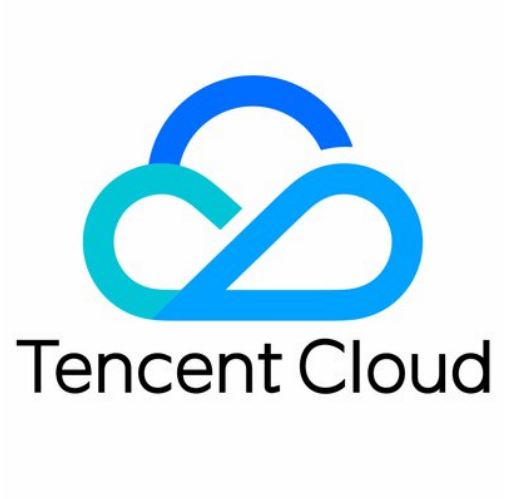
Cloud Log Service

FAQs

Product Documentation



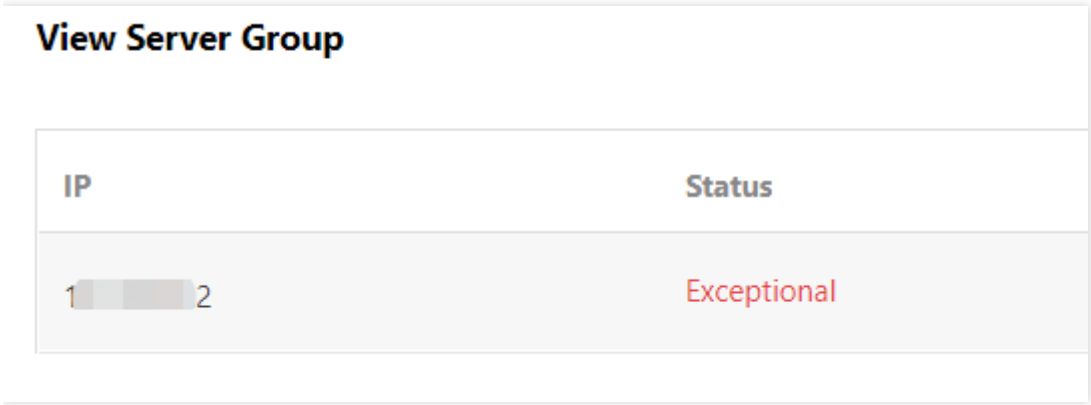
Contents

FAQs
LogListener
Server Group Exception

Last updated : 2020-11-02 15:34:01

Error Description

When the server group is configured, LogListener may have an exception, such as disconnection from the CLS server and log upload failure. In this case, the server group is exceptional, as shown below:



Troubleshooting

Note :

These troubleshooting steps only apply to LogListener 2.2.4 or later. If you're using an earlier version, see Troubleshooting Earlier LogListener Versions.

1. Use the LogListener diagnostic tool

This tool helps you quickly check the LogListener operation, heartbeat and configuration.
Run the following CLI commands.

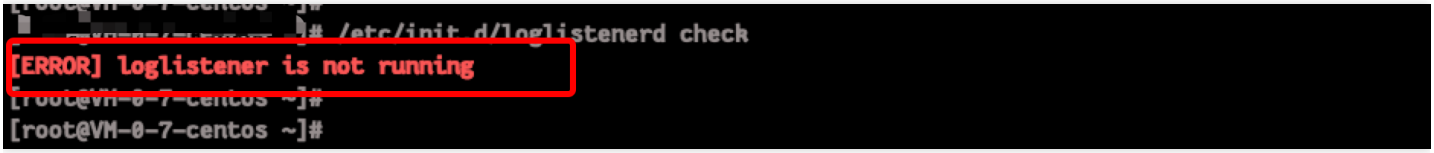
```
/etc/init.d/loglistenerd check
```

The following output indicates that LogListener is running properly.

```
[root@VM_30_69_centos etc]# sudo /etc/init.d/loglistenerd check
[OK] loglistener is running ok
[OK] check loglistener hearbeat ok
group ip:
host:ap-chengdu.cls.myqcloud.com
port:80
gethostbyname ip:
[OK] check loglistener config ok
{"logconf":[],"needupdate":false}
```

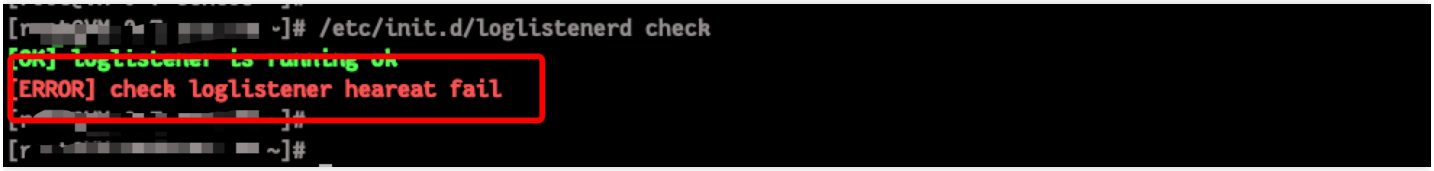
LogListener process exception

If the result returns “[ERROR] loglistener is not running” as shown in the following figure, it indicates that LogListener is not started. Run the `/etc/init.d/loglistenerd start` command to start it. For more information about the operation commands, see Using LogListener.



LogListener heartbeat exception

If the result returns “[ERROR] check loglistener heareat fail” as shown in the following figure, it indicates that LogListener has a heartbeat exception.



Many causes can lead to LogListener heartbeat exception. Possible causes include:

- Network error

  ```
  telnet <cls domain name> 80
  ```

  Check the network connectivity. For more information about the CLS domain name, see Available Regions.

- Incorrect key

  To check the LogListener key, access the LogListener installation directory and run the following command.

```
grep secret etc/loglistener.conf
```

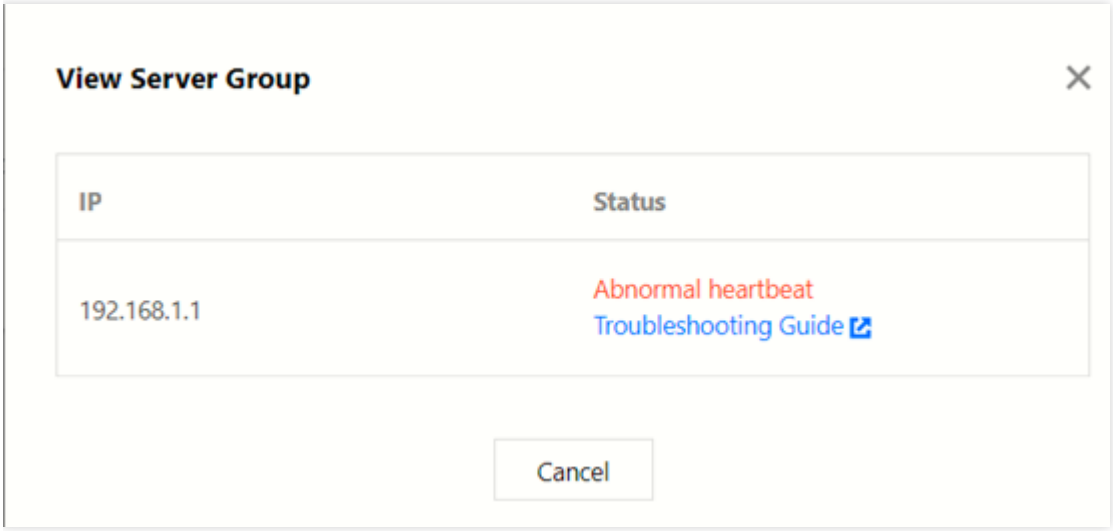
2. Check for IP address of the server group

Check that the IP address added to the server group is the one configured on LogListener during installation. Run the following command to check the IP address configured on LogListener.

```
grep group_ip etc/loglistener.conf
```

Log in to the CLS Console, and select **Server Group** on the left sidebar. On the **Server Group Management** page, view and verify that the IP address of the server group is the same as that

configured on LogListener.



LogListener FAQs

Last updated : 2021-05-26 11:45:06

How do I pin the LogListener process to a CPU?

For the CPU pinning, use the taskset tool and run the `taskset -cp ${cpu number} ${pid>}` command.

How do I control the high memory and resource usage of LogListener?

- We recommend that you upgrade LogListener to the latest version and set `memory_tight_mode = true` .
- Use CGroup to control CPU and MEM usage.

Does LogListener support log collection via a soft link?

Yes. But LogListener earlier than version 2.3.0 does not collect those log files in soft links, or in shared file directories of NFS, CIFS, etc.

Can LogListener upload data to multiple log topics?

- Yes, provided that these log topics are in the same region.
- A log file will only be collected into one log topic.

Are servers automatically added to a server group when LogListener is initialized?

Yes, provided that you Server Group Management.

In what situations will LogListener upload logs?

- More than 4 MB logs are cached.
- More than 10,000 logs are cached.
- LogListener finishes reading a file.

What does the maximum performance of LogListener mean?

- Collecting logs with full text in a single line: 115 MB/sec.
- Collecting logs with full text in multi lines: 40 MB/sec.
- Collecting JSON logs: 25 MB/sec.
- Collecting CSV logs: 50 MB/sec.
- Collecting full RegEx logs: 18 Mb/sec, depending on the regex complexity.

How do I modify the LogListener configuration after the server IP address is changed?

- If you configure the server group by server ID, you don’t need to modify the LogListener configuration. This method is recommended when the server IP frequently changes. For more information, see Configuring the server group by server ID.

- If you configure the server group by server IP address, modify the configuration as follows:
  a. Add the new IP address to the `group_ip` field in the configuration file.

```
sed -i '' "s/group_ip *=.*/group_ip = ${group_ip}/" etc/loglistener.conf
```

  b. Restart LogListener.

```
/etc/init.d/loglistenerd restart
```

  c. Log in to the CLS Console and select **Server Group** on the left sidebar. Locate the server group on which you want to change the server IP, and click **Modify**. In the pop-up window, enter the new IP address, and click **OK**.

LogListener Installation Exception

Last updated : 2020-09-17 11:45:36

For details about how to install and use LogListener, see LogListener Installation Guide

Possible causes

Loglistener may not be installed correctly for the following reasons:

1. The kernel version only supports 64-bit.
2. The installation method is incorrect.
3. The latest features rely on a later version of LogListener.

Directions

1. Check the kernel version.
   The executable file in the bin directory under the LogListener installation directory only supports Linux 64-bit kernel. Execute the command **uname -a** to check whether the kernel version is x86_64.
2. Check the installation command.
   Be sure to perform operations according to the LogListener Installation Guide.
3. Check the LogListener version.
   Some of new CLS features may be available only for the latest version of Loglistener. In this case, please download and install the latest version. For step-by-step directions, see LogListener Installation Guide.
4. Verify the LogListener installation.
   Check for process and heartbeat of LogListener and check whether it can properly obtain collection configuration of users. To do this, please see LogListener Diagnostic Tool.

Log Search
Log Search Failure

Last updated : 2020-11-02 15:33:35

The log search may fail sometimes. In case of a search failure, use the following methods for troubleshooting.

Checking Search Criteria

A log search failure is often caused by an incorrect time range or search statement. To address this issue, first select a larger time range (such as `last 30 minutes`), leave the search bar empty, and search for logs.

If logs are found, it indicates that the log search is available. We recommend that you check the search syntax and rules or modify the time range.

Checking Index Configuration

The index configuration is required for CLS log search. In the top right of the **Search Analysis** page, click **Index Configuration** to enable both full-text index and key-value index. For more information, see Enabling Index.

> ⚠ **Note :**
>
> The index configuration takes effect in about 1 minute. The new configuration is only effective for log data written subsequently.

Checking Log Collection

Log collection from Tencent Cloud services

To collect logs from other Tencent Cloud services including TKE and CLB, see Collection for Tencent Cloud Services to verify the configuration. If you have any question, please submit a ticket.

Log collection by LogListener client

If you're using CLS's LogListener client to collect logs, perform the following steps for troubleshooting:

1. Check the server group.
   In the top right of the **Search Analysis** page, click **LogListener Collection Configuration** to check the server group from which you want to collect logs.

> ⚠ **Note :**
>
> If the server is exceptional, see Server Group Exception.
> 2. Check if LogListener obtains the collection configuration from the CLS server.
> Run the following CLI commands:

```
/etc/init.d/loglistenerd check
```

```
If the result returns "[OK] check loglistener config ok" as shown in the following figure, it indicates that the API is successfully called to obtain the configuration from the CLS server.
![](https://main.qcloudimg.com/raw/95022fc7832b36e2e8d51b6fe8ed3ab7.jpg)
The `logconf` field in the result refers to the collection configuration. If this field is empty, it indicates that no collection configuration is obtained. See [LogListener Use Process](https://intl.cloud.tencent.com/document/product/614/31578) to create a server group and bind the collection configuration via the console.
```

3. Use the latest version of LogListener.
   Run the following command to check the version number. See LogListener Installation Guide to install the latest version of LogListener.

```
/etc/init.d/loglistenerd -v
```

> ⚠ **Note :**
>
> LogListener earlier than 2.3.0 cannot collect log files in soft links.

4. Check that logs are successfully reported.
   Open the LogListener Debug log and access the LogListener installation directory. Set **level** to `DEBUG` in the `etc/loglistener.conf` configuration file and restart LogListener.

```
<log>
    level   = DEBUG
    path    = log/
    name    = loglistener
    size    = 10000000
    num     = 10
</log>
```

Run the following command to restart LogListener.

```
/etc/init.d/loglistenerd restart
```

Run the following commands to check if logs are successfully reported.

```
tail -f log/loglistener.log | grep "ClsFileProc::readFile" | grep send
```

If log information similar to that shown in the following figure is displayed, logs are successfully reported to the CLS server.

```
$ tail -f loglistener.log | grep "ClsFileProc::readFile" | grep send
2018-06-21 10:14:48|27338|INFO||cls_file_proc.cpp:391|ClsFileProc::readFile send topicid:69a0207f-f3ec-4beb-a50f-9572546c1e8c,
2018-06-21 10:14:48|27338|INFO||cls_file_proc.cpp:431|ClsFileProc::readFile send topicid:69a0207f-f3ec-4beb-a50f-9572546c1e8c,
2018-06-21 10:14:49|27338|INFO||cls_file_proc.cpp:391|ClsFileProc::readFile send topicid:69a0207f-f3ec-4beb-a50f-9572546c1e8c,
2018-06-21 10:14:49|27338|INFO||cls_file_proc.cpp:391|ClsFileProc::readFile send topicid:69a0207f-f3ec-4beb-a50f-9572546c1e8c,
2018-06-21 10:14:49|27338|INFO||cls_file_proc.cpp:431|ClsFileProc::readFile send topicid:69a0207f-f3ec-4beb-a50f-9572546c1e8c,
2018-06-21 10:14:50|27338|INFO||cls_file_proc.cpp:391|ClsFileProc::readFile send topicid:69a0207f-f3ec-4beb-a50f-9572546c1e8c,
2018-06-21 10:14:50|27338|INFO||cls_file_proc.cpp:391|ClsFileProc::readFile send topicid:69a0207f-f3ec-4beb-a50f-9572546c1e8c,
```

⚠ Note :

If logs are reported through HTTP, you can capture packets from port 80 to verify whether logs are successfully reported.

If logs are not reported, perform the following steps for troubleshooting:
a. Run the following commands in the installation directory to check whether the LogListener collection configuration is correct.

```
tail -f log/loglistener.log | grep "ClsServerConf::load"
```

If the configuration has been delivered to LogListener, log information is as follows:

```
$ tail -f log/loglistener.log | grep "ClsServerConf::load"
2018-06-21 10:01:49|20706|DEBUG||cls_server_conf.cpp:24|ClsServerConf::load begin
"path":"/log","topicid":"56ed3e87-c895-49ba-a1cc-2f2c30e57a35"},{"extract_rule":{"
a0207f-f3ec-4beb-a50f-9572546c1e8c"}],"needupdate":false}
```

In the delivered configuration, check whether the information of `log_type` and `path` is correct:

- `log_type` indicates the log parsing type. Valid values: `minimalist_log` (full text in a single line), `delimiter_log` (separator), `json_log` (JSON logs), and `regex_log` (full text in multi lines).
- `path` indicates the log collection directory.

b. Run the following command in the installation directory to check whether files are correctly listened to:

```
grep [Name of the reported log file] log/loglistener.log
```

- If no log information is displayed, run the `grep regex_match log/loglistener.log` command to search for log information and check whether the regular expression is correctly configured in the console. If the content shown in the following figure is displayed, the file name match based on the regular expression fails. In this case, please log in to the console and change the regular expression.

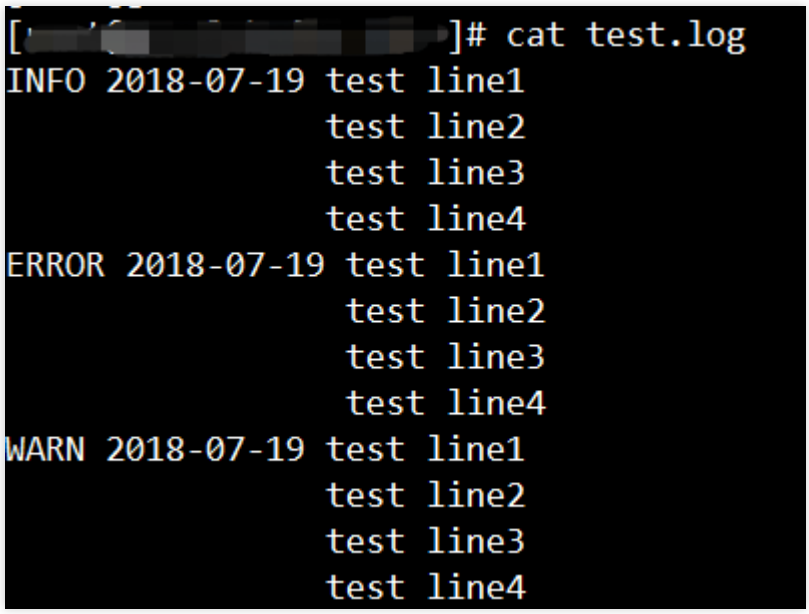
```
2018-07-06 17:04:08|8746|ERROR||cls_file_proc.cpp:137|ClsFileProc::readEvent regex_match error! name:live_info_20180706.log,reg:live_debug_.*\.log
2018-07-06 17:04:08|8746|INFO||cls_file_proc.cpp:120|ClsFileProc::readEvent new event! mask:2 ,wd:1 ,name:live_debug_20180706.log
2018-07-06 17:04:08|8746|INFO||Transceiver.cpp:230|TcpTransceiver doResponse, postfile,fd:11,recvbuf:194
```

c. Check whether the log regular expression parse is correct.

For the extraction modes of full regular expression and full text in multi lines, regular expressions need to be specified. For full text in multi lines, the first line regular expression must match the entire content of the first line, instead of the beginning part of the first line.

Use the log content shown in the following figure as an example. Lines beginning with `INFO`, `ERROR`, and `WARN` are the first lines of logs. In addition to `(INFO|ERROR|WARN)`, the characters

following `INFO` , `ERROR` , and `WARN` also need to be matched.



- Incorrect configuration: `^(INFO|ERROR|WARN)`
- Correct configuration: `^(INFO|ERROR|WARN).*`

5. A file can only be collected to one log topic and a single log line cannot exceed 1 MB.
   Meet these requirements to ensure the complete log collection.

Search Page

Last updated : 2021-08-31 16:24:03

When users use the search page to analyze the logs, the search results may be empty or error messages may appear, such as `QueryError` , `SyntaxError` . The common problems and scenarios are summarized as below:

- The page displays that the search result is empty
- Error messages appear for the search syntax

The page displays that the search result is empty

- **Common reason 1:** the log was not collected successfully.
  Solution: for more information on troubleshooting, please see Log Search Failure.

- **Common reason 2**: no wildcard is used when logs that contain only a part of the keyword segment are searched for.
  Scenario: you wanted to search for logs whose `user-agent` field contained `Window` , such as `Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)` . After you entered the search statement `user-agent:Window` , the search result was empty. The reason is that `Window` is not a complete segment and cannot be searched separately.
  Solution: use wildcard `*` to search for `user-agent:Window*` .

- **Common reason 3:** an SQL statement is used to analyze log data, but spaces are not added before and after the pipe symbol.
  Scenario: the SQL statement you entered was `*|SELECT *` . As you didn't add spaces before and after the pipe symbol, CLS used the entire statement as a keyword for full-text search for log data containing " `*|SELECT *` ".
  Solution: Add a space before and after the pipe character, e.g. `*|SELECT *` .

Query statement with error message

Common error messages, causes and solutions are as follows:

.

Error Message	Cause	Solution

Error Message	Cause	Solution
QueryError [illegal_argument_exception.Cannot search on field [xxx] since it is not indexed	The index is not enabled for the queried field `xxx`	Enable the index for this field. For details, please see Configuring Index
QueryError [illegal_argument_exception.Cannot search on Full-Text since it is not indexed.]	Full-text index is not enabled	Enable the full-text index. For details, please see Full-Text Index
QueryError [illegal_argument_exception.syntax error on field [and|or|not], or full text search is closed]	The search condition does not support lowercase logical operators, which will be regarded as normal fields for full-text search	Use the upper-case logical operators `AND|OR|NOT`. If you do not need to use logical operators but to search for `and/or/not`, please enable full-text index.
QueryError [number_format_exception.For input string: "&dxgt;"]	Syntax error of numerical comparison statement	Check whether there are special symbols such as spaces around the numerical comparison symbols. An example of correct format: `status:>400`

Error Message	Cause	Solution
QueryError [parent_circuit_breaking_exception. [parent] Data too large, data for [] would be [xxx/xxxgb]	The query data volume is too large	Reduce the query time range as appropriate, and specify more precise query conditions
QueryError [parse_exception.parse_exception: Cannot parse 'xxx': '*' or '?' not allowed as first character in WildcardQuery	Fuzzy query by prefix is not allowed, e.g. content:*example `content:*example`	We recommend using separators to split a field into multiple ones. For details, please see Configuring Index
QueryError [sql_illegal_argument_exception.cannot cast [13/Jul/2021:17:04:34] to [datetime]: failed to parse date field [13/Jul/2021:17:04:34] with format [date_optional_time]]	`cast` cannot convert dates in `13/Jul/2021:17:04:34` format. Only ISO standard format and millisecond-level Unix timestamp are supported, e.g. `yyyy-MM-dd'T'HH:mm:ss.SSSZ` or `yyyy-MM-dd`.	Modify the format of the time field or use the `__TIMESTAMP__` built-in field
QueryError [verification_exception.Cannot order by non-grouped column [xxx], expected [xxx] or an aggregate function	Statistics is not enabled for the field `xxx` and thus it cannot be used for sorting	Enable statistics for this field. For details, please see Log Analysis Overview
QueryError [verification_exception.Cannot use non-grouped column [xxx], expected [xxx]]	Statistics is not enabled for the query field `xxx`	Enable statistics for this field. For details, please see Log Analysis Overview

Error Message	Cause	Solution
QueryError [verification_exception.Field [xxx] of data type [text] cannot be used for grouping]	Statistics is not enabled for the field `xxx` and thus it cannot be used for grouping	Enable statistics for this field. For details, please see Log Analysis Overview
QueryError [verification_exception.Unknown column [xxx]]	The query field `xxx` does not exist	Check whether the field name is correct
SyntaxError[xxx]	There is a syntax error in part of the SQL statement	Please see the detailed tips in the error message to fix the syntax error, where `line x,column x` does not contain the search condition part (i.e. "|" and the part before it)
SearchTimeout	The query is timed out	Reduce the scope of data query and SQL complexity as appropriate, or try again later.
LimitExceeded.LogSearch	The search concurrency exceeds the limit	Try again later

FAQs

Last updated：2021-05-18 14:39:37

What is Cloud Log Service?

Cloud Log Service (CLS) is Tencent Cloud's one-stop log data service platform with the following features:

- Log collection: supports multiple access methods like LogListener, API, etc.
- Log storage: stores and manages log data centrally
- Search analysis: provides log query and filtering features
- Shipping and consumption: provides the log shipping/consumption features for further log data processing
- CLS integrates seamlessly with Tencent Cloud services.

How does CLS define a log?

A complete CLS log contains mainly the log timestamp, the log content and the metadata:

- Log timestamp: the basic time attribute of logs
- Log content: contents in the format of key-value pairs
- Metadata: basic metadata such as the log source IP address, log source file path, etc.

How long can logs be kept?

CLS provides log lifecycle management. When you create a logset, you may configure a storage cycle, beyond which the data will be cleared without incurring storage fees. If you need to extend the storage cycle, submit a ticket.

After you ship logs to Cloud Object Storage (COS), the lifecycle management of the destination bucket, and the COS billing rules will be used.

> 注意：
> It may take a period of time for CLS to clear expired data, during which no charges will apply.

What are the differences between logset and log topic?

CLS provides two levels of conceptual logic: logset and log topic. A logset contains multiple log topics, similar to a project containing multiple application services. Generally, each service has different log formats. Therefore, a log topic is the smallest unit of configuration management such as collection and search.

What are the differences between full-text index and key-value index?

- Full-text index: breaks a full log into segments by delimiter, and executes keyword query based on the segments.
- Key-value index: breaks a full log into key-value pairs according to the specifications, and executes field query based on the key-value pairs.

Is CLS available for services not on Tencent Cloud?

Yes. CLS does not restrict log sources. Logs are collected to CLS provided that the log source is reachable to our server over the network.

How do I modify the Loglistener configuration after the server IP address is changed?

- If the server is bound to the server group by server ID, there is no need to modify the Loglistener configuration. This method is recommended when the server IP frequently changes. For more information, see Machine Group Management.
- If the server is bound to the server group by server IP, modify the configuration as follows:
  i. Modify the /etc/loglistener.conf file in the Loglistener installation directory (/user/local in this example).
  vi /usr/local/loglistener-2.3.0/etc/loglistener.conf
  ii. Press **i** to enter the edit mode.
  iii. Enter the new IP address in the group_ip section of the configuration file.
  iv. Press **Esc**, enter **:wq**, and press **Enter** to save and exit the editor.
  v. Run the following command to restart Loglistener.
  /etc/init.d/loglistenerd restart
  vi. Log in to the CLS Console and click **Server Group Management** on the left sidebar. Locate the server group to which the server binds and click **Modify** to enter the **Modify Server Group** page. Replace the old IP address with the new one, and click **OK**.