ALIBABA CLOUD

Alibaba Cloud

Message Service

Log Management

Document Version: 20220524

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.Log management

You can use the log management feature of to push operations logs of messages to a specified logging bucket. You can specify the configurations in the Message Service (MNS) console to push logs to Object Storage Service (OSS) or Log Service, and enable the logging feature for the queues or topics in a region. pushes the operations logs of messages in the queues and topics to the specified logging bucket.

Scenarios

The log management feature can be applied in the following scenarios:

- Track the messages sent to a message queue if consumer clients cannot receive the messages.
- Identify the clients that have consumed a message and check the number of times that the message is consumed.
- Determine when a message can be consumed again if it fails to be consumed due to consumer client breakdown.
- Identify the cause if endpoints cannot receive messages that are published to a topic.
- View operations logs that are generated for messages a month ago.

In these scenarios, you can solve the problems by using the log management feature of .

- Push logs to Log Service and view operations logs of messages in the Log Service console.
- Specify the parameters to view operations logs of messages by using the log query tool provided by Alibaba Cloud.
- Log on to the OSS console and configure the LifeCycle parameter of the logging bucket. You can even view the operations logs that are generated during the past year.
- In addition to the official query tool, you can also call the GetObject API operation of OSS to download log files.

Push logs to Log Service

- For more information about the configuration method, see Push logs to Log Service.
- For more information about how to view logs, see View MNS logs in the Log Service console.
- When you create a Logstore, you must specify an appropriate data retention period. If you want to modify the data retention period after the Logstore is created, you can specify only a shorter data retention period.
- If you delete the project or Logstore that corresponds to a logging bucket, or revoke the permissions that are granted to to access Log Service, MNS logs cannot be pushed to Log Service.
- Logs can be pushed from MNS to Log Service about five minutes after the logs are generated.

Push logs to OSS

- For more information about configuration methods, see Push logs to OSS.
- For more information about how to view logs, see View MNS logs in the OSS console.
- If you delete the OSS bucket that corresponds to a logging bucket, or cancel the permissions that are granted to to access OSS, MNS logs cannot be pushed to OSS.
- Logs can be pushed from MNS to Log Service about 15 minutes after the logs are generated.

Analysis of details

- Each region has a logging bucket. All operations logs of messages in the queues and topics for which the logging feature is enabled are pushed to the logging bucket.
- You can enable the logging feature for queues or topics based on your needs. The logging feature is disabled by default.

Billing

- You are not charged for using the log management feature of .
- However, you are charged for the memory usage, transferred data, and number of requests when you use to push logs to OSS or Log Service. For more information, see Overview of Log Service pricing and Overview of OSS pricing.
- The size of generated logs depends on queries per second (QPS) of the server and types of operations. For example, if MNS calls the SendMessage API operation 1,000 times per second, the size of generated log entries is about 10 MB (`178 bytes × 1000 × 60 / 1024 / 1024 ≈ 10 MB`). In this formula, `178 bytes` indicates the size of a log that is generated by a single SendMessage operation.

Operation logs of queue messages

Operation logs of queue messages are generated when operations are performed on queue messages, for example, when you send, consume, and delete messages. Each operations log contains multiple fields that indicate different information. The fields contained in a log vary based on different operations. The following tables describe the log fields and the relationships between the operation types and log fields.

- Log fields

  Each operations log contains multiple fields. The following table describes the fields.

Field	Description
Time	The time when the operation is performed.
MessageId	The ID of the message involved in the operation.
QueueName	The ID of the queue involved in the operation.
AccountId	The Alibaba Cloud account or RAM user to which the queue belongs.
RemoteAddress	The endpoint of the client that performs the operation.
NextVisibleTime	The time when the message is visible after the operation is complete.
ReceiptHandleInRequest	The value of the ReceiptHandle parameter that is passed into the request when the operation is performed.
ReceiptHandleInResponse	The value of the ReceiptHandle parameter that is returned after the operation is complete.
ProcessTime	The duration in which the operation is performed.

Field	Description
RequestId	The ID of the operation.
Action	The specific action of the operation. Valid values: Delete and Send.

- Fields of different operations

  Logs that are generated by different operations contain different fields. The following table shows the log fields of different operations.

Operation	Time	QueueName	AccountId	MessageId	RemoteAddress	NextVisibleTime	ReceiptHandleInResponse	ReceiptHandleInRequest
SendMessage/BatchSendMessage	Yes	Yes	Yes	Yes	Yes	Yes	No	No
PeekMessage/BatchPeekMessage	Yes	Yes	Yes	Yes	Yes	No	No	No
ReceiveMessage/BatchReceiveMessage	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
ChangeMessageVisibility	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
DeleteMessage/BatchDeleteMessage	Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Operation logs of topic messages

Operation logs of topic messages are generated when operations are performed on topic messages, for example, when messages are published and pushed. The following tables describe the log fields and the relationships between the operation types and log fields.

- Log fields

  Each operations log contains multiple fields. The following table describes the fields.

Field	Description
Time	The time when the operation is performed.
MessageId	The ID of the message involved in the operation.
TopicName	The ID of the topic involved in the operation.
SubscriptionName	The ID of the subscription involved in the operation.
AccountId	The Alibaba Cloud account or RAM user to which the topic belongs.
RemoteAddress	The endpoint of the client that performs the operation.
NotifyStatus	The status code or error message returned when pushes a message to a client.
ProcessTime	The duration in which the operation is performed.
MessageTag	The tags of the message.
RequestId	The ID of the operation.
Action	The specific action of the operation. Valid values: Delete and Send.

- Fields of different operations

  Logs that are generated by different operations contain different fields. The following table shows the log fields of different operations.

Operation	Time	MessageId	TopicName	SubscriptionName	AccountId	RemoteAddress	NotifyStatus	SubscriptionName
PublishMessage	Yes	Yes	Yes	No	Yes	Yes	No	No
Notify	Yes	Yes	Yes	Yes	Yes	No	Yes	Yes

- NotifyStatus

  NotifyStatus is a field that identifies the reason why fails to push messages to endpoints. The following table describes the error codes and the corresponding solutions.

Error code	Description	Recommended solution
2xx	The message is pushed.	N/A

Error code	Description	Recommended solution
Other HTTP status codes	After the message is pushed to the endpoint, an HTTP status code other than 2xx is returned.	Check the processing logic of the endpoint.
InvalidHost	The specified endpoint in the subscription is invalid.	Use the curl or telnet command to check whether the specified endpoint in the subscription is valid.
ConnectTimeout	MNS failed to connect to the specified endpoint in the subscription.	Use the curl or telnet command to check whether the specified endpoint in the subscription is accessible.
ConnectFailure	MNS failed to connect to the specified endpoint in the subscription.	Use the curl or telnet command to check whether the specified endpoint in the subscription is accessible.
UnknownError	An unexpected error has occurred.	Contact the technical support.

2.Authorize a RAM user to manage MNS logs

Before you manage Message Service (MNS) logs as a RAM user, you must authorize the RAM user. This article describes how to authorize a RAM user to manage MNS logs.

Step 1: Create custom policies

1. Log on to the RAM console.
2. In the left-side navigation pane, choose **Permissions > Policies**.
3. On the **Policies** page, click **Create Policy**.
4. On the **Create Custom Policy** page, enter a policy name and note, and select **Script** as the configuration mode. In the **Policy Document** section, enter a script. Then, click **OK**.

   The following table lists the required policies.

Policy name	Description	Policy script
RamListRolesPolicy	Permissions to access the list of RAM roles	`{ "Version":"1", "Statement":[ { "Effect":"Allow", "Action":"ram:ListRoles", "Resource":"acs:ram:*:*:*" } ] }`

Policy name	Description	Policy script

MNSAccessAccountAttr	Permissions to view and configure Alibaba Cloud accounts	{
		"Version":"1",
		"Statement":[
		{
		"Effect":"Allow",
		"Action":[
		"mns:SetAccountAttributes",
		"mns:GetAccountAttributes"
		],
		"Resource":"acs:mns:*:*:*"
		}
		]
		}

Policy name	Description	Policy script

LogServiceListPolicy	Permissions to access the list of Log Service projects and Logstores	<pre>{
		"Version":"1",
		"Statement":[
		{
		"Effect":"Allow",
		"Action":"log:List*",
		"Resource":"acs:log:*:*:*"
		}
		]
		}</pre>

OSSListBuckets	Permissions to access the list of OSS buckets	<pre>{
		"Version":"1",
		"Statement":[
		{
		"Effect":"Allow",
		"Action":"oss:ListBuckets",
		"Resource":"acs:oss:*:*:*"
		}
		]
		}</pre>

Step 2: Authorize the RAM user

After you create the policies, you must attach the policies to the RAM user.

1. Log on to the RAM console.
2. In the left-side navigation pane, choose **Identities > Users**.

3. On the **Users** page, find the user to which you want to grant permissions, and click **Add Permissions** in the **Actions** column.
4. In the **Add Permissions** dialog box, select **Custom Policy** in the **Select Policy** section. Specify the four permission policies that you created in Step 1. Click **OK**.
5. Click **Complete**.

3.Instructions

3.1. Push logs to Log Service

You can push Message Service (MNS) logs to Log Service and view operations logs in the Log Service console. You can query message traces based on the message ID to diagnose exceptions. This article describes how to push logs to Log Service.

Prerequisites

- A project and a Logstore are created. For more information, see 快速入门.

  You can push operations logs of queue messages and topic messages to a project that resides in the same region as the queues and topics.

- MNS is authorized to use the AliyunMNSLoggingRole role to push logs to Log Service.

  You can go to the Cloud Resource Access Authorization page to complete the authorization.

  > Notice
  > - This operation is required only when you enable the log management feature for the first time. You must complete the authorization by using your Alibaba Cloud account.
  > - If you use a RAM user to log on to MNS, you must grant required permissions to the RAM user. For more information, see RAM user authorization.
  > - To ensure that MNS operations logs can be pushed to Log Service, do not revoke permissions from the RAM role or delete the RAM role.

Procedure

1.
2.
3.
4. In the **Select Target** step of the **Logging** page, select **Log Service**.
5. In the **Configure Target** step, specify the **Project Name** and **Logstore Name** parameters, and click **Enable**.

Result

The project and the Logstore appear on the **Logging** page.

Related information

- Enable logging for a queue
- Enable logging for a topic
- Query and analyze logs
- View MNS logs in the Log Service console

3.2. Push logs to OSS

You can push Message Service (MNS) logs to Object Storage Service (OSS) and view operations logs in the OSS console. You can diagnose exceptions based on MNS logs. This article describes how to push logs to OSS.

Prerequisites

- Activate OSS
- A bucket is created. For more information, see Create buckets.

> **Note** Only a bucket that resides in the same region as the queue or topic can be used to store logs. Therefore, when you create a bucket, you must select the region where the queue or topic reside.

Procedure

1.
2.
3.
4. In the **Select Target** step of the **Logging** page, select **OSS**.
5. In the **Configure Target** step, specify the **Bucket Name** parameter, and click **Enable**.

Result

The bucket appears on the **Logging** page.

Related information

- Enable logging for a queue
- Enable logging for a topic
- View MNS logs in the OSS console

3.3. Enable logging for a queue

This article describes how to enable the logging feature for a queue.

Prerequisites

Create a queue

Procedure

1.
2.
3.
4.
5. In the **Edit Parameter of Queue** dialog box, set **Enable Logging Feature** to **Yes**.

Result

On the **Queues** page, the status of the **Logging Feature** column turns to **Enabled**.

Related information

- View MNS logs in the Log Service console
- View MNS logs in the OSS console

3.4. Enable logging for a topic

This article describes how to enable the logging feature for a topic.

Prerequisites

Create a topic

Procedure

1.
2.
3.
4. On the **Topics** page, find the topic and click **Edit** in the **Actions** column.
5. In the **Edit Parameter of Topic** dialog box, set **Enable Logging Feature** to **Yes**.

Result

On the **Topics** page, the status of the **Logging Feature** column turns to **Enabled**.

Related information

- View MNS logs in the Log Service console
- View MNS logs in the OSS console

3.5. View MNS logs in the Log Service console

This topic describes how to query logs in the Log Service console. This topic describes several common scenarios of real-time query. You can use multiple keywords to run complex queries.

> **Notice** Logs can be pushed from to Log Service about three minutes after the logs are generated.

Procedure

1.
2.
3.
4. Enter a query statement in the input field.

   A query statement consists of a search statement and an analytic statement in the format of Search statement|Analytic statement. For more information, see Search syntax and SQL syntax.
5. Click **15 Minutes(Relative)** to specify the time range for the query statement.

You can select a relative time, select a time frame, or customize a time range. However, the time range that you can specify is only accurate to the minute at most. If you want to use a time range that is accurate to the second, you must specify the time range in the analytic statement. Example: `* | SELECT * FROM log WHERE __time__>1558013658 AND __time__< 1558013660` .

> **Note** The query and analysis results may contain logs that are generated 1 minute earlier or later than the specified time range.

6. Click **Search & Analyze** to view the query and analysis results.

View the tracing of a message in a queue

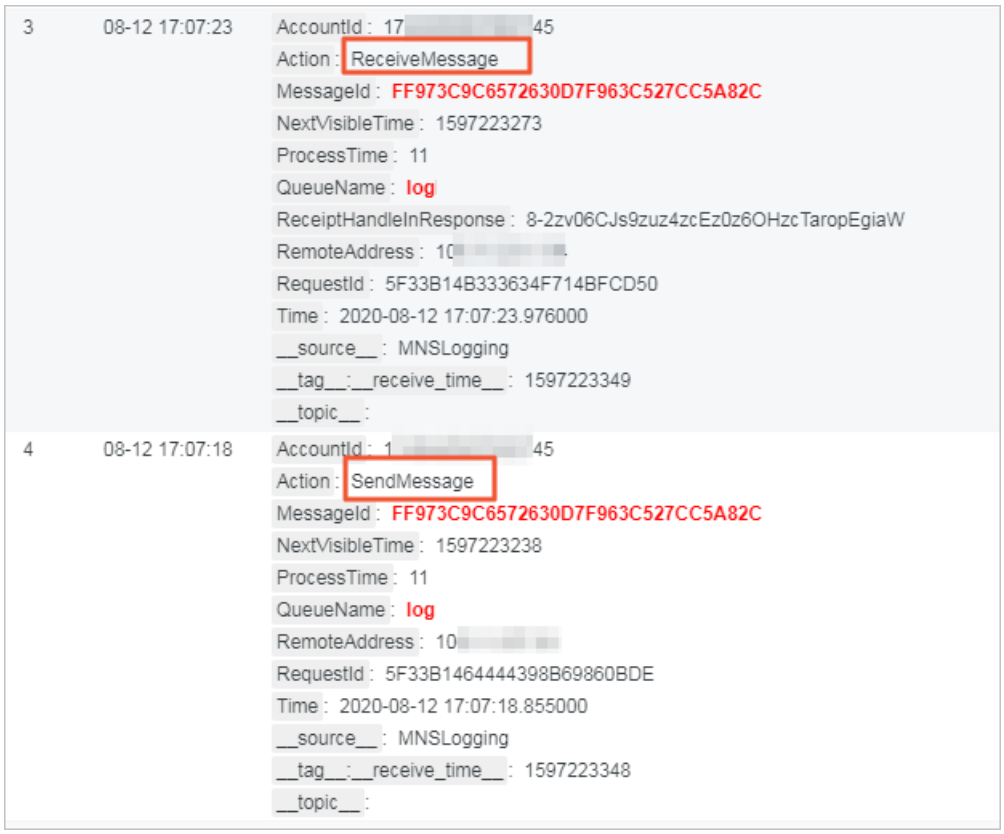
1.
2. In the **Projects** list, click the project where the message resides.
3. On the page that appears, choose **Log Storage > Logstores**, and then click the Logstore in which the message is stored.
4. Enter a search statement.

   In this example, the message tracing of a message in a queue is queried. You must enter the queue name and the message ID in the format of **$QueueName and $MessageId**, for example, **log and FF973C9C6572630D7F963C527CC5A82C**.
5. In the upper-right corner of the page, click **15 Minutes (Relative)** to set a time range for the query.

   You can select a relative time, set a time frame, or customize a time range.

   > **Note** The query results may contain logs that are generated one minute earlier or later than the specified time range.
6. Click **Search & Analyze**.

The following query result records the process from the time when the message is sent to the time when the message is received.



View the number of messages that are sent to Log Service in a queue

1. Enter a search statement on the Search & Analysis page of the Logstore where the messages are stored.

   In this example, the number of messages sent in a queue is queried. You must enter the queue name and send operation in the format of **$QueueName and (SendMessage or BatchSendMessage)**, for example, **log and (SendMessage or BatchSendMessage)**.

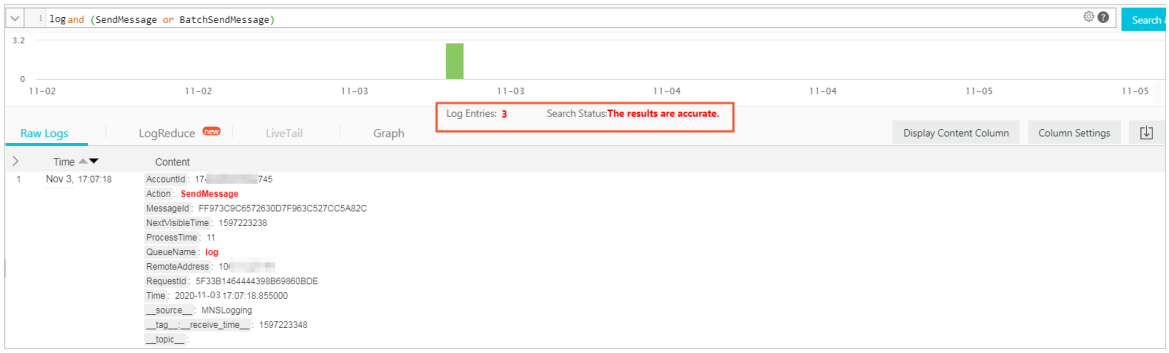
2. In the upper-right corner of the page, click **15 Minutes (Relative)** to set a time range for the query.

   You can select a relative time, set a time frame, or customize a time range.

   > **Note** The query results may contain logs that are generated one minute earlier or later than the specified time range.

3. Click **Search & Analyze**.

   The following figure shows the query results. Three queue messages are sent by the message producer to a queue named log in the specified time range.



View the number of messages that are consumed by Log Service in a queue

1. Enter a search statement on the Search & Analysis page of the Logstore where the messages are stored.

   In this example, the number of messages that are consumed by Log Service in a queue is queried. You must enter the queue name and consumption operation in the format of **$QueueName and (ReceiveMessage or BatchReceiveMessage)**, for example, **log and (ReceiveMessage or BatchReceiveMessage)**.

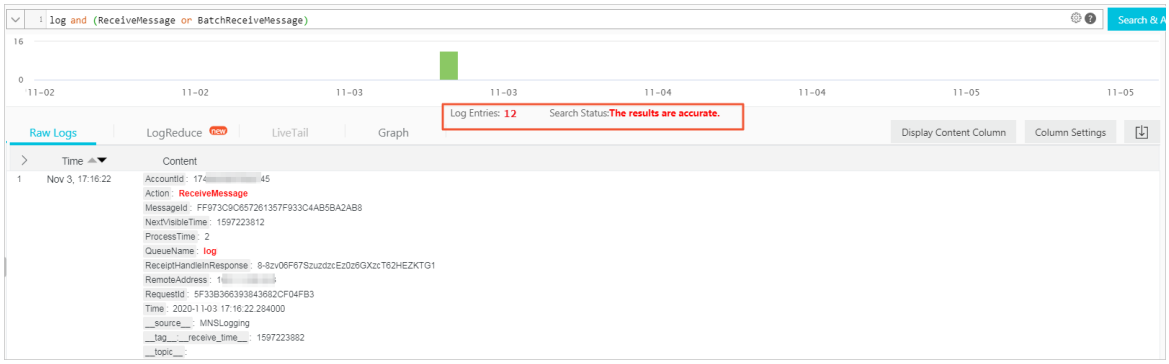
2. In the upper-right corner of the page, click **15 Minutes (Relative)** to set a time range for the query.

   You can select a relative time, set a time frame, or customize a time range.

   > **Note** The query results may contain logs that are generated one minute earlier or later than the specified time range.

3. Click **Search & Analyze**.

   The following figure shows the query results. Twelve queue messages are consumed in the specified time range.



View the number of messages that are deleted from a queue

1. Enter a search statement on the Search & Analysis page of the Logstore where the messages are stored.

   In this example, the number of messages that are deleted from a queue is queried. You must enter the queue name and delete operation in the format of **$QueueName and (DeleteMessage or BatchDeleteMessage)**, for example, **log and (DeleteMessage or BatchDeleteMessage)**.

2. In the upper-right corner of the page, click **15 Minutes (Relative)** to set a time range for the

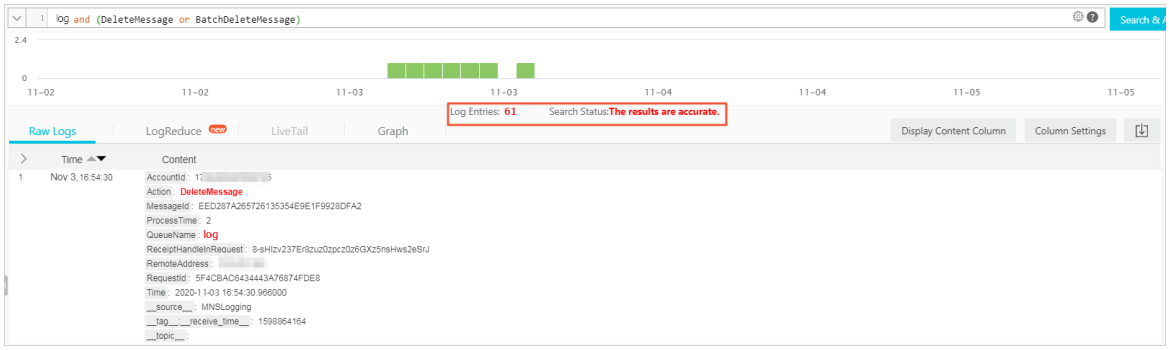
query.

You can select a relative time, set a time frame, or customize a time range.

> **Note** The query results may contain logs that are generated one minute earlier or later than the specified time range.

3. Click **Search & Analyze**.

The following figure shows the query results. Sixty-one queue messages are deleted in the specified time range.



View the tracing of a message in a topic

1. Enter a search statement on the Search & Analysis page of the Logstore where the messages are stored.

   In this example, the message tracing of a message in a topic is queried. You must enter the topic name and MessageId in the format of **$TopicName and $MessageId**, for example, **logtest and 979628CD657261357FCB3C8A68BFA0E3**.

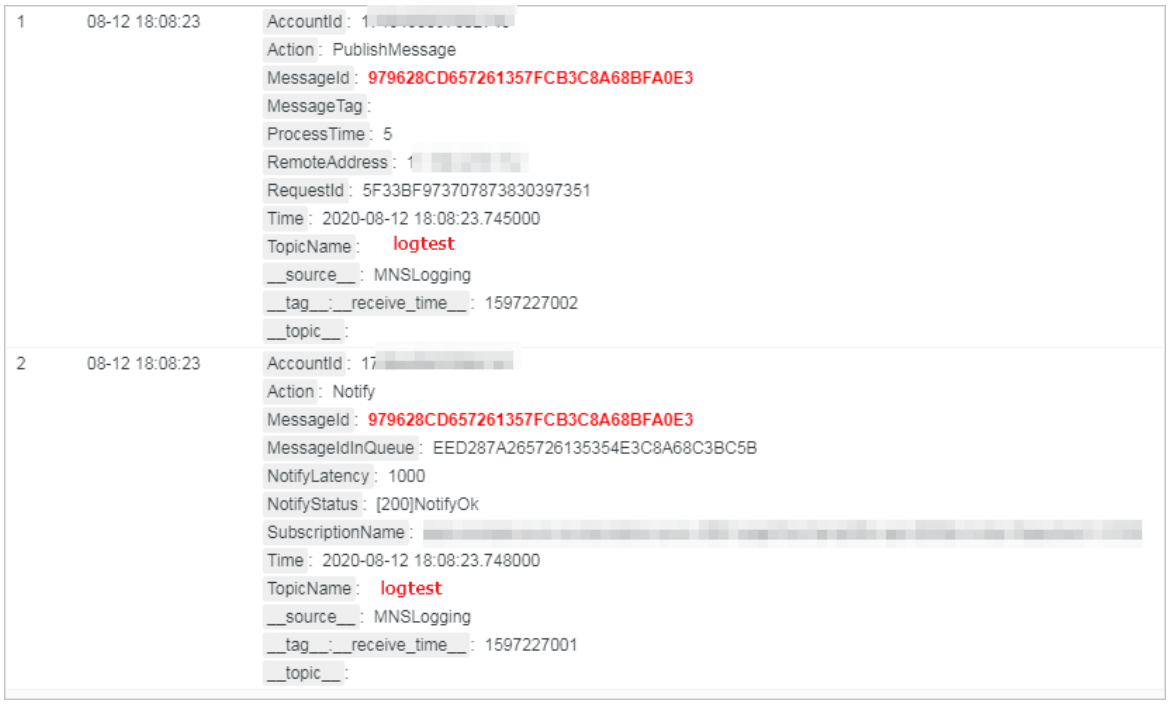
2. In the upper-right corner of the page, click **15 Minutes (Relative)** to set a time range for the query.

   You can select a relative time, set a time frame, or customize a time range.

   > **Note** The query results may contain logs that are generated one minute earlier or later than the specified time range.

3. Click **Search & Analyze**.

The following query result records the process from the time when the message is sent to the time when the message is received.



View the number of messages that are published in a topic

1. Enter a search statement on the Search & Analysis page of the Logstore where the messages are stored.

   In this example, the number of messages that are published in a topic is queried. You must enter the topic name and publish operation in the format of **$TopicName and PublishMessage**, for example, **logtest and PublishMessage**.

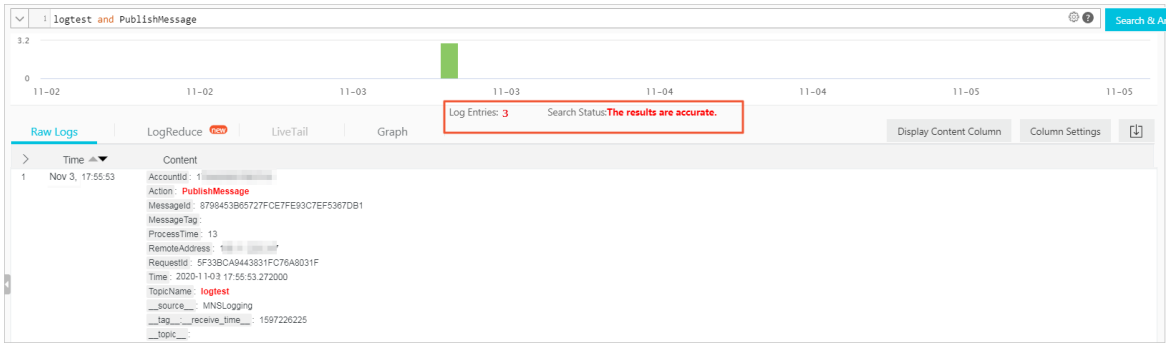
2. In the upper-right corner of the page, click **15 Minutes (Relative)** to set a time range for the query.

   You can select a relative time, set a time frame, or customize a time range.

   > **Note** The query results may contain logs that are generated one minute earlier or later than the specified time range.

3. Click **Search & Analyze**.

   The following figure shows the query results. Three messages are published to the logtest topic in the specified time range.



View the number of messages that are processed by a client

1. Enter a search statement on the Search & Analysis page of the Logstore where the messages are stored.

   In this example, the number of messages that are processed by a client is queried. You must enter the client IP address in the format of **$ClientIP**, for example, **10.10.10.0**.

   If you need to query a specific type of operations log, you can use multiple keywords, for example, **$ClientIP and (SendMessage or BatchSendMessage)**.

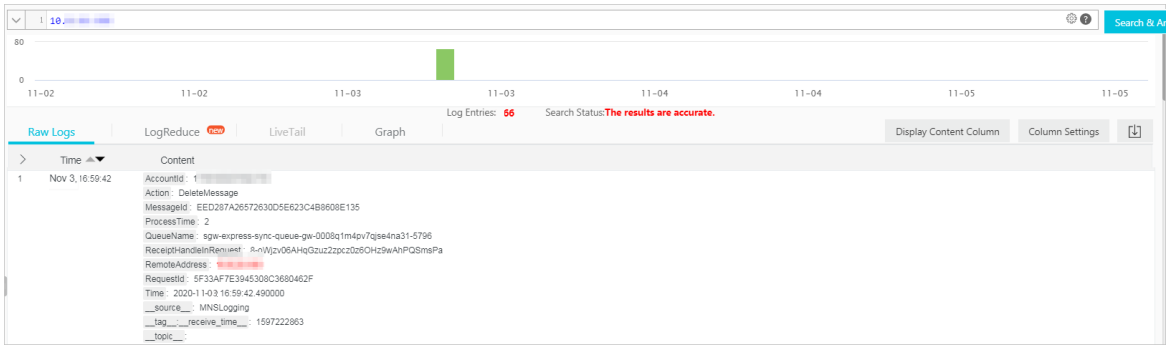
2. In the upper-right corner of the page, click **15 Minutes (Relative)** to set a time range for the query.

   You can select a relative time, set a time frame, or customize a time range.

   > **Note** The query results may contain logs that are generated one minute earlier or later than the specified time range.

3. Click **Search & Analyze**.

   The following figure shows the query results. The client processed 66 messages in the specified time range.



3.6. View MNS logs in the OSS console

This topic describes how to view Message Service (MNS) operations logs in the Object Storage Service (OSS) console.

Usage notes

- MNS operations logs are generated at an interval of one minute and stored as OSS objects that comply with specific naming conventions in a specified OSS bucket.
- Operation logs of queues and topics have different paths. For more information about specific paths, see the following sections: Operation logs of queues and Operation logs of topics.
- The log files are stored in the JSON format. You can download and process log files.
- Each log file is a map. The key is the message ID and the value is multiple logs that record operations on the message. Each operations log contains multiple fields, such as Action and Time.
- Logs can be pushed from to Log Service about 15 minutes after the logs are generated.

Prerequisites

- Log Service is activated.

If you have not activated Log Service, go to the Log Service product page.

- Log Service is authorized to access OSS.

  If you have not authorized Log Service to access OSS, visit Cloud Resource Access Authorization and follow the instructions to complete the authorization.

Background information

Enable real-time log query

You can use one of the following methods to enable real-time log query:

- i. Log on to the OSS console.
  ii. On the **Overview** page, click **Create Bucket** on the right side.
  iii. In the **Create Bucket** dialog box, set **Real-time Log Query** to **Enable**. For more information about other parameters, see Create buckets.
  iv. Click **OK**.

Method 1: Enable real-time log query when you create a bucket

- i. Log on to the OSS console.
  ii. In the left-side navigation pane, click **Buckets**. On the Buckets page, click the name of the bucket for which you want to enable real-time log query.
  iii. In the left-side navigation pane, choose **Logging > Real-time Log Query**.
  iv. Click **Activate Now**.

Method 2: Enable real-time log query for an existing bucket

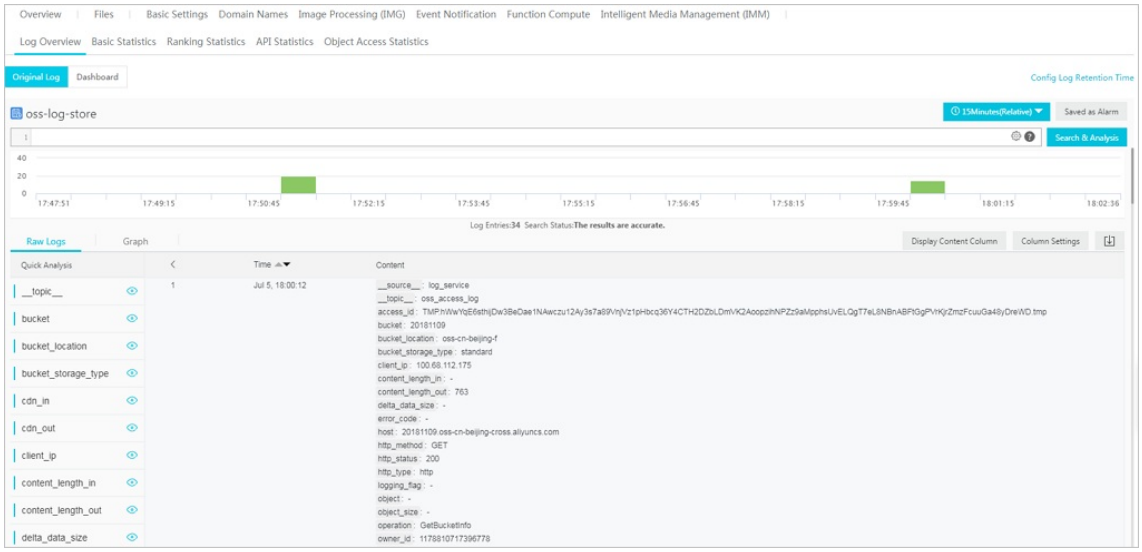
Real-time log query allows you to query logs over the last seven days free of charge. You can click **Config Log Retention Time** in the upper-right corner to modify the retention time of logs.

Query real-time logs

You can use one of the following methods to query real-time logs:

- i. Log on to the OSS console.
  ii. In the left-side navigation pane, click **Buckets**. On the Buckets page, click the name of the bucket whose logs you want to query.
  iii. In the left-side navigation pane, choose **Logging > Real-time Log Query**.
  iv. Click **Original Log** to analyze logs.

You can specify the time range and query statement in real-time log queries. For example, you can analyze the distribution of a specified field such as an API operation within a specified time range. You can also filter the query results by conditions to view required access records.



Method 1: Query real-time logs on the Original Log page

- i. Log on to the OSS console.
  ii. In the left-side navigation pane, click **Buckets**. On the Buckets page, click the name of the bucket whose logs you want to query.
  iii. In the left-side navigation pane, choose **Logging > Real-time Log Query**.
  iv. Click **Dashboard** to analyze logs.

  Dashboard allows you to view the following types of reports:

  - **Access Center**: displays the overall operating status including the PV, UV, traffic, and access distribution over the Internet.
  - **Audit Center**: displays statistics on object operations including read, write, and delete operations.
  - **Operation Center**: displays statistics on access logs including the number of requests and distribution of failed operations.
  - **Performance Center**: displays statistics on performance including the performance of downloads and uploads over the Internet, the performance of transmission over different networks or with different object sizes, and the list of differences between stored and downloaded objects.

Method 2: Query real-time logs on the Dashboard page

- Log on to the Log Service console to query real-time OSS logs. For more information, see OSS access logs.

Method 3: Query real-time logs in the Log Service console

Use the command-line tool to query logs

The command-line tool provides the **queryqueuelog** and **querytopiclog** commands. These commands allow you to specify a queue name, topic name, message ID, and time range to query operations logs. For more information, see Log query tool.