Alibaba Cloud
Log Service

V

Issue: 20190814

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 Monitor Log Service

You can view the monitoring data of Log Service in the CloudMonitor console or Log Service console.

- In the CloudMonitor console, you can view:
  - Log reading/writing in Logstores
  - Logs collected by agents (Logtail)
- In the Log Service console, you can view:
  - Current point of real-time subscription consumption (Spark Streaming, Storm, and consumer library)
  - Log shipping status

This document describes how to view monitoring data in the Alibaba Cloud CloudMonitor console. For how to view monitoring data in the Log Service console, see View consumer group status, Manage LogShipper tasks and Configure an alarm.

Procedure

> Note:
> You must authorize the sub-accounts before using them to configure the cloud monitoring.

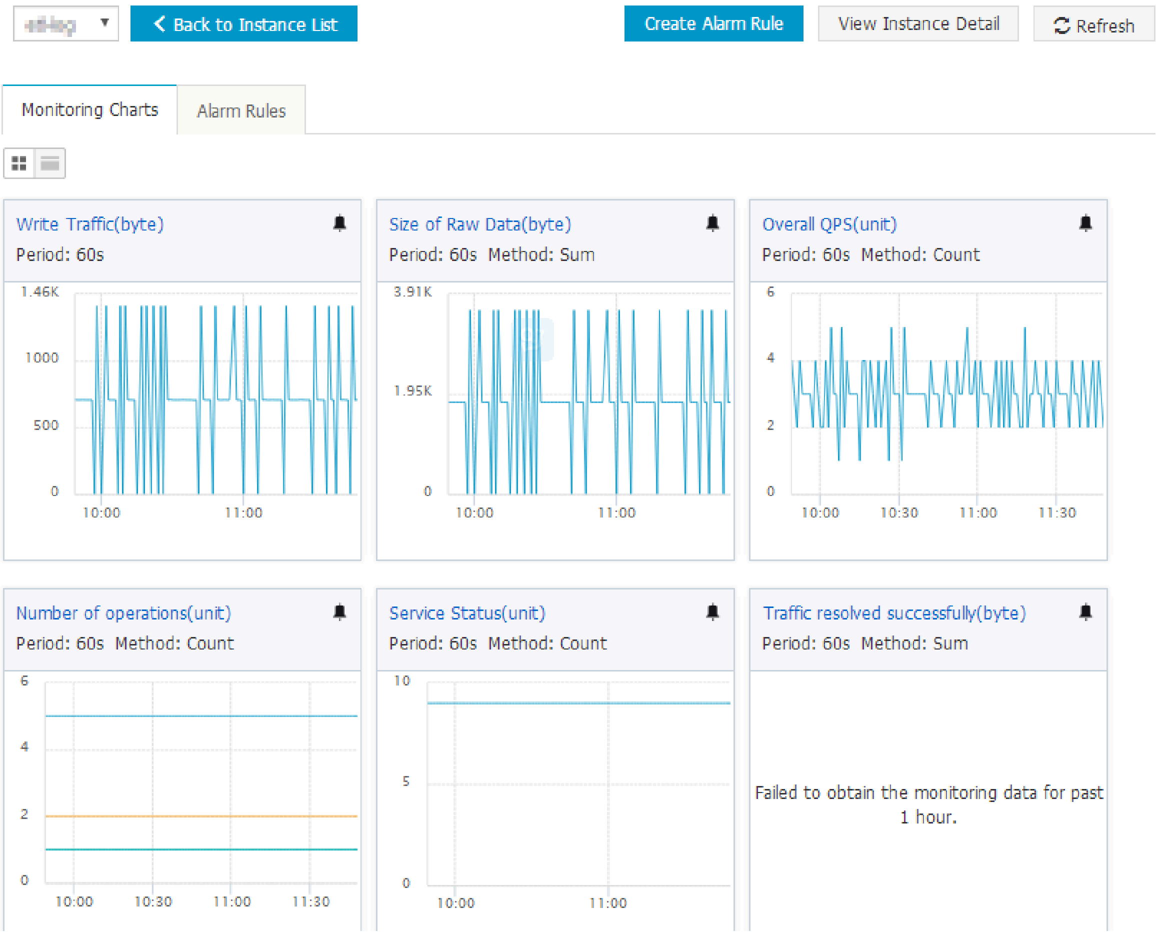
1. Log on to the Log Service console.
2. On the Project List page, click the project name.

3. Click the Monitor icon at the right of the Logstore to enter the CloudMonitor console.

   You can log on to the CloudMonitor console directly and then click Cloud Service > Log Servicein the left-side navigation pane to enter the monitoring configuration page.

   Monitor the log data in CloudMonitor. For more information, see Log Service monitoring.

   Figure 1-1: Monitoring item description



See

Log Service monitoring metrics.

Set alarm rules

Click Create Alarm Rule in the upper-right corner of the Monitoring Charts page. Configure the related resource, alarm rules, and notification method. For more information, see Use CloudMonitor to set alarm rules.

2 Service log

2.1 Service log overview

Alibaba Cloud Log Service provides the service log function, which supports recording various types of logs (including operational logs) and provides several dashboards for a variety of analysis dimensions. This function can help you gain real-time insights into the resource usage of Log Service, allowing you improve your overall O&M efficiency.

Limits

- A dedicated Logstore only stores logs generated by Log Service and does not support reading other data. Currently, there are no limits for queries, statistics, alarms, and stream consumption.
- RAM users can activate Log Service only after they are authorized by their corresponding Alibaba Cloud accounts.
- Logs generated by a Project can be stored in other Projects that are in the same region. However, storage across regions is not currently supported.
- Logs generated by the service log function follows the standard pricing policy of Log Service. The billing method is Pay-As-You-Go and a free quota is provided each month. For more information, see Billing method.
- If you want to disable the service log function, you can deselect the service logs check box of the Enable Operations Logs field. Log Service then forbids service log writing but retains historical service logs, which may result in fees. If you want to delete historical service logs, you can directly delete the Logstore that stores the logs.

Default configurations

Table 2-1: Default configurations

Default configuration item	Details
Logstore	By default, Log Service creates five Logstores for you, each of which stores a different log type. For example: · `internal - operation_ log` : Records operational logs and stores them for 30 days by default. This log type uses the common billing method. · `internal - diagnostic _log` : Records metering logs, consumption group delays, and Logtail-related logs based on topics. This Logstore stores the logs and information for 30 days by default and can be used free of charge. For more information about log types and fields, see Log types.
Region	· If you select Automatic creation (recommended) for the Log Storage field, Log Service creates a Project within the same region. · Service logs can be stored only in Projects within the current region.
Shard	By default, Log Service creates two Shards for each Logstore and enables the automatic sharding function.
Log storage duration	By default, logs are stored for 30 days. However, you can modify this setting. For more information, see Manage a Logstore.
Index	By default, the index function is enabled for all collected logs. If you do not need query, analysis, or alarm settings, you can disable the index function on the query page.

Default configuration item	Details
Dashboard	By default, Log Service creates five dashboards pertaining to the following: · User operations · Metering data · Logtail log collection · Logtail exception monitoring · Consumer group monitoring For more information, see Dashboards.

Scenarios

- View metering data

  After you Log Service, Log Service immediately begins to calculate the storage space occupied by logs and indexes on an hourly basis and collects billing data (including the number of read and write operations and index traffic) for the current collection period and stores this information as metering logs. Metering logs are then stored in an independent Logstore. You can view the collected metering logs to gain insight into your storage and consumption information.

- Balance Shard writers and your overall consumption

  You can compare write operations into Shards and overall consumption trends through predefined dashboards to determine whether your Shard write operations and consumption are balanced.

  If there are multiple Logstores under a Project, the same Shards may be repeated for several Logstores. In such case, if you want to view the write distribution of a Shard in a specific Logstore, you can add the target Project and Logstore as filter conditions in the upper-left corner of the dashboard.

- Monitor API request status

  All user operations (such as log writes, consumption, and the creation of Projects and Logstores) are performed through API requests. Every user operation generates a log in the internal-operation_log Logstore.

  If a request fails, the `Status` field of the corresponding log is of a 3xx, 4xx, or 5xx status code. Therefore, you can determine whether API requests are normal by monitoring the number of logs with a `Status` field of the preceding code formats.

- View the Logtail status

  By default, Log Service creates two Logtail-related dashboards, which are used for exception monitoring and data statistics. The exception monitoring dashboard shows specific exceptions, such as log parsing failure and regular expression mismatch.

2.2 Feature enabling, disabling, and configuration

You can enable or disable the service log feature and change the logging settings for a specified project in the project list. Log Service stores all the logs generated for the project to a new or existing project. By default, the service log feature is disabled.

Prerequisites

1. Projects are created.
2. Permissions are granted to a RAM user from your Alibaba Cloud account if you log on to the Log Service console as the RAM user.

Background

Log Service provides the service log feature to record operations logs and other logs (such as Logtail alert logs) of a specified project. Log Service stores the logs in a new or exiting project. Log Service automatically creates Logstores in your specified storage location to separately store operations logs and other logs. Log Service also provides five dashboards for various log scenarios so that you can view and monitor the running status of Log Service in real time.

Note:

- After you enable the service log feature, Log Service creates Logstores and dashboards in your specified storage location. The Logstore used to store operations logs is charged based on your specified billing method. The Logstore used to store other logs can be used free of charge.
- We recommend that you store logs generated within the same region in the same project that is automatically created by Log Service.
- Only service logs generated after feature enabling are recorded.

Enable the service log feature

1. Log on to the Log Service console and find the target project.
2. In the Actions column, click Operations Log.
3. In the Enable Operations Log dialog box that appears, select the type of logs that you want to record in the Enable Operations Log field.

   You can select the Operations logs and Other logs check boxes as required.

   - Operations logs: record all operations performed on resources in the target project, including the creation, modification, update, deletion, write, and read operations. These logs are stored in the internal-operation_log Logstore of the target project.
   - Other logs: include metering logs, logs about delayed consumption in a consumer group, and Logtail-related error, heartbeat, and statistical logs in each Logstore. These logs are stored in the internal-diagnostic_log Logstore of the target project.
4. Set Log Storage.
   - If you select Automatic creation (recommended), Log Service automatically creates a project named `log - service -{ User ID }-{ Current region }` in the same region as the target project. We recommend that you store logs generated within the same region in this created project.
   - If you select an existing project, Log Service stores service logs in this project.
5. Click Confirm.

   The service log feature is enabled. Log Service records the logs generated for the target project in the specified location in real time.

Change the log type and storage location

1. Log on to the Log Service console with your Alibaba Cloud account and find the target project.
2. In the Actions column, click Operations Log.
3. Change the log type.

   Select or clear the Operations logs or Other logs check box as required in the Enable Operations Log field.

4. Change the value of Log Storage.

   In the Log Storage drop-down list, select another project.

   > Note:
   >
   > - We recommend that you store service logs in the project that is automatically created by Log Service. We also recommend that you store logs generated within the same region in the same project.
   > - After you change the value of Log Storage, new log data is stored in the specified project. The log data and dashboards stored in the original project are not automatically deleted or migrated to the newly specified project. If you no longer need the data, you can manually delete it.

Disable the service log feature

> Note:
>
> After the service log feature is disabled, the log data and dashboards stored in the project are not automatically deleted. If you no longer need the log data, you can manually delete the project or Logstore that stores the log data.

1. Log on to the Log Service console with your Alibaba Cloud account and find the target project.
2. In the Actions column, click Operations Log.
3. Clear both the Operations logs and Other logs check boxes.
4. Click Confirm.

Authorize a RAM user

Before using the service log feature with a RAM user, you must obtain necessary permissions from your Alibaba Cloud account. For more information, see Grant RAM sub-accounts permissions to access Log Service. The following code lists the permission policies:

```
{
  " Version ": " 1 ",
  " Statement ": [
    {
      " Action ": [
        " log : CreateDash  board ",
        " log : UpdateDash  board "
      ],
      " Resource ": " acs : log :*:*: project /{ Project   where
 logs   are   stored }/ dashboard /*",
      " Effect ": " Allow "
    },
    {
      " Action ": [
        " log : GetProject ",
        " log : CreateProj  ect ",
        " log : ListProjec  t "
      ],
      " Resource ": " acs : log :*:*: project /*",
      " Effect ": " Allow "
    },
    {
      " Action ": [
        " log : List *",
        " log : Create *"
        " log : Get *",
        " log : Update *",
      ],
      " Resource ": " acs : log :*:*: project /{ Project   where
 logs   are   stored }/ logstore /*",
      " Effect ": " Allow "
    },
    {
      " Action ": [
        " log :*"
      ],
      " Resource ": " acs : log :*:*: project /{ Project   for   which
   the   service   log   feature   is   enabled }/ logging ",
      " Effect ": " Allow "
    }
  ]
}
```

2.3 Log types

The service log function records multiple log types. This topic describes the fields used by each type of log in detail.

Log types

When you enable the service log function, you can choose one of the following log types:

- Operational logs: Record all operations to yourresources in a Project, including create, modify, delete, update, write, and read operations. They are stored in the internal-operation_log Logstore of a specified Project.
- Other logs: Include metering logs at a Logstore granularity, which are consumption group delay logs, Logtail error information, heartbeat information, and statistical logs. They are stored in the internal-diagnostic_log Logstore of a specified Project.

Log type	Logstore	Log source	Description
Operational logs	internal-operation_log	User operational logs	All API requests and operational logs, including requests sent from consoles, consumer groups, SDKs, and clients.
Other logs	internal-diagnostic_log	Consumer group snapshot logs	The consumption delay logs of a consumption group, which are reported every 2 minutes. To query snapshot logs of a certain consumption group, you need to specify `__topic__ : consumergroup_log` in the query statement.
		Logtail alarm logs	The Logtail error logs, which are recorded every 30 seconds. The errors of the same type occurring within 30 seconds only accumulate the total number of errors, but only one error message is randomly selected and sent. To query a certain alarm log, you need to specify `__topic__ : logtail_alarm` in the query statement.
		Logtail collection logs	The Logtail collection logs, which are recorded every 10 minutes. To query a certain Logtail collection log, you need to specify `__topic__ : logtail_profile` in the query statement.

Log type	Logstore	Log source	Description
		Metering logs	The user metering logs, which are collected every hour. The logs include information relating to storage space at a Logstore granularity, read and write traffic, index traffic, and the number of requests. To query a certain metering log, you need to specify `__topic__ : metering` in the query statement.
		Logtail status logs	The status logs that are regularly reported by Logtail. The logs are recorded every minute. To query a certain Logtail status log, you need to specify `__topic__ : logtail_st atus` in the query statement.

User operational logs

Operational logs involve data read and write operations and other operations on various resources according to the `Method` field.

Type	Method
Data read operations	By calling the following APIs: · GetLogStoreHistogram · GetLogStoreLogs · PullData · GetCursor · GetCursorTime
Data write operations	By calling the following APIs: · PostLogStoreLogs · WebTracking
Other operations on resources	By calling the CreateProject and DeleteProject APIs.

Common fields

The following table lists common fields that can be used by various operations.

Field	Description	Example
APIVersion	The API version	0.6.0
InvokerUid	The account ID of the user who performs the operation	1759218115323050
NetworkOut	The inbound Internet read traffic in bytes	10
Latency	The request delay in microseconds	123279
LogStore	The name of a Logstore	logstore-1
Method	The method being used	GetLogStoreLogs
Project	The name of a Project	project-1
NetOutFlow	The read traffic in bytes	120
RequestId	The request ID	8AEADC8B0AF2FA2592C9509E
SourceIP	The IP address of the client that sent the request	1.2.3.4
Status	The response status code	200
UserAgent	The user agent on the client	sls-java-sdk-v-0.6.1

Data read fields

The following tables lists the fields specific to read requests.

Field	Description	Example
BeginTime	The request start time in Unix timestamps	1523868463
DataStatus	The response status, including `Complete` , `OK` , and `Unknown` .	OK
EndTime	The request end time in Unix timestamps	1523869363

Field	Description	Example
Offset	The offset of the GetLog request	20
Query	The original query statement	UserAgent: [consumer-group-java]*
RequestLines	The number of lines that are expected to be returned	100
ResponseLines	The number of lines of the query results	100
Reverse	Indicates whether to return logs in reverse order of log timestamps, where: · 1 indicates the reverse order. · 0 indicates the normal order. The default value is 0.	0
TermUnit	The number of words included in a search statement	0
Topic	The name of the read topic	topic-1

Data write fields

The following tables lists the fields specific to write requests.

Field	Description	Example
InFlow	The number of the original write bytes	200
InputLines	The number of requested write lines	10
NetInflow	The number of write bytes after compression	100
Shard	The ID of the Shard to which data is written	1

Field	Description	Example
Topic	The name of the topic to which data is written	topic-1

Consumption group snapshot logs

Field	Description	Example
consumer_group	The name of a consumption group	consumer-group-1
fallbehind	The period of time from the current consumption point to the most recent write log (in seconds)	12345
logstore	The name of a Logstore	logstore-1
project	The name of a Project	project-1
shard	The ID of a Shard	1

Logtail alarm logs

Field	Description	Example
alarm_count	The number of alarms in the sampling window	10
alarm_message	The sample of original logs that triggered the alarm	M_INFO_COL,all_status_monitor,T22380,0,2018-04-17 10:48:25.0,AY66K,AM5,2018-04-17 10:48:25.0,2018-04-17 10:48:30.561,i-23xebl5ni.1569395.715455,901,00789b
alarm_type	The alarm type	REGISTER_INOTIFY_FAIL_ALARM
logstore	The name of a Logstore	logstore-1
source_ip	The IP address of the server at which Logtail runs	1.2.3.4
os	The operating system, such as Linux or Windows	Linux
project	The name of a Project	project-1

Field	Description	Example
version	The Logtail version	0.14.2

Logtail collection logs

Based on the `file_name` field, Logtail collection logs can be divided into two types: single-file statistics and Logstore-level logs. For the second type, `logstore_statistics` in `file_name` indicates that the log collects statistics for the entire Logstore. For this log type, file-related fields, such as `file_dev` and `file_inode`, can be disregarded. The following tables lists fields that are used in Logtail collection logs.

Field	Description	Example
logstore	The name of a Logstore	logstore-1
config_name	The name of a Logtail Config, which is unique and consists of `## Config version##Project name$Config name`.	##1.0##project-1$logstore-1
error_line	The raw log that caused the error	M_INFO_COL,all_status_monitor,T22380,0,2018-04-17 10:48:25.0,AY66K,AM5,2018-04-17 10:48:25.0,2018-04-17 10:48:30.561,i-23xebl5ni.1569395.715455,901,00789b
file_dev	The device ID of the log file	123
file_inode	The inode of the log file	124
file_name	The storage path of the log file or `logstore_statistics`	/abc/file_1
file_size	The size of the log file (in bytes)	12345
history_data_failures	The number of historical processing failures	0
last_read_time	The latest read time in the window (in Unix timestamps)	1525346677

Field	Description	Example
project	The name of a Project	project-1
logtail_version	The Logtail version	0.14.2
os	The OS	Windows
parse_failures	The number of lines with a parsing failure in the log in the current window	12
read_avg_delay	The average value of the difference between the offset at every read and the file size in the current window	65
read_count	The number of log reads in the current window	10
read_offset	The offset of the current file read (in bytes)	12345
regex_match_failures	The number of regular expression matching failures	1
send_failures	The number of request sending failures in the current window	12
source_ip	The IP address of the server where Logtail runs	1.2.3.4
succeed_lines	The number of log lines that are successfully processed	123
time_format_failures	The number of log time matching failures	122
total_bytes	The total number of reads (in bytes)	12345

The following table lists the fields that are valid only when `file_name` is `logstore_s tatistics`.

Field	Description	Example
send_block_flag	Indicates whether the sending queue is blocked at the end of the window.	false
send_discard_error	The number of discarded data packets due to data exceptions or permission unavailability in the current window	0
send_network_error	The number of data packets that were not sent due to network errors in the current window	12
send_queue_size	The number of unsent data packets in the current send queue at the end of the window	3
send_quota_error	The number of data packets that were not sent due to quota insufficiency in the current window	0
send_success_count	The number of data packets that are successful ly sent in the current window	12345
sender_valid_flag	Indicates whether the sending flag of the current Logstore is valid at the end of the window, where: · The value `true` indicates that the flag is valid. · The value `false` indicates that the flag may be forbidden due to network or quota errors.	true

Field	Description	Example
max_send_success_time	The maximum time period during which data can be successfully sent in the window (in Unix timestamps)	1525342763
max_unsend_time	The maximum time period during which no data is sent in the sending queue at the end of the window (in Unix timestamps). The field is 0 when the queue is empty.	1525342764
min_unsend_time	The minimum time period during which no data is sent in the sending queue at the end of the window (in Unix timestamps). The field is 0 when the queue is empty.	1525342764

Metering logs

Field	Description	Example
begin_time	The start time of a statistics window (in Unix timestamps)	1525341600
index_flow	The index traffic in the statistics window (in bytes)	12312
inflow	The write traffic in the statistics window (in bytes)	12345
logstore	The name of a Logstore	logstore-1
network_out	The outbound traffic from the statistics window to the Internet (in bytes)	12345
outflow	The read traffic in the statistics window (in bytes)	23456
project	The name of a Project	project-1

Field	Description	Example
read_count	The number of data reads in the statistics window	100
shard	The average number of Shards used in the statistics window	10.0
storage_index	The total amount of the index storage in a Logstore at the statistics time point (in bytes)	10000000
storage_raw	The total number of logs in a Logstore at the statistics time point (in bytes)	20000000
write_count	The number of data writes in the statistics window	199

Logtail status logs

Field	Description	Example
cpu	The load of a CPU	0.001333156
hostname	The host name	abc2.et12
instance_id	The instance ID, which is randomly assigned	05AFE618-0701-11E8-A95B-00163E025256_10.11.12.13_1517456122
ip	The IP address	1.0.1.0
load	The average system load	0.01 0.04 0.05 2/376 5277
memory	The amount of the memory occupied by the Logtail process (in MB)	12
detail_metric	The value of a metered item (in JSON format). For more information, see detail_metric.	detail_metric
os	The OS	Linux
os_cpu	The overall CPU usage	0.004120005
os_detail	Details relating to the OS	2.6.32-220.23.8.tcp1.34.el6.x86_64

Field	Description	Example
status	The client status, which can be: · ok · busy · many_log_files · process_block · send_block · send_error For more information, see Logtail Run Status.	busy
user	The user name	root
user_defined_id	The user-defined ID	aliyun-log-id
uuid	The UUID of the server	64F28D10-D100-492C-8FDC-0C62907F1234
version	The Logtail version	0.14.2
project	The Project to which the Logtail Config belongs	my-project

The following table lists the fields that are included in `detail_metric`.

Field	Description	Example
config_count	The number of Logtail Configs	1
config_get_last_time	The time when the Config information was last obtained	1525686673
config_update_count	The number of Config updates after Logtail is started	1
config_update_item_count	The total number of configuration item updates after Logtail is started	1
config_update_last_time	The time when the Config is last updated after Logtail is started	1
event_tps	The TPS	1

Field	Description	Example
last_read_event_time	The time when the event was last obtained	1525686663
last_send_time	The time when data was last sent	1525686663
open_fd	The number of files that are currently open	1
poll_modify_size	The number of files with listener modification events	1
polling_dir_cache	The number of scanned folders	1
polling_file_cache	The number of scanned files	1
process_byte_ps	The number of logs processed per second (in bytes)	1000
process_lines_ps	The number of logs processed per second	1000
process_queue_full	The number of sending queues that have reached the maximum queue length	1
process_queue_total	The number of processing queues	10
process_tps	The processing TPS	0
reader_count	The number of files being processed	1
region	The region to which Logtail belongs	cn-hangzhou,cn-shanghai
register_handler	The number of folders registered with listeners	1
send_byte_ps	The number of raw logs sent per second (in bytes)	11111
send_line_ps	The number of logs sent per second	1000

Field	Description	Example
send_net_bytes_ps	The amount of network data sent per second (in bytes)	1000
send_queue_full	The number of sending queues that have reached the maximum queue length	1
send_queue_total	The number of sending queues	12
send_tps	The sending TPS	0.075
sender_invalid	The number of abnormal sending queues	0

2.4 Service log dashboards

After the service log function is enabled, Log Service automatically creates five dashboards for displaying statistics relating to user operations, metering, Logtail log collection, Logtail exception monitoring, and consumption group monitoring.

Dashboard description

When enabling the service log function, you can choose from the following log types:

- If you select Operational logs, Log Service creates an operation statistics dashboard, displaying the statistics for the number of requests and the proportion of request failures on the current day.
- If you select Other logs, Log Service creates dashboards for displaying metering statistics, Logtail log collection statistics, Logtail running monitoring, and consumption group monitoring.

Operation statistics dashboard

This dashboard displays user access and operation information, such as the queries per second (QPS) and request delay for API requests and other operations on any of the resources under a Project.

Metering statistics dashboard

This dashboard displays metering statistics, which include data storage, index traffic, data read and write operations, and read and write traffic.

Logtail log collection statistics dashboard

This dashboard displays statistics relating to Logtail log collection.

Logtail running monitoring dashboard

This dashboard displays statistics for Logtail errors and alarms for you to monitor the health status of Logtail in real time.

Consumption group monitoring dashboard

This dashboard displays statistics for consumption groups, including Shard consumption data, consumption delays, and the consumption group list.

3 Log moniroring by CloudMonitor

3.1 Log Service monitoring metrics

For details about metric data, see Monitor Log Service.

1. Read/Write traffic
   - Meaning: Data traffic that is written to and read from each Logstore in real time . It makes statistics on the traffic that is written to and read from the specified Logstore through iLogtail, SDKs, and APIs in real time. The traffic volume is the volume of transferred data (or compressed data). The measurement period is one minute.
   - Unit: Bytes/min
2. Raw data size
   - Meaning: Volume of the raw data (before compression) written to each Logstore.
   - Unit: Byte/min
3. Total QPS
   - Meaning: Number of QPSs of all operations. The measurement period is one minute.
   - Unit: Count/min

4. Operation count

   - Meaning: Number of QPSs of various operations types. The measurement period is one minute.
   - Unit: Count/min
   - The following types of operations are measured:

     - Write:

       - PostLogStoreLogs: API later than 0.5
       - PutData: API earlier than 0.4
     - Keyword query:

       - GetLogStoreHistogram: Query of keyword distribution, which is an API later than 0.5.
       - GetLogStoreLogs: Query of keyword-matched logs, which is an API later than 0.5.
       - GetDataMeta: Same as GetLogStoreHistogram, which is an API earlier than 0.4.
       - GetData: Same as GetLogStoreLogs, which is an API earlier than 0.4.
     - Batch data acquisition:

       - GetCursorOrData: obtains cursors and data in batches.
       - ListShards: obtains all shards in a Logstore.
     - List:

       - ListCategory: same as ListLogStoreLogs, which is an API earlier than 0.4
       - ListTopics: traverses all topics in a Logstore.
5. Service status

   - Meaning: This view collects statistics on the QPSs that correspond to the HTTP status codes returned for all types of operations. You can locate the operation exception based on the return error code and adjust programs in a timely manner.
   - Status codes:

     - 200: is the normal return code, indicating that the operation is successful.
     - 400: indicates an error of one of the following parameters: Host, Content-length, APIVersion, RequestTimeExpired, query time range, Reverse,

AcceptEncoding, AcceptContentType, Shard, Cursor, PostBody, Parameter, and ContentType.

- 401: indicates that authentication fails because the AccessKey ID does not exist, the signature does not match, or the signature account has no permission. Check whether the project permission list on SLSweb contains the AccessKey.
- 403: indicates a quota overrun. For example, the maximum number of Logstores, shards, or read/write operations per minute is exceeded. Locate the specific error based on the returned message.
- 404: indicates that the requested resource does not exist. Resources include projects, Logstores, topics, and users.
- 405: indicates that the operation method is incorrect. Check the URL of the request.
- 500: indicates a Log Service error. Please try again.
- 502: indicates a Log Service error. Please try again.

6. Traffic successfully parsed by the agent
   - Meaning: size of the logs (raw data) successfully collected by Logtail
   - Unite: byte
7. Number of lines successfully parsed by the agent (Logtail)
   - Meaning: number of logs (counted by lines) successfully collected by Logtail
   - Unit: line
8. Number of lines the agent fails to parse
   - Meaning: number of lines Logtail fails to collect due to an error. An error occurs if this view has data.
   - Unit: line
9. Agent error count
   - Meaning: number of IP addresses that encounter an error when Logtail collects logs
   - Unit: count
10. Number of machines with an agent error
   - Meaning: number of alarms that indicate a collection error when Logtail collects logs
   - Unit: count

11.IP address error count (measured every 5 minutes)

- Meaning: number of IP addresses under various collection error categories, including:
  - LOGFILE_PERMINSSION_ALARM: The agent has no permission to access the log file.
  - SENDER_BUFFER_FULL_ALARM: Data is discarded because the data collection speed exceeds the network transfer speed.
  - INOTIFY_DIR_NUM_LIMIT_ALARM (INOTIFY_DIR_QUOTA_ALARM): The number of monitored directories exceeds 3,000. Please set the monitored root directory to a lower-level directory.
  - DISCARD_DATA_ALARM: Data is lost because the data time is 15 minutes earlier than the system time. Ensure that the time of the data written to log files is less than 15 minutes before the system time.
  - MULTI_CONFIG_MATCH_ALARM: When multiple configurations are applied to collect the same file, Logtail selects a configuration randomly for collection and no data is collected by other configurations.
  - REGISTER_INOTIFY_FAIL_ALARM: Inotify event registration fails. For details , view the Logtail log.
  - LOGDIR_PERMINSSION_ALARM: The agent has no permission to access the monitored directory.
  - REGEX_MATCH_ALARM: regular expression match error. Please adjust the regular expression.
  - ENCODING_CONVERT_ALARM: An error occurs when the log encoding format is converted. For details, view the Logtail log.
  - PARSE_LOG_FAIL_ALARM: log parsing error, which may be due to an incorrect regular expression at the beginning of the line or incorrect log splitting by line because the size of a single log exceeds 512 KB. For details, view the Logtail log. Adjust the regular expression if it is incorrect.
  - DISCARD_DATA_ALARM: Data is discarded because Logtail fails to write the data to the local cached file when the data cannot be sent to the Log Service. The possible cause is that the speed at which log files are generated exceeds the speed at which data is written to the cached file.
  - SEND_DATA_FAIL_ALARM: Logtail fails to send parsed logs to the Log Service . For details, view the error code and message related to data sending failures

in the Logtail log. Common errors include Log Service quota overruns and network exceptions at the agent side.

- PARSE_TIME_FAIL_ALARM: An error occurs when the time field of the log is parsed. The time field parsed by Logtail using the regular expression cannot be parsed based on the time format configuration. Please modify the configuration.
- OUTDATED_LOG_ALARM: Logtail discards historical data. Ensure that the difference between the time of currently written data and the system time is less than 5 minutes.

- Locate the specific IP address based on the error. Log on to the machine and view the /usr/logtail/ilogtail.LOG file to identify the cause.

3.2 Use CloudMonitor to set alarm rules

Log Service allows you to use CloudMonitor to set alarm rules. An alarm SMS or email is sent when the service status meets the configured alarm rules. Configure the alarm rules to monitor Log Service in the CloudMonitor console. Then, you can monitor the log collection status of Logtail, shard usage status, and write traffic of projects.

Procedure

On the CloudMonitor console, click xCloudMonitor console > Log Serviceclick Alarm Rules at the right of the Logstore. Then, click Create Alarm Rule in the upper-right corner.

1. Configure the related resource.

   a. From the Products drop-down list, select Log Service.

   b. Select the resource range.

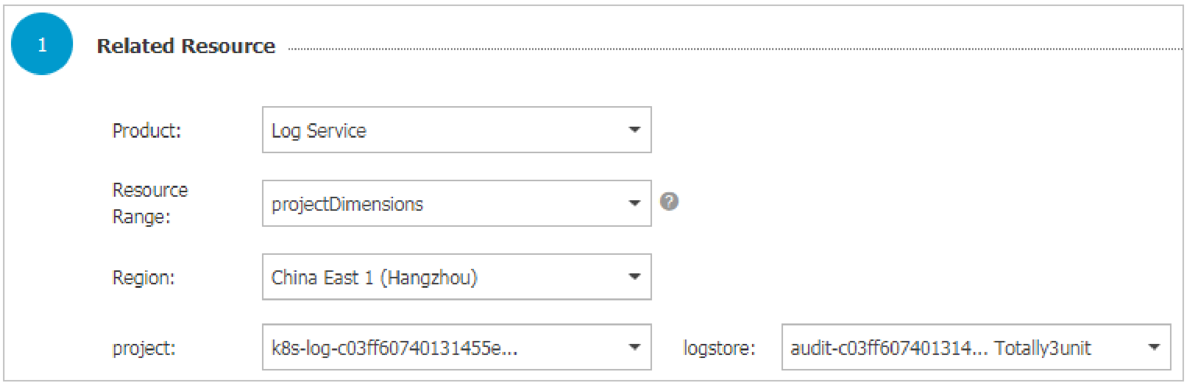
      You can select All Resources, Application Group, or projectDimensions.

      - All Resources – An alarm notification is sent when any instance in Log Service meets the alarm rules.
      - Application Group - An alarm notification is sent when any instance in an application group meets the alarm rules.
      - projectDimensions - An alarm notification is sent only when the selected instances meet the alarm rules.

   c. Select the region.

   d. Select one or more Projectand Logstore. You can select one or more projects and logstores.

Figure 3-1: Associated resources



1 Related Resource

Product: Log Service

Resource Range: projectDimensions

Region: China East 1 (Hangzhou)

project: k8s-log-c03ff60740131455e... logstore: audit-c03ff607401314... Totally3unit

2. Set the alarm rules.

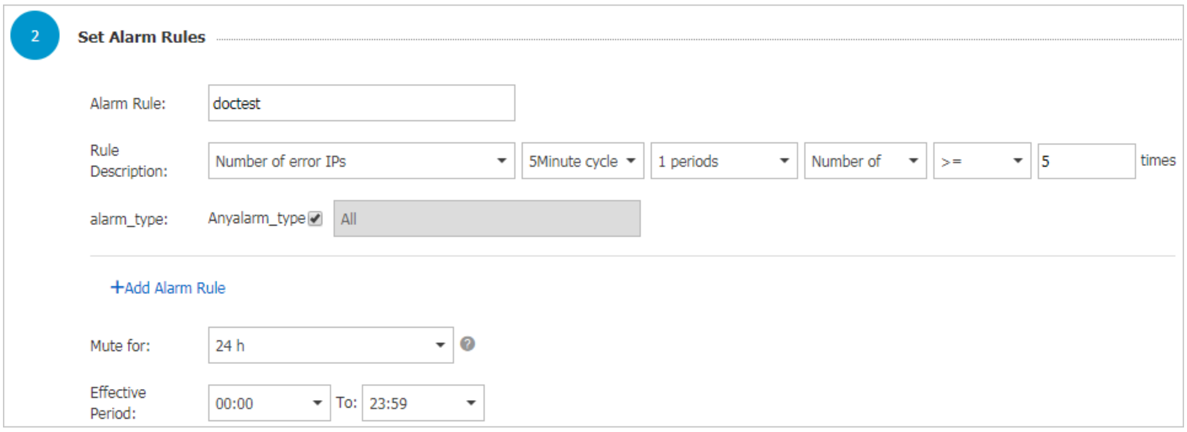
   You can set one or more alarm rules.

   a. Enter the alarm rule name.
   b. Configure the rule description.

      Define your monitoring policy here by selecting the monitoring item and configuring the threshold for the monitoring item. CloudMonitor sends an alarm notification when the threshold is exceeded.

      For more information about the description of each monitoring item, see Log Service monitoring metrics. For more information about the statistical method, see Monitor Log Service.
   c. Select thealarm_type. By default, Any alarm_type is selected.
   d. Set the mute time , which is the time interval between two alarm notifications if the condition that triggers the alarm is still abnormal after an alarm notification is sent.
   e. Select a number from the Triggered when threshold is exceeded for drop-down list. The alarm is triggered after the threshold is exceeded for the selected number of times successively, that is, the alarm is triggered after the alarm detection results meet your configured rule description for the selected number of times successively.
   f. Select the effective period for your monitoring policy.The monitoring alarm policy only works within the selected period.

Figure 3-2: Set alarm rules


2 Set Alarm Rules

Alarm Rule: doctest

Rule Description: Number of error IPs | 5Minute cycle | 1 periods | Number of | >= | 5 times

alarm_type: Anyalarm_type ☑ All

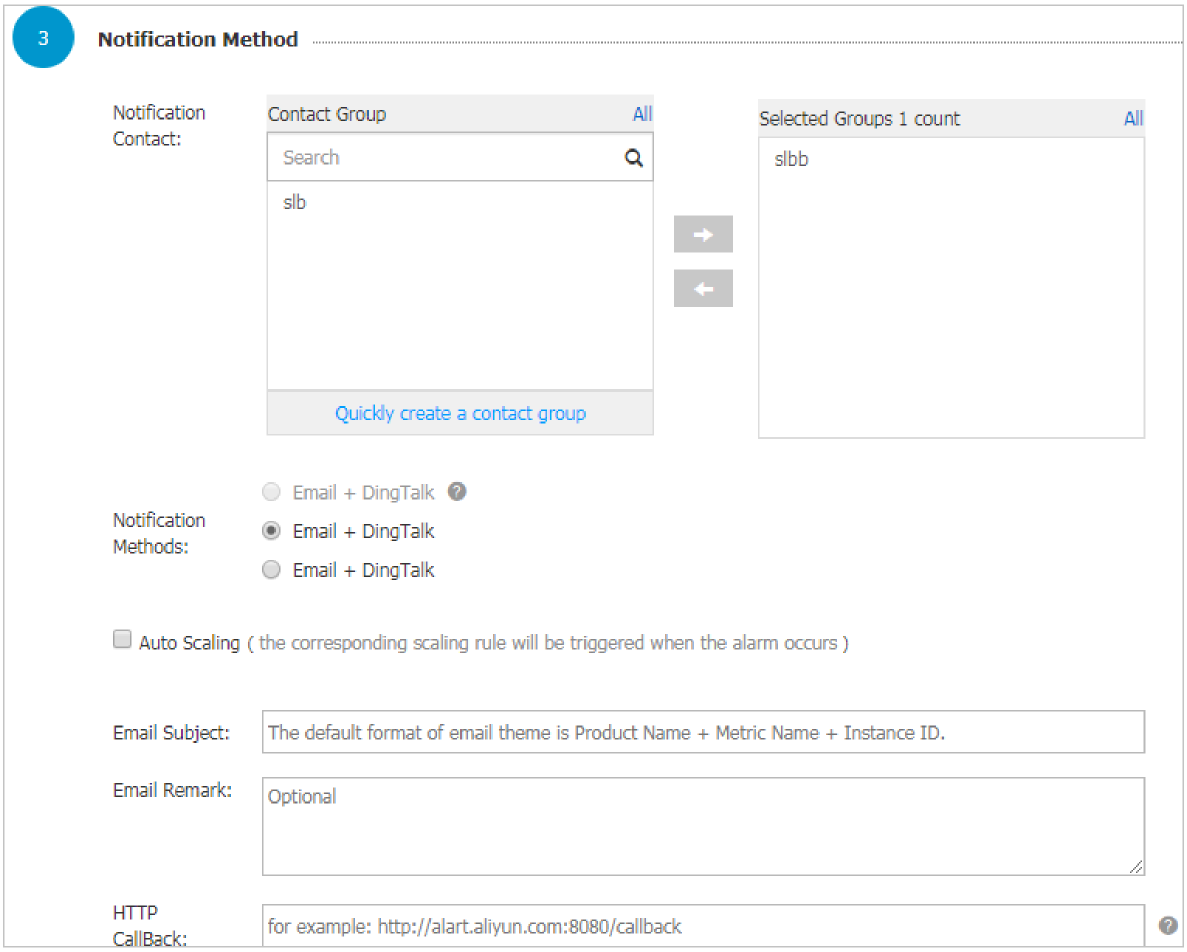
Mute for: 24 h

Effective Period: 00:00 To: 23:59

3. Configure the notification method.

   a. Notification contact. Send a notification in the contact group level.
   b. Alarm level. Select Warningor Info as per your needs. Different levels have different notification methods.
   c. Notification subject and remark By default, the notification subject is the product name + monitoring item name + instance ID.
   d. HTTP callback. Enter a URL that can be accessed by the Internet. CloudMonitor pushes the alarm notification to this address by using the POST request. Currently, only HTTP protocol is supported.

Figure 3-3: Notification Method



3 Notification Method

Notification Contact: Contact Group (All) — Search — slb — Quickly create a contact group; Selected Groups 1 count (All) — slbb

Notification Methods:
○ Email + DingTalk
● Email + DingTalk
○ Email + DingTalk

□ Auto Scaling (the corresponding scaling rule will be triggered when the alarm occurs)

Email Subject: The default format of email theme is Product Name + Metric Name + Instance ID.

Email Remark: Optional

HTTP CallBack: for example: http://alart.aliyun.com:8080/callback

Click Confirm after the configurations to complete the configuration of monitoring policy.

Example

Monitor log collection status of Logtail

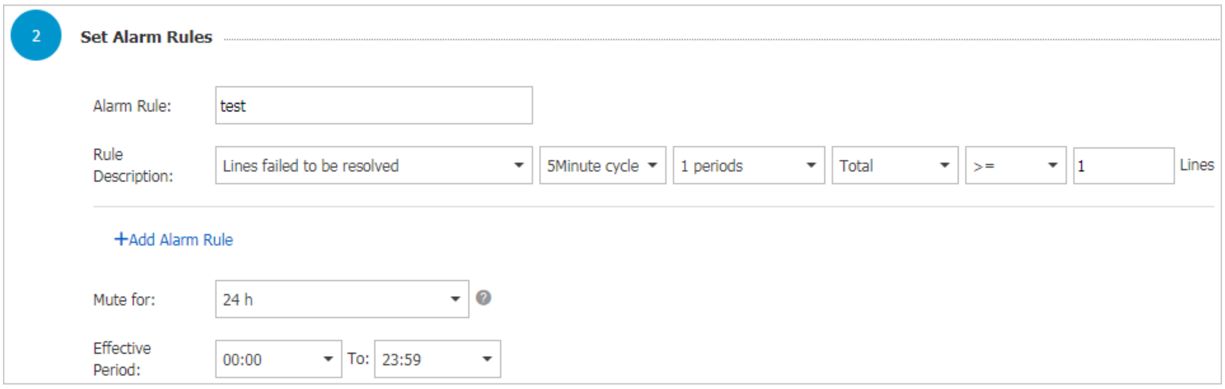
Errors may occur because of incorrect configurations when Logtail is running. For example, some log formats do not match or a log file is repetitively collected. For more information, see Basic questions of Logtail. To find such errors in time, you can monitor the metrics such as lines failed to be resolved and number of errors on Logtail.

The monitoring rule configuration is as follows:

Enter the alarm rule name and configure the rule description. Select Lines failed to be resolved or Number of errors as needed. Configure the rule items such as statistical period and method. You can also set alarm rules based on other errors of Logtail. Then, you can find the log collection errors in time.

The following figure shows that an alarm is triggered when the number of lines failed to be resolved within five minutes is greater than one. The monitoring lasts 24 hours.

Figure 3-4: Monitor logtail log collection status



2 Set Alarm Rules

Alarm Rule: test

Rule Description: Lines failed to be resolved | 5Minute cycle | 1 periods | Total | >= | 1 Lines

+Add Alarm Rule

Mute for: 24 h

Effective Period: 00:00 To: 23:59

Monitor shard usage status

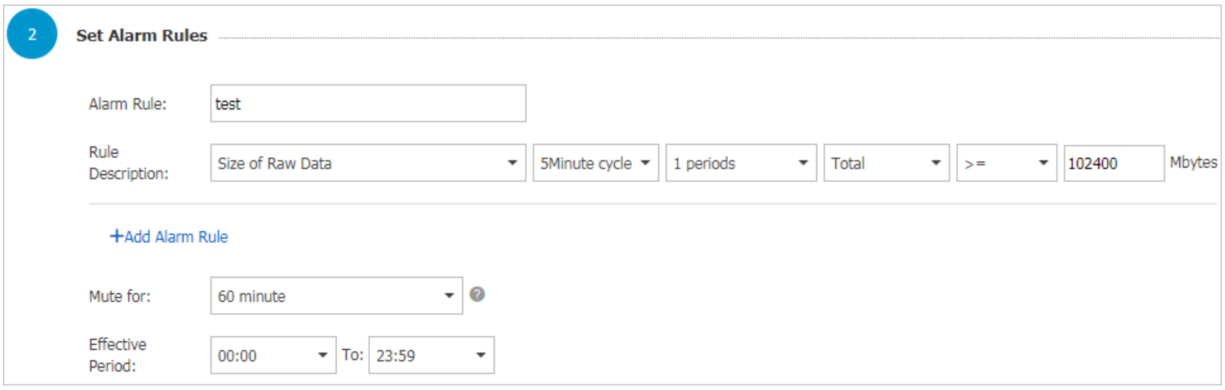
Each shard in a Logstore provides the write capability of 5 MB/s (500 times per second), which is sufficient in most cases. When the capability limit is exceeded, Log Service attempts to serve (rather than deny) your requests, but does not guarantee the availability of data that exceeds the limit during peak hours. You can detect this situation by setting an alarm rule on Logstore outbound and inbound traffic. If your data volume is large and needs more shards, adjust the number of shards in the console in time.

Use the following solutions to set an alarm rule on Logstore traffic.

Solution 1: Set an alarm rule on traffic

Enter the alarm rule name. Select Size of Raw Data. Configure the statistical period and method. For example, to trigger the alarm when 100 GB/5 minutes is exceeded, set the rule description to 5 mins, Total, >=, and 102400, which means the alarm is triggered if the total traffic within five minutes exceeds 102400 MB.

Figure 3-5: Set up traffic alert



2 Set Alarm Rules

Alarm Rule: test

Rule Description: Size of Raw Data | 5Minute cycle | 1 periods | Total | >= | 102400 Mbytes

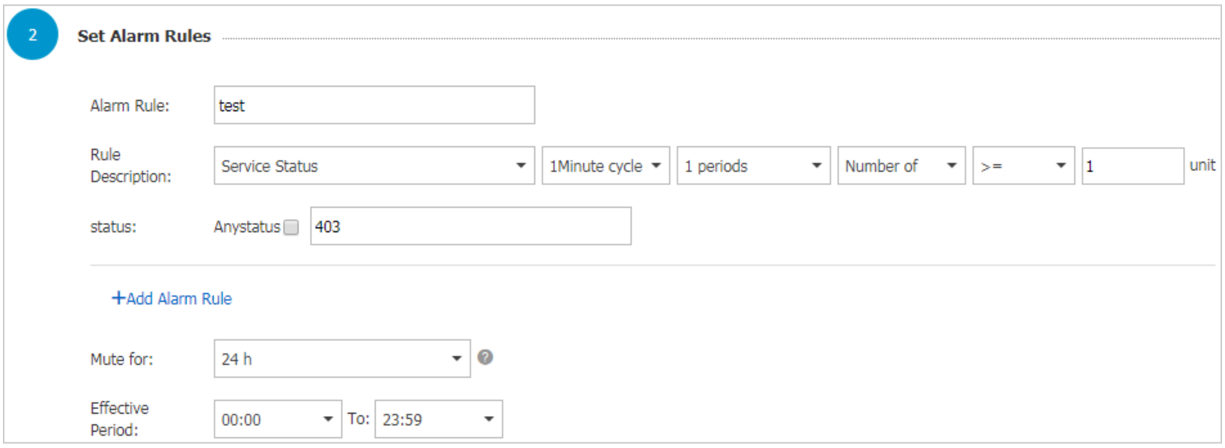
Mute for: 60 minute

Effective Period: 00:00 To: 23:59

Solution 2: Set an alarm rule on service status

Enter the alarm rule name. Select Service Status. Configure the statistical period and method. For example, to trigger the alarm when 403 service status occurs more than once within five minutes, set the rule description to 5 mins, Number of, >=, and 1, and enter 403 in the status field.

Figure 3-6: Set service status alarm



2 Set Alarm Rules

Alarm Rule: test

Rule Description: Service Status | 1Minute cycle | 1 periods | Number of | >= | 1 unit

status: Anystatus □ 403

Mute for: 24 h

Effective Period: 00:00 To: 23:59

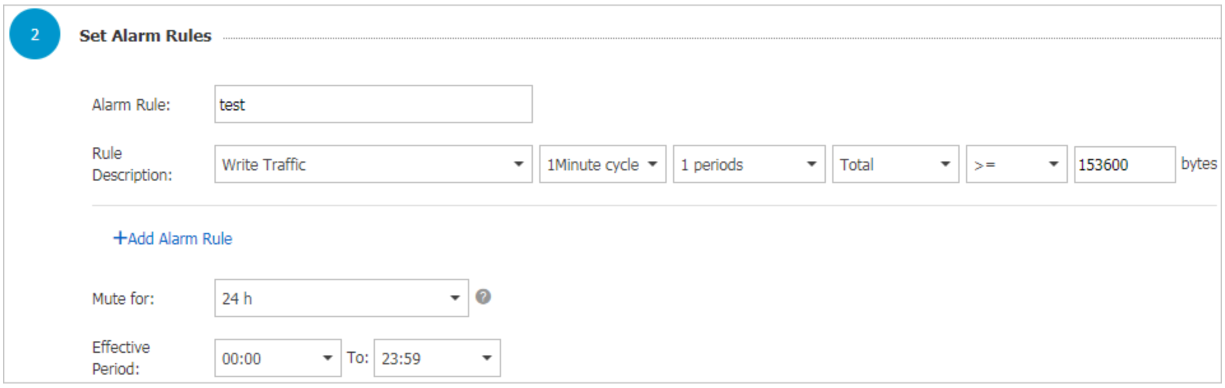
Monitor write traffic of projects

By default, each project provides the write capability of 30 GB/min (the size of raw data), which is used to protect you from generating large amounts of logs because of program errors. In most cases, this write capability is sufficient. The capability limit may be exceeded if your log volume is large. Open a ticket to increase the value.

Configure the monitoring policy of project quota as described in the following figure.

This example indicates that an alarm notification is sent when the write traffic within five minutes is greater than 150 GB.

Figure 3-7: Monitors write traffic for Project



2 Set Alarm Rules

Alarm Rule: test

Rule Description: Write Traffic | 1Minute cycle | 1 periods | Total | >= | 153600 bytes

Mute for: 24 h

Effective Period: 00:00 To: 23:59