Log Tank Service

Service Overview

Issue 01

Date 2023-07-19

HUAWEI

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Contents

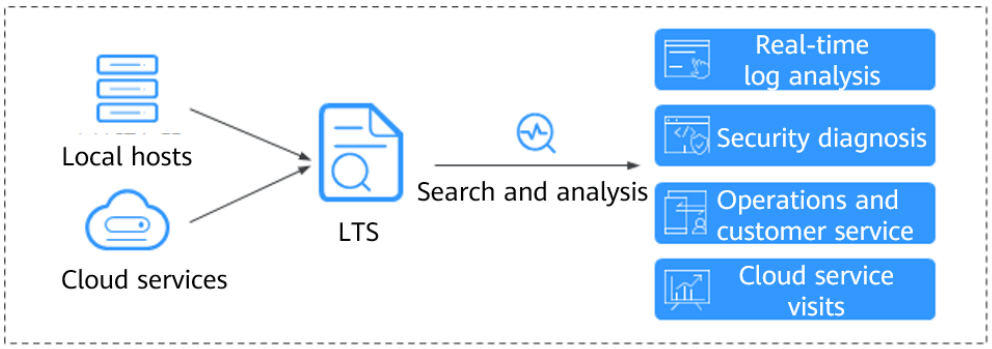
1 What Is Log Tank Service?

Log Tank Service (LTS) enables you to collect logs from hosts and cloud services for centralized management, and analyze large volumes of logs efficiently, securely, and in real time. LTS provides you with the insights for optimizing the availability and performance of cloud services and applications. It allows you to make faster data-driven decisions, perform device O&M with ease, and analyze service trends.

Log Collection and Analysis

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

Figure 1-1 Log collection and analysis



2 Basic Functions

Real-time Log Collection

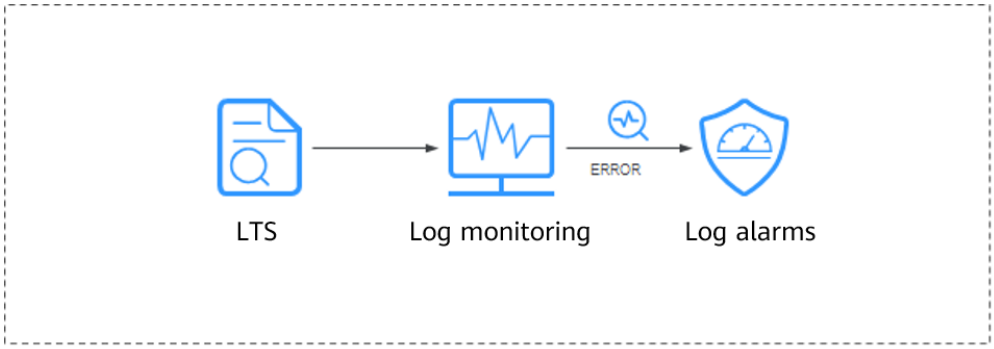
LTS collects real-time logs and displays them on the LTS console in an intuitive and orderly manner. You can query logs or transfer logs for long-term storage.

Log Query and Real-Time Analysis

Collected logs can be quickly queried by keyword or fuzzy match. You can analyze real-time logs for security diagnosis and analysis, or obtain operations statistics, such as cloud service visits and clicks.

Log Monitoring and Alarm Reporting

LTS works with Application Operations Management (AOM) to count the frequency of specified keywords in logs retained in LTS. In this way, you can monitor service running status.



Log Transfer

Logs reported from hosts and cloud services are retained in LTS for seven days by default. You can set the retention period to 1 to 365 days. Retained logs are deleted once the period is over. For long-term storage, you can transfer logs to Object Storage Service (OBS). Log transfer is to replicate logs to the target cloud service. It means that, after log transfer, the original logs will still be retained in LTS until the configured retention period ends.

3 Application Scenarios

Log Collection and Analysis

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

Service Performance Optimization

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

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

Quickly Locating Network Faults

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

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

4 Usage Restrictions

4.1 Basic Resources

This section describes restrictions on LTS basic resources.

Table 4-1 Basic resource restrictions

Item	Description	Remarks
Log groups	Up to 100 log groups can be created in a Huawei account.	To increase the upper limit, **create a service ticket**.
Log streams	Up to 100 log streams can be created in a log group. **NOTE** The log stream name must be unique.	To increase the upper limit, **create a service ticket**.
Log retention	Logs can be retained for 1 to 365 days.	N/A
Host groups	Up to 200 host groups can be created in a Huawei account.	To increase the upper limit, **create a service ticket**.
Quick searches	Up to 10 quick searches can be created in a log stream.	N/A
LogItem (single-line log event)	Using APIs: A single-line log event should be at most 1 MB during ingestion.	N/A
	Using APIs: A single-line log event can contain up to 100 labels.	
	Using ICAgent: A single-line log event should be at most 500 KB during ingestion.	

4.2 Log Read/Write

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

Table 4-2 Log read/write restrictions

Category	Item	Description	Remarks
Huawei account	Log write traffic	Logs are written at a rate up to 500 MB/s in a Huawei account.	To increase the upper limit, **create a service ticket**.
	Log writes	Logs are written up to 10,000 times per second in a Huawei account.	To increase the upper limit, **create a service ticket**.
	Log query	Up to 10 MB of logs are returned in a single API query for a Huawei account.	To increase the upper limit, **create a service ticket**.
	Log reads	Logs are read up to 1000 times per minute in a Huawei account.	To increase the upper limit, **create a service ticket**.
Log group	Log write traffic	Logs are written at a rate up to 200 MB/s in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log writes	Logs are written up to 1000 times per second in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log query traffic	Up to 10 MB of logs are returned in a single API query for a log group.	N/A

Category	Item	Description	Remarks
	Log reads	Logs are read up to 500 times per minute in a log group.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
Log stream	Log write traffic	Logs are written at a rate up to 100 MB/s in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log writes	Logs are written up to 500 times per second in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log query traffic	Up to 10 MB of logs are returned in a single API query for a log stream.	N/A
	Log reads	Logs are read up to 100 times per minute in a log stream.	Not mandatory. Service quality cannot be ensured if this limit is exceeded.
	Log time	Logs in a period of 24 hours can be collected. Logs generated 24 hours before or after the current time cannot be collected. For example: • If the current time is 11:00 on January 7, 2022, logs generated before 11:00 on January 6 cannot be collected. • If the current time is 11:00 on January 7, 2022, logs generated after 11:00 on January 8 cannot be collected.	N/A

4.3 ICAgent

This section describes the restrictions on the log collector ICAgent.

Table 4-3 ICAgent file collection restrictions

Item	Description	Remarks
File encoding	Only UTF 8 is supported. Other encoding formats may cause garbled characters. For example, binary files.	N/A
Log file size	Unlimited.	N/A
Log file rotation	ICAgent supports configuration of fixed log file names or fuzzy match of log file names. You need to rotate log files manually.	N/A

Item	Description	Remarks
Log collection path	**Linux** • Collection paths support recursion. You can use double asterisks (**) to collect logs from up to five directory levels. Example: **/var/logs/**/a.log** • Collection paths support fuzzy match. You can use an asterisk (*) to represent one or more characters of a directory or file name. Example: **/var/logs/*/a.log** or **/var/logs/service/a*.log** • If the collection path is set to a directory, for example, **/var/logs/**, only **.log**, **.trace**, and **.out** files in the directory are collected. If the collection path is set to name of a text file, that file is directly collected. • Each collection path must be unique. That is, the same path of the same host cannot be configured for different log groups and log streams. **Windows** • Collection paths support recursion. You can use double asterisks (**) to collect logs from up to five directory levels. Example: **C:\var\service**\a.log** • Collection paths support fuzzy match. You can use an asterisk (*) to represent one or more characters of a directory or file name. Examples: **C:\var\service*\a.log** and **C:\var\service\a*.log** • Each collection path must be unique. That is, the same path of the same host cannot be configured for different log groups and log streams. • Each collection path must be unique. That is, the same path of the same host cannot be configured for different log groups and log streams.	N/A

Item	Description	Remarks
Symbolic link	Symbolic links are not supported.	N/A
Single log size	The maximum size of each log is 500 KB. Excess content will be truncated by ICAgent.	N/A
Regular expression	Perl regular expressions are supported.	N/A
File collection configuration	A file can be reported to only one log group and stream. If a file is configured for multiple log streams, only one configuration takes effect.	N/A
File opening	Files are opened when being read, and closed after being read.	N/A
First log collection	All logs are collected.	N/A

Table 4-4 ICAgent performance specifications

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

Item	Description	Remarks
Default resource restrictions	CPU • Max. two CPU cores. Memory • Max. min{4 GB, Physical memory / 2}. A restart is triggered if this memory limit is exceeded. "min{4 GB, Physical memory / 2}" means that the smaller value between half of the physical memory and 4 GB is used.	N/A
Resource limit reached	A forcible restart is triggered. Logs may be lost or duplicate if rotated during the restart.	N/A
Agent installation, upgrade, or uninstallation	No restrictions.	N/A

Table 4-5 Other restrictions on ICAgent

Item	Description	Remarks
Configuration update	Configuration updates take effect in 1 to 3 minutes.	N/A
Dynamic configuration loading	Console configurations can be dynamically delivered. The update of one configuration does not affect other configurations.	N/A
Configurations	Unlimited.	N/A
Tenant isolation	Tenants are isolated from each other by default.	N/A

Item	Description	Remarks
Log collection delay	Normally, the delay from writing logs to the disk to collecting the logs is less than 2s (congestion not considered).	N/A
Log upload	File changes are read and uploaded immediately once detected. One or more logs can be uploaded a time.	N/A
Network error handling	Network exceptions trigger retries at an interval of 5s.	N/A
Resource quota used up	If the resources allocated to the ICAgent are insufficient due to massive amounts of logs, the ICAgent continues and retries upon a failure. Logs will be stacked if resources are still insufficient.	N/A
Max. retry timeout	Retry attempts are periodically made.	N/A
Status check	The collector status is monitored through heartbeat detection.	N/A
Checkpoint timeout	Checkpoints are automatically deleted if no updates are made within 12 hours.	N/A
Checkpoint saving	Checkpoints are updated if logs are reported successfully.	N/A
Checkpoint saving path	By default, checkpoints are saved in **/var/share/oss/manager/ICProbeAgent/internal/TRACE**.	N/A

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

Table 4-6 IP addresses accessible to ICAgent

Component/Service	IP Address	Description
OpenStack	http://169.254.169.254/openstack/latest/meta_data.json	Obtain the metadata, name, and ID of a node.

Component/Service	IP Address	Description
	http://169.254.169.254/openstack/latest/securitykey	Obtain a temporary AK/SK and security token with an agency.
	http://169.254.169.254/latest/meta-data/public-ipv4	Obtain the EIP bound to a node.
CCE	http://127.0.0.1:4194/api/v2.0/ps	Obtain process information with the cAdvisor API.
	http://127.0.0.1:4194/api/v1.2/docker	Obtain all container metrics with the cAdvisor API.
	http://nodeip:10255/pods	Obtain pod information with a Kubernetes API.

Table 4-7 Ports accessible to ICAgent

Port No.	Description
#icmgr-service {podlb}:30200	ICAgent registration
icmgr-controller {podlb}:30201	ICAgent status configuration
#als-access {podlb}:8102	Log reporting
#ams-access {podlb}:8149	Metric reporting
#ats-access apm {podlb}:8923	Data reporting to APM

4.4 Log Transfer

This section describes the restrictions on log transfer.

Table 4-8

Category	Item	Description	Remarks
Log transfer to OBS	Transfer tasks for a log stream	A log stream can have only one task for transferring logs to OBS.	N/A
	Log transfer interval	2 minutes, 5 minutes, 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours	N/A

Category	Item	Description	Remarks
	Data size of each log transfer task	0 MB to 2 GB	N/A
	Transfer rate threshold	100 MB/s The transfer may fail if this limit is exceeded.	N/A
	Log transfer delay	10 minutes For example, if the transfer interval is 30 minutes and the transfer starts at 8:30, transfer files will be generated at 8:40 at the latest.	N/A
	Target bucket	Standard buckets are supported. Parallel file systems are not supported.	N/A
Log transfer to DIS	Transfer tasks for a log stream	A log stream can have only one task for transferring logs to DIS.	N/A
	Log transfer interval	Real time	N/A
	Data size of each log transfer task	N/A	N/A
	Log transfer delay	N/A	N/A
	Transfer rate threshold	Same as the maximum write rate of the relevant DIS stream. The transferred data will be unstable if this limit is exceeded.	N/A
Log transfer to DMS	Transfer tasks for a log stream	A log stream can have only one task for transferring logs to DMS.	N/A
	Log transfer interval	Real time	N/A
	Data size of each log transfer task	N/A	N/A
	Log transfer delay	N/A	N/A

Category	Item	Description	Remarks
	Transfer rate threshold	Same as the upper traffic limit of the relevant DMS (Kafka) cluster. The transferred data will be unstable if this limit is exceeded.	N/A
Log transfer to GaussDB(DWS)	Transfer tasks for a log stream	A log stream can have only one task for transferring logs to GaussDB(DWS).	N/A
	Log transfer interval	1 minute	N/A
	Data size of each log transfer task	< 5 MB	N/A
	Log transfer delay	5 minutes For example, if the transfer starts at 8:30, transfer files will be generated at 8:35 at the latest.	N/A
	Transfer rate threshold	40 MB/s The transferred data will be unstable if this limit is exceeded.	N/A
	Data reliability	If the format of a batch of data is valid, the data is transferred at least once. However, if the GaussDB(DWS) cluster is heavily loaded or a network error occurs, the write response will time out, which may cause duplicate data. In this case, data accuracy (Exactly Once) cannot be ensured.	N/A

Category	Item	Description	Remarks
	Table structure change	• Adding non-mandatory columns to DWS tables does not affect log transfer. • Adding mandatory columns to DWS tables during log delivery will cause a data write failure. • Deleting columns that contain transfer rules from DWS tables during log delivery will cause a data write failure.	N/A
	Invalid data columns	The common scenarios include mismatch and type conversion failure. This batch of data will not be written to GaussDB(DWS), while other batches will be written normally.	N/A
	Oversized data columns	The common scenarios include long string and varchar type data. This batch of data will not be written to GaussDB(DWS), while other batches will be written normally.	N/A

4.5 Operating Systems

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

Table 4-9 Supported OSs and versions (Linux)

OS	Version			
SUSE	SUSE Enterprise 11 SP4 64-bit	SUSE Enterprise 12 SP1 64-bit	SUSE Enterprise 12 SP2 64-bit	SUSE Enterprise 12 SP3 64-bit
openSUSE	13.2 64-bit	42.2 64-bit	15.0 64-bit (Currently, syslog logs cannot be collected.)	
EulerOS	2.2 64-bit	2.3 64-bit		

OS	Version					
CentOS	6.3 64-bit	6.5 64-bit	6.8 64-bit	6.9 64-bit	6.10 64-bit	
	7.1 64-bit	7.2 64-bit	7.3 64-bit	7.4 64-bit	7.5 64-bit	7.6 64-bit
	7.7 64-bit	7.8 64-bit	7.9 64-bit	8.0 64-bit	8.1 64-bit	8.2 64bit
Ubuntu	14.04 server 64-bit	16.04 server 64-bit	18.04 server 64-bit			
Fedora	24 64-bit	25 64-bit	29 64-bit			
Debian	7.5.0 32-bit	7.5.0 64-bit	8.2.0 64-bit	8.8.0 64-bit	9.0.0 64-bit	

NOTE

- For Linux x86_64 hosts, LTS supports all the OSs and versions listed in the preceding table.
- For Linux Arm hosts, LTS supports all the OSs and versions listed in the preceding table except the CentOS of 7.3 and earlier versions.

Table 4-10 Supported OSs and versions (Windows)

OS	Version
Windows (64-bit)	Windows Server 2019
	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

5 Privacy and Sensitive Information Protection Statement

O&M data will be displayed on the LTS console. It is recommended that you do not upload your personal or sensitive data to LTS. Encrypt such data if you need to upload it.

ICAgent Deployment

When you install ICAgent on an ECS, your AK/SK pair is required in the installation command. Before the installation, disable history collection in the ECS to protect your AK/SK pair. After the installation, ICAgent will encrypt your AK/SK pair and store it.

6 Basic Concepts

Log Groups

A log group is a collection of log streams and the basic unit for LTS to manage logs. You can set log retention duration for a log group.

Log groups can be created in two ways:

- You can create log groups manually on the LTS console.
- When other HUAWEI CLOUD services are connected with LTS, log groups and log streams are automatically created to retain the logs collected from the services.

Log Streams

A log stream is the basic unit for log reads and writes.

You can sort logs of different types, such as operation logs and access logs, into different log streams. ICAgent will package and send the collected logs to LTS on a log stream basis. It makes it easier to find specific logs when you need them.

The use of log streams greatly reduces the number of log reads and writes and improves efficiency.

ICAgent

ICAgent is the log collection tool of LTS. If you want to use LTS to collect logs from a host, you need to install ICAgent on the host. Batch ICAgent installation is supported if you want to collect logs from multiple hosts. After ICAgent installation, you can check the ICAgent status on the LTS console in real time.

7 Permissions Management

Description

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

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

If your account does not need individual IAM users for permissions management, you may skip over this section.

IAM can be used for free. You pay only for the resources in your account. For more information about IAM, see .

LTS Permissions

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

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

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

The system permissions supported by LTS are listed in Table 7-1.

Table 7-1 LTS system permissions

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

Table 7-2 lists the common operations supported by each system-defined policy and role of LTS. Choose the appropriate policies and roles according to this table.

Table 7-2 Common operations supported by each LTS system policy or role

Operation	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
Querying a log group	√	√	√
Creating a log group	√	×	√
Modifying a log group	√	×	√
Deleting a log group	√	×	√
Querying a log stream	√	√	√
Creating a log stream	√	×	√
Modifying a log stream	√	×	√
Deleting a log stream	√	×	√

Operation	LTS FullAccess	LTS ReadOnlyAccess	LTS Administrator
Configuring log collection from hosts	√	×	√
Querying a filter	√	√	√
Disabling a filter	√	×	√
Enabling a filter	√	×	√
Deleting a filter	√	×	√
Querying an alarm rule	√	√	√
Creating an alarm rule	√	×	√
Modifying an alarm rule	√	×	√
Deleting an alarm rule	√	×	√
Viewing a log transfer task	√	√	√
Creating a log transfer task	√	×	√
Modifying a log transfer task	√	×	√
Deleting a log transfer task	√	×	√
Enabling a log transfer task	√	×	√
Disabling a log transfer task	√	×	√
Installing ICAgent	√	×	√
Upgrading ICAgent	√	×	√
Uninstalling ICAgent	√	×	√

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

Table 7-3 describes fine-grained permission dependencies of LTS.

Table 7-3 Fine-grained permission dependencies of LTS

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

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

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

8 Related Services

The relationships between LTS and other services are described in **Table 1**.

Table 8-1 Relationships with other services

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

9 Billing

9.1 Overview

This section describes the billing mode, billing items, and billing period of LTS.

NOTE

For pricing details, go to **Price Calculator**.

Mode

Cloud service logs are billed in the pay-per-use mode. Fees are settled based on the actual usage of each billing item. You can use the service first and pay for it. A certain free quota is provided monthly.

NOTE

The free quota is provided based on the Huawei account level and can be shared by all LTS log groups under the account.

Billing Items

For details, see **Price Calculator**.

Table 9-1 Billing items

Category	Item	Description	Mode	Free Quota
Traffic	Log read and write traffic	Includes write traffic and read traffic. • **Write traffic**: When the compressed data is uploaded to LTS, the write traffic is billed based on the amount of transmitted data. For example, if 5 GB data is uploaded to LTS, 1 GB write traffic (compression rate: 20%) will be generated. • **Read traffic**: Read traffic is not counted and is free of charge.	Pay-per-use: Read and write traffic fee = Write traffic (GB, 20% compression rate) x Unit price per GB	500 MB/month

Category	Item	Description	Mode	Free Quota
	Log index traffic	Details are as follows: • By default, full-text indices are created for raw logs. The index traffic is billed based on the index data volume generated by uncompressed logs. • Index traffic is billed at a time when data is written, i.e., full-text index traffic. • For a field for which both a full-text index and a field index are constructed, index traffic is billed only once, i.e., full-text index traffic. • When the full-text index is disabled and only the field index is enabled, fields of long and float types are not counted in the index traffic. The index traffic occupied by each field value is 8 bytes. If the type is string, the log field name (Key) and field value (Value) are stored as the text type, and the field name and value are included in the index traffic. Field indexes can be used to reduce index traffic fees. **Example:** 1. If an index (string type) is set for the **request_uri** field and the field value is **/request/path**, both **request_uri** and **/request/path** are counted in the index traffic. 2. If an index (long type) is set for the **status** field and the field value is 400, **status** is not counted in the index traffic. The index traffic of 400 is 8 bytes. **NOTE** This function is now under internal testing by some users. It will be available soon for all users.	Pay-per-use: Log index fee = Index traffic (GB) x Unit price per GB	500 MB/month

Category	Item	Description	Mode	Free Quota
		Example: • If 10 GB raw logs are written and the full-text index is enabled, the 10 GB index traffic is billed. • For example, if 10 GB raw logs are written and the index for two fields is enabled, the data volume is 5 GB, and the 5 GB index traffic is billed. • If 10 GB raw logs are written and the index for two fields is enabled, the 10 GB index traffic is billed.		
Storage	Log volume	Log volume generated when raw logs (backup and compressed logs) and logs are indexed (uncompressed logs). **Example:** If 10 GB raw logs are uploaded and the full-text index is enabled, the log volume of raw logs (backup and compressed logs) and indexed logs is 10 GB.	Pay-per-use: Log volume fee = Log volume (GB) x Unit price per GB	500 MB/month

Billing Period

LTS reports service detail records (SDR) **every hour**, collects statistics on the usage of all LTS resources **by hour**, and calculates fees based on your usage.

9.2 Billing Cases

This section describes LTS billing cases.

NOTE

If the billing amount is not a whole number, round the number to the nearest two decimal places. For example, if the estimated price is less than $0.01 USD after rounding off, $0.01 USD will be displayed.

Case 1: Free of Charge

Assume that you have a server generating 10 MB raw logs every day, full-text index is enabled, and logs are retained for seven days (the earliest logs are deleted first).

You want to analyze daily logs using LTS for one month. Billing details are shown in the following table.

Table 9-2 Billing details (free of charge)

Item	Description	Monthly Usage	Monthly Billing
Read/ Write traffic	Daily read/write traffic: 10/5 (compression rate) = 2 MB. Accumulated read and write traffic for 30 days: 30 x 2 = 60 MB.	60 MB	Free
Index traffic	Accumulated index traffic for 30 days: 10 x 30 = 300 MB	300 MB	Free
Storag e	Log volume = 7 x 10 MB	70 MB	Free

Case 2: Full-Text Index

Assume that you have a server generating 100 GB raw logs every day, full-text index is enabled, and logs are retained for 30 days (the earliest logs are deleted first).

You want to analyze daily logs using LTS for one month. Billing details are shown in the following table.

Table 9-3 Billing details (full-text index)

Item	Description	Monthly Usage	Unit Price	Monthly Billing
Read/ Write traffic	Daily read and write traffic: 100 GB/5 (compression rate) = 20 GB. Accumulated read and write traffic for 30 days: 20 GB x 30 = 600 GB.	600 GB	$0.05 USD/GB	(600 GB – 500 MB/ 1024) x 0.05 = $29.98 USD
Index traffic	100 GB x 30 = 3000 GB	3000 GB	$0.08 USD/GB	(3000 GB – 500 MB free quota/1024) x 0.08 = $239.96 USD
Storage	Log volume = 100 GB/day x 30 days = 3000 GB	3000 GB	$0.000 125 USD/GB-hour	(3000 GB – 500 MB free quota/1024) x 0.00125 x 24 hours x 30 days = $269.96 USD

Case 3: Disabling the Full-Text Index and Enabling the Index Field

Assume that you have a server generating 100 GB raw logs every day, full-text index is disabled, logs are written to the log service, and the index for five fields is enabled. The data volume is 50 GB.

Logs are retained for 30 days (the earliest logs are deleted first).

You want to analyze daily logs using LTS for one month. Billing details are shown in the following table.

Table 9-4 Billing details (disabling the full-text index and enabling the index field)

Item	Description	Monthly Usage	Unit Price	Monthly Billing
Read/ Write traffic	Daily read and write traffic: 100 GB/5 (compression rate) = 20 GB. Accumulated read and write traffic for 30 days: 20 GB x 30 = 600 GB.	600 GB	$0.05 USD/GB	(600 GB – 500 MB/ 1024) x 0.05 = $29.98 USD
Index traffic	50 GB x 30 = 1500 GB	1500 GB	$0.08 USD/GB	(1500 GB – 500 MB free quota/1024) x 0.08 = $119.96 USD
Storage	Log volume = 100 GB/day x 30 days = 3000 GB	3000 GB	$0.000 125 USD/GB-hour	(3000 GB – 500 MB free quota/1024) x 0.00125 x 24 hours x 30 days = $269.96 USD

9.3 Bill Query

This section describes how to query bills.

Step 1 Log in to the management console.

Step 2 Choose **Billing & Costs** > **Bills** to go to the billing center.

Step 3 In the navigation pane, choose **Billing** > **Transaction and Detailed Bills**.

Step 4 On the **Bill Details** page, set **Billing Cycle** and set **Product Type** to **LTS** to view transactions and detailed bills.

----End

10 Glossary

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

Table 10-1 Terms

Abbreviation	Full Spelling	Definition
LTS	Log Tank Service	LTS collects, analyzes, and stores logs. You can use LTS for efficient device O&M, service trend analysis, security audits, and monitoring.
-	Log group	A log group is a group of log streams and is the basic unit for log management in LTS. You need to create a log group before collecting, querying, and transferring logs.
-	Log stream	A log stream is the basic unit for log reads and writes. If there are many logs to collect, you are advised to separate logs into different log streams based on log types, and name log streams in an easily identifiable way.
-	ICAgent	ICAgent is the log collection tool of LTS. If you want to use LTS to collect logs from a host, you need to install ICAgent on the host. Batch agent installation is supported if you want to collect logs from multiple hosts. After agent installation, you can check the ICAgent status on the LTS console in real time.

