Alibaba Cloud
Log Service

FAQ

Issue: 20190917

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed due to product version upgrades , adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults " and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity , applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd / d  C :/ windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae  log  list  --  instanceid` *`Instance_ID`*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *`[-all|-t]`*

Style	Description	Example
{} or {a|b}	**It indicates that it is a required value, and only one item can be selected.**	`swich` *{stand | slave}*

Contents

1 Log collection

1.1 Troubleshoot collection errors

If the log collection fails or the collection status is abnormal when you use Logtail, follow these steps to troubleshoot the errors.

Procedure

1. Check whether the Logtail heartbeat in the machine group is normal

   Log on to the Log Service console and click Machine Status to view the status of the machine group. For more information, see Manage a machine group. If the heartbeat status is normal, move to the next step.

   If the heartbeat status is fail, see Logtail heartbeat error for troubleshooting.

2. Check whether the collection configuration is created and applied to the machine group

   After you confirm that the Logtail client status is normal, check the following configurations.

   a) Check whether Logtail configuration is created

      For more information, see Logtail configuration. Make sure that the log monitoring directory and the log file name match with the files on the machine. The directory does not support fuzzy match and must be set to an absolute path, while the log file name supports fuzzy match.

   b) Check whether Logtail configuration is applied to the machine group

      See Manage configurations in Manage a machine group. Check if the target configuration is applied to the machine group.

3. Check for collection errors

   If Logtail is properly configured, check whether new data is generated in real time in the log file. Logtail collects incremental data only, it does not read inventory

files if the files are not updated. If the log file is updated but the updates cannot be queried in Log Service, diagnose the problem in the following ways:

· Diagnose collection errors

  See #unique_6 to handle the errors according to the error type reported by Logtail.

· View Logtail logs

  Client logs include key INFO logs and all the WARNING and ERROR logs. To see complete and real-time errors, view the client logs in the following paths:

  - **Linux:** */ usr / local / ilogtail / ilogtail . LOG*

  - **Linux:** /usr/local/ilogtail/logtail_plugin.LOG (logs of input sources such as HTTP, MySQL binlog, and MySQL query results)

  - **Windows x64:** *C :\ Program   Files   Program   Files (x86)\ Alibaba \ Logtail \ logtail_ *. log*

  - **Windows x32:** *C :\ Program   Files \ Alibaba \ Logtail \ logtail_ *. log*

· Usage exceeds the limit

  - To collect large volumes of logs, files, or data, you can modify the Logtail startup parameters for higher log collection throughput. For more information, see #unique_7.

If the problem persists, open a ticket to contact Log Service engineers and attach the key information collected during troubleshooting to the ticket.

1.2 What can I do if the Logtail client has no heartbeat?

If the heartbeat status of the Logtail machine group is abnormal when you use Logtail to collect logs, you can troubleshoot the error manually or by using the Logtail automatic diagnostic tool.

After you install Logtail on your server to collect logs, the Logtail client regularly sends heartbeat packets to the server. If the machine group status shows that the Logtail client has no heartbeat, the Logtail client is disconnected from the server. In this case, you can troubleshoot the error manually or by using the Logtail automatic diagnostic tool as required.

· Automatic diagnosis: Log Service provides the Logtail automatic diagnostic tool for Linux. For more information, see How do I use the Logtail automatic diagnostic tool?

· Manual diagnosis: If the Logtail diagnostic tool fails to troubleshoot the error or your server is running in Windows, troubleshoot the error by performing the following steps.
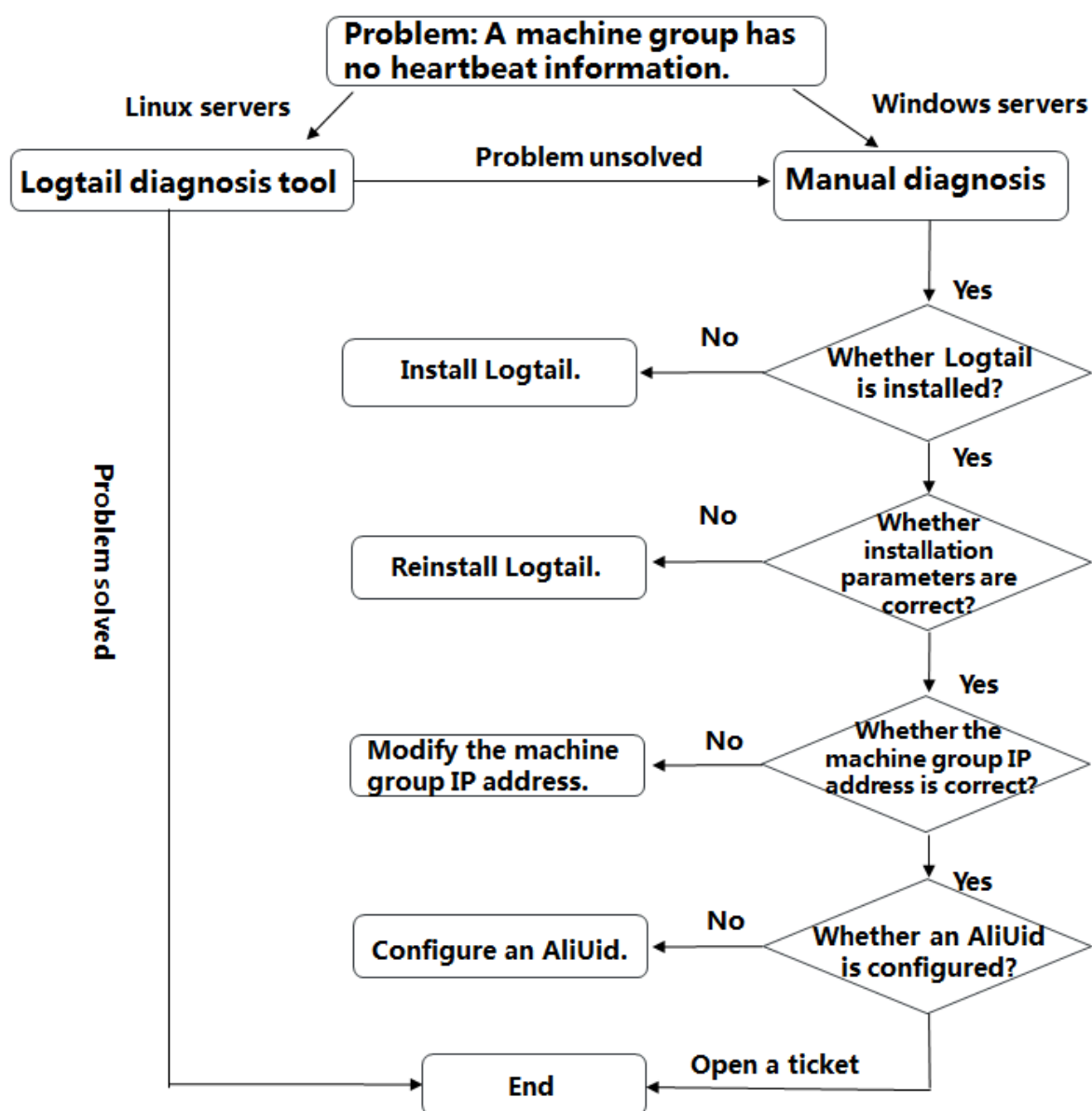
1. Check whether Logtail is installed

Run the following command to check whether Logtail is installed. If you do not install Logtail, see #unique_10 or #unique_11 to install it. You must install Logtail based on the region of your Log Service project and the network type.

Check the Logtail installation status:

- **Linux:**

```
sudo  / etc / init . d / ilogtaild   status
```

If `ilogtail   is   running` is returned, Logtail is installed, as shown in the following example:

```
[ root @****************~]#  sudo  / etc / init . d / ilogtaild
 status
 ilogtail   is   running
```

- **Windows:**

   1. **On Control Panel, choose System and Security > Administrative Tools, and then double-click Services.**
   2. **Check the running status of LogtailDaemon and LogtailWorker. If they are running normally, Logtail is installed.**

   If Logtail is running, go to the next step.

2. Check whether the Logtail installation parameter is correct

   Before installing Logtail, you must to specify the correct network endpoint. That is, you must select a correct Logtail installation parameter from #unique_12/ unique_12_Connect_42_table_eyz_pmv_vdb based on the region of the Log Service project and decide how to install Logtail based on the network type. If the installation script or parameter is incorrect, the Logtail client may have no heartbeat.

   The Logtail configuration file `ilogtail_c  onfig . json` records the Logtail installation parameter and the installation method that you used. This file is stored in:
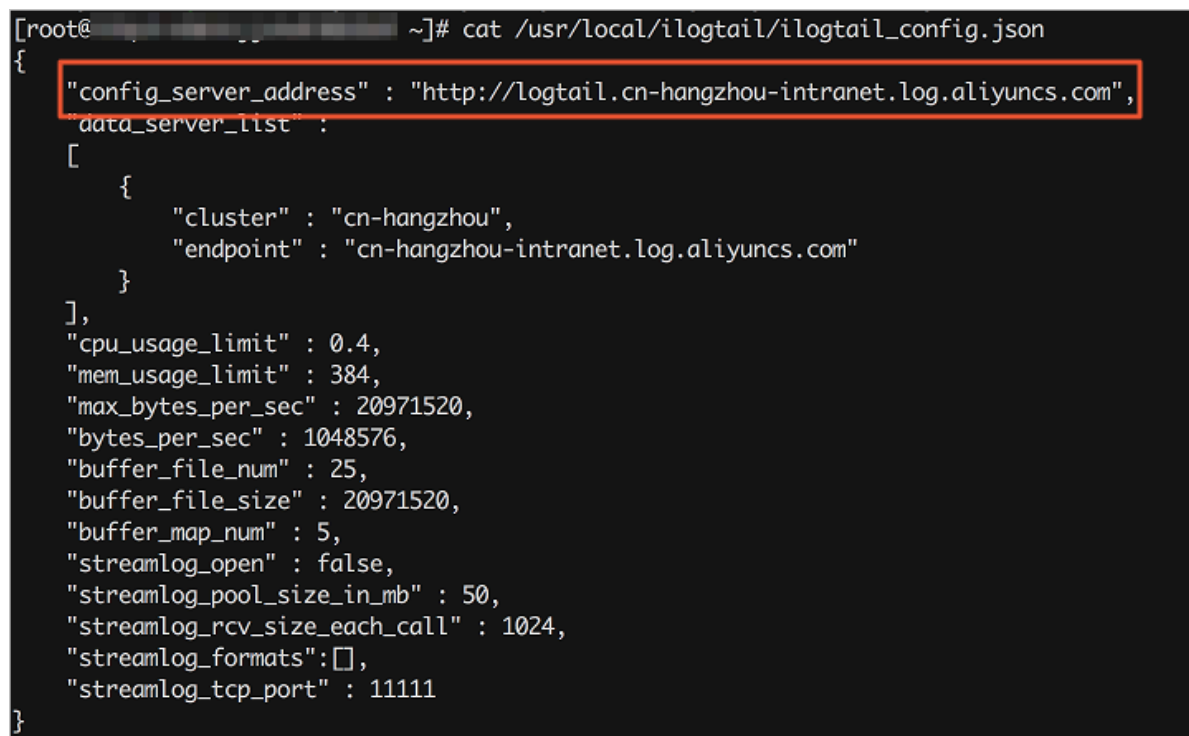
   - **Linux:** `/ usr / local / ilogtail / ilogtail_c  onfig . json`
   - **Windows x64:** `C :\ Program   Files  ( x86 )\ Alibaba \ Logtail \ ilogtail_c  onfig . json`
   - **Windows x32:** `C :\ Program   Files \ Alibaba \ Logtail \ ilogtail_c onfig . json`

1. Check the installation parameter.

   Check whether the region of the network endpoint recorded in the *ilogtail_c onfig . json* file is the same as that of your Log Service project.

   For example, the returned information in the following figure indicates that Logtail is installed on an ECS instance in China (Hangzhou).

   Figure 1-1: Check the installation parameter

2. Check the installation method.

   Telnet the domain name configured in the *ilogtail_c onfig . json* file to check whether Logtail is properly installed based on the network type of the server.

   For example, the domain name recorded in the *ilogtail_c onfig . json* file is `cn - hangzhou - intranet` . You can run the `telnet    logtail . cn - hangzhou - intranet . log . aliyuncs . com    80` command to check the network connectivity. If Logtail is connected to the server, Logtail is properly installed.

   For example, run the following command to check whether Logtail is connected to an ECS instance that is running in Linux:

```
[ root @*********** ~]#  telnet    logtail . cn - hangzhou - intranet
 . log . aliyuncs . com    80
 Trying    100 * 0 * 7 * 5 ...
```

```
Connected    to    logtail . cn - hangzhou - intranet . log .
aliyuncs . com .
Escape    character    is    '^]'.
```

If the telnet command fails, the Logtail installation parameter is incorrect, so that the installation command is incorrect. For more information about how to select a correct installation parameter, see #unique_10 or #unique_11.

If Logtail is properly installed, go to the next step.

3. Check whether the IP address configuration of the machine group is correct

The server IP address obtained by the Logtail client must be configured in the machine group. Otherwise, the Logtail client has no heartbeat in the machine group or Logtail cannot collect logs.

The Logtail client obtains the server IP address as follows:

· If no hostname is bound, the Logtail client obtains the IP address of the first NIC of the server.

· If a hostname is bound in the `/ etc / hosts` file, the Logtail client obtains the bound IP address. You can run the hostname command to view the hostname.

Troubleshooting procedure

1. Check the server IP address obtained by the Logtail client.

   The `ip` field in the `app_info . json` file indicates the server IP address obtained by the Logtail client. This file is stored in:

   · Linux: `/ usr / local / ilogtail / app_info . json`

   · Windows x64: `C :\ Program  Files  ( x86 )\ Alibaba \ Logtail \ app_info . json`

   · Windows x32: `C :\ Program  Files \ Alibaba \ Logtail \ app_info . json`

   > **Note:**
   >
   > · Logtail cannot work if the `ip` field in the `app_info . json` file is empty. In this case, you must to configure an IP address for the server and restart Logtail.

- The `app_info . json` file only records information. Any modification to this file does not change the server IP address obtained by the Logtail client.

Figure 1-2: Check the server IP address obtained by the Logtail client

```
[root@iZbp1fi3ce8nd9qzl7dbd4Z ~]# cat /usr/local/ilogtail/app_info.json
{
    "UUID" : "D75AA533-44B9-46C8-B071-614BC7A196B5",
    "hostname" : "iZbp1fi3ce8nd9qzl7dbd4Z",
    "instance_id" : "AE9FDA16-B279-11E8-A011-00163E0E5573_192.168.35.4_1536309632",
    "ip" : "192.168.35.4",
    "logtail_version" : "0.16.13",
    "os" : "Linux; 3.10.0-693.2.2.el7.x86_64; #1 SMP Tue Sep 12 22:26:13 UTC 2017; x86_64",
    "update_time" : "2018-09-07 16:40:32"
}
```

2. Check the IP address configuration of the machine group.

    Log on to the Log Service console, click the target project, and then click Logtail Machine Group in the left-side navigation pane. On the Machine Groups page, click Status in the Actions column of the target machine group.

    Figure 1-3: Check the machine group status

    If the server IP addresses configured in the machine group do not include the server IP address obtained by the Logtail client, you must to modify the IP address configuration.

    · If an incorrect server IP address is configured in the machine group, modify the IP address and save it. Then, check the heartbeat status again in 1 minute.
    · If you have modified the network configuration of the server where Logtail is installed, for example, `/ etc / hosts`, you must restart Logtail to obtain the new server IP address. In addition, you must modify the server IP address configured in the machine group based on the `ip` field in the `app_info .`
      `json` file.

Logtail restart methods

· Linux:

```
sudo  / etc / init . d / ilogtaild   stop
```

```
sudo  / etc / init . d / ilogtaild   start
```

· Windows: On Control Panel, choose System and Security > Administrative Tools, and then double-click Services. Find LogtailWorker and restart it.

If the server IP address obtained by the Logtail client is configured in the machine group, go to the next step.

4. Check whether an AliUid is configured for the ECS instance under another Alibaba Cloud account

If your ECS instance and Log Service project belong to different Alibaba Cloud accounts, or you use a server deployed in an on-premises IDC or provided by another cloud product vendor, you must configure an AliUid to authorize the server where Logtail is installed.

Check whether a file named after your AliUid exists in the `/ etc / ilogtail / users` directory.

If such a file does not exist, configure an AliUid. For more information, see #unique_14.

📋 **Note:**

· The AliUid must be an Alibaba Cloud account ID.
· You can view your Alibaba Cloud account ID in the Alibaba Cloud console as follows: Move the point over your avatar and choose User Info > Security Settings.

Figure 1-4: View your Alibaba Cloud account ID

If the problem persists, submit a ticket to Log Service engineers. Along with the ticket, provide the information about your project, Logstore, and machine group, the app_info.json and ilogtail_config.json files, and the output of the Logtail automatic diagnostic tool.

1.3 Do I need to update Logtail settings after the network type is changed?

After the network type is changed from classic network to VPC, you need to restart Logtail and update the settings of the Logtail machine group.

After Logtail is installed, if your ECS network type is changed from classic network to VPC, you need to update Logtail settings by performing the following steps:

1. Restart Logtail as the admin user.

   · In Linux:

   ```
   sudo  / etc / init . d / ilogtaild   stop
   sudo  / etc / init . d / ilogtaild   start
   ```

   · In Windows:

   In Control Panel, choose System and Security > Administrative Tools. Open the Services program, locate the `LogtailWor  ker` file, and then right-click the file and click Restart in the shortcut menu.

2. Update the machine group settings.

   · **Custom identity**

     If a custom identity is configured for the machine group, a VPC is accessible without the need to manually update the machine group settings.

   · **IP address**

     If the IP address of the ECS server is configured for the machine group, you need to replace the machine group IP address to the one that is obtained after the Logtail restart, namely, the ip field in the `app_info . json` file.

     The `app_info . json` file is stored in:

     - `/ usr / local / ilogtail / app_info . json` in Linux
     - `C :\ Program  Files  ( x86 )\ Alibaba \ Logtail \ app_info . json` in Windows x64
     - `C :\ Program  Files \ Alibaba \ Logtail \ app_info . json` in Windows x32

1.4 Diagnose collection errors

Errors may occur during log collection by Logtail, such as regular expression parsing failures, incorrect file paths, and traffic exceeding the shard service capability. Currently, the diagnosis function is provided in the Log Service console for diagnosing log collection errors.

Procedure

1. Log on to the Log Service console, and then click the target project name.

2. On the Logstores page, click Diagnose in the Log Collection Mode column.

   Figure 1-5: Diagnosis

3. Check log collection errors.

   In the displayed dialog box, view the list of log collection errors. To view error details, move your cursor to the Error Type column.

   For more information, see #unique_17.

   Figure 1-6: View collection errors

4. Query log collection errors of a specified machine

   To query all log collection errors occurred to a specific machine, enter the IP address of the machine in the search box on the query page. Logtail reports errors every 5 minutes.

   After fixing these errors and resuming business, check if the errors persist based on the timeframe. Historical error reports are still displayed before they expire. Ignore the historical error reports and only check whether new errors occurred after these historical errors are fixed.

   > **Note:**
   > To view all the complete log lines that are discarded because of parsing failure, you can log on to the machine to view the `/ usr / local / ilogtail / ilogtail . LOG` file.

1.5 Log collection error types

On the Logstores page, you can click Diagnose of a Logstore to view all log collection errors about it. This topic describes the specific error types and handling methods.

If you encounter an error not mentioned in this topic, you can open a ticket and submit error details.

Error type	Description	Handling method
LOGFILE_PERMINSSION_ ALARM	Logtail has no permission to read the specified file.	Check the Logtail startup account on the server. We recommend that you start Logtail as the root user.

Error type	Description	Handling method
SPLIT_LOG_FAIL_ALARM	The line start regular expression cannot match line starts of the log, and the log cannot be split into lines.	Check the correctness of the line start regular expression. If the log contains only one line, you can set the line start regular expression to `.*`.
MULTI_CONF IG_MATCH_ALARM	Each file can only be collected by one Logtail Config.	Check whether a file is collected in multiple Configs. If yes, delete unnecessary Configs.
REGEX_MATCH_ALARM	The log content does not match the regular expression upon regular expression parsing.	Copy a part from the unmatched content as a sample for a rematch, and then generate a new regular expression.
PARSE_LOG_FAIL_ALARM	Log parsing fails because the formats of JSON and delimiter logs do not conform to format definitions.	Click the error message to view details.
CATEGORY_CONFIG_ALAR M	The Logtail Config is invalid.	We recommend that you modify the regular expression because generally the process of extracting a file path as the Topic through the regular expression fails. If the error is due to another reason, open a ticket and submit error details.
LOGTAIL_CRASH_ALARM	Logtail cannot respond because its server resource usage has exceeded the upper limit.	Modify the upper limits of the CPU usage and memory usage by following the instructions provided in #unique_7. You can also open a ticket for additional support.

Error type	Description	Handling method
REGISTER_INOTIFY_FAIL_ALARM	Registering log monitoring has failed on Linux. A possible cause is that Logtail does not have the permission to access the folder or the folder has been deleted.	Check whether Logtail has the permission to access the folder and whether the folder has been deleted.
DISCARD_DATA_ALARM	The CPU resources for configuring Logtail are insufficient or the incoming traffic to Log Service is restricted.	Modify the upper limit of the CPU usage or limits on concurrent incoming traffic to Log Service by following the instructions provided in #unique_7. You can also open a ticket for additional support.
SEND_DATA_FAIL_ALARM	· The Alibaba Cloud account have not created any AccessKey (AK). · The Logtail client cannot connect to the Log Service server, or the connection quality is poor. · The writing quota on the server is insufficient.	· Use the Alibaba Cloud account to create an AK. · Check the local Config file `/ usr / local / ilogtail / ilogtail_c  onfig . json` and run `curl<endpoint>` to check whether any result is returned. · Increase the number of Shards for the Logstore so that more data can be written to the Logstore.
REGISTER_INOTIFY_FAIL_ALARM	Logtail fails to register inotify watcher for the log directory.	Check whether the directory exists. If yes, check the directory permissions.
SEND_QUOTA_EXCEED_ALARM	The log writing amount exceeds the limit.	Expand the Shard capacity in the console.

Error type	Description	Handling method
READ_LOG_D ELAY_ALARM	Log collection lags behind log generation. In normal cases, this is because the CPU resources for configuring Logtail are insufficient or the incoming traffic to Log Service is restricted.	Modify the upper limit of the CPU usage or limits on concurrent incoming traffic to Log Service by following the instructions provided in #unique_7. You can also open a ticket for additional support.
DROP_LOG_ALARM	Log collection lags behind log generation, and unprocessed log rotations outnumbers 20. In normal cases, this is because the CPU resources for configuring Logtail are insufficient or the incoming traffic to Log Service is restricted.	Modify the upper limit of the CPU usage or limits on concurrent incoming traffic to Log Service by following the instructions provided in #unique_7. You can also open a ticket for additional support.
LOGDIR_PERMINSSION_A LARM	Logtail has no permission to read the log monitoring directory.	Check whether the log monitoring directory exists. If yes, check the directory permissions.
ENCODING_C ONVERT_ALARM	Code conversion fails.	Check whether the log encoding format conforms to the specified format.

Error type	Description	Handling method
OUTDATED_LOG_ALARM	The log is outdated because the time when Logtail received the log has exceeded more than 12 hour and the log is expired. Possible causes are as follows: · Log parsing is more than 12 hours behind schedule. · Custom time fields are incorrect. · The time of the log recording program is incorrect.	· Check whether READ_LOG_D ELAY_ALARM exists. If yes, use the method of handling READ_LOG_D ELAY_ALARM to handle this error. If no, check the time filed settings. · Check the time filed settings. If the time field settings are correct, check whether the time of the log recording program is correct. You can also open a ticket for additional support.
STAT_LIMIT_ALARM	The number of files in the Logtail Config directory exceeds the upper limit.	Check whether the Logtail Config directory contains an excessive number of files and subdirectories. If yes, configure the root monitoring directory and the maximum directory monitoring depth as needed.
DROP_DATA_ALARM	When the log collection process exits, writing logs to the local disk expires. In this case, the logs that have not been written to the local disk will be discarded.	Modify the upper limit of the CPU usage or limits on concurrent incoming traffic to Log Service by following the instructions provided in #unique_7. Generally, the error is caused by severe collection blocks. You can also open a ticket for additional support.
INPUT_COLLECT_ALARM	An error occurs during input source collection.	Handle the error according to the error message.
HTTP_LOAD_ADDRESS_AL ARM	The address in the HTTP input source is invalid.	Check the validity of the address.

Error type	Description	Handling method
HTTP_COLLECT_ALARM	An error occurs during HTTP input source collection.	Handle the error according to the error message. In normal cases, the error is caused by expiration.
FILTER_INIT_ALARM	An error occurs during filer initialization.	Handle the error according to the error message. In normal cases, the error is caused by invalid filter regular expressions.
INPUT_CANAL_ALARM	An error occurs when MySQL binlogs run.	Handle the error according to the error message. The canal service may restart when Logtail Config is updated. Errors caused by service restart can be ignored.
CANAL_INVALID_ALARM	The internal state of MySQL binlogs is abnormal.	Check whether the table schema is being modified when the error occurs . This error generally occurs when meta data changes are caused by table schema modificati ons during binlog running . Open a tick if the cause is another one.
MYSQL_INIT_ALARM	An error occurs during MySQL initialization.	Handle the error according to the error message.
MYSQL_CHEC KPOING_ALARM	The MySQL checkpoint format is incorrect.	Check whether to modify the checkpoint settings in the current Logtail Config . If the error persists after you modify the checkpoint settings, open a ticket and submit error details.
MYSQL_TIMEOUT_ALARM	The MySQL query expires.	Check whether the error is caused by MySQL server faults or abnormal network status.

Error type	Description	Handling method
MYSQL_PARSE_ALARM	Parsing MySQL query results fails.	Check whether the checkpoint format configured in MySQL matches the format of the corresponding field.
AGGREGATOR _ADD_ALARM	Logtail fails to add data to the queue.	Ignore the error if the actual data amount is large because the error is caused by excessive fast data sending.
ANCHOR_FIND_ALARM	Possible error causes are anchor plug-in faults, Config faults, or mismatch between the Config and log .	Click the error message to view details, which may contain the following error types. Check whether the corresponding Config encounters faults accordingly. · anchor cannot find key: The SourceKey is specified in the Config but its corresponding field cannot be found in the log. · anchor no start: The keywords specified by Start cannot be found in the value of SourceKey. · anchor no stop: The keywords specified by Stop cannot be found in the value of SourceKey.
ANCHOR_JSON_ALARM	An error occurs when the anchor plug-in performs JSON expansion on the keywords specified by Start and Stop.	Click the error message to view details. Check the keywords and the related Config. Check whether there is any Config fault or invalid log.

Error type	Description	Handling method
CANAL_RUNTIME_ALARM	An error occurs when the binlog plug-in runs.	Click the error message to view details, and then handle the error accordingly. The error is related to the connected MySQL master database.
CHECKPOINT_INVALID_A LARM	The plug-in fails to parse the checkpoint.	Click the error message to view details, and then handle the error according to the checkpoint key, checkpoint content (the first 1,024 bytes), and other information.
DIR_EXCEED_LIMIT_ALA RM	The number of directorie s for simultaneous monitoring exceeds the upper limit.	Check whether the Config of the current Logstore and other Configs applied on Logtail contain excessive directories. If yes, configure the root monitoring directory and the maximum directory monitoring depth as needed.
DOCKER_FILE_MAPPING_ ALARM	Logtail fails to add Docker file mapping by executing commands.	Click the error message to view details, and then handle the error accordingly.
DOCKER_FIL E_MATCH_ALARM	The specified file cannot be found in Docker.	Click the error message to view details, and then handle the error according to the container information and file path.
DOCKER_REG EX_COMPILE_ALARM	The docker stdout plug -in fails to construct a regular expression based on BeginLineRegex in the Config.	Click the error message to view details, and then check whether the regular expression is correct.

Error type	Description	Handling method
DOCKER_STDOUT_INIT_ALARM	The docker stdout collection initialization fails.	Click the error message to view details, which may contain the following error types: · host... version... error: Check whether the Docker engine specified in the Config is accessible. · load checkpoint error: Ignore the error if there is no impact because the error is caused by checkpoint loading failure. · container...: Set either stdout or stderr as a label. The error is caused because the specified container has an invalid label value. Handle the error according to the error details.
DOCKER_STDOUT_START_ALARM	The stdout file size exceeds the upper limit during docker stdout collection initialization.	Ignore the error because, in normal cases, the stdout file already exists at the first collection.
DOCKER_STDOUT_STAT_ALARM	The docker stdout plug-in cannot check the stdout file.	Ignore the error because the container cannot access the stdout file after the container exits.
FILE_READER_EXCEED_ALARM	The number of objects opened by Logtail exceeds the upper limit.	Check whether the Config settings are appropriate because the error is caused by excessive files being collected.

Error type	Description	Handling method
GEOIP_ALARM	The geoip plug-in is faulty.	Click the error message to view details, which may contain the following error types: · invalid ip...: The plug-in fails to obtain the IP address. Check whether SourceKey in the Config is correct or whether an invalid log exists. · parse ip...: The plug-in fails to parse the city information based on the obtained IP address. Handle the error according to the error details. · cannot find key...: The plug-in cannot find the specified SourceKey from the log. Check whether the Config is faulty or whether an invalid log exists.
HTTP_INIT_ALARM	The http plug-in incorrectly compiles the ResponseStringMatch regular expression specified in the Config.	Click the error message to view details, and then check whether the regular expression is correct.
HTTP_PARSE_ALARM	The http fails to receive HTTP responses.	Click the error message to view details, and then check the Config or the requested HTTP server.
INIT_CHECKPOINT_ALARM	The binlog plug-in fails to load the checkpoint. In this case, the plug-in will ignore the checkpoint and recollect the log.	Click the error message to view details, and then determine whether the error can be ignored.

Error type	Description	Handling method
LOAD_LOCAL_EVENT_ALARM	Logtail handles a local event.	Ignore the error if it is caused by manual operations. For other cases , open a ticket and submit error details. Click the error message to view details, and then handle the error according to the file name, Config name , project, Logstore, and other information.
LOG_REGEX_ FIND_ALARM	The processor_split_log_ regex and processor_ split_log_string plug-ins cannot obtain the SplitKey specified by the Config from the log.	Click the error message to view details, and then check whether the Config is faulty.
LUMBER_CON NECTION_ALARM	The server cannot be powered off when the service_lumberjack plug-in is stopped.	Click the error message to view details, and then handle the error accordingly. In normal cases, this error can be ignored.
LUMBER_LISTEN_ALARM	An error occurs when the service_lumberjack plug-in is being initiated for log monitoring.	Click the error message to view details, which may contain the following error types: · init tls error…: Check whether the TLS configurations are correct. · listen init error…: Check whether the address-related settings are correct.

Error type	Description	Handling method
LZ4_COMPRESS_FAIL_AL ARM	An error occurs when Logtail executes LZ4 compression.	Click the error message to view details, and then handle the error according to the values of log lines , project, category, and region.
MYSQL_CHEC KPOINT_ALARM	The MySQL plug encounters a checkpoint error.	Click the error message to view details, which may contain the following error types: · init checkpoint error …: Initializing the checkpoint fails. In this case, check whether the checkpoint column specified by the Config and the corresponding values are correct. · not matched checkpoint …: The checkpoint information does not match. In this case , check whether the mismatch is caused by manual operations, for example, Config updates . If yes, ignore the error.
NGINX_STATUS_COLLECT _ALARM	An error occurs when the nginx_status plug-in obtains the server status.	Click the error message to view details, and then handle the error according to the URL and other information.
NGINX_STATUS_INIT_AL ARM	The nginx_status plug-in fails to initiate and parse the URL specified by the Config.	Click the error message to view details, and then check whether the address is correct according to the URL.

Error type	Description	Handling method
OPEN_FILE_LIMIT_ALARM	Logtail cannot open new files because the number of opened files has exceeded the upper limit.	Click the error message to view details, and then handle the error according to the log file path, project , Logstore, and other information.
OPEN_LOGFILE_FAIL_ALARM	An error occurs when Logtail opens a file.	Click the error message to view details, and then handle the error according to the log file path, project , Logstore, and other information.
PARSE_DOCKER_LINE_ALARM	The service_docker_stdout plug-in fails to parse the log.	Click the error message to view details, which may contain the following error types: · parse docker line error : empty line: The log is empty. · parse json docker line error…: The plug-in fails to parse the log in JSON format. In this case, handle the error according to the error message and the first 512 bytes of the log. · parse cri docker line error…: The plug-in fails to parse the log in CRI format. In this case, handle the error according to the error message and the first 512 bytes of the log.

Error type	Description	Handling method
PLUGIN_ALARM	An error occurs when the plug-in is initialized or called.	Click the error message to view details, which may contain the following error types. Handle the error accordingly. · init plugin error...: Initiating the plug-in fails. · hold on error...: Stopping the plug-in fails. · resume error...: Recovering the plug-in fails. · start service error...: Starting service input-type plug-ins fails. · stop service error...: Stopping service input-type plug-ins fails.
PROCESSOR_INIT_ALARM	The regex plug-in fails to compile the Regex regular expression specified by the Config.	Click the error message to view details, and then check whether the regular expression is correct.

Error type	Description	Handling method
PROCESS_TOO_SLOW_ALA RM	Logtail parses logs too slowly.	1. Click the error message to view details, and then determine whether the slow parsing is normal according to the number of logs, buffer size, and parsing time. 2. If the slow parsing is abnormal, check whether inappropriate parsing configurations exist. For example, the processes on the node where Logtail resides occupy excessive CPU resources, or an inefficient regular expression exists.
REDIS_PARSE_ADDRESS_ ALARM	The redis plug-in fails to parse the ServerUrls specified by the Config.	Click the error message to view details, and then check the URL.
REGEX_FIND_ALARM	The regex plug-in cannot find the fields specified by SourceKey in the Config from the log.	Click the error message to view details, and then check whether the SourceKey is incorrect or an invalid log exists.

Error type	Description	Handling method
REGEX_UNMA TCHED_ALARM	The regex plug-in fails to match the log.	Click the error message to view details, which may contain the following error types. Handle the error accordingly, for example, determine whether the Config is correct. · unmatch this log content...: The log cannot match the regular expression in the Config. · match result count less...: The number of matched logs is less than that of Keys specified in the Config.
SAME_CONFIG_ALARM	There are Configs with the same name in a Logstore. In this case, Logtail chooses one to collect the log, and the others will be discarded.	Click the error message to view details, and then handle the error according to the Config path and other information.
SPLIT_FIND_ALARM	The split_char and split_string plug-ins cannot find the fields specified by SourceKey in the Config from the log.	Click the error message to view details, and then check whether SourceKey settings are incorrect or an invalid log exists.
SPLIT_LOG_ALARM	The number of parsed fields parsed by the processor_split_char and processor_split_string plug-ins does not match that of fields specified by SplitKeys.	Click the error message to view details, and then check whether SourceKey settings are incorrect or an invalid log exists.
STAT_FILE_ALARM	An error occurs when the plug-in collects files through the LogFileReader object.	Click the error message to view details, and handle the error according to the file path and other information.

Error type	Description	Handling method
SERVICE_SYSLOG_INIT_ ALARM	The service_syslog plug-in initialization fails.	Click the error message to view details, and check whether Address in the Config is correct.
SERVICE_SYSLOG_STREA M_ALARM	An error occurs when the service_syslog plug-in collects data through TCP.	Click the error message to view details, which may contain the following error types. Handle the error accordingly. · accept error...: An error occurs during Accept execution. In this case, the plug-in waits for a while and restarts. · setKeepAlive error...: Setting Keep Alive fails . In this case, the plug-in ignores the error and runs properly. · connection i/o timeout ...: Reading data through TCP expires. In this case, the plug-in resets the expiration duration and reads data properly. · scan error...: An error occurs when the plug-in reads data through TCP . In this case, the plug-in waits for a while and tries again.

Error type	Description	Handling method
SERVICE_SYSLOG_PACKET_ALARM	An error occurs when the service_syslog plug-in collects data through UDP.	Click the error message to view details, which may contain the following error types. Handle the error accordingly. · connection i/o timeout …: Reading data through UDP expires. In this case, the plug-in resets the expiration duration and reads data properly. · read from error…: An error occurs when the plug-in reads data through UDP. In this case, the plug-in waits for a while and tries again.

1.6 Query local collection status

Logtail is used to query its own health status and log collection progress, helping you troubleshoot log collection issues and customize status monitoring for log collection.

1. User guide

    a. all command

    b. active command

    c. logstore command

    d. logfile command

    e. history command

2. Return values

3. Use cases

    a. Monitor the running status of Logtail

    b. Monitor log collection progress

    c. Determine whether or not Logtail has finished collecting log files

    d. Troubleshoot log collection issues

User guide

If a Logtail client supporting status query function is installed, you can query local log collection status by entering commands on the client. To install Logtail, see #unique_12.

Enter the `/ etc / init . d / ilogtaild  - h` command on the client to check if the client supports querying local log collection status. If the `logtail   insight` `,  version` keyword is returned, it indicates that this function is supported on the Logtail client.

```
/ etc / init . d / ilogtaild  - h
 Usage : ./ ilogtaild  {  start  |  stop  ( graceful ,  flush   data
 and  save  checkpoint  s ) |  force - stop  |  status  | - h   for
   help }$
 logtail  insight ,  version  :  0 . 1 . 0
 commond  list  :
      status  all  [ index ]
          get  logtail  running  status
      status  active  [-- logstore  | -- logfile ]  index  [
 project ] [ logstore ]
          list  all  active  logstore  |  logfile . if  use
 -- logfile ,  please  add  project  and  logstore . default  --
 logstore
      status  logstore  [-- format = line  |  json ]  index
 project  logstore
          get  logstore  status  with  line  or  json
 style .  default  -- format = line
      status  logfile  [-- format = line  |  json ]  index
 project  logstore  fileFullPa  th
          get  log  file  status  with  line  or  json
 style .  default  -- format = line
      status  history  beginIndex  endIndex  project  logstore
 [ fileFullPa  th ]
          query  logstore  |  logfile  history  status .
 index :  from  1  to  60 .  in  all ,  it  means  last  $(
 index )  minutes ;  in  active / logstore / logfile / history ,  it
   means  last  $( index )* 10   minutes
```

Currently, Logtail supports the following query commands, command functions, time intervals to query and time windows for result statistics:

Command	Functions	Time interval to query	Time window for statistics
all	Query the running status of Logtail.	Last 60 min	1 min

Command	Functions	Time interval to query	Time window for statistics
active	Query Logstores or log files that are currently active (that is, with data collected).	Last 600 min	10 minutes.
logstore	Query the collection status of a Logstore.	Last 600 min	10 minutes.
logfile	Query the collection status of a log file.	Last 600 min	10 minutes.
history	Query the collection status of a Logstore or log file over a period of time.	Last 600 min	10 minutes.

Note:

· The `index` parameter in the command represents the index value of the time window, which is counted from the current time. Its valid range is 1–60. If the time window for statistics is one minute, windows in the last `( index , index − 1 ]` minutes are queried. If the time window for statistics is 10 minutes, windows in the last `( 10 * index , 10 *( index − 1 )]` minutes are queried.

· All query commands belong to status subcommands, so the main command is status.

all command

Command format

```
/etc/init.d/ilogtaild  status   all  [ index ]
```

Note:

The all command is used to view the running status of Logtail. The index parameter is optional. If left blank, 1 is taken by default.

Example

```
/ etc / init . d / ilogtaild    status    all    1
 ok
/ etc / init . d / ilogtaild    status    all    10
 busy
```

Output description

Item	Description	Priority	Resolution:
ok	The current status is normal.	None.	No action is needed .
busy	The current collection speed is high and the Logtail status is normal.	None.	No action is needed .
many_log_files	The number of logs being collected is large.	Low	Check if the configuration contains files that do not need to be collected.
process_block	Current log parsing is blocked.	Low	Check if logs are generated too quickly. If you still get this output, #unique_21 as per your needs to modify the upper limit of CPU usage or the limit on concurrent sending by using network.

Item	Description	Priority	Resolution:
send_block	Current sending is blocked.	Relatively high	blocked. Check if logs are generated too quickly and if the network status is normal. If you still get this output, #unique_21 as per your needs to modify the upper limit of CPU usage or the limit on concurrent sending by using network.
send_error	Failed to upload log data.	High	To troubleshoot the issue, see #unique_6.

active command

Command format

```
/ etc / init . d / ilogtaild   status   active  [-- logstore ]  index
 / etc / init . d / ilogtaild   status   active  -- logfile   index
 project - name   logstore - name
```

📋 **Note:**

· The `active  [-- logstore ]  index` command is used to query Logstores that are currently active. The `-- logstore` parameter can be omitted without changing the meaning of the command.

· The `active  -- logfile   index   project - name   logstore - name` command is used to query all active log files in a Logstore for a project.

· The active command is used to query active log files level by level. We recommend that you first locate the currently active Logstore and then query active log files in this Logstore.

Example

```
/ etc / init . d / ilogtaild   status   active   1
 sls - zc - test  :  release - test
 sls - zc - test  :  release - test - ant - rpc - 3
 sls - zc - test  :  release - test - same - regex - 3
```

```
/ etc / init . d / ilogtaild  status  active  -- logfile  1  sls -
 zc - test  release - test
/ disk2 / test / normal / access . log
```

Output description

- To run the `active  -- logstore   index` command, all currently active
  Logstores are output in the format of `project - name  :  logstore - name`
  . To run the `active -- logfile   index   project - name   logstore -
   name` command, the complete paths of active log files are output.
- A Logstore or log file with no log collection activity in the current query window
  does not appear in the output.

logstore command

Command format

```
/ etc / init . d / ilogtaild  status  logstore  [-- format ={ line |
 json }]  index  project - name  logstore - name
```

> **Note:**
> - The logstore command is used to output the collection statuses of the specified
>   project and Logstore in LINE or JSON format.
> - If the `-- format =` parameter is not configured, `-- format = line` is selected
>   by default. The echo information is output in LINE format. Note that `-- format`
>   parameter must be placed behind `logstore` .
> - If this Logstore does not exist or has no log collection activity in the current query
>   window, you get an empty output in LINE format or a `null` value in JSON format.

Example

```
/ etc / init . d / ilogtaild  status  logstore  1  sls - zc - test
  release - test - same
 time_begin  _readable  :  17 - 08 - 29   10 : 56 : 11
 time_end_r  eadable  :  17 - 08 - 29   11 : 06 : 11
 time_begin  :  1503975371
 time_end  :  1503975971
 project  :  sls - zc - test
 logstore  :  release - test - same
 status  :  ok
 config  : ## 1 . 0 ## sls - zc - test $ same
 read_bytes  :  65033430
 parse_succ  ess_lines  :  230615
 parse_fail  _lines  :  0
 last_read_  time  :  1503975970
 read_count  :  687
```

```
  avg_delay_   bytes   :   0
  max_unsend   _time   :   0
  min_unsend   _time   :   0
  max_send_s   uccess_tim   e   :   1503975968
  send_queue   _size   :   0
  send_netwo   rk_error_c   ount   :   0
  send_netwo   rk_quota_c   ount   :   0
  send_netwo   rk_discard   _count   :   0
  send_succe   ss_count   :   302
  send_block   _flag   :   false
  sender_val   id_flag   :   true
/ etc / init . d / ilogtaild   status   logstore   -- format = json   1
   sls - zc - test   release - test - same
{
   " avg_delay_   bytes " :   0 ,
   " config " : "## 1 . 0 ## sls - zc - test $ same ",
   " last_read_   time " :   1503975970 ,
   " logstore " : " release - test - same ",
   " max_send_s   uccess_tim   e " :   1503975968 ,
   " max_unsend   _time " :   0 ,
   " min_unsend   _time " :   0 ,
   " parse_fail   _lines " :   0 ,
   " parse_succ   ess_lines " :   230615 ,
   " project " : " sls - zc - test ",
   " read_bytes " :   65033430 ,
   " read_count " :   687 ,
   " send_block   _flag " :   false ,
   " send_netwo   rk_discard   _count " :   0 ,
   " send_netwo   rk_error_c   ount " :   0 ,
   " send_netwo   rk_quota_c   ount " :   0 ,
   " send_queue   _size " :   0 ,
   " send_succe   ss_count " :   302 ,
   " sender_val   id_flag " :   true ,
   " status " : " ok ",
   " time_begin " :   1503975371 ,
   " time_begin   _readable " : " 17 - 08 - 29   10 : 56 : 11 ",
   " time_end " :   1503975971 ,
   " Maid ": " 17 - 08 - 29   11 : 06 : 11 "
}
```

Output description

Reserved Word	Meaning	Unit
Status	The overall status of this Logstore. For specific statuses, descriptions, and change methods, see the following table.	None.
time_begin_readable	The start time that can be read.	None.
time_end_readable	The end time that can be read.	None.
time_begin	The start time of statistics.	UNIX timestamp, measured in seconds.

Reserved Word	Meaning	Unit
time_end	The end time of statistics.	UNIX timestamp, measured in seconds.
project	The project name.	None.
logstore	The Logstore name.	None.
config	The collection configuration name, which is globally unique and consisted of `## 1 . 0 ##`, project, `$`, and config.	None.
read_bytes	The number of logs read in the window.	Byte
parse_success_lines	The number of successfully parsed log lines in the window.	Line
parse_fail_lines	The number of log lines that failed to be parsed in the window.	Line
last_read_time	The last read time in the window.	UNIX timestamp, measured in seconds.
Read_count	The number of times that logs are read in the window.	Number
avg_delay_bytes	The average of the differences between the current offset and the file size each time logs are read in the window.	Byte
max_unsend_time	The maximum time that unsent data packets are in the send queue when the window ends. The value is 0 when the queue is empty.	UNIX timestamp, measured in seconds.
min_unsend_time	The minimum time that unsent data packets are in the send queue when the window ends. The value is 0 when the queue is empty.	UNIX timestamp, measured in seconds.

Reserved Word	Meaning	Unit
max_send_success_time	The maximum time that data is successfully sent in the window.	UNIX timestamp, measured in seconds.
send_queue_size	The number of unsent data packets in the current send queue when the window ends.	Packet
send_network_error_count	The number of data packets that failed to be sent in the window because of network errors.	Packet
send_network_quota_count	The number of data packets that failed to be sent in the window because the quota is exceeded.	Packet
send_network_discard_count	The number of discarded data packets in the window because of data exceptions or insufficient permissions.	Packet
send_success_count	The number of successfully sent data packets in the window.	Packet
send_block_flag	Whether or not the send queue is blocked when the window ends.	None.
sender_valid_flag	Whether or not the send flag of this Logstore is valid when the window ends. true means the flag is valid, and false means the flag is disabled because of network errors or quota errors.	None.

Logstore status

Status	Meaning	Handling method
ok	The status is normal.	No action is needed.
process_block	Log parsing is blocked.	Check if logs are generated too quickly. If you still get this output, Configure #unique_21 as per your needs to modify the upper limit of CPU usage or the limit on concurrent sending by using network.
parse_fail	Log parsing failed.	Check whether or not the log format is consistent with the log collection configuration.
send_block	Current sending is blocked.	blocked. Check if logs are generated too quickly and if the network status is normal. If you still get this output, #unique_21 as per your needs to modify the upper limit of CPU usage or the limit on concurrent sending by using network.
sender_invalid	An exception occurred when sending log data.	Check the network status. If the network is normal, see #unique_6 in Query diagnosis errors to troubleshoot the issue.

logfile command

Command format

```
/ etc / init . d / ilogtaild   status    logfile   [-- format ={ line |
 json }]   index   project - name    logstore - name   fileFullPa  th
```

📋 **Note:**

· The logfile command is used to output the collection status of a specific log file in LINE or JSON format.

- If the `-- format =` parameter is not configured, `-- format = line` is selected by default. The echo information is output in LINE format.
- If this log file does not exist or has no log collection activity in the current query window, you get an empty output in LINE format or a `null` value in JSON format.
- The `-- format` parameter must be placed behind `logfile` .
- The `filefullpa    th` must be a full path name.

Example

```
/ etc / init . d / ilogtaild   status   logfile   1   sls - zc - test
   release - test - same  / disk2 / test / normal / access . log
 time_begin  _readable  :  17 - 08 - 29   11 : 16 : 11
 time_end_r  eadable  :  17 - 08 - 29   11 : 26 : 11
 time_begin  :  1503976571
 time_end  :  1503977171
 project  :  sls - zc - test
 logstore  :  release - test - same
 status  :  ok
 config  : ## 1 . 0 ## sls - zc - test $ same
 file_path  : / disk2 / test / normal / access . log
 file_dev  :  64800
 file_inode  :  22544456
 file_size_  bytes  :  17154060
 file_offse  t_bytes  :  17154060
 read_bytes  :  65033430
 parse_succ  ess_lines  :  230615
 parse_fail  _lines  :  0
 last_read_  time  :  1503977170
 read_count  :  667
 avg_delay_  bytes  :  0
/ etc / init . d / ilogtaild   status   logfile  -- format = json   1
   sls - zc - test   release - test - same  / disk2 / test / normal /
 access . log
{
   " avg_delay_  bytes " :  0 ,
   " config " : "## 1 . 0 ## sls - zc - test $ same ",
   " file_dev " :  64800 ,
   " file_inode " :  22544456 ,
   " file_path " : "/ disk2 / test / normal / access . log ",
   " file_size_  bytes " :  17154060 ,
   " last_read_  time " :  1503977170 ,
   " logstore " : " release - test - same ",
   " parse_fail  _lines " :  0 ,
   " parse_succ  ess_lines " :  230615 ,
   " project " : " sls - zc - test ",
   " read_bytes " :  65033430 ,
   " read_count " :  667 ,
   " read_offse  t_bytes " :  17154060 ,
   " status " : " ok ",
   " time_begin " :  1503976571 ,
   " time_begin  _readable " : " 17 - 08 - 29   11 : 16 : 11 ",
   " time_end " :  1503977171 ,
   " time_end_r  eadable " : " 17 - 08 - 29   11 : 26 : 11 "
}
```

Output description

Reserved Word	Meaning	Unit
Status	The collection status of this log file in the current query window. See the status of logstore command.	None.
time_begin_readable	The start time that can be read.	None.
time_end_readable	The end time that can be read.	None.
time_begin	The start time of statistics.	UNIX timestamp, measured in seconds.
time_end	The end time of statistics.	UNIX timestamp, measured in seconds.
project	The project name.	None.
logstore	The Logstore name.	None.
file_path	The path of the log file.	None.
file_dev	The device ID of the log file.	None.
file_inode	The inode of the log file.	None.
file_size_bytes	The size of the last scanned file in the window.	Byte
read_offset_bytes	The parsing offset of this file.	Byte
config	The collection configuration name, which is globally unique and consisted of `## 1 . 0 ##`, project, $ and config.	None.
read_bytes	The number of logs read in the window.	Byte
parse_success_lines	The number of successfully parsed log lines in the window.	Line
parse_fail_lines	The number of log lines that failed to be parsed in the window.	Line

Reserved Word	Meaning	Unit
last_read_time	The last read time in the window.	UNIX timestamp, measured in seconds.
read_count	The number of times that logs are read in the window.	Number of times
avg_delay_bytes	The average of the differences between the current offset and the file size each time logs are read in the window.	Byte

history command

Command format

```
/ etc / init . d / ilogtaild   status   history   beginIndex
 endIndex   project – name   logstore – name  [ fileFullPa  th ]
```

📋 **Note:**

· The history command is used to query the collection status of a Logstore or log file over a period of time.

· `beginIndex` and `endIndex` represent the start and end values for the code query window index respectively. `beginIndex <= endIndex`.

· If the `fileFullPa th` is not entered in the parameter, the code queries the collection information of the Logstore. Otherwise, the collection information of the log file is queried.

Example

```
/ etc / init . d / ilogtaild   status   history   1   3   sls – zc –
 test   release – test – same  / disk2 / test / normal / access . log
      begin_time   status   read   parse_succ  ess   parse_fail
     last_read_  time   read_count   avg_delay   device   inode
 file_size   read_offse  t
 17 – 08 – 29   11 : 26 : 11   ok   62 . 12MB   231000   0   17 – 08
 – 29   11 : 36 : 11   671   0B   64800   22544459   18 . 22MB   18 .
 22MB
 17 – 08 – 29   11 : 16 : 11   ok   62 . 02MB   230615   0   17 – 08
 – 29   11 : 26 : 10   667   0B   64800   22544456   16 . 36MB   16 .
 36MB
 17 – 08 – 29   11 : 06 : 11   ok   62 . 12MB   231000   0   17 – 08
 – 29   11 : 16 : 11   687   0B   64800   22544452   14 . 46MB   14 .
 46MB
```

```
$/ etc / init . d / ilogtaild   status   history   2   5    sls - zc -
 test   release - test - same
         begin_time   status   read   parse_succ   ess   parse_fail
         last_read_  time   read_count   avg_delay   send_queue
 network_er  ror   quota_erro  r   discard_er  ror   send_succe  ss
   send_block   send_valid   max_unsend   min_unsend      max_send_s
 uccess
  17 - 08 - 29   11 : 16 : 11   ok   62 . 02MB   230615   0   17 - 08
 - 29   11 : 26 : 10   667   0B   0   0   0   0   300   false   true
 70 - 01 - 01   08 : 00 : 00   70 - 01 - 01   08 : 00 : 00   17 - 08 -
 29   11 : 26 : 08
  17 - 08 - 29   11 : 06 : 11   ok   62 . 12MB   231000   0   17 - 08
 - 29   11 : 16 : 11   687   0B   0   0   0   0   303   false   true
 70 - 01 - 01   08 : 00 : 00   70 - 01 - 01   08 : 00 : 00   17 - 08 -
 29   11 : 16 : 10
  17 - 08 - 29   10 : 56 : 11   ok   62 . 02MB   230615   0   17 - 08
 - 29   11 : 06 : 10   687   0B   0   0   0   0   302   false   true
 70 - 01 - 01   08 : 00 : 00   70 - 01 - 01   08 : 00 : 00   17 - 08 -
 29   11 : 06 : 08
  17 - 08 - 29   10 : 46 : 11   ok   62 . 12MB   231000   0   17 - 08
 - 29   10 : 56 : 11   692   0B   0   0   0   0   302   false   true
 70 - 01 - 01   08 : 00 : 00   70 - 01 - 01   08 : 00 : 00   17 - 08 -
 29   10 : 56 : 10
```

Output description

· This command outputs historical collection information of a Logstore or log file in the form of list, one line for each window.

· For the description of each output field, see the `logstore` and `logfile` commands.

Return values

Normal return value

0 is returned if a command input is valid (including failure to query a Logstore or log file), for example:

```
/ etc / init . d / ilogtaild   status   logfile  -- format = json   1
   error - project   error - logstore  / no / this / file
 null
 echo  $?
 0
/ etc / init . d / ilogtaild   status   all
 ok
 echo  $?
 0
```

Exceptional return values

A non-zero return value indicates an exception. See the following table.

Return value	Type	output	Troubleshooting
10	**Invalid command or missing parameters**	`invalid param , use - h for help .`	**Enter** `- h` **to view help.**
1	**The query goes beyond the 1–60 time window**	`invalid query interval`	**Enter** `- h` **to view help.**
1	**Cannot query the specified time window**	`query fail , error : $( error )`. For more information, see [errno interpretation]().	**This issue might occur when the startup time of Logtail is less than the query time span . For other cases, open a ticket.**
1	**No matching query window time**	`no match time interval , please check logtail Status`	**Check if Logtail is running. For other cases, open a ticket.**
1	**No data in the query window**	`invalid profile , maybe logtail Restart`	**Check if Logtail is running. For other cases, open a ticket.**

Example

```
/ etc / init . d / ilogtaild   status   nothiscmd
 invalid   param , use - h   for   help .
 echo  $?
 10
/ etc / init . d / ilogtaild   status / all   99
 invalid   query   interval
 echo  $?
 1
```

Use cases

You can obtain the overall status of Logtail by querying its health status, and obtain the related metrics during collection by querying the collection progress. With the obtained information, you can monitor log collection in a customized manner.

Monitor the running status of Logtail

Monitor the running status of Logtail by using the `all` command.

How it works: The current status of Logtail is queried every minute. If Logtail is under `process_bl ock`, `send_block`, or `send_error` status for five successive minutes, an alarm is triggered.

The alarm duration and the status range being monitored can be adjusted according to the importance of log collection in specific scenarios.

Monitor log collection progress

Monitor the collection progress of a Logstore by using the `logstore` command.

How it works: The `logstore` command is called every ten minutes to obtain the status information of this Logstore. If the `avg_delay_ bytes` is over 1 MB (1024*1024) or `status` is not `ok`, an alarm is triggered.

The `avg_delay_ bytes` alarm threshold can be adjusted according to the log collection traffic.

Determine whether or not Logtail has finished collecting log files

Determine whether or not Logtail has finished collecting log files by using the `logfile` command.

How it works: After writing to the log file stops, the `logfile` command is called every ten minutes to obtain the status information of this file. If this file shows the same value for `read_offse t_bytes` and `file_size_ bytes`, it means that Logtail has finished collecting this log file.

Troubleshoot log collection issues

If the log collection is delayed on a server, use the `history` command to query related collection information on this server.

1. If the `send_block _flag` is true, it indicates that the log collection delays because of the network.

   · If the `send_netwo rk_quota_c ount` is greater than 0, you must split the [Shard](#) of the Logstore.
   · If the `send_netwo rk_error_c ount` is greater than 0, you must check the network connectivity.
   · ◦ If no related network error occurs, you must adjust the limit on concurrent sending and [traffic limit](#) of Logtail.

2. Sending-related parameters are normal, but the `avg_delay_ bytes` is relatively high.

   · The average log parsing speed can be calculated by using `read_bytes` to determine if traffic generated by logs is normal.

   · Resource usage limits of Logtail can be adjusted as appropriate.

3. The `parse_fail _lines` is greater than 0.

   Check if the parsing configurations for log collection match with all the logs.

1.7 How do I use the Logtail automatic diagnostic tool?

If an exception occurs during log collection, you can use the Logtail automatic diagnostic tool to check whether the exception exists on the Logtail client and quickly locate and resolve errors as instructed by the tool.

> **Note:**
> This tool is currently available only to Linux servers.

Preparations

1. Download the script of the diagnostic tool.

   ```
   wget  http :// logtail - release . oss - cn - hangzhou . aliyuncs
   . com / linux64 / checkingto  ol . sh  - O   checkingto  ol . sh
   ```

   > **Note:**
   > If you fail to download the tool, use the following URL and try again.
   >
   > ```
   > wget  http :// logtail - corp . oss - cn - hangzhou - zmf .
   > aliyuncs . com / linux64 / checkingto  ol . sh  - O   checkingto
   > ol . sh
   > ```

2. Install the curl tool.

   The diagnostic tool uses curl to check the network connectivity. Ensure that the curl tool is installed on the server where Logtail is installed.

Startup of the diagnostic tool

1. Run the following command to run the diagnostic tool:

   ```
   chmod   744  ./ checkingto  ol . sh
   ./ checkingto  ol . sh
   ```

```
sh   checkingto  ol . sh
```

The returned information is as follows:

```
[ Info ]:      Logtail   checking   tool   version  :  0 . 3 . 0
[ Input ]:   please   choose   which   item   you   want   to
 check  :
          1 .  MachineGro  up   heartbeat   fail .
          2 .  MachineGro  up   heartbeat   is   ok ,  but   log
  files   have   not   been   collected .
    Item  :
```

2. Enter `1` or `2` as prompted. The script performs different checks based on your choice.

   where:

   · `1` indicates the machine group heartbeat check. Select this option if the heartbeat status of the machine group is abnormal.

   · `2` indicates the log collection check. Select this option if the heartbeat status of the machine group is normal but log files are not collected.

   After you select the required option, the diagnostic tool automatically performs the corresponding check.

Diagnostic flowchart
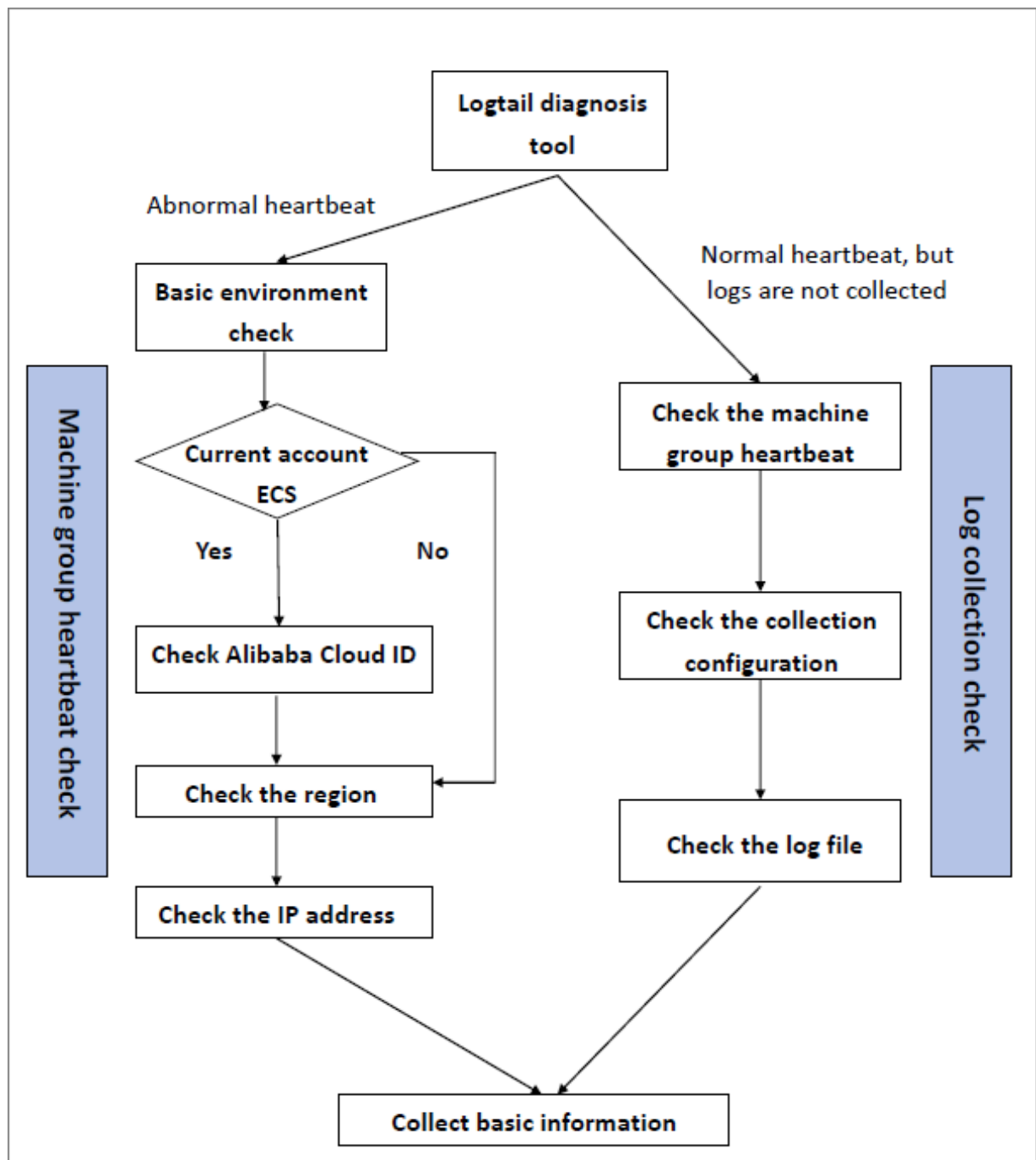
Machine group heartbeat check

After you select the machine group heartbeat check, the diagnostic tool checks the following items:

1. **Check the basic environment.**

   · **Whether Logtail is installed.**

   · **Whether Logtail is running.**

   · **Whether the SSL status is normal.**

   · **Whether the network connection with Log Service is normal.**

```
[ Info ]:        Logtail    checking    tool    version   :  0 . 3 . 0
[ Input ]:   please    choose    which    item    you    want    to
 check   :
                1 .  MachineGro   up    heartbeat    fail .
                2 .  MachineGro   up    heartbeat    is   ok , but
 log   files   have   not   been    collected .
        Item   : 1
[ Info ]:        Check   logtail    install    files
[ Info ]:        Install    file : ilogtail_c  onfig . json    exists .
                    [  OK   ]
[ Info ]:        Install    file : / etc / init . d / ilogtaild
 exists .                        [  OK   ]
[ Info ]:        Install    file : ilogtail    exists .
                  [  OK   ]
[ Info ]:        Bin    file : / usr / local / ilogtail / ilogtail_0 .
 14 . 2    exists .             [  OK   ]
[ Info ]:        Logtail    version   :
                  [  OK   ]
[ Info ]:        Check    logtail    running    status
[ Info ]:        Logtail    is    runnings .
                    [  OK   ]
[ Info ]:        Check    network    status
[ Info ]:        Logtail    is    using    ip :  11 . XX . XX . 187
[ Info ]:        Logtail    is    using    UUID :  0DF18E97 – 0F2D – 486F
 – B77F – XXXXXXXXXX   XX
[ Info ]:        Check    SSL    status
[ Info ]:        SSL    status    OK .
                  [  OK   ]
[ Info ]:        Check    logtail    config    server
[ Info ]:        config    server    address :  http :// config . sls .
 aliyun – inc . com
[ Info ]:        Logtail    config    server    OK
```

If an `Error` message appears during the check, troubleshoot the error as prompted.

2. Check whether you are the owner of the Elastic Compute Service (ECS) instance.

   After checking the basic environment, check whether your server is an ECS instance and whether you buy it with your Alibaba Cloud account.

   If this server is not an ECS instance or the account used to buy the server is different from that used to access Log Service, enter `y` . Otherwise, enter `N` .

   ```
   [ Input ]: Is   your   server   non – Alibaba   Cloud   ECS   or
    not   belong   to   the   same   account   with   the   current
    Project   of   Log   Service  ? ( y / N )
   ```

   If you enter `y` , the diagnostic tool returns the AliUid information configured on the server where Logtail is installed. Check whether it includes your AliUid. If not, configure an AliUid for an ECS instance under another Alibaba Cloud account or a server in an on-premises IDC.

   ```
   [ Input ]:   Is   your   server   non – Alibaba   Cloud   ECS   or
      not   belong   to   the   same   account   with   the   current
    Project   of   Log   Service  ? ( y / N ) y
   [ Info ]:      Check   aliyun   user   id ( s )
   [ Info ]:      aliyun   user   id :   126XXXXXXX   XXX79  .
                     [ OK  ]
   [ Info ]:      aliyun   user   id :   165XXXXXXX   XXX50  .
                     [ OK  ]
   [ Info ]:      aliyun   user   id :   189XXXXXXX   XXX57  .
                     [ OK  ]
   [ Input ]:   Is   your   project   owner   account   ID   is   the
    above   IDs  ? ( y / N )
   ```

3. Check the region.

   Check whether the region of your project is the same as that selected during Logtail installation. If not, reinstall Logtail.

   ```
   [ Input ]:  please   make   sure   your   project   is   in   this
    region  : {  cn – hangzhou  } ( y / N ) :
   ```

4. Check the IP address configuration.

   Check whether the IP address of the server where Logtail is installed is configured in your machine group. If not, modify the IP address configuration. For more information, see Create a machine group with IP addresses as its identifier.

   If your machine group is identified by a custom ID, check whether the custom ID configured on the server where Logtail is installed is the same as that configured

in your machine group. If not, modify the custom ID configuration. For more information, see Create a machine group with a custom ID as its identifier.

```
[ Input ]:    please    make    sure    your    machine    group ' s    ip
   is    same    with  : {   11 . XX . XX . 187   }   or    your    machine
   group ' s    userdefine  d - id    is    in  : {   XX - XXXXX   } ( y
 / N ) :
```

Log collection check

After you select the log collection check, the diagnostic tool checks the following items:

1. Check the IP address configuration.

   Check whether the IP address of the server where Logtail is installed is configured in your machine group, and whether the heartbeat status is normal. If not, modify the machine group.

```
[ Input ]:    please    make    sure    your    machine    group ' s    ip
   is    same    with  : {   11 . XX . XX . 187   } ( y / N ) :
```

2. Check the application of the Logtail configuration.

   Check whether your Logtail configuration is applied to the machine group. For more information about how to check the Logtail configurations that are applied to a machine group, see #unique_26.

```
[ Input ]:    please    make    sure    you    have    applied    collection
   config    to    the    machine    group  ( y / N ) : Y
```

3. Check a specified log file.

   Enter the full path of the log file to be checked. Check whether this log file can be matched in the log path of your Logtail configuration.

   If the Logtail configuration is incorrect, modify the configuration and save it. Run the script again one minute later to check this item for a second time.

```
[ Input ]:    please    input    your    log    file ' s    full    path  (
 eg . / var / log / nginx / access . log ) :/ disk2 / logs / access
 . log
[ Info ]:      Check    specific    log    file
[ Info ]:      Check    if    specific    log    file  [ / disk2 / logs
 / access . log  ]   is    included    by    user    config .
[ Warning ]:    Specific    log    file    doesnt    exist .
                        [  Warning  ]
[ Info ]:      Matched    config    found :
                  [  OK  ]
[ Info ]:      [ Project ] ->  sls - zc - xxxxxx
[ Info ]:      [ Logstore ] ->  release - xxxxxxx
[ Info ]:      [ LogPath ] -> / disk2 / logs
```

```
[ Info ]:      [ FilePatter  n ] -> *. log
```

Persisted exception after all checks

If the Logtail client passes all the checks but still fails to collect logs, enter `y` for the last option of the script and press Enter.

Add the output of the script as an attachment and submit a ticket to Alibaba Cloud after-sales engineers.

```
[ Input ]: please   make   sure   all   the   check   items   above
   have   passed . If   the   problem   persists , please   copy
  all   the   outputs   and   submit   a   ticket   in   the   ticket
  system . : ( y / N ) y
```

Quick check

The quick check runs without confirmation. You can encapsulate and customize a quick check script.

> **Note:**
> During quick check, the diagnostic tool returns the AliUid and custom ID that identifies the machine group configured on the server where Logtail is installed. If either of them does not exist, no alert is reported. If an AliUid or a custom ID that identifies the machine group is configured for the Logtail client, check whether the configuration returned by the diagnostic tool is the same as that you configured. If not, modify the configuration as required. For more information, see Configure an AliUid for an ECS instance under another Alibaba Cloud account or a server in an on-premises IDC and Create a machine group with a custom ID as its identifier.

Procedure

Run the script `./ checkingto  ol . sh  -- logFile  [ LogFileFul  lPath ]` to perform the check. If an exception is detected, proceed as instructed by the script.

> **Note:**
> If the Logtail client passes the specified log file check and the Logtail running environment is normal, we recommend that you log on to the Alibaba Cloud console to view the exception logs of the relevant Logtail configuration. For more information, see #unique_27.

```
[vagrant@localhost ilogtail]$ ./checkingtool.sh --logFile /usr/x.log
[Info]:      Logtail checking tool version : 0.2.0                          [ OK ]
[Info]:      Check specific log file
[Info]:      Check if specific log file [ /usr/x.log ] is included by user config.
[Warning]:   Specific log file doesnt exist.                                [ Warning ]
[Info]:      Check user config file
[Info]:      User config file exists.                                       [ OK ]

[Error]:     No match config for your log file.                             [ Error ]
[Suggestion]:  Please check your logtail project/logstore config and make sure you have applied config to your machine group
[Suggestion]:  For more about logtail config, follow this link for more help: https://help.aliyun.com/document_detail/49010.html

[Info]:      Check system support
[Info]:      Check system support OK.                                       [ OK ]

[Info]:      Check logtail install files
[Info]:      Install file: ilogtail_config.json exists.                     [ OK ]
[Info]:      Install file: /etc/init.d/ilogtaild exists.                    [ OK ]
[Info]:      Install file: ilogtail exists.                                 [ OK ]
[Info]:      Bin file: /usr/local/ilogtail/ilogtail_0.12.0 exists.          [ OK ]
[Info]:      Logtail version : 0.12.0                                       [ OK ]

[Info]:      Check logtail running status
[Error]:     Logtail is stopped                                            [ Error ]
[Suggestion]:  Try [/etc/init.d/ilogtaild start] to start logtail.

[Info]:      Check aliyun user id(s)
[Info]:      aliyun user id : 1xxxxxxxxxxxxxxx .                             [ OK ]

[Info]:      Check user defined id
[Info]:      User defined id is : xx_vagrant_001 .                          [ OK ]

[Info]:      Check user config file
[Info]:      User config file exists.                                       [ OK ]

[Info]:      Check network status
[Info]:      Logtail is using ip: 10.0.2.15
[Info]:      Logtail is using UUID: FE15C1A0-E237-43C8-9475-7641860xx463T
[Info]:      Check SSL status
[Info]:      SSL status OK.                                                 [ OK ]
[Info]:      Logtail config file : ilogtail_config.json exists.             [ OK ]
[Info]:      Check logtail config server
[Info]:      Logtail config server OK                                       [ OK ]
Check complete.

 [ 1 ] warning(s) found.

 [ 2 ] error(s) found.
```

Common Logtail collection errors

After running the Logtail automatic diagnostic tool, you can identify the causes of Logtail collection errors, and then use an appropriate solution to resolve the error accordingly. The following table describes the causes of common Logtail collection errors and their solutions.

Error	Solution
Installation files are incomplete.	Reinstall Logtail.
Logtail is not running.	Run the `/ etc / init . d / ilogtaild  start` command to start Logtail.
Multiple Logtail processes exist.	Run the `/ etc / init . d / ilogtaild  stop` command to stop Logtail, and then run the `/ etc / init . d / ilogtaild  start` command to restart Logtail.
Port 443 is disabled.	Configure the firewall to enable port 443.
The configuration server cannot be found.	Check whether Logtail is properly installed on a Linux server. If not, uninstall and then reinstall Logtail. For more information, see Install Logtail in Linux.

Error	Solution
The user configuration does not exist.	Check whether the following operations are performed: 1. A Logtail configuration is created in the console. 2. The server is included in a machine group. 3. The Logtail configuration is applied to the machine group.
The specified log file cannot be matched.	Check whether the Logtail configuration is correct.
The specified log file is matched more than once.	Logtail selects a Logtail configuration randomly if you match the specified log file multiple times. We recommend that you keep only one Logtail configuration that matches the specified log file.

Common parameters for the diagnostic tool

Parameter	Description
`-- help`	Views the help documentation.
`-- logFile [ LogFileFul lPath ]`	Checks whether Logtail collects logs from `LogFileFul lPath` and checks the basic running environment of Logtail, such as the integrity of installation files, running status, AliUid, and network connectivity.
`-- logFileOnl y [ LogFileFul lPath ]`	Only checks whether Logtail collects logs from `LogFileFul lPath`.
`-- envOnly`	Only checks the running environment of Logtail.

1.8 Collect logs in complete regular mode

1.8.1 How do I modify a regular expression?

When configuring Logtail to collect text logs, you must specify a regular expression based on your log sample if you parse and collect logs in full regex mode. This topic describes how to modify a regular expression.

To modify a regular expression that you specified in the Log Service console, you can click Validate to check the following items:

· For the regular expression used to specify the starting header of a cross-line log, check whether the current regular expression can correctly match the expected number of log entries.

· For the regular expression used to extract fields, check whether the value of each field meets your requirements.

If you need to verify more items and modify a regular expression, you can use online tools such as Regex101 and RegexTester. You can copy and paste the regular expression automatically generated in the console to a tool, and then enter actual logs for further verification and modification.

In full regex mode, Log Service automatically generates regular expressions, which may not be suitable for the message field of cross-line logs. This topic describes how to use Regex101 to verify a regular expression.

Procedure

1. Copy the regular expression automatically generated by Log Service based on the log sample.

2. Go to the website of Regex101.

3. In the REGULAR EXPRESSION field, paste the automatically generated regular expression:

```
\[([^]]+)]\ s \[(\ w +)]\ s ([^:]+:\ s \ w +\ s \ w +\ s [^:]+:\ S +
\ s [^:]+:\ S +\ s \ S +). *
```

The meaning of the regular expression appears in the right pane of the page.

4. In the TEST STRING field, paste part of the log sample.

In the following figure, some content after `at` is not included in the `message` field. The log entries included and not included in the message field are highlighted in orange and blue, respectively. Therefore, this regular expression

does not fully match the log sample. That is, this regular expression is incorrect for the log sample and cannot be used to collect all required log data.
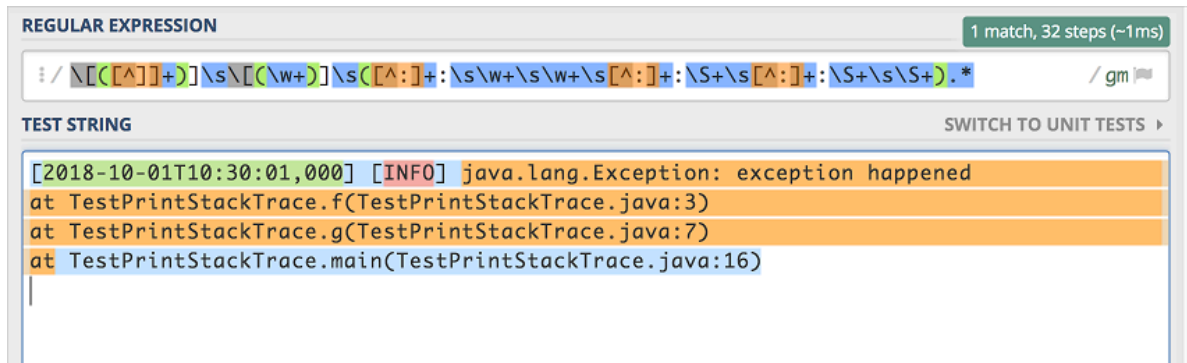
5. Verify another error: The entered log sample contains only two colons.

   In the following figure, the regular expression fails to match the log sample.
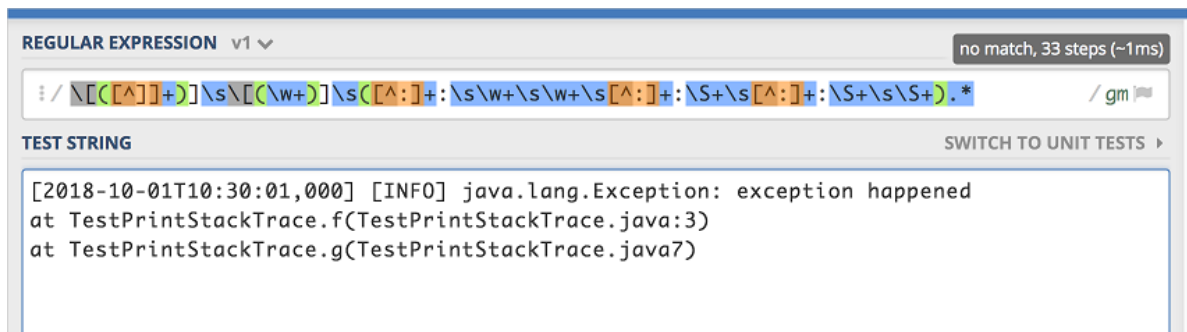
6. Replace the last element in the regular expression with `[\ S \ s ]+` and check whether the regular expression matches the log sample.

In the following figure, the regular expression matches the content after `at` .
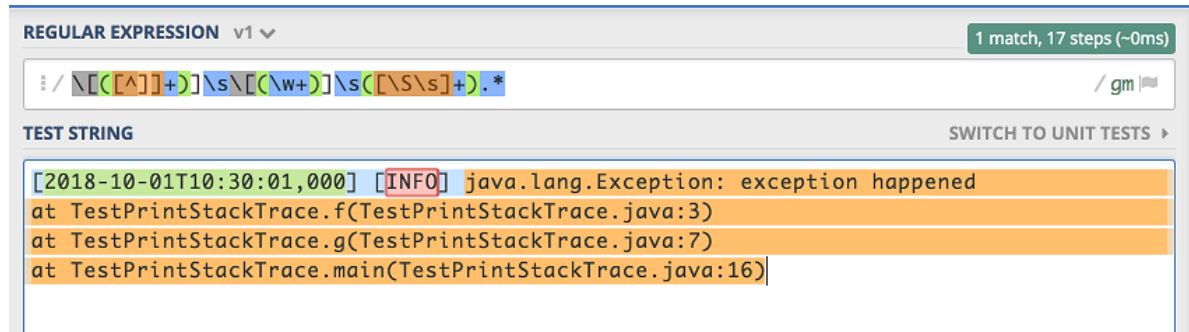
In the following figure, the regular expression matches the log sample that contains only two colons.
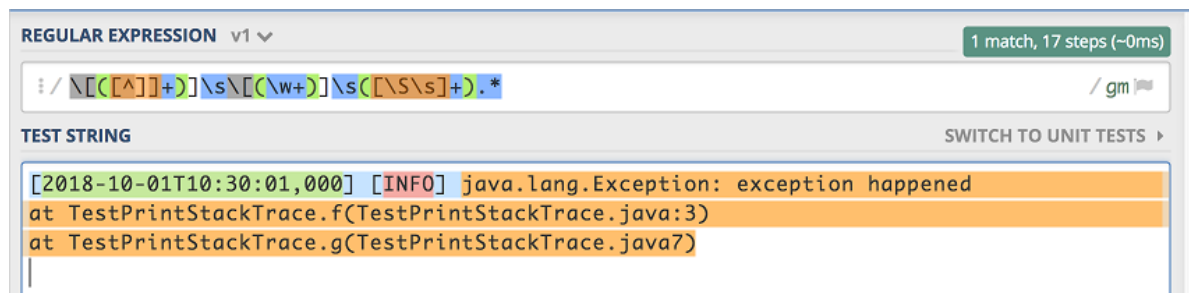
You can use the preceding method to specify and modify your regular expression and apply it to a Logtail configuration.

1.8.2 How do I optimize regular expressions?

You can optimize regular expressions to improve the Logtail collection performance.

The following describes some suggestions about how to optimize regular expressions:

· Use precise characters.

Do not arbitrarily use `.*` to match fields because this regular expression can match with a wide range of search results. Such actions can to lead to mismatches occurring or a decrease in matching performance. For example, to return results of fields that consist only of letters, use `[ A - Za - z ]`.

· Use correct measure words.

Do not arbitrarily use plus signs (+), commas (,), or asterisks. For example, to match target IP addresses, use `\ d` instead of `\ d +` or `\ d { 1 , 3 }` because of its higher efficiency.

· Debug multiple times.

  Debugging is similar to troubleshooting. You can debug the time consumed by your regular expressions at the Regex101 website, and promptly optimize them if there is a large amount of backtracking.

1.8.3 How do I collect various formats of logs in complete regular mode?

The complete regular mode requires format consistency among all logs. However, some logs may contain content in multiple formats. In this case, you can use the Schema-On-Write or Schema-On-Read mode to process the logs.

For example, a Java log is a program log that contains both correct information and error information (such as information about abnormal stacks), including:

· Multi-line WARNING logs

· Simple text INFO logs

· Key-value DEBUG logs

```
[ 2018 - 10 - 01T10 : 30 : 31 , 000 ] [ WARNING ]  java . lang .
 Exception :  another   exception   happened
    at   TestPrintS  tackTrace . f ( TestPrintS  tackTrace . java : 3
 )
    at   TestPrintS  tackTrace . g ( TestPrintS  tackTrace . java : 7
 )
    at   TestPrintS  tackTrace . main ( TestPrintS  tackTrace . java
 : 16 )
[ 2018 - 10 - 01T10 : 30 : 32 , 000 ] [ INFO ]  info   something
[ 2018 - 10 - 01T10 : 30 : 33 , 000 ] [ DEBUG ]  key : value   key2 :
 value2
```

You can use the following modes to process such logs:

· Schema-On-Write: In this mode, Logtail applies multiple Logtail Configs with different regular settings to a log so that correct fields can be extracted.

> 📋 **Note:**
>
> Logtail cannot apply multiple Logtail Configs to a file. Therefore, you need to set up multiple symbolic links for the directory where the file is stored. Then, each Logtail Config works on a symbolic link, thereby allowing you to aggregate multiple Logtail Configs to collect the file at the same time.

· Schema-on-read: In this mode, you need to use the common regular expressions of the multi-format logs.

For example, for collection of a multi-line log, you can use the time and log level as line start regular expressions and the residual parts as the message field. If you want to analyze the message field, you can set up an index for it, extract the required content, and then analyze the content based on query and analysis functions provided by Log Service, such as regular expression extraction.

> 📋 Note:
> This mode is recommended only when you need to analyze at a small-scale (for example, tens of millions) of logs.

1.9 Why am I unable to collect SLB access logs?

This topic describes how to troubleshoot in cases where you are unable to collect SLB access logs.

1. Check whether the access log collection function has been activated for SLB instances.

Activate the access log collection function for each SLB instance separately. Then, the generated access logs can be written into your Logstore in real time.

To do so, log on to the SLB console, and choose Logs > Access Logs to view the Access Logs (Layer-7) list.

· Verify that the specified SLB instance exists.
· Confirm the Storage Path of the SLB instance.

This column displays information about the project and Logstore. In this case, make sure that you check whether SLB logs exist in the correct location in the console.

2. Check whether RAM users are correctly authorized.

During activation of the access log collection function, the system guides you through RAM user authorization. The function can be successfully activated only after RAM users are successfully authorized. If RAM users are incorrectly created or deleted, the collected logs cannot be delivered to your Logstore.

Troubleshooting

Log on to the RAM Console. On the RAM Roles page, check whether the AliyunLogArchiveRole role exists.

- If AliyunLogArchiveRole does not exist, use your Alibaba Cloud account to log on to the RAM console and click the quick authorization link to create the RAM users required for authorization.

- If AliyunLogArchiveRole exists, click the role name and check whether the role is correctly authorized.

  The following shows the default policy. If your policy has been modified, we recommend that you replace the current policy with the default policy.

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Action ": [
        " log : PostLogSto  reLogs "
      ],
      " Resource ": "*",
      " Effect ": " Allow "
    }
  ]
}
```

3. Check whether any log is generated.

If you do not find any SLB access log in the Log Service console, it is likely that no log has been generated. Possible causes include:

- Layer-7 listening is not configured for the current instance.

  Currently, only instances configured with layer-7 listening are supported. Common layer-7 listening protocols include HTTP and HTTPS. For more information, see #unique_33.

- Historical logs that were generated before activation of the access log collection function are not collected.

  Instead, only logs that are generated after activation of the access log collection function are collected.

- The specified instance did not receive a request.

  Logs are generated only when you request access to the listener of the instance.

1.10 How do I set the time format?

This topic describes how to set the time format for Logtail Configs and the precautions you need be aware of first.

- The minimum granularity that you can configure for timestamps in Log Service is seconds.
- In the time field, only the front part that contributes to time parsing is required.

The following shows a setting example:

```
 Custom1    2017 – 12 – 11    15 : 05 : 07
% Y –% m –% d   % H :% M :% S
 Custom2   [ 2017 – 12 – 11    15 : 05 : 07 . 012 ]
[% Y –% m –% d   % H :% M :% S
 RFC822      02    Jan    06    15 : 04    MST
% d   % b   % y   % H :% M
 RFC822Z     02    Jan    06    15 : 04   – 0700
% d   % b   % y   % H :% M
 RFC850       Monday ,  02 – Jan – 06    15 : 04 : 05    MST
% A , % d –% b –% y   % H :% M :% S
 RFC1123      Mon ,  02    Jan    2006    15 : 04 : 05    MST
% A , % d –% b –% y   % H :% M :% S
 RFC3339       2006 – 01 – 02T15 : 04 : 05Z07 : 00
% Y –% m –% dT % H :% M :% S
 RFC3339Nan  o   2006 – 01 – 02T15 : 04 : 05 . 999999999Z   07 : 00
% Y –% m –% dT % H :% M :% S
```

1.11 Troubleshoot log collection exceptions in containers

This topic provides solutions to exceptions that may occur when you use a Logtail container (a common container or Kubernetes) to collect logs.

Troubleshooting operations:

- Troubleshoot heartbeat exceptions in a machine group
- Troubleshoot log collection exceptions in a container

Other O&M operations:

- Log on to the Logtail container
- View Logtail operational logs
- View Logtail standard output (stdout)
- View the status of log-related components in a Kubernetes cluster
- View the version information, IP address, and time of Logtail
- What do I do if I mistakenly delete a Logstore that is created through CRD?

Troubleshoot heartbeat exceptions in a machine group

You can determine whether the Logtail on a container is correctly installed by checking the heartbeat status of a machine group.

1. Check the heartbeat status of the machine group.

    a. Log on to the Log Service console, and then click the target project name.

    b. In the left-side navigation pane, click Logtail Machine Group.

    c. Find the target machine group and click Status.

    Record the number of nodes for which heartbeat status is OK.

2. Check the number of Worker nodes in the cluster.

    Run `kubectl get node | grep -v master` to view the number of Worker nodes.

    ```
    $ kubectl   get   node | grep  -v  master
     NAME                                      STATUS      ROLES        AGE
            VERSION
     cn - hangzhou . i - bp17enxc2u  s3624wexh2    Ready     < none >
        238d        v1 . 10 . 4
     cn - hangzhou . i - bp1ad2b02j  tqd1shi2ut    Ready     < none >
        220d        v1 . 10 . 4
    ```

3. Compare whether the number of the nodes with heartbeat status of OK is the same as the number of Worker nodes. Then, use an appropriate troubleshooting method according to the following possible comparison results:

    · The heartbeat status of all nodes is Failed.

        - If you use standard Docker logs, check whether $\{your\_region\_name\}$, $\{your\_aliyun\_user\_id\}$, and $\{your\_machine\_group\_user\_defined\_id\}$ are correct by following the instructions provided in parameter description.

        - If you use installation for Kubernetes on Alibaba Cloud Container Service, open a ticket.

        - If you use self-built Kubernetes installation, check whether $\{your\text{-}project\text{-}suffix\}$, $\{regionId\}$, $\{aliuid\}$, $\{access\text{-}key\text{-}id\}$, and $\{access\text{-}key\text{-}secret\}$ are correct by following the instructions provided in parameter description. If the parameters are incorrect, run `helm del -- purge`

`alibaba - log - controller` to delete the installation package and reinstall Kubernetes.

· The number of nodes for which the heartbeat status is OK is smaller than the number of Worker nodes.

    a. Determine whether to use the yaml file to manually deploy DaemonSet.

       Run `kubectl get po - n kube - system - l k8s - app = logtail`. If any result is returned, you have manually deployed DaemonSet by using the yaml file.

    b. Download the latest DaemonSet template.

    c. Set *${your_region_name}*, *${your_aliyun_user_id}*, and *${your_machine_group_name}* as needed.

    d. Run `kubectl apply - f ./ logtail - daemonset . yaml` to update the DaemonSet yaml file.

    For other comparison results, open a ticket.

Troubleshoot log collection exceptions in a container

If you cannot find any log on the preview or query page in the console, Log Service has not collected any log from your container. In this case, check the container status and perform the following steps:

1. Check whether the machine group status is normal.

2. Check whether the Config identifier is correct.

    Check whether `IncludeLab el`, `ExcludeLab el`, `IncludeEnv`, and `ExcludeEnv` in the Config match the configurations of the target container.

    📋 Note:

    `Label` indicates the container label (label information in `docker inspect`) instead of the one defined in Kubernetes. You can temporarily remove the parameters and check whether any log can be collected. If yes, the exception is caused by an incorrect Config identifier.

3. Check other items.

   If you want to collect files from your container, note that:

   · Logtail does not collect any file if there are no modified files in your container.

   · Only the files that are stored by default or mounted to your local PC can be collected.

Log on to the Logtail container

· **Common Docker**

  1. On the host, run `docker  ps  |  grep  logtail` to search for the Logtail container.

  2. Run `docker  exec  - it  ****** bash` to log on to the Logtail container.

```
$ docker  ps  |  grep  logtail
 223fbd3ed2  a6e           registry . cn - hangzhou . aliyuncs . com
/ log - service / logtail                        "/ usr /
 local / ilogta ..."   8   days   ago        Up   8   days
                        logtail - iba
$ docker  exec  - it  223fbd3ed2  a6e  bash
```

· **Kubernetes**

  1. Run `kubectl  get  po  - n  kube - system  |  grep  logtail` to search for the Logtail Pod.

  2. Run `kubectl  exec  - it  - n  kube - system  ****** bash` to log on to the Pod.

```
$ kubectl  get  po  - n  kube - system  |  grep  logtail
 logtail - ds - g5wgd
 1 / 1        Running    0          8d
 logtail - ds - slpn8
 1 / 1        Running    0          8d
$ kubectl  exec  - it  - n  kube - system  logtail - ds - g5wgd
 bash
```

View Logtail operational logs

Logtail logs named *ilogtail . LOG* and *logtail_pl ugin . LOG* are stored in the */ usr / local / ilogtail /* directory.

1. Log on to the Logtail container.

2. Open the */ usr / local / ilogtail /* **directory.**

```
cd  / usr / local / ilogtail
```

3. **View the** *ilogtail . LOG* **and** *logtail_pl ugin . LOG* **files.**

```
cat   ilogtail . LOG
cat   logtail_pl  ugin . LOG
```

View Logtail standard output (stdout)

You can ignore the following stdout because the container stdout has no reference for application.

```
start    umount    useless    mount    points , / shm $|/ merged $|/
mqueue $
umount : / logtail_ho  st / var / lib / docker / overlay2 /
3fd0043af1  74cb0273c3  c7869500fb  e2bdb95d13  b1e110172e
f57fe840c8  2155 / merged :  must    be    superuser    to    unmount
umount : / logtail_ho  st / var / lib / docker / overlay2 /
d5b10aa193  99992755de  1f85d25009  528daa749c  1bf8c16edf
f44beab6e6  9718 / merged :  must    be    superuser    to    unmount
umount : / logtail_ho  st / var / lib / docker / overlay2 /
5c3125dadd  acedec29df  72ad0c52fa  c800cd56c6  e880dc4e8a
640b1e16c2  2dbe / merged :  must    be    superuser    to    unmount
......
xargs :  umount :  exited    with    status    255 ;  aborting
umount    done
start    logtail
ilogtail   is    running
logtail    status :
ilogtail   is    running
```

View the status of log-related components in a Kubernetes cluster

To view the status of log-related components in a Kubernetes cluster, you can run

```
helm    status    alibaba - log - controller .
```

View the version information, IP address, and time of Logtail

The related information is stored in the *app_info . json* file under the */ usr / local / ilogtail /* directory in the Logtail container. The following is an example:

```
kubectl   exec   logtail - ds - gb92k  - n   kube - system    cat  /
usr / local / ilogtail / app_info . json
{
   " UUID " : "",
   " hostname " : " logtail - gb92k ",
   " instance_i  d " : " 0EBB2B0E - 0A3B - 11E8 - B0CE - 0A58AC1404
02_172 . 20 . 4 . 2_15178109  40 ",
   " ip " : " 172 . 20 . 4 . 2 ",
   " logtail_ve  rsion " : " 0 . 16 . 2 ",
   " os " : " Linux ;  3 . 10 . 0 - 693 . 2 . 2 . el7 . x86_64 ; # 1
SMP   Tue   Sep   12   22 : 26 : 13   UTC   2017 ;  x86_64 ",
   " update_tim  e " : " 2018 - 02 - 05   06 : 09 : 01 "
```

```
    }
```

What do I do if I mistakenly delete a Logstore that is created through CRD?

If you delete a Logstore that is automatically created through CRD, the collected data cannot be recovered, and the CRD configurations of the Logstore become invalid. In this case, you can use either of the following methods to prevent possible log collection exceptions:

- Use another CRD-created Logstore and take care to name the Logstore with a different name to the Logstore that was mistakenly deleted.
- Restart the `alibaba - log - controller` Pod. You can run `kubectl    get    po  - n   kube - system  |  grep   alibaba - log - controller` to search for the Pod.

2 Log query

2.1 What can cause an inaccurate query result to return?

When you query or analyze logs, a message indicating The results are inaccurate. may be displayed. This is displayed when only partial logs are scanned for query and analysis results, meaning the results do not include scans of full-log queries or analysis, and are therefore considered inaccurate.

Possible causes include:

1. The time range for queries is excessive.

Cause: The time range for queries is excessively wide, for example, three months or a year. In this case, Log Service cannot scan all logs generated within this time period.

Solution: Narrow down the time range for queries and perform multiple queries.

2. The query condition is exceedingly complex.

Cause: The query condition is exceedingly complex, or Log Service cannot read query results because the query condition contains multiple frequently used words.

Solution: Narrow down the query scope and perform multiple queries.

3. The SQL database reads an abnormally large amount of data.

Cause: The SQL database reads an abnormally large amount of data, which leads to inaccurate query results. For example, if the SQL database reads strings from multiple columns, it can read only 1 GB of data from each Shard. If this threshold is exceeded, inaccurate query results will be returned.

Solution: Narrow down the query scope and perform multiple queries.

2.2 How do I configure an index for a historical log?

Log Service cannot configure indexes for historical logs directly. However, you can rewrite the logs into a new Logstore through DataWorks or use CLI commands to configure indexes as needed.

Indexes are valid only for the logs that are collected after index configuration, and historical logs cannot be queried or analyzed. If you want to configure indexes for historical logs, use either of the following methods:

· Rewrite data into a new Logstore through DataWorks and then configure indexes.

  After configuring an index for the new Logstore, use DataWorks to export historical logs from the old Logstore and then import them to the new Logstore. By dong so, you can query and analyze historical logs.

· Rewrite data into the Logstore through CLI commands and then configure indexes.

  Use a command-line tool to rewrite logs into the Logstore to configure indexes.

  For more information, see Aliyun Log Service CLI.

> Note:
>
> Both the methods achieve index configuration through data duplication and import, which does not change or delete existing historical logs.

3 Alarm

3.1 Alarm configuration examples

This topic describes typical examples of alarm configurations.

Set the alarm notification to contain the error logs for which an alarm is set

Scenario: If the number of error logs exceed 5 within five minutes, an alarm is triggered and the alarm notification contains the error logs.

Configuration solution

- Statements associated with the alarm.

  - Sequence number 0: indicates `level : ERROR`.

  - Sequence number 1: indicates `level : ERROR | select COUNT (*) as count`.

- The condition for triggering the alarm is `$ 1 . count > 5`.

- The notification content is `${ results [ 0 ]. rawresults }`.

4 Pricing

4.1 Disable Log Service

If you no longer require Log Service, you can delete all data to disable Log Service.

Context

If you no longer require Log Service, you can delete all projects and Logstores to delete logs.

> 📋 Note:
>
> · A storage fee is still calculated on the day when you delete the logs, and you will receive a bill for the storage fee the next day. However, you will not continue to receive any bill thereafter.
>
> · After a project is deleted, all logs and configurations in the project will be permanently released and cannot be recovered. Therefore, we recommend that you exercise caution when performing this action.

Procedure

1. Log on to the Log Service Console.

2. On the Projects page, find the project you want to delete.

3. Click Delete.

4.2 Billing-related FAQ

FAQ list:

1. What should I do if I have overdue payment in Log Service?

2. I only created projects and Logstores. Why do I have a bill?

3. How do I disable Log Service?

4. Will any write or read traffic be generated on the Internet if I query and analyze logs in the console?

1. What should I do if I have overdue payment in Log Service?

Log Service charges resources in pay-as-you-go mode. It generates a bill every day and automatically deducts fees. The bill lists the resources that you used on the last

day. If the bill is overdue for more than 24 hours, Log Service automatically stops to
provide services for you. However, it still charges you for the storage space that you
are using, and the overdue amount increases. We recommend that you pay off the
overdue bill within 24 hours to avoid any business loss caused by service interruption
. You can continue to use Log Service after paying off the overdue bill.

2. I only created projects and Logstores. Why do I have a bill?

If you have created a project and a Logstore, shards are created by default to reserve
resources. As indicated on the page when you create a Logstore, Log Service charges
a small amount of resource reservation fees for shards. Based on the current billing
policy, you can use a shard free of charge for 31 days. If you create two shards, they
are charged after 15 days. You can delete the project and Logstore if you no longer
need the shards. If you delete the resources, Log Service sends you the bill of resource
usage the next day. You will not receive any project bills from the third day.

3. How do I disable Log Service?

If you no longer need Log Service, you can delete all the projects under your account
. In this case, Log Service is disabled. You will not be charged from the next day. If
you have overdue payment, pay off the overdue bill and delete the projects. If no Log
Service services or resources exist under your account, you will not receive any Log
Service bills from the third day.

4. Will any write or read traffic be generated on the Internet if I query and analyze logs in the
console?

If you perform any operations in the console, for example, you query and analyze logs
, you access Log Service on the intranet. Your intranet access does not generate write
or read traffic on the Internet. Therefore, no such traffic is billed.