

Cloud Log Service

Appendix

Product Documentation



Copyright Notice

©2013-2019 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Appendix

Historical Documentation

Operation guide of earlier LogListener versions

Troubleshooting earlier LogListener versions

Legacy CLS Search Syntax

Appendix

Historical Documentation

Operation guide of earlier LogListener versions

Last updated : 2020-06-30 15:49:53

This document provides an operation guide for LogListener 2.2.4 and earlier. We recommend that you update to the latest version as this document may no longer be maintained. For information on how to install the latest version, see the [LogListener Installation Guide](#).

Starting LogListener

Go to the installation directory `loglistener` and start LogListener by running the following script:

```
cd loglistener/tools; ./start.sh
```

Stopping LogListener

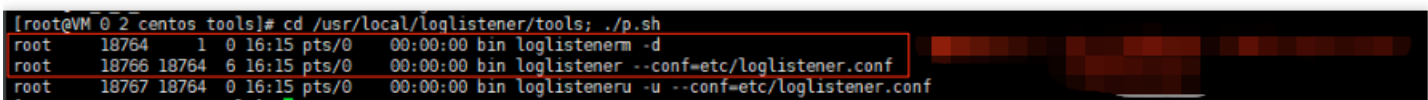
Go to the installation directory `loglistener` and stop LogListener by running the following script:

```
cd loglistener/tools; ./stop.sh
```

Checking LogListener process status

Go to the installation directory `loglistener` and check the status of the LogListener processes by running the following command:

```
cd loglistener/tools; ./p.sh
```



```
[root@VM 0 2 centos tools]# cd /usr/local/loglistener/tools; ./p.sh
root  18764  1  0 16:15 pts/0    00:00:00 bin loglistenerm -d
root  18766 18764 6 16:15 pts/0    00:00:00 bin loglistener -c /etc/loglistener.conf
root  18767 18764 0 16:15 pts/0    00:00:00 bin loglisteneru -u -c /etc/loglistener.conf
```

Normally, there are three processes:

```
bin/loglistenerm -d #Daemon process
bin/loglistener --conf=etc/loglistener.conf #Main process
bin/loglisteneru -u --conf=etc/loglistener.conf #Update process
```

Uninstalling LogListener

Go to the installation directory `loglistener` and uninstall LogListener by running the following command:

```
cd loglistener/tools; ./uninstall.sh
```

Checking LogListener heartbeat and configuration

Go to the installation directory `loglistener` and check the heartbeat and configuration of LogListener by running the following command:

```
cd loglistener/tools; ./check.sh
```

Troubleshooting earlier LogListener versions

Last updated : 2020-04-13 16:44:54

This document provides troubleshooting information for LogListener 2.2.4 and earlier. For information on troubleshooting the latest version, see [Server Group Exceptions](#).

Error Description

An exception occurred with log collection, and the associated server group is found to be exceptional.

Possible Causes

The heartbeat between the server group and the CLS system is interrupted, resulting in failure to collect and report logs. Possible causes for the server group exception include:

1. The IP address is incorrect.
2. The network is disconnected.
3. LogListener process failure.
4. LogListener is configured incorrectly.

Solution

Troubleshoot problems according to the above causes.

Directions

1. Check whether the IP address added to the server group is correct.
 - i. Check the IP address obtained by LogListener by running the following command:

```
cd loglistener/tools && ./check.sh
```

```
[root@VM 30 69 centos tools]# ./check.sh
group ip:10.163.30.69
host:ap-chengdu.cls.myqcloud.com
port:80
```

- ii. Log in to the [Cloud Log Service Console](#), and click **Server Group** in the leftside bar. On the Server Group Management page, check the IP address of the server group. The IP address must be the same as that for collection.

2. Check whether the network is connected by running the following command:

```
telnet <region>.cls.myqcloud.com 80
```

<region> is the abbreviation for the region where CLS resides. For more information on regions, see [Available Regions](#).

The following code appears upon normal network connection. Otherwise, connection fails. Check the network and ensure normal connection.

```
[root@VM 30 69 centos tools]# telnet ap-shanghai.cls.myqcloud.com 80
Trying 10.163.30.69...
Connected to ap-shanghai.cls.myqcloud.com.
Escape character is '^]'.
```

3. Check whether LogListener processes are running normally. Go to the installation directory and run the following command:

```
cd loglistener/tools && ./p.sh
```

Normally, there are three processes:

```
bin/loglistenerm -d #Daemon process
bin/loglistener --conf=etc/loglistener.conf #Main process
bin/loglisteneru -u --conf=etc/loglistener.conf #Update process
```

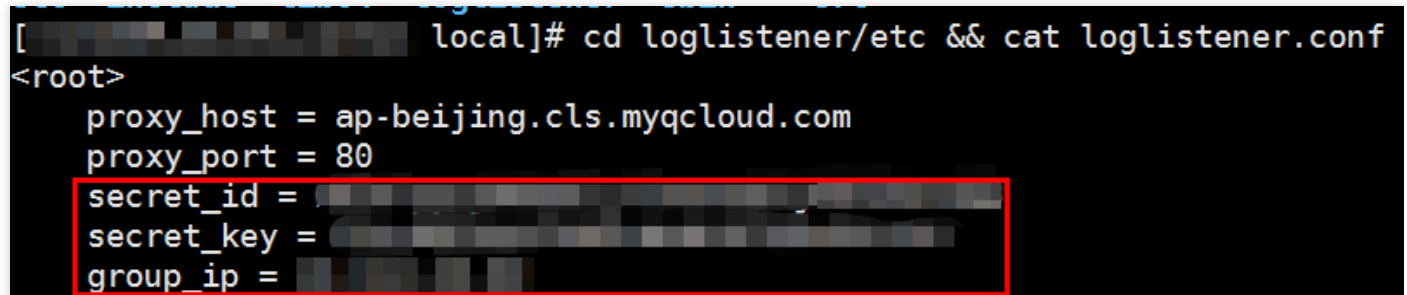
If any process fails, restart it. Go to the installation directory and run the following command:

```
cd loglistener/tools && ./start.sh
```

4. Check whether the key and IP address are correctly configured in LogListener. Go to the installation directory to check the configuration information by running the following command:

```
cd loglistener/etc && cat loglistener.conf
```

See the following figure:



```
[root@localhost ~]# cd loglistener/etc && cat loglistener.conf
<root>
  proxy_host = ap-beijing.cls.myqcloud.com
  proxy_port = 80
  secret_id = [REDACTED]
  secret_key = [REDACTED]
  group_ip = [REDACTED]
```

- The key is the API key for the Tencent Cloud account or the collaborator. Project keys are not supported.
- group_ip in the configuration file must be consistent with the IP address entered in the server group on the console. Since LogListener obtains the server IP address automatically, check the consistency regularly when the server is bound to multiple ENIs.

Legacy CLS Search Syntax

Last updated : 2020-09-01 14:52:02

CLS provides a variety of search features. You can search for logs in real time by search syntax and rules, and get results within seconds. CLS gives you insights into your business operations.

Starting Search

Log search is an important CLS feature. You can define the search criteria for billions of log data and obtain results within seconds. Specific steps are as follows:

1. Log in to the [CLS Console](#).
2. Click **Log Search** in the left sidebar to enter the **Search Analysis** page.
3. Select the time range, logset, and log topic.
4. Enter the keyword, and click **Search Analysis** to obtain the query result.

Search Syntax

The following query statements are supported:

| Syntax | Semantics |
|-----------|--|
| key:value | The "key-value" search format. You need to enable the key-value index . The <code>value</code> supports fuzzy search by <code>?</code> or <code>*</code> |
| A and B | The "AND" logic that returns the intersection of A and B. If several keywords are separated by spaces, the "AND" logic is used by default |
| A or B | The "OR" logic that returns the union of A or B |
| not B | The "NOT" logic that returns the results excluding B |
| A not B | The "MINUS" logic that returns the results including A but excluding B, i.e., <code>A - B</code> |
| 'a' | The character <code>a</code> will be considered as a regular character and will not be processed as a syntax keyword |
| "A" | All characters in <code>A</code> will be considered as regular characters and will not be processed as syntax keywords |
| | |

| | |
|---------------------------|---|
| \ | Escape character. An escaped character represents the literal meaning of the character, such as <code>¥</code> for quotation mark or <code>¥:</code> for colon |
| * | Fuzzy query of keywords that can match zero, single, or multiple random characters. But the search cannot start with <code>*</code> . For example, enter <code>abc*</code> to search for all logs beginning with <code>abc</code> |
| ? | Fuzzy query of keywords that can match a single character at a specific position. For example, enter <code>ab?c</code> to search for logs that begin with <code>ab</code> , end with <code>c</code> , and contain only one character between <code>ab</code> and <code>c</code> |
| > | "GREATER THAN" logic, which is used for numeric fields |
| >= | "GREATER THAN OR EQUAL TO" logic, which is used for numeric fields |
| < | "LESS THAN" logic, which is used for numeric fields |
| <= | "LESS THAN OR EQUAL TO" logic, which is used for numeric fields |
| = | "EQUAL TO" logic, which can be used for numeric or text fields (Fuzzy search is not supported. If you need fuzzy search, please see the key-value search <code>key:value</code>) |
| <code>__SOURCE__</code> | The operator that specifies the IP address of a source whose logs you want to query, and wildcard is supported, such as <code>__SOURCE__:127.0.0.*</code> |
| <code>__FILENAME__</code> | The operator that specifies the file path from which you want to query logs, and wildcard is supported, such as <code>__FILENAME__: /var/log/access.*</code> |

Note :

- Before using the range search, set the numeric fields to a double or long type; otherwise, you may have unexpected results.
- If **b** is text, the difference between `a=b` and `a:b` lies in that **a** equals **b** in the former, while **a** contains **b** in the latter (the search is processed based on the segment logic and fuzzy search is supported).

Search Rules

Time range, logset, and log topic are required for log search. The default time range is the current day, while the logset and log topic are at your discretion. You can search for all logs without entering anything in the search box.

Full-text search

Log data of log topics with full-text index enabled is split into segments by delimiter, so you can execute keyword query based on the segments.

For example, enter `error` in the search box to search for log data containing the keyword `error`.

Key-value search

Log data of the log topics with key-value index enabled is managed based on the specified key-value pairs. You can search for the log by specifying a key field.

For example, enter `status:error` in the search box to search for log data whose `status` field is `error`.

Fuzzy keyword search

CLS supports fuzzy search by special keywords as shown below:

| Metacharacter | Description |
|---------------|---|
| * | Fuzzy query of keywords that can match zero, single, or multiple random characters. For example, enter <code>abc*</code> to search for all logs beginning with <code>abc</code> |
| ? | Fuzzy query of keywords that can match a single character at a specific position. For example, enter <code>ab?c</code> to search for logs that begin with <code>ab</code> , end with <code>c</code> , and contain only one character between <code>ab</code> and <code>c</code> |

Notes

1. Before performing a log search, make sure the log topic has index enabled. Otherwise, no valid logs will be found.
2. Before performing a key-value search, make sure the index field for searching is successfully configured in the index configuration of the log topic.
3. The results are displayed in reverse order by default.