ALIBABA CLOUD

Alibaba Cloud

Log Service

Monitor Log Servic

Document Version: 20210806

Alibaba Cloud

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 because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should 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 this document based on the "status quo", "being defective", and "existing functions" of its products and services. 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 take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, 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 contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, 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 this document 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 directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice 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.
Warning	A warning notice 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 restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Overview

This topic describes how to monitor Log Service.

You can monitor Log Service by using one of the following methods:

- Service logs
- Cloud Monitor

2.Service log

2.1. Overview

The service log feature of Log Service helps you record log data about the operations that are performed in a project. This feature also provides dashboards that allow you to analyze data from multiple dimensions. You can use this feature to view the service status of Log Service in real time and improve O&M efficiency.

Default configuration

Default configuration item	Description
Logstore	When the service log feature is enabled for a project, generated log data is classified and stored in one of the following Logstores. Two Logstores are automatically created for the project that you specify to store service logs. • **internal-operation_log**: stores operations log data. A log entry corresponds to an API request. By default, log data in the Logstore is retained for 30 days. The Logstore is charged as a common Logstore. • **internal-diagnostic_log**: stores consumption delay logs of consumer groups and Logtail heartbeat logs. The logs are classified by topic. By default, log data in the Logstore is retained for 30 days. The Logstore is free of charge. For more information about log types and fields, see Log types. **Note** • The automatically created Logstores are used to store only the logs generated by Log Service. You cannot write other data to these Logstores. However, you can perform other operations on the automatically created Logstores. For example, you can query and analyze data in the Logstores, configure alerts, or use the Logstore data for streaming consumption. • You are charged for log data recorded by the service log feature on a pay-as-you-go basis. For more information, see Billable items.

Default configuration item	Description
Region	• If you select **Automatic creation (recommended)**, a project is automatically created in the same region as the project for which the service log feature is enabled. • You can also select another option from the Log Storage Location drop-down list. If you specify a project to store service logs, the specified project must reside in the same region as the project for which the service log feature is enabled.
Shard	By default, two shards are created for each Logstore and the automatic sharding feature is enabled. For more information, see Enable automatic sharding.
Log retention period	By default, log data is retained for 30 days. You can modify the retention period. For more information, see Manage a Logstore.
Index	By default, the index feature is enabled for all collected log data. If you do not need to query and analyze data or configure alerts, you can disable the index feature by using **Index Attributes** in the upper-right corner of the **Search & Analysis** page.
Dashboard	The following five dashboards are automatically created: • Operation statistics dashboard • Logtail log collection statistics dashboard • Logtail status monitoring dashboard • Consumer group monitoring dashboard For more information about dashboards, see Service log dashboards.

Scenarios

- **Check whether data is evenly written and consumed among shards**

  You can use predefined dashboards to view the data write and consumption trends of shards and check whether data is evenly written or consumed among shards.

  Multiple Logstores under a project may share the same shards. To view the data writes to multiple shards of a Logstore, you can add filter conditions on the dashboard to filter Logstores.

- **Monitor API request status**

  You can call API operations to write log data, consume log data, and create projects or Logstores. A log entry is generated in the **internal-operation_log** Logstore when an operation is performed. If an API request fails, the value of the **Status** field in the generated log entry is an integer greater than 200, such as 404. You can monitor API requests by viewing the number of log entries whose **Status** field value is greater than 200.

- **View Logtail status**

  By default, two Logtail-related dashboards are created after the service log feature is enabled. They are **Logtail status monitoring** and **Logtail log collection statistics**. The Logtail status monitoring dashboard helps you monitor Logtail exceptions such as regular expression mismatches and log data parsing failures.

2.2. Manage service logs

This topic describes how to enable and disable the service log feature and how to modify service log configurations.

Prerequisites

- A project is created. For more information, see Quick Start.
- If you log on to the Log Service console as a RAM user, the RAM user must be granted relevant permissions by your Alibaba Cloud account. For more information, see Authorize a RAM user to use the service log feature.

Enable the service log feature

1. Log on to the Log Service console.
2. Click the project for which you want to enable the service log feature.
3. On the **Overview** page, click **Enable Service Logs** in the **Operations Log** section.
4. The following table describes the parameters for enabling the service log feature.

Parameter	Description
Service Logs	○ **Detailed Logs**: Detailed logs include logs of operations performed on all resources in the project, including creation, modification, deletion, read, and write operations. These logs are stored in the **internal-operation_log** Logstore of the project. ○ **Important Logs**: Important logs include consumption delay logs of consumer groups and Logtail heartbeat logs in each Logstore. These logs are stored in the **internal-diagnostic_log** Logstore of the project.
Log Storage Location	○ **Automatic creation (recommended)**: Log Service automatically creates a project named **log-service-{User ID}-{region}** in the same region as the project for which the service log feature is enabled. We recommend that you store all logs generated within the same region in this project. ○ **Current Project**: Log Service stores service logs in the current project. ○ Other projects in the drop-down list: Log Service stores service logs in other projects that already exist in the current region. If you specify a project to store service logs, the specified project must reside in the same region as the project for which the service log feature is enabled.

5. Click **OK**.

> **Note**
> - After the service log feature is enabled, corresponding Logstores are created in the specified log storage location. The billing method of the Logstore used to store **detailed logs** is the same as that of common Logstores. For more information, see Billable items. You are not charged for the Logstore that stores **important logs**.
> - Only service logs generated after you enable the feature are recorded.

Modify service log configurations

1. Log on to the Log Service console.
2. In the Projects section, click the name of the project that you want to view.
3. On the **Overview** page, click **Modify** in the **Operations Log** section.
4. In the **Modify Service Logs Settings** dialog box, select required log types and clear log types that are not required.
5. Select a project to store service logs from the **Log Storage Location** drop-down list.

   > **Note**
   > - We recommend that you select **Automatic creation (recommended)** and store service logs in the automatically created project. You can also specify a project and store service logs generated under different projects in the project. These projects reside in the same region as the specified project.
   > - After you modify the **Log Storage Location** value, new log data is stored in the specified project. The log data stored in the original project is not synchronously deleted or migrated to the new project. You can manually delete the original project if you no longer need the data in it.

6. Click **OK**.

Disable the service log feature

1. Log on to the Log Service console.
2. In the project list, click the project for which you want to disable the service log feature.
3. On the **Overview** page, click **Modify** in the **Operations Log** section.
4. In the **Modify Service Logs Settings** dialog box, clear all log types.
5. Click **OK** to disable the service log feature.

   > **Note** After the service log feature is disabled, the log data stored in the project is not automatically deleted. You can manually delete the project if you no longer need to store the data.

Authorize a RAM user to use the service log feature

Before you can use the service log feature as a RAM user, you must use your Alibaba Cloud account to grant the RAM user relevant permissions. For more information, see Create a RAM user and authorize the RAM user to access Log Service. The following code shows the content of the permission policy:

```
{
 "Version": "1",
 "Statement": [
  {
   "Action": [
    "log:CreateDashboard",
    "log:UpdateDashboard"
   ],
   "Resource": "acs:log:*:*:project/{The project where logs are stored}/dashboard/*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "log:GetProject",
    "log:CreateProject",
    "log:ListProject"
   ],
   "Resource": "acs:log:*:*:project/*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "log:List*",
    "log:Create*",
    "log:Get*",
    "log:Update*"
   ],
   "Resource": "acs:log:*:*:project/{The project where logs are stored}/logstore/*",
   "Effect": "Allow"
  },
  {
   "Action": [
    "log:*"
   ],
   "Resource": "acs:log:*:*:project/{The project for which the service log feature is enabled}/logging",
   "Effect": "Allow"
  }
 ]
}
```

2.3. Log types

The service log feature of Log Service can record a variety of log types. This topic describes these log types and their log fields.

Log types

When you enable the service log feature for a project, you can select one of the following log types.

Log type	Overview	Logstore	Log source	Description
Detailed logs	Detailed logs include operations logs generated when you create, modify, or delete resources in the project. Detailed logs also include log data about read and write operations.	internal-operation_log	Operations logs	Logs about all API requests, including requests sent by using the console and SDKs.
Important logs	Important logs include log data about consumption delay of consumer groups, Logtail errors, heartbeats, and collection statistics in each Logstore.	internal-diagnostic_log	Consumption delay logs of consumer groups	The consumption delay logs of consumer groups. These logs are recorded every 2 minutes. To query consumption delay logs of a consumer group, you must include `__topic__: consumergroup_log` in the query statement.
			Logtail alert logs	The error logs of Logtail. Error logs are recorded every 30 seconds. If the same type of error log entry occurs multiple times within 30 seconds, the total number of errors and one error log entry are recorded in the Logstore. To query Logtail alert logs, you must include `__topic__: logtail_alarm` in the query statement.
			Logtail collection logs	The logs about the log data collected by Logtail. These logs are recorded every 10 minutes. To query Logtail collection logs, you must include `__topic__: logtail_profile` in the query statement.
			Logtail status logs	The Logtail status logs that are recorded at regular intervals. These logs are recorded every 1 minute. To query Logtail status logs, you must include `__topic__: logtail_status` in the query statement.

Operations logs

Operations logs can be divided into three types based on the Method field: read operations log, write operations log, and resource operations log.

Type	API operation
Read operations log	Read operations logs are generated when you call the following API operations: • GetLogStoreHistogram • GetLogStoreLogs • PullData • GetCursor • GetCursorTime
Write operations log	Write operations logs are generated when you call the following API operations: • PostLogStoreLogs • WebTracking
Resource operations log	Resource operations logs are generated when you call the following API operations: Operations such as CreateProject and DeleteProject

The following table describes the common fields of operations logs.

Field	Description	Example
APIVersion	The version of the API.	0.6.0
AccessKeyId	The AccessKey ID used to access Log Service.	LTAI4FkSqNGBsVTqVZYx****
CallerType	The type of the caller.	Subuser
InvokerUid	The account ID of the user who performs the operation.	175921811532****
Latency	The latency of the request. Unit: microseconds.	123279
LogStore	The name of the Logstore.	logstore-1
Method	The API operation that generates the log.	GetLogStoreLogs
NetOutFlow	The amount of read traffic. Unit: bytes.	120
NetworkOut	The amount of read traffic sent over the Internet. Unit: bytes.	10
Project	The name of the project.	project-1

Field	Description	Example
RequestId	The ID of the request.	8AEADC8B0AF2FA2592C9****
SourceIP	The IP address of the client that sends the request.	1.2.3.4
Status	The HTTP response status code.	200
UserAgent	The agent that is used by the client to call API operations.	sls-java-sdk-v-0.6.1

The following table describes the unique fields in read operations logs.

Field	Description	Example
BeginTime	The start time of the request. The value is a Unix timestamp.	1523868463
DataStatus	The status that indicates whether all data is read. The data status can be Complete, OK, or Unknown.	OK
EndTime	The end time of the request. The value is a Unix timestamp.	1523869363
Offset	The offset of log entries returned when you call the GetLogStoreLogs or GetLogStoreHistogram API operation.	20
Query	The original query statement.	UserAgent: [consumer-group-java]*
RequestLines	The number of lines requested by the user.	100
ResponseLines	The number of returned lines.	100
Reverse	Indicates whether logs are returned in descending order of timestamps. • 1: Logs are returned in descending order of timestamps. • 0: This is the default value. Logs are returned in ascending order of timestamps.	0
TermUnit	The number of keywords in the query statement.	0

Field	Description	Example
Topic	The topic of the read data.	topic-1

The following table describes the unique fields in write operations logs.

Field	Description	Example
InFlow	The raw data size. Unit: bytes.	200
InputLines	The number of lines that the user requests to write.	10
NetInflow	The size of the compressed data. Unit: bytes.	100
Shard	The ID of the shard to which data is written.	1
Topic	The topic of the written data.	topic-1

Consumption delay logs of consumer groups

The following table describes the fields in consumption delay logs.

Field	Description	Example
consumer_group	The name of the consumer group.	consumer-group-1
fallbehind	The duration of time between when the current consumption data was generated and when the latest log was written. Unit: seconds.	12345
logstore	The name of the Logstore.	logstore-1
project	The name of the project.	project-1
shard	The ID of the shard from which data is consumed.	1

Logtail alert logs

The following table describes the fields in Logtail alert logs.

Field	Description	Example
alarm_count	The number of alerts during the specified time window.	10

Field	Description	Example
alarm_message	The sample raw log data that triggers the alert.	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 type of the alert.	REGISTER_INOTIFY_FAIL_ALARM
logstore	The name of the Logstore.	logstore-1
os	The operating system of the server on which Logtail runs, such as Linux or Windows.	Linux
project	The name of the project.	project-1
source_ip	The IP address of the server on which Logtail runs.	1.2.3.4
version	The version of Logtail.	0.14.2

Logtail collection logs

Based on the `file_name` field, Logtail collection logs are divided into the following categories:

- Collection statistics of a single log file.
- Logstore statistics whose `file_name` is set to `logstore_statistics`.

The following table describes the fields in Logtail collection logs.

Field	Description	Example
logstore	The name of the Logstore.	logstore-1
config_name	The globally unique name of the configuration file. The name must be in the format of *##configuration version##projectName$configuration name*.	##1.0##project-1$logstore-1
error_line	The raw log that records 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

Field	Description	Example
file_dev	The device ID of the log file. **Note** This field is invalid if the `file_name` field is set to `logstore_statistics`.	123
file_inode	The inode of the log file. **Note** This field is invalid if the `file_name` field is set to `logstore_statistics`.	124
file_name	The full path of the log file, or `logstore_statistics`.	*/abc/file_1*
file_size	The size of the current log file. Unit: bytes.	12345
history_data_failures	The number of data processing failures.	0
last_read_time	The last read time in the specified time window. The value is a Unix timestamp.	1525346677
project	The name of the project.	project-1
logtail_version	The version of Logtail.	0.14.2
os	The operating system of the server on which Logtail runs.	Windows
parse_failures	The number of lines that fail to be parsed during the specified time window.	12
read_avg_delay	The average difference between the current offset and the file size at each read during the specified time window.	65
read_count	The number of times that logs are read during the specified time window.	10
read_offset	The read offset of the current file. Unit: bytes.	12345

Field	Description	Example
regex_match_failures	The number of regular expression mismatches.	1
send_failures	The number of times that log data fails to be sent during the specified time window.	12
source_ip	The IP address of the server on which Logtail runs.	1.2.3.4
succeed_lines	The number of processed log lines.	123
time_format_failures	The number of log time mismatches.	122
total_bytes	The total size of read data. Unit: bytes.	12345

The unique fields in Logstore statistics are available only when the `file_name` field is set to `logstore_statistics`. The following table describes these fields.

Field	Description	Example
send_block_flag	Indicates whether the data sending queue is blocked when the specified time window expires.	false
send_discard_error	The number of packets dropped due to data errors or insufficient permissions during the specified time window.	0
send_network_error	The number of packets that fail to be sent due to network errors during the specified time window.	12
send_queue_size	The number of unsent packets in the current sending queue when the specified time window expires.	3
send_quota_error	The number of packets that fail to be sent because the quota is exhausted during the specified time window.	0
send_success_count	The number of packets sent during the time window.	12345

Field	Description	Example
sender_valid_flag	Indicates whether the send flag of the current Logstore is valid when the specified time window expires. Valid values: • true: The flag is valid. • false: The flag is disabled due to a network error or quota error.	true
max_send_success_time	The last time when data was sent during the specified time window. The value is a Unix timestamp.	1525342763
max_unsend_time	The last time when packets in the sending queue failed to be sent during the specified time window. The value is a Unix timestamp. The value is 0 if the queue is empty.	1525342764
min_unsend_time	The time when packets in the sending queue fail to be sent for the first time during the specified time window. The value is a Unix timestamp. The value is 0 if the queue is empty.	1525342764

Logtail status logs

The following table describes the fields in Logtail status logs.

Field	Description	Example
cpu	The load of the CPU.	0.001333156
hostname	The hostname of the server.	abc2. ****
instance_id	The unique ID of Logtail. This ID is randomly assigned.	05AFE618-0701-11E8-A95B-00163E025256_10.11.12.13_151745****
ip	The IP address of the server on which Logtail runs.	1.0.1.0
load	The average system load.	0.01 0.04 0.05 2/376 5277
memory	The amount of memory occupied by the Logtail process. Unit: MB.	12

Field	Description	Example
detail_metric	The metric values in the JSON format. For more information, see detail_metric.	detail_metric
os	The operating system of the server on which Logtail runs.	Linux
os_cpu	The CPU utilization of the system.	0.004120005
os_detail	The details of the operating system.	2.6.32-220.23.8.tcp1.34.el6.x86_64
status	The status of Logtail. Valid values: • ok • busy • many_log_files • process_block • send_block • send_error For more information, see Monitor the running status of Logtail.	busy
user	The username that is used to log on to the server.	root
user_defined_id	The user-defined ID of the server.	aliyun-log-id
uuid	The universally unique identifier (UUID) of the server.	64F28D10-D100-492C-8FDC-0C62907F****
version	The version of Logtail.	0.14.2
project	The project to which the Logtail configuration files belong.	my-project

The following table describes the fields of the detail_metric field.

Field	Description	Example
config_count	The number of Logtail configuration files.	1
config_get_last_time	The last time when the configuration file was obtained.	1525686673
config_update_count	The number of configuration updates after Logtail was started.	1

Field	Description	Example
config_update_item_count	The total number of updated configuration items after Logtail was started.	1
config_update_last_time	The time of the last configuration update after Logtail was started.	1525686663
event_tps	The transactions per second (TPS).	1
last_read_event_time	The last time when events were read.	1525686663
last_send_time	The last time when data was sent.	1525686663
open_fd	The number of open log files.	1
poll_modify_size	The number of modified log files that are monitored.	1
polling_dir_cache	The number of scanned folders.	1
polling_file_cache	The number of scanned files.	1
process_byte_ps	The size of log data processed per second. Unit: bytes.	1000
process_lines_ps	The number of log entries processed per second.	1000
process_queue_full	The number of queues that reach the maximum data processing capacity.	1
process_queue_total	The number of queues that are processing data.	10
process_tps	The number of data processing transactions per second.	0
reader_count	The number of log files that are being processed.	1
region	The region to which Logtail belongs.	cn-hangzhou, cn-shanghai
register_handler	The number of folders to monitor.	1

Field	Description	Example
send_byte_ps	The size of raw log data sent per second. Unit: bytes.	11111
send_line_ps	The number of log entries sent per second.	1000
send_net_bytes_ps	The amount of network data sent per second. Unit: bytes.	1000
send_queue_full	The number of queues that reach the maximum data sending capacity.	1
send_queue_total	The number of queues that send log data.	12
send_tps	The number of data sending transactions per second.	0.075
sender_invalid	The number of abnormal queues that send data.	0

2.4. Service log dashboards

After the service log feature is enabled, Log Service creates visual dashboards based on the selected log type to display statistics of user operations, Logtail log collection, Logtail status monitoring, and consumer group monitoring.

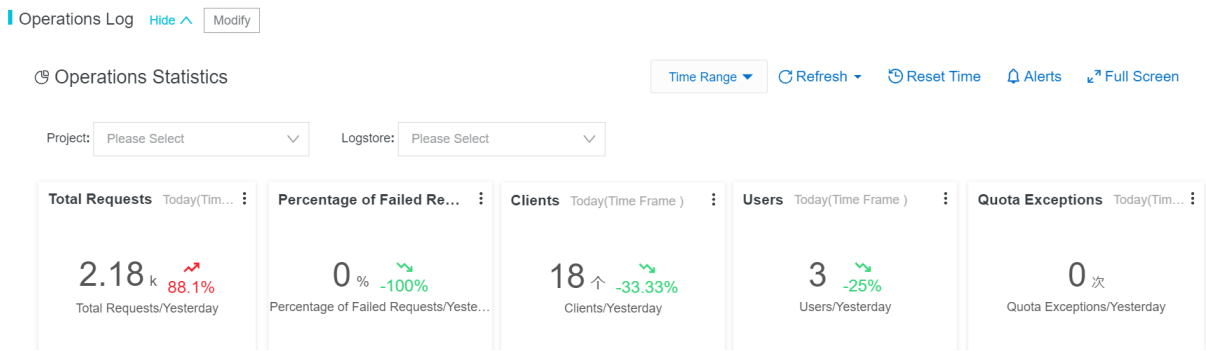
Dashboard types

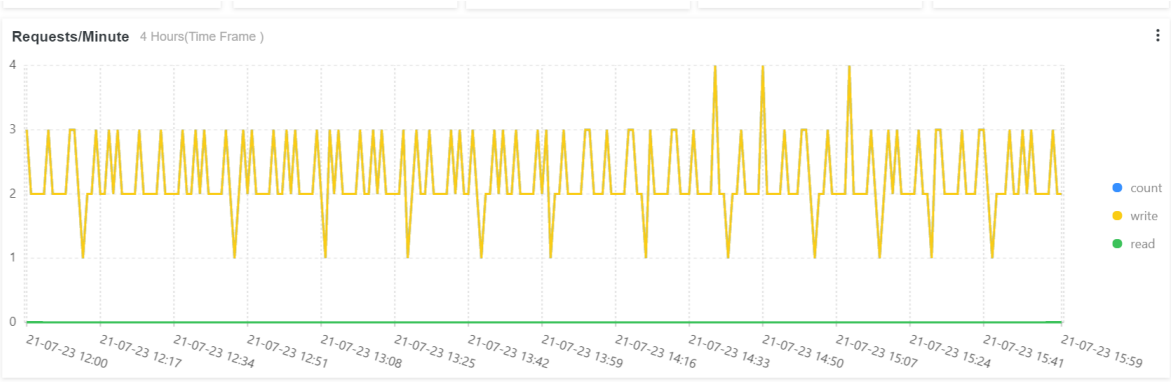
When you enable the service log feature for a project, you can select one of the following log types:

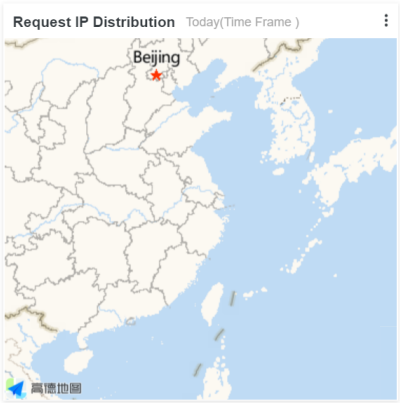
- **Detailed Logs**. If you select this log type, Log Service creates an operation statistics dashboard. For more information, see Operation statistics.
- **Important Logs**. If you select this log type, Log Service creates the Logtail log collection statistics, Logtail status monitoring, and Consumer group monitoring dashboards.

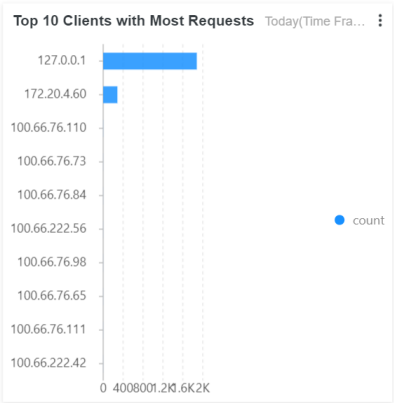
Operation statistics

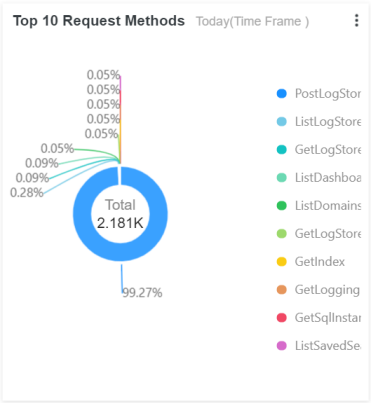
This dashboard displays statistics of user operations, such as API operation requests and project operation requests.

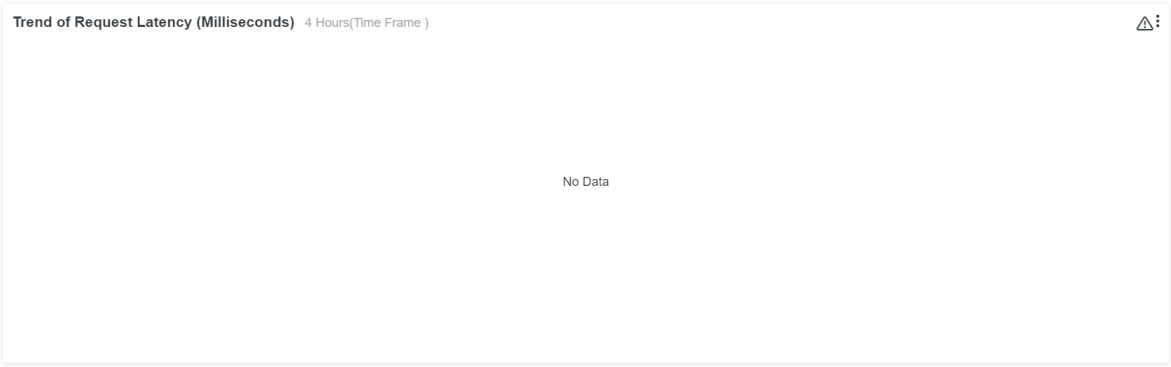


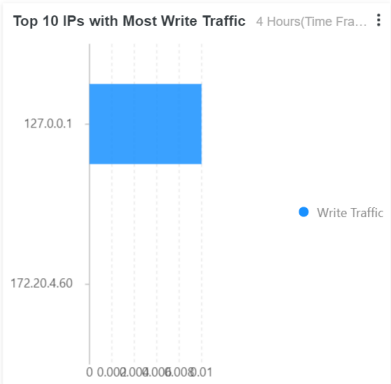

Requests/Minute 4 Hours(Time Frame)
4
3
2
1
0
21-07-23 12:00
21-07-23 12:17
21-07-23 12:34
21-07-23 12:51
21-07-23 13:08
21-07-23 13:25
21-07-23 13:42
21-07-23 13:59
21-07-23 14:16
21-07-23 14:33
21-07-23 14:50
21-07-23 15:07
21-07-23 15:24
21-07-23 15:41
21-07-23 15:59
count
write
read

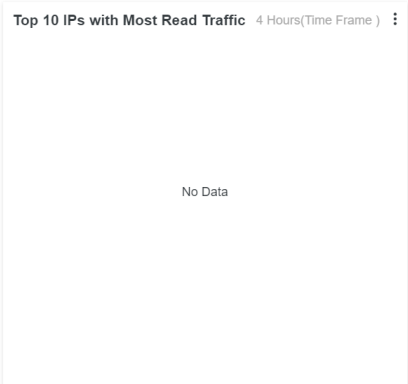

Request IP Distribution Today(Time Frame)
Beijing
高德地图

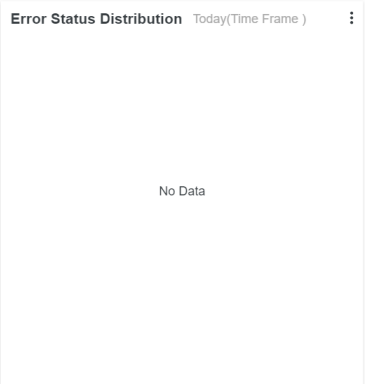

Top 10 Clients with Most Requests Today(Time Fra...
127.0.0.1
172.20.4.60
100.66.76.110
100.66.76.73
100.66.76.84
100.66.222.56
100.66.76.98
100.66.76.65
100.66.76.111
100.66.222.42
0 400800 1.2K 1.6K 2K
count


Top 10 Request Methods Today(Time Frame)
0.05%
0.05%
0.05%
0.05%
0.05%
0.05%
0.09%
0.09%
0.28%
Total
2.181K
99.27%
PostLogStor
ListLogStore
GetLogStore
ListDashboa
ListDomains
GetLogStore
GetIndex
GetLogging
GetSqlInstar
ListSavedSe

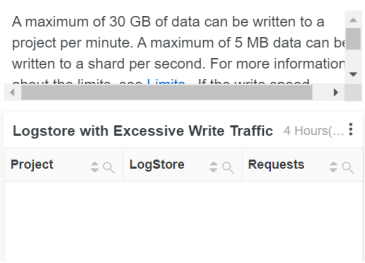

Trend of Request Latency (Milliseconds) 4 Hours(Time Frame)
No Data


Top 10 IPs with Most Write Traffic 4 Hours(Time Fra...
127.0.0.1
172.20.4.60
0 0.002 0.004 0.006 0.008 0.01
Write Traffic


Top 10 IPs with Most Read Traffic 4 Hours(Time Frame)
No Data


Error Status Distribution Today(Time Frame)
No Data


Read/Write Traffic/Minute (GB) 4 Hours(Time Frame)
1
Write Traffic
Read Traffic


A maximum of 30 GB of data can be written to a project per minute. A maximum of 5 MB data can be written to a shard per second. For more information
Logstore with Excessive Write Traffic 4 Hours(...
Project
LogStore
Requests

Logtail log collection statistics

This dashboard displays statistics of Logtail log collection.

Logtail status monitoring

This dashboard displays statistics of Logtail errors and alerts to help you monitor the status of Logtail in real time.

Consumer group monitoring

This dashboard displays statistics of consumer groups, including shard consumption data, consumption delay, and consumer group list.

3.Cloud Monitor

You can use Cloud Monitor to monitor Log Service. The monitoring metrics include write traffic, overall QPS, and service status. You can also create alert rules to monitor exceptions that occurred during log collection and shard usage.

Prerequisites

If you use a RAM user to view monitoring metrics, the RAM user must be granted the read-only permissions or read/write permissions on Cloud Monitor. You can use an Alibaba Cloud account to authorize the RAM user. For more information, see Grant permissions to a RAM user.

View monitoring metrics

1. Log on to the Log Service console.
2. Click the project for which you want to enable the service log feature.
3. Choose **Log Management** > **Logstores**. On the Logstores tab, find the target Logstore, and choose > **Monitor**. In the Cloud Monitor console, view the monitoring metrics.

Monitoring metrics

Monitoring metric	Description
Write Traffic	The size of the data that is written in real time to the Logstore per minute.
Size of Raw Data	The size of the uncompressed data that is written to the Logstore per minute.
Overall QPS	The QPS of all operations.
Number of operations	The number of API operations per minute. For more information, see API reference.
Service Status	The number of returned HTTP status codes.
Traffic resolved successfully	The raw log data that Logtail collects.
Lines resolved successfully	The number of log lines that Logtail collects.
Lines failed to be resolved	The number of log lines that Logtail fails to collect. If data is collected for this metric, errors occurred during log data collection.
Number of errors	The number of errors that occurred during log collection.
Number of error instances	The number of servers where errors occurred when Logtail collected logs.

Monitoring metric	Description
Number of Error IPs	The number of IP addresses that correspond to the servers where log collection errors occurred. Locate the IP address of the server based on the error. Log on to the server and check the `/usr/logtail/ilogtail.LOG` file to analyze the cause of the error.
The number of rows written.	The number of log lines that are written to the Logstore per minute.
Read Traffic	The size of the data that is read from the Logstore per minute.
Delay Time of Consumption	The difference between the receiving time of the log that is being consumed and the latest data receiving time. This is the difference between the consumption times of the shards with the largest difference In a consumer group, the delay time is the largest difference between the latest data receiving time of shards.

Set alert rules

This topic describes how to configure alert rules by using Cloud Monitor. If the trigger conditions of an alert rule are met, an SMS or email notification is sent to the specified recipients. You can configure alert rules in the Cloud Monitor console to monitor the status of log collection and shard usage and detect exceptions. For more information, see Cloud service monitoring.