TDMQ for Apache Pulsar

Operation Guide

Product Documentation

Contents

Operation Guide
Cluster Management
Creating Cluster

Last updated：2025-04-01 11:34:26

Overview

Cluster is a resource dimension in TDMQ for Apache Pulsar, and namespaces, topics, and role permissions of different clusters are completely isolated from each other. Each cluster has its own resource limits, such as the total number of topics and message retention period. It is common for the development, test, and production environments to use their respective dedicated clusters.

Professional cluster: Physical resources are exclusive, and data is secure. There are almost no use limits. Resource usage fees will be charged even if resources are idle.

Note:

Currently, clusters are available in multiple versions. For more information, see Cluster Version Updates.

TDMQ for Apache Pulsar resource hierarchy

Directions

Creating a cluster

1. Log in to the TDMQ for Apache Pulsar console and enter the **Cluster** page.
2. On the **Cluster** page, select the region and click **Create Cluster** to enter the **Create Cluster** window.
3. In the **Create Cluster** window, select the cluster type and set the cluster attributes:

Cluster type: Select a professional cluster. see Product Selection.

Billing mode: Professional cluster supports monthly subscription mode. For more details, see Billing Overview.

Region: Select a region closest to your business. Cloud products in different regions cannot communicate over the private network. The choice cannot be changed after purchase. Choose with caution. For example, cloud servers in the Guangzhou region cannot access clusters in the Shanghai region over the private network. For cross-region private network communication, see Peering Connection.

Cluster Name: Define the cluster name. It cannot be empty. Alphanumeric characters as well as symbols “-_=:.” are supported. The length cannot exceed 64 characters.

Tenant alias: Used to customize the tenant name for client access to the cluster. Defaults to the cluster ID. If you do not use it for self-build migration to the cloud, it is recommended not to enable it.

Elastic storage or fixed storage form: select.
Specification: Select the cluster specifications that suit your business needs. For a description of different cluster configurations, see Pro Cluster Specifications.
Storage: Select the storage specifications that suit your business needs. The Pulsar pro cluster is deployed with 3 replicas by default.
Cross-AZ Deployment:The Professional Edition Cluster supports deployment in three different availability zones.For more details, see Cross Availability Zone Deployment.
Virtual Private Cloud: Bind the newly purchased cluster's access point domain name to the specified Virtual Private Cloud.
Public network access: It is not enabled by default. To enable it, submit a ticket for application. We recommend you only enable this option for development and test clusters as it cannot be disabled once enabled.
Resource tag: Set a resource tag. For more information, see Managing Resource with Tag.
4. Select **I have read and agree to TDMQ Terms of Service** , and then click **Buy Now** .
5. On the order payment page, click **Pay** , and within 3-5 minutes, the created cluster will be visible on the cluster management list page.
Note:
Each user can create up to 5 virtual clusters.

Subsequent steps

1. Get the access address to get the connection information of the server.
2. Create a namespace as instructed in Namespace in the cluster.
3. Create a role as instructed in Role and Authentication in the cluster and grant it the production/consumption permissions of the namespace.
4. Create a topic as instructed in Topic Management in the namespace.
5. Write a demo as instructed in SDK Overview and configure the connection information and token for message production/consumption.

Viewing cluster details

On the **Cluster Management** list page, click the ID of the target cluster to enter the cluster details page, where you can view the following information:
Professional Cluster
Virtual Cluster

Metrics	Description
Real-Time Production Speed	The number of messages produced to the cluster per second at the current time.

Average Message Size	The average size of message data within the selected time range, including the size of the message header and body.
Average Production Speed	The average rate at which messages are produced to the cluster within the selected time range.
Average Consumption Speed	The average rate at which the cluster pushes messages to clients within the selected time range.
Total Produced Messages	The number of messages produced to the cluster within the selected time range.
Storage Use	At the last time point of the selected time range, the actual size of message data consumed by storage. (This value changes only with the end point of the time range).

Basic information of the cluster: cluster name/ID, version, access address, region, cluster specification, billing mode, etc.

Cluster statistics: Displays the average message size, average production and consumption rate, number of produced messages, and cumulative storage duration within a specific time range.

Note：

Statistics data is not supported for clusters on version 2.6.x.

Metrics	Description
Average Message Size	The average size of message data within the selected time range, including the size of the message header and body.
Production Speed	The average rate at which messages are produced to the cluster within the selected time range.
Consumption Speed	The average rate at which the cluster pushes messages to clients within the selected time range.
Produced Messages	The number of messages produced to the cluster within the selected time range.
Actual Storage Usage	At the last time point of the selected time range, the actual size of message data consumed by storage. (This value changes only with the end point of the time range).

Basic information of the cluster: Cluster name/ID, version, access address (can only view in clusters v2.7.1 and above), region, billing mode, creation time, description, resource tags.

Cluster configuration:

Cluster Configuration	Configuration Instructions
Max Production TPS per Topic Partition	Maximum number of messages that can be produced per second per single Topic partition.
Max Consumption TPS per Topic Partition	Maximum number of messages that can be pushed to the client per second per single Topic partition.
Max Production Bandwidth per Topic Partition	Maximum message size that can be produced per second per single Topic partition.
Max Consumption Bandwidth per Topic Partition	Maximum message size that can be pushed to the client per second per single Topic partition.
Max Namespaces	Maximum number of namespaces that can be created within a cluster.
Max Topics	Maximum number of Topics that can be created per namespace.
Max Message Storage	Maximum disk capacity used by message backlog, exceeding this will prevent the production of new messages (under normal circumstances, message backlog should not be too large. If such a situation occurs, check whether the business is normally consuming messages).
Max Retention Period	Maximum message retention period that can be configured. A shorter period can be configured at the namespace level.
Max Message Delay	Maximum message consumption time delay.

Getting the access address

On the **Cluster Management** list page, click **Access Address** in the **Operation** column of the target cluster. You can get the access address in the following ways:

Note:

A cluster can be configured with multiple access points. Currently only VPC network access is supported. For configuration method, see VPC Access.

Pro Cluster Send-Receive Ratio Configuration

Configuration path: **Pro Cluster Details** > **Basic Information** > **Cluster Configuration** > **Send-Receive Ratio Configuration Item** . At the top right corner, click **Edit** for configuration.

Upgrading Cluster

Last updated：2025-04-01 11:34:26

Overview

If the current cluster specifications and storage specifications do not meet your business needs, you can upgrade both the cluster specifications and storage specifications in the console.

Note:

Currently, only pro clusters support upgrading cluster specifications. Virtual clusters do not support this upgrade.

Theoretically, the upgrade process should be seamless for the business. However, during server-side Rebalance Topic operations, clients may experience disconnections followed by reconnections.

Directions

1. Log in to the TDMQ for Apache Pulsar console.
2. In the left sidebar, choose **pulsar** > **Cluster Management**. In the cluster management list, find the target cluster, and click the operation column's **More** > **Upgrade**.
3. After selecting the target cluster specifications, click **Confirm Adjustment**.

Returning Cluster

Last updated：2024-06-28 11:31:37

Overview

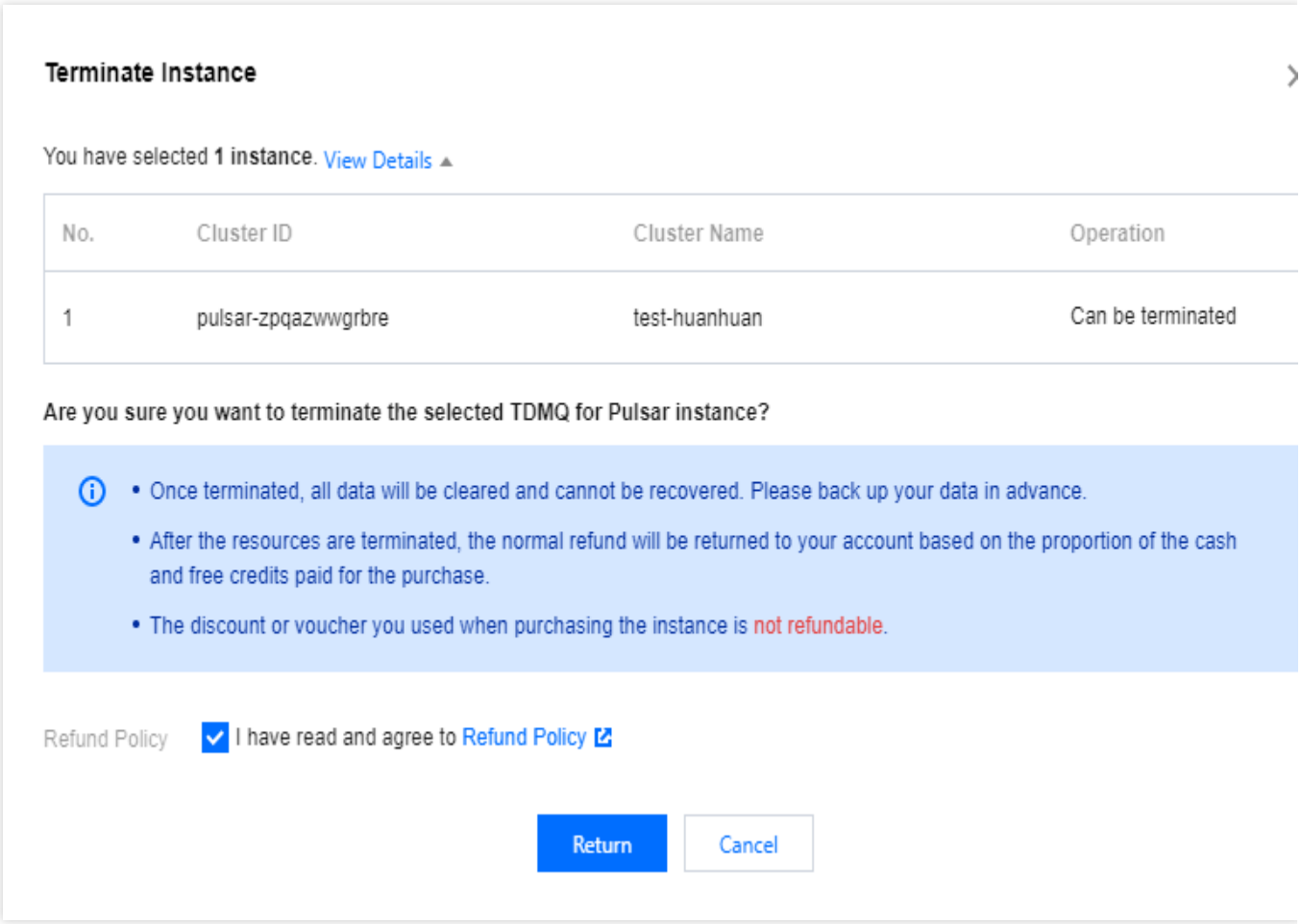
You can delete a TDMQ for Apache Pulsar cluster when it is no longer needed.
The lifetime of a TDMQ for Apache Pulsar cluster refers to the states a cluster goes through from startup to release. By managing the cluster reasonably from startup to deletion, you can ensure that applications running on the cluster can provide services efficiently and economically. The cluster has the following statuses:

Status	Attribute	Description
Creating	Intermediate status	After the cluster is created, it enters the status before running.
Normal	Steady status	The cluster is in a normal operating status, indicating that the condition of your nodes, disk utilization rate, and other metrics are all within the normal range.
Deleting	Intermediate status	The cluster is being deleted through the console or API.
Isolated	Intermediate status	The cluster is overdue and has entered a 7-day isolation period. Instances in isolation cannot produce or consume, and data and configurations saved within the cluster will not be deleted.
Provisioning Failed	Intermediate status	You have purchased a cluster through the console or API and the charge was successful, but the cluster allocation failed. In this case, contact us.
Deletion Failed	Steady status	The cluster was manually deleted or not renewed within 7 days of its expiration, resulting in TDMQ for Apache Pulsar failing to release resources.

Directions

Manual Deletion

For clusters that have not yet expired, you can choose to manually delete them. The steps are as follows:
1. Log in to the TDMQ for Apache Pulsar console.
2. In the left sidebar, choose **Pulsar** > **Cluster Management**. On the cluster management page, click the operation column's **More**> **Return**.
3. In the instance termination confirmation pop-up, check the Refund Information, and click **Return** to delete the cluster.



Note:

After termination, all data will be cleared and cannot be recovered. Backup data in advance.

Automatic Deletion upon Expiration/Overdue

After an instance expires/is overdue, it can be retained in the console for up to 7 calendar days. If you complete the renewal within 7 days after expiry, you can continue to use it. For more details, see Payment Overdue.

If you do not renew your TDMQ for Apache Pulsar cluster within 7 days (including the 7th day) of its expiration, the system will start releasing resources at midnight on the 8th day after expiration. The data in the expired instances will be cleared and cannot be recovered.

Note:

Clusters in a quarantined state cannot produce or consume, but the data and configurations saved within the cluster will not be deleted.

For clusters in a quarantined state within 7 days, you can go to the cluster list page in the console, and click Renew in the operation column. Once the renewal is successful, the cluster will return to a running state and can be used normally.

Access management

Last updated：2025-04-01 11:34:26

Overview

This document describes how to implement mutual access between the resources in your current VPC and TDMQ for Apache Pulsar. Therefore, it can be ensured that the deployed producer/consumer clients can properly communicate with TDMQ for Apache Pulsar.

Prerequisites

You have purchased CVM or TKE resources and configured a VPC.

Directions

1. Log in to the TDMQ for Apache Pulsar console. Enter the **Cluster Managent** page, and click the ID of the target cluster to enter the basic information page.
2. Select the **Access Point** tab, and click **Create**. In the new VPC access point dialog box, select the VPC and subnet, and fill in the remarks.
VPC: Select the VPC network where your deployed producer or consumer resides.
Subnet: Select the subnet according to your IP allocation method.
3. Click **Submit** to complete the access to the VPC network.

4. Configure a security group policy. Ensure that the security group hosting the test program allows traffic through on TCP ports 6000-7000.
Note
You can copy the access point address from the address bar within the access point list. For detailed information, see SDK Overview.

Public Network Access

Currently, only the professional edition supports creating public network access points. Unless necessary, recommend you use VPC internal network access.

Operation Steps

1. Log in to the TDMQ for Apache Pulsar console, enter the **cluster management** page, click the "ID" of the target cluster, and enter the basic information page.
2. Select the **Access Point** tab, click **Create**, and select Public Network for the routing type.
3. Click **Submit** to complete public network access.
4. Operation list. Click **security policy configuration** to configure the IP list to be allowed.

Instructions

1. Public network access point. A cluster can only create one.
2. If you do not configure a security policy, default to all deny. Display 127.0.0.1 on the interface.
3. The number of security policies cannot exceed 50.
4. Supports configuration of subnet ranges: /24 ~ /32.

Billing Information

Public network bandwidth cost. Currently only support annual and monthly billing mode.

Bandwidth	Price (USD/Month)				
	Beijing, Guangzhou, Shenzhen Finance, Shanghai, Nanjing, Chengdu, Chongqing, Qingyuan	**Hong Kong (China), Taipei (China), Silicon Valley, Virginia, São Paulo**	**Singapore, Frankfurt**	**Bangkok, Tokyo, Seoul**	**Shanghai Auto-Driving Zone**
1Mbps	3.150	4.110	3.151	3.425	4.726
2Mbps	6.301	8.219	6.301	6.849	9.452
3Mbps	9.726	12.329	9.452	10.274	14.589
4Mbps	13.151	16.438	12.603	13.699	19.726
5Mbps	17.123	20.548	15.753	17.123	25.685
6 Mbps or higher (n is the	17.123+ 10.959 ×(n - 5)	20.548+ 13.699 ×(n - 5)	15.753+ 10.959 ×(n - 5)	17.123+ 10.959 ×(n - 5)	25.685+ 16.438 ×(n - 5)

configured bandwidth limit)					

Direct Connection/Cross-Region Access

Last updated：2025-04-01 11:34:27

Background

VPC access points provided by the TDMQ for Apache Pulsar only support client access in the same region VPC network. Users accessing through Direct Connect or across regions cannot directly access through the VPC access point.

For users in the above-mentioned access scenario, they need to configure the domain name parsing of the access point to gain access.

Note:

Supported only by professional clusters.

Access Through Direct Connect

Step 1: Obtaining the VIP Address of the Cluster Access Point

The current feature has not yet been productized, and the VIP Address can be accessed through submitting a ticket or post-sales architecture.

Step 2: Configuring Domain Name Parsing

Use Private DNS for domain name parsing, and configure the domain name to parse to the VIP provided by the product side.

1. Creating a Private Domain

Click to enter the Private DNS Console, and then click **Private Domain List**.

Enter the creation page.

In section 1, fill in the TDMQ for Apache Pulsar access point domain name.

In section 2, configure the region and VPC network where the client is located.

In section 3, enable recursive parsing of subdomains.

2. Adding Domain Name Parsing Records

After creation, click to enter the created private domain and set the domain name parsing records.

In section 1, fill in the domain name prefix. It is recommended that the field be cluster id.vpcid.pulsar.ap-region.qcloud.
In section 2, fill in the VIP provided by the product side.
After you fill in the information, save and submit. Then, the client will request verification.

Cross-Region Access

Cross-region access requires using the Cloud Connect Network product to establish a network access channel.
For details on the configuration, please see the Cloud Connect Network Operation Guide, and follow these directions:
1. Create a Cloud Connect Network instance
2. Associating a Network Instance

Namespace

Last updated：2024-06-28 11:31:36

Overview

Namespace is a resource management concept in TDMQ for Apache Pulsar. It can typically be used to isolate different business scenarios and to configure dedicated settings, such as message retention period. Different namespaces are isolated from each other in terms of topics, subscriptions, and role permissions.
This document describes how to create multiple namespaces in TDMQ for Apache Pulsar to use the same TDMQ for Apache Pulsar cluster in different scenarios.
Note:
Topic and subscription names must be unique in the same namespace.

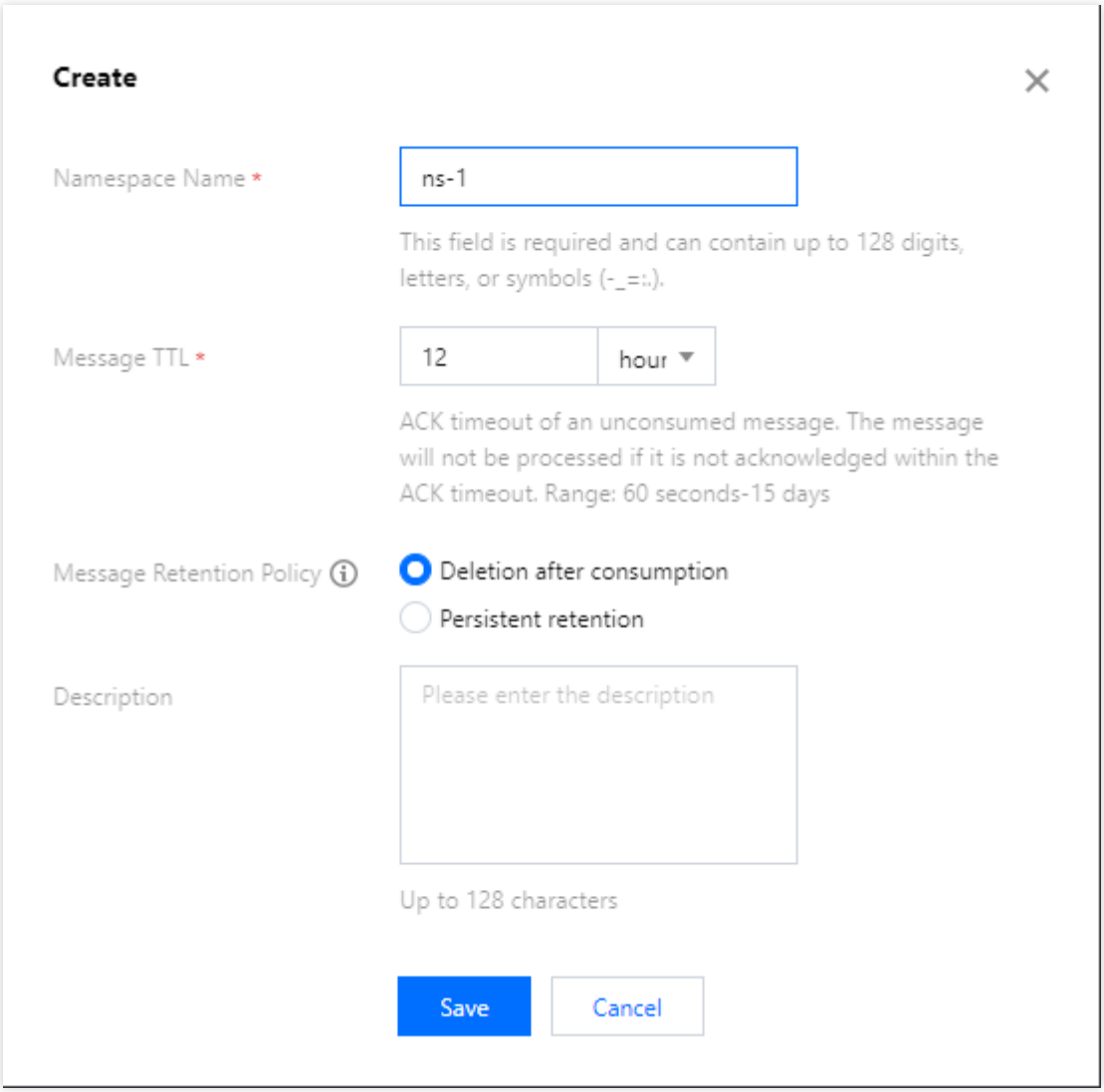
Directions

Note:
If the TDMQ for Apache Pulsar cluster you create is on v2.6.1, a default namespace called `default` will be created with a default message TTL of 7 days. This namespace can be modified but not deleted.
If the TDMQ for Apache Pulsar cluster you create is on v2.7.1 or later, no default namespace will be automatically created.

Creating a namespace

1. Log in to the TDMQ for Apache Pulsar console and enter the **Namespace** page.
2. On the **Namespace** page, select a region and click **Create**.
3. In the **Create Namespace** dialog box, configure the namespace attributes:
Namespace Name: Enter the namespace name, which is required and cannot be modified after creation. The name can contain up to 128 letters, digits, and symbols "-_=:.".
Message TTL: Set the acknowledgement timeout for an unconsumed message. The message will not be processed if it is not acknowledged within the timeout. Value range: 60 seconds to 24 hours.
Message retention policy
Deletion after consumption: Messages will be cleared within a certain period of time after being acknowledged successfully to save storage space.
Note:
If there are no subscriptions under a topic, the messages just produced will be asynchronously cleared.

Persistent retention: No matter whether messages are consumed or not, they will be stored persistently within the maximum retention period and maximum storage space and then deleted chronologically after the limit is reached.
Auto-Create Subscription: Whether a subscription can be automatically created by the client.
Description: Enter the namespace descriptions.
4. Click **Save**.



Note:

After the above steps, you can create a topic in the namespace as instructed in Topic Management to produce and consume messages.

Modifying a namespace

You can modify a namespace in the following steps:
1. On the Namespace list page, click **Edit** in the **Operation** column of the target namespace to enter the editing page.
2. Modify the message retention period or description and click **Save**.

Deleting a namespace

You can delete a created namespace in the following steps:

1. On the Namespace list page, click **Delete** in the **Operation** column of the target namespace.
2. In the pop-up deletion confirmation window, click **OK**, and the namespace will be deleted.

Note:

A namespace with topics cannot be deleted.

A role cannot be deleted if it has permissions configured in namespaces.

A namespace associated with VPCs cannot be deleted.

Topic Management

Last updated：2024-06-28 11:31:37

Overview

Topic is a core concept in TDMQ for Apache Pulsar. It is usually used to categorize and manage various messages produced by the system in a centralized manner; for example, messages related to transactions can be placed in a topic named "trade" for other consumers to subscribe to.
In actual application scenarios, a topic often represents a business category. You can decide how to design different topics based on your system and data architectures.
This document describes how to use topics to categorize and manage messages in TDMQ for Apache Pulsar.

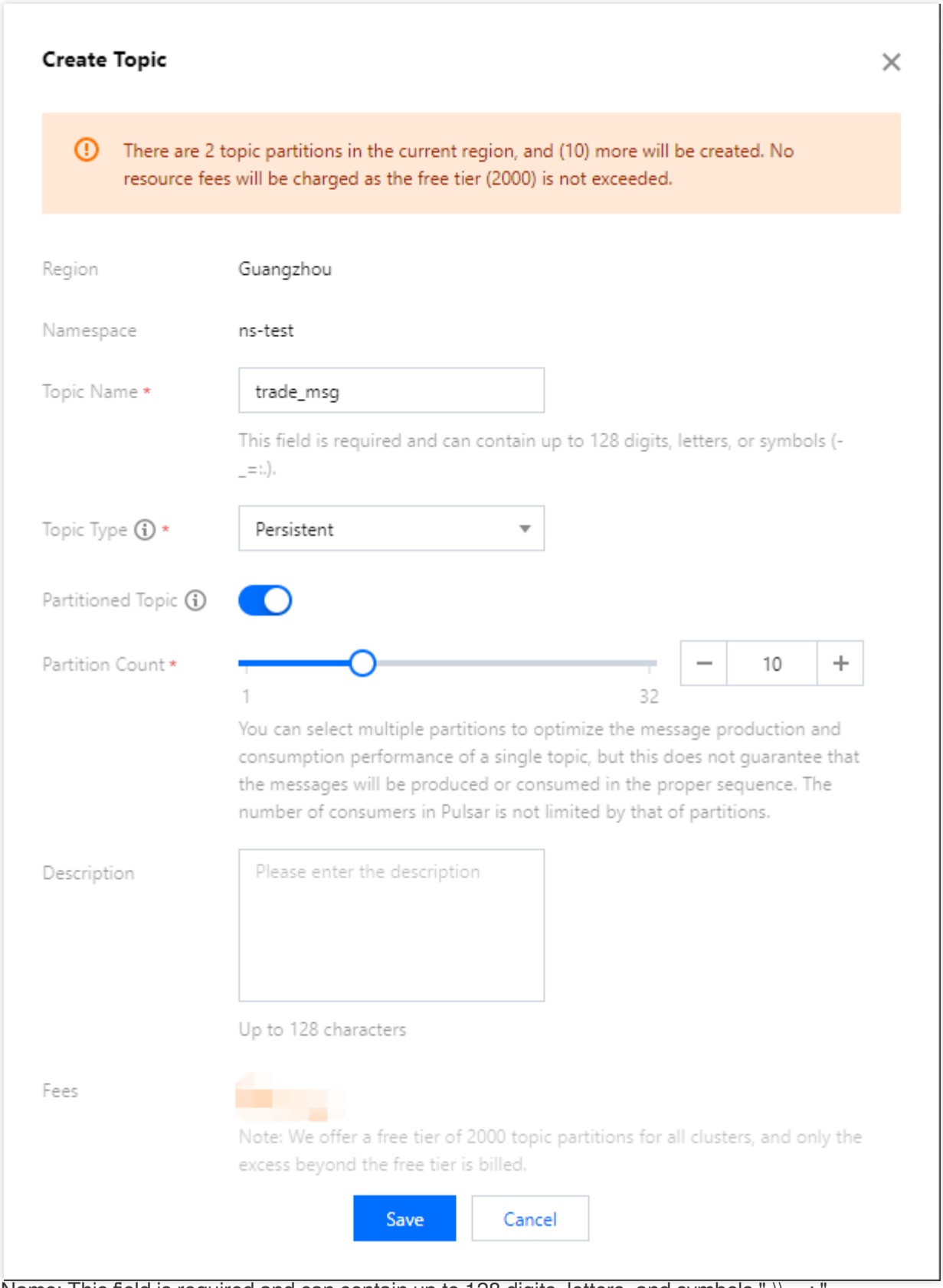
Prerequisite

You have created a namespace.

Directions

Creating a topic

1. Log in to the TDMQ for Apache Pulsar console and click **Topic** on the left sidebar.
2. On the topic management page, click **Create** to pop up the **Create Topic** window.
3. In the **Create Topic** window, enter the following information:



Topic Name: This field is required and can contain up to 128 digits, letters, and symbols "-_=:.".

Topic Type: **Persistent** or **Non-persistent**.

Persistent: Persistently stored messages are stored in the disk with multiple replicas to avoid message loss. Such messages are suitable for scenarios that require high data reliability such as financial or business transactions.

Non-persistent: Non-persistently stored messages are directly delivered to an online subscriber and will be deleted upon successful delivery. They will be directly deleted if there are no online subscribers. Such messages are suitable for stream processing or other scenarios that do not require high data reliability. They can only be sent and received as general messages and don't support features such as query, tracing, delaying, filtering, and rewinding.

Note:

For a non-persistent topic, enter a complete topic name prefixed with `non-persistent://` .

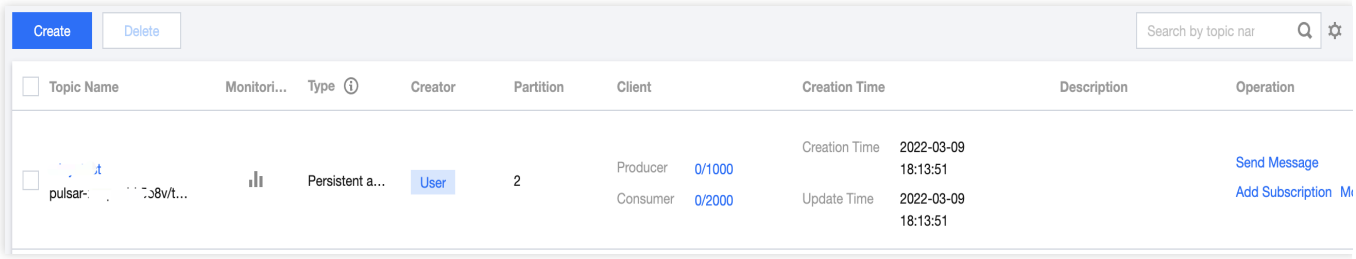
Partitioned Topic:

Pulsar guarantees that messages in a single partition are sequential. If there is only one partition in a topic, messages are globally sequential there.

Multi-partition topics have better performance than single-partition topics. To balance performance and sequence, you can use the Key-Shared subscription mode as instructed in Subscription Mode to make messages partitionally sequential. You only need to mark messages that need to be sequential with the same key and deliver them to the same partition.

Description: Enter the topic descriptions of up to 128 characters.

4. Click **Save**, and you can see the created topic in the topic list.



Parameter	Description
Topic Name	The topic name in the format of `pulsar-****/namespace/topicName`
Monitoring	Click  to view the topic monitoring details. For more information on monitoring metrics, see Viewing Monitoring Information.
Type	The message type, including general, globally sequential, and partitionally sequential. For more information, see Message Type.
Creator	**User** or **System
Partition Count	The number of topic partitions

Client	Producer: It displays the number of producers/the maximum number of producers. Click it to enter the producer details page. For more information, see Producer Management. Consumer: It displays the number of consumers/the maximum number of consumers. Click it to enter the consumer details page. For more information, see Subscription Management. Note: When the value is displayed in orange (warning), the fraction has reached 80%. When it is displayed in red (error), the fraction has reached 90%, in which case you need to close unnecessary client connections.
Creation Time	The creation time of the topic
Description	The topic descriptions

Querying a topic

You can search for topics by topic name in the search box in the top-right corner of the Topic page. TDMQ for Apache Pulsar will perform a fuzzy match and display the search results.

You can also filter topics by **Type** and **Creator** in the topic list.

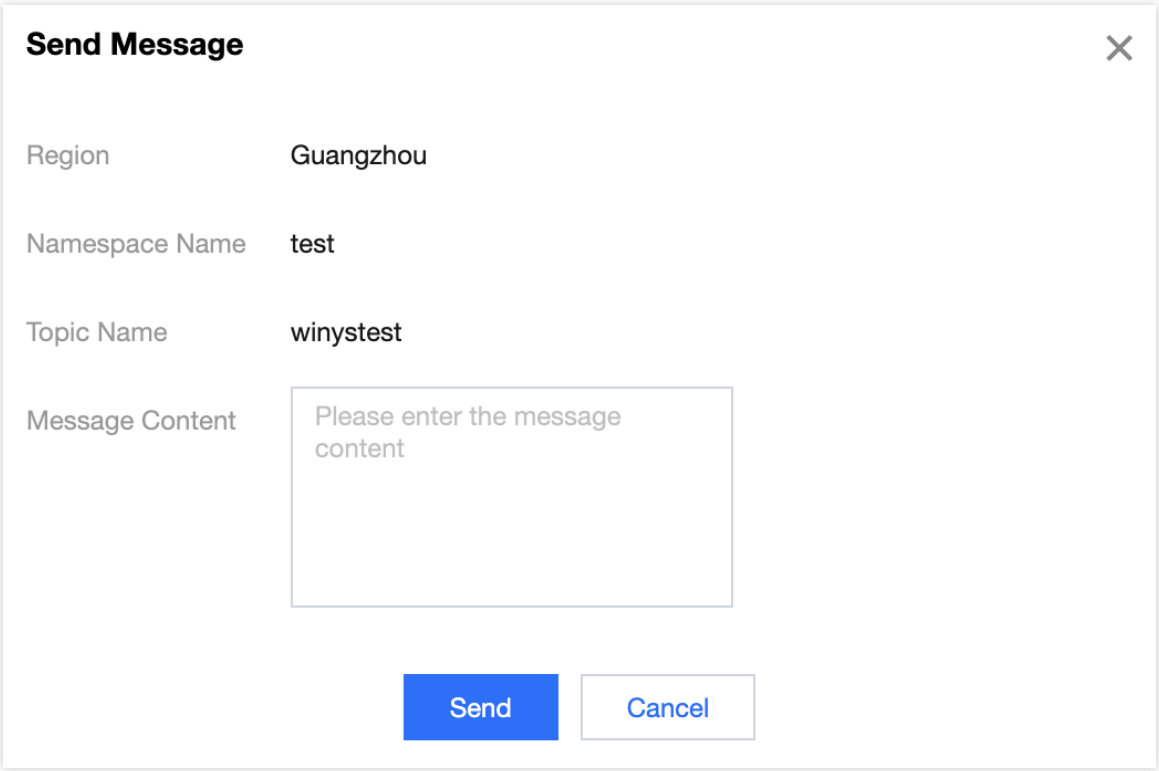
Editing a topic

1. On the Topic page, click **Edit** in the **Operation** column of the target topic.
2. In the pop-up window, you can edit the number of topic partitions (which is 1 for globally sequential messages and cannot be modified) as well as the description.
3. Click **Submit** to complete your edits.

Sending a message

You can manually send a message to the specified topic in the TDMQ for Apache Pulsar console.

1. On the Topic, click **Send Message** in the **Operation** column of the target topic.
2. In the pop-up dialog box, enter the message content. The message size is up to 64 KB.



3. Click **Submit** to send the message. After the message is sent, it can be consumed by any subscribers to the topic.

Adding a subscription

You can manually create a subscription in the TDMQ for Apache Pulsar console.

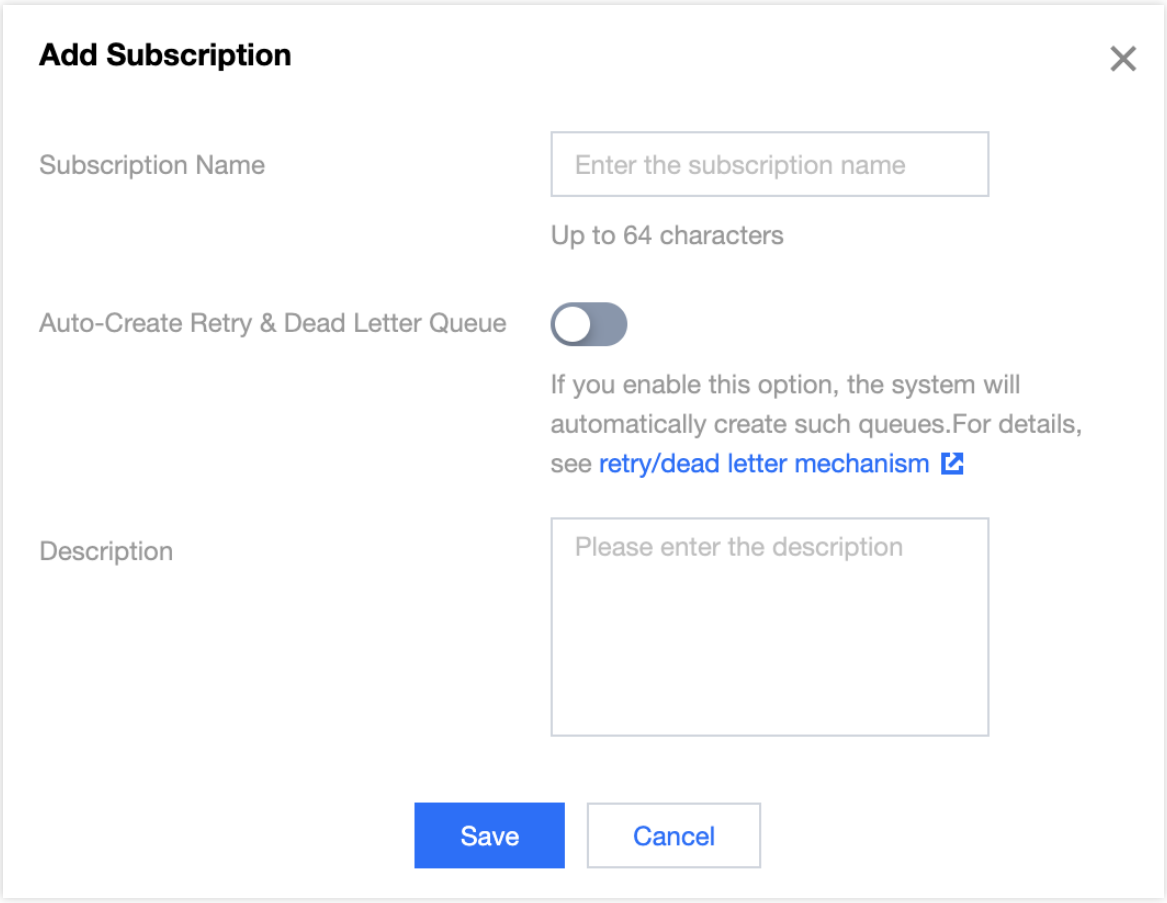
1. On the Topic page, click **Add Subscription** in the **Operation** column of the target topic.

2. Enter the subscription name and description in the pop-up window.

Subscription Name: It can contain up to 64 characters.

Auto-Create Retry & Dead Letter Queue: You can choose whether to automatically create a retry letter topic and a dead letter topic.

Description: Enter descriptions of up to 200 characters.



3. Click **Save** to complete the creation.

You can click **View Subscription** in the **Operation** column of a topic to view its subscriptions, and the subscription just created will be displayed in the list.

Note:

If you select **Auto-Create Retry & Dead Letter Queue**, TDMQ for Apache Pulsar will automatically create a retry topic and a dead letter topic, which will be displayed in the topic list as two new topics named "subscription name + RETRY" and "subscription name + DLQ", respectively.

For the concepts and usage of retry letter and dead letter topics, see Retry Letter Topic and Dead Letter Topic.

Deleting a topic

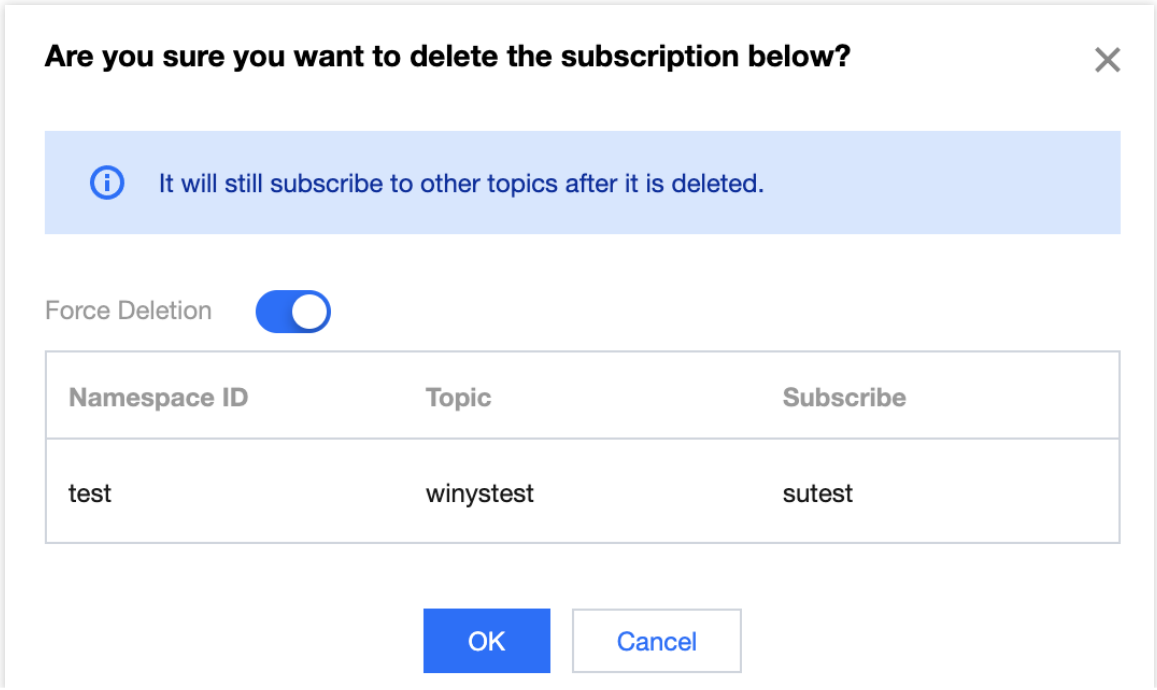
Note:

After a topic is deleted, all unconsumed messages retained in it will be cleared; therefore, proceed with caution.

1. On the **Topic** page, click **More** > **Delete** in the **Operation** column of the target topic. You can also select multiple topics and click **Delete** at the top of the topic list.

2. In the pop-up window, click **Delete**.

Force Deletion: After this option is enabled, a topic will be forcibly deleted even if it has subscriptions. Its subscriptions will also be deleted.


Are you sure you want to delete the subscription below?
It will still subscribe to other topics after it is deleted.
Force Deletion
Namespace ID
Topic
Subscribe
test
winystest
sutest
OK
Cancel

Subscription Management

Last updated：2024-06-28 11:31:37

Overview

In the TDMQ for Apache Pulsar console, a subscription represents a specific consumer and its subscription to a topic. A consumer can consume all messages in a topic after subscribing to it. One subscription can subscribe to multiple topics; for example, after a subscription is created under a topic, it will subscribe to both the current topic and the automatically created retry queue topic.
This document describes how to configure the subscriptions to a topic in **Subscription Management** in TDMQ for Apache Pulsar.

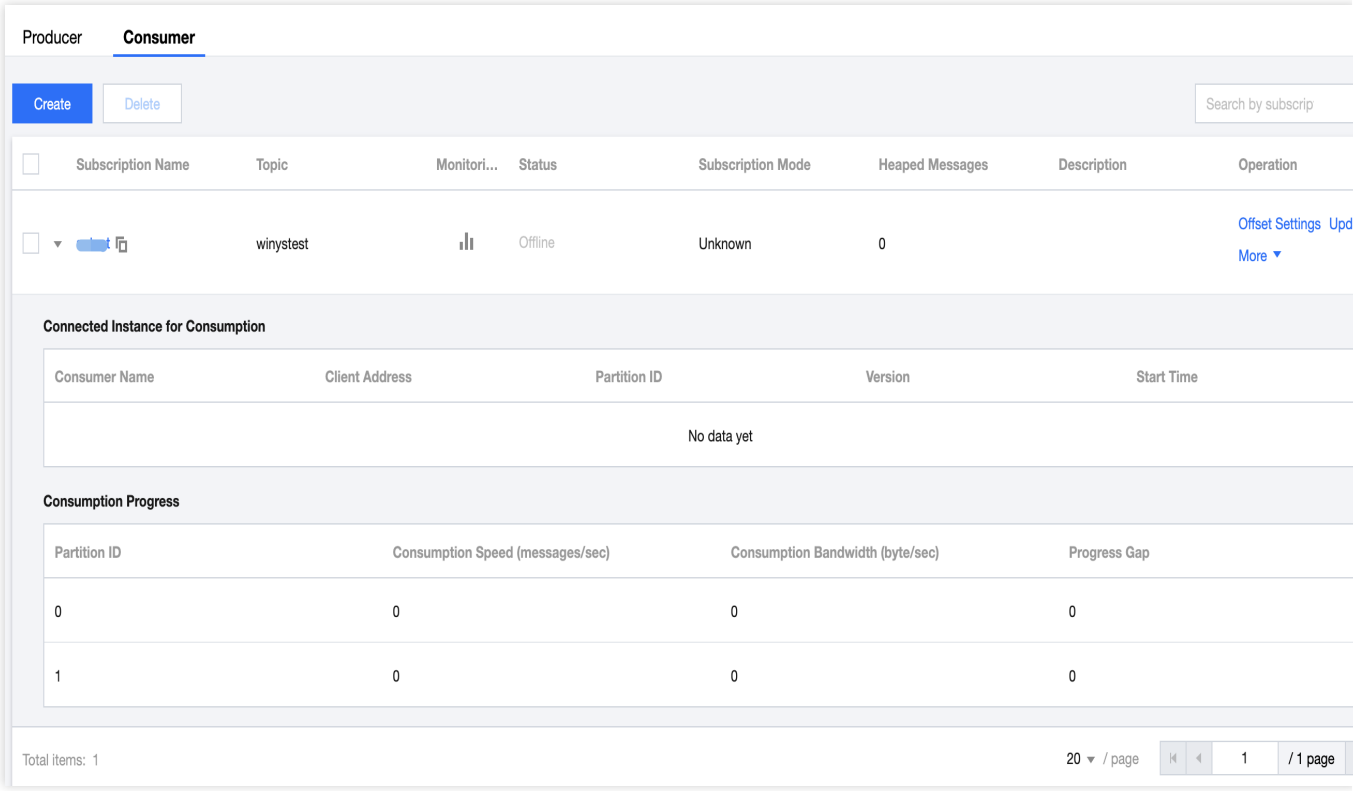
Prerequisites

You have created a namespace and a topic.
You have created a message producer and consumer based on the SDK provided by TDMQ for Apache Pulsar, and they run properly.

Directions

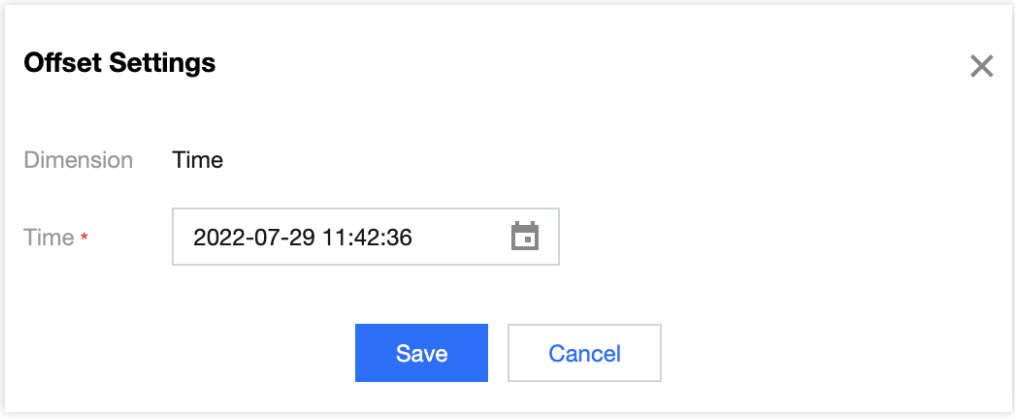
Viewing subscription details

1. Log in to the TDMQ for Apache Pulsar console and click **Topic Management** on the left sidebar.
2. On the **Topic Management** list page, click **View Subscription/Consumer** in the **Operation** column of the target topic to enter the subscription list.
3. In the subscription list, the first-level list displays all subscriptions to the current topic. After expanding the second-level list, you can see the consumer instances connected to each subscription and the consumption progress of each segment.



Setting an offset

1. In the subscription list, click **Offset Settings** in the **Operation** column to manually set the consumer offset for each subscription by time (that is, specify the time point from which the consumers under the subscription start to consume messages).
2. Click **Submit**.



Recreating retry/dead letter topics

As you can manually delete a topic, if you want the deleted retry/dead letter topics to be created again by the system, you can click **Recreate Retry/Dead Letter Queues** in the **Operation** column of the subscription.

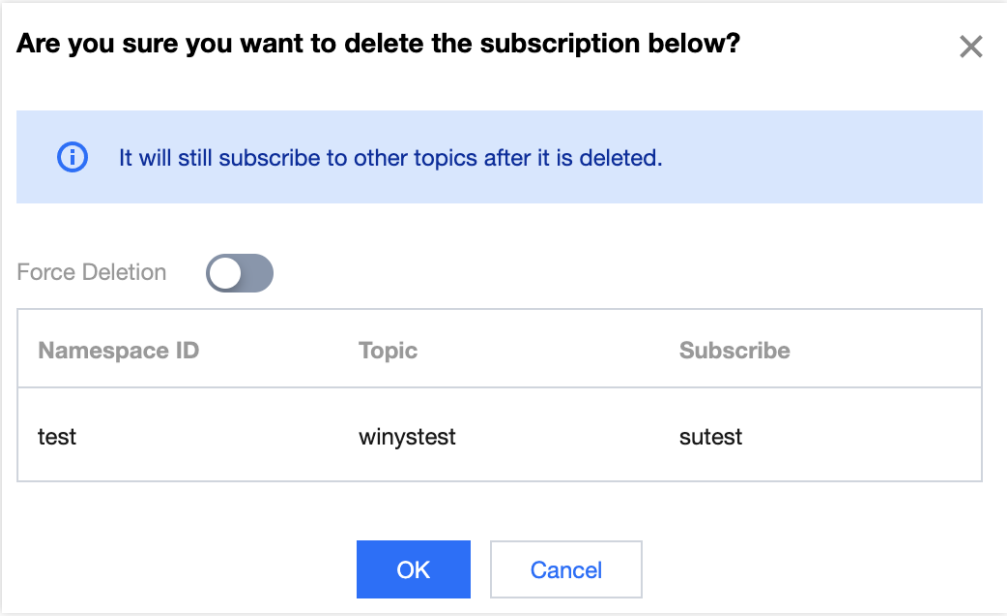
Deleting a subscription

Note:

When a subscription under a topic is deleted, if it has also subscribed to other topics (including the automatically created retry/dead letter topics), it will not be removed from such topics.

1. In the subscription list, click **More** > **Delete** in the **Operation** column of the target subscription. You can also select multiple subscriptions and click **Delete** at the top of the subscription list.
2. In the pop-up window, click **Submit**.

Force deletion: After this option is enabled, a subscription will be forcibly deleted even if it has active consumer connections.



Producer Management

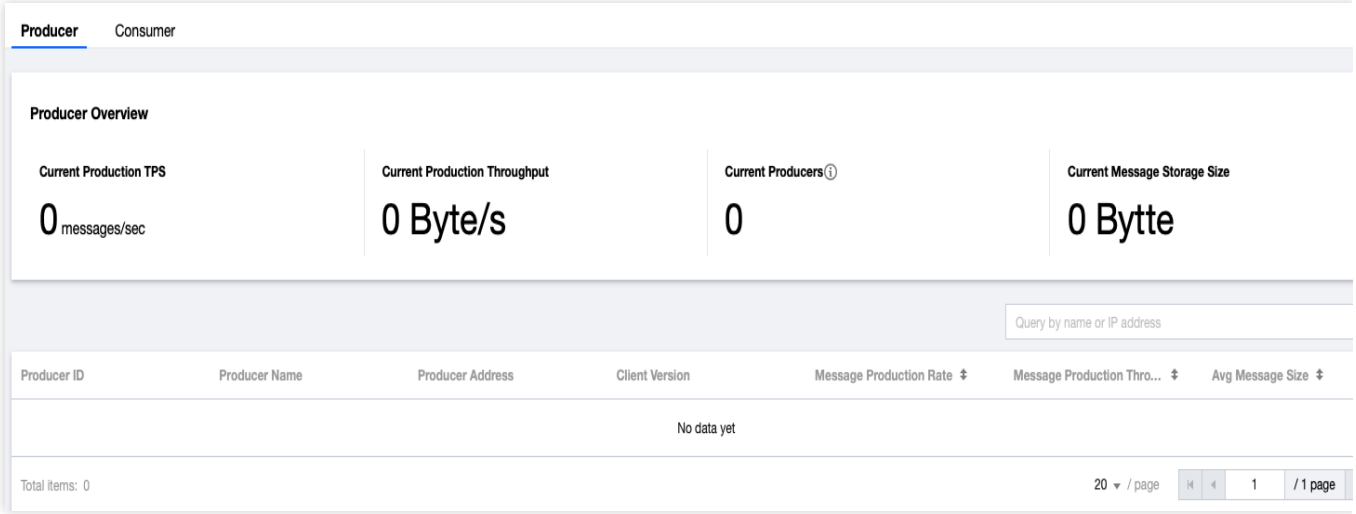
Last updated：2024-06-28 11:31:37

Overview

This document describes how to view the details of a producer connected to a topic in the TDMQ for Apache Pulsar console, so that you can stay up to date with the status of the connected producer and troubleshoot problems promptly.

Directions

1. Log in to the TDMQ for Apache Pulsar console and click **Topic Management** on the left sidebar.
2. On the **Topic Management** list page, click **View Producer** in the **Operation** column of the target topic to enter the producer list.



Producer overview

Current Production TPS: Total number of messages produced by producers currently connected to the topic per second.
Current Production Throughput: Size of messages produced by producers currently connected to the topic per second.
Current Producers: Total number of producers currently connected to the topic (the listed items are combinations of producers and partitions; therefore, if there are multiple AZs, the number of producers displayed on the overview page

will be less than the number of listed items).

Current Message Storage Size: Total size of messages currently stored in the topic memory.

Producer details

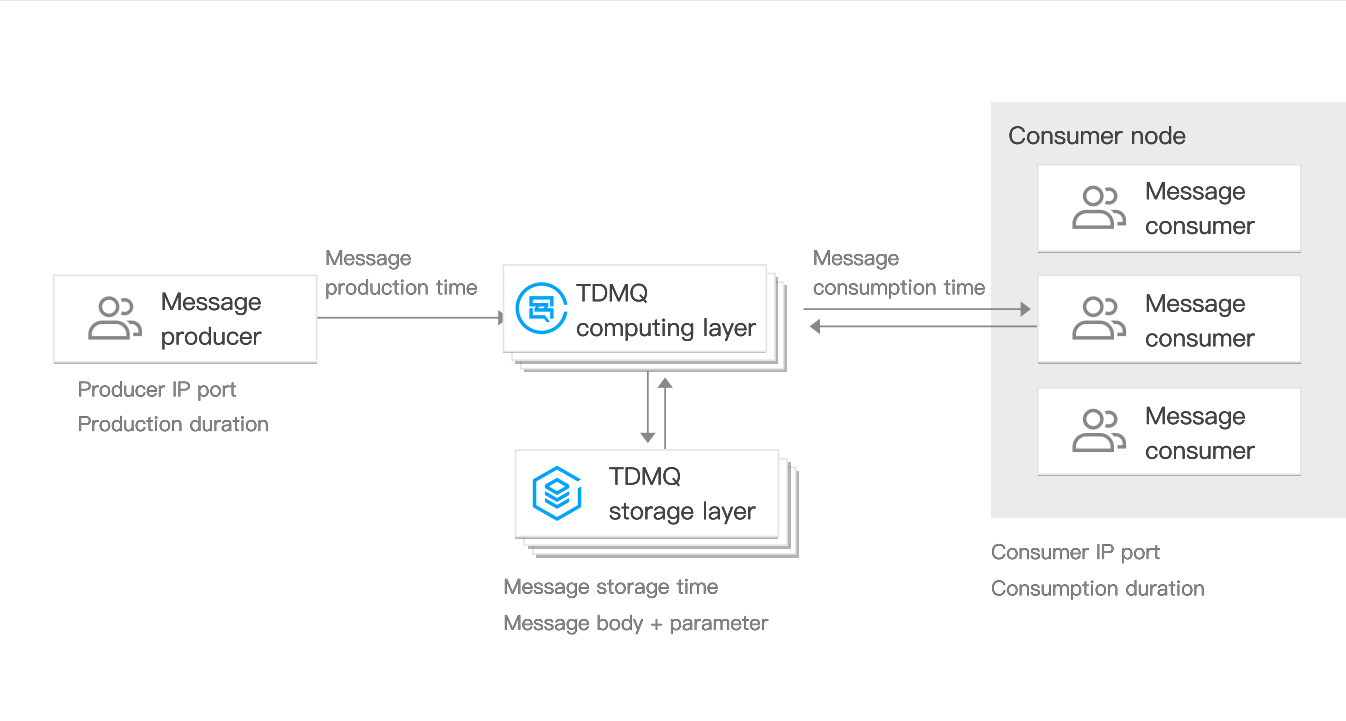
Parameter	Description
Producer ID	Producer ID.
Producer Name	Message producer name.
Producer Address	Message producer address and port.
Client Version	Pulsar client version.
Message Production Rate (Messages/Sec)	Number of messages produced by producers to the topic per second.
Message Production Throughput (Mbps)	Size of messages produced by producers per second.
Avg Message Size (Bytes)	Average size of messages produced by producers to the topic.

Message Query and Trace

Last updated：2024-06-28 11:31:37

TDMQ for Apache Pulsar records the complete flow in which a message is sent from the producer to the TDMQ for Apache Pulsar server and then consumed by the consumer, and then displays the flow as a message trace in the console.

A message trace records the entire process in which the message is sent from the producer to the TDMQ for Apache Pulsar server and eventually to the consumer, including the duration of each stage (accurate down to the microsecond), execution result, producer IP, and consumer IP.



Overview

You can use the message query feature in the TDMQ for Apache Pulsar console to view the content, parameters, and trace of a specific message by time or by the message ID displayed in the log. This enables you to:

View the specific content and parameters of the message.

View from which producer IP a message was sent, whether it was sent successfully, and the specific time when it arrived at the server.

View whether the message was persistently stored.

View which consumers consumed the message, whether it was consumed successfully, and the specific time when its consumption was acknowledged.

View the MQ's message processing latency to analyze the performance of the distributed system.

Query Limits

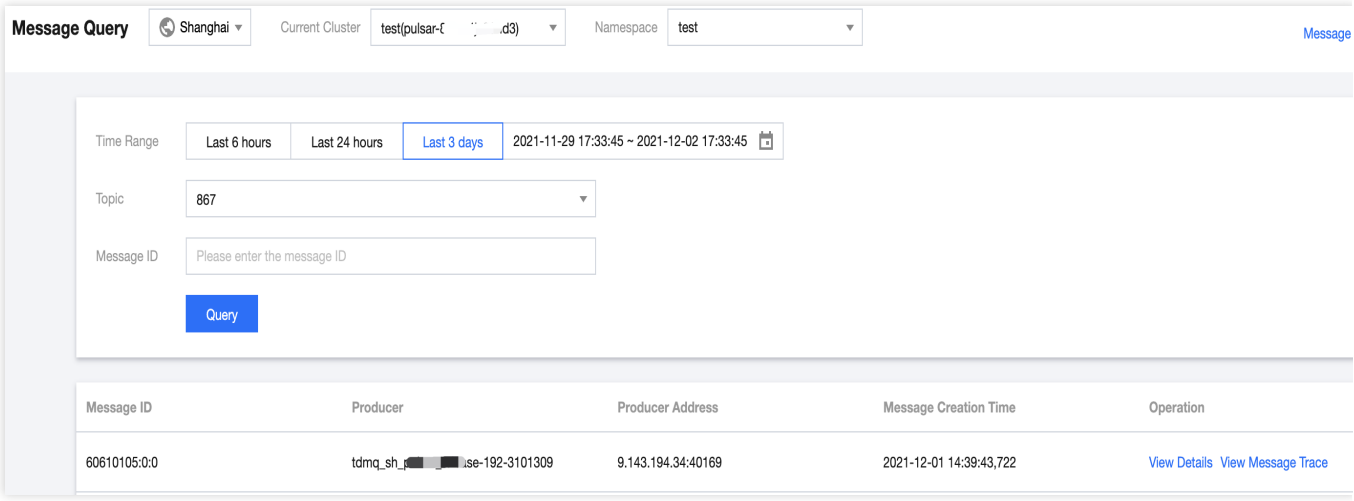
You can query messages in the last 3 days.
You can query up to 65,536 messages at a time.

Prerequisites

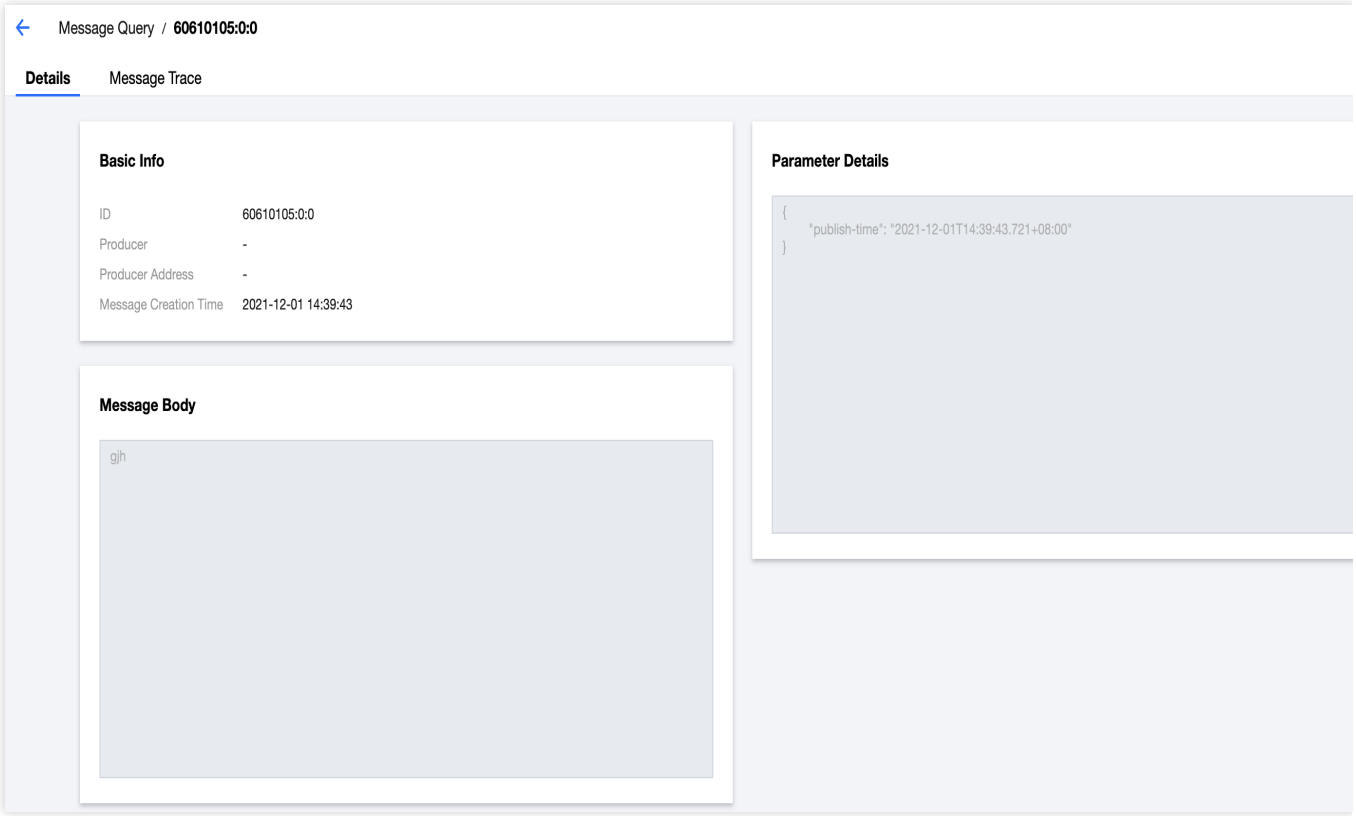
You have deployed the producer and consumer services as instructed in the SDK documentation, and they produced and consumed messages in the last 7 days.

Directions

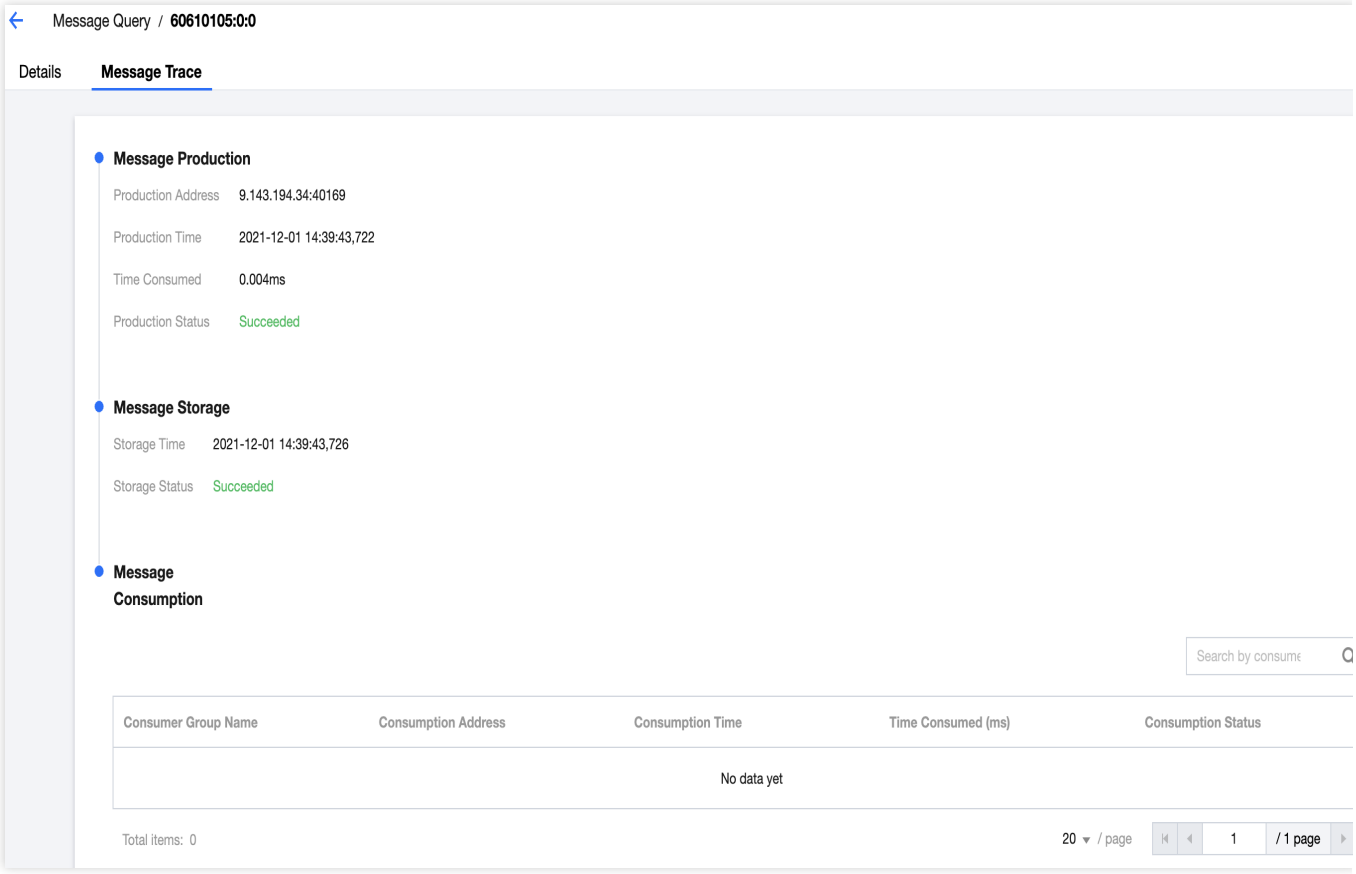
1. Log in to the TDMQ for Apache Pulsar console and click **Message Query** on the left sidebar.
2. On the **Message Query** page, select the region and environment first and then the time range for query. If you know the message ID, you can also enter it for exact match query.
3. Click **Query**, and the list below will display paginated results.



4. Click **View Details** in the **Operation** column of the target message to view its basic information, content (message body), and parameters.



5. Click **View Message Trace** in the **Operation** column or select the **Message Trace** tab on the details page to view the trace of the message. For more information, see Message Trace Query Result Description.



Message Trace Query Result Description

A message trace query result consists of three parts: message production, message storage, and message consumption.

Message production

Parameter	Description
Producer Address	Address and port of the producer.
Production Time	The time when the TDMQ for Apache Pulsar server acknowledged message receipt, accurate down to the millisecond.
Sending Duration	The time it took to send the message from the producer to the TDMQ for Apache Pulsar server, accurate down to the microsecond.
Production Status	Message production success or failure. If the status is **Failed**, it is generally because the header of the message was lost during sending, and the above fields may be empty.

Message storage

Parameter	Description
Storage Time	The time when the message was persistently stored (TDMQ for Apache Pulsar currently adopts the strong consistency mode where messages will be acknowledged only after being stored, so the storage time is the same as the production time; if in high performance mode, they are different).
Storage Status	Message storage success or failure. If the status is **Failed**, the message failed to be stored on the disk, which is possibly because the underlying disk was damaged or full. In this case, submit a ticket for assistance as soon as possible.

Message consumption

Message consumption is displayed in the form of a list. TDMQ for Apache Pulsar supports multi-subscription mode, where a message may be consumed by multiple consumers in multiple subscriptions.
The information displayed in the list is as described below:

Parameter	Description
Consumer Group Name	Subscription name.
Consumer Address	Address and port of the consumer receiving the message.
Consumption Time	The time when the TDMQ for Apache Pulsar server received an acknowledgment (ack) from the consumer.
Consumption Duration	Elapsed time between message delivery by the server to the consumer and ack receipt by the server from the consumer, accurate down to the microsecond.
Consumption Status	Message consumption success or failure. This field will be displayed as **Failed** if the consumer returns a negative-acknowledgment (nack).

Monitoring and Alarms
Cluster Monitoring

Last updated：2024-08-19 16:26:10

Overview

TDMQ for Apache Pulsar supports cluster monitoring features, including computing metrics, storage metrics, and statistical distribution of message size for clusters. You can analyze cluster usage based on these monitoring data and process potential risks promptly. You can also set alarm rules for monitoring item, so you can receive alarm messages when there are data exceptions, address risks promptly, and ensure the stable operation of the system.

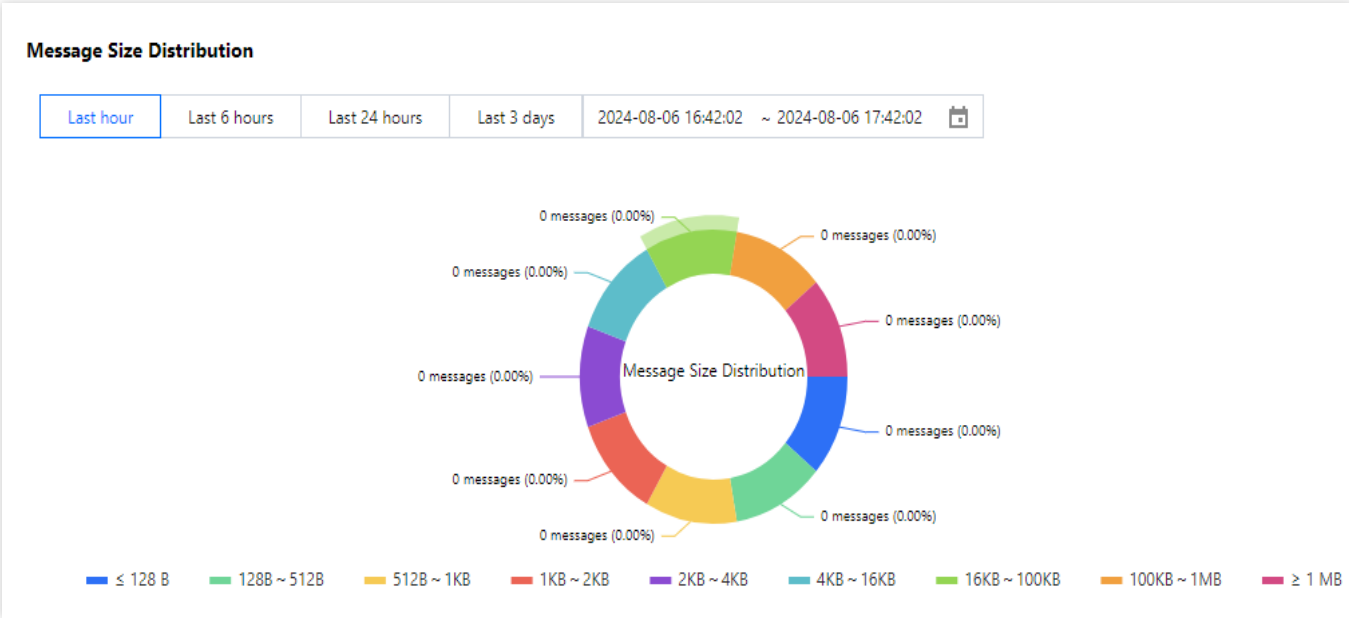
Monitoring Metric

The cluster monitoring metrics supported by the TDMQ for Apache Pulsar are as follows:

Key Metric Monitoring

Metric Type	Metrics	Unit
Computing Metrics	Pulsar Cluster TPS	Count/s
	Production TPS Peak	Count/s
	Consumption TPS Peak	Count/s
	Production Bandwidth Peak	Bytes/s
	Consumption Bandwidth Peak	Bytes/s
Storage Metrics	Storage Usage	Bytes

Message Size Distribution Statistics



Viewing Monitoring

1. Log in to the TDMQ for Apache Pulsar console.
2. Go to the **Cluster Management** page, and click the target cluster's ID to enter the basic information page.
3. Select the **Monitoring Information** tab. After selecting the time range and time granularity, you can view the cluster monitoring data.

Topic Monitoring

Last updated：2024-08-19 16:24:22

Overview

TDMQ for Apache Pulsar allows you to monitor the topic resources created under your account, so that you can keep track of the status of your topics in real time and troubleshoot possible issues to ensure stable business operations. This document describes how to view monitoring metrics and their descriptions in the TDMQ console.

Descriptions of Monitoring Metrics

Metrics	Description
Production Rate (Count/s)	Number of messages sent to the topic by producers per second in the selected time range.
Consumption Rate (Count/s)	Number of messages consumed by all consumers under the topic per second in the selected time range.
Production Traffic (Bytes/s)	Data size of messages sent to the topic by producers per second in the selected time range.
Consumption Traffic (Bytes/s)	Data size of messages consumed by all consumers under the topic per second in the selected time range.
Heaped Message Size (Bytes/s)	Size of heaped messages.
Number of Producers (Count)	Number of producers producing messages to the topic.
Number of Consumers (Count)	Number of subscribers to the topic.

Viewing Monitoring

1. Log in to the TDMQ for Apache Pulsar Console.
2. In the left sidebar, click **Topic** , and select the region, cluster, and namespace resources.
3. In the Topic list, find the target Topic, click **Monitoring** column


icon, and select the time range and granularity. Then you can view the monitoring data of Topic.

Alarm Configuration

Last updated：2024-12-02 17:10:17

Overview

Tencent Cloud provides the Cloud Monitor service for all users by default; therefore, you do not need to manually activate it. TCOP will start collecting monitoring data only after a Tencent Cloud product is used.
TDMQ for Apache Pulsar allows you to monitor the resources created under your account, so that you can keep track of the status of your resources in real time. You can configure alarm rules for monitoring metrics. When a monitoring metric reaches the set alarm threshold, TCOP will notify you of exceptions in time via the notification channels you specified.

Directions

Configuring alarm policy

An alarm policy can determine whether an alarm notification should be sent based on the comparison between the monitoring metric and the given threshold in the selected time period. You can promptly take appropriate precautionary or remedial measures when the alarm is triggered by a TDMQ for Apache Pulsar status change. Properly configured alarm policies help improve the robustness and reliability of your applications.
Note:
Be sure to configure alarms for your instance to prevent exceptions caused by traffic spikes or specification limits.
1. Log in to the TCOP console.
2. On the left sidebar, select **Alarm Configuration** > **Alarm Policy** and click **Create**.
3. On the **Alarm Policy** page, select a policy type and instance and set the alarm rule and notification template.
Policy Type: select **TDMQ alarm**.
Alarm Object: select the TDMQ for Apache Pulsar resource for which to configure the alarm policy.
Trigger Condition: you can select **Select template** or **Configure manually**. The latter is selected by default. For more information on manual configuration, see the description below. For more information on how to create a template, see Creating trigger condition template.
Metric: For example, if the Tenant-Level Message Production Rate is selected with a statistical granularity of 1 minute. An alarm will be triggered if the tenant-level message production rate exceeds the threshold continuously for N data points within that 1 minute.
Alarm Frequency: for example, "Alarm once every 30 minutes" means that there will be only one alarm triggered every 30 minutes if a metric exceeds the threshold in several consecutive statistical periods. Another alarm will be triggered only if the metric exceeds the threshold again in the next 30 minutes.

Notification Template: you can select an existing notification template or create one to set the alarm recipient objects and receiving channels.

4. Click **Complete**.

For more information on alarms, see Creating Alarm Policy.

Creating trigger condition template

1. Log in to the TCOP console.

2. On the left sidebar, click **Alert Management** > **Alarm Configuration** > **Trigger Condition Template** to enter the template list page.

3. Click **Create** on the **Trigger Condition Template** page.

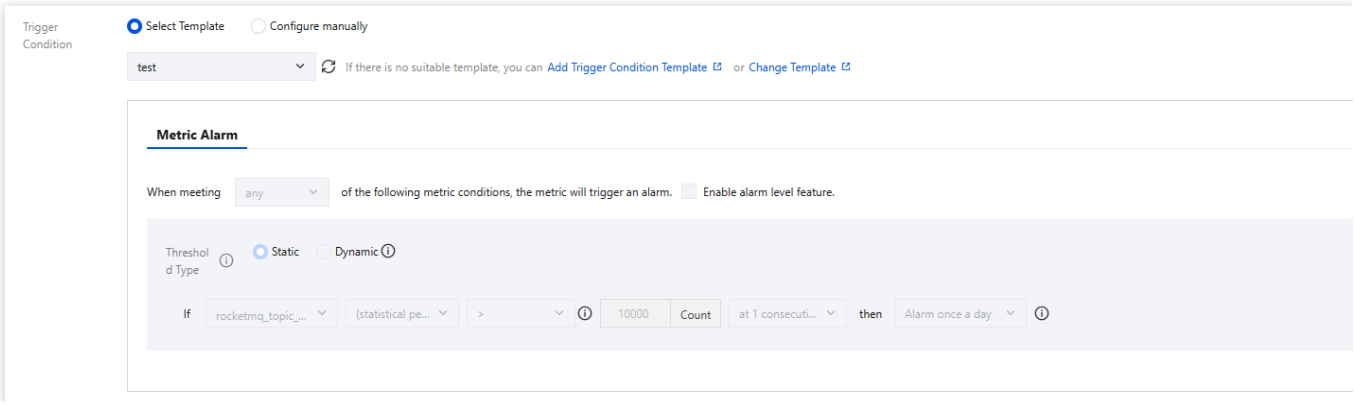
4. On the **Create Template** page, configure the policy type.

Policy Type: select **TDMQ /Pulsar**.

Use preset trigger condition: select this option and the system recommended alarm policy will be displayed.

5. After confirming that everything is correct, click **Save**.

6. Return to the **Create Alarm Policy** page, click **Refresh**, and the alarm policy template just configured will be displayed.



Connecting to Prometheus

Last updated：2025-04-01 11:37:52

TDMQ for Apache Pulsar supports integrating pro cluster monitoring data into users' self-built Prometheus, which facilitates the observation of the TDMQ cluster's operations. It also allows for timely HPA of business workloads through Prometheus monitoring data, making overall online ops more automated.

Advanced Usage:

Using the standard Prometheus monitoring format, you can access data with your own Prometheus through our provided Exporter;

For instance, configuring a Prometheus data source in Grafana or accessing Prometheus data with K8s for Workload HPA, etc.

Note：

If your professional cluster was created before March 25, 2024, enabling this feature requires a cluster upgrade. Contact us for assistance.

User Guide

1. Log in to the TDMQ for Apache Pulsar Pro Cluster console.
2. In the left sidebar, choose **Cluster Management**, and click the target instance's ID to enter the instance basic information page.
3. Click to enter the **Monitoring Information** Sheet page.
4. In the top right corner, click the **TMP Entry Access** button to **Access Monitoring Targets**, and select the appropriate network type and network configuration.

5. Click **Submit** to access a set of monitoring targets.

6. Modify the configuration file prometheus.yml to add a node_exporter scraping task.

```
job_name: prometheus-tdmq-pulsar
honor_timestamps: true
scrape_interval: 60s
metrics_path: /tencent-cloud-metrics/
scheme: http
static_configs:
- targets:
  - 10.x.x.x:10001
  - 10.x.x.x:10002
```

When `honor_timestamps` is set to **true**, Prometheus will use the timestamps provided by the Exporter for its metrics rather than using the timestamps at which the Prometheus server receives these metrics.
`scrape_interval` , the frequency of scraping monitoring metrics data. Currently at **minute-level**.
`metrics_path` , the path to access monitoring metrics. Set it to /**tencent-cloud-metrics/.**
`scheme` , the protocol for accessing resources in the configuration. Currently it only supports **http.**
7. Access the corresponding visualization interface to view the configured monitoring metrics.
Note:
1. This feature provides monitoring data at the cluster level, Topic level, and subscription level for pro clusters, aligning perfectly with the metric items on the console. However, unlike the console, where the monitoring data is pre-aggregated, the data through Prometheus is post-aggregated and requires you to manually aggregate and display it on the Grafana dashboard.
2. Due to the different paths of monitoring data collection and different aggregation logic, the data captured by this feature may differ in specific values from the data displayed on the user console.
3. This feature is only supported by pro clusters.

Metric Description

Cluster Level

Metric	Metric Name
Cluster message production rate	pulsar_caculate_rate_in
Cluster message consumption rate	pulsar_caculate_rate_out
Cluster message storage size	pulsar_storage_size
Cluster production bandwidth peak	pulsar_throughput_in
Cluster consumption bandwidth peak	pulsar_throughput_out

Topic Level

Metric	Metric Name
Message production rate	pulsar_caculate_rate_in
Message consumption rate	pulsar_caculate_rate_out
Message production throughput	pulsar_throughput_in

Message consumption throughput	pulsar_throughput_out
Producer count	pulsar_producers_count
Consumer count	pulsar_consumers_count
Message storage size	pulsar_storage_size
Message backlog count	pulsar_msg_backlog
Message backlog size	pulsar_storage_backlog_size
Producer rate limiting count	pulsar_publish_rate_limit_times
Filtered message count	pulsar_tag_filter_rejected_msg_rate

Subscription Level

Metric	Metric Name
Message backlog entries	pulsar_subscription_back_log
Message consumption rate	pulsar_subscription_msg_rate_out
Message consumption throughput	pulsar_subscription_msg_throughput_out
Unacknowledged message count	pulsar_subscription_unacked_messages
Consumer count	pulsar_subscription_consumers_count
Delayed message count	pulsar_subscription_delayed
Message deletion rate	pulsar_subscription_msg_rate_expired
Filtered message count	pulsar_subscription_tag_filter_rejected_msg_rate

Monitoring and Alarm Practices

Last updated：2025-04-01 14:26:16

Based on the professional cluster specifications and usage limits provided by the product, the following are some recommended metrics and alert items for your reference.

Core Metrics and Impact

Dimension	{alarm item}	Configuration Suggestion	Limit Exceeded Impact
Topic	Message backlog used quota percentage	80%	Sending failure will occur after exceeding the limit, and the client will repeatedly reconnect.
	Percentage of used quota for message production number	80%	The default single partition is 5000 TPS. After exceeding the limit, the server will return with a delay, and the sending duration of the client will increase.
	Percentage of used quota for message production traffic	80%	The default single partition is 40 Mbps. After exceeding the limit, the server will return with a delay, and the sending duration of the client will increase.
	Percentage of used quota for message consumption count	80%	The default single partition is 5000 TPS. After exceeding the limit, it may be due to the push rate limit of messages, resulting in message backlog.
	Percentage of used quota for message consumption traffic	80%	The default single partition is 40 Mbps. After exceeding the limit, it may be due to the push rate limit of messages, causing message backlog.
	Number of Producers	800	The upper limit of the number of producers for a single default partition is 1000. After exceeding the limit, new producers cannot be created.
	Number of Consumers	1500	The upper limit of the number of consumers for a single default partition is 2000. After exceeding the limit, new consumers cannot be created.

Subscription	Percentage of used quota for number of unconfirmed messages	80%	The default is 5000 for a single subscription and a single partition. After exceeding the limit, the server will stop pushing messages until the client confirms completion of unacknowledged messages.
	Number of Consumers	800	The upper limit of the number of consumers for a single default subscription in a single partition is 1000. After exceeding the limit, new consumers cannot be created.
Instance	[Pro Edition] Fixed storage utilization of professional cluster	80%	Sending failure will occur after exceeding the limit, and the cluster cannot be written.
	[Pro Edition] TPS usage percentage of Pulsar cluster	80%	Exceeding the limit can lead to high-load running of the cluster, posing a stability risk.
	[Pro Edition] Limited number of tenant throttling write requests per minute	1	After traffic throttling occurs, the server will return with a delay, which will increase the sending duration.

Permission Management

Permission Management Overview

Last updated：2024-08-19 16:35:36

This document introduces the permission management content for the TDMQ for Apache Pulsar.

Permission Management and Control Service	Introduction	Related Links
CAM	CAM is an access management service provided by Tencent Cloud, which helps you to manage access to Tencent Cloud services and resources securely and conveniently. You can use CAM to create sub-users, user groups, and roles, and control their access scope through policies. For more details, see Tencent Cloud Cloud Access Management product.	-
JWT	JWT is an authentication tool provided by TDMQ for Apache Pulsar, which is used for securely producing and consuming messages. You can access the corresponding Topic resources by configuring the Token in the client parameters.	Role and Authentication JWT Authentication Configuration

Pulsar Instance Permission Management Granting Sub-Account Access Permissions

Last updated：2024-08-19 16:39:56

Basic Concepts of CAM

The root account authorizes sub-accounts by binding policies, which can be precisely set at the **[API, resource, user/user group, allow/deny, condition]** dimension.

Account System

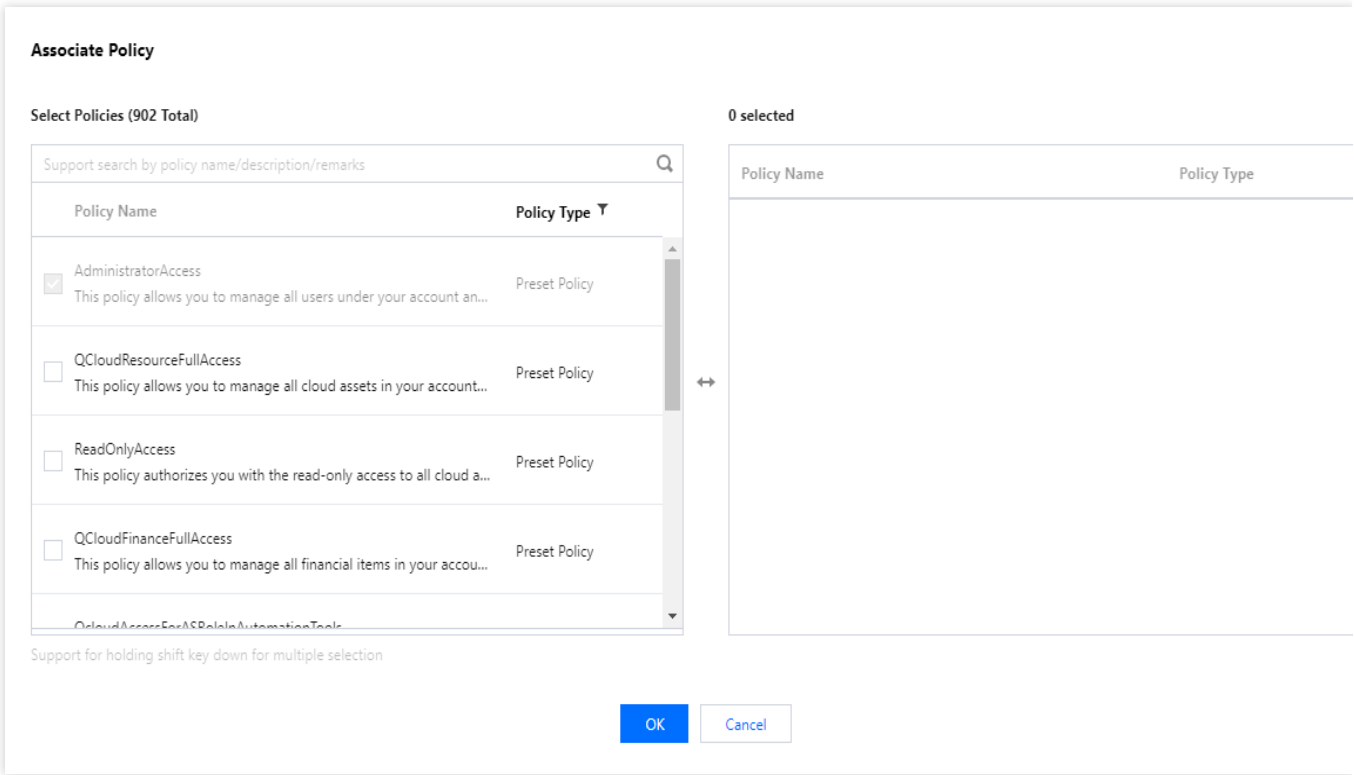
Root account: Owns and has unrestricted access to all Tencent Cloud resources.
Sub-account: Includes sub-users and collaborators.
Sub-user: Created by the main account and completely belongs to the root account that created the Sub-user.
Collaborator: A user with a main account identity added as a collaborator to the current root account, becoming one of its sub-accounts and able to switch back to the root account identity
Identity credentials: Includes log-in credentials and access certificates. **Log-in credentials** refer to a user's log-in name and password. **Access certificates** refer to Tencent Cloud API keys (SecretId and SecretKey).

Resource and Permission

Resource: An object being operated in Tencent Cloud services, such as a CVM instance, a COS bucket, or a VPC instance
Permission: An authorization to allow or disallow some users to perform certain operations. By default, **a root account has full access to all the resources under the account**, while **a sub-account does not have access to any resources under the root account**.
Policy: A syntax rule that defines and describes one or more permissions. **The root account** performs authorization by **associating policies** with users/user groups.

Sub-Account Using Pulsar

To ensure that the sub-account can successfully use Pulsar, the root account needs to authorize the sub-account.
Root account logs in to CAM Console, finds the corresponding sub-account in the sub-account list, and clicks the **Authorize** in the operation column.
Pulsar offers two preset policies for sub-accounts: QcloudTDMQReadOnlyAccess and QcloudTDMQFullAccess. The former can only view related information in the console, while the latter can perform read-write operations in the product console.



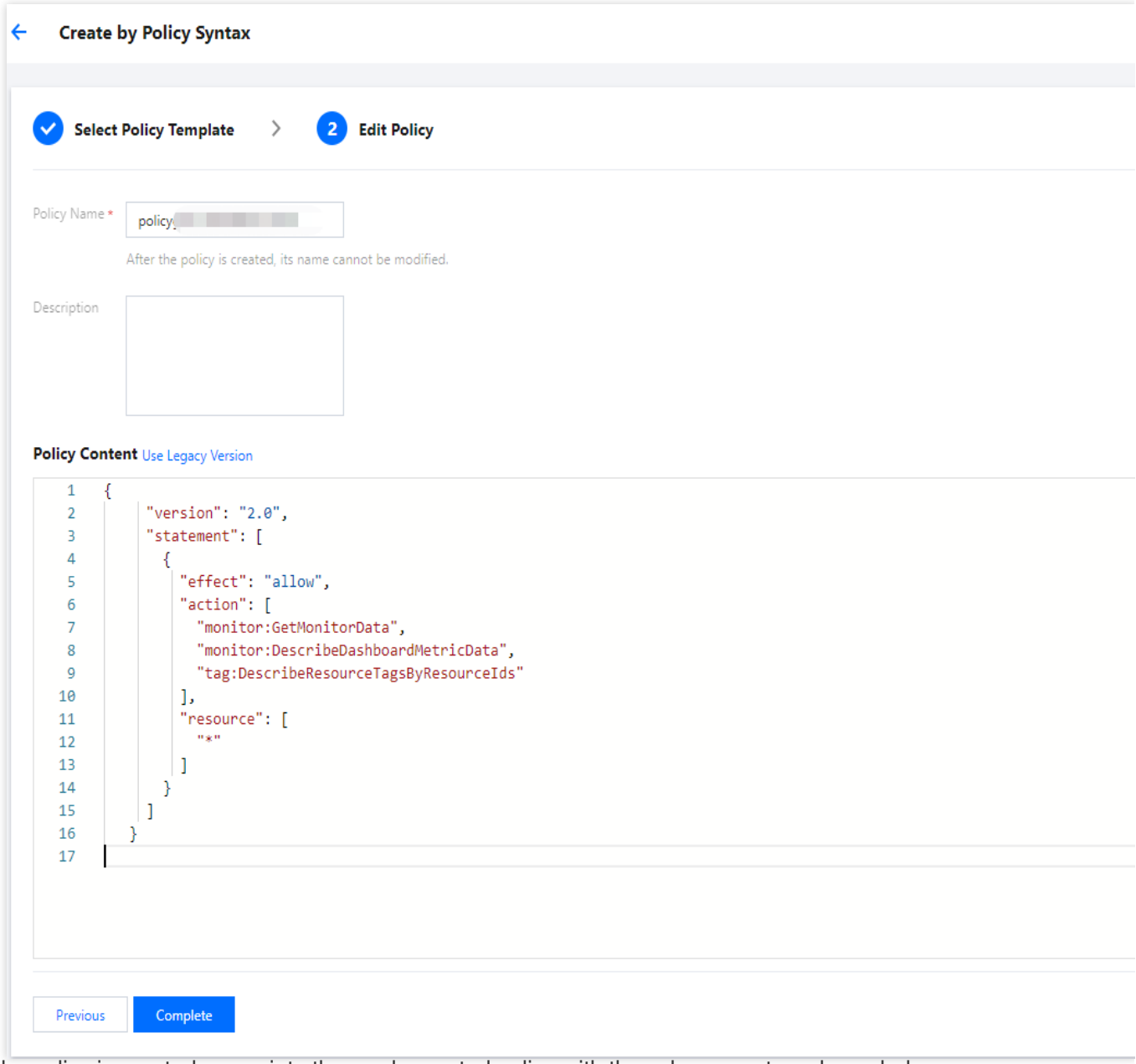
In addition to the above preset policies, for ease of use, the root account needs to grant the sub-accounts appropriate permissions to call other cloud services based on actual needs. The use of Pulsar involves the following API permissions of various cloud services:

Tencent Cloud Services	API Name	API Function	Corresponding Role in Pulsar
TCOP (Monitor)	GetMonitorData	Query metric monitoring data.	View the corresponding monitoring metrics displayed in the console.
TCOP (Monitor)	DescribeDashboardMetricData	Query metric monitoring data.	View the corresponding monitoring metrics displayed in the console.
Resource Tag (Tags)	DescribeResourceTagsByResourceIds	Query resource tag.	View cluster resource tags.

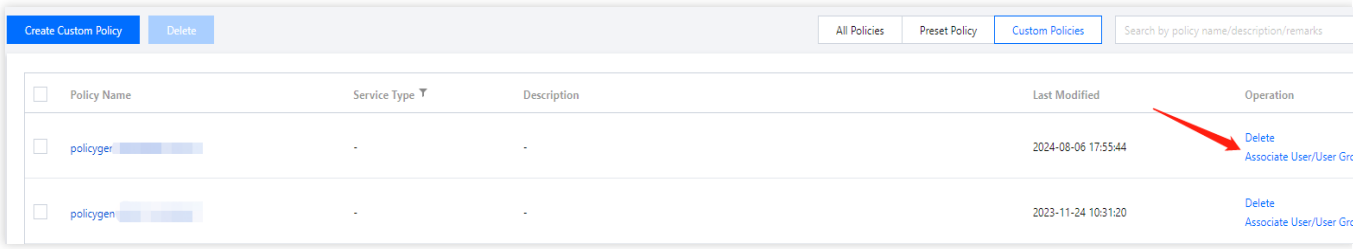
To grant the sub-account the above permissions, for the root account, you need to go to the CAM Console on the **Policies** page, and perform the **Create Custom Policy** operation. Click **Create by****Policy Syntax** for creation, then select **Blank Template**, and enter the following policy syntax:

```
{
  "version": "2.0",
  "statement": [
    {
```

```
        "effect": "allow",
        "action": [
          "monitor:GetMonitorData",
          "monitor:DescribeDashboardMetricData",
          "tag:DescribeResourceTagsByResourceIds"
        ],
        "resource": [
          "*"
        ]
      }
    ]
}
```



After the policy is created, associate the newly created policy with the sub-account as shown below:


Create Custom Policy
Delete
All Policies
Preset Policy
Custom Policies
Search by policy name/description/remarks
Policy Name
Service Type
Description
Last Modified
Operation
policyger
-
-
2024-08-06 17:55:44
Delete
Associate User/User Grc
policygen
-
-
2023-11-24 10:31:20
Delete
Associate User/User Grc

Granting Sub-Account Operation-Level Permissions

Last updated：2024-08-19 16:40:40

Overview

This document guides you on how to use the Tencent Cloud root account to grant operation-level authorization to a sub-account. You can grant different read and write permissions to the sub-account based on actual needs.

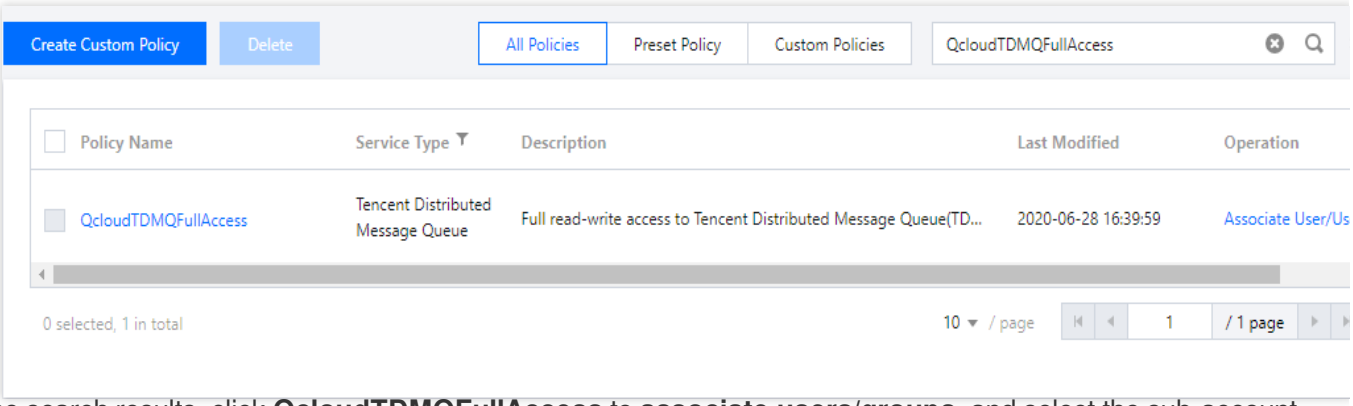
Directions

Granting Full Read/Write Permissions

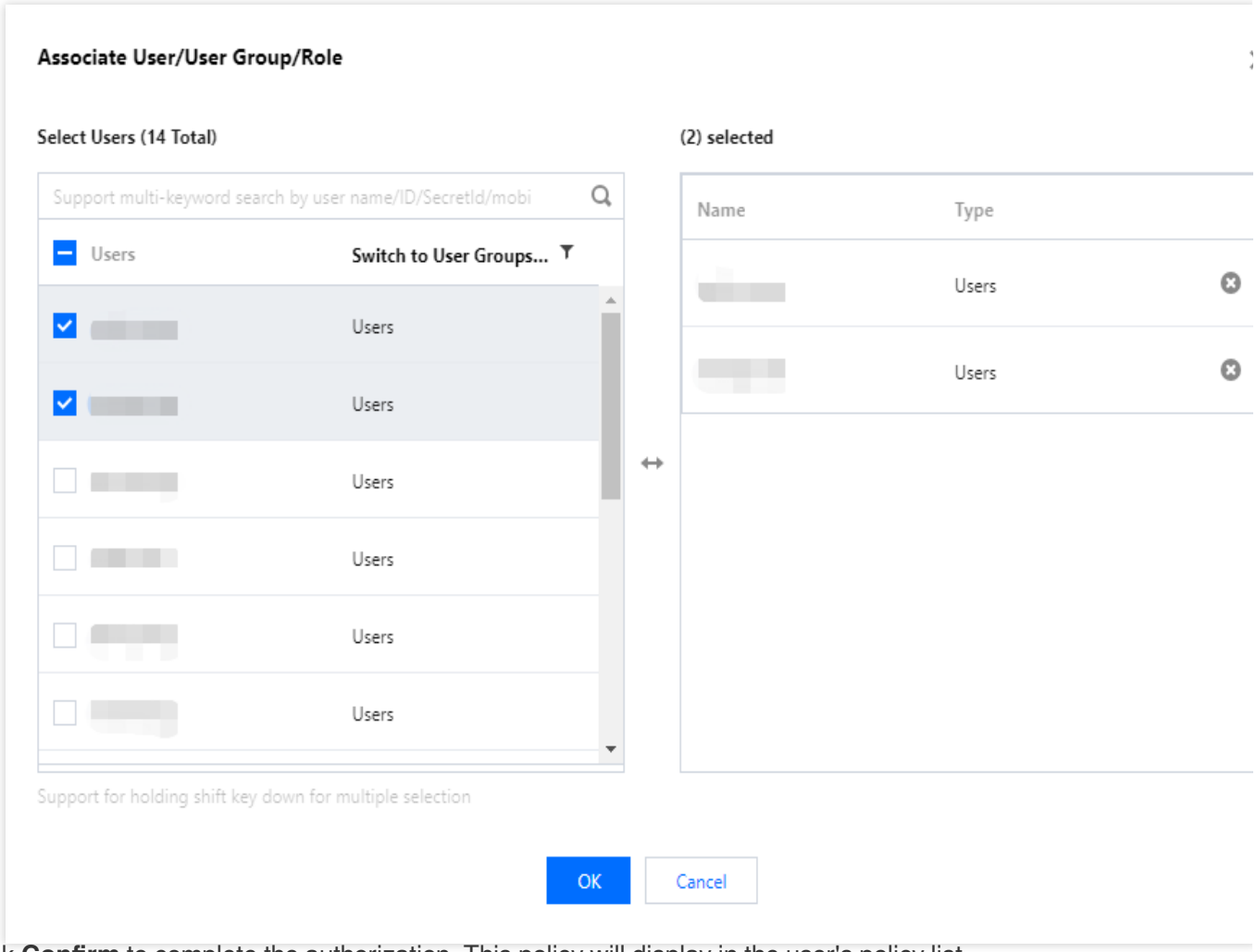
Note

After full read and write permissions are granted to the sub-account, the sub-account will have **full read and write capability** of **all resources** under the root account.

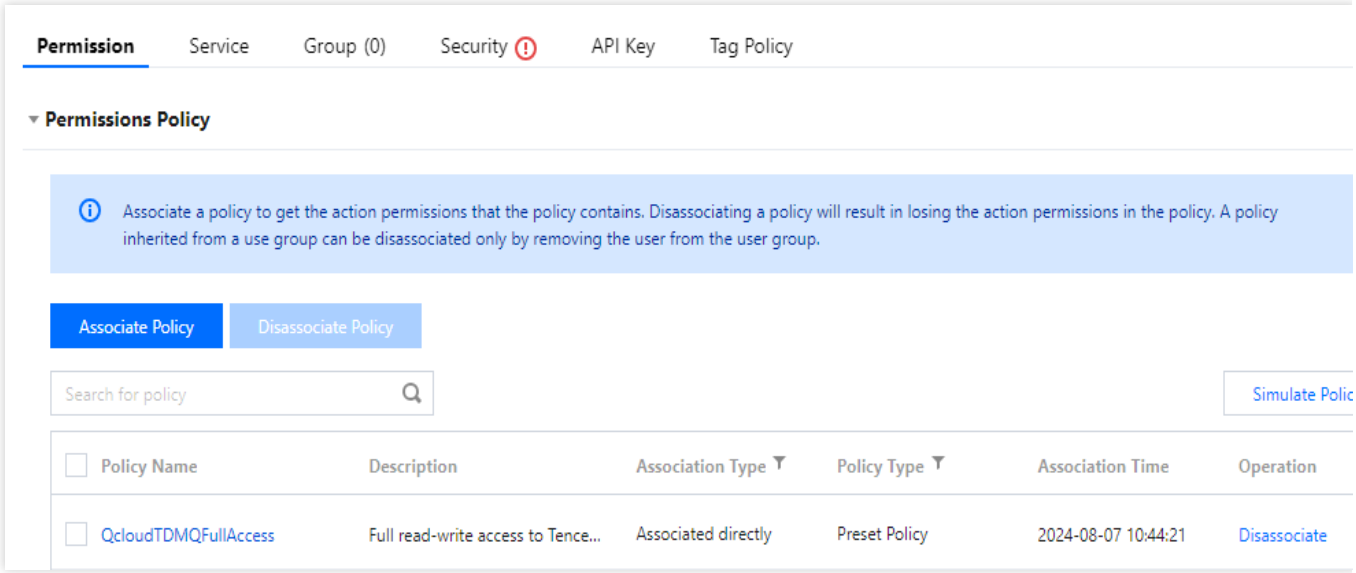
1. Log in to the CAM Console with the root account.
2. In the left sidebar, click **Policies** to enter the Policy Management List Page.
3. In the search bar on the right, enter **QcloudTDMQFullAccess** to search.



4. In the search results, click **QcloudTDMQFullAccess** to **associate users/groups**, and select the sub-account that needs to be authorized.



5. Click **Confirm** to complete the authorization. This policy will display in the user's policy list.

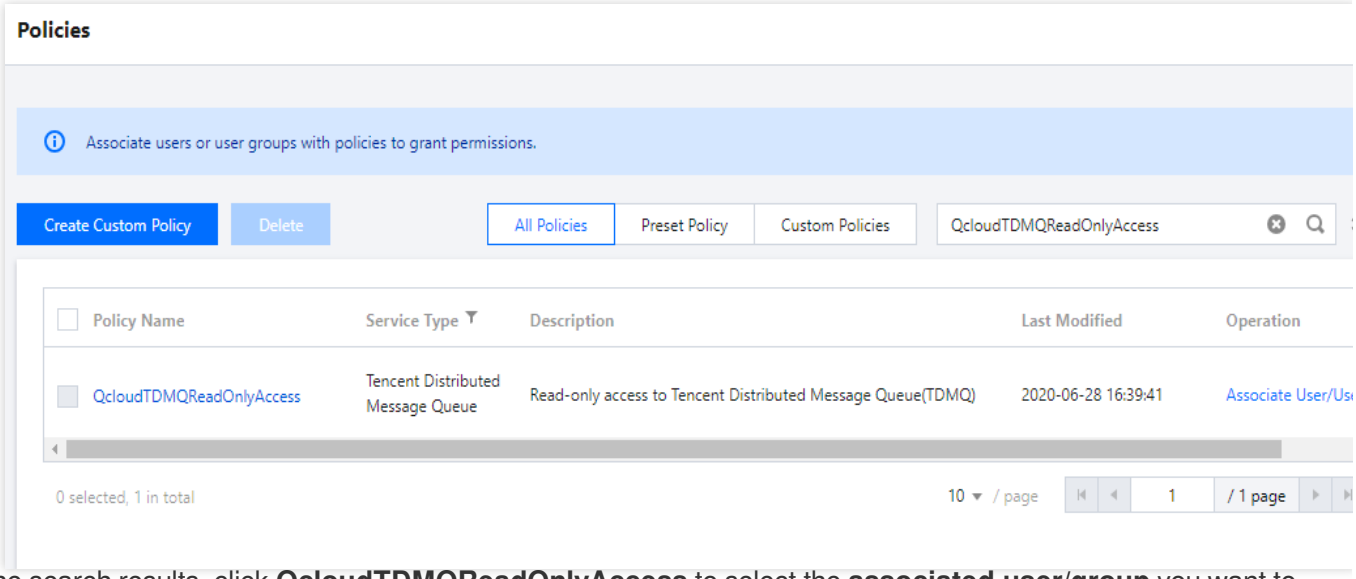


Granting Read-Only Permission

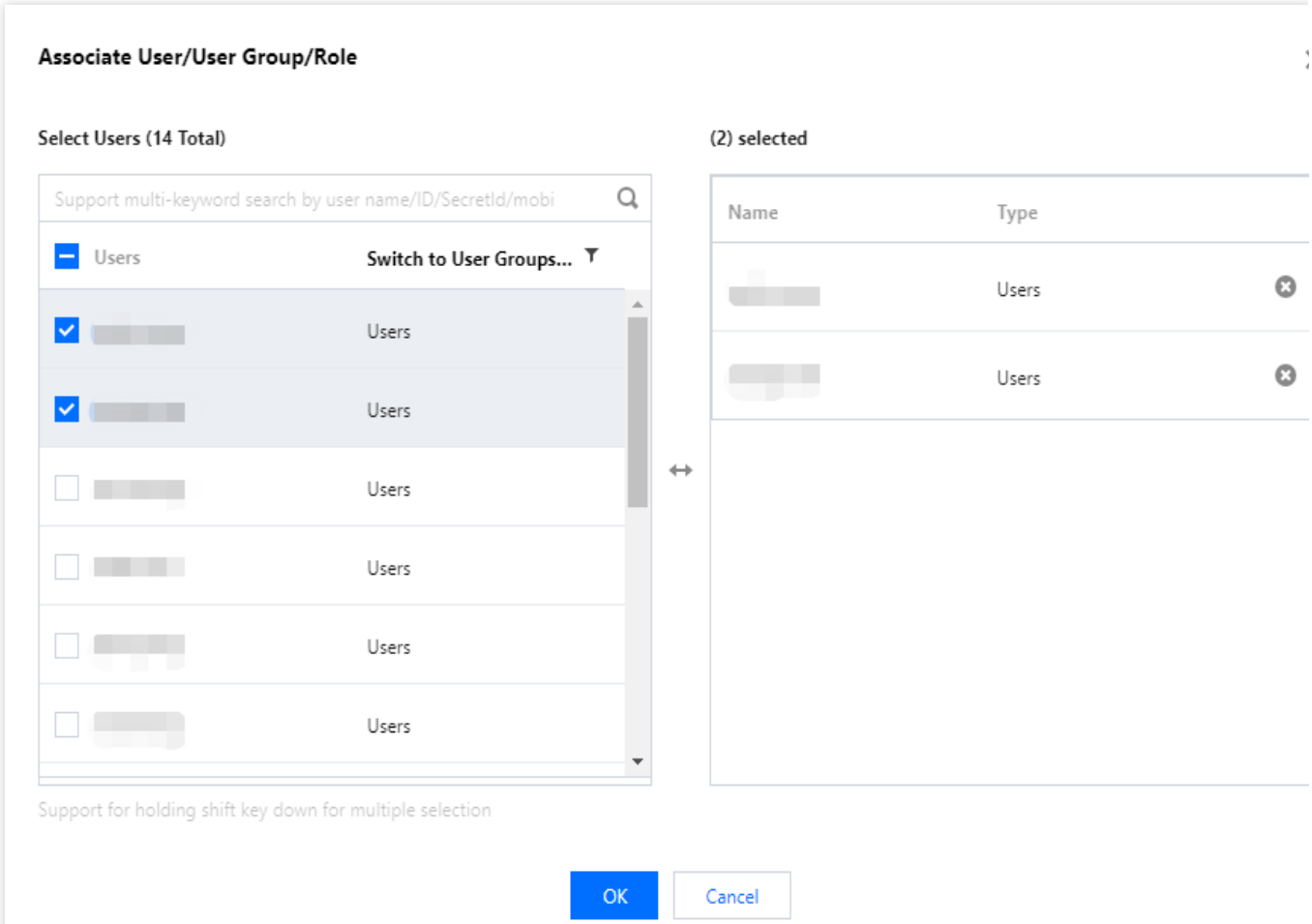
Note

After the read-only permission is granted to the sub-account, the sub-account will have **read-only capability** over **all resources** under the root account.

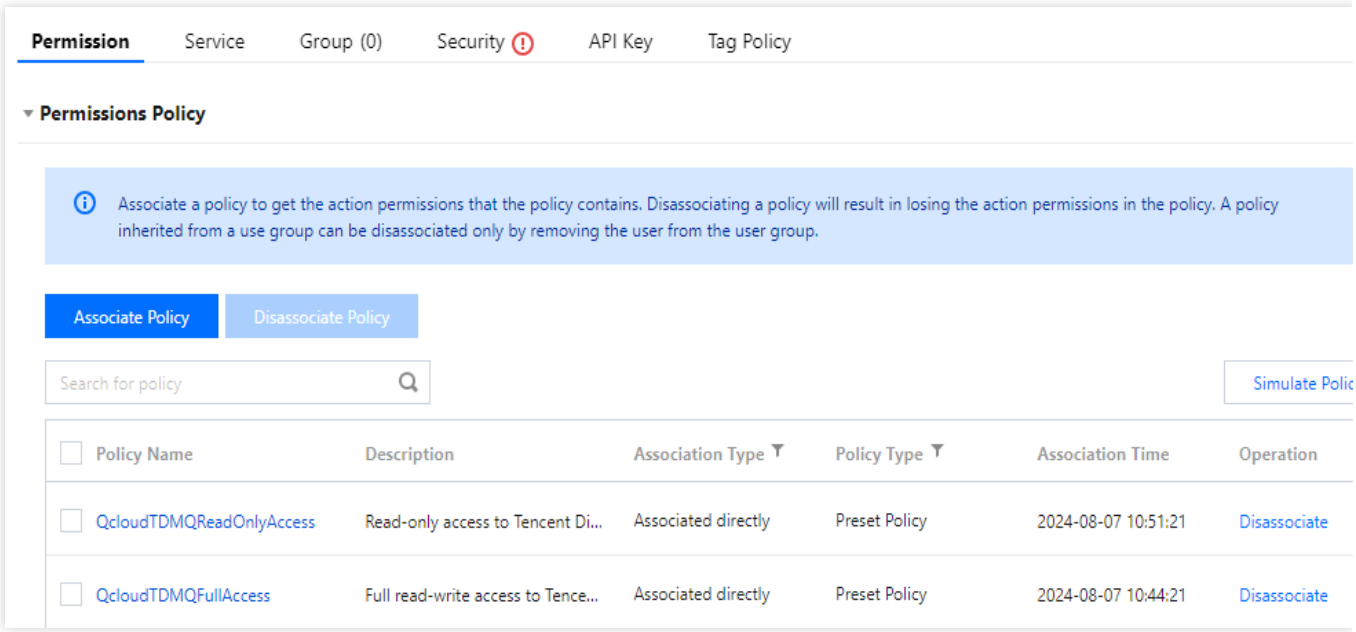
1. Log in to the CAM Console with the root account.
2. In the left sidebar, click **Policies** to enter the Policy Management List Page.
3. In the search bar on the right, enter **QcloudTDMQReadOnlyAccess** to search.



4. In the search results, click **QcloudTDMQReadOnlyAccess** to select the **associated user/group** you want to authorize for the sub-account.



5. Click **Confirm** to complete the authorization. This policy will display in the user's policy list.



Granting Sub-Account Resource-Level Permissions

Last updated：2024-08-19 16:41:48

Overview

This task guides you to grant resource-level permissions to a sub-account using the root account. The sub-account with the granted permissions can have control capability over a specific resource.

Prerequisites

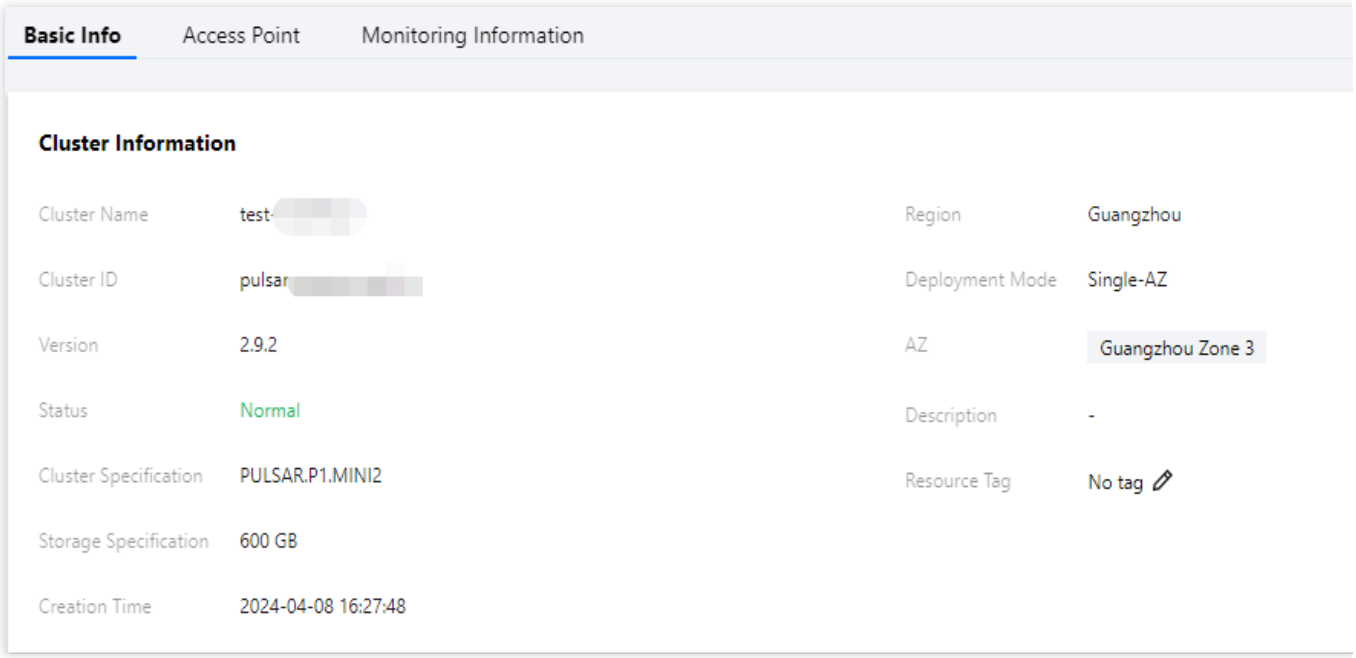
You have a Tencent Cloud root account and have already activated the CAM service.
You have at least one sub-account under the root account, and the authorization has been completed according to sub-account access authorization.
You have at least one Pulsar instance.

Directions

You can use the policy feature of the CAM console to authorize the Pulsar resources owned by the root account to sub-accounts. Detailed Pulsar **resource authorization to sub-accounts** is as follows. This example demonstrates how to authorize a cluster resource to a sub-account, with similar directions for other types of resources.

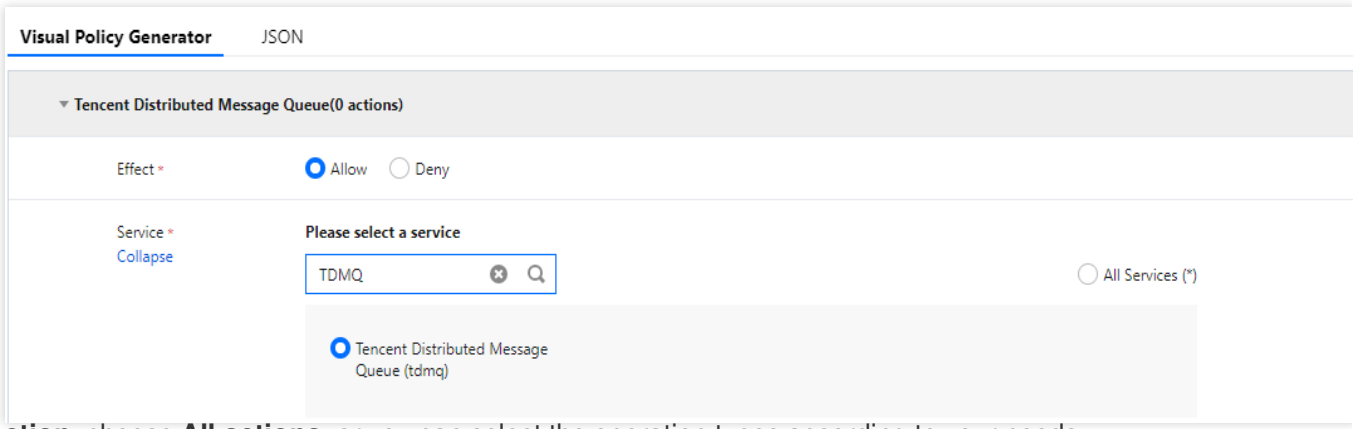
Step 1: Obtaining a Pulsar Cluster ID

1. Log in to the TDMQ for Apache Pulsar console using the **root account**, select an existing cluster instance, and click to enter its details page.
2. In the **Basic Information**, the field **ID** represents the ID of the current Pulsar cluster.



Step 2: Creating a Authorization Policy

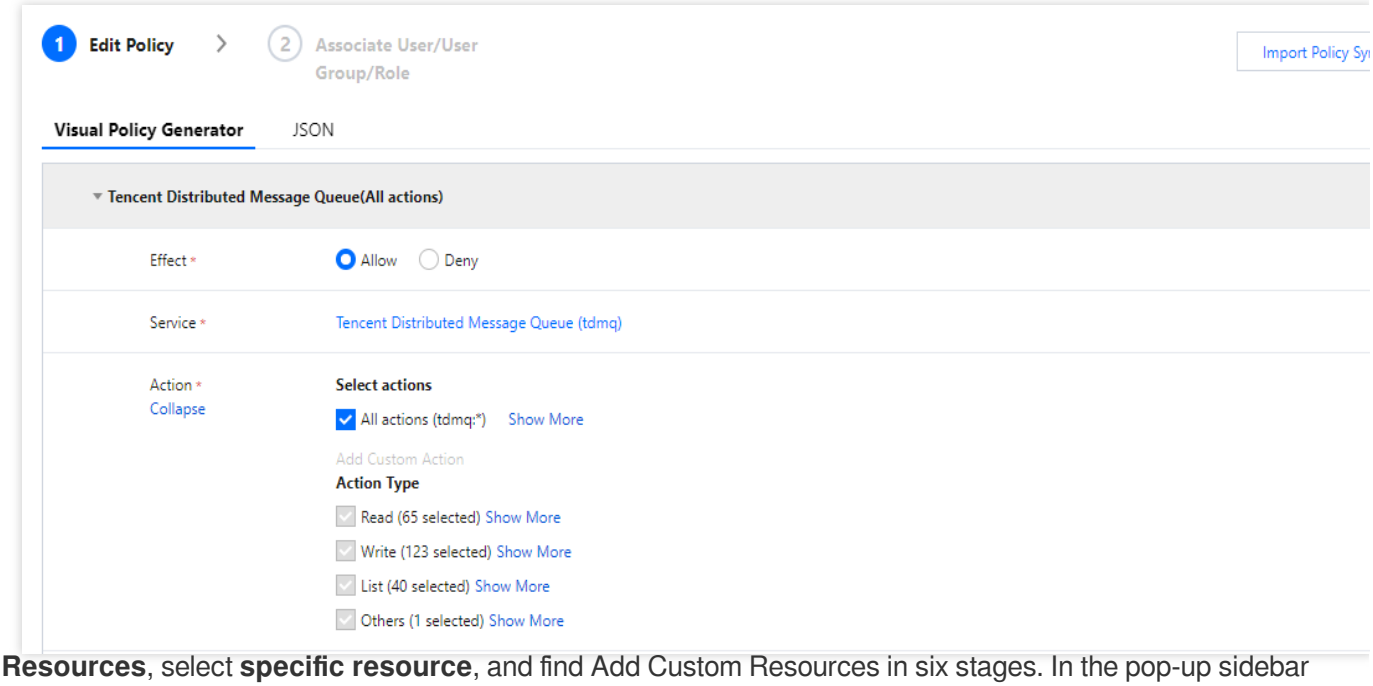
1. Enter the CAM Console, and click Policies in the left sidebar.
2. Click **Create custom Policy,** and select **Create by Policy Generator**.
3. In the visual policy generator, keep the **Effect** as **Allow**. In the **Service** field, enter TDMQ for filtering, and select **Message Queue TDMQ (tdmq)** from the results.



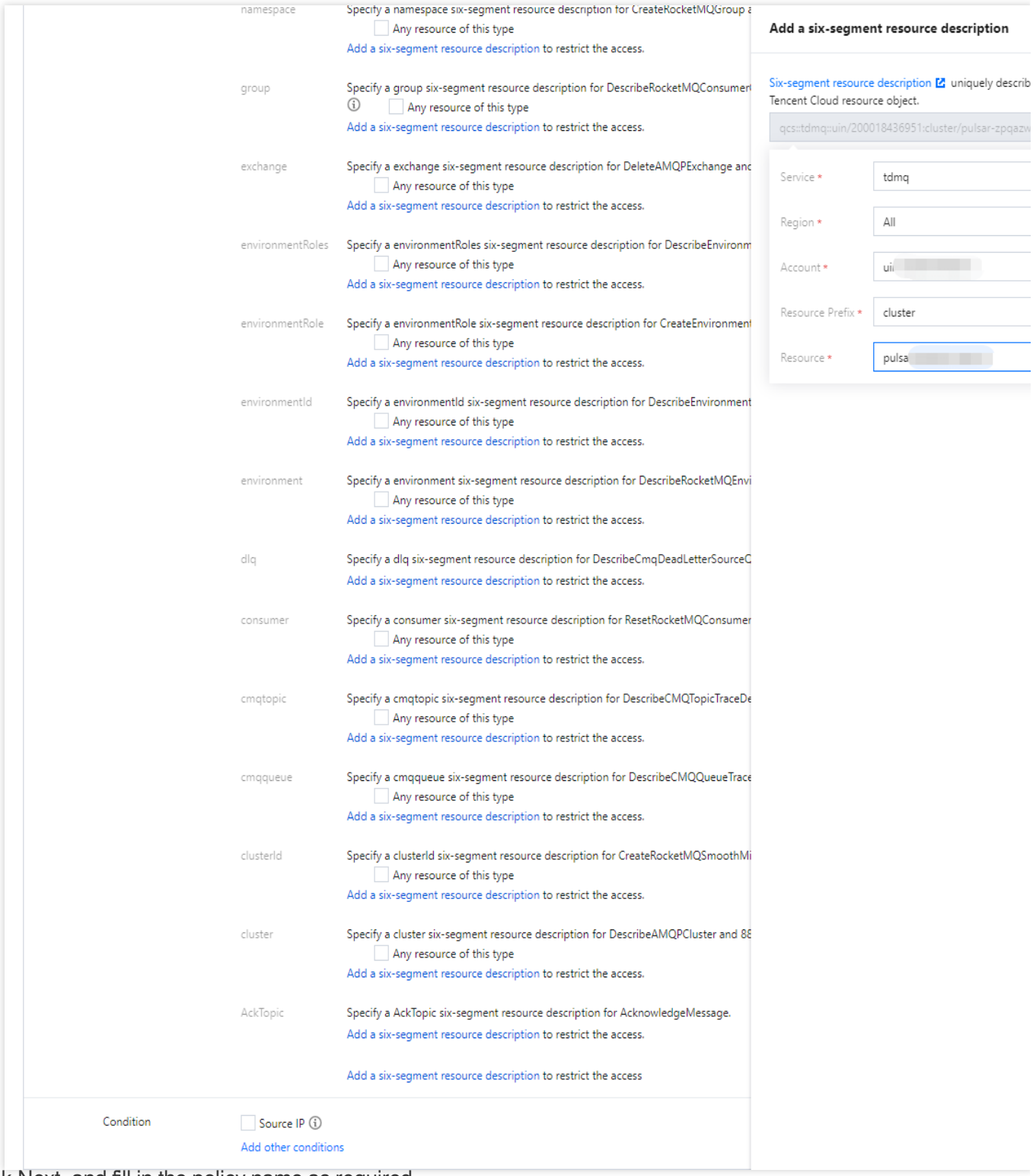
4. In **Action**, choose **All actions**, or you can select the operation types according to your needs.

Note:

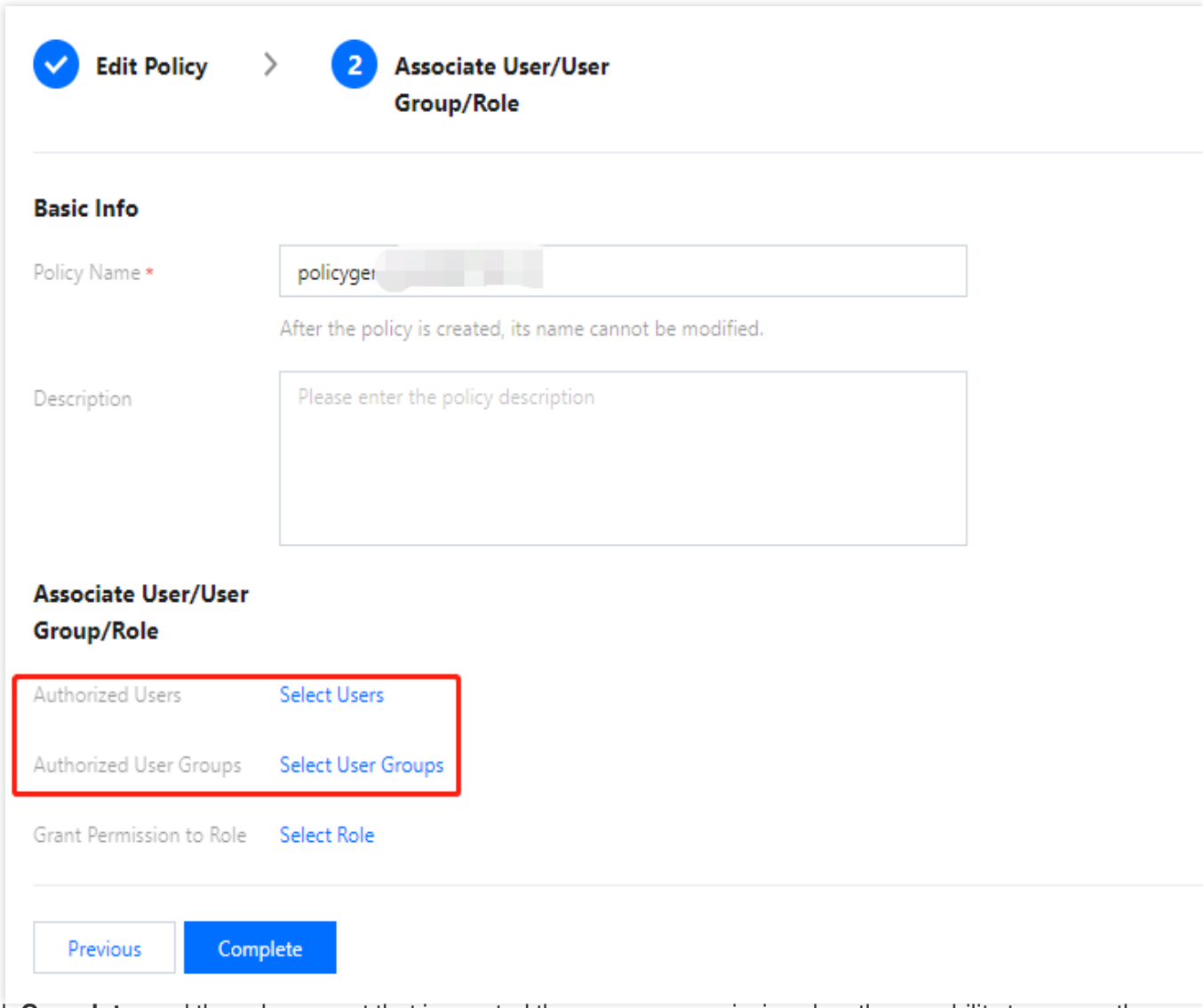
Some APIs do not support resource-level authorization at the moment, which is based on the display on the console page. For a list of APIs that support resource-level authorization, you can see the list of APIs that support resource-level authorization in the appendix of this document.



5. In **Resources**, select **specific resource**, and find Add Custom Resources in six stages. In the pop-up sidebar dialog, enter the **cluster prefix** and **resource ID**. For the obtaining process, see Step 1.



6. Click Next, and fill in the policy name as required.
7. Click **select user** or **select user group**, and choose the user or user group to grant resource permissions to.



8. Click **Complete**, and the sub-account that is granted the resource permissions has the capability to access the related resource.

List of APIs Supporting Authorization at Resource-Level

TDMQ for Apache Pulsar supports resource-level authorization. You can grant a specified sub-account API permissions for specific resources.

APIs supporting resource-level authorization include:

API Name	API Description	Resource Type	Six-Segment Example of Resource
DescribeClusterDetail	Gets the cluster detail.	cluster	qcs::tdmq:${region}:uin/${uin}:cluste
DescribeClusters	Gets the	cluster	qcs::tdmq:${region}:uin/${uin}:cluste

	cluster list.		
ModifyCluster	Modifies the cluster.	cluster	qcs::tdmq:${region}:uin/${uin}:cluste
DeleteCluster	Deletes the cluster.	cluster	qcs::tdmq:${region}:uin/${uin}:cluste
CreateRole	Creates a role.	cluster	qcs::tdmq:${region}:uin/${uin}:cluste
DeleteRoles	Deletes a role.	cluster	qcs::tdmq:${region}:uin/${uin}:cluste
CreateEnvironment	Creates an environment.	cluster	qcs::tdmq:${region}:uin/${uin}:cluste
CreateTopic	Creates a topic.	environment	qcs::tdmq:${region}:uin/${uin}:envir
ModifyEnvironmentAttributes	Modifies the environmental attribute.	environment	qcs::tdmq:${region}:uin/${uin}:envir
DeleteEnvironments	Deletes the environment.	environment	qcs::tdmq:${region}:uin/${uin}:envir
DescribeEnvironments	Gets the environment list.	environmentId	qcs::tdmq:${region}:uin/${uin}:envir
DescribeEnvironmentAttributes	Gets the environment attribute.	environmentId	qcs::tdmq:${region}:uin/${uin}:envir
DescribeEnvironmentRoles	Gets the environment role list.	environmentRoles	qcs::tdmq:${region}:uin/${uin}:envir
CreateEnvironmentRole	Creates the environment role authorization.	environmentRole	qcs::tdmq:${region}:uin/${uin}:envir
DeleteEnvironmentRoles	Deletes the environment role authorization.	environmentRole	qcs::tdmq:${region}:uin/${uin}:envir

ModifyEnvironmentRole	Modifies the environment role authorization.	environmentRole	qcs::tdmq:${region}:uin/${uin}:envir
DescribeMsgTrace	Message trace.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
DescribeMsg	Message details.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
DescribeTopicMsgs	Message query.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
DescribeTopics	Queries the topic list.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
DescribeProducers	Gets the producer list.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
DeleteTopics	Batch deletes topics.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
ModifyTopic	Modifies the topic.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
CreateSubscription	Creates a subscription relationship for a topic.	topic	qcs::tdmq:${region}:uin/${uin}:topic/
ResetMsgSubOffsetByTimestamp	Performs message retrospection based on timestamp, accurate to milliseconds.	subscription	qcs::tdmq:${region}:uin/${uin}:subs
DeleteSubscriptions	Deletes the subscription relationship.	subscription	qcs::tdmq:${region}:uin/${uin}:subs
DescribeRealTimeSubscription	Real-time consumption and	subscription	qcs::tdmq:${region}:uin/${uin}:subs

	subscription list.		
DescribeSubscriptions	Consumption and subscription list.	subscription	qcs::tdmq:${region}:uin/${uin}:subsc
ModifyRole	Modifies the role.	role	qcs::tdmq:${region}:uin/${uin}:role/$
DescribeRoles	Obtains the list of the role.	role	qcs::tdmq:${region}:uin/${uin}:role/$

List of APIs not Supporting Authorization at Resource-Level

API Name	API Description
CreateCluster	Creates a cluster.

Granting Sub-Account Tag-Level Permissions

Last updated：2024-08-19 16:42:37

Overview

This task guides you on how to authorize sub-accounts to access resources under a specific tag using the root account by tag-based authentication. The authorized sub-account can then manage resources with the corresponding tag.

Prerequisites

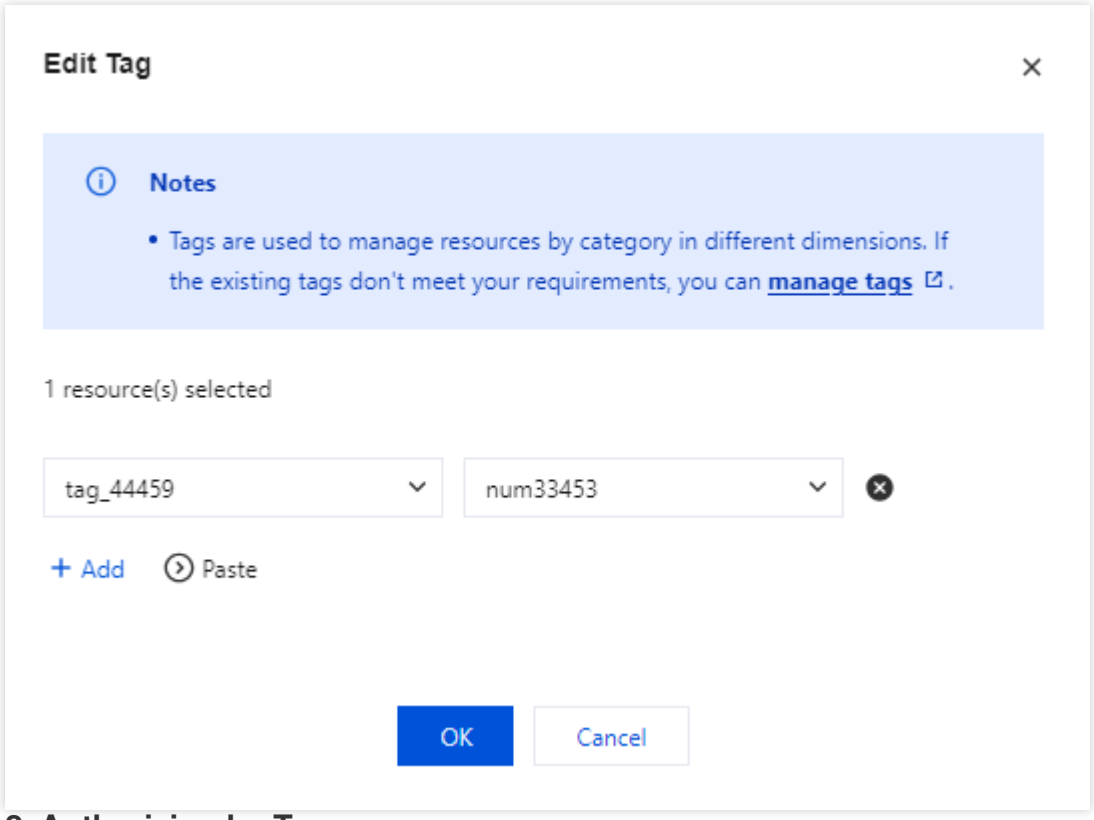
You should have a Tencent Cloud root account and have already activated the Tencent Cloud Access Management Service.
You should have at least one sub-account under the root account, and the authorization has been completed according to sub-account access authorization.
You should have at least one Pulsar Cluster Resource Instance.
You should have at least one **Tag**. If you don't have one, you can go to the Tag console > **Tag list** to create one.

Directions

You can use the policy feature in the CAM console to grant sub-accounts read and write permissions to the Pulsar resources that are owned by the root account and bound to tag, through the method of **authorizing by Tag**. The detailed directions for **granting resource permissions to sub-accounts by Tag** are as follows.

Step 1: Binding Tags to the Resource

1. Use the **root account** to log in to the TDMQ for Apache Pulsar console, and go to the cluster management page.
2. Select the target cluster, click **Edit Resource Tag** at the top left corner, and bind the resource tag for the cluster.

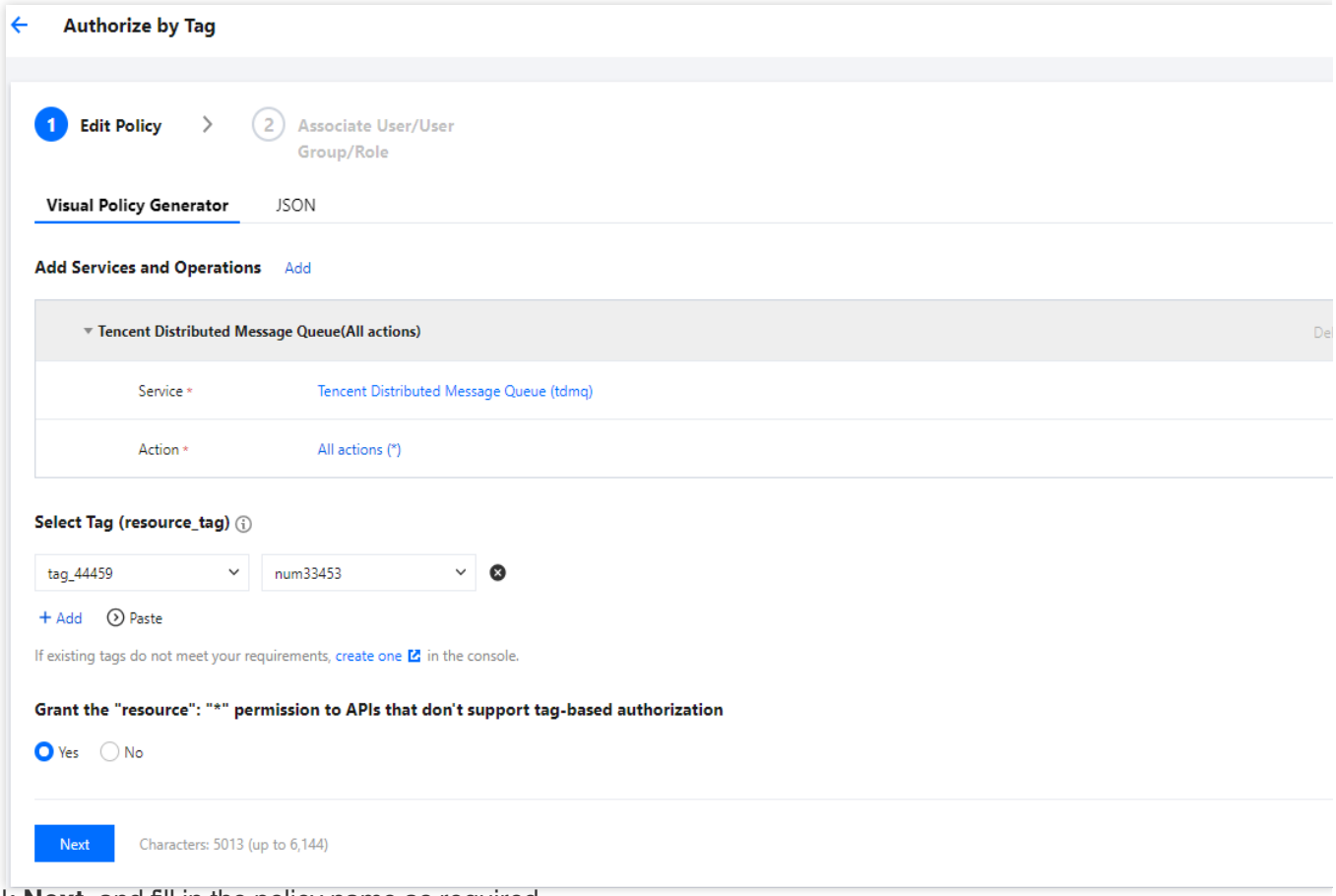


Step 2: Authorizing by Tag

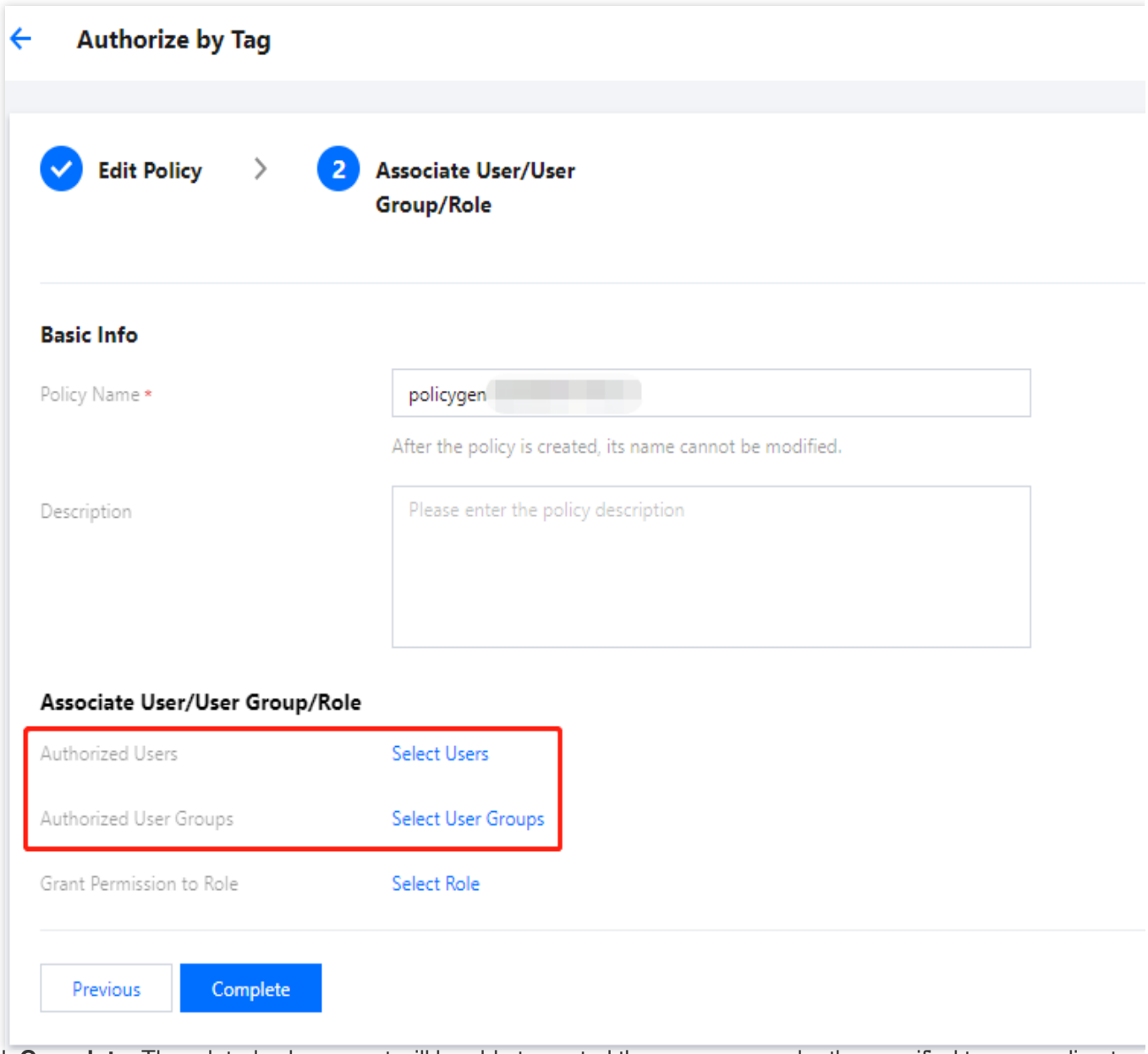
1. Go to the CAM Console, and click Policies in the left sidebar.
2. Click **Create Custom Policy,** and select **Authorize by Tag.**
3. In the visual policy generator, enter tdmq in the **Service** field to filter. From the results, select **Tencent Distributed Message Queue (TDMQ) (tdmq). In** Operations, choose **All Operations**, or select the corresponding operations as needed.

Note:

Some APIs do not support tag authentication for now. See the console page for accurate information.



4. Click **Next**, and fill in the policy name as required.
5. Click **Select User** or **Select User Group**, and choose the user or user group to grant resource permissions to.

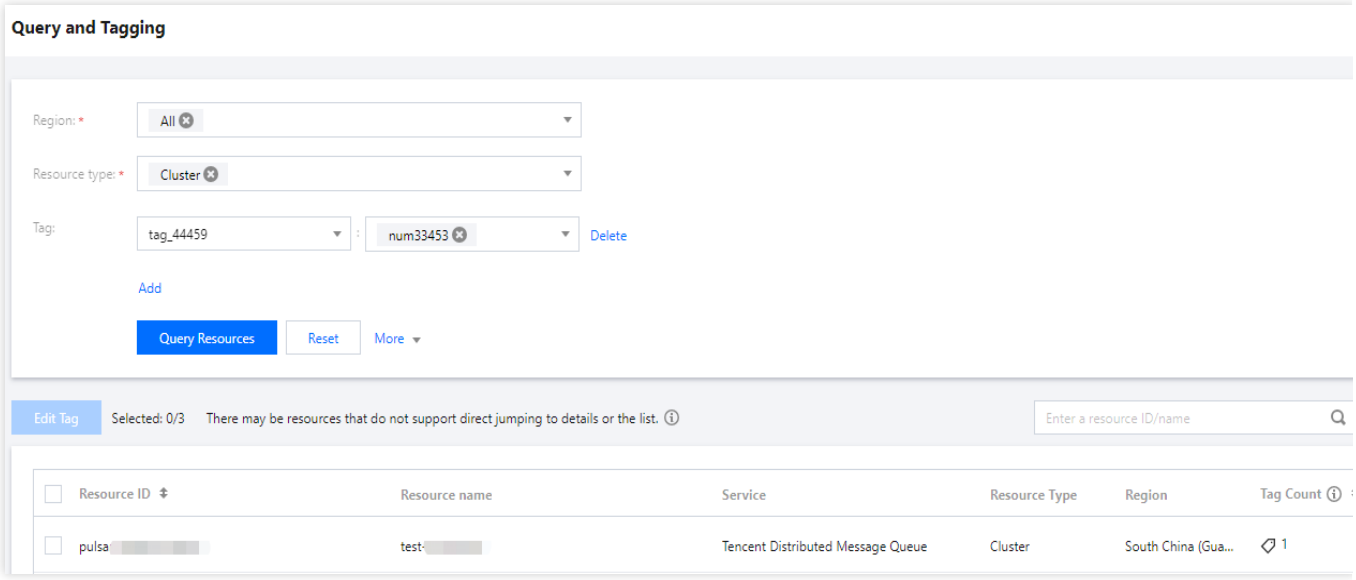


6. Click **Complete**. The related sub-account will be able to control the resources under the specified tag according to the policy.

Unified Management of Resource Tags

You can also perform unified management of resource tags in the Tag Console. Detailed operations are as follows:

1. Log in to the Tencent Cloud Tag Console.
2. In the left sidebar, select **Resource Tag**. Choose the query conditions as needed, and select **TDMQ** > **Cluster** under **Resource Type**.
3. Click **Query Resources**.
4. In the results, select the required resources, and click **Edit Tag** to bind or unbind tags in batch.


Query and Tagging
Region: *
All
Resource type: *
Cluster
Tag:
tag_44459
num33453
Delete
Add
Query Resources
Reset
More
Edit Tag
Selected: 0/3
There may be resources that do not support direct jumping to details or the list.
Enter a resource ID/name
Resource ID
Resource name
Service
Resource Type
Region
Tag Count
pulsa
test-
Tencent Distributed Message Queue
Cluster
South China (Gua...
1

Role and Authentication

Last updated：2024-12-02 17:10:17

Glossary

Role: different from a role in Tencent Cloud, a role in TDMQ for Apache Pulsar is a proprietary concept. It is the smallest unit of permission division performed by you in TDMQ. You can add multiple roles and assign them the production/consumption permissions of different namespaces.
Token: it is an authentication tool in TDMQ for Apache Pulsar. You can add a token in a client to access TDMQ for Apache Pulsar for message production/consumption. Tokens correspond to roles one by one, and each role has its own unique token.

Use Cases

You need to securely use TDMQ for Apache Pulsar to produce/consume messages.
You need to set production/consumption permissions of different namespaces for different roles.
For example, your company has departments A and B, and department A's system produces transaction data and department B's system performs transaction data analysis and display. In line with the principle of least privilege, two roles can be configured to grant department A only the permission to produce messages to the transaction system namespace and grant department B only the permission to consume messages. This helps greatly avoid problems caused by unclear division of permissions, such as data disorder and dirty business data.

Directions

Creating role

1. Log in to the TDMQ for Apache Pulsar console and click **Role Management** on the left sidebar to enter the **Role Management** page.
2. On the **Role Management** page, select the region and cluster and click **Create** to enter the **Create Role** page.
3. On the **Create Role** page, enter the role name and remarks:
Role Name: it can contain up to 32 digits, letters, and delimiters (underscore or hyphen).
Remarks (optional): enter remarks of up to 100 characters.
4. Click **Submit**.

Granting permission to role

1. Find the newly created role in **Role Management** in the TDMQ for Apache Pulsar console and copy the role token in the following methods:
Method 1. Copy in the Token column
Method 2. View and copy in the Operation column
Click **Copy** in the **Token** column.

Click **View Token** in the **Operation** column and click **Copy** in the pop-up window.

2. Add the copied role token to the client parameters. For directions on how to add the token parameter to the client code, see JWT Authentication Configuration.
Note:
Token leakage may lead to data leakage; therefore, you should keep your token confidential.
3. In **Namespace** in the TDMQ for Apache Pulsar console, select the target namespace and click **Configure Permission** in the **Operation** column.

4. Click **Add Role**, find the role just created in the drop-down list, select the required permission, and click **Save**.

5. Check whether the permission has taken effect.
6. You can run the configured client to access the topic resources in the namespace and produce/consume messages according to the configured permission. Check whether a no permission error is reported, and if not, the permission has been configured successfully.

Batch Importing Roles

In scenarios where user business systems are complex and require the configuration of multiple roles, TDMQ for Apache Pulsar provides a batch import roles feature. You can use the provided configuration template to fill in fields such as roles and permissions. After the file is uploaded to the console, TDMQ for Apache Pulsar will automatically create the roles and configure the corresponding permissions for you, reducing repetitive operational costs.
Note:
All fields are mandatory except for the description field.
Permissions only support Produce Messages and Consume Messages, and multiple permissions should be separated by commas.
A maximum of 300 entries can be imported at a time.
1. On the Role Management List page, click **Batch Import Roles** in the top-left corner.

2. In the pop-up dialog box, download the configuration template, complete the relevant fields as required, and save it. Below is an example of a completed template:

Role Name	Description	Cluster Name	Cluster ID	Namespace	Permissions
role-test	test	cluster-test	pulsar-xxxxxxxxxxxx	env-test	Produce messages and consume messages.

3. During file upload, submit the completed role template. TDMQ for Apache Pulsar will automatically create the roles and configure the associated permissions for you.

Editing permission

1. In **Namespace** in the TDMQ for Apache Pulsar console, find the target namespace and click **Configure Permission** in the **Operation** column to enter the permission configuration list.
2. In the permission configuration list, click **Edit** in the **Operation** column of the target role.
3. In the pop-up window, modify the permission information and click **Save**.

Deleting permission

Note:
Before deleting a permission, make sure that the current business no longer uses the role to produce/consume messages; otherwise, a client exception may occur due to the failure to produce/consume messages.
A role cannot be deleted if it has permissions configured in namespaces.
1. In **Namespace** in the TDMQ for Apache Pulsar console, find the target namespace and click **Configure Permission** in the **Operation** column to enter the permission configuration list.
2. In the permission configuration list, click **Delete** in the **Operation** column of the target role.
3. In the pop-up window, click **OK**.

JWT Authentication Configuration

Last updated：2024-06-28 11:31:37

Overview

TDMQ for Apache Pulsar provides the same JWT authentication method used by native Pulsar, which allows you to access TDMQ for Apache Pulsar resources by configuring the token in the client parameters. For directions on how to configure the relationships between different role tokens and TDMQ for Apache Pulsar resources in the console, see Roles and Permissions.
This document describes how to configure JWT authentication in a TDMQ for Apache Pulsar client, so that you can securely use the client to produce and consume messages. You can also add a token when creating a client.

Authentication Configuration

Java client

Configure JWT authentication in a Java client:
Access sample for cluster on v2.7.1 or above
Access sample for cluster on v2.6.1

```
PulsarClient client = PulsarClient.builder()
     // Access address, which can be copied from **Access Address** in the **Operat
     .serviceUrl("http://*")
        // Replace it with the role token displayed on the **Role Management** page
     .authentication(AuthenticationFactory.token("eyJh****"))
     .build();
```

```
PulsarClient client = PulsarClient.builder()
      // Access address, which can be copied from the access point list in **Cluste
         .serviceUrl("pulsar://*.*.*.*:6000/")
         // Replace it with the role token displayed on the **Role Management** pag
      .authentication(AuthenticationFactory.token("eyJh****"))
         // Replace the value of `custom:` with the route ID in the access point li
      .listenerName("custom:1********0/vpc-******/subnet-********")
      .build();
```

Go client

Configure JWT authentication in a Go client:

Access sample for cluster on v2.7.1 or above

Access sample for cluster on v2.6.1

```
client, err := NewClient(ClientOptions{
      // Access address, which can be copied from the access point list in **Cluste
         URL: "http://*",
         // Replace it with the role token displayed on the **Role Management** pag
      Authentication: NewAuthenticationToken("eyJh****"),
})
```

```
client, err := NewClient(ClientOptions{
      // Access address, which can be copied from the access point list in **Cluste
         URL: "pulsar://*.*.*.*:6000",
         // Replace it with the role token displayed on the **Role Management** pag
      Authentication: NewAuthenticationToken("eyJh****"),
         // Replace the value of `custom:` with the route ID in the access point li
      ListenerName: "custom:1300*****0/vpc-******/subnet-********",
})
```

Tag Management

Last updated：2024-08-19 16:44:21

Overview

Tags are key-value pairs provided by Tencent Cloud to mark and identify resources in the cloud. They help you easily classify and manage the TDMQ for Apache Pulsar resources in many dimensions such as business, purpose, and owner.

Note

Tencent Cloud will not use the tags you set, and they will only be used for your management of the TDMQ for Apache Pulsar resources.

Use Limits

For the use limits of tags, see Use Limits.

Operation Methods and Cases

Case Description

Case: A company has 6 TDMQ for Apache Pulsar clusters on Tencent Cloud, with the department, business scope, and owner information as described below:

Queue ID	Department	Business Scope	Owner
pulsar-rgxj35jgo3d1	E-commerce	Marketing campaigns	Tom
pulsar-rgxj35jgo3d2	E-commerce	Marketing campaigns	Harry
pulsar-rgxj35jgo3d3	Games	Game A	Jane
pulsar-rgxj35jgo3d4	Games	Game B	Harry
pulsar-rgxj35jgo3d5	Entertainment	Post-production	Harry
pulsar-rgxj35jgo3d6	Entertainment	Post-production	Tom

Taking pulsar-rgxj35jgo3d1 as an example, we can add the following three sets of tags to this instance:

Tag key	Tag value
dept	ecommerce
business	mkt
owner	Tom

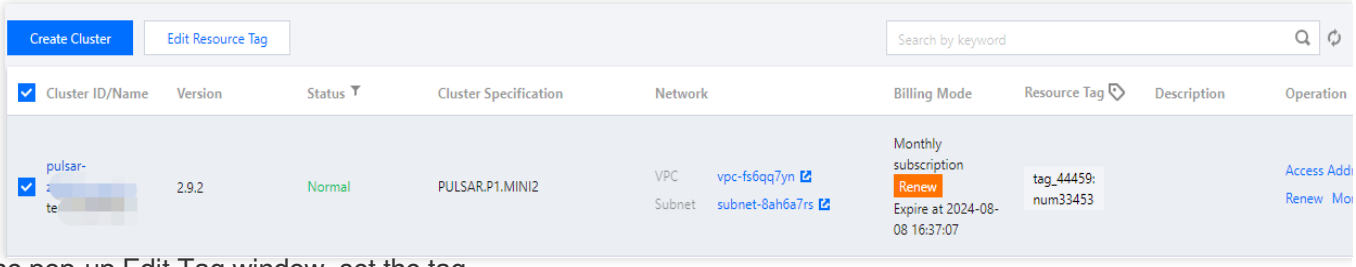
Similarly, other queue resources can also set their corresponding tags based on their department, business scope, and owner.

Setting Tags in the TDMQ for Apache Pulsar Console

Taking the above scenario as an example, after you have designed the tag keys and tag values, you can log in to the TDMQ for Apache Pulsar console to set the tags.

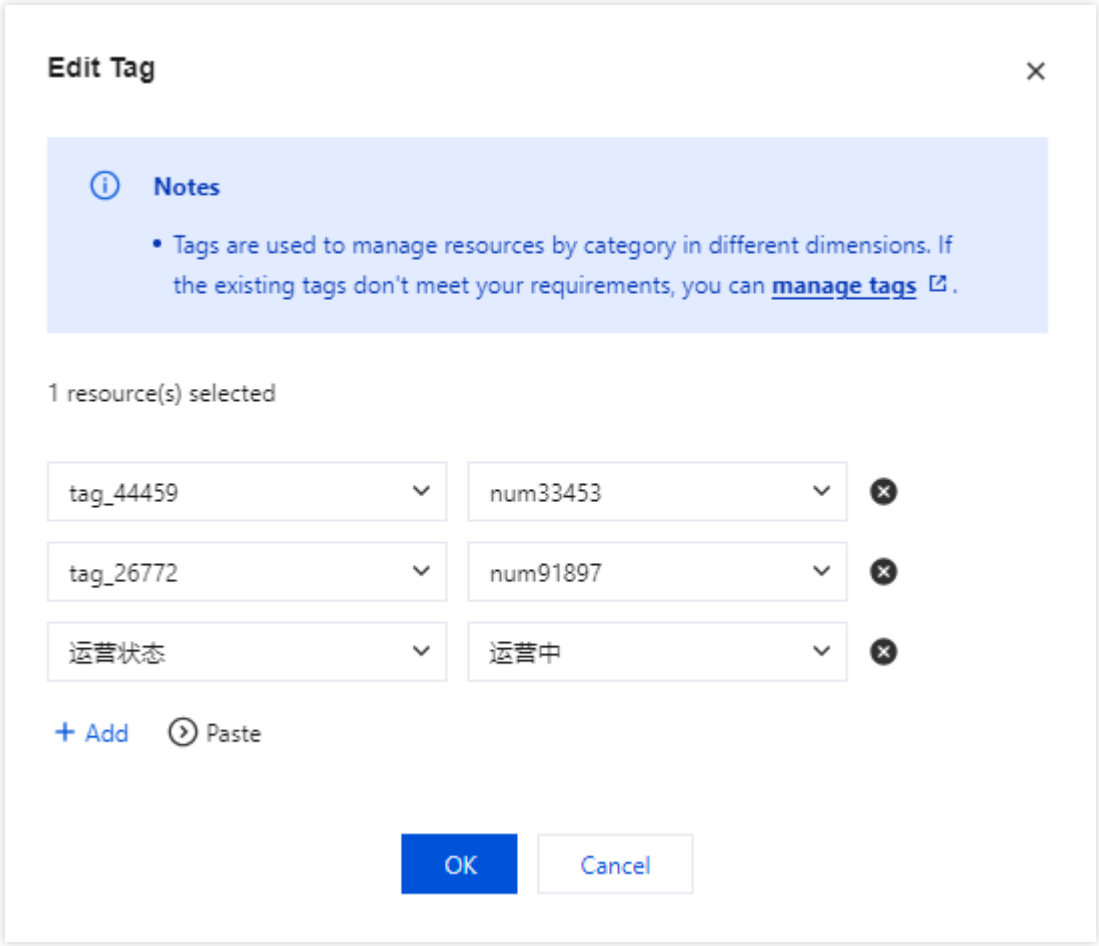
1. Log in to the TDMQ for Apache Pulsar console.

2. On the Cluster Management list page, select the region, check the clusters that need tag editing, and click **Edit Resource Tags** at the top of the page.



3. In the pop-up Edit Tag window, set the tag.

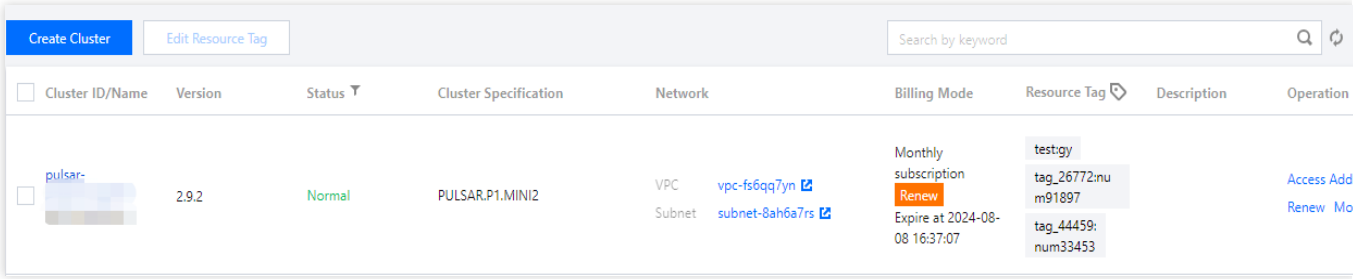
For example: Add three sets of tags to the cluster of pulsar-rgxj35jgo3d1.



Note

If the existing tags do not meet your requirements, please go to Tag Management to create new tags.

4. Click **OK**. The system will display a successful modification prompt, and you can view the associated tags in the resource tag column of the cluster.

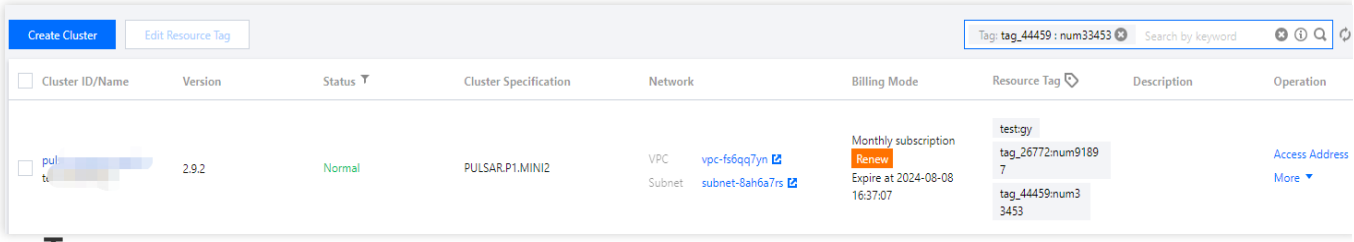


Filtering Resources by Tag Key

When you want to filter clusters that are bound to specific tags, use the following operations to filter them.

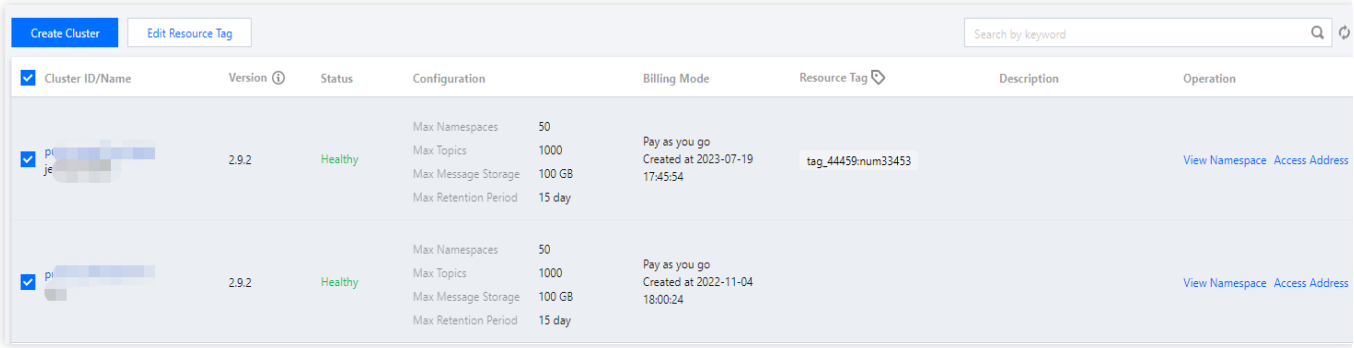
1. In the search box at the top-right corner of the page, select **Tag**.
2. In the window that pops up after **Tag:**, select the tag you want to search for, and click **Confirm** to search.

For example: Select `Tag: owner:zhangsan` to filter out clusters bound to the tag key `owner:zhangsan`.



Editing Tag

1. On the cluster management list page, select the region, check the clusters that need tag editing, and click **Edit Resource Tags** at the top of the page.



Note

You can batch edit tags for up to 20 resources at a time.

2. In the pop-up Edit Tag window, add, modify, or delete tags as needed.

Cross-Region Replication
Cross-Region Replication/Feature Description

Last updated：2024-12-03 10:11:09

Overview

Scenario 1: Cross-Region Disaster Recovery

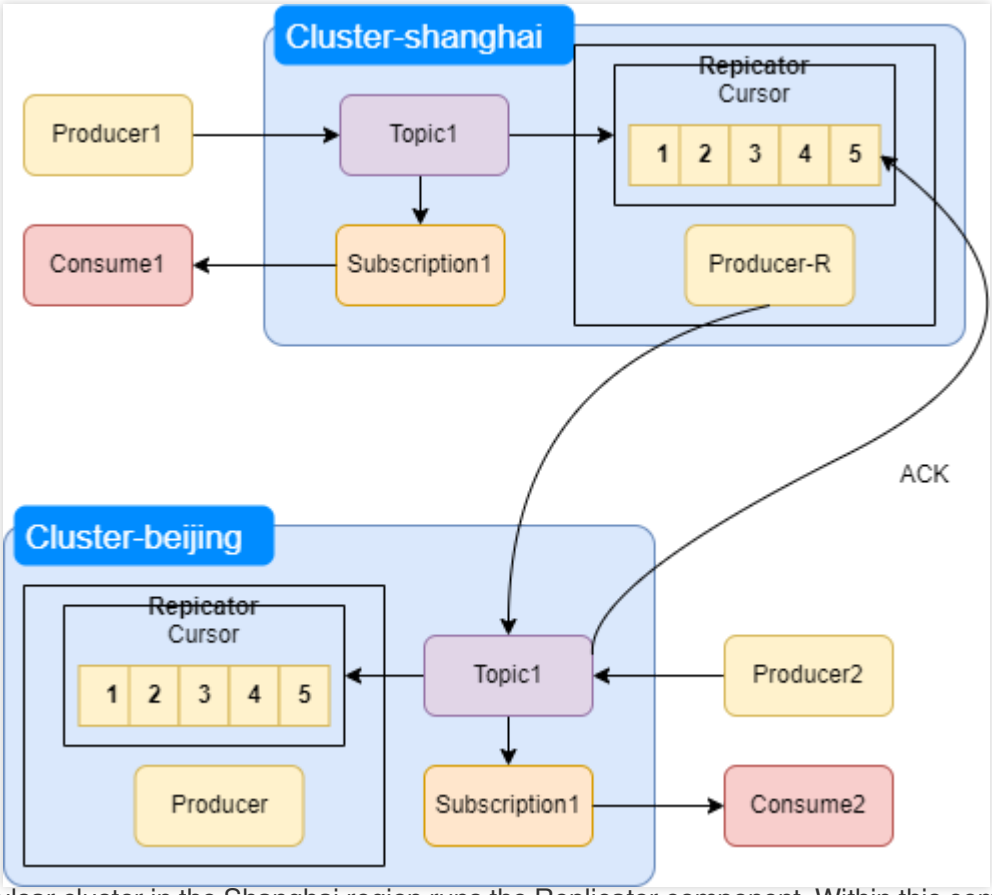
Pulsar Professional Edition supports deployment across availability zones (AZs). When purchasing a Pulsar cluster in a region with three or more AZs, you can choose up to three AZs to deploy cross-AZ instances. The instance's partition replicas are enforced to distribute across nodes in different AZs, ensuring service continuity even if a single AZ becomes unavailable. However, this 3-AZ deployment within the same city does not meet the disaster recovery requirements of financial clients. They require cross-region disaster recovery to quickly switch to a backup region in the event of a region-wide disaster, ensuring business continuity.

Scenario 2: Global Data Archiving

For a global team, business systems may span multiple regions worldwide, requiring cross-region data transmission and centralized data archiving. Data generated from several major cities worldwide can be transmitted via cross-region replication to a specific regional data center for unified archiving. Since these regions may have Topics with identical names, it is necessary to merge same-named Topics from multiple regions into a single Topic in the target cluster.
To address the above scenarios, TDMQ for Apache Pulsar Professional Edition, based on the GEO Replication solution, enables cross-region cluster replication. This supports use cases such as disaster recovery, global data archiving, and cross-region consumption.

How It Works

When Pulsar enables cross-region replication, a Replicator is initiated in the cluster. For details, see Understanding Pulsar's Cross-region Replication. Taking replication from the Shanghai region to the Beijing region as an example (as shown in the diagram):



The Pulsar cluster in the Shanghai region runs the Replicator component. Within this component, a Producer-R is initiated and bound to the Topic1 of the counterpart cluster in the Beijing region. This replicator sends message data to the Beijing IDC in the role of a producer.

Note:

Messages produced in the Shanghai cluster are first persisted locally within the cluster and then asynchronously forwarded to the Beijing cluster.

The Producer-R in the Replicator of the Shanghai cluster is independent of the client Producer1 in the same cluster. The cluster address configured for Producer-R points to the Beijing cluster.

Replication Process Description

1. Producer1 produces a message to Topic1 in the Shanghai cluster;
2. The Shanghai cluster persists the message to BookKeeper;
3. Upon successful persistence in BookKeeper, the message is pushed to the Cursor of the Replicator;
4. The Cursor in the Replicator forwards the message to Topic1 in the Beijing cluster via Producer-R;
5. Once Topic1 in the Beijing cluster is successfully written to BookKeeper, an ACK is sent back to the Cursor of the Replicator in the Shanghai cluster. Upon receiving the ACK, the Cursor in the Shanghai IDC pushes the next message through Producer-R.

Operation Guide

1. Create a professional cluster in the target replication region. On the cluster purchase page, enable the **Cross-region replication** switch and select the source data cluster;
2. Configure the metadata synchronization linkage for the cluster through the console:
Replication linkage name: Define a name for the synchronization linkage.
Linkage type: Select message level.
Source cluster selection: Select the Pulsar cluster to serve as the data source.
Target cluster selection: Select the pre-created target cluster in a different region. Only clusters with the same Cluster ID will be displayed.
Replication level: Supports three levels: cluster, namespace, and topic.
Cluster level: Suitable for cluster-wide replication.
Namespace level: Ideal for scenarios where clusters in different regions are both active, with namespaces distributed across regions.
Topic level: The smallest granularity for cross-region replication.
3. Once created, the message-level replication tasks will appear on the monitoring page, where you can review real-time replication rates, message backlogs, and other metrics.

Billing Description

Cross-region replication tasks at the message level will incur fees, while metadata-level replication will not. The console provides relevant monitoring metrics to assist with observation.
For detailed billing information on cross-region message-level replication, see Pro Cluster Billing.

Usage Restrictions

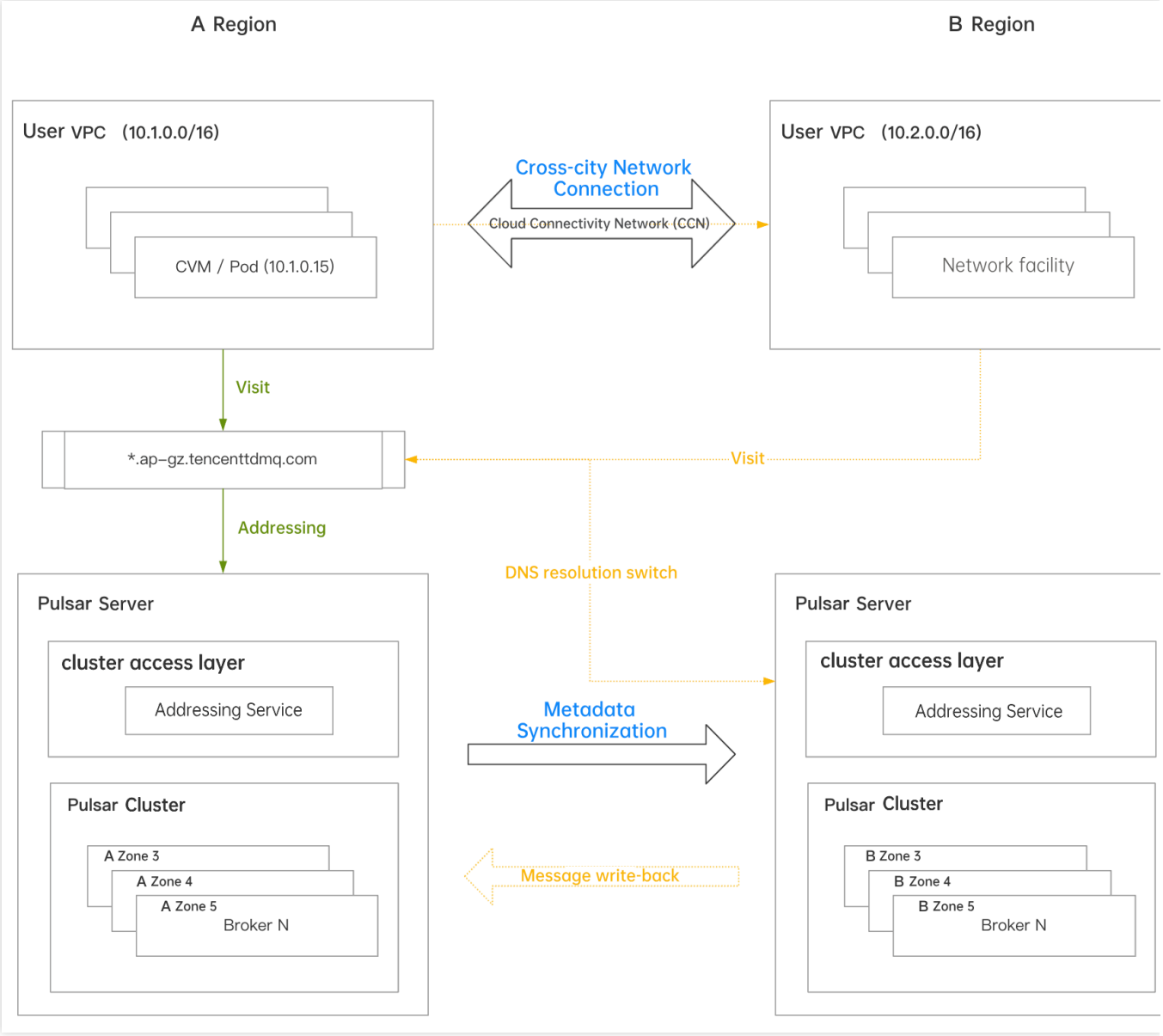
1. **Feature Support Scope**
This feature is supported only in professional clusters.
2. **Linkage Replication Direction**
Currently, cross-region replication, whether at the message level or metadata level, is unidirectional.
3. **Regarding Replication Objects**
For a single object, only one synchronization task can be created, even at higher hierarchical levels.
Topics that are part of a synchronization linkage cannot be deleted unless the synchronization linkage is removed first.
4. **Overwrite Issues**
For existing resources with the same name but different configurations, such as partition count or TTL attributes, the target cluster will not overwrite the configurations after creating a replication task.

Cross-Region Disaster Recovery Practices

Last updated：2024-12-02 17:25:44

Cross-Region Disaster Recovery

Message middleware is a vital component in the technical architecture of business systems. While TDMQ for Apache Pulsar already supports disaster recovery across multiple availability zones, it introduces the **Cross-region disaster recovery** solution to address region-level disasters. This solution enables customers to quickly migrate their business operations, ensuring uninterrupted continuity.
The following document provides an overview of the cross-region disaster recovery solution.



Under normal circumstances, business operations in Region A access the Pulsar server. Users need to complete two main actions:
1. Establish cross-city network connectivity using Cloud Connect Network (CCN) to enable cross-region VPC communication.
2. Synchronize metadata between the two regions via the Pulsar console, including namespaces, Topics, subscriptions, and roles.
When an exception occurs, the TDMQ for Apache Pulsar console provides a domain name parsing switch feature. This feature redirects the domain name originally used in Region A to the disaster recovery cluster in Region B. This avoids the need for clients to modify access point addresses, enabling seamless access to the Region B cluster and ensuring business continuity.
Once the exception in Region A is resolved, users need to determine whether to write back the messages generated in Region B to Region A to ensure message integrity. If a write-back is needed, please contact our after-sales team for assistance. Afterward, users can switch the access point domain name parsing back to the Region A cluster from Region B. Once the switch is completed, clients can resume normal access to Region A.

Operation Guide

Configuring Disaster Recovery Features

1. In the backup region, create a professional cluster. On the cluster purchase page, enable the **Cross-region Replication** switch and select the cluster to be backed up;
2. Configure the cluster metadata synchronization linkage through the console:
Replication linkage name: Define a name for the synchronization linkage.
Linkage type: Select metadata.
Source cluster selection: Choose the Pulsar cluster for disaster recovery backup.
Target cluster selection: Select the pre-created disaster recovery cluster in a different region. Only clusters with the same cluster ID will be displayed.
Replication level: Choose between cluster-level and namespace-level replication.
Cluster level: Suitable for cold backups at the cluster level.
Namespace Level: Suitable for scenarios where clusters in both regions are actively used, with different namespaces distributed across regions. Regions act as mutual primary and backup for each other.

Establishing CCN

Use Cloud Connect Network to link the production region and the backup region, creating a network access channel. This ensures that, in the event of a disaster, clients in the production region can access the backup cluster across regions.
For detailed configuration steps, see CCN Operation Guide and perform the following operations:
1. Create a Cloud Connect Network instance

2. Associating a Network Instance

When Disaster Occurs

Users can decide to switch client access to the backup region:
1. If the console is available: Initiate a domain name parsing switch via the console;
2. If the console is unavailable: Contact the after-sales architect to request a switch, which will be initiated by the TDMQ service.

After Disaster Recovery

Users can decide to switch client access back to the original region cluster:
1. Evaluate whether messages need to be written back to the original region. If write-back is required, contact our after-sales team for assistance.
2. Initiate a domain name switch-back via the console to restore normal client access to the original region.

Notes

1. Supported Scope

This feature is supported only in professional clusters.

2. Message Write-Back

Message write-back is a prerequisite assessment when switching traffic back to the original region. It aims to prevent data loss and ensure data integrity. Be sure to decide whether to perform a write-back before initiating the domain name switch-back.
User-provided information:
The list of Topics to be migrated, including details such as cluster ID, namespace, or specific Topic lists.
The start and end time. Messages sent within this time range, based on the publishTime field in the message header, will be identified as data to be migrated.
Impacts of message write-back:
A large number of duplicate messages may occur. The server does not account for the complex state machine of offset synchronization between the source and target clusters. All migrated messages are treated as new messages, even if identical messages already exist in the historical data. They will be regarded as separate messages. If duplicate messages impact your business, it is recommended to implement idempotent processing on the client side.
A small number of messages may arrive out of order.

3. About Roles

The source cluster should have at least one Role, which does not need to be bound to a namespace. This ensures that during synchronization, the Role and Token remain consistent with the disaster recovery cluster.

4. CCN Configuration

When you configure CCN, the VPC CIDRs of the two regions should not overlap. For example, use 10.0.0.0/16 for Guangzhou and 10.1.0.0/16 for Shanghai. This ensures that CCN can link the two VPCs without IP conflicts.

5. Domain Name Switch Effectiveness Time

The domain name switch takes approximately 5 seconds to 5 minutes to become effective. This duration includes two parts: domain name parsing switch and client disconnection and reconnection to the new cluster's Broker.

6. Post-Switch Actions During a Disaster

After traffic is switched to the disaster recovery cluster during a disaster, avoid making metadata changes on the backup cluster, such as modifying namespace attributes or creating Topics.

Cluster Migration
Single Write and Multiple Read Migration Solution

Last updated：2025-04-01 14:18:35

This document provides an overview of feasible solutions for migrating between different clusters. You can choose the migration solution that suits your business scenario.

Application Scenarios

1. Unable to migrate at the virtual cluster level.
2. Hope to migrate resources under a virtual cluster to different Professional Edition Clusters.
3. Self-built Pulsar to Tencent Cloud Pulsar.

Single-Write Multiple-Read Solution

The overall solution is simple and clear, easy to implement, with no data backlog and a smooth transition. Under this solution, users can have more flexible control over the resource granularity and grayscale method of migration.

Migration Process

1. Start up business consumers that connect to the new cluster access point (dual-read, with consumers consuming data from both the old and new clusters simultaneously).
2. Modify the access point address of the original producer to the new cluster and restart it, making new messages produced to the new cluster, until all producers of the original cluster are modified/closed (switch writing, switching production flow from the old cluster to the new cluster).
3. Pay attention to the message backlog situation of the original cluster.
4. After there are no backlog messages in the original cluster, the consumers of the old cluster can be closed. At this point, the business has been migrated to the new cluster (single-read, with consumers only consuming from the new cluster).
5. Upon migration completion, delete the existing cluster.

Cluster Migration Capability Description

Last updated：2025-04-01 14:19:29

Application Scenarios

To meet user needs in different usage scenarios, TDMQ Pulsar provides two product forms: **professional cluster** and **virtual cluster**.
Virtual clusters are at risk of instability. We stopped adding new ones in 2023. Professional clusters have stronger product capabilities and a more optimized console (for management, renewal, scale-out, etc.). To provide better service, for your **virtual clusters** currently in use, we provide the ability for smooth inter-cluster migration, supporting smooth migration from **virtual clusters** to **professional clusters**.

Capability Description

The migration process of cluster data is almost transparent to users, that is, the migration process is smooth (no adjustment needed for access points, no code modification required for users' services).
Migration Process
1. The system will deduct according to the specifications of the professional cluster. When starting migration, the deduction status can be seen as in processing on the order interface; during the migration process, if a rollback occurs due to a problem, the order will be automatically refunded; after migration is completed, the order status is completed and timing officially starts.
2. On the List Interface of **Professional Cluster** in the console, you can see the cluster information after migration and complete subsequent operations such as management, upgrade, and renewal.

Smooth Prerequisite

Smooth migration has one **prerequisite**: Some access point addresses are unable to smoothly migrate to the new cluster because the cluster was created earlier or the network was established in a special way.
Therefore, users need to provide information about the access point address in use to confirm the feasibility.

Operation Process

1. Initiate migration. The frontend will initiate verification of the current access point address. If there is a non-standard access point, a pop-up notification will appear.

2. Target specification selection. Based on the current concurrency status of the virtual cluster, you can select a professional cluster with the corresponding specification.
3. Access point scanning. The server will scan whether the client is using a non-standard access point;
4. Initiate upgrade. Start the migration action.

Possible Issues

1. **Message duplication issue**
Idempotent processing has been realized for progress synchronization through individual ack to reduce the number of duplicate messages during the migration process as much as possible. However, duplicates during the migration process may not be completely avoided. Usually, the duplication time does not exceed 1 minute. If necessary, users are required to perform idempotent processing in advance.
2. **Message disorder**
A potential issue that may exist in cluster migration. No solution can completely avoid the disorderly situation during the migration process. Users need to be notified in advance.
3. **Monitoring data**
Switching clusters may lead to inaccurate instantaneous monitoring data, which usually recovers within 1 - 2 minutes.
4. **Fluctuation in generation time**
Switching clusters may cause temporary fluctuations in generation time. The time taken is similar to that during the cluster upgrade process. It usually recovers within 1 minute.
5. **Message trace**
During the process of data synchronization, there will be messages generated for consumption progress synchronization. Users will see such messages when using message query. Querying message details may have certain impacts during the migration process. There may be situations where they cannot be viewed.
6. **Migration duration**
The time for the entire migration is related to the quantity of namespaces, production flow, and the quantity of stored data in message storage. For a namespace, with 1000 TPS and 100G message storage, the cluster migration can usually be completed within 1 hour; in the case of a large data volume, for example, 1T storage will probably take about 2 hours.
7. **Retention time of the existing cluster**
After migration, the Tencent Cloud product research and development side will wait for 1 - 3 days before cleaning up the resources on the old physical cluster. After clearance, it will not be able to roll back.
8. **Message backlog issue**
The synchronization of consumption progress during the migration process is performed through the user's topic. Therefore, there will be some internal messages in the user's topic. These messages will be filtered out on the server side when consumed. In business reality, these messages will not actually be consumed. For subscriptions without consumers, there will be a message backlog situation.

9. **Message replication scope**
During the message replication process, due to Pulsar's implementation mechanism, only messages within the TTL range of the existing cluster can be guaranteed to be replicated to the new cluster. If your message retention period is relatively large and you need to synchronize the data within the retention period, you need to adjust the TTL configuration first.

Migration Principle

Technical Solution

Adopt the Pulsar Geo Replication solution and enable cross-cluster two-way replication to achieve synchronization of data and message progress to meet the needs of cluster migration.

Migration Main Process

The main process of migration is shown as illustrated below. Go to next step upon success of each stage.

1. Console operations initiate the migration action. The platform initiates the shipment. After you pay for the order, you start building a new professional cluster.
2. Cluster metadata synchronization, namespace, topic, subscription, role, namespace policies, etc.
3. Enable cross-cluster data synchronization.
4. Switch cluster. The operation platform sends a tenant cluster switch instruction to the old cluster, actively triggering the unload of topics on the old cluster, triggering the client lookup, and returning the new cluster address information during the lookup stage.
5. Confirm that the user data has been successfully migrated, then disable cross-cluster data synchronization and clean up the old cluster resources.
6. You can see the new cluster in the console.