY path)
ORDER BY pv desc
```
- Top URL Failure Rates.** The associated query and analysis statement is:

```
SELECT path, pv, round(CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)"
ELSE 0 END, 2) AS "Access Failure Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN
"Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "P90
Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE
WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)"
FROM(SELECT path, count(1) AS pv, sum(CASE WHEN "response_code" >= 400 THEN 1 ELSE 0
END) * 100.0 / count(1) AS "Access Failure Rate (%)", avg(duration) * 1000 AS "Average Latency
(ms)", APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90 Latency (ms)",
APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "upstream_host" != "
GROUP BY path) ORDER BY "Access Failure Rate (%)" desc
```
- Top Backend Requests.** The associated query and analysis statement is:

```
SELECT addr, pv, uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate
(%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0
THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN
"Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN
"Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT
authority as addr, count(1) AS pv, APPROX_COUNT_DISTINCT (authority) AS uv, sum(CASE WHEN
"response_code" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)",
avg(duration) * 1000 AS "Average Latency (ms)", sum(bytes_received) / 1024.0 AS "Inbound (KB)",
sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "upstream_host" != " GROUP BY addr
having length(authority) > 2) ORDER BY "pv" desc
```
- Top Backend Latencies.** The associated query and analysis statement is:

```
SELECT addr,pv,round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)"
ELSE 0 END, 2) AS "Access Success Rate (%)",round(CASE WHEN "Average Latency (ms)" > 0 THEN
"Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)",round(CASE WHEN "P90 Latency
(ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)",round(CASE WHEN "P99
Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)" FROM (SELECT
authority as addr,count(1) AS pv,sum(CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END) *
100.0 / count(1) AS "Access Success Rate (%)",avg(duration) * 1000 AS "Average Latency
(ms)",APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90 Latency
(ms)",APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "upstream_host" !
= " and "authority" != '-' GROUP BY addr) ORDER BY "Average Latency (ms)" desc
```
- Top Backend Failure Rates.** The associated query and analysis statement is:

```
SELECT addr, pv, round(CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)"
ELSE 0 END, 2) AS "Access Failure Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN
"Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "P90
Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE
```

```
WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)"
FROM (SELECT authority as addr, count(1) AS pv, sum(CASE WHEN "response_code" >= 400 THEN
1 ELSE 0 END) * 100.0 / count(1) AS "Access Failure Rate (%)", avg(duration) * 1000 AS "Average
Latency (ms)", APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90 Latency (ms)",
APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "upstream_host" != "
and "authority" != '-' GROUP BY addr) ORDER BY "Access Failure Rate (%)" desc
```

- **Top URL Latencies.** The associated query and analysis statement is:  

```
SELECT path, pv,round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)"
ELSE 0 END, 2) AS "Access Success Rate (%)",round(CASE WHEN "Average Latency (ms)" > 0 THEN
"Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)",round(CASE WHEN "P90 Latency
(ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)",round(CASE WHEN "P99
Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)" FROM (SELECT
path, count(1) AS pv, sum(CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END) * 100.0 /
count(1) AS "Access Success Rate (%)", avg(duration) * 1000 AS "Average Latency (ms)",
APPROX_QUANTILE_DS(duration, 0.9) * 1000 AS "P90 Latency (ms)",
APPROX_QUANTILE_DS(duration, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "upstream_host" != "
GROUP BY path) ORDER BY "Average Latency (ms)" desc
```

----End

## Viewing CSE Layer Monitoring in Seconds

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **CSE dashboard templates** under **Dashboard Templates** and click **CSE Layer Monitoring in Seconds** to view the chart details.

- **upstream\_host** allows you to filter upstream IP addresses. The associated query and analysis statement is:  

```
select distinct(upstream_host)
```
- **trace\_id** allows you to filter traces. The associated query and analysis statement is:  

```
select distinct(trace_id)
```
- **QPS.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-dd HH:mm:ss') AS
__time_ , COUNT(*) as QPS from log group by __time_
```
- **Success Rate.** The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Success rate" > 0 THEN "Success rate" else 0 end,2) as "Success
rate" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-dd
HH:mm:ss') as __time, sum(case when response_code < 400 then 1 else 0 end) * 100.0 / count(1) as
'Success rate' from log group by __time)
```
- **Latency.** The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Access latency" > 0 THEN "Access latency" else 0 end,2) as "Access
latency",round(CASE WHEN "Upstream latency" > 0 THEN "Upstream latency" else 0 end,2) as
"Upstream latency" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-
dd HH:mm:ss') as __time, avg(duration)* 1000 as 'Access latency',avg(upstream_service_time)* 1000
as 'Upstream latency' from log group by __time)
```
- **Traffic.** The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Incoming" > 0 THEN "Incoming" ELSE 0 END, 3) AS
"Incoming",round(CASE WHEN "Outgoing body" > 0 THEN "Outgoing body" ELSE 0 END, 3) AS
"Outgoing body" from (select TIME_FORMAT(TIME_CEIL(TIME_PARSE(start_time),'PT5S'),'yyyy-MM-
dd HH:mm:ss') as __time , sum("bytes_received") / 1024.0 as "Incoming", sum("bytes_sent") / 1024.0
as "Outgoing body" group by __time)
```
- **Status Codes.** The associated query and analysis statement is:  

```
SELECT TIME_CEIL (TIME_PARSE (start_time), 'PT5S') AS "time", SUM(CASE WHEN
"response_code" >= 200 AND "response_code" < 300 THEN 1 ELSE 0 END) AS "2XX", SUM(CASE
WHEN "response_code" >= 300 AND "response_code" < 400 THEN 1 ELSE 0 END) AS "3XX",
SUM(CASE WHEN "response_code" >= 400 AND "response_code" < 500 THEN 1 ELSE 0 END) AS
"4XX", SUM(CASE WHEN "response_code" >= 500 AND "response_code" < 600 THEN 1 ELSE 0 END)
AS "5XX", SUM(CASE WHEN "response_code" < 200 OR "response_code" >= 600 THEN 1 ELSE 0
```

```
END) AS "Other" FROM log WHERE TIME_PARSE (start_time) IS NOT NULL GROUP BY "time"
ORDER BY "time" ASC LIMIT 100000
```

----End

### 6.3.3.6 DCS Dashboard Template

DCS is an in-memory database service. It is compatible with Redis, an in-memory database engine, and meets your requirements for high concurrency and fast data access. LTS collects, stores, and queries cloud resource operation records. You can use these records to perform security analysis, track resource changes, audit compliance, and locate faults.

LTS provides a one-stop wizard to collect DCS logs. The DCS audit log center dashboard displays charts such as the number of access users, access clients, and audit logs.

## Prerequisites

Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

## DCS Audit Log Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **DCS dashboard templates** under **Dashboard Templates** and click **DCS audit log center** to view the chart details.

- **Users.** The associated query and analysis statement is:  

```
select count(distinct(user)) as user_num
```
- **Clients.** The associated query and analysis statement is:  

```
select count(distinct(client_addr)) as client_num
```
- **Audit Logs.** The associated query and analysis statement is:  

```
select count(1) as log_num
```
- **Average Response Time.** The associated query and analysis statement is:  

```
select avg(use_time) as avg_time
```
- **Average QPS.** The associated query and analysis statement is:  

```
select count(*) / CAST((TIMESTAMPDIFF (minute, MIN(_time),MAX(_time))+1) as FLOAT)
```
- **Top 5 Users.** The associated query and analysis statement is:  

```
select user, count(1) as 'user_count' group by user order by count(1) desc LIMIT 5
```
- **Top 5 Clients.** The associated query and analysis statement is:  

```
select client_addr, count(1) as 'remote_count' group by client_addr order by count(1) desc limit 5
```
- **Top 5 Commands.** The associated query and analysis statement is:  

```
select command_name, count(1) as 'command_count' group by command_name order by count(1) desc
```
- **Hot Keys.** The associated query and analysis statement is:  

```
SELECT count(*) as 'count', command_keys GROUP by command_keys order by count(*) desc limit 5
```
- **Audit Log Details.** The associated query and analysis statement is:  

```
select "client_addr" as 'Client IP Address',"client_type" as 'Client Type',"server_addr" as 'Server IP Address',"command_name" as 'Command',"command_keys" as 'Keys',"command_param" as 'Command Content',"command_type" as 'Command Type',"use_time" as 'Execution Duration',"time" as 'Executed',"db" as 'DB',"user" as 'Username',"instance_id" as 'Instance ID',"role" as 'Node Role',"extend" as 'Extended Information'
```

----End



### 6.3.3.7 DDS Dashboard Template

DDS is a MongoDB-compatible database service that is secure, highly available, reliable, scalable, and easy to use. You can use DB instance creation, scaling, redundancy, backup, restoration, monitoring, and alarm reporting functions with just a few clicks on the DDS console. LTS allows you to analyze, search, visualize, and download logs, and view real-time logs.

LTS provides a one-stop wizard to collect DDS logs. The DDS audit log center dashboard displays charts such as the number of audit logs, access users, and access clients.

#### Prerequisites

- Logs have been collected from DDS. For details, see [Ingesting DDS Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

#### DDS Audit Log Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **DDS dashboard templates** under **Dashboard Templates** and click **DDS audit log center** to view the chart details.

- Filter by operation type. The associated query and analysis statement is:  
`select distinct(optype)`
- Filter by client IP address. The associated query and analysis statement is:  
`select distinct(user_ip)`
- Filter by database name. The associated query and analysis statement is:  
`select distinct(db)`
- Filter by username. The associated query and analysis statement is:  
`select distinct(user)`
- Filter by collection name. The associated query and analysis statement is:  
`select distinct(coll)`
- **Audit Logs**. The associated query and analysis statement is:  
`select count(1) as log_num`
- **Users**. The associated query and analysis statement is:  
`select count(distinct(user)) as user_num`
- **Clients**. The associated query and analysis statement is:  
`select count(distinct(user_ip)) as client_num`
- **Top 5 Commands**. The associated query and analysis statement is:  
`select optype, count(1) as 'command_count' group by optype order by count(1) desc LIMIT 5`
- **Top 5 Users**. The associated query and analysis statement is:  
`select user, count(1) as 'user_count' group by user order by count(1) desc LIMIT 5`
- **Top 5 Clients**. The associated query and analysis statement is:  
`select user_ip, count(1) as 'remote_count' group by user_ip order by count(1) desc LIMIT 5`
- **Audit Log Details**. The associated query and analysis statement is:  
`select "time" as "Executed","user" as "Username","param" as "Query Statement","instanceid" as "Instance ID","db" as "DB","coll" as "Collection Name ","user_ip" as "Client IP Address"`

----End

### 6.3.3.8 DMS Dashboard Template

DMS for Kafka is a message queuing service using open-source Apache Kafka. It provides Kafka instances with isolated computing, storage, and bandwidth resources. Rebalancing logs record rebalancing details, including the time, reason, and triggering client of rebalancing.

LTS provides a one-stop wizard to collect DMS rebalancing logs. It also supports multi-dimensional analysis and structuring, and offers a dashboard for DMS rebalancing logs. The dashboard displays the number of rebalancing consumer groups, number of rebalances, number of rebalances for consumer groups, rebalancing reasons, and group details of DMS rebalancing logs.

#### Prerequisites

- Logs have been collected from DMS. For details, see [Ingesting CFW Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

#### DMS Rebalancing Log Center

**Step 1** Log in to the LTS console.

**Step 2** In the navigation pane, choose **Dashboards**.

**Step 3** Choose **DMS dashboard templates** under **Dashboard Templates** and click **DMS Rebalancing Log Center** to view the chart details.

- **Group ID.** The associated query and analysis statement is:  

```
select distinct("message.groupId")
```
- Filter by rebalancing reason.
- **Consumer Groups for Rebalancing.** The associated query and analysis statement is:  

```
select count(distinct("message.groupId")) as "total" from log where ("message.type"!='RESPONSE' and "message.type"!='REQUEST')
```
- **Rebalances.** The associated query and analysis statement is:  

```
select count(*) as 'total' where ("message.type"!='RESPONSE' and "message.type"!='REQUEST')
```
- **Consumer Group Rebalances.** The associated query and analysis statement is:  

```
select "message.groupId" as 'GroupId', count(*) as 'Count' where ('message.type'!='RESPONSE' and 'message.type'!='REQUEST') group by "message.groupId"
```
- **Rebalancing Reasons and Group Details.** The associated query and analysis statement is:  

```
select __time as 'Time', "message.type" as 'Type', "message.groupId" as 'GroupId', "message.reason" as 'Reason', "message.group" as 'Group' where ('message.type'!='RESPONSE' and 'message.type'!='REQUEST')
```

----End

### 6.3.3.9 DSL Dashboard Template

LTS provides DSL processing for you to achieve one-stop log processing. Using domain-defined script languages and more than 200 built-in functions, you can implement end-to-end log processing tasks on the LTS console, such as log normalization, enrichment, transfer, anonymization, and filtering.

LTS provides the DSL processing task monitoring center dashboard template to display information such as the processing task ID/name and number of input/output lines.

## Prerequisites

- A DSL processing task has been created.
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

## DSL Processing Task Monitoring Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **DSL dashboard templates** under **Dashboard Templates** and click **DSL processing task monitoring center** to view the chart details.

- Filter by processing task ID. The associated query and analysis statement is:  

```
select distinct(task_id)
```
- Filter by processing task name. The associated query and analysis statement is:  

```
select distinct(task_name)
```
- **Input Lines.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "input" < 1000 THEN concat(cast("input" AS VARCHAR), 'Lines') WHEN "input" < 1000 * 1000 THEN concat(cast(round("input"/ 1000, 1) AS VARCHAR), 'Thousands lines') WHEN "input" < 1000000000 THEN concat(cast(round("input"/ 1000000.0, 1) AS VARCHAR), 'Million lines') WHEN "input"/ 1000.0 < 1000000000 THEN concat(cast(round("input"/ 1000 / 1000000.0, 1) AS VARCHAR), 'Billion lines') ELSE concat(cast(round("input"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), 'Trillion lines') END AS "total" from (select sum("process.accept") as "input")
```
- **Output Lines.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "delivered" < 1000 THEN concat(cast("delivered" AS VARCHAR), 'Lines') WHEN "delivered" < 1000 * 1000 THEN concat(cast(round("delivered"/ 1000, 1) AS VARCHAR), 'Thousands lines') WHEN "delivered" < 1000000000 THEN concat(cast(round("delivered"/ 1000000.0, 1) AS VARCHAR), 'Million lines') WHEN "delivered"/ 1000.0 < 1000000000 THEN concat(cast(round("delivered"/ 1000 / 1000000.0, 1) AS VARCHAR), 'Billion lines') ELSE concat(cast(round("delivered"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), 'Trillion lines') END AS "total" from (select sum("process.delivered") as "delivered")
```
- **Filtered Lines.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "drop" < 1000 THEN concat(cast("drop" AS VARCHAR), 'Lines') WHEN "drop" < 1000 * 1000 THEN concat(cast(round("drop"/ 1000, 1) AS VARCHAR), 'Thousands lines') WHEN "drop" < 1000000000 THEN concat(cast(round("drop"/ 1000000.0, 1) AS VARCHAR), 'Million lines') WHEN "drop"/ 1000.0 < 1000000000 THEN concat(cast(round("drop"/ 1000 / 1000000.0, 1) AS VARCHAR), 'Billion lines') ELSE concat(cast(round("drop"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), 'Trillion lines') END AS "total" from (select sum("process.drop") as "drop")
```
- **Failed Lines.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "failed" < 1000 THEN concat(cast("failed" AS VARCHAR), 'Lines') WHEN "failed" < 1000 * 1000 THEN concat(cast(round("failed"/ 1000, 1) AS VARCHAR), 'Thousands lines') WHEN "failed" < 1000000000 THEN concat(cast(round("failed"/ 1000000.0, 1) AS VARCHAR), 'Million lines') WHEN "failed"/ 1000.0 < 1000000000 THEN concat(cast(round("failed"/ 1000 / 1000000.0, 1) AS VARCHAR), 'Billion lines') ELSE concat(cast(round("failed"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), 'Trillion lines') END AS "total" from (select sum("process.failed") as "failed")
```
- **Execution Records.** The associated query and analysis statement is:  

```
select TIME_FORMAT(MILLIS_TO_TIMESTAMP("start"), 'yyyy-MM-dd HH:mm:ss:SSS', '+08:00') as "Started",TIME_FORMAT(MILLIS_TO_TIMESTAMP("end"), 'yyyy-MM-dd HH:mm:ss:SSS', '+08:00') as "Ended", "process.accept" as "Input Lines", "process.delivered" as "Output Lines", "process.drop" as "Filtered Lines", "process.failed" as "Failed Lines" limit 1000
```

----End

### 6.3.3.10 ER Dashboard Template

An enterprise router connects VPCs and on-premises networks to build a central hub network that features high-specification, high-bandwidth, and high-performance. Enterprise routers use the Border Gateway Protocol (BGP) to learn routes, dynamically select routes, or switch between connections, thereby significantly improving network scalability and O&M efficiency and ensuring service continuity.

LTS provides a one-stop wizard to collect enterprise router logs. It also supports multi-dimensional analysis and structuring, and offers a dashboard for enterprise router logs. This dashboard displays data such as the top 20 packets, top 20 traffic, and number of flow logs in enterprise router logs.

#### Prerequisites

- Flow logs have been collected from Enterprise Router. For details, see [Ingesting Enterprise Router Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

#### Enterprise Router Flow Log Center

**Step 1** Log in to the LTS console.

**Step 2** In the navigation pane, choose **Dashboards**.

**Step 3** Choose **ER dashboard templates** under **Dashboard Templates** and click **Enterprise Router Flow Log Center** to view the chart details.

- Filter by instance ID. The associated query and analysis statement is:  

```
SELECT DISTINCT(instance_id)
```
- Filter by attachment ID. The associated query and analysis statement is:  

```
SELECT DISTINCT(resource_id)
```
- **Traffic Flow.** You can filter the traffic data by **ingress** and **egress**. The associated query and analysis statement is:
- Filter by source IP address. The associated query and analysis statement is:  

```
SELECT DISTINCT(srcaddr)
```
- Filter by destination IP address. The associated query and analysis statement is:  

```
SELECT DISTINCT(dstaddr)
```
- Filter by protocol. The associated query and analysis statement is:  

```
SELECT DISTINCT(protocol)
```
- **Top 20 by Packets.** The associated query and analysis statement is:  

```
SELECT "srcaddr" as "Source IP", "dstaddr" as "Destination IP", sum("packets") as "Packets", "resource_id" as "Attachment ID", "instance_id" as "Instance ID" group by "instance_id", "resource_id", "srcaddr", "dstaddr" order by "Packets" desc limit 20
```
- **Top 20 by Traffic.** The associated query and analysis statement is:  

```
SELECT "srcaddr" as "Source IP", "dstaddr" as "Destination IP", sum("bytes") as "Bytes", "resource_id" as "Attachment ID", "instance_id" as "Instance ID" group by "instance_id", "resource_id", "srcaddr", "dstaddr" order by "Bytes" desc limit 20
```
- **Flow Logs.** The associated query and analysis statement is:  

```
select time_series(__time, 'PT1H', 'yyyy-MM-dd HH:mm:ss', '0', '+08:00') as "Time", count(*) as "Flow Logs" group by "Time" order by "Time"
```
- **Flow Log Details.** The associated query and analysis statement is:

```
SELECT "instance_id" as "Instance ID", "resource_id" as "Attachment ID", "project_id" as "Project ID",
"srcaddr" as "Source IP", "dstaddr" as "Destination IP", "srcport" as "Source Port", "dstport" as
"Destination Port", "protocol" as "Protocol", "direct" as "Traffic Flow", "packets" as "Packets", "bytes"
as "Bytes", TIME_FORMAT(MILLIS_TO_TIMESTAMP("start"*1000), 'yyyy-MM-dd HH:mm:ss', '+08:00')
as "Started", TIME_FORMAT(MILLIS_TO_TIMESTAMP("end"*1000), 'yyyy-MM-dd HH:mm:ss',
'+08:00') as "Ended"
```

----End

### 6.3.3.11 METRIC Dashboard Template

You can create metric rules on the LTS console to generate statistical reports as required. You can also set a single log filter or add associations and groups to set multiple log filters to retain logs that meet the filters. Statistics on the structured logs within a specified time range can be collected dynamically and displayed on the Prometheus instances of AOM, which is easy to operate and powerful.

#### Prerequisites

- A metric generation rule has been created. For details, see [Generating Metrics from Logs \(Beta\)](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

#### Monitoring Center for Metric Generation Tasks

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **METRIC dashboard templates** under **Dashboard Templates** and click **DSL processing task monitoring center** to view the chart details.

- **Filter by rule ID.** The associated query and analysis statement is:  

```
select distinct(task_set)
```
- **Input Lines.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "input" < 1000 THEN concat(cast("input" AS VARCHAR), 'Lines') WHEN
"input" < 1000 * 1000 THEN concat(cast(round("input"/ 1000, 1) AS VARCHAR), 'Thousands
lines') WHEN "input" < 1000000000 THEN concat(cast(round("input"/ 1000000.0, 1) AS
VARCHAR), 'Million lines') WHEN "input"/ 1000.0 < 1000000000 THEN
concat(cast(round("input"/ 1000 / 1000000.0, 1) AS VARCHAR), 'Billion lines') ELSE
concat(cast(round("input"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), 'Trillion lines') END
AS "total" from (select sum("input") as "input")
```
- **Output Lines.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "output" < 1000 THEN concat(cast("output" AS VARCHAR), 'Lines') WHEN
"output" < 1000 * 1000 THEN concat(cast(round("output"/ 1000, 1) AS VARCHAR), 'Thousands
lines') WHEN "output" < 1000000000 THEN concat(cast(round("output"/ 1000000.0, 1) AS
VARCHAR), 'Million lines') WHEN "output"/ 1000.0 < 1000000000 THEN
concat(cast(round("output"/ 1000 / 1000000.0, 1) AS VARCHAR), 'Billion lines') ELSE
concat(cast(round("output"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), 'Trillion lines') END
AS "total" from (select sum("output") as "output")
```
- **Filter Criteria Met.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "filters" < 1000 THEN concat(cast("filters" AS VARCHAR), 'Lines') WHEN
"filters" < 1000 * 1000 THEN concat(cast(round("filters"/ 1000, 1) AS VARCHAR), 'Thousands
lines') WHEN "filters" < 1000000000 THEN concat(cast(round("filters"/ 1000000.0, 1) AS
VARCHAR), 'Million lines') WHEN "filters"/ 1000.0 < 1000000000 THEN
concat(cast(round("filters"/ 1000 / 1000000.0, 1) AS VARCHAR), 'Billion lines') ELSE
concat(cast(round("filters"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), 'Trillion lines') END
AS "total" from (select sum("filters") as "filters")
```
- **Filter Criteria Unmet.** The associated query and analysis statement is:  

```
SELECT CASE WHEN "filter_drops" < 1000 THEN concat(cast("filter_drops" AS VARCHAR),
'Lines') WHEN "filter_drops" < 1000 * 1000 THEN concat(cast(round("filter_drops"/ 1000, 1) AS
```

```

VARCHAR) , 'Thousands lines') WHEN "filter_drops" < 1000000000 THEN
concat(cast(round("filter_drops"/ 1000000.0, 1) AS VARCHAR) , 'Million lines') WHEN
"filter_drops"/ 1000.0 < 1000000000 THEN concat(cast(round("filter_drops"/ 1000 / 1000000.0, 1)
AS VARCHAR) , 'Billion lines') ELSE concat(cast(round("filter_drops"/ 1000.0 / 1000 / 1000 / 1000 ,
1) AS VARCHAR) , 'Trillion lines') END AS "total" from (select sum("filter_drops") as "filter_drops")

```

- Sampled Lines.** The associated query and analysis statement is:

```

SELECT CASE WHEN "samples" < 1000 THEN concat(cast("samples" AS VARCHAR) , 'Lines')
WHEN "samples" < 1000 * 1000 THEN concat(cast(round("samples"/ 1000, 1) AS VARCHAR) ,
'Thousands lines') WHEN "samples" < 1000000000 THEN concat(cast(round("samples"/ 1000000.0,
1) AS VARCHAR) , 'Million lines') WHEN "samples"/ 1000.0 < 1000000000 THEN
concat(cast(round("samples"/ 1000 / 1000000.0, 1) AS VARCHAR) , 'Billion lines') ELSE
concat(cast(round("samples"/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR) , 'Trillion lines') END
AS "total" from (select sum("samples") as "samples")

```
- Unsampled Lines.** The associated query and analysis statement is:

```

SELECT CASE WHEN "sample_drops" < 1000 THEN concat(cast("sample_drops" AS VARCHAR) ,
'Lines') WHEN "sample_drops" < 1000 * 1000 THEN concat(cast(round("sample_drops"/ 1000, 1)
AS VARCHAR) , 'Thousands lines') WHEN "sample_drops" < 1000000000 THEN
concat(cast(round("sample_drops"/ 1000000.0, 1) AS VARCHAR) , 'Million lines') WHEN
"sample_drops"/ 1000.0 < 1000000000 THEN concat(cast(round("sample_drops"/ 1000 / 1000000.0,
1) AS VARCHAR) , 'Billion lines') ELSE concat(cast(round("sample_drops"/ 1000.0 / 1000 / 1000 /
1000, 1) AS VARCHAR) , 'Trillion lines') END AS "total" from (select sum("sample_drops") as
"sample_drops")

```
- Lines Out of Log Time Range.** The associated query and analysis statement is:

```

SELECT CASE WHEN "out_of_bounds" < 1000 THEN concat(cast("out_of_bounds" AS VARCHAR) ,
'Lines') WHEN "out_of_bounds" < 1000 * 1000 THEN concat(cast(round("out_of_bounds"/ 1000,
1) AS VARCHAR) , 'Thousands lines') WHEN "out_of_bounds" < 1000000000 THEN
concat(cast(round("out_of_bounds"/ 1000000.0, 1) AS VARCHAR) , 'Million lines') WHEN
"out_of_bounds"/ 1000.0 < 1000000000 THEN concat(cast(round("out_of_bounds"/ 1000 /
1000000.0, 1) AS VARCHAR) , 'Billion lines') ELSE concat(cast(round("out_of_bounds"/ 1000.0 /
1000 / 1000 / 1000, 1) AS VARCHAR) , 'Trillion lines') END AS "total" from (select
sum("out_of_bounds") as "out_of_bounds")

```
- Execute Records(Lines).** The associated query and analysis statement is:

```

select TIME_FORMAT("__time", 'yyyy-MM-dd HH:mm:ss:SSS', '+08:00') as "Log Time", sum("input")
as "Input",sum("output") as "Output",sum("filters") as "Filter Criteria Met",sum("filter_drops") as
"Filter Criteria Unmet",sum("samples") as "Sampled",sum("sample_drops") as
"Unsampled",sum("out_of_bounds") as "Out of Log Time Range" group by __time order by __time
desc limit 1000

```

----End

### 6.3.3.12 Nginx Dashboard Templates

LTS can collect Nginx logs and analyze them from multiple dimensions. LTS provides a one-stop wizard to collect Nginx logs. It also enables structuring and offers dashboards for Nginx logs. Nginx is a high-performance HTTP and reverse proxy web server that also provides IMAP, POP3, and SMTP services.

Nginx dashboard templates support [Viewing Nginx Monitoring by the Second](#), [Viewing Nginx Access Center](#), and [Viewing Nginx Monitoring Center](#).

## Prerequisites

Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

## Viewing Nginx Monitoring by the Second

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **NGINX dashboard templates** under **Dashboard Templates** and click **Nginx monitoring by the second** to view the chart details.

- **QPS.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(TIME_CEIL(__time,'PT1S'),'yyyy-MM-dd HH:mm:ss','+08:00') AS __time ,
COUNT(*) as QPS from log group by __time
```
- **Success Rate.** The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Success Rate" > 0 THEN "Success Rate" else 0 end,2) as "Success
Rate" from (select TIME_FORMAT(TIME_CEIL(__time,'PT5S'),'yyyy-MM-dd HH:mm:ss','+08:00') as
__time, sum(case when status < 400 then 1 else 0 end) * 100.0 / count(1) as 'Success Rate' from log
group by __time)
```
- **Latency.** The associated query and analysis statement is:  

```
select __time,round(CASE WHEN "Access latency" > 0 THEN "Access latency" else 0 end,2) as "Access
latency",round(CASE WHEN "Upstream latency" > 0 THEN "Upstream latency" else 0 end,2) as
"Upstream latency" from (select TIME_FORMAT(TIME_CEIL(__time,'PT5S'),'yyyy-MM-dd
HH:mm:ss','+08:00') as __time, avg(request_time)* 1000 as 'Access
latency',avg(upstream_response_time)* 1000 as 'Upstream latency' from log group by __time)
```
- **Traffic.** The associated query and analysis statement is:  

```
select TIME_FORMAT(TIME_CEIL(__time,'PT5S'),'yyyy-MM-dd HH:mm:ss','+08:00') as __time ,
sum("request_length") as "Incoming", sum("body_bytes_sent") as "Outgoing body" group by __time
```
- **Status Codes.** The associated query and analysis statement is:  

```
select t.t as "time",
CASE WHEN a."2XX" IS NOT NULL THEN CAST(a."2XX" AS BIGINT) ELSE 0 END as "2XX",
CASE WHEN b."3XX" IS NOT NULL THEN CAST(b."3XX" AS BIGINT) ELSE 0 END as "3XX",
CASE WHEN c."4XX" IS NOT NULL THEN CAST(c."4XX" AS BIGINT) ELSE 0 END as "4XX",
CASE WHEN d."5XX" IS NOT NULL THEN CAST(d."5XX" AS BIGINT) ELSE 0 END as "5XX",
CASE WHEN e."Other" IS NOT NULL THEN CAST(e."Other" AS BIGINT) ELSE 0 END as "Other"
from (select TIME_CEIL(__time,'PT5S') as t from log group by t order by t asc) t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "2XX" from log WHERE "status" >=
200 and "status" < 300 group by t order by t asc) a on t.t =a.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "3XX" from log WHERE "status" >=
300 and "status" < 400 group by t order by t asc) b on t.t =b.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "4XX" from log WHERE "status" >=
400 and "status" < 500 group by t order by t asc) c on t.t =c.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "5XX" from log WHERE "status" >=
500 and "status" < 600 group by t order by t asc) d on t.t =d.t left join (select
TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "Other" from log WHERE "status" <
200 or "status" >= 600 group by t order by t asc) e on t.t =e.t
```
- **Backend Response Codes.** The associated query and analysis statement is:  

```
select t.t as "time",
CASE WHEN a."2XX" IS NOT NULL THEN CAST(a."2XX" AS BIGINT) ELSE 0 END as "2XX",
CASE WHEN b."3XX" IS NOT NULL THEN CAST(b."3XX" AS BIGINT) ELSE 0 END as "3XX",
CASE WHEN c."4XX" IS NOT NULL THEN CAST(c."4XX" AS BIGINT) ELSE 0 END as "4XX",
CASE WHEN d."5XX" IS NOT NULL THEN CAST(d."5XX" AS BIGINT) ELSE 0 END as "5XX",
CASE WHEN e."Other" IS NOT NULL THEN CAST(e."Other" AS BIGINT) ELSE 0 END as "Other"
from (
select TIME_CEIL(__time,'PT5S') as t from log group by t order by t asc
) t
left join(
select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "2XX" from log WHERE
"upstream_status" >= 200 and "upstream_status" < 300 group by t order by t asc) a
on t.t = a.t
left join (
select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "3XX" from log WHERE
"upstream_status" >= 300 and "upstream_status" < 400 group by t order by t asc) b
on t.t =b.t
left join (
select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "4XX" from log WHERE
"upstream_status" >= 400 and "upstream_status" < 500 group by t order by t asc) c
on t.t =c.t
left join (
select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "5XX" from log WHERE
"upstream_status" >= 500 and "upstream_status" < 600 group by t order by t asc) d
on t.t =d.t
left join (
select TIME_CEIL(__time,'PT5S') as t , CAST(COUNT(1) as VARCHAR) as "Other" from log WHERE
```



```
"upstream_status" < 200 or "upstream_status" >= 600 group by t order by t asc) e
on t.t =e.t
```

----End

## Viewing Nginx Access Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **NGINX dashboard templates** under **Dashboard Templates** and click **Nginx access center** to view the chart details.

- **Day-over-day PV Change.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100, 2) as inc from(select compare( "pv" , 86400) as diff from (select count(1) as "pv" from log))
- **Week-on-week PV Change.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100, 2) as inc from(select compare( "pv" , 604800) as diff from (select count(1) as "pv" from log))
- **Day-over-day UV Change.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100, 2) as inc from(select compare( "uv" , 86400) as diff from (select APPROX\_COUNT\_DISTINCT(my\_remote\_addr) as "uv" from log))
- **Week-on-week UV Change.** The associated query and analysis statement is:  
select diff[1] as "total", round((diff[1] - diff[2]) / diff[2] \* 100, 2) as inc from(select compare( "uv" , 604800) as diff from (select APPROX\_COUNT\_DISTINCT(my\_remote\_addr) as "uv" from log))
- **PV Distribution (China).** The associated query and analysis statement is:  
select ip\_to\_province(remote\_addr) as province, count(1) as pv where IP\_TO\_COUNTRY (remote\_addr) = 'China' group by province HAVING province not in ('', 'Reserved address', '\*')
- **PV Distribution (Global).** The associated query and analysis statement is:  
SELECT ip\_to\_country(remote\_addr) as country, COUNT(1) as PV GROUP BY country HAVING country not in ('', 'Reserved address', '\*')
- **UV Distribution (China).** The associated query and analysis statement is:  
select ip\_to\_province(remote\_addr) as province, APPROX\_COUNT\_DISTINCT(remote\_addr) as UV where IP\_TO\_COUNTRY (remote\_addr) = 'China' group by province HAVING province not in ('', 'Reserved address', '\*')
- **UV Distribution (Global).** The associated query and analysis statement is:  
select ip\_to\_country(remote\_addr) as country, APPROX\_COUNT\_DISTINCT(remote\_addr) as uv group by country HAVING country not in ('', 'Reserved address', '\*')
- **Average Latency Distribution (China).** The associated query and analysis statement is:  
SELECT province, round( CASE WHEN "Average latency (ms)" > 0 THEN "Average latency (ms)" ELSE 0 END, 3 ) AS "Average latency (ms)" FROM (SELECT ip\_to\_province(remote\_addr) as province, avg(request\_time) \* 1000 AS "Average latency (ms)" WHERE IP\_TO\_COUNTRY (remote\_addr) = 'China' GROUP BY province HAVING province not in ('', 'Reserved address', '\*'))
- **Average Latency Distribution (Global).** The associated query and analysis statement is:  
SELECT country, round( CASE WHEN "Average latency (ms)" > 0 THEN "Average latency (ms)" ELSE 0 END, 2 ) AS "Average latency (ms)" FROM (SELECT ip\_to\_country(remote\_addr) as country, avg(request\_time) \* 1000 AS "Average latency (ms)" GROUP BY country HAVING country not in ('', 'Reserved address', '\*'))
- **PV/UV Today.** The associated query and analysis statement is:  
SELECT TIME\_FORMAT( \_\_time\_ , 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as \_\_time\_ , PV, UV FROM (select TIME\_CEIL(\_\_time\_ , 'PT600S') AS \_\_time\_ , count(1) as PV, APPROX\_COUNT\_DISTINCT(my\_remote\_addr) as UV from log WHERE \_\_time\_ <= CURRENT\_TIMESTAMP and \_\_time\_ >= DATE\_TRUNC( 'DAY', (CURRENT\_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR group by \_\_time\_ order by \_\_time\_ ) WHERE \_\_time\_ <= CURRENT\_TIMESTAMP LIMIT 100000 OFFSET 1
- **PV/UV in 7 Days.** The associated query and analysis statement is:  
SELECT TIME\_FORMAT( \_\_time\_ , 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as \_\_time\_ , PV, UV FROM (select TIME\_CEIL(\_\_time\_ , 'PT600S') AS \_\_time\_ , count(1) as PV, APPROX\_COUNT\_DISTINCT(remote\_addr) as



```
UV from log WHERE __time <= CURRENT_TIMESTAMP and __time >= DATE_TRUNC('DAY',
(CURRENT_TIMESTAMP + INTERVAL '8' HOUR)) - INTERVAL '8' HOUR - INTERVAL '7' DAY group by
__time_ order by __time_) WHERE __time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```

- **Top 10 Provinces by Visits.** The associated query and analysis statement is:  
select ip\_to\_province(remote\_addr) as "province", count(1) as "Visits" group by "province" HAVING "province" <> '-1' order by "Visits" asc limit 10
- **Top 10 Cities by Visits.** The associated query and analysis statement is:  
select ip\_to\_city(remote\_addr) as "city", count(1) as "Visits" group by "city" HAVING "city" <> '-1' order by "Visits" asc limit 10
- **Top 10 Hosts by Visits.** The associated query and analysis statement is:  
select host as "Host", count(1) as "PV" group by "Host" order by "PV" asc limit 10
- **Top 10 UserAgents by Visits.** The associated query and analysis statement is:  
select http\_user\_agent as "UserAgent", count(1) as "PV" group by "UserAgent" order by "PV" asc limit 10
- **Device Distribution by Type.** The associated query and analysis statement is:  
select case when regexp\_like(lower(http\_user\_agent), 'iphone|ipod|android|ios') then 'Mobile' else 'PC' end as type , count(1) as total group by type
- **Device Distribution by System.** The associated query and analysis statement is:  
select case when regexp\_like(lower(http\_user\_agent), 'iphone|ipod|ios') then 'IOS' when regexp\_like(lower(http\_user\_agent), 'android') then 'Android' else 'other' end as type , count(1) as total group by type HAVING type != 'other'
- **TOP URL.** The associated query and analysis statement is:  
select request\_uri , count(1) as PV, APPROX\_COUNT\_DISTINCT(remote\_addr) as UV, round(sum( case when status < 400 then 1 else 0 end ) \* 100.0 / count(1), 2) as "Access Success Rate" group by request\_uri ORDER by PV desc
- **Top IP Addresses by Visits.** The associated query and analysis statement is:  
select remote\_addr as "Source IP Address",ip\_to\_country(remote\_addr) as "Country/Region",ip\_to\_province(remote\_addr) as "Province",ip\_to\_city(remote\_addr) as "City",ip\_to\_provider(remote\_addr) as "Carrier",count(1) as "PV",http\_user\_agent as "UserAgent Sampling",request\_uri as "URL Sampling" group by remote\_addr,http\_user\_agent,request\_uri ORDER by "PV" desc

----End

## Viewing Nginx Monitoring Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **NGINX dashboard templates** under **Dashboard Templates** and click **Nginx monitoring center** to view the chart details.

- **PV.** The associated query and analysis statement is:  
SELECT TIME\_FORMAT( \_\_time\_ , 'yyyy-MM-dd HH:mm:ss', '+08:00' ) as \_\_time\_ , PV FROM ( SELECT TIME\_CEIL ( \_\_time\_ , 'PT300S' ) AS \_\_time\_ , count( 1 ) AS PV FROM log GROUP BY \_\_time\_ ) WHERE \_\_time\_ <= CURRENT\_TIMESTAMP LIMIT 100 OFFSET 1
- **Request Success Rate.** The associated query and analysis statement is:  
select ROUND(sum(case when status < 400 then 1 else 0 end ) \* 100.0 / count(1),2) as cnt
- **Average Latency.** The associated query and analysis statement is:  
select round(avg(request\_time) \* 1000, 3) as cnt
- **4xx Requests.** The associated query and analysis statement is:  
SELECT COUNT(1) as cnt WHERE "status" >= 400 and "status" < 500
- **404 Requests.** The associated query and analysis statement is:  
SELECT COUNT(1) as cnt WHERE "status" = 404
- **429 Requests.** The associated query and analysis statement is:  
SELECT COUNT(1) as cnt WHERE "status" = 429
- **504 Requests.** The associated query and analysis statement is:  
SELECT COUNT(1) as cnt WHERE "status" = 504

- **5xx Requests.** The associated query and analysis statement is:  

```
select TIME_FORMAT(TIME_CEIL(_time,'PT300S'),'yyyy-MM-dd HH:mm:ss','+08:00') AS _time_,
count(1) as cnt where "status" >= 500 group by _time_
```
- **Status Code Distribution.** The associated query and analysis statement is:  

```
SELECT status, COUNT(1) AS rm GROUP BY status
```
- **UV.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_ , 'yyyy-MM-dd HH:mm:ss', '+08:00') as _time_,UV FROM (select
TIME_CEIL(_time,'PT600S') AS _time_ , APPROX_COUNT_DISTINCT(remote_addr) as UV from log
group by _time_) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```
- **Traffic.** The associated query and analysis statement is:  

```
select TIME_FORMAT(_time_,'yyyy-MM-dd HH:mm:ss','+08:00') AS _time_,round(CASE WHEN
"Inbound" > 0 THEN "Inbound" ELSE 0 END, 2) AS "Inbound",round(CASE WHEN "Outbound" > 0
THEN "Outbound" ELSE 0 END, 2) AS "Outbound" FROM (SELECT TIME_CEIL(_time,'PT600S') AS
time,sum(request_length) / 1024.0 AS "Inbound",sum(bytes_sent) / 1024.0 AS "Outbound" group
by _time_) WHERE _time_ <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```
- **Access Failure Rate.** The associated query and analysis statement is:  

```
SELECT TIME_FORMAT(_time_ , 'yyyy-MM-dd HH:mm:ss', '+08:00') as _time_,round(CASE WHEN
"Failure rate" > 0 THEN "Failure rate" ELSE 0 END, 2) AS "Failure rate",round(CASE WHEN "5XX" > 0
THEN "5XX" ELSE 0 END, 2) AS "5XX" from (select TIME_CEIL(_time,'PT600S') AS _time_,sum(case
when status >= 400 then 1 else 0 end) * 100.0 / count(1) as 'Failure rate' , sum(case when status
>=500 then 1 ELSE 0 END)*100.0/COUNT(1) as '5XX' group by _time_) WHERE _time_ <=
CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```
- **Latency.** The associated query and analysis statement is:  

```
select TIME_FORMAT(_time_ , 'yyyy-MM-dd HH:mm:ss', '+08:00') as _time_,round(CASE WHEN
"Avg." > 0 THEN "Avg." ELSE 0 END, 2) AS "Avg.",round(CASE WHEN "P50" > 0 THEN "P50" ELSE 0
END, 2) AS "P50",round(CASE WHEN "P90" > 0 THEN "P90" ELSE 0 END, 2) AS "P90",round(CASE
WHEN "P99" > 0 THEN "P99" ELSE 0 END, 2) AS "P99",round(CASE WHEN "P9999" > 0 THEN
"P9999" ELSE 0 END, 2) AS "P9999" from (select TIME_CEIL(_time,'PT600S') as
time,avg(request_time) * 1000 as "Avg.", APPROX_QUANTILE_DS("request_time", 0.50)*1000 as
"P50", APPROX_QUANTILE_DS("request_time", 0.90)*1000 as
"P90",APPROX_QUANTILE_DS("request_time", 0.99)*1000 as
'P99',APPROX_QUANTILE_DS("request_time", 0.9999)*1000 as 'P9999' group by _time_) WHERE
time <= CURRENT_TIMESTAMP LIMIT 100000 OFFSET 1
```
- **Top Host Requests.** The associated query and analysis statement is:  

```
SELECT "host", pv, uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate
(%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0
THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN
"Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN
"Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT
"host", count(1) AS pv, APPROX_COUNT_DISTINCT (remote_addr) AS uv, sum(CASE WHEN
"status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)",
avg(request_time) * 1000 AS "Average Latency (ms)", sum(request_length) / 1024.0 AS "Inbound
(KB)", sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "host" != " " GROUP BY "host")
ORDER BY pv DESC
```
- **Top Host Latencies.** The associated query and analysis statement is:  

```
SELECT "host", pv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate
(%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0
THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "P90
Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE
WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)"
FROM (SELECT "host", count(1) AS pv, sum(CASE WHEN "status" < 400 THEN 1 ELSE 0 END) *
100.0 / count(1) AS "Access Success Rate (%)", avg(request_time) * 1000 AS "Average Latency
(ms)",APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)",
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != "
GROUP BY "host") ORDER BY "Average Latency (ms)" desc
```
- **Top Host Failure Rates.** The associated query and analysis statement is:  

```
SELECT "host", pv,round(CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)"
ELSE 0 END, 2) AS "Access Failure Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN
"Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "P90
Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE
WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)"
FROM (SELECT "host", count(1) AS pv, sum(CASE WHEN "status" >= 400 THEN 1 ELSE 0 END) *
100.0 / count(1) AS "Access Failure Rate (%)", avg(request_time) * 1000 AS "Average Latency
(ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)",
```

```
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != " "
GROUP BY "host") ORDER BY "Access Failure Rate (%)" desc
```

- **Top URL Requests.** The associated query and analysis statement is:  

```
SELECT request_uri, pv,uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN "Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT request_uri, count(1) AS pv, APPROX_COUNT_DISTINCT (remote_addr) AS uv, sum(CASE WHEN "status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)", avg(request_time) * 1000 AS "Average Latency (ms)", sum(request_length) / 1024.0 AS "Inbound (KB)", sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "host" != " " GROUP BY request_uri) ORDER BY pv desc
```
- **Top URL Latencies.** The associated query and analysis statement is:  

```
SELECT request_uri, pv,round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)" ELSE 0 END, 2) AS "Access Success Rate (%)",round(CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)",round(CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)",round(CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)" FROM (SELECT request_uri, count(1) AS pv, sum(CASE WHEN "status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)", avg(request_time) * 1000 AS "Average Latency (ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)", APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != " " GROUP BY request_uri) ORDER BY "Average Latency (ms)" desc
```
- **Top URL Failure Rates.** The associated query and analysis statement is:  

```
SELECT request_uri, pv, round(CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)" ELSE 0 END, 2) AS "Access Failure Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)",round(CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)" FROM(SELECT request_uri, count(1) AS pv, sum(CASE WHEN "status" >= 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Failure Rate (%)", avg(request_time) * 1000 AS "Average Latency (ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)", APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != " " GROUP BY request_uri)ORDER BY "Access Failure Rate (%)" desc
```
- **Top Backend Requests.** The associated query and analysis statement is:  

```
SELECT addr, pv, uv, round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)" ELSE 0 END, 2) AS "Access Success Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "Inbound (KB)" > 0 THEN "Inbound (KB)" ELSE 0 END, 3) AS "Inbound (KB)", round(CASE WHEN "Outbound (KB)" > 0 THEN "Outbound (KB)" ELSE 0 END, 3) AS "Outbound (KB)" FROM (SELECT upstream_addr as addr, count(1) AS pv, APPROX_COUNT_DISTINCT (remote_addr) AS uv, sum(CASE WHEN "status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)", avg(request_time) * 1000 AS "Average Latency (ms)", sum(request_length) / 1024.0 AS "Inbound (KB)", sum(bytes_sent) / 1024.0 AS "Outbound (KB)" WHERE "host" != " " GROUP BY addr having length(upstream_addr) > 2) ORDER BY "pv" desc
```
- **Top Backend Latencies.** The associated query and analysis statement is:  

```
SELECT addr,pv,round(CASE WHEN "Access Success Rate (%)" > 0 THEN "Access Success Rate (%)" ELSE 0 END, 2) AS "Access Success Rate (%)",round(CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)",round(CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)",round(CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)" FROM (SELECT upstream_addr as addr,count(1) AS pv,sum(CASE WHEN "status" < 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Success Rate (%)",avg(request_time) * 1000 AS "Average Latency (ms)",APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)",APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != " " GROUP BY addr having length(upstream_addr) > 2) ORDER BY "Average Latency (ms)" desc
```
- **Top Backend Failure Rates.** The associated query and analysis statement is:  

```
SELECT addr, pv, round(CASE WHEN "Access Failure Rate (%)" > 0 THEN "Access Failure Rate (%)" ELSE 0 END, 2) AS "Access Failure Rate (%)", round(CASE WHEN "Average Latency (ms)" > 0 THEN "Average Latency (ms)" ELSE 0 END, 3) AS "Average Latency (ms)", round(CASE WHEN "P90 Latency (ms)" > 0 THEN "P90 Latency (ms)" ELSE 0 END, 3) AS "P90 Latency (ms)", round(CASE WHEN "P99 Latency (ms)" > 0 THEN "P99 Latency (ms)" ELSE 0 END, 3) AS "P99 Latency (ms)" FROM (SELECT upstream_addr as addr, count(1) AS pv, sum(CASE WHEN "status" >= 400 THEN 1 ELSE 0 END) * 100.0 / count(1) AS "Access Failure Rate (%)", avg(request_time) * 1000 AS "Average Latency (ms)", APPROX_QUANTILE_DS(request_time, 0.9) * 1000 AS "P90 Latency (ms)",
```

```
APPROX_QUANTILE_DS(request_time, 0.99) * 1000 AS "P99 Latency (ms)" WHERE "host" != "
GROUP BY addr having length(upstream_addr) > 2)ORDER BY "Access Failure Rate (%)" desc
```

----End

### 6.3.3.13 VPC Dashboard Template

A VPC is an isolated and private virtual network environment. You can configure the IP address ranges, subnets, and security groups, assign EIPs, and allocate bandwidth for a VPC. A VPC flow log records traffic information. It helps you monitor network traffic, analyze network attacks, and validate security group and Access Control List (ACL) rules.

LTS provides a one-stop wizard to collect VPC logs. It also enables structuring and offers a dashboard for VPC logs. The **VPC Flow Logs** dashboard displays the total number of actions, accepted bytes/packets, rejected bytes/packets, action sources, number of actions per minute, action distribution, flow log records distribution by status, carrier distribution of action sources, top 5 source/destination addresses by bytes, packets per minute, and ENIs of each protocol.

#### Prerequisites

- Logs have been collected from VPC. For details, see [Ingesting VPC Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

#### Viewing VPC Flow Logs

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

**Step 2** In the **Log Applications** area, click **VPC Flow Log Center** and choose **Go to the Dashboard**.

**Step 3** Choose **VPC dashboard templates** under **Dashboard Templates** and click **VPC Flow Logs** to view the chart details.

- **Total Actions.** The associated query and analysis statement is:  

```
select CASE WHEN total_actions < 1000 THEN concat(cast(total_actions AS VARCHAR), 'Actions')
WHEN total_actions < 1000 * 1000 THEN concat(cast(round(total_actions / 1000.0, 2) AS
VARCHAR),'Thousand actions') WHEN total_actions < 1000000000 THEN
concat(cast(round(total_actions / 1000000.0, 2) AS VARCHAR),'Million actions') WHEN total_actions /
1000.0 < 1000000000 THEN concat(cast(round(total_actions / 1000 / 1000000.0, 1) AS
VARCHAR),'Billion actions') ELSE concat(cast(round(total_actions / 1000.0 / 1000 / 1000, 1) AS
VARCHAR),'Trillion actions') END AS "total_actions" from (select count(1) as total_actions where
log_status='OK' and version=1)
```
- **Total Accepted Bytes.** The associated query and analysis statement is:  

```
select CASE WHEN accept_bytes < 1024 THEN concat(cast(accept_bytes AS VARCHAR), 'B') WHEN
accept_bytes < 1024 * 1024 THEN concat(cast(round(accept_bytes / 1024, 2) AS VARCHAR),'KB')
WHEN accept_bytes < 1000000000 THEN concat(cast(round(accept_bytes /1024.0 /1024, 2) AS
VARCHAR),'MB') WHEN accept_bytes / 1000.0 < 1000000000 THEN concat(cast(round(accept_bytes /
1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE concat(cast(round(accept_bytes / 1000.0 / 1000 /
1000 / 1000, 1) AS VARCHAR),'TB') END AS "accept_bytes" from (select sum(bytes) as accept_bytes
where log_status='OK' and version=1 and action='ACCEPT')
```
- **Total Accepted Packets.** The associated query and analysis statement is:  

```
select CASE WHEN accept_packets < 1024 THEN concat(cast(accept_packets AS VARCHAR), 'B')
WHEN accept_packets < 1024 * 1024 THEN concat(cast(round(accept_packets / 1024, 2) AS
VARCHAR),'KB') WHEN accept_packets < 1000000000 THEN concat(cast(round(accept_packets /
1024.0 /1024, 2) AS VARCHAR),'MB') WHEN accept_packets / 1000.0 < 1000000000 THEN
concat(cast(round(accept_packets / 1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE
```

```
concat(cast(round(accept_packets / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR),'TB') END AS
"accept_packets" from (select sum(packets) as accept_packets where log_status='OK' and version=1
and action='ACCEPT')
```

- **Total Rejected Bytes.** The associated query and analysis statement is:  

```
select CASE WHEN reject_bytes < 1024 THEN concat(cast(reject_bytes AS VARCHAR), 'B') WHEN
reject_bytes < 1024 * 1024 THEN concat(cast(round(reject_bytes / 1024, 2) AS VARCHAR),'KB') WHEN
reject_bytes < 1000000000 THEN concat(cast(round(reject_bytes /1024.0 /1024, 2) AS
VARCHAR),'MB') WHEN reject_bytes / 1000.0 < 1000000000 THEN concat(cast(round(reject_bytes /
1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE concat(cast(round(reject_bytes / 1000.0 / 1000 / 1000 /
1000, 1) AS VARCHAR),'TB') END AS "reject_bytes" from (select sum(bytes) as reject_bytes where
log_status='OK' and version=1 and action='REJECT')
```
- **Total Rejected Packets.** The associated query and analysis statement is:  

```
select CASE WHEN reject_packets < 1024 THEN concat(cast(reject_packets AS VARCHAR), 'B') WHEN
reject_packets < 1024 * 1024 THEN concat(cast(round(reject_packets / 1024, 2) AS VARCHAR),'KB')
WHEN reject_packets < 1000000000 THEN concat(cast(round(reject_packets /1024.0 /1024, 2) AS
VARCHAR),'MB') WHEN reject_packets / 1000.0 < 1000000000 THEN
concat(cast(round(reject_packets / 1024 / 1000000.0, 2) AS VARCHAR),'GB') ELSE
concat(cast(round(reject_packets / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR),'TB') END AS
"reject_packets" from (select sum(packets) as reject_packets where log_status='OK' and version=1 and
action='REJECT')
```
- **Action Sources.** The associated query and analysis statement is:  

```
select IP_TO_PROVINCE(srcaddr) as province, count(1) as total_actions where IP_TO_COUNTRY
(srcaddr) = 'China' group by province HAVING address not in ('','Reserved address','*')
```
- **Actions/Min.** The associated query and analysis statement is:  

```
select TIME_FORMAT(date_trunc('minute', MILLIS_TO_TIMESTAMP("start" * 1000)),'MM-dd HH:mm')
as "t", "action", count(1) as "total_actions" where log_status='OK' and version=1 group by "t",
"action" order by t asc limit 1000
```
- **Action Results.** The associated query and analysis statement is:  

```
select action, count(1) as total_actions where log_status='OK' and version=1 group by action
```
- **Flow Log Records By Status.** The associated query and analysis statement is:  

```
select log_status, count(1) as total_actions where version=1 group by log_status
```
- **Carriers of Action Source.** The associated query and analysis statement is:  

```
select ip_to_provider(srcaddr) as src_addr_provider, count(1) as total_actions where log_status='OK'
and version=1 group by src_addr_provider order by total_actions desc limit 5
```
- **Top 5 Sources by Bytes.** The associated query and analysis statement is:  

```
select ip_to_provider(srcaddr) as src_addr_provider, count(1) as total_actions where log_status='OK'
and version=1 group by src_addr_provider order by total_actions desc limit 5
```
- **Top 5 Destinations by Bytes.** The associated query and analysis statement is:  

```
select dstaddr, sum(bytes) as total_bytes where log_status='OK' and version=1 group by dstaddr order
by total_bytes desc limit 5
```
- **Top 5 Destination Ports by Packets.** The associated query and analysis statement is:  

```
select dstport, sum(packets) as total_packets where log_status='OK' and version=1 group by dstport
order by total_packets desc limit 5
```
- **Packets/Min by Protocol.** The associated query and analysis statement is:  

```
select TIME_FORMAT(date_trunc('minute', MILLIS_TO_TIMESTAMP("start" * 1000)),'MM-dd HH:mm')
as t, protocol, sum(packets) as total_packets where log_status='OK' and version=1 group by t,
protocol order by t asc limit 1000
```
- **ENIs.** The associated query and analysis statement is:  

```
select interface_id as "ID", sum(packets) as 'Data Packets', sum(bytes) as 'Data Packet Size' where
log_status='OK' and version=1 group by "ID"
```

----End

### 6.3.3.14 WAF Dashboard Templates

WAF keeps web services stable and secure. It examines all HTTP and HTTPS requests to detect and block the following attacks: Structured Query Language (SQL) injection, cross-site scripting (XSS), web shells, command and code

injections, file inclusion, sensitive file access, third-party vulnerability exploits, Challenge Collapsar (CC) attacks, malicious crawlers, and cross-site request forgery (CSRF).

For [Log Search and Analysis](#), the corresponding WAF dashboard templates are those for [Viewing WAF Security Log Center](#) and [Viewing WAF Access Log Center](#).

## Prerequisites

- Logs have been collected from WAF. For details, see [Ingesting WAF Logs to LTS](#).
- Logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).

## Viewing WAF Security Log Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **WAF dashboard templates** under **Dashboard Templates** and click **WAF security log center** to view the chart details.

- **Attacked Websites.** The associated query and analysis statement is:

```
SELECT diff [1] AS "VALUE", COALESCE (diff [1]- diff [2], 0) AS "BEFORE" FROM
(
 SELECT
 compare ("DATA", 86400) AS diff
 FROM
 (SELECT count(DISTINCT "host") AS "DATA" FROM log
 WHERE action != "
))
```

- **Originating Countries.** The associated query and analysis statement is:

```
SELECT
diff [1] AS
"VALUE"
,
COALESCE (diff [1]- diff [2], 0) AS "BEFORE"
FROM
(
 SELECT
 compare ("DATA", 86400) AS diff
 FROM
 (SELECT count(DISTINCT ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END))
AS "DATA" FROM log
 WHERE action != "
)
)
```

- **Web Attacks Intercepted.** The associated query and analysis statement is:

```
SELECT
CASE
 WHEN
 diff [1] < 1000 THEN
 concat(cast(diff [1] AS VARCHAR), ' attacks')
 WHEN diff [1] < 1000 * 1000 THEN
 concat(cast(round(diff [1]/ 1000, 1) AS VARCHAR), ' thousand attacks')
 WHEN diff [1] < 1000000000 THEN
 concat(cast(round(diff [1]/ 1000000.0, 1) AS VARCHAR), ' million attacks')
 WHEN diff [1]/ 1000.0 < 1000000000 THEN
 concat(cast(round(diff [1]/ 1000.0 / 1000000, 1) AS VARCHAR), ' billion attacks') ELSE
 concat(cast(round(diff [1]/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), ' trillion attacks')
 END AS
"value"
```

```

,
CASE WHEN diff [2]= 0 THEN 0 ELSE round(diff [3]- 1, 2) END AS ratio
FROM
(SELECT compare ("data", 86400) AS diff FROM (SELECT count(1) AS "data" FROM log
WHERE action = "))

```

- **CC Attacks Intercepted.** The associated query and analysis statement is:

```

SELECT
CASE
WHEN
diff [1] < 1000 THEN
concat(cast(diff [1] AS VARCHAR), ' attacks')
WHEN diff [1] < 1000 * 1000 THEN
concat(cast(round(diff [1]/ 1000, 1) AS VARCHAR), ' thousand attacks')
WHEN diff [1] < 1000000000 THEN
concat(cast(round(diff [1]/ 1000000.0, 1) AS VARCHAR), ' million attacks')
WHEN diff [1]/ 1000.0 < 1000000000 THEN
concat(cast(round(diff [1]/ 1000.0 / 1000000, 1) AS VARCHAR), ' billion attacks') ELSE
concat(cast(round(diff [1]/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), ' trillion attacks')
END AS
"value"
,
CASE WHEN diff [2]= 0 THEN 0 ELSE round(diff [3]- 1, 2) END AS ratio
FROM
(SELECT compare ("data", 86400) AS diff FROM (SELECT count(1) AS "data" FROM log
WHERE attack != 'default'))

```

- **Attacker UV.** The associated query and analysis statement is:

```

SELECT
CASE
WHEN
diff [1] < 1000 THEN
concat(cast(cast (diff [1] AS INTEGER) AS VARCHAR), ' attackers')
WHEN diff [1] < 1000 * 1000 THEN
concat(cast(round(diff [1]/ 1000, 1) AS VARCHAR), ' thousand attackers')
WHEN diff [1] < 1000000000 THEN
concat(cast(round(diff [1]/ 1000000.0, 1) AS VARCHAR), ' million attackers')
WHEN diff [1]/ 1000.0 < 1000000000 THEN
concat(cast(round(diff [1]/ 1000.0 / 1000000, 1) AS VARCHAR), ' billion attackers') ELSE
concat(cast(round(diff [1]/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), ' trillion attackers')
END AS "value",
CASE WHEN diff [2]= 0 THEN 0 ELSE round(diff [3]- 1, 2) END AS ratio
FROM
(
SELECT
compare ("data", 86400) AS diff
FROM
(SELECT count(DISTINCT CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS "data"
FROM log
))

```

- **Total Attacks Intercepted.** The associated query and analysis statement is:

```

SELECT
CASE
WHEN
diff [1] < 1000 THEN
concat(cast(diff [1] AS VARCHAR), ' attacks')
WHEN diff [1] < 1000 * 1000 THEN
concat(cast(round(diff [1]/ 1000, 1) AS VARCHAR), ' thousand attacks')
WHEN diff [1] < 1000000000 THEN
concat(cast(round(diff [1]/ 1000000.0, 1) AS VARCHAR), ' million attacks')
WHEN diff [1]/ 1000.0 < 1000000000 THEN
concat(cast(round(diff [1]/ 1000.0 / 1000000, 1) AS VARCHAR), ' billion attacks') ELSE
concat(cast(round(diff [1]/ 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), ' trillion attacks')
END AS
"value",
CASE WHEN diff [2]= 0 THEN 0 ELSE round(diff [3]- 1, 2) END AS "ratio"
FROM
(
SELECT

```

```
compare ("data", 86400) AS diff
FROM
(SELECT count(1) AS "data" FROM log WHERE action != ")
)
```

- **CC Attacks.** The associated query and analysis statement is:

```
SELECT
ip_to_province (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS province,
count(1) AS " attacks"
WHERE attack != 'default' and ip_to_country(CASE WHEN sip = '-' THEN remote_ip ELSE sip END)
= 'China'
GROUP BY
province
```

- **Attack Types.** The associated query and analysis statement is:

```
SELECT time_format(MILLIS_TO_TIMESTAMP(TIMESTAMP_TO_MILLIS(__time) -
MOD(TIMESTAMP_TO_MILLIS(__time), 3600)), 'HH:mm') AS dt, count(1) AS cnt, CASE WHEN
action = 'block' THEN 'Intercepted' WHEN action = 'log' THEN 'Log only' WHEN action = 'captcha'
THEN 'Verification code' END AS attack FROM log WHERE action != " GROUP BY
TIMESTAMP_TO_MILLIS(__time) - MOD(TIMESTAMP_TO_MILLIS(__time), 3600), attack ORDER BY cnt
DESC
```

- **Web Attacks.** The associated query and analysis statement is:

```
SELECT
ip_to_province (
CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS province,
count(1) AS " attacks"
WHERE action = 'block' and ip_to_country(CASE WHEN sip = '-' THEN remote_ip ELSE sip END) =
'China'
GROUP BY
province
```

- **CC Attacks(World).** The associated query and analysis statement is:

```
SELECT
ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS country,
count(1) AS " attacks"
WHERE attack != 'default'
GROUP BY
country
```

- **Web Attacks(World).** The associated query and analysis statement is:

```
SELECT
ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS country,
count(1) AS " attacks"
WHERE action = 'block'
GROUP BY
country
```

----End

## Viewing WAF Access Log Center

**Step 1** Log in to the LTS console. In the navigation pane, choose **Dashboards**.

**Step 2** Choose **WAF dashboard templates** under **Dashboard Templates** and click **WAF access log center** to view the chart details.

- **PV.** The associated query and analysis statement is:

```
SELECT CASE WHEN diff [1] < 1000 THEN concat(cast(diff [1] AS
VARCHAR), ") WHEN diff [1] < 1000 * 1000 THEN concat(cast(round(diff [1] / 1000,
1) AS VARCHAR), ' thousand') WHEN diff [1] < 1000000000 THEN
concat(cast(round(diff [1] / 1000000.0, 1) AS VARCHAR), ' million') WHEN diff [1] / 1000.0
< 1000000000 THEN concat(cast(round(diff [1] / 1000 / 1000000.0, 1) AS VARCHAR), '
billion') ELSE concat(cast(round(diff [1] / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), '
trillion') END AS "VALUE" , CASE WHEN diff [2] = 0 THEN 0 ELSE round(diff [3] -
1, 2) END AS ratio FROM (SELECT compare (DATA, 86400) AS diff FROM
(SELECT count(1) AS DATA FROM log))
```

- **UV.** The associated query and analysis statement is:



```
SELECT CASE WHEN diff [1] < 1000 THEN concat(cast(diff [1] AS
VARCHAR), '') WHEN diff [1] < 1000 * 1000 THEN concat(cast(round(diff [1] / 1000,
1) AS VARCHAR), ' thousand') WHEN diff [1] < 1000000000 THEN
concat(cast(round(diff [1] / 1000000.0, 1) AS VARCHAR), ' million') WHEN diff [1] / 1000.0
< 1000000000 THEN concat(cast(round(diff [1] / 1000 / 1000000.0, 1) AS VARCHAR), '
billion') ELSE concat(cast(round(diff [1] / 1000.0 / 1000 / 1000 / 1000, 1) AS VARCHAR), '
trillion') END AS "VALUE" , CASE WHEN diff [2] = 0 THEN 0 ELSE
round(diff [3] - 1, 2) END AS ratio FROM (SELECT compare (DATA, 86400)
AS diff FROM (SELECT count(DISTINCT CASE WHEN sip = '-' THEN remote_ip ELSE sip
END) AS "DATA" FROM log))
```

- **Incoming Traffic.** The associated query and analysis statement is:

```
SELECT CASE WHEN diff [1] < 102 THEN concat(cast(diff [1] AS
VARCHAR), ' B') WHEN diff [1] < 1024 * 1024 THEN concat(cast(round(diff [1] / 1024,
1) AS VARCHAR), ' KB') WHEN diff [1] < 1024 * 1024 * 1024 THEN
concat(cast(round(diff [1] / 1024.0 / 1024, 1) AS VARCHAR), ' MB') WHEN diff [1] / 1024.0
< 1024 * 1024 * 1024 THEN concat(cast(round(diff [1] / 1024.0 / 1024 / 1024, 1) AS
VARCHAR), ' GB') ELSE concat(cast(round(diff [1] / 1024.0 / 1024 / 1024 / 1024, 1) AS
VARCHAR), ' TB') END AS "VALUE" , CASE WHEN diff [2] = 0 THEN
0 ELSE round(diff [3] - 1, 2) END AS ratio FROM (SELECT compare ("DATA",
86400) AS diff FROM (SELECT COALESCE (sum(request_length), 0) AS "DATA" FROM
log))
```

- **Peak In-Bandwidth.** The associated query and analysis statement is:

```
SELECT CASE WHEN diff [1] < 102 THEN concat(cast(round(diff [1], 2) AS
VARCHAR), ' B/s') WHEN diff [1] < 1024 * 1024 THEN concat(cast(round(diff [1] /
1024, 1) AS VARCHAR), ' KB/s') WHEN diff [1] < 1024 * 1024 * 1024 THEN
concat(cast(round(diff [1] / 1024.0 / 1024, 1) AS VARCHAR), ' MB/s') WHEN diff [1] /
1024.0 < 1024 * 1024 * 1024 THEN concat(cast(round(diff [1] / 1024.0 / 1024 / 1024, 1) AS
VARCHAR), ' GB/s') ELSE concat(cast(round(diff [1] / 1024.0 / 1024 / 1024 / 1024, 1) AS
VARCHAR), ' TB/s') END AS "VALUE" , CASE WHEN diff [2] = 0
THEN 0 ELSE round(diff [3] - 1, 2) END AS ratio FROM (SELECT compare
("DATA", 86400) AS diff FROM (SELECT COALESCE (max("DATA"), 0) AS
"DATA" FROM (SELECT TIME_FLOOR(_time, 'PT1M') AS dt, sum(request_length) / 60.0 AS
"DATA" FROM log GROUP BY dt LIMIT 10000)))
```

- **Peak Out-Bandwidth.** The associated query and analysis statement is:

```
SELECT CASE WHEN diff [1] < 102 THEN concat(cast(round(diff [1], 2) AS VARCHAR), ' B/s')
WHEN diff [1] < 1024 * 1024 THEN concat(cast(round(diff [1] / 1024, 1) AS VARCHAR), ' KB/s')
WHEN diff [1] < 1024 * 1024 * 1024 THEN concat(cast(round(diff [1] / 1024.0 / 1024, 1) AS
VARCHAR), ' MB/s') WHEN diff [1] / 1024.0 < 1024 * 1024 * 1024 THEN concat(cast(round(diff
[1] / 1024.0 / 1024 / 1024, 1) AS VARCHAR), ' GB/s') ELSE concat(cast(round(diff [1] / 1024.0 /
1024 / 1024 / 1024, 1) AS VARCHAR), ' TB/s') END AS "value", case when diff [2] = 0 then 0 else
round(diff [3] - 1, 2) END AS "ratio" FROM (SELECT compare ("DATA", 86400) AS diff FROM
(SELECT COALESCE (max(bytes_out), 0) AS "DATA" FROM (SELECT time_ceil(_time, 'PT1M') AS
dt, sum(body_bytes_sent) / 60.0 AS bytes_out FROM log GROUP BY dt LIMIT 10000)))
```

- **Traffic Bandwidth Trend.** The associated query and analysis statement is:

```
SELECT TIME_FORMAT(MILLIS_TO_TIMESTAMP(TIMESTAMP_TO_MILLIS(_time) -
MOD(TIMESTAMP_TO_MILLIS(_time), 600000)), 'HH:mm') AS dt,
round(sum(request_length) / 1024.0 / 600, 2) AS "Incoming (KB/s)",
round(sum(body_bytes_sent) / 1024.0 / 600, 2) AS "Outgoing (KB/s)" where request_length is
not null GROUP BY TIMESTAMP_TO_MILLIS(_time) - MOD(TIMESTAMP_TO_MILLIS(_time),
600000) ORDER BY dt LIMIT 1000
```

- **PV/UV Trend.** The associated query and analysis statement is:

```
SELECT TIME_FORMAT(MILLIS_TO_TIMESTAMP(TIMESTAMP_TO_MILLIS(_time) -
MOD(TIMESTAMP_TO_MILLIS(_time), 3600000)), 'HH:mm') AS dt, count(1) AS PV,
APPROX_COUNT_DISTINCT (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS UV
FROM log GROUP BY TIMESTAMP_TO_MILLIS(_time) -
MOD(TIMESTAMP_TO_MILLIS(_time), 3600000) ORDER BY dt LIMIT 1000
```

- **Visit Statuses.** The associated query and analysis statement is:

```
SELECT TIME_FORMAT(MILLIS_TO_TIMESTAMP(TIMESTAMP_TO_MILLIS(_time) -
MOD(TIMESTAMP_TO_MILLIS(_time), 3600000)), 'HH:mm') AS dt, count(1) AS cnt,
concat(cast("response_code" / 100 AS VARCHAR), 'XX') AS "status" GROUP BY
TIMESTAMP_TO_MILLIS(_time) - MOD(TIMESTAMP_TO_MILLIS(_time), 3600000) ,
"response_code" / 100 ORDER BY dt DESC LIMIT 10000
```

- **Source.** The associated query and analysis statement is:

```
SELECT ip_to_province (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS country,
count(1) AS "Visits" where ip_to_country(CASE WHEN sip = '-' THEN remote_ip ELSE sip END) =
'China' GROUP BY country
```

- **Incoming Traffic Source (China).** The associated query and analysis statement is:

```
SELECT ip_to_province (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS region,
round(sum(request_length)/ 1024.0 / 1024, 4) AS "Incoming (MB)" where ip_to_country(CASE
WHEN sip = '-' THEN remote_ip ELSE sip END) = 'China' GROUP BY region
```

- **Incoming Traffic Source (World).** The associated query and analysis statement is:

```
SELECT ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS region,
round(sum(request_length)/ 1024.0 / 1024, 4) AS "Incoming (MB)" where request_length is not
null GROUP BY region
```

- **Source Network Providers.** The associated query and analysis statement is:

```
SELECT ip_to_provider (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) AS provider,
round(sum(request_length)/ 1024.0 / 1024.0, 3) AS mb_in GROUP BY provider
HAVING ip_to_provider (CASE WHEN sip = '-' THEN remote_ip ELSE sip END) != '*' ORDER
BY mb_in DESC LIMIT 10
```

- **Domain Names.** The associated query and analysis statement is:

```
SELECT http_host, count(1) AS "Visits" GROUP BY http_host ORDER BY
"Visits" DESC LIMIT 30
```

- **URLs with the Slowest Response.** The associated query and analysis statement is:

```
SELECT http_host AS "Website",url_extract_path (COALESCE (url, '/')) AS URL,sum(request_time)/
count(1) AS "Response Duration (ms)",count(1) AS "Visits" GROUP BY http_host, url ORDER BY
"Response Duration (ms)" DESC LIMIT 100
```

- **Clients with the Most Visits.** The associated query and analysis statement is:

```
SELECT ip AS "Client", client AS "Network", concat(cast((CASE WHEN pv IS NULL THEN 0 ELSE pv
END) AS VARCHAR), '(', cast(case when head_pv = 'null' then 0 else (case when head_pv > 0
then head_pv else 0 end) end AS VARCHAR), '/', cast(case when get_pv = 'null' then 0 else (case
when get_pv > 0 then get_pv else 0 end) end AS VARCHAR), '/', cast(case when put_pv = 'null'
then 0 else (case when put_pv > 0 then put_pv else 0 end) end AS VARCHAR), '/', cast(case when
post_pv = 'null' then 0 else (case when post_pv > 0 then post_pv else 0 end) end AS VARCHAR), '/',
cast(case when delete_pv = 'null' then 0 else (case when delete_pv > 0 then delete_pv else 0 end)
end AS VARCHAR), '/', ')') AS "PV(Head, Get, Put, Post, Delete)", error_count AS "Wrong Visits"
FROM (SELECT ip, client, sum(CASE WHEN "method" = 'PUT' AND "status" < 400 THEN pv ELSE
0 END) AS put_pv, sum(CASE WHEN "method" = 'GET' AND "status" < 400 THEN pv ELSE 0 END)
AS get_pv, sum(CASE WHEN "method" = 'POST' AND "status" < 400 THEN pv ELSE 0 END) AS
post_pv, sum(CASE WHEN "method" = 'DELETE' AND "status" < 400 THEN pv ELSE 0 END) AS
delete_pv, sum(CASE WHEN "method" = 'HEAD' AND "status" < 400 THEN pv ELSE 0 END) AS
head_pv, sum(throughput) AS throughput, sum(pv) AS pv, sum(CASE WHEN "status" < 400
THEN 1 ELSE 0 END) AS error_count FROM (SELECT CASE WHEN sip = '-' THEN remote_ip
ELSE sip END AS ip, "method", CASE WHEN ip_to_country (CASE WHEN sip = '-' THEN
remote_ip ELSE sip END)= 'Shanghai' THEN 'Shanghai, China' WHEN ip_to_province (CASE WHEN
sip = '-' THEN remote_ip ELSE sip END)= '*' THEN 'Unknown IP' WHEN ip_to_provider (CASE
WHEN sip = '-' THEN remote_ip ELSE sip END)= 'Private IP' THEN 'Private IP' ELSE
concat(ip_to_country (CASE WHEN sip = '-' THEN remote_ip ELSE sip END), '/', ip_to_province
(CASE WHEN sip = '-' THEN remote_ip ELSE sip END), '/', CASE WHEN ip_to_city (CASE WHEN
sip = '-' THEN remote_ip ELSE sip END)= '*' THEN '' ELSE ip_to_city (CASE WHEN sip = '-' THEN
remote_ip ELSE sip END) END, '', ip_to_provider (CASE WHEN sip = '-' THEN remote_ip ELSE sip
END)) END AS client, sum(CASE WHEN "response_code" < 400 THEN 1 ELSE 0 END) AS pv,
round(sum(request_length)/ 1024.0 / 1024, 1) AS throughput, "response_code" AS "status"
FROM log GROUP BY ip, client, "method", "response_code" ORDER BY pv DESC, client,
"method" LIMIT 1000) GROUP BY ip, client ORDER BY pv DESC) LIMIT 100
```

----End

# 7 Log Alarms

---

## 7.1 Overview

LTS allows you to create log alarm rules of the keyword statistics, and SQL statistics types to trigger alarms. You can view alarm details in the alarm list to monitor the service running status. You can also configure alarm action rules to send alarm notifications by SMS message, mobile phone, or email. This helps you handle alarms in real time.

### Advantages

- Easy to use and copy  
Simply ingest logs to LTS, then you can create alarm rules and notification policies to receive and respond to potential alarm events in real time.
- High availability and reliability  
The alarm availability reaches 99.9%, and the alarm data reliability exceeds 99.99999999%.
- Cost-effective and O&M-free  
Currently, LTS does not charge for alarm rules and alarm management, reducing the O&M costs of the alarm system and the time costs of O&M personnel. You will be notified at least one month in advance if there is any charging plan.  
SMS notifications are billed on a pay-per-use basis. For details, see [Billing](#). The voice function is available only to whitelisted users. For details about its pricing, see [Pricing](#).
- Quickly respond to exceptions  
Comprehensive and intelligent alarm monitoring and alarm action rule capabilities enable fast responses to alarms and efficient problem resolution, reducing potential losses caused by service exceptions.

### Constraints

For details, see [Log Alarm Constraints](#).

## 7.2 Configuring Log Alarm Rules

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

You can create multiple alarm rules in a batch. For details, see [Creating Multiple Alarm Rules](#).

### Prerequisites

A log group and stream have been created. For details, see [Managing Log Groups](#) and [Managing Log Streams](#).


### Creating a Keyword Alarm Rule

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

- Step 1** Log in to the [LTS console](#).
- Step 2** Choose **Log Alarms** in the navigation pane.
- Step 3** Click the **Alarm Rules** tab.
- Step 4** Click **Create**. The **Create Alarm Rule** right panel is displayed.
- Step 5** Configure alarm rule parameters.

**Table 7-1** Keyword alarm rule parameters

Category	Parameter	Description
Basic Info	Rule Name	Name of the alarm rule. Enter 1 to 64 characters and do not start or end with a hyphen (-) or underscore (_). Only letters, digits, hyphens, and underscores are allowed. <b>NOTE</b> After an alarm rule is created, the rule name can be modified. After the modification, move the cursor over the rule name to view the new and original rule names. The original rule name cannot be changed.
	Description	Brief description of the rule. Enter up to 64 characters.
Statistical Analysis	Statistics	<b>By keyword:</b> applicable when keywords are used to search for and configure log alarms.
	Query Condition	<b>Log Group Name:</b> Select a log group.

Category	Parameter	Description
		<p><b>Log Stream Name:</b> Select a log stream.</p> <p><b>NOTE</b> If a log group contains more than one log stream, you can select multiple log streams when creating a keyword alarm rule.</p> <p><b>Query Time Range:</b> Specify the query period of the statement. It is one period earlier than the current time. For example, if <b>Query Time Range</b> is set to one hour and the current time is 9:00, the period of the query statement is 8:00–9:00.</p> <ul style="list-style-type: none"> <li>• The value ranges from 1 to 60 in the unit of minutes.</li> <li>• The value ranges from 1 to 24 in the unit of hours.</li> </ul> <p><b>Keywords:</b> Enter keywords that you want LTS to monitor in logs. Exact and fuzzy matches are supported. A keyword is case-sensitive and contains up to 1,024 characters. For details about how to set keyword search, see <a href="#">Using LTS Search Syntax</a>.</p>
	Check Rule	<p>Configure a condition that will trigger the alarm.</p> <p><b>Matching Log Events:</b> When the number of log events that contain the configured keywords reaches the specified value, an alarm is triggered. Four comparison operators are supported: greater than (&gt;), greater than or equal to (&gt;=), less than (&lt;), and less than or equal to (&lt;=).</p> <ul style="list-style-type: none"> <li>• Click + to add a conditional expression with an OR relationship. A maximum of 20 conditional expressions can be added.</li> <li>• Click  to delete a conditional expression.</li> </ul> <p>The number of queries refers to the <b>Query Frequency</b> set in <b>Advanced Settings</b> and the number of times the condition must be met to trigger the alarm. The number of queries must be greater than or equal to the number of times the condition must be met.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• The alarm severity can be <b>critical</b> (default), <b>major</b>, <b>minor</b>, or <b>info</b>.</li> <li>• Number of queries: 1–10</li> </ul>

Category	Parameter	Description
Advanced Settings	Query Frequency	<p>The options for this parameter are:</p> <ul style="list-style-type: none"> <li>• <b>Hourly:</b> The query is performed at the top of each hour.</li> <li>• <b>Daily:</b> The query is run at a specific time every day.</li> <li>• <b>Weekly:</b> The query is run at a specific time on a specific day every week.</li> <li>• <b>Custom interval:</b> You can specify the interval from 1 minute to 60 minutes or from 1 hour to 24 hours. For example, if the current time is 9:00 and the <b>Custom interval</b> is set to 5 minutes, the first query is at 9:00, the second query is at 9:05, the third query is at 9:10, and so on.</li> </ul> <p><b>NOTE</b> When the query time range is set to a value larger than 1 hour, the query frequency must be set to every 5 minutes or a lower frequency.</p> <ul style="list-style-type: none"> <li>• <b>CRON:</b> CRON expressions support schedules down to the minute and use 24-hour format. Examples: <ul style="list-style-type: none"> <li>- <b>0/10 * * * *:</b> The query starts from 00:00 and is performed every 10 minutes. That is, queries start at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50.</li> <li>- <b>0 0/5 * * * *:</b> The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00.</li> <li>- <b>0 14 * * * *:</b> The query is performed at 14:00 every day.</li> <li>- <b>0 0 10 * * * *:</b> The query is performed at 00:00 on the 10th day of every month.</li> </ul> </li> </ul>
Advanced Settings	Restores	<p>Configure a policy for sending an alarm clearance notification.</p> <p>If alarm clearance notification is enabled and the trigger condition has not been met for the specified number of statistical periods, an alarm clearance notification is sent.</p> <p>Number of last queries: 1–10</p>

Category	Parameter	Description
Advanced Settings	Notify When	<ul style="list-style-type: none"><li>● <b>Alarm triggered:</b> Specify whether to send a notification when an alarm is triggered. If this option is enabled, a notification will be sent when the trigger condition is met.</li><li>● <b>Alarm cleared:</b> Specify whether to send a notification when an alarm is cleared. If this option is enabled, a notification will be sent when the recovery policy is met.</li></ul>
Advanced Settings	Frequency	You can select <b>Once</b> , <b>Every 5 minutes</b> , <b>Every 10 minutes</b> , <b>Every 15 minutes</b> , <b>Every 30 minutes</b> , <b>Every hour</b> , <b>Every 3 hours</b> , or <b>Every 6 hours</b> to send alarms. <b>Once</b> indicates that a notification is sent once an alarm is generated. <b>Every 10 minutes</b> indicates that the minimum interval between two notifications is 10 minutes, preventing alarm storms.
Advanced Settings	Alarm Action Rules	Select a desired rule from the drop-down list. If no rule is available, click <b>Create Alarm Action Rule</b> on the right.
Advanced Settings	Language	Specify the language ( <b>Chinese (simplified)</b> or <b>English</b> ) in which alarms are sent.

**Step 6** Click **OK**. For examples, see [Example 1: Alarms Triggered by a Keyword](#).

 **NOTE**

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

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

----End

## Creating a SQL Alarm Rule

LTS can regularly run the SQL queries that you specify on structured logs and trigger an alarm when the alarm rule is met. You can view SQL alarms on the LTS console. Each SQL alarm rule can be associated with one to three charts. Each chart contains a SQL statement for querying a log stream.

 **NOTE**



Currently, this function is available to all users in regions CN South-Guangzhou, CN North-Beijing4, CN East-Shanghai1, CN East-Shanghai2, CN-Hong Kong, CN Southwest-Guiyang1, AP-Singapore, and CN North-Beijing1. It is also available to whitelisted users in regions CN South-Shenzhen, AP-Bangkok, ME-Riyadh, and AP-Jakarta.


- Step 1** Log in to the LTS console and choose **Log Alarms** in the navigation pane.
- Step 2** Click the **Alarm Rules** tab.
- Step 3** Click **Create**. The **Create Alarm Rule** right panel is displayed.
- Step 4** Configure alarm rule parameters by referring to [Table 7-2](#).

**Table 7-2** SQL alarm rule parameters

Category	Parameter	Description
Basic Info	Rule Name	Name of the alarm rule. Enter 1 to 64 characters and do not start or end with a hyphen (-) or underscore (_). Only letters, digits, hyphens, and underscores are allowed.  <b>NOTE</b> After an alarm rule is created, the rule name can be modified. After the modification, move the cursor over the rule name to view the new and original rule names. The original rule name cannot be changed.
	Description	Rule description. Enter up to 64 characters.
Statistical Analysis	Statistics	<b>By SQL:</b> Use SQL analysis to configure an alarm rule.



Category	Parameter	Description
	Charts	<p>You can add a chart in two ways.</p> <ul style="list-style-type: none"> <li> <b>Configure from Scratch:</b> Click <b>Configure from Scratch</b> and then select a log group and stream. Set parameters as follows: <ul style="list-style-type: none"> <li><b>Log Group Name:</b> (Required) Select a log group.</li> <li><b>Log Stream Name:</b> (Required) Select a log stream.</li> </ul> <p><b>NOTE</b> If the logs in the log stream have not been structured, <a href="#">configure log structuring</a> first.</p> <p><b>Query Time Range:</b> (Optional) the period specified for querying logs. It can be 1 to 60 minutes or 1 to 24 hours.</p> <p><b>Query Statement:</b> required.</p></li> </ul> <ul style="list-style-type: none"> <li> <b>Import Configuration:</b> Click <a href="#">+ Import Configuration</a> . On the displayed <b>Custom</b> page, select a log group and stream, select a chart, and click <b>OK</b>. If there are no charts available or the charts do not fit your needs, click <b>Create Chart</b>. Configure the chart parameters, click <b>OK</b>, and click <b>Save and Back</b> in the upper right corner to return to the <b>Create Alarm Rule</b> right panel. You can see that the chart you just created has been selected, and the query statement has been filled in. Specify the query time range (1 to 60 minutes or 1 to 24 hours). When the query frequency is set to every 1 to 4 minutes, the query time range can only be set to a value no larger than 1 hour. You can continue to add more charts by clicking <a href="#">+ Import Configuration</a> .</li> </ul> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>Click  to go to the visualization page of the log stream.</li> <li>Click  to delete an added chart.</li> <li>Click <b>Preview</b> to view the data after visualized analysis. You must click <b>Preview</b>; otherwise, the alarm rule cannot be saved.</li> <li>Up to three charts can be added.</li> <li>The chart and the query statement are required.</li> </ul>

Category	Parameter	Description
	Check Rule	<p>Enter a specific conditional expression. When the expression execution result is <b>true</b>, an alarm is generated.</p> <p><b>NOTE</b></p> <ul style="list-style-type: none"> <li>• Conditional expressions support Chinese characters.</li> <li>• Conditional expressions cannot contain only digits or start with a digit.</li> <li>• Specify the number of queries and the number of times the condition must be met to trigger the alarm. The number of queries must be greater than or equal to the number of times the condition must be met.</li> <li>• The alarm severity can be <b>critical</b> (default), <b>major</b>, <b>minor</b>, or <b>info</b>.</li> <li>• Number of queries: 1–10</li> <li>• Click + to add a conditional expression with an OR relationship. A maximum of 20 conditional expressions can be added.</li> <li>• Click  to delete a conditional expression.</li> </ul> <p>Basic syntax and syntax across multiple charts are supported.</p> <ul style="list-style-type: none"> <li>• Basic syntax <ul style="list-style-type: none"> <li>– Basic arithmetic operators: addition (+), subtraction (-), multiplication (*), division (/), and modulo (%). Example: <b>x * 10 + y &gt; 100</b></li> <li>– Comparison operators: greater than (&gt;), greater than or equal to (&gt;=), less than (&lt;), less than or equal to (&lt;=), equal to (==), and not equal to (!=). Example: <b>x &gt;= 100</b>.</li> <li>– Logical operators: &amp;&amp; (and) and    (or). Example: <b>x &gt; 0 &amp;&amp; y &lt; 200</b></li> <li>– Logical negation (!). Example: <b>!(x &lt; 1 &amp;&amp; x &gt; 100)</b></li> <li>– Numeric constants: They are processed as 64-bit floating point numbers. Example: <b>x &gt; 10</b></li> <li>– String constants. Example: <b>str == "string"</b></li> <li>– Boolean constants: true and false. Example: <b>(x &lt; 100)!=true</b></li> <li>– Parentheses: used to change the order of operations. Example: <b>x *(y + 10) &lt; 200</b></li> <li>– contains function: used to check whether a string contains a substring. For example, if you run <b>contains(str, "hello")</b> and <b>true</b> is returned, the string contains the <b>hello</b> substring.</li> </ul> </li> <li>• Syntax across multiple charts</li> </ul>

Category	Parameter	Description
		<ul style="list-style-type: none"> <li>- Basic arithmetic operators: addition (+), subtraction (-), multiplication (*), division (/), and modulo (%).</li> <li>- Comparison operators: greater than (&gt;), greater than or equal to (&gt;=), less than (&lt;), less than or equal to (&lt;=), equal to (==), and not equal to (!=).</li> <li>- Logical operators: &amp;&amp; (and) and    (or).</li> <li>- Logical negation (!)</li> <li>- contains function</li> <li>- Parentheses</li> </ul>
Advanced Settings	Query Frequency	<p>The options for this parameter are:</p> <ul style="list-style-type: none"> <li>● <b>Hourly:</b> The query is performed at the top of each hour.</li> <li>● <b>Daily:</b> The query is run at a specific time every day.</li> <li>● <b>Weekly:</b> The query is run at a specific time on a specific day every week.</li> <li>● <b>Custom interval:</b> You can specify the interval from 1 minute to 60 minutes or from 1 hour to 24 hours. For example, if the current time is 9:00 and the <b>Custom interval</b> is set to 5 minutes, the first query is at 9:00, the second query is at 9:05, the third query is at 9:10, and so on.</li> </ul> <p><b>NOTE</b></p> <p>When the query time range is set to a value larger than 1 hour, the query frequency must be set to every 5 minutes or a lower frequency.</p> <ul style="list-style-type: none"> <li>● <b>CRON:</b> CRON expressions support schedules down to the minute and use 24-hour format. Examples: <ul style="list-style-type: none"> <li>- <b>0/10 * * * *:</b> The query starts from 00:00 and is performed every 10 minutes. That is, queries start at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50.</li> <li>- <b>0 0/5 * * *:</b> The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00.</li> <li>- <b>0 14 * * *:</b> The query is performed at 14:00 every day.</li> <li>- <b>0 0 10 * *:</b> The query is performed at 00:00 on the 10th day of every month.</li> </ul> </li> </ul>

Category	Parameter	Description
Advanced Settings	Restores	Configure a policy for sending an alarm clearance notification.  If alarm clearance notification is enabled and the trigger condition has not been met for the specified number of statistical periods, an alarm clearance notification is sent.  Number of last queries: 1–10
Advanced Settings	Notify When	<ul style="list-style-type: none"> <li>• <b>Alarm triggered:</b> Specify whether to send a notification when an alarm is triggered. If this option is enabled, a notification will be sent when the trigger condition is met.</li> <li>• <b>Alarm cleared:</b> Specify whether to send a notification when an alarm is cleared. If this option is enabled, a notification will be sent when the recovery policy is met.</li> </ul>
Advanced Settings	Frequency	You can select <b>Once</b> , <b>Every 5 minutes</b> , <b>Every 10 minutes</b> , <b>Every 15 minutes</b> , <b>Every 30 minutes</b> , <b>Every hour</b> , <b>Every 3 hours</b> , or <b>Every 6 hours</b> to send alarms.  <b>Once</b> indicates that a notification is sent once an alarm is generated. <b>Every 10 minutes</b> indicates that the minimum interval between two notifications is 10 minutes, preventing alarm storms.
Advanced Settings	Alarm Action Rules	Select a desired rule from the drop-down list.  If no rule is available, click <b>Create Alarm Action Rule</b> on the right. For details, see <a href="#">Creating an Alarm Action Rule</a> .
Advanced Settings	Language	Specify the language ( <b>Chinese (simplified)</b> or <b>English</b> ) in which alarms are sent.

**Step 5** Click **OK**. For examples, see [Example 2: Alarms Triggered by the Keyword Frequency](#).

----End

## Creating Multiple Alarm Rules

You can create multiple alarm rules in a batch.

**Step 1** On the **Alarm Rules** tab page, import alarm rules in a batch.

1. Click **Import**. The **Import Alarm Rule** dialog box is displayed.
2. Click **Download Alarm Template.xlsx** to download the template to the local PC and fill in the template.

3. Click **Select File** and select the file that has been filled in.
4. Check the imported rule information and click **Import**.
5. After the import is successful, view the alarm rule details in the rule list.

**Step 2** Click **Modify**. The **Edit Alarm Rules** page is displayed.

**Step 3** Under **Basic Settings**, enter the number of alarm rules and click **Add**.

Alternatively, click **Import** to import alarm rules in a batch.

 **NOTE**

A maximum of 200 rules can be created. By default, there is one alarm rule in the rule list. Therefore, you can add up to 199 more rules.

**Step 4** In the **Rule List** area, set alarm rules by referring to [Creating a Keyword Alarm Rule](#) and [Creating a SQL Alarm Rule](#), and click **Submit**.

- After setting an alarm rule, you can click **Apply to Other Rules** to copy its settings to other alarm rules.
- The created alarm rules will be displayed on the **Alarm Rules** tab page after the batch creation is successful.

----End

## Follow-up Operations on Alarm Rules

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

- You can perform the following operations on a single alarm rule.
  - Modifying an alarm rule: Click **Modify** in the **Operation** column of the target alarm rule. On the displayed page, modify the rule name, query condition, and check rule, and click **OK**.
  - Enabling an alarm rule: Click **More** > **Enable** in the **Operation** column of the target alarm rule.
  - Disabling an alarm rule: Click **More** > **Disable** in the **Operation** column of the target alarm rule.
  - Temporarily disabling an alarm rule: Click **More** > **Disable Temporarily** in the **Operation** column of the target alarm rule.
  - Copying an alarm rule: Click **More** > **Copy** in the **Operation** column of the target alarm rule.
  - Deleting an alarm rule: Click **Delete** in the **Operation** column of the target alarm rule. In the displayed dialog box, click **OK**.

 **NOTE**

Deleted alarm rules cannot be recovered. Exercise caution when performing this operation.

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

## Example 1: Alarms Triggered by a Keyword

If you want to trigger an alarm upon the detection of a specific keyword in a log, follow this example to set a query statement and a keyword alarm rule. The example is for reference only.

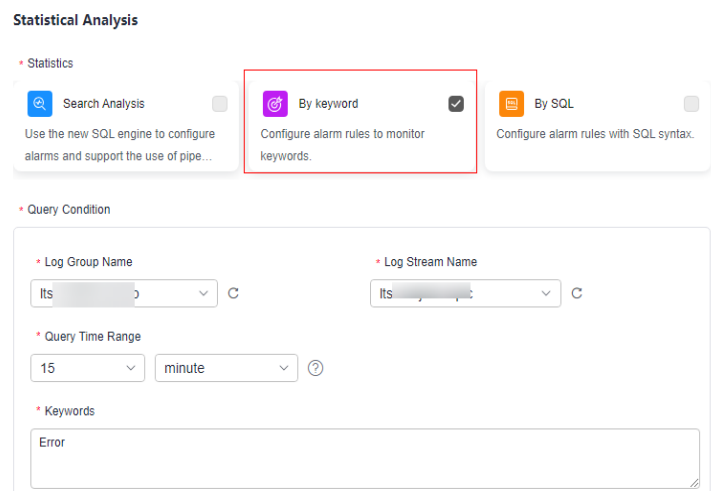
Ensure that the keyword you specify exists in the log stream. In this example, the key word is **Error**.

Figure 7-1 Querying result



- Query statement: Set the query time range to 15 minutes and run the following statement to query logs containing the keyword **Error**. For other search syntaxes, see [Using LTS Search Syntax](#).

Figure 7-2 Query statement



- Alarm notification: After creating the preceding alarm rule, you will receive an alarm in the alarm list as long as the keyword **Error** appears in a log. You can also click an alarm name to view the alarm details and sources.

**Figure 7-3 Alarm**

**Error**

---

Alarm Severity Critical

Generated Sep 4, 2024 17:29:41.709 GMT+08:00

Duration 2minute15second

**Details**

Rule Name	Error
Original Rule Name	[Redacted]
Conditional expression	Matching Log Events > 1
Current Value	{"Error":90}
Query Frequency	Every 5 minutes
Alarm Status	[Redacted]
Log Group Name	[Redacted]
Log Stream Name	[Redacted]
Keywords	Error
Query Time Range	15minute

**Alarm Objects** Handling Suggestions

---

Alarm Name Error

Resource Type Log Group/Stream

Log Group/Stream Its-x-[Redacted]-topic

## Example 2: Alarms Triggered by the Keyword Frequency

If you want to trigger an alarm when the number of occurrences of a specified keyword reaches a specified value in a specified period, follow this example to set a query analysis statement and SQL alarm rule. The example is for reference only.

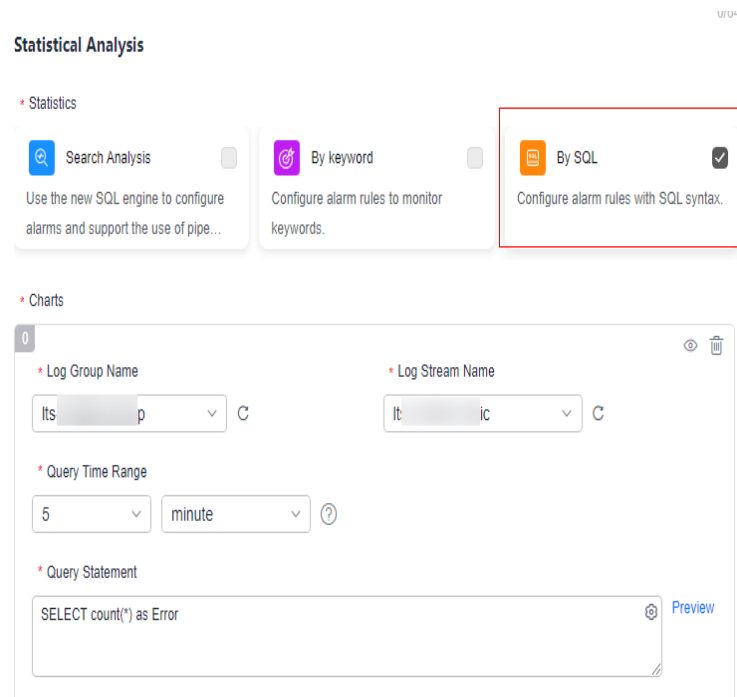
Run **SELECT count(\*) as Error**. The result indicates that **Error** appears 90 times in total in the target log stream.

**Figure 7-4 Querying result**

The screenshot shows the Log Tank Service interface. At the top, there is a search bar with the text 'Its-xunjian-group'. Below the search bar, the query '1 SELECT count(\*) as Error' is entered. The interface is divided into two main sections: 'Log Search' and 'Real-Time Logs'. The 'Log Search' section shows a list of fields: '\_\_time', 'Num', 'field1', and 'field2'. The 'Real-Time Logs' section displays the query result for 'Error' as '90.00', which is highlighted with a red box. The interface also includes a 'Fields' panel on the left and a 'Log Analysis' tab.

- Query statement: Set the query time range to 5 minutes and run the statement **SELECT count(\*) as Error** to collect statistics on the number of times that the keyword **Error** appears within 5 minutes. For other search syntaxes, see [SQL Analysis Syntax](#).

Figure 7-5 Query statement



- Alarm notification: After creating the preceding alarm rule, you will receive an alarm in the alarm list as long as the keyword **Error** appears in logs for two times or more. You can also click an alarm name to view the alarm details and sources.



**Figure 7-6 Alarm**

**Errortest**

---

Alarm Severity Critical

Generated Sep 4, 2024 17:30:38.433 GMT+08:00

Duration 1minute18second

**Details**

Rule Name	Errortest
Original Rule Name	<span style="background-color: #ccc; display: inline-block; width: 100px; height: 1em;"></span>
Conditional expression	Error > 2
Current Value	{"Error":30}
Query Frequency	Every minute
Alarm Status	<span style="background-color: #ccc; display: inline-block; width: 50px; height: 1em;"></span>
Log Group/Stream Name	lts-xu- <span style="background-color: #ccc; display: inline-block; width: 100px; height: 1em;"></span> n-topic
Query Statement	SELECT count(*) as Error
Query Time Range	5minute

**Alarm Objects** Handling Suggestions

---

Alarm Name [Errortest](#)

Resource Type Log Group/Stream

Log Group/Stream lts-xu-topic

## 7.3 Configuring Log Alarm Action Rules

### 7.3.1 Creating a Message Template on the LTS Console

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

#### Creating a Message Template

**Step 1** Log in to the [LTS console](#).

**Step 2** Choose **Log Alarms** in the navigation pane and click the **Alarm Action Rules** tab.

 **NOTE**

By default, LTS provides the following built-in message templates. If no message content is configured in your selected template, LTS uses a built-in template instead.

- **keywords\_template** (Chinese): keyword alarm template
- **keywords\_template** (English): keyword alarm template
- **sql\_template** (Chinese): SQL alarm template
- **sql\_template** (English): SQL alarm template

**Step 3** Click **Create** on the **Message Templates** tab page. On the displayed page, set the required parameters.

 **NOTE**

- The email content supports HTML tags and message preview.
- Templates such as WeCom, Lark, and DingTalk support markdown syntax and message preview.
- You can create up to 100 message templates for AOM and LTS. If there are already 100 templates, delete unnecessary templates before creating a new one.

**Table 7-3** Message template parameters

Parameter	Description	Verification Rule	Example
Template Name	Message template name.	Include digits, letters, underscores (_), and hyphens (-). Do not start or end with an underscore or hyphen. (Max. 100 characters)	LTS-test
Description	Description of the template.	Include digits, letters, and underscores (_). Do not start or end with an underscore. (Max. 1,024 characters)	-
Message Header	Default message header to be added in messages.	<ul style="list-style-type: none"> <li>• Chinese (Simplified)</li> <li>• English</li> </ul>	<ul style="list-style-type: none"> <li>• English: "Dear user,"</li> <li>• "Dear user,"</li> </ul>
Notification method	Notification method.	<ul style="list-style-type: none"> <li>• Email</li> <li>• SMS</li> <li>• HTTP/HTTPS</li> <li>• DingTalk</li> <li>• Lark</li> <li>• WeCom</li> <li>• Voice</li> </ul> <p><b>NOTE</b> The voice function is available only to whitelisted users. To use it, <a href="#">submit a service ticket</a>.</p>	-

Parameter	Description	Verification Rule	Example
Topic	Message topic.	Customize the topic name or use variables. (Max. 512 characters) Only email templates need a topic name.	test

Parameter	Description	Verification Rule	Example
Body	Message content.	<p><b>Add Variable</b></p> <ul style="list-style-type: none"> <li>Original rule name: <i>\${event_name}</i></li> <li>Alarm severity: <i>\${event_severity}</i></li> <li>Occurrence time: <i>\${starts_at}</i></li> <li>Occurrence region: <i>\${region_name}</i></li> <li>Huawei Cloud account: <i>\${domain_name}</i></li> <li>Alarm source: <i>\${event.metadata.resource_provider}</i></li> <li>Resource type: <i>\${event.metadata.resource_type}</i></li> <li>Resource ID: <i>\${resources}</i></li> <li>Alarm status: <i>\${event.annotations.alarm_status}</i></li> <li>Expression: <i>\${event.annotations.condition_expression}</i></li> <li>Current value: <i>\${event.annotations.current_value}</i></li> <li>Expression with a value: <i>\${event.annotations.condition_expression_with_value}</i></li> <li>Statistical period: <i>\${event.annotations.frequency}</i></li> <li>Rule name: <i>\${event.annotations.alarm_rule_alias}</i></li> <li>Frequency: <i>\${event.annotations.notification_frequency}</i></li> <li>Original log group name: <i>\${event.annotations.results[0].log_group_name}</i></li> <li>Original log stream name: <i>\${event.annotations.results[0].log_stream_name}</i></li> </ul>	<p><i>\${event_name}</i> <i>\${event_severity}</i> <i>\${starts_at}</i> <i>\${region_name}</i></p>

Parameter	Description	Verification Rule	Example
		<ul style="list-style-type: none"> <li>• Variables supported by keyword alarms:               <ol style="list-style-type: none"> <li>1. Query time: <i>\$event.annotations.results[0].time</i></li> <li>2. Query logs: (The maximum log size is 2 KB. If a log exceeds 2 KB, the extra part will be truncated and discarded.) <i>\$event.annotations.results[0].raw_results</i></li> <li>3. Query URL: <i>\$event.annotations.results[0].url</i></li> <li>4. Log group/stream name: <i>\$event.annotations.results[0].resource_id</i></li> </ol> <p><b>NOTE</b> Only the original name of the log group or log stream created for the first time can be added. The modified log group or log stream name cannot be added.</p> <ol style="list-style-type: none"> <li>5. Enterprise project ID of the log stream: <i>\$event.annotations.results[0].eps_id</i></li> <li>6. Query custom field: <i>\$event.annotations.results[0].fields.xxx</i></li> </ol> <p><b>NOTE</b> <i>xxx</i> indicates the structured fields and system fields (such as <b>hostIP</b> and <b>hostName</b>) of the raw logs. The maximum size of a log field is 1 KB. If a field exceeds 1 KB, the extra part will be truncated and discarded.</p> </li> <li>• Variables supported by SQL alarms:               <ol style="list-style-type: none"> <li>1. Log group/stream names of chart 0:</li> </ol> </li> </ul>	

Parameter	Description	Verification Rule	Example
		<p><i>\$event.annotations.results[0].resource_id</i></p> <p><b>NOTE</b> Only the original name of the log group or log stream created for the first time can be added. The modified log group or log stream name cannot be added.</p> <p><b>0</b> indicates the first chart, <b>1</b> indicates the second chart, and so on.</p> <p>2. Query statement of chart 0: <i>\$event.annotations.results[0].sql</i></p> <p>3. Query time of chart 0: <i>\$event.annotations.results[0].time</i></p> <p>4. Query URL of chart 0: <i>\$event.annotations.results[0].url</i></p> <p>5. Query log of chart 0: <i>\$event.annotations.results[0].raw_results</i></p> <p>6. Chart 0 Log Stream Enterprise Project ID: <i>\$event.annotations.results[0].eps_id</i></p> <p><b>Copy from Existing</b></p> <ul style="list-style-type: none"> <li>• keywords_template</li> <li>• sql_template</li> <li>• sql_template</li> <li>• keywords_template</li> <li>• Custom templates (created with variables)</li> </ul>	

**Step 4** When the configuration is complete, click **OK**.

 **NOTE**

When creating a message template on the LTS console, if you are prompted that the creation fails because the template name is not unique, perform the following steps to rectify the fault:

1. Check whether the message template name already exists.  
If yes, change the name. Message template names must be unique in both LTS and AOM because the two services share the same data source. If you have created a message template named **test** in AOM, you cannot create a message template with the same name in LTS.
2. Check whether the number of message templates exceeds the quota.  
You can create up to 100 message templates for AOM and LTS. If there are already 100 templates, delete unnecessary templates before creating a new one.

----End

## Modifying a Message Template

- Step 1** In the message template list, click **Modify** in the row that contains the target template, and modify the template according to [Table 7-3](#). The template name cannot be modified.

 **NOTE**

Built-in message templates cannot be modified.

- Step 2** Click **OK**.

----End

## Copying a Message Template

- Step 1** In the message template list, click **Copy** in the row that contains the target template. Set a new template name.
- Step 2** Click **OK**.

----End

## Deleting a Message Template

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

 **NOTE**

Built-in message templates cannot be deleted.

- Step 2** Click **OK**.

----End

## Deleting Message Templates in a Batch

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

**Step 2** Click **OK**.

----End

## Exporting Message Templates

**Step 1** In the message template list, select the templates to be exported and click **Export**.

**Step 2** Click **Export all data to an XLSX file** or **Export selected data to an XLSX file**.  
After the data is exported, you can view it on the local PC.

----End

## 7.3.2 Creating an Alarm Action Rule

LTS allows you to customize alarm action rules. You can create an alarm action rule to associate an SMN topic with a message template. You can also customize notification content when creating a message template.

### Prerequisites

- A topic has been created. For details, see [Creating a Topic](#).
- A topic policy has been configured. For details, see [Configuring Topic Policies](#).
- A subscriber has been added to the topic. A subscriber is the recipient of the notification, for example, an email or SMS message receiver. For details, see [Adding a Subscription to a Topic](#).

### Precaution

You can create a maximum of 1,000 alarm action rules. If this number has been reached, delete unnecessary rules.

## Creating an Alarm Action Rule

**Step 1** Log in to the [LTS console](#).

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

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

**Step 4** Click **Create**. Set parameters such as the action rule name and action rule configuration.



**Figure 7-7** Creating an alarm action rule

Create Alarm Action Rule

---

**Basic Information**

\* Action Rule


\* Enterprise Project

Description  
  
0/1024

---

**Alarm action rule config**

\* Topic  
 [create a new topic](#)

\* Message Templates   
 [Create Message Template](#)

**Table 7-4** Parameters for configuring an alarm action rule

Parameter	Description
Action Rule	Enter 1 to 64 characters. Only digits, letters, underscores (_), and hyphens (-) are allowed. Do not start or end with an underscore or hyphen.
Enterprise Project	Select an enterprise project. This parameter is displayed only when the enterprise project function is enabled for the current account.
Description	Enter a description for the rule. Up to 1,024 characters are allowed.
Topic	SMN topic. Select your desired topic from the drop-down list. If there is no topic you want to select, create one on the SMN console.
Message Template	Notification message template. Select your desired template from the drop-down list. If no proper message template is available, click <b>Create Template</b> to create one. For details, see <a href="#">Creating a Message Template on the LTS Console</a> .


**Step 5** Click **OK**.

----End

## More Operations

After an alarm action rule is created, you can perform operations described in [Table 7-5](#).

**Table 7-5** Related operations

Operation	Description
Modifying an alarm action rule	Click <b>Modify</b> in the <b>Operation</b> column.
Exporting an alarm action rule	Select one or more alarm action rules and click <b>Export</b> . If no alarm action rule is selected, clicking <b>Export</b> will export all alarm action rules.
Deleting an alarm action rule	<ul style="list-style-type: none"> <li>To delete a single rule, click <b>Delete</b> in the <b>Operation</b> column in the row that contains the rule, and then click <b>Yes</b> on the displayed page.</li> <li>To delete one or more rules, select them, click <b>Delete</b> above the rule list, and then click <b>Yes</b> on the displayed page.</li> </ul> <p><b>NOTE</b> Before deleting an alarm action rule, you need to delete the alarm rule bound to the action rule.</p>
Searching for an alarm action rule	Enter a rule name in the search box in the upper right corner and click  .

## 7.4 Viewing Alarms in LTS

LTS allows you to configure keyword or SQL alarm rules to periodically query log data. When an alarm rule is met, an alarm will be reported. You can view the alarms on the LTS console.

### Prerequisites

You have created an alarm rule.

### Procedure

**Step 1** Log in to the [LTS console](#).

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


**Step 3** Click the **Alarms** tab. The alarms generated in 30 minutes from now and their trend charts are displayed by default.

**Step 4** Set criteria to search for your target alarms.

- In the search box above the alarm list, select a log group, log stream, alarm severity, and rule name.
- Set a time range. By default, 30 minutes is specified (relative time from now). There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required.


 **NOTE**

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

**Step 5** Click  after you set the search criteria. The details and trend of the alarms that match the criteria will be displayed.

**Step 6** You can point to the **Details** column of an alarm on the **Active Alarms** tab to view the complete alarm details. Alternatively, click the name in the **Alarm Name** column of an alarm. Details about the alarm are displayed in the right panel that pops up.

After the reported fault is rectified, you can click the deletion button in the row that contains the corresponding alarm on the **Active Alarms** tab to clear the alarm. The cleared alarm will then be displayed on the **Historical Alarms** tab.

If you have configured search criteria to filter alarms, you need to manually refresh the alarm list. To enable automatic refresh, click  in the upper right corner and select **Refresh Every 30s**, **Refresh Every 1m**, or **Refresh Every 5m** from the drop-down list box. You can still manually refresh the alarm list when automatic refresh is enabled by selecting **Refresh Now** from the drop-down list box.

----End

# 8 Log Transfer

## 8.1 Overview

After being reported from hosts and cloud services to LTS, logs will be retained in LTS for the retention period you specify. Once this period ends, LTS will delete them. For example, if you set the retention period to 30 days, logs will be kept for 30 days before being deleted. You can specify the retention period when creating a log group or stream. For details, see [Managing Log Groups](#) and [Managing Log Streams](#). Retained logs are deleted once the period is over. For long-term storage or persistent logging, you can transfer logs to other cloud services.

 **NOTE**

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

Currently, LTS allows you to transfer logs to the following services. Select services as required.

**Table 8-1** Transfer destination services

Service	Scenario
OBS	<p>OBS provides mass, secure, and cost-effective data storage for you to store data of any type and size. It is suitable for various scenarios, such as enterprise-level backup/archiving, video on demand (VoD), and video monitoring.</p> <p>OBS offers the following storage classes: Standard, Infrequent Access, Archive, and Deep Archive (under restricted OBT), to meet different requirements for storage performance and cost.</p>

Service	Scenario
DMS for Kafka	<p>DMS for Kafka is a message queuing service using open-source Apache Kafka. It features highly reliable, asynchronous message delivery, and provides Kafka instances with isolated computing, storage, and bandwidth resources.</p> <p>It is widely used for transmitting data between different systems in many industries, including enterprise application, payment, telecommunications, e-commerce, social networking, instant messaging, video, Internet of Things (IoT), and Internet of Vehicle (IoV).</p> <p>Kafka can handle the transmission of massive logs. Applications asynchronously send log messages to message queues. Other components can read the log messages from message queues for further analysis, either in real time or offline. In addition, Kafka can collect key log information to monitor applications.</p>
DIS	<p>Data Ingestion Service (DIS) addresses the challenge of transmitting data from outside the cloud to inside the cloud. It builds data streams for custom applications capable of processing or analyzing streaming data. DIS continuously captures, transmits, and stores terabytes of data from hundreds of thousands of data sources every hour, such as IoT data collection, logs, location-tracking events, website clickstreams, and social media.</p>

## 8.2 Transferring Logs to OBS

You can transfer logs to OBS and download log files from the OBS console. You can choose scheduled or one-time transfers.

- [Creating a Scheduled Log Transfer Task](#)
- [Creating a One-off Log Transfer Task](#)

### NOTE

- When creating a log transfer task, you must have the following permissions in addition to the LTS permissions: bucket ACL (**obs:bucket:PutBucketAcl**), bucket list obtaining (**obs:bucket:ListAllMyBuckets**), bucket metadata (**obs:bucket:HeadBucket**), and bucket ACL (**obs:bucket:GetBucketAcl**), and bucket encryption configuration obtaining (**obs:bucket:GetEncryptionConfiguration**). For details, see [Bucket Actions](#).
- LTS transfers only logs generated after the transfer task is configured, not historical logs.

### Prerequisites

- Logs have been ingested to LTS. For details, see [Log Ingestion](#).
- You have created an OBS bucket.

 NOTE

You will be billed for the storage you use in OBS. For details, see [Product Pricing Details](#).

## Creating a Scheduled Log Transfer Task

- Step 1** Log in to the [LTS console](#).
- Step 2** Choose **Log Transfer** in the navigation pane.
- Step 3** Click **Configure Log Transfer** in the upper right corner.
- Step 4** On the displayed page, configure the log transfer parameters.

**Table 8-2** Transfer parameters

Parameter	Description	Example
Log Source Account	<ul style="list-style-type: none"> <li>• <b>Current:</b> Logs of the current account will be transferred.</li> <li>• <b>Other:</b> Logs of the delegator account will be transferred. Ensure that the delegator has created an agency for log transfer delegation in IAM. For details, see <a href="#">Creating an Agency</a>.</li> </ul>	Current
Agency Name	This parameter is required when <b>Log Source Account</b> is set to <b>Other</b> . Enter the name of the agency created by the delegator in IAM.	-
Delegator Account Name	This parameter is required when <b>Log Source Account</b> is set to <b>Other</b> . Enter the account name of the delegator.	-
Enable Transfer	Enabled by default.	Enabled
Transfer Destination	Select a cloud service for log transfer.	OBS
Log Group Name	Select a log group.	N/A

Parameter	Description	Example
Enterprise Project Name	<p>Select an enterprise project.</p> <ul style="list-style-type: none"> <li>This parameter is displayed only when the enterprise project function is enabled for the current account.</li> <li>If the enterprise project function is enabled for the current account: <ul style="list-style-type: none"> <li>All enterprise projects under the current account are displayed in the drop-down list when <b>Log Source Account</b> is set to <b>Current</b>.</li> <li><b>default</b> is displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is not enabled for the delegator account.</li> <li>All enterprise projects under the delegator account are displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is enabled for the delegator account.</li> </ul> </li> </ul>	-
Log Stream Name	<p>Select a log stream.</p> <p><b>NOTE</b> Log streams that have been configured with OBS transfer settings cannot be configured again.</p>	-
OBS Bucket	<ul style="list-style-type: none"> <li>Select an OBS bucket. <ul style="list-style-type: none"> <li>If no OBS buckets are available, click <b>View OBS Bucket</b> to access the OBS console and create an OBS bucket.</li> <li>If encryption has been enabled for the selected OBS bucket, select a key name and select <b>I agree to grant permissions on Key Management Service (KMS) to LTS so LTS can create and use keys to encrypt and decrypt transferred logs</b>.</li> <li>The selected bucket will grant the read and write permissions to LTS. Exercise caution when modifying the bucket policy to prevent log transfer failures.</li> </ul> </li> <li>Currently, LTS supports only standard OBS buckets with the single-AZ storage policy.</li> </ul>	-
Key Name	<p>Select a key name for an OBS bucket for which encryption has been enabled. If no keys are available, click <b>Create Key and Authorize</b> to go to the Data Encryption Workshop (DEW) console and create a key.</p>	-

Parameter	Description	Example
Custom Log Transfer Path	<ul style="list-style-type: none"> <li>Enabled: Logs will be transferred to a custom path to separate transferred log files of different log streams. The format is <b>/LogTanks/Region name/Group name/Stream name/Custom path</b>. The default custom path is <b>lts/%Y/%m/%d</b>, where <b>%Y</b> indicates the year, <b>%m</b> indicates the month, and <b>%d</b> indicates the day. A custom path must meet the following requirements: <ul style="list-style-type: none"> <li>Must start with <b>/LogTanks/Region name</b>.</li> <li><b>%Group name</b> indicates the log group, and <b>%Stream name</b> indicates the log stream.</li> <li>Can contain only letters, digits, and the following special characters: <b>&amp;\$@;,:=+?-._/ %</b>. The character <b>%</b> can only be followed only by <b>Y</b> (year), <b>m</b> (month), <b>d</b> (day), <b>H</b> (hour), and <b>M</b> (minute). Any number of characters can be added before and after <b>%Y</b>, <b>%m</b>, <b>%d</b>, <b>%H</b>, and <b>%M</b>, and the sequence of these variables can be changed.</li> <li>Can contain 1–128 characters.</li> </ul> </li> </ul> <p>Example:</p> <ol style="list-style-type: none"> <li>If you enter <b>LTS-test/%Y/%m/%d/%H/%M</b>, the path is <b>LogTanks/Region name/LTS-test/Y/m/d/H/M/Log file name</b>.</li> <li>If you enter <b>LTS-test/%d/%H/%m/%Y</b>, the path is <b>LogTanks/Region name/LTS-test/d/H/m/Y/Log file name</b>.</li> </ol> <ul style="list-style-type: none"> <li>Disabled: Logs will be transferred to the default path. The default path is <b>LogTanks/Region name/2019/01/01/Log group/Log stream/Log file name</b>.</li> </ul>	LTS-test/ %GroupName/ %StreamName /%Y/%m/%d/ %H/%M
Log Prefix	<p>The file name prefix of the log files transferred to an OBS bucket</p> <p>The prefix must meet the following requirements:</p> <ul style="list-style-type: none"> <li>Can contain 0 to 64 characters.</li> <li>Can contain only letters, digits, hyphens (-), underscores (_), and periods (.</li> </ul> <p>Example: If you enter <b>LTS-log</b>, the log file name will be <b>LTS-log_Log file name</b>.</p>	LTS-log



Parameter	Description	Example
Format	<p>The storage format of logs. The value can be <b>Raw Log Format</b> or <b>JSON</b>.</p> <ul style="list-style-type: none"> <li>Example of the raw log format: (Logs displayed on the LTS console are in the raw format.) Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh &gt; /dev/null 2&gt;&amp;1)</li> <li>The following is an example of the JSON format: <pre>{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh &gt; /dev/null 2&gt;&amp;1)\n","path":"/var/log/syslog","time":1569825602303}</pre></li> </ul>	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	<p>During transfer, logs will be filtered by tag fields collected by ICAgent.</p> <ul style="list-style-type: none"> <li>Disabled: Logs will not be filtered by tag fields.</li> <li>Enabled: Default tag fields include those for hosts (<b>hostIP</b>, <b>hostId</b>, <b>hostName</b>, <b>pathFile</b>, and <b>collectTime</b>) and for Kubernetes (<b>clusterName</b>, <b>clusterId</b>, <b>nameSpace</b>, <b>podName</b>, <b>containerName</b>, and <b>appName</b>). Optional public tag fields are <b>regionName</b>, <b>logStreamName</b>, <b>logGroupName</b>, and <b>projectId</b>.</li> </ul> <p><b>NOTE</b> When <b>Filter by Tag Fields</b> is enabled, <b>Format</b> must be <b>JSON</b>.</p> <ul style="list-style-type: none"> <li><b>Filter by Tag Fields:</b> When this parameter is enabled, logs will be filtered by tags.</li> </ul>	Enabled
Compressed Format	<p>Non-compression and gzip/zip/snappy compression are supported.</p> <p><b>NOTE</b> This function is available only to whitelisted users. To use it, <a href="#">submit a service ticket</a>.</p>	gzip

**Step 5** Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created.

**Step 6** Click the OBS bucket name in the **Transfer Destination** column to switch to the OBS console and view the transferred log files.

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

 **NOTE**

Logs stored in OBS are in raw or JSON format.

----End

## Creating a One-off Log Transfer Task

 **NOTE**

Currently, this function is available only in region AP-Singapore. To use it in other regions, [submit a service ticket](#).

**Step 1** Click **Configure Log Transfer** in the upper right corner.

**Step 2** On the displayed page, configure the log transfer parameters.

**Table 8-3** Transfer parameters

Parameter	Description	Example
Transfer Mode	<b>One-time:</b> Logs are transferred to OBS for long-term storage in a one-time way.	One-time
Transfer Destination	Select a cloud service for log transfer.	OBS
Log Group Name	Select a log group.	N/A
Enterprise Project Name	<p>Select an enterprise project.</p> <ul style="list-style-type: none"> <li>● This parameter is displayed only when the enterprise project function is enabled for the current account.</li> <li>● If the enterprise project function is enabled for the current account:                             <ul style="list-style-type: none"> <li>– All enterprise projects under the current account are displayed in the drop-down list when <b>Log Source Account</b> is set to <b>Current</b>.</li> <li>– <b>default</b> is displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is not enabled for the delegator account.</li> <li>– All enterprise projects under the delegator account are displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is enabled for the delegator account.</li> </ul> </li> </ul>	-

Parameter	Description	Example
Log Stream Name	Select a log stream. <b>NOTE</b> Log streams that have been configured with OBS transfer settings cannot be configured again.	-
Filter By	<b>Keyword</b> is selected by default. Enter the keyword to be filtered in the text box.	-
Log Time Range	There are three types of time range: relative time from now, relative time from last, and specified time. Select a time range as required. <ul style="list-style-type: none"> <li>• <b>From now:</b> 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 <b>1 hour</b> 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.</li> <li>• <b>From last:</b> 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 <b>1 hour</b> 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.</li> <li>• <b>Specified:</b> queries log data that is generated in a specified time range.</li> </ul>	-
Total Log Events	Total number of log events.	-
Log Files	Max log events for each transfer: 20 million. Max transfer files: 200.	-

Parameter	Description	Example
OBS Bucket	<ul style="list-style-type: none"> <li>Select an OBS bucket. If no OBS buckets are available, click <b>View OBS Bucket</b> to access the OBS console and create an OBS bucket.</li> <li>Currently, LTS supports only <b>Standard</b> OBS buckets.</li> <li>Data cannot be transferred to an OBS bucket whose storage class is <b>Archive</b> or for which cross-region replication has been configured.</li> </ul> <p><b>NOTE</b> If you select an unauthorized OBS bucket, LTS will take 15 minutes to authorize the ACL for the bucket. After you configure a one-off transfer task, if the task fails for the first time, it will be automatically retried 15 minutes later. To prevent log transfer failures, exercise caution when modifying the bucket policy.</p>	-
Bucket Directory	OBS bucket directory.	-
Transfer File Name	Custom transfer file name. Only letters, digits, hyphens (-), underscores (_), and periods (.) are allowed.	-
Format	<p>Storage format of logs. The value can be <b>Raw Log Format</b>, <b>JSON</b>, or <b>CSV</b>.</p> <ul style="list-style-type: none"> <li>Example of the raw log format: (Logs displayed on the LTS console are in the raw format.)  <pre>Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh &gt; /dev/null 2&gt;&amp;1)</pre> </li> <li>Example of the JSON format:  <pre>{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh &gt; /dev/null 2&gt;&amp;1)\n","path":"/var/log/syslog","time":1569825602303}</pre> </li> <li><b>CSV</b>: Log content is displayed in a table.</li> </ul>	Json

**Step 3** Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created.

**Step 4** Click the OBS bucket name in the **Transfer Destination** column to switch to the OBS console and view the transferred log files.

**Step 5** Download the transferred logs from OBS for viewing.

----End

## Modifying a Log Transfer Task

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

## Viewing Transfer Details

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

## Deleting a Log Transfer Task

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

### 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:
  - 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.
- **Closed**: The log transfer task is stopped.

## 8.3 Transferring Logs to DIS

DIS provides both log storage and big data analysis. It can perform offline analysis, and transmit a large number of log files to the cloud for backup, query, and machine learning. You can also use it for data recovery and fault analysis on

data losses or exceptions. During transfer, a large number of small text files can be merged into large files to accelerate data processing. Select DIS to transfer logs based on your service scenario.

 **NOTE**

- You are advised to [transfer logs to DMS](#).
- Currently, this function is available only in regions CN North-Beijing4, CN North-Beijing1, CN East-Shanghai2, CN South-Guangzhou, CN-Hong Kong, and AP-Singapore. For other regions, you need to submit a service ticket to DIS. For details, see [Submitting a Service Ticket](#).

## Prerequisites

- Logs have been ingested to LTS. For details, see [Log Ingestion](#).
- DIS has been enabled. For details, see [Creating a DIS Stream](#).

 **NOTE**

You will be billed for the storage you use in DIS. For details, see [Product Pricing Details](#).

## Transferring Logs to DIS

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

**Table 8-4** Transfer parameters

Parameter	Description	Example
Log Source Account	<ul style="list-style-type: none"><li>• <b>Current:</b> Logs of the current account will be transferred.</li><li>• <b>Other:</b> Logs of the delegator account will be transferred. Ensure that the delegator has created an agency for log transfer delegation. For details, see <a href="#">Creating an Agency</a>. Note down the names of the created agency and the delegator account.</li></ul>	Current
Agency Name	This parameter is required when <b>Log Source Account</b> is set to <b>Other</b> . Enter the name of the IAM agency created by the delegator.	N/A
Delegator Account Name	This parameter is required when <b>Log Source Account</b> is set to <b>Other</b> . Enter the account name of the delegator.	N/A
Whether to Enable Transfer	Whether log transfer is enabled.	Enabled

Parameter	Description	Example
Transfer Destination	Select a cloud service for log transfer.	DIS
Log Group Name	Select a log group.	N/A
Enterprise Project Name	<p>Select an enterprise project.</p> <ul style="list-style-type: none"> <li>This parameter is displayed only when the enterprise project function is enabled for the current account.</li> <li>If the enterprise project function is enabled for the current account: <ul style="list-style-type: none"> <li>All enterprise projects under the current account are displayed in the drop-down list when <b>Log Source Account</b> is set to <b>Current</b>.</li> <li><b>default</b> is displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is not enabled for the delegator account.</li> <li>All enterprise projects under the delegator account are displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is enabled for the delegator account.</li> </ul> </li> </ul>	N/A
Log Stream Name	<p>Select a log stream.</p> <p><b>NOTE</b> Log streams that have been configured with DIS transfer settings cannot be configured again.</p>	N/A
DIS Stream Name	Select a DIS stream. If no streams are available, click <b>View DIS Streams</b> to access the DIS console and create a stream.	N/A
Format	<p>The storage format of logs. The value can be <b>Raw Log Format</b> or <b>JSON</b>.</p> <ul style="list-style-type: none"> <li>Examples of the raw log format: (Logs displayed on the LTS console are in the raw format.)  <pre>Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh &gt; /dev/null 2&gt;&amp;1)</pre> </li> <li>The following is an example of the JSON format:  <pre>{"host_name":"ecs-bd70","ip":"192.168.0.54","line_no":249,"message":"Sep 30 14:40:01 ecs-bd70 CRON[4363]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh &gt; /dev/null 2&gt;&amp;1)\n","path":"/var/log/syslog","time":1569825602303}</pre> </li> </ul>	JSON

Parameter	Description	Example
Log Transfer Interval	Logs are transferred to the DIS stream in real time.	Real time
Filter by Tag Fields	<p>During transfer, logs will be filtered by tag fields collected by ICAgent.</p> <ul style="list-style-type: none"> <li>Disabled: Logs will not be filtered by tag fields.</li> <li>Enabled: Default tag fields include those for hosts (<b>hostIP, hostId, hostName, pathFile,</b> and <b>collectTime</b>) and for Kubernetes (<b>clusterName, clusterId, namespace, podName, containerName,</b> and <b>appName</b>). Optional public tag fields are <b>regionName, logStreamName, logGroupName,</b> and <b>projectId</b>.</li> </ul> <p><b>NOTE</b> When <b>Filter by Tag Fields</b> is enabled, <b>Format</b> must be <b>JSON</b>.</p> <ul style="list-style-type: none"> <li><b>Filter by Tag Fields:</b> When this parameter is enabled, logs will be filtered by tags.</li> </ul>	Enabled

**Step 4** Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created. If you transfer logs of another account, the log group and stream belong to the delegator. When you click the name of the delegator's log group or stream on the **Log Transfer** page, you will be directed to the log group or stream through the agency.

**Step 5** Click the DIS stream name in the **Transfer Destination** column to access the DIS console and view transferred log files.

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

 **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 DIS.
- To delete the transfer task, log in to the DIS console, choose **Stream Management**, and select the DIS instance to go to the instance details page. Delete the upload permission under **Permissions**.

----End

## 8.4 Transferring Logs to DMS

You can use DMS APIs to retrieve logs in real time.

 **NOTE**

Currently, this function is available only to whitelisted users. To use it, [submit a service ticket](#).



## Prerequisites

- Logs have been ingested to LTS.
- You have purchased a DMS instance.

### NOTE

- You will be billed for the storage you use in DMS. For details, see [Product Pricing Details](#).
- Before registering a DMS Kafka instance, configure an **inbound rule** to allow access from **198.19.128.0/17** over port **9011**. If DMS's subnet is associated with a network ACL, you need to configure an inbound rule for the network ACL. For this rule, set the protocol to TCP, the source IP address to 198.19.128.0/17, the port number range to 1 to 65535, and the destination port to 9011, and allow the destination IP address.

## Transferring Logs to DMS

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

**Table 8-5** Transfer parameters

Parameter	Description	Example
Log Source Account	<ul style="list-style-type: none"> <li>• <b>Current:</b> Logs of the current account will be transferred.</li> <li>• <b>Other:</b> Logs of the delegator account will be transferred. Ensure that the delegator has created an agency for log transfer delegation. For details, see <a href="#">Creating an Agency</a>.</li> </ul>	Current
Agency Name	This parameter is required when <b>Log Source Account</b> is set to <b>Other</b> . Enter the name of the IAM agency created by the delegator.	-
Delegator Account Name	This parameter is required when <b>Log Source Account</b> is set to <b>Other</b> . Enter the account name of the delegator.	-
Enable Transfer	Enabled by default.	Enabled
Transfer Destination	Select a cloud service for log transfer.	DMS
Log Group Name	Select a log group.	N/A

Parameter	Description	Example
Enterprise Project Name	<p>Select an enterprise project.</p> <ul style="list-style-type: none"> <li>This parameter is displayed only when the enterprise project function is enabled for the current account.</li> <li>If the enterprise project function is enabled for the current account: <ul style="list-style-type: none"> <li>All enterprise projects under the current account are displayed in the drop-down list when <b>Log Source Account</b> is set to <b>Current</b>.</li> <li><b>default</b> is displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is not enabled for the delegator account.</li> <li>All enterprise projects under the delegator account are displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is enabled for the delegator account.</li> </ul> </li> </ul>	-
Log Stream Name	<p>Select a log stream.</p> <p><b>NOTE</b> Log streams that have been configured with DMS transfer settings cannot be configured again.</p>	-
Kafka Instance	<p>Select a Kafka instance. If no instances are available, click <b>View Kafka Instances</b> to access the DMS console and create a Kafka instance.</p> <p>If a Kafka instance has been registered, you can modify it. For details about how to register a Kafka instance, see <a href="#">Registering a Kafka Instance</a>.</p> <p><b>NOTE</b> When creating a Kafka instance, set the instance access mode as follows: Enable ciphertext access for private network access, set the kafka security protocol to SASL_SSL, set the username and password, and enable <b>SASL/PLAIN</b>. For details, see <a href="#">Buying a Kafka Instance</a>.</p>	-
Topic	<p>Select a topic for the Kafka instance. If no topics are available, access the DMS console and create a topic for the Kafka premium instance.</p>	topic-01

Parameter	Description	Example
Format	<p>The storage format of logs. The value can be <b>Raw Log Format</b> or <b>JSON</b>.</p> <ul style="list-style-type: none"> <li>Example of the raw log format: (Logs displayed on the LTS console are in the raw format.) Sep 30 07:30:01 ecs-bd70 CRON[3459]: (root) CMD (/opt/oss/servicemgr/ICAgent/bin/manual/mstart.sh &gt; /dev/null 2&gt;&amp;1)</li> <li>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 &gt; /dev/null 2&gt;&amp;1)\n", "path": "/var/log/syslog", "time": 1569825602303 }</li> </ul>	Raw Log Format
Log Transfer Interval	Logs are transferred to the Kafka instance in real time.	Real time
Log Stream Fields	<p>This parameter is available when <b>Format</b> is set to <b>JSON</b>.</p> <p>It is used to enable the function of transferring log fields.</p> <p><b>All</b>: transfers all fields in a log. <b>Specified</b>: transfers only manually configured ones.</p>	-
Built-in Fields and Custom Tags	<p>This parameter is available when <b>Format</b> is set to <b>JSON</b>.</p> <p>It is used to enable the function of transferring built-in fields and custom tags.</p> <p><b>All</b>: transfers all built-in and specified fields in a log. <b>Specified</b>: transfers only manually configured ones.</p>	-
Stream Tag Fields	<p>This parameter is available when <b>Format</b> is set to <b>JSON</b>.</p> <p>It is used to enable the function of transferring stream tag fields. You can select <b>All</b> or <b>Specified</b> as required.</p> <p><b>All</b>: transfers all stream tag fields in a log. <b>Specified</b>: transfers only manually configured ones. For details about how to set tags, see <a href="#">Managing Log Streams</a>.</p>	-
More Settings	<p>This parameter is available when <b>Format</b> is set to <b>JSON</b>.</p> <p>If no value in the log corresponds to the configured key, an invalid field is used.</p>	-

**Step 4** Click **OK**. When the log transfer status changes to **Normal**, the transfer task has been created. If you transfer logs of another account, the log group and stream

belong to the delegator. When you click the name of the delegator's log group or stream on the **Log Transfer** page, you will be directed to the log group or stream through the agency.

- Step 5** Click the Kafka premium instance in the **Transfer Destination** column to access its basic information page.

 **NOTE**

After a transfer task is created, you can view, modify, and delete it.

- 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 DMS.

----End

## Registering a Kafka Instance

1. If you select a Kafka instance that is not registered, access the page for registering the Kafka instance.
2. Configure the parameters for registering a Kafka instance.

**Table 8-6** Parameters

Parameter	Description	Example
Kafka Instance	DMS instance name.	Kafka-01
Create DMS Network	Connect the Kafka instance to LTS so that LTS can send data through this network.	-
Username	If SASL authentication is enabled for the Kafka instance, enter the username for SASL authentication.	DMS
Password	If SASL authentication is enabled for the Kafka instance, enter the password for SASL authentication.	-

3. Click **OK**.

## 8.5 Transferring Logs to DWS

GaussDB(DWS) is an online data processing database that uses the Huawei Cloud infrastructure to provide scalable, fully-managed, and out-of-the-box analytic database service. Transferring logs to GaussDB(DWS) allows you to transfer structured fields in logs to GaussDB(DWS) database tables. You can determine whether to transfer logs to GaussDB(DWS) as required.

 **NOTE**

Currently, this function is available only in regions CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, and AP-Singapore. To use this function in other regions, [submit a service ticket](#).

## Prerequisites

- Logs have been ingested to LTS.
- Structuring rules have been configured for log streams.
- You have purchased [a dedicated load balancer](#).
- [Create a GaussDB\(DWS\) cluster with coupled storage and compute](#) and bind it to the load balancer.

 **NOTE**

Currently, a GaussDB(DWS) cluster cannot be bound to a load balancer if they are in different VPCs.




## Transferring Logs to DWS

- Step 1** Log in to the LTS console. In the navigation pane on the left, choose **Log Transfer**.
- Step 2** On the **Log Transfer** page, click **Configure Log Transfer** in the upper right corner.
- Step 3** On the **Configure Log Transfer** page, select **DWS Cluster** for **Transfer Destination** and configure parameters.

**Table 8-7** Transfer parameters

Parameter	Description	Example
Enable Transfer	Whether log transfer is enabled.	Enabled
Transfer Destination	Select a cloud service for log transfer.	DWS Cluster
Log Group Name	Select a log group.	-

Parameter	Description	Example
Enterprise Project Name	<p>Select an enterprise project.</p> <ul style="list-style-type: none"> <li>This parameter is displayed only when the enterprise project function is enabled for the current account.</li> <li>If the enterprise project function is enabled for the current account: <ul style="list-style-type: none"> <li>All enterprise projects under the current account are displayed in the drop-down list when <b>Log Source Account</b> is set to <b>Current</b>.</li> <li><b>default</b> is displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is not enabled for the delegator account.</li> <li>All enterprise projects under the delegator account are displayed when <b>Log Source Account</b> is set to <b>Other</b> and the enterprise project function is enabled for the delegator account.</li> </ul> </li> </ul>	default
Log Stream Name	<p>Select a log stream.</p> <p><b>NOTE</b> Log streams that have been configured with DWS cluster transfer settings cannot be configured again.</p>	-
Cluster	Name of the created cluster.	test
Database	Database name of the cluster. There are two database types: gaussdb and postgres. The default cluster database is gaussdb.	gaussdb
Username	Username of the database administrator.	lts-test
Password	Password of the database administrator.	-
Schema	Name of a collection of database objects.	-
Table	Name of a table in the schema.	-

Parameter	Description	Example
Field Mapping	<p>Maps built-in fields and structured fields and types configured in logs to database fields.</p> <p><b>NOTE</b> There are 13 built-in fields: <b>hostIP</b>, <b>hostId</b>, <b>hostName</b>, <b>pathFile</b>, <b>collectTime</b>, <b>clusterName</b>, <b>clusterId</b>, <b>podName</b>, <b>containerName</b>, <b>regionName</b>, <b>projectId</b>, <b>logGroupName</b>, and <b>logStreamName</b>.</p> <p>Structured fields in logs can be transferred to GaussDB(DWS) only when the structured field type and the database table field type are the same.</p> <ul style="list-style-type: none"> <li>• Click  of the structured field and table field drop-down lists to select the fields to transfer.</li> <li>• Click  in the <b>Operation</b> column to delete unnecessary transfer fields.</li> <li>• Click  <b>Add</b> to add fields to be transferred.</li> </ul>	hostIP

**Step 4** Click **OK**.

After a transfer task is created, you can view, modify, and delete it.

 **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 DWS.

----End

# 9 Log Processing

## 9.1 Processing Logs with SQL Scheduled Jobs

LTS supports SQL scheduled jobs, allowing you to periodically analyze log content. SQL scheduled jobs use standard SQL syntax to periodically analyze logs as configured in scheduling rules, and store analysis results to a target log stream.

### NOTE

Currently, this function is available only to whitelisted users in regions CN North-Beijing<sup>4</sup>, CN South-Guangzhou, and CN East-Shanghai<sup>1</sup>. To use it, [submit a service ticket](#).

### Prerequisites

- Logs have been collected.
- Raw logs have been structured. For details, see [Setting Cloud Structuring Parsing](#).


### Constraints

A maximum of 20 SQL scheduled jobs can be created.

### Creating a SQL Scheduled Job

**Step 1** Log in to the LTS console.

**Step 2** Choose **Log Jobs** in the navigation pane and click **SQL Scheduled Jobs > Create SQL Scheduled Job**.

Alternatively, choose **Log Management** in the navigation pane and click the name of a log group or log stream. On the log stream details page, click . On the displayed page, click **SQL Scheduled Jobs > Create SQL Scheduled Job**.



 **NOTE**

- When creating a SQL scheduled job on the log stream details page, the source log group/stream cannot be changed.
- The created job is displayed in the SQL scheduled job list. To [view details](#), click the job name.

**Step 3** On the **Create SQL Scheduled Job** page, configure required parameters.

- In the **Configure Computation** step, complete the following settings and click **Next**.

**Table 9-1** Computation parameters

Parameter	Description
Job Name	SQL scheduled job name. Enter 1 to 64 characters, including letters, digits, hyphens (-), and underscores (_). Do not start or end with a hyphen or underscore.
Description	Description of the SQL scheduled job. Enter up to 1000 characters.
Source Log Group/Stream	Select a log group/stream for which log structuring has been enabled. Log content in the source log group/stream will be stored in the target log group/stream after being processed by the SQL scheduled job.
Statistics	<b>By SQL:</b> uses the old SQL engine.
SQL Code	Enter a query and analysis statement, which will be executed to analyze logs during the SQL scheduled job execution. Specify a time range to query logs from. Click <b>Preview</b> to preview the result.
Target Log Group/Stream	Log group/stream that store the SQL analysis results.

- Configure the following scheduling parameters.

**Table 9-2** Scheduling parameters

Parameter	Description
Interval	<p>Frequency of executing the SQL scheduled job. An execution instance is generated every time the job is executed. The interval determines the time of each execution instance.</p> <ul style="list-style-type: none"> <li>- <b>Hourly:</b> The job is executed every hour.</li> <li>- <b>Daily:</b> The job is executed at a fixed time every day.</li> <li>- <b>Weekly:</b> The job is executed at a fixed time on a fixed day in a week.</li> <li>- <b>Custom interval:</b> The job is executed at a specified interval.</li> <li>- <b>CRON:</b> The job is executed at the interval defined in a cron expression. Cron expressions use the 24-hour format and are precise down to the minute. Examples: <ul style="list-style-type: none"> <li>▪ <b>0/10 * * * *:</b> The query starts from 00:00 and is performed every 10 minutes at 00:00, 00:10, 00:20, 00:30, 00:40, 00:50, 01:00, and so on. For example, if the current time is 16:37, the next query is at 16:50.</li> <li>▪ <b>0 0/5 * * * *:</b> The query starts from 00:00 and is performed every 5 hours at 00:00, 05:00, 10:00, 15:00, 20:00, and so on. For example, if the current time is 16:37, the next query is at 20:00.</li> <li>▪ <b>0 14 * * * *:</b> The query is performed at 14:00 every day.</li> <li>▪ <b>0 0 10 * * * *:</b> The query is performed at 00:00 on the 10th day of every month.</li> </ul> </li> </ul>
Scheduling Time Range	<p>Scheduling time range. Options:</p> <ul style="list-style-type: none"> <li>- <b>Start time:</b> The scheduling starts from a specified time, and no time range needs to be set. If the job is deleted, no new instances will be generated.</li> <li>- <b>Time range:</b> The scheduling time defined by the interval must be within this range. Otherwise, no new instances will be generated.</li> </ul>
Start Time	<p>The time when the job will first be executed. Set the start time or the time range based on the scheduling time range you select.</p>

Parameter	Description
SQL Window	<p>Runtime of the SQL scheduled job. Only logs in this period will be analyzed. The time expression can be precise to second (s: second; m: minute; h: hour), and the maximum period is 24 hours. Select <b>5 minutes</b>, <b>15 minutes</b>, <b>1 hour</b>, or <b>1 day</b> from the drop-down list, or select <b>Custom</b> and enter a time expression. Format: <b>[+/-{num}h+/-{num}m+/-{num}s@s,+/-{num}@h)</b>, where:</p> <ul style="list-style-type: none"> <li>- [: Indicates that the endpoint is included.</li> <li>- ): Indicates that the endpoint is excluded.</li> <li>- +: Indicates that the time starts forward from the current time. For example, if the current time is 16:00, <b>+1h</b> means 17:00. The plus sign (+) is not recommended.</li> <li>- -: Indicates that the time starts backward from the current time. For example, if the current time is 16:00, <b>-1h</b> means 15:00.</li> <li>- {num}: Indicates an integer. The time difference before and after the comma cannot exceed 24 hours.</li> <li>- @: Indicates rounding up. <b>@h</b> means rounding up to the nearest hour while ignoring the minute and second. <b>@m</b> means rounding up to the nearest minute while ignoring the second. <b>@s</b> means rounding up to the nearest second.</li> </ul> <p>Example time expressions:</p> <ul style="list-style-type: none"> <li>- 5 minutes: <b>[-5m@m,@m)</b></li> <li>- 15 minutes: <b>[-15m@m,@m)</b></li> <li>- 1 hour: <b>[-1h@h,@h)</b></li> <li>- 1 day: <b>[-24h@h,@h)</b></li> <li>- Custom (no more than one day): <b>[-65m@h,-5m@h)</b></li> </ul> <p><b>NOTE</b> The maximum interval indicated by a time expression is five times the scheduling interval.</p>
Timeout	<p>Threshold for automatic retry when the SQL analysis fails. An execution instance ends if it reaches the specified timeout or has timed out for the specified number of times. The status of the instance is <b>Failed</b>.</p> <ul style="list-style-type: none"> <li>- Timeout: 60–180 seconds</li> <li>- Timeout times: 1–10</li> </ul>

**Step 4** Click **OK**.

----End

## Viewing a SQL Scheduled Job

**Step 1** On the **SQL Scheduled Jobs** tab page, click the name of the target job to view its details, including the basic information and execution instance.

 **NOTE**

A maximum of 100 logs can be reported for each instance.

----End

## Modifying a SQL Scheduled Job

**Step 1** On the **SQL Scheduled Jobs** tab page, locate the target job and click **Modify** in the **Operation** column.

**Step 2** On the displayed page, modify the settings by referring to [Table 9-2](#).

 **NOTE**

The SQL scheduled job name and source log group/stream names cannot be modified.

----End

## Deleting a SQL Scheduled Job

**Step 1** On the **SQL Scheduled Jobs** tab page, locate the target job and click **Delete** in the **Operation** column.

Alternatively, click the name of the target job. On the displayed page, click **Delete** in the upper right corner.

**Step 2** Click **OK**.

----End

## 9.2 Processing Logs with FunctionGraph Function Templates

You can create functions from templates or scratch to normalize, transfer, anonymize, and filter logs.

 **NOTE**

Currently, this function is available only in the following regions. To use it in other regions, [submit a service ticket](#).

CN North-Beijing1, CN North-Beijing4, CN East-Shanghai1, CN East2, CN-Hong Kong, AP-Bangkok, AP-Singapore, AP-Jakarta, AF-Johannesburg, TR-Istanbul, LA-Mexico City1, LA-Mexico City2, LA-Sao Paulo1, and LA-Santiago

**Step 1** Log in to the LTS console.

**Step 2** Choose **Log Jobs** in the navigation pane and click the **Function Processing** tab.

**Step 3** Create functions from desired templates.

 NOTE

For details, see the [FunctionGraph User Guide](#).

----End

## 9.3 Generating Metrics from Logs (Beta)

You can create log metric rules to extract log data reported to LTS as metrics and view them on the metric browsing and dashboard pages of the AOM console.

 NOTE

Currently, this function is in closed beta testing. It is available to whitelisted users in regions CN North-Beijing4 and CN North-Ulanqab1, and will be available to all users in all regions later.

### Background

- You can create metric rules on the LTS console to generate statistical reports as required. You can also set a single log filter or add associations and groups to set multiple log filters to retain logs that meet the filters. Statistics on the structured logs within a specified time range can be collected dynamically and displayed on the Prometheus instances of AOM, which is easy to operate and powerful.
- Each metric rule can generate only one result. To obtain multiple results, you need to create multiple metric rules.

### Prerequisites

- A Prometheus instance has been created on the AOM console.
- Logs have been ingested to LTS.
- Log data has been structured. Currently, only structured log data can be used to generate metrics.

 NOTE

To generate metrics based on logs, the log time sequence deviation must be within a small range (5s if **Frequency** is set to **5s**, 1 minute if **Frequency** is set to **1 min**, and 1 minute and 30 seconds if **Frequency** is set to **5 min**). It is recommended that ICAgent be used to report logs in structured mode. If cloud structuring parsing is used, the log time may be out of order. As a result, logs cannot be processed within the statistical period and the statistical result is inaccurate.

### Constraints

A single user can create a maximum of 10 log metric rules. The total number of metrics added to all rules cannot exceed 10.

### Creating a Log Metric Rule

**Step 1** Log in to the LTS console.

**Step 2** Log in to the LTS console and choose **Log Jobs** in the navigation pane.

**Step 3** On the **Metric Generation** tab page, click **Create Rule**.

**Step 4** Configure basic log information.

1. Enter a rule name. A rule name can contain a maximum of 256 characters, including letters, digits, underscores (\_), and hyphens (-).
2. Enter the description information.
3. Retain the default setting of **Status** (enabled).
4. **Agency Authorization** is enabled by default. To create a log metric generation task, authorize LTS and AOM to create cloud service agencies **lts\_admin\_trust** and **aom\_admin\_trust**.
5. Enable **Task Monitoring** so that the execution status of each task is written to the log stream **lts-system/lts-logtometric-statistics**. You can view the monitoring center for metric generation tasks or configure alarm rules to detect exceptions that occur during processing in a timely manner.

**Step 5** Configure the data source.

1. Select a source log group. If no group is available, click **Create Log Group**.

 **NOTE**

- The logs that exceed the retention period will be automatically deleted. You can transfer logs to OBS buckets for long-term storage.
  - If your logs have not been ingested to LTS, create a log ingestion rule by referring to [Log Ingestion](#) and configure a log structuring parsing rule.
2. Select a source log stream. If no stream is available, click **Create Log Stream**.
  3. Enable **Log Sampling**. This function randomly samples the log source at a rate ranging from 0.1 to 0.9.

**Step 6** Configure the metric storage location.

1. Metrics generated from logs will be stored in AOM as user-defined metrics. Select the Prometheus instance where the metrics are to be stored. If no instance is available, click **Create an instance**.
2. Customize a name for the log generation metric. The value can contain only letters, digits, underscores (\_), and colons (:), and cannot start with a digit, underscore (\_), or colon (:).
3. Enter metric description.

**Step 7** Click **Next**.

**Step 8** Preview the information below **Metric Preview**. This simulates the metrics generated by executing SQL queries on log streams using the configured log filtering and statistics rules. To do so, you must first collect logs to LTS and configure structuring parsing rules and indexes. Otherwise, the preview is empty.

**Step 9** Implement statistical settings.

1. Set a log filtering rule. Then you can preview the effect. If you cannot find the desired log fields in the **Log Filtering** and **Log Statistics** areas, configure them in the collection settings first by referring to [Setting Cloud Structuring Parsing](#).

 **NOTE**

- You can filter logs using **OR** and **AND** conditions.
  - Different fields support different filtering rules.
  - The log filtering and statistics fields must be **string**, **float**, or **long** types, not **json**.
  - Log filtering is to reserve the logs that meet the conditions and discard the logs that do not meet the conditions.
  - The group by function must be **string** or **integer** types.
2. Select or customize the field to count and specify **Group by**. The data collected one minute later than the allowed period will not be counted.

 **NOTE**

- The following statistics types are supported:  
**count**: number of logs. **countKeyword**: number of times a keyword appears. **sum**: sum value of a specified field. **avg**: average value of a specified field. **max**: maximum value of a specified field. **min**: minimum value of a specified field. **P50**: the value below which 50% of the data falls. **P75**: the value below which 75% of the data falls. **P90**: the value below which 90% of the data falls. **P95**: the value below which 95% of the data falls. **P99**: the value below which 99% of the data falls.
  - For the P-series statistical type, the numbers are sorted and the value of *xx%* is used as the statistical result.
  - Log statistics are performed on logs that meet the conditions. During the execution, a log stream is generated in log group **system**. If the log stream is deleted, the execution details of all metric generation rules cannot be viewed.
3. Set the frequency. Options: **5s**, **1 min**, or **5 min**. The frequency not only represents the data reporting interval, but also represents the time window of the statistics operation. For example, **5 min** means that after a 5-minute interval is reached, the data of the previous 5 minutes is collected and reported.
4. After the setting is complete, the dimension is automatically generated based on the content selected in the query.
5. Select a unit. For example, select a unit for angle, bandwidth, or frequency.

**Step 10** (Optional) Click **Real-Time Log Preview** to view real-time logs.

**Step 11** Click **OK**.

**Step 12** View the new rule on the **Metric Generation** tab page.

 **NOTE**

- Metric visualization and alarm reporting: After a metric is created, you can go to the AOM console to configure a visualized metric chart on the **Dashboard** page or metric alarms on the **Alarm Rules** page.
- You are advised to configure a maximum of five rules for each log stream.
- You can click the buttons in the **Operation** column of the rule list to copy, modify, or delete a rule.

----End

# 10 Configuration Center

---

## 10.1 Setting LTS Log Collection Quota and Usage Alarms

### Enabling or Disabling Log Collection Beyond Free Quota

When the monthly free quota (500 MB) is used up, you will be billed for any excess usage on a pay-per-use basis. To avoid extra expenses, you can configure log collection to stop when the quota runs out.

 **NOTE**

- The function is enabled by default. If it is enabled, logs will continue to be collected after the free quota (500 MB) is used up. You will be billed for the excess usage on a pay-per-use basis.
- Log usage, including log read/write, log indexing, and log retention, are billed in LTS. If log collection is disabled when the free quota is used up, no fee is generated for log read/write and indexing because these operations will not be performed. However, log data that beyond the free quota is still retained in LTS and fees are generated for the log retention. When the logs age out after the specified retention period, no fees will be generated.
- If you enable or disable **Continue to Collect Logs When the Free Quota is Exceeded** in AOM, this function will be synchronously enabled or disabled in LTS.

**Step 1** Log in to the [LTS console](#).

**Step 2** In the navigation pane, choose **Configuration Center**. The **Quota Configuration** tab page is displayed by default.

**Step 3** Disable **Continue to Collect Logs When the Free Quota Is Exceeded**.

When the free quota (500 MB) is used up, log collection will be suspended. You can view the current resource usage in **Overview** area on the **Log Management** page. For details, see [Viewing Log Management](#).

----End




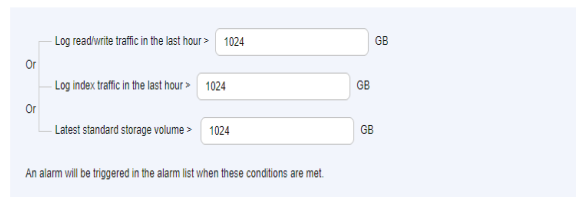
## Configuring Usage Alerts

Enabling the custom log resource usage alarm will automatically create an alarm rule. If the log resource usage exceeds a specified limit, the system gives an alarm. The log resource usage includes the read and write traffic, index traffic, and standard storage volume.

**Step 1** On the **Quota Configuration** tab page, enable **Custom Quota Alarm**.

After this function is enabled, the **statistics** data on the home page is delivered to the automatically created log stream (**lts-system/lts-resource-statistics**). You can set the log usage alarm limits.

 After this function is enabled, log resource statistics on the LTS home page are sent to lts-system/lts-resource-statistics. You can customize log resource usage warnings based on the log alarm function.



**Table 10-1** Parameter description

Parameter	Description
Log read/write traffic in the last hour	The default value is <b>1,024 GB</b> and the minimum value is <b>0</b> . The value can only contain digits and up to four decimal places. It cannot start or end with a decimal point. A maximum of 10 characters are allowed. An alarm is given when the log read/write traffic exceeds this limit.
Log index traffic in the last hour	The default value is <b>1,024 GB</b> and the minimum value is <b>0</b> . The value can only contain digits and up to four decimal places. It cannot start or end with a decimal point. A maximum of 10 characters are allowed. An alarm is given when the log index traffic exceeds this limit.
Latest standard storage volume	Log volume quota in the last hour. The default value is <b>1,024 GB</b> and the minimum value is <b>0</b> . The value can only contain digits and up to four decimal places. It cannot start or end with a decimal point. A maximum of 10 characters are allowed. An alarm is given when the latest standard storage volume exceeds this limit.

 NOTE

- The preceding parameters are in the "OR" relationship, which means an alarm will be given if any of these limits is exceeded.
- This function is disabled by default. After it is enabled, an alarm rule will be triggered when the log resource usage exceeds 1,024 GB.
- Enabling this function automatically creates a log group/stream (**lts-system/lts-resource-statistics**) and alarm rule (**log-statistics-alarm**). Disabling it automatically deletes the alarm rule.
- The log resource usage is updated every hour.
- The automatically created alarm rule includes this SQL statement: **select write\_traffic,index\_traffic,storage**. The conditional expression is **write\_traffic > 1024E12 || index\_traffic > 1024E12 || storage > 1024E13**. If you want to be notified of alarms by SMS or email, modify the alarm rule.
- If the alarm rule does not exist, enable the log resource usage alarm again to create one.

----End

## 10.2 Configuring Log Content Delimiters

You can configure delimiters to split log content into words, so you can search for logs by these words. LTS has preconfigured the following delimiters:

```
,";=()[]{}@&<>/:\\?\n\t\r
```

If the default delimiters cannot meet your needs, you can set custom delimiters.

### Precautions

- Your custom delimiters are applicable only to the log events generated after the delimiters are configured.
- The delimiter configured on the **Delimiters** tab page takes effect for all log streams in the current region. For details about how to configure delimiters for a single log stream, see [Setting Indexes](#).

### Procedure

**Step 1** Log in to the [LTS console](#).

**Step 2** Choose **Configuration Center** in the navigation pane and click the **Delimiters** tab.

**Step 3** Configure delimiters.

You can configure delimiters in either of the following ways. If you use both ways, the delimiters configured in the two ways will all take effect.

- **Common Delimiters:** Click **Edit** and enter custom delimiters in the text box.
- **ASCII Delimiters:** Click **Edit** > **Add ASCII Delimiter**, and enter ASCII values by referring to [ASCII Table](#).

**Step 4** Preview the parsing result.

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

**Step 5** Check whether the parsing result is correct. If it is correct, click **Save**.

 NOTE

You can click **Reset** to restore the default delimiters.

----End

## ASCII Table

Table 10-2 ASCII table

AS CII Val ue	Character	ASC II Val ue	Character	AS CII Val ue	Character	AS CII Val ue	Character
0	NUL (Null)	32	Space	64	@	96	`
1	SOH (Start of heading)	33	!	65	A	97	a
2	STX (Start of text)	34	"	66	B	98	b
3	ETX (End of text)	35	#	67	C	99	c
4	EOT (End of transmission)	36	\$	68	D	100	d
5	ENQ (Enquiry)	37	%	69	E	101	e
6	ACK (Acknowledge)	38	&	70	F	102	f
7	BEL (Bell)	39	'	71	G	103	g
8	BS (Backspace)	40	(	72	H	104	h
9	HT (Horizontal tab)	41	)	73	I	105	i
10	LF (Line feed)	42	*	74	J	106	j
11	VT (Vertical tab)	43	+	75	K	107	k
12	FF (Form feed)	44	,	76	L	108	l
13	CR (Carriage return)	45	-	77	M	109	m

AS CII Value	Character	ASC II Value	Character	AS CII Value	Character	AS CII Value	Character
14	SO (Shift out)	46	.	78	<b>N</b>	110	<b>n</b>
15	SI (Shift in)	47	/	79	<b>O</b>	111	<b>o</b>
16	DLE (Data link escape)	48	<b>0</b>	80	<b>P</b>	112	<b>p</b>
17	DC1 (Device control 1)	49	<b>1</b>	81	<b>Q</b>	113	<b>q</b>
18	DC2 (Device control 2)	50	<b>2</b>	82	<b>R</b>	114	<b>r</b>
19	DC3 (Device control 3)	51	<b>3</b>	83	<b>S</b>	115	<b>s</b>
20	DC4 (Device control 4)	52	<b>4</b>	84	<b>T</b>	116	<b>t</b>
21	NAK (Negative acknowledge)	53	<b>5</b>	85	<b>U</b>	117	<b>u</b>
22	SYN (Synchronous idle)	54	<b>6</b>	86	<b>V</b>	118	<b>v</b>
23	ETB (End of transmission block)	55	<b>7</b>	87	<b>W</b>	119	<b>w</b>
24	CAN (Cancel)	56	<b>8</b>	88	<b>X</b>	120	<b>x</b>
25	EM (End of medium)	57	<b>9</b>	89	<b>Y</b>	121	<b>y</b>
26	SUB (Substitute)	58	:	90	<b>Z</b>	122	<b>z</b>
27	ESC (Escape)	59	;	91	<b>[</b>	123	<b>{</b>
28	FS (File separator)	60	<	92	<b>\</b>	124	<b> </b>
29	GS (Group separator)	61	=	93	<b>]</b>	125	<b>}</b>
30	RS (Record separator)	62	>	94	<b>^</b>	126	<b>~</b>
31	US (Unit separator)	63	?	95	<b>_</b>	127	<b>DEL (Delete)</b>

## 10.3 Setting ICAgent Collection

On the **ICAgent Collection** tab page, you can disable or enable ICAgent collection (that is, specify whether ICAgent collects log data), syslog log collection to AOM, ICAgent diagnosis, and container standard output to AOM.

### Setting Collection

- Step 1** Log in to the [LTS console](#).
- Step 2** Choose **Configuration Center** in the navigation pane and click the **ICAgent Collection** tab.
- Step 3** Toggle the **ICAgent Collection** switch to control whether ICAgent collects logs.
- **ICAgent Collection** is toggled on by default. If you do not need to collect logs, toggle it off to reduce resource usage.
  - After it is toggled off, ICAgent will stop collecting logs, and the log collection function on the AOM console will also be disabled.
- Step 4** Toggle the **Collect Syslog Logs to AOM** switch to set whether ICAgent collects Syslogs to AOM 1.0. If it is toggled off, ICAgent does not collect Syslog logs to AOM 1.0. This function is only available with ICAgent 5.12.182 and later.
- Step 5** **Output to AOM:** Select a CCE cluster and toggle on or off the **Apply to Cluster** switch for it. If it is toggled off, ICAgent does not collect the cluster stdout logs to AOM. This function is only available with ICAgent 5.12.133 and later. You are advised to collect container standard output to LTS instead of AOM. For details, see [Ingesting CCE Application Logs to LTS](#).
- Step 6** Toggle the **ICAgent Diagnosis** switch to enable or disable collection diagnosis. If it is toggled off, ICAgent run logs are reported to log group/stream **lts-system/lts-icagent-statistics** for monitoring ICAgent running status and exceptions in real time. This function is only available with ICAgent 5.12.196 and later.

----End

# 11 Querying Real-Time LTS Traces

## Overview

CTS can record operations (traces) related to LTS for query, audit, and backtracking.

After you enable CTS, the system starts to record LTS operations. CTS stores operation records from the last seven days.

## Enabling CTS

To enable CTS, see [Enabling CTS](#).

After CTS is enabled, if you want to view LTS traces, see [Querying Real-Time Traces](#).

## LTS Operations That Can Be Recorded by CTS

**Table 11-1** LTS operations that can be logged by CTS

Operation	Resource Type	Trace Name
Creating a log group	group	createLogGroup
Modifying a log group	group	updateLogGroup
Deleting a log group	group	deleteLogGroup
Creating a log stream	topic	createLogStream
Modifying a log stream	topic	updateLogStream
Deleting a log stream	topic	deleteLogStream
Deleting a log bucket	logPailSetting	deleteLogPail
Creating an OBS log transfer task	als	addLogPailToOBS
Modifying an OBS log transfer task	als	updateLogPailToOBS

Operation	Resource Type	Trace Name
Deleting an OBS log transfer task	als	deleteLogPailToOBS
Batch enabling and disabling log transfer tasks	als	batchActionLogPail-ToOBS
Creating a metric filter	filter	createLogFilter
Modifying a metric filter	filter	updateLogFilter
Deleting a metric filter	filter	deleteLogFilter
Modifying metric filter status	filter	updateLogFilterStatus
Enabling log transfer	transfer	createLogTransfer
Modifying log transfer	transfer	updateLogTransfer
Deleting log transfer	transfer	deleteLogTransfer
Creating quick search criteria	searchCriteria	createLogSearchCriteria
Modifying quick search criteria	searchCriteria	updateLogSearchCriteria
Deleting quick search criteria	searchCriteria	deleteLogSearchCriteria
Adding a collection path	LogAgent	createLogAgent
Modifying a collection path	LogAgent	updateLogAgent
Deleting a collection path	LogAgent	deleteLogAgent
Creating a structuring template	structLogConfig	createLogStreamStruct-Config
Modifying a structuring template	structLogConfig	updateLogStreamStruct-Config
Deleting a structuring template	structLogConfig	deleteLogStreamStruct-Config
Creating a quick analysis task	wordFreqConfig	updateWordFreqConfig
Saving the path configuration	path	addLogPath
Adding a statistical rule	rule	addRuleStatistics

Operation	Resource Type	Trace Name
Modifying a statistical rule	rule	updateRuleStatistics
Deleting a statistical rule	rule	deleteRuleStatistics
Creating a structuring rule	structurization	addStructurization
Deleting a structuring rule	structurization	deleteStructurization
Adding a Kafka instance	dmsKafka	registerKafkaInfo
Modifying a Kafka instance	dmsKafka	updateKafkaInfo
Deleting a Kafka instance	dmsKafka	deleteKafkaInfo
Creating a DIS transfer task	transfer	createDisTransfer
Modifying a DIS transfer task	transfer	updateDisTransfer
Deleting a DIS transfer task	transfer	deleteDisTransfer
Creating a Kafka transfer task	kafkaTransfer	createKafkaTransfer
Modifying a Kafka transfer task	kafkaTransfer	updateKafkaTransfer
Deleting a Kafka transfer task	kafkaTransfer	deleteKafkaTransfer
Creating a log cleaning rule	logFilter	createLogFilterRules
Modifying a log cleaning rule	logFilter	updateLogFilterRules
Deleting a log cleaning rule	logFilter	deleteLogFilterRules
Creating a chart	logChart	createLogChart
Modifying a chart	logChart	updateLogChart
Deleting a chart	logChart	deleteLogChart
Creating a dashboard	logDashboard	createLogDashboard
Modifying a dashboard	logDashboard	updateLogDashboard
Deleting a dashboard	logDashboard	deleteLogDashboard



Operation	Resource Type	Trace Name
Enabling continuation of log collection when the free quota is exceeded	LogCollectionSwitchOperation	LogCollectionSwitchOperation
Disabling continuation of log collection when the free quota is exceeded	LogCollectionSwitchOperation	LogCollectionSwitchOperation
Creating an ELB log bucket	elbPailType	createElbPail
Modifying an ELB log bucket	elbPailType	updateElbPail
Deleting an ELB log bucket	elbPailType	deleteElbPail
Adding a log path collection rule	logPathCollectionType	createLogPathCollection
Modifying a log path collection rule	logPathCollectionType	updateLogPathCollection
Deleting a log path collection rule	logPathCollectionType	deleteLogPathCollection
Clearing Redis cache	cleanTenantResource-Type	deleteCleanTenantResource