Log Tank Service

Getting Started

Issue   01
Date   2025-02-27

Contents

1 Using ICAgent to Collect ECS Text Logs to LTS

Log Tank Service (LTS) is a one-stop log data solution for collecting, storing, searching, processing, and analyzing logs, viewing logs in dashboards, and reporting log alarms. LTS provides stable and reliable services, eliminating resource concerns like scalability. It also makes log O&M easier and improves the fault locating and metric monitoring efficiency.

This section uses ECS text logs as an example to help you get started with LTS. You need to create a log group and stream for storing ECS text logs, install ICAgent on the ECS from which you want collect logs, and configure ECS text log ingestion. Then, you can view the reported real-time logs on the LTS console.

Procedure

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

Figure 1-1 Flowchart
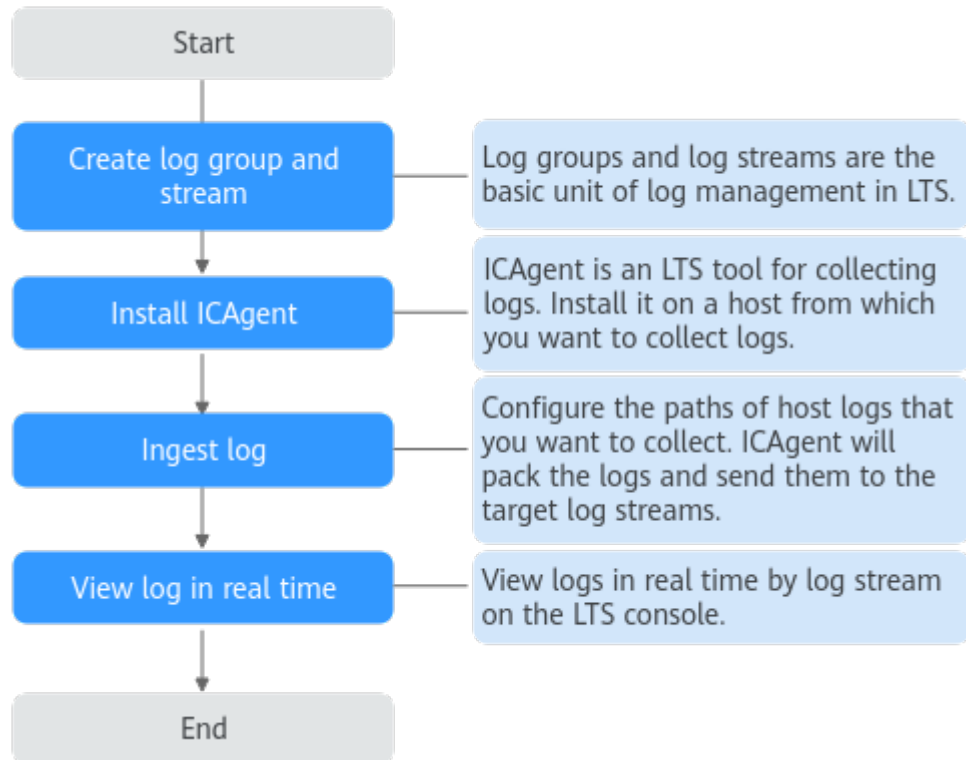
1. **Step 1: Creating a Log Group and Stream**

2. **Step 2: Installing ICAgent**

3. **Step 3: Ingesting ECS Logs to LTS**

4. **Step 4: Viewing Logs in Real Time**

Prerequisites

- Grant the LTS operation permissions to the user.

  To do so, you must have the LTS administrator permissions **LTS Full Access**. For details, see **Granting LTS Permissions to IAM Users**.

- This section uses a Linux ECS as an example. Prepare an ECS for log collection. For details, see **Purchasing an ECS in Custom Config Mode**. If you already have an available ECS, skip this step.

Step 1: Creating a Log Group and Stream

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

Step 1 Log in to the **LTS console**.

Step 2 On the **Log Management** page, click **Create Log Group**. On the displayed page, set parameters by referring to **Table 1-1**.

Figure 1-2 Creating a log group

Table 1-1 Parameter description

Parameter	Description	Example Value
Log Group Name	• Enter 1 to 64 characters, including only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period. • Collected logs are sent to the log group. If there are too many logs to collect, separate logs into different log groups based on log types, and name log groups in an easily identifiable way.	lts-group-ECS
Enterprise Project Name	Select the required enterprise project. The default value is **default**.	default
Log Retention (Days)	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. By default, logs are retained for 30 days (customizable for 1 to 365 days). 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.	30
Tag	You can tag log groups as required. In this practice, you do not need to set this parameter.	-

Parameter	Description	Example Value
Remark	Enter remarks. The value contains up to 1,024 characters. In this practice, you do not need to set this parameter.	-

Step 3 Click **OK**. The created log group will be displayed in the log group list.

Step 4 Click ∨ on the left of target log group.

Step 5 Click **Create Log Stream**. On the displayed page, set parameters by referring to **Table 1-2**.

Figure 1-3 Creating a log stream

Table 1-2 Parameter description

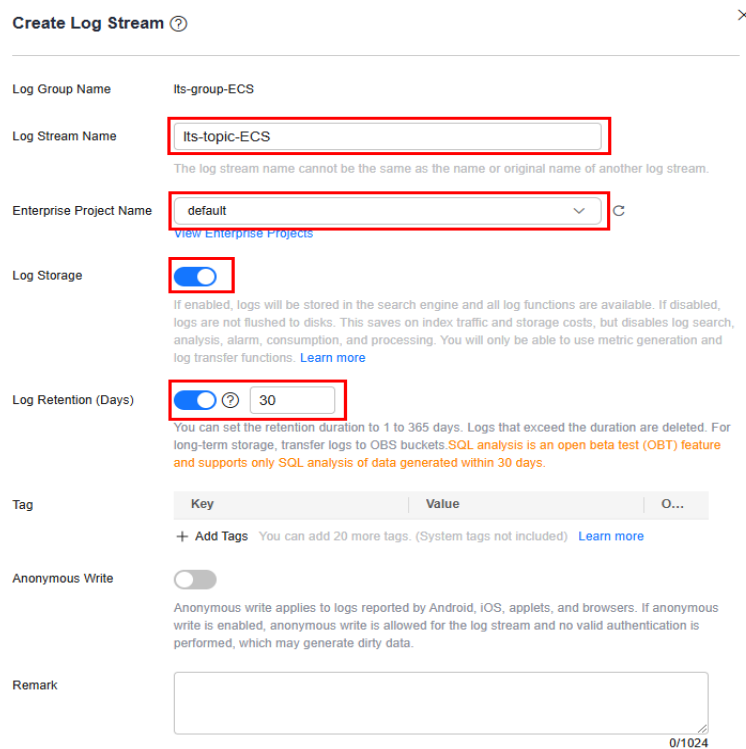| Parameter	Description	Example Value
Log Group Name	The name of the target log group is displayed by default.	-

Parameter	Description	Example Value
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. - Collected logs are sent to the created log stream. If there are a large number of logs, you can create multiple log streams and name them for quick log search.	lts-topic-ECS
Enterprise Project Name	Select the required enterprise project. The default value is **default**.	default
Log Storage	If this function is enabled, logs will be stored in the search engine and all log functions are available. If this function is disabled, **Log Retention (Days)** cannot be enabled.	Enable
Log Retention (Days)	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. By default, logs are retained for 30 days (customizable for 1 to 365 days). - If **Log Retention (Days)** is enabled for the log stream, the log retention duration set for the log stream is used. - 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.	30
Tag	You can tag log groups as required. In this practice, you do not need to set this parameter.	-
Anonymous Write	Disabled by default. In this practice, retain the default setting. This function is applicable to logs reported by Android, iOS, applets, and browsers.	Disable
Remark	Enter remarks. The value contains up to 1,024 characters. In this practice, you do not need to set this parameter.	-

Step 6 Click **OK**.

Step 7 Check the created log stream under the target log group.

----End

Step 2: Installing ICAgent

ICAgent is the log collection tool of LTS. Install ICAgent on a host from which you want to collect logs. Then, you can collect logs of the host without installing ICAgent again.

The following describes how to install ICAgent. In this practice, set **Host** to **Intra-region hosts**, **OS** to **Linux**, and **Installation Mode** to **Obtain AK/SK**.

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

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

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

Table 1-3 Installing ICAgent

Parameter	Description	Example Value
Host	**Intra-region hosts** is selected by default. Check whether the host whose logs need to be collected is in or out of the region. An intra-region host is in the same region as the LTS console, for example, CN North-Beijing4.	-
OS	**Linux** is selected by default.	-
Installation Mode	**Obtain AK/SK** is selected by default. For details, see **How Do I Obtain an Access Key (AK/SK)?**	-

Figure 1-4 Installing ICAgent
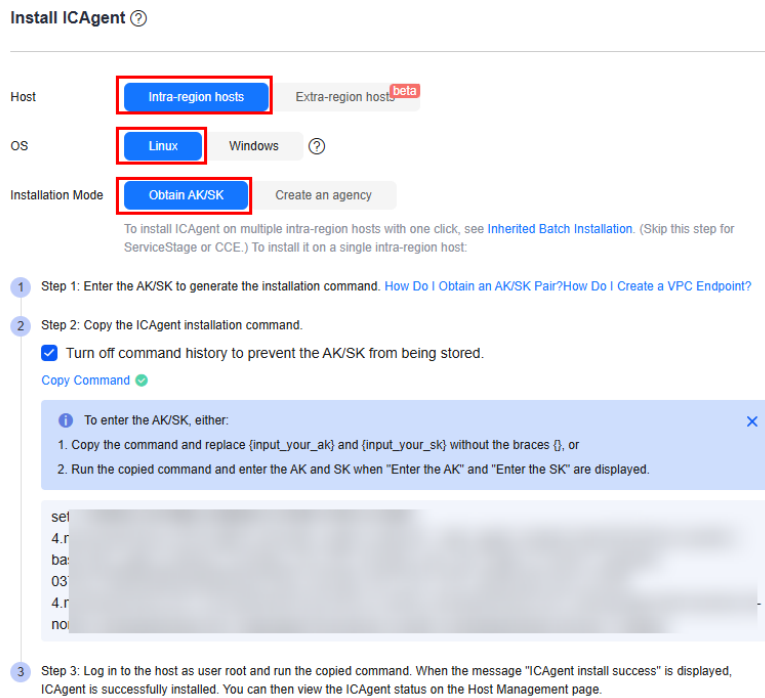
Step 3 Click **Copy Command** to copy the ICAgent installation command.

Step 4 Log in to the ECS. 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 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.)

6. When message **ICAgent install success** is displayed, ICAgent has been installed in the **/opt/oss/servicemgr/** directory of the host.

Figure 1-5 Installation command output

Step 5 After the installation is successful, choose **Host Management** in the LTS navigation pane and click **Hosts** to check whether the ICAgent status is **Running** for the host (**ECS-test-dqy** in this practice).

Figure 1-6 Hosts

----End

Step 3: Ingesting ECS Logs to LTS

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

Step 1 Choose **Log Ingestion** > **Ingestion Center** in the navigation pane and click **ECS (Elastic Cloud Server)**.

Step 2 The page for selecting a log stream is displayed.

1. Select a log group from the drop-down list of **Log Group**, for example, **lts-group-ECS**.

2. Select a log stream from the drop-down list of **Log Stream**, for example, **lts-topic-ECS**.

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

Step 3 Select one or more host groups.

1. Click **Create** in the upper left corner of the host group list. In the displayed right pane, create a host group by referring to **Table 1-4** and click **OK**.

Figure 1-7 Creating a host group
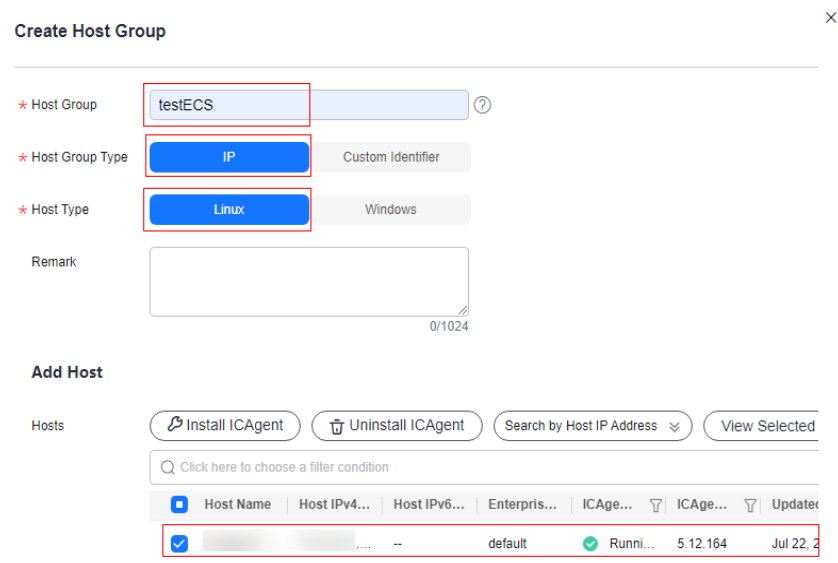
Table 1-4 Creating a host group

Parameter	Description	Example Value
Host Group	Enter a custom host group name. Use only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period.	testECS
Host Group Type	**IP** is selected by default. Host groups of the **IP** type: The IP addresses of servers are added to the host group so that the servers can be identified by the IP address.	IP
Host Type	**Linux** is selected by default. The host type must be the same as that selected during **ICAgent installation**.	Linux
Remark	Enter remarks. The value contains up to 1,024 characters. In this practice, you do not need to set this parameter.	-
Add Host	In the host list, select one or more hosts with ICAgent installed. The screenshot is for reference only. Select hosts based on site requirements.	ECS-test-dqy

2. After the host group is created, select the host group to collect its logs.

3. Click **Next: Configurations**.

Step 4 Configure collection rules. For details, see **Table 1-5**.
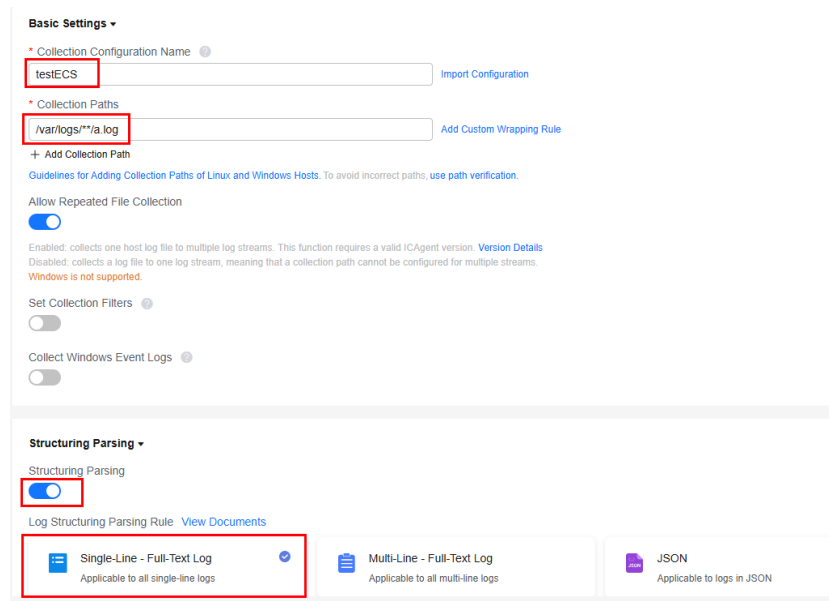
Figure 1-8 Collection configuration


Table 1-5 Collection configuration

Parameter	Description	Example Value
Collection Configuration Name	Enter a custom name. Use only letters, digits, hyphens (-), underscores (_), and periods (.). Do not start with a period or underscore or end with a period.	testECS
Collection Paths	Add one or more host paths. LTS will collect logs from these paths. For example, **/var/logs/**/a.log** matches the following logs: /var/logs/1/a.log /var/logs/1/2/a.log /var/logs/1/2/3/a.log /var/logs/1/2/3/4/a.log /var/logs/1/2/3/4/5/a.log ● **/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.	/var/logs/**/a.log

Parameter	Description	Example Value
Allow Repeated File Collection	This function is not available to Windows. After you enable this function, one host log file can be collected to multiple log streams.	Enable
Set Collection Filters	Blacklisted directories or files will not be collected. Filters can be exact matches or wildcard matches. If you specify a directory, all its files are filtered out. Collection filters cannot be set for Windows hosts. In this practice, retain the default setting (disabled) for this parameter to collect all files.	Disable
Collect Windows Event Logs	In this practice, the host is a Linux host and this option is disabled by default.	Disable
Structuring Parsing	Enable structuring parsing and select **Single Line - Full-Text Log** for **Log Structuring Parsing Rule**. For more rules, see **Setting ICAgent Structuring Parsing Rules**.	Enable
Max Directory Depth	The maximum directory depth is 20 levels. 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 **/var/logs/department/app/a.log** and your collection path is **/var/logs/**/a.log**, logs will not be collected when this parameter is set to **1**, but will be collected when this parameter is set to **2** or a larger number.	20
Split Logs	Splits single-line logs larger than 500 KB into multiple lines for collection. For example, a 600 KB single-line log will be split into a line of 500 KB and a line of 100 KB. In this practice, enable this function.	Enable
Collect Binary Files	In this practice, enable this option to collect binary files. Run the **file -i** *File name* command to view the file type. **charset=binary** indicates that a log file is a binary file. If this option is enabled, binary log files will be collected, but only UTF-8 strings are supported. Other strings will be garbled on the LTS console.	Enable
Log File Code	The encoding format of log files is UTF-8.	-

Parameter	Description	Example Value
Collection Policy	In this practice, set the collection policy to **Incremental**. **Incremental**: When collecting a new file, ICAgent reads the file from the end of the file.	-
Custom Metadata	Disabled by default. In this practice, retain the default setting. ICAgent will collect logs based on system built-in fields and your custom key-value pairs.	-
Log Format	Set the display format of logs reported to LTS. In this practice, select **Single-line**. If **Structuring Parsing** is enabled, you do not need to set this parameter. **Single-line**: Each log line is displayed as a single log event.	Single-line
Log Time	Set the log collection time to be displayed at the beginning of each log line. In this practice, select **System time**. If **Structuring Parsing** is enabled, you do not need to set this parameter. **System time**: log collection time by default. It is displayed at the beginning of each log event.	System time

Step 5 Click **Next: Index Settings**. On the displayed page, retain the default parameter settings. After configuring the index, you can query and analyze logs. For more information, see **Setting Indexes**.

Figure 1-9 Index settings
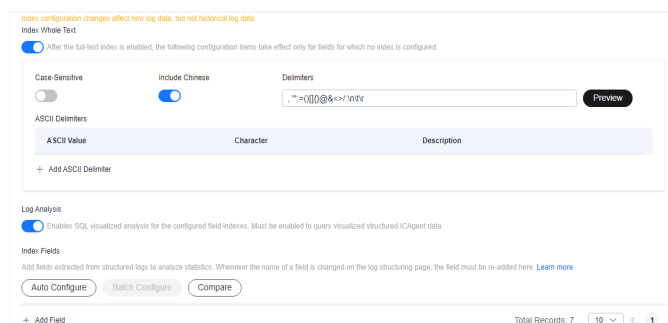
- **Index Whole Text**: enabled by default, indicating a full-text index is created. By default, **Case-Sensitive** and **Include Chinese** are enabled, and the delimiters are '";=()[]{}@&<>/:\\?\n\t\r

- **Log Analysis**: enables SQL visualized analysis for the configured field indexes. This parameter is enabled by default.

- **Index Fields**: LTS creates index fields for certain system reserved fields (such as **hostIP**, **hostName**, and **pathFile**) by default. For more system reserved fields, see **Setting Indexes**.

Step 6 Click **Submit**. After the log ingestion is complete, click **Back to Ingestion Configurations**. An ingestion configuration will be displayed on the **Ingestion Management** page.

----End

Step 4: Viewing Logs in Real Time

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

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

Step 1 On the **Ingestion Management** page, click the log stream name in the **Log Stream** column of the target ingestion task to access the log stream details page.

Step 2 Click the **Real-Time Logs** tab to view logs in real time.

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

Figure 1-10 Real-time logs
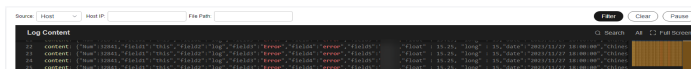
----End

Related Information

After logs are ingested, click the log stream name in the **Log Stream** column of the target log ingestion task on the **Log Ingestion** page. On the log stream details page displayed, you can search and analyze reported logs by referring to **Log Search and Analysis**.

2 Getting Started with Common Practices

After completing basic operations such as log groups and log streams, you can follow LTS's common practices to implement your services.

Table 2-1 Common practices

Practice	Description
Analyzing Huawei Cloud ELB Logs on LTS	This solution describes how to search and analyze logs after Elastic Load Balance (ELB) logs are ingested to LTS and log structuring is configured.
Serverless Real-Time Log Analysis	This solution helps you collect, analyze, and archive ECS logs with a serverless architecture. It uses LTS to collect ECS logs, FunctionGraph LTS trigger to obtain logs and analyze alarms in logs, Simple Message Notification (SMN) to push alarms to users, and Object Storage Service (OBS) to archive alarms.