



Console User Manual

Apusic Distributed Message Queue V2.0.6_for_mqtt

Copyright Notice

All intellectual property rights including software copyrights involved in this document have been legally registered and duly owned by Kingdee Apusic Cloud Computing Co., Ltd. Such rights are protected by Copyright Law of the People's Republic of China, Regulations on Protection of Computer Software, Regulations on Intellectual Property Protection, relevant international copyright conventions, laws, regulations and other intellectual property legislations. Unauthorized use is strictly prohibited.

Disclaimer

All copyright information contained herein is legally owned by Kingdee Apusic Cloud Computing Co., Ltd. and protected by applicable laws. The Company shall bear no liability for any information unrelated to Kingdee Apusic contained in this document. You may view, copy and print this document only within the scope permitted by Copyright Law of the People's Republic of China. No entity or individual may use, modify or republish any part or content of this document without written authorization from Kingdee Apusic Cloud Computing Co., Ltd. Any violation shall constitute infringement, and the Company reserves the right to pursue legal liabilities accordingly.

Updates to this document shall not be notified separately. You may consult the Company regarding issues related to this document. All rights not expressly granted by the Company are reserved.

Trademark Notice

 is a registered trademark filed with the National Intellectual Property Administration of PRC by Kingdee Apusic Cloud Computing Co., Ltd. Shenzhen. Exclusive rights to the registered trademark are legally owned by Kingdee Apusic and protected by law. Without written consent of Kingdee Apusic, no entity or individual shall use, copy, modify, disseminate, transcribe, or bundle and sell any part of this trademark with other products in any manner or for any reason. Kingdee Apusic shall pursue legal liabilities against any infringement of its trademark rights. All other trademarks or registered trademarks mentioned in this document belong to their respective owners.

Contents

- 1 Preface
 - 1.1 Target Audience
 - 1.2 Related Documents
 - 1.3 Technical Support
- 2 Terminology
- 3 Management Console Access
 - 3.1 Access URL
- 4 Core Concepts
 - 4.1 Topic
 - 4.2 QoS (Quality of Service)
 - 4.3 Retained Message
 - 4.4 Clean Session and Session Persistence
 - 4.5 Will Message
 - 4.6 ACL (Access Control List)
 - 4.7 Authenticator
 - 4.8 Authorization Source
 - 4.9 Message Flow Diagram
- 5 Overview
 - 5.1 Resource Overview
 - 5.2 Connection Information
 - 5.3 Common Use Cases
- 6 Users and Permissions
 - 6.1 User Management
 - 6.1.1 Prerequisites
 - 6.1.2 Top Filtering
 - 6.1.3 User List
 - 6.1.4 Operations
 - 6.2 Permission Management (ACL)
 - 6.2.1 Prerequisites
 - 6.2.2 Top Filtering and Tabs
 - 6.2.3 Rule List
 - 6.2.4 Operations

- 6.3 Blacklist Management
 - 6.3.1 Top Filtering
 - 6.3.2 Blacklist List
 - 6.3.3 Operations
- 7 Resource Management
 - 7.1 Topic Management
 - 7.1.1 Top Filtering
 - 7.1.2 Topic List
 - 7.1.3 Operations
 - 7.2 Subscription Management
 - 7.2.1 Top Filtering
 - 7.2.2 Subscription List
 - 7.2.3 Operations
 - 7.3 Message Management
 - 7.3.1 Retained Messages
 - 7.3.2 Topic Rewrite
 - 7.3.3 Auto Subscribe
 - 7.4 Client Management
 - 7.4.1 Top Filtering
 - 7.4.2 Client List
 - 7.4.3 Operations
 - 7.4.4 Connection Details
- 8 Monitoring and Operations
 - 8.1 Monitoring Dashboard
 - 8.2 Resource Monitoring
 - 8.2.1 Topic Monitoring
 - 8.2.2 Node Monitoring
 - 8.2.3 Slow Subscriptions
 - 8.3 Logs and Alerts
 - 8.3.1 Log Trace
 - 8.3.2 Alerts
- 9 System Configuration
 - 9.1 Authenticator Management
 - 9.1.1 Top Filtering

- 9.1.2 List
- 9.1.3 Add Authenticator (Three-step Wizard, Full Page)
- 9.1.4 Other Operations
- 9.2 Authorization Source Management
 - 9.2.1 Top Filtering
 - 9.2.2 List
 - 9.2.3 Add Authorization Source (Two-step Wizard, Full Page)
 - 9.2.4 Other Operations
- 9.3 Listeners
 - 9.3.1 List
 - 9.3.2 Add / Edit Listener
 - 9.3.3 Other Operations
- 9.4 System Configuration
 - 9.4.1 Configuration Sections (Tabs)
 - 9.4.2 Operations
- 9.5 Data Backup
 - 9.5.1 List
 - 9.5.2 Operations
- 10 Frequently Asked Questions
 - 10.1 I. Connection and Authentication
 - 10.1.1 Q1: Client connection shows authentication failure. How to troubleshoot?
 - 10.1.2 Q2: Why can the client still connect after changing the user password?
 - 10.1.3 Q3: What is the difference between a super user and a regular user?
 - 10.2 II. Topics and Subscriptions
 - 10.2.1 Q4: Subscribed to a topic but not receiving messages. How to troubleshoot?
 - 10.2.2 Q5: What is the purpose of retained messages? How to clear them?
 - 10.2.3 Q6: Will QoS 0 and QoS 1 subscribers receive the same message?
 - 10.3 III. Authentication and Authorization
 - 10.3.1 Q7: ACL rules are configured but still shows no permission. What to do?
 - 10.3.2 Q8: How are multiple authorization sources matched?
 - 10.4 IV. Monitoring and Operations
 - 10.4.1 Q9: How to view the real-time operational status of the MQTT cluster?
 - 10.4.2 Q10: How are slow subscription records generated?
 - 10.4.3 Q11: Why can only 100 topics be added to Topic Monitoring?

- 10.4.4 Q12: Where can I view log traces and alerts?
- 10.5 V. System Configuration
 - 10.5.1 Q13: How long does it take for system configuration changes to take effect?
 - 10.5.2 Q14: What impact does resetting system configuration have?
- 10.6 VI. Other
 - 10.6.1 Q15: What is the relationship between MQTT and ADMQ MQTT mentioned in the documentation?

1 Preface

This document is a user manual for the Apusic Distributed Message Queue for MQTT (Apusic Distributed Message Queue, referred to as: ADMQ for MQTT) console product, detailing the functionality usage, configuration methods, and management operations of the ADMQ for MQTT web console.

1.1 Target Audience

This document is intended for IT information business leaders, R&D managers, software project managers, software architects, and operations engineers.

1.2 Related Documents

To learn more about ADMQ for MQTT, please refer to the following ADMQ for MQTT product documentation set:

No.	Document	Description
1	Apusic Distributed Message Queue for MQTT Quick Start Guide	Briefly introduces how to quickly get started with ADMQ for MQTT.
2	Apusic Distributed Message Queue for MQTT Installation Guide	Details how to install ADMQ for MQTT on various operating systems, as well as service start/stop operations.
3	Apusic Distributed Message Queue for MQTT Message Engine User Manual	Details the use, configuration, and management of ADMQ for MQTT message engine features and supporting tools.
4	Apusic Distributed Message Queue for MQTT Console User Manual	Details the use and operation of the ADMQ for MQTT console.
5	Apusic Distributed Message Queue for MQTT Development Guide	Details how to develop ADMQ for MQTT client applications in various development languages.
6	Apusic Distributed Message Queue for MQTT Migration Guide	Details the migration from MQTT Broker to ADMQ for MQTT.
7	Apusic Distributed Message Queue for MQTT Operations Manual	Details monitoring, operations, and security hardening for ADMQ for MQTT.
8	Apusic Distributed Message Queue for MQTT Performance Optimization Guide	Details performance tuning for ADMQ for MQTT.

1.3 Technical Support

ADMQ for MQTT provides comprehensive technical support services. You can obtain technical support through the following channels:

- Website: www.apusic.com
- Phone: 400-855-5800
- Email: support@apusic.com
- Kingdee Cloud Community: <https://vip.kingdee.com/?productId=73&productLineId=14&lang=zh-CN>

When seeking technical support, please provide the following information:

1. Your name
2. Company information and contact details
3. Operating system and its version
4. Product version number
5. Detailed information such as logs and screenshots of the exception or error

2 Terminology

Term	Description
Cluster	MQTT cluster, consisting of multiple MQTT nodes
Node	A single service node in an MQTT cluster
Client	MQTT client, including publishers and subscribers
ClientID	Unique identifier for an MQTT client
Topic	Message classification identifier
QoS	Quality of Service level, defines message delivery reliability
Retain	Retained message flag
Will	Will message
Clean Session	Whether to clear the session
ACL	Access Control List
Authenticator	Authentication mechanism
Authorization Source	Authorization data source

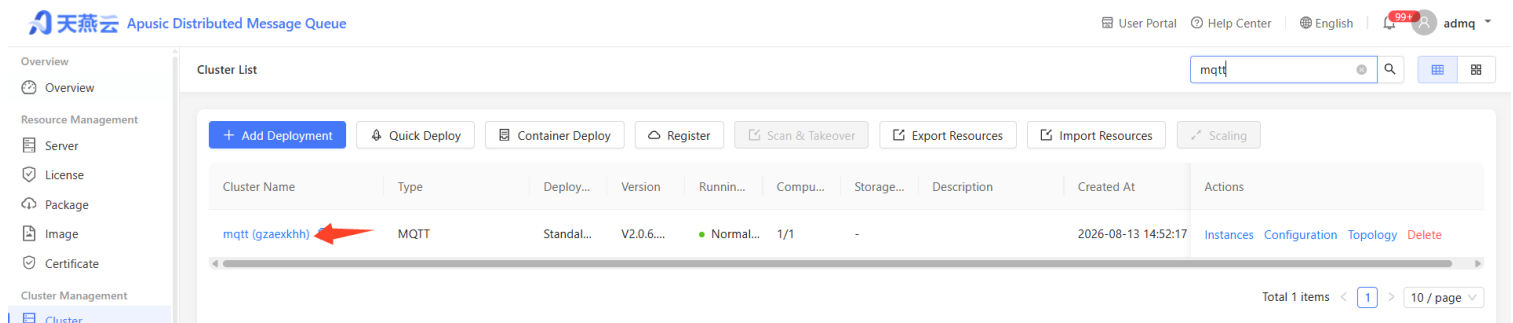
3 Management Console Access

3.1 Access URL

Enter the following URL in your browser's address bar to access the ADMQ console login page:

```
http://{console_ip}:12305
```

Where `{console_ip}` is the console server IP address.



4 Core Concepts

Before using ADMQ MQTT, it is recommended to understand the following core concepts:

4.1 Topic

A topic is a **logical categorization unit** for messages in MQTT. Producers publish messages to topics, and consumers subscribe to topics to receive messages.

- Topics use `/` to separate levels, e.g., `sensor/living-room/temperature`.
- Two wildcards are supported:
 - `+` : Matches a single level, e.g., `sensor+/temperature`.
 - `#` : Matches zero or more levels, must be at the end of the topic, e.g., `sensor/#`.

4.2 QoS (Quality of Service)

QoS defines the reliability level of message delivery.

QoS Level	Name	Description	Typical Scenario
0	At most once	Message is sent once, delivery is not guaranteed	High-frequency, loss-tolerant telemetry data
1	At least once	Message is guaranteed to be delivered, may be duplicated	General business messages
2	Exactly once	Message is guaranteed to be delivered without duplication	Scenarios with high consistency requirements

4.3 Retained Message

Retained messages are a special mechanism in MQTT:

- When a publisher sends a retained message, the Broker retains the last retained message for that topic.
- When a new subscriber subscribes to that topic, they immediately receive this retained message.
- Commonly used in scenarios such as device status and configuration delivery.
- Sending an empty retained message can clear the retained message for that topic.

4.4 Clean Session and Session Persistence

- **Clean Session = true:** After the client disconnects, the Broker does not save its subscription relationships and unacknowledged messages.
- **Clean Session = false:** The Broker saves subscription relationships, unacknowledged messages, and offline messages (QoS 1/2). The client can resume upon reconnection.
- In MQTT 5.0, the corresponding concepts are **Clean Start** and **Session Expiry Interval**.

4.5 Will Message

The will message is automatically published by the Broker when a client disconnects abnormally:

- The client presets the will topic, will content, QoS, and Retain when connecting.
- When the connection is abnormally interrupted without sending a DISCONNECT, the Broker automatically publishes the will message.
- Commonly used for device online/offline status notifications.

4.6 ACL (Access Control List)

ACL controls client access permissions to MQTT resources:

- **Subject:** All, Username, Client ID.
- **Action:** Publish, Subscribe, All.
- **Permission:** Allow, Deny.
- **Topic:** Supports wildcards.
- **QoS/Retain Restrictions:** Can further restrict allowed QoS levels and Retain behavior.

4.7 Authenticator

The authenticator defines how to verify identity when a client connects:

- **Password-Based:** Username/password authentication, data sources can be built-in database, MySQL, PostgreSQL, HTTP, etc.
- **JWT:** JSON Web Token based authentication.
- **SCRAM:** SCRAM challenge-response mechanism.

4.8 Authorization Source

The authorization source defines the data source for ACL rules:

- **built_in_database:** Built-in database, supports managing rules directly on the platform.
- **file:** Configured through acl.conf file.
- **HTTP/MySQL/PostgreSQL etc.:** External data sources.
- Multiple authorization sources are matched sequentially by priority.

4.9 Message Flow Diagram

```

Publisher —→ MQTT Broker
      |
      |— Topic Matching —→ Subscriber A (QoS 0)
      |
      |— Topic Matching —→ Subscriber B (QoS 1)
      |
      |— Retained Message Storage —→ New subscriber receives
immediately

```

5 Overview

Corresponding menu: **Overview** → **Overview**

The overview page is the homepage after entering an MQTT cluster, used for quickly understanding the cluster's resource scale and connection status.

The overview page consists of two parts:

1. **Resource Overview:** Displays key resource metrics of the current cluster in statistical card format (e.g., connection count, topic count, subscription count, retained message count, etc.; specific items depend on cluster response).
2. **Connection Information:** Displays the cluster's connection endpoints and online status in a table format.

The top-right corner of the page provides a **Refresh** button for manually fetching the latest data.

5.1 Resource Overview

The resource overview area displays the core resource statistics of the current cluster, used for quickly assessing cluster load and scale. Metrics are dynamically rendered based on actual cluster response, commonly including:

- Online connection count
- Topic count
- Subscription count
- Retained message count

Values are snapshots at the time of fetching. Click **Refresh** in the top-right corner to update.

5.2 Connection Information

The connection information table displays the access points where the current cluster provides external services. Fields are as follows:

Column	Description
Cluster Name	Name of the cluster
Cluster Type	Middleware type of the cluster (MQTT / EMQX)
Connection Address	Cluster access address, multiple addresses displayed on separate lines
Connection Status	online / offline badge, reflects connectivity between platform and cluster

Function	Purpose of this access point
----------	------------------------------

Connection Address is the address used by business clients to connect to the Broker. It can be used together with the port information in *System Configuration → Listeners*.

5.3 Common Use Cases

- Quickly confirm whether the cluster is online and whether resource scale is abnormal during daily inspections.
- Provide access addresses for business parties.
- Serve as an overall status reference before entering other functional modules.

6 Users and Permissions

Corresponding menu: *Users and Permissions*

This chapter covers three functions related to users, permissions, and blacklists: *User Management*, *Permission Management (ACL)*, and *Blacklist Management*.

6.1 User Management

Corresponding menu: *Users and Permissions → User Management*

Manages MQTT users stored in the **built-in database authenticator**, supporting add, edit, delete, and sync to MQTT cluster.

6.1.1 Prerequisites

Users depend on a built-in database authenticator. If one has not been created, the page will display a prompt "No available built-in database authenticator, please go to [Authenticator Management] to create one" and provide a **Go to Authenticator Management** button. Please create a Built-in Database authenticator in **System Configuration → Authenticator Management** first.

6.1.2 Top Filtering

- **Authenticator:** Dropdown to select the target `built_in_database` authenticator (searchable). All user operations apply to the selected authenticator.
- **Search Username:** Fuzzy search by username.

6.1.3 User List

Column	Description
Username	Username used for client login
Is Super User	Yes (red tag) / No
Description	Remarks
Creation Time	User creation time
Actions	Edit / Delete

6.1.4 Operations

Toolbar

- **Add:** Opens an add drawer to create a user.
- **Sync to MQTT:** Opens "User Sync Preview", showing users to be added, deleted, or updated (columns: Username, Is Super User), pushes to cluster after confirmation.

Add / Edit User (Drawer)

Field	Type	Required	Description
Authenticator	Read-only	—	Displays current authenticator
Username	Text	Yes	Cannot be modified during edit
Password	Password	Required for add	Leave blank during edit to keep unchanged
Is Super User	Radio	—	Yes / No, default No
Description	Multi-line text	No	Max 4096 characters

*Tip: It is recommended not to enable super user for regular business accounts. Super users bypass all ACL checks. After adding or modifying a user, you must click **Sync to MQTT** for it to take effect on the cluster.*

6.2 Permission Management (ACL)

Corresponding menu: *Users and Permissions → Permission Management*

Manages ACL rules in the **built-in database authorization source**, controlling client publish/subscribe permissions on topics. Supports configuration by username, client ID, or global rules.

6.2.1 Prerequisites

ACL rules depend on a built-in database authorization source. If one has not been created, the page will prompt "No available built-in database authorization source, please go to [Authorization Source Management] to create one" and provide a **Go to Authorization Source Management** button. Please create a Built-in Database authorization source in **System Configuration → Authorization Source Management** first.

6.2.2 Top Filtering and Tabs

- **Authorization Source:** Dropdown to select the target `built_in_database` authorization source (searchable).
- **Permission:** `Allow` / `Deny` .
- **Action:** `Publish` / `Subscribe` / `All` .
- **Username / Client ID:** Filter by subject (label changes with tab).

- **Tabs:** `All Rules` / `Username Rules` / `Client ID Rules` . Switching tabs resets pagination, filters, and selections.

6.2.3 Rule List

Columns vary slightly across different tabs:

Column	Description
Username / Client ID	Only displayed in corresponding tab
Permission	<code>Allow</code> (green) / <code>Deny</code> (red)
Action	<code>Publish</code> / <code>Subscribe</code> / <code>All</code>
Topic	Rule matching topic (supports wildcards)
QoS	Allowed QoS, <code>Unlimited</code> means no restriction
Retain	<code>Allow</code> / <code>Deny</code> / <code>Unlimited</code>
Creation Time	Rule creation time
Description	Remarks
Actions	Edit / Delete

6.2.4 Operations

Toolbar

- **Add:** Opens add drawer.
- **Sync to MQTT:** Pushes ACL rules to cluster for effect.
- **Batch Delete (N):** Appears after checking multiple rows, batch deletes selected rules.

Add / Edit Rule (Drawer, title varies by subject type)

Field	Type	Required	Description
Authorization Source	Read-only	—	Displays current authorization source
Username	Text	Yes	Only shown for "Username Rules"
Client ID	Text	Yes	Only shown for "Client ID Rules"
Permission	Dropdown	Yes	<code>Allow</code> / <code>Deny</code>
Action	Dropdown	Yes	<code>Publish</code> / <code>Subscribe</code> / <code>All</code>

Topic	Text	Yes	e.g., sensor/# OR +/+temp
QoS Limit	Number	No	-1~2, -1 means unlimited
Retain Limit	Number	No	-1 unlimited, 0 deny, 1 allow
Description	Multi-line text	No	Max 4096 characters

*Tip: Rules need to be clicked **Sync to MQTT** after adding or modifying to take effect. If configured rules are still being denied, click "Clear Authorization Cache" in **Client Management** → **Details** to force a refresh.*

6.3 Blacklist Management

*Corresponding menu: **Users and Permissions** → **Blacklist Management***

Bans by dimensions such as client ID, username, and IP address, supporting exact match, regex/CIDR rule matching, and expiration time setting. The blacklist directly affects the cluster without needing to select an authenticator/authorization source.

6.3.1 Top Filtering

- **Type:** Client ID / Username / IP Address / Client ID Rule / Username Rule / IP Range.
- **Ban Value:** Search by ban value.

6.3.2 Blacklist List

Column	Description
Type	Ban dimension (different colors for different types)
Ban Value	Specific value or rule being banned
Expiration Time	Expiry time; displays <code>Permanent</code> if none; expired items shown in red "(Expired)"
Reason	Ban reason, displays - if empty
Creation Time	Ban creation time
Actions	Edit / Delete

6.3.3 Operations

Toolbar

- **Add:** Opens add drawer.

- **Sync:** Opens "Blacklist Sync Preview", showing entries to be added/deleted (columns: Type, Ban Value, Reason), syncs to cluster after confirmation.

Add / Edit Ban (Drawer)

Field	Type	Required	Description
Type	Dropdown	Yes	Client ID / Username / IP Address / Client ID Rule / Username Rule / IP Range
Ban Value	Text	Yes	Placeholder changes by type (see below)
Expiration Time	Date-time	No	Leave blank for permanent
Reason	Multi-line text	No	Ban reason

Ban Value Format and Validation

Type	Input Example	Validation
Client ID	Specific client ID	—
Username	Specific username	—
IP Address	192.168.1.1	Must be valid IPv4/IPv6
Client ID Rule / Username Rule	Regex expression	Must be valid regex
IP Range	192.168.1.0/24	Must be valid CIDR

Tip: After adding or modifying, you must click **Sync** for the ban to take effect on the cluster. Expired entries are marked in red in the list and can be manually deleted.

7 Resource Management

Corresponding menu: *Resource Management*

This chapter covers four functions: *Topic Management*, *Subscription Management*, *Message Management*, and *Client Management*.

7.1 Topic Management

Corresponding menu: *Resource Management → Topic Management*

Manages cluster topics, displaying each topic's QoS, Retain, source, status, and node. Supports manual creation, editing, deletion, and single/batch message sending.

7.1.1 Top Filtering

- **Search Topic:** Fuzzy search by topic name.

7.1.2 Topic List

Column	Description
Topic	Topic name
QoS	Default QoS
Retain	Whether to retain messages
Source	Topic source
Status	Topic status
Node	Cluster node where the topic resides
Description	Remarks
Creation Time	Creation time
Actions	Send Message / Edit / Delete

7.1.3 Operations

Toolbar

- **Add:** Create topic.
- **Sync:** Preview differences from cluster (add/delete/update) and sync.

- **Batch Publish:** Publish messages to multiple topics at once.

Add / Edit Topic (Drawer)

Field	Type	Required	Description
Topic	Text	Yes	Cannot be modified during edit
Default QoS	Number	—	0~2, only configurable during add, default 0
Retain	Radio	—	yes / No, only configurable during add, default No
Description	Multi-line text	No	Max 4096 characters

Send Message (Row-level "Send Message" drawer)

Field	Type	Required	Description
Topic	Text (read-only)	—	Current row topic
Message Content	Text	Yes	Message Payload
QoS	Radio	—	0 / 1 / 2
Retain	Radio	—	Yes / No

Batch Publish (Toolbar "Batch Publish" drawer)

Uses an editable table to fill in messages row by row, with columns including Topic, Payload, QoS, Retain. Provides **Add Message** to add rows, **Confirm Publish** to submit; cannot delete when only one row remains.

7.2 Subscription Management

Corresponding menu: Resource Management → Subscription Management

Manages client subscription relationships, displaying QoS, source, status, and node by client ID and topic. Supports manual addition and deletion of subscriptions.

7.2.1 Top Filtering

- **Search Client ID:** Fuzzy search by client ID.
- **Search Topic:** Fuzzy search by topic.

7.2.2 Subscription List

Column	Description
--------	-------------

Client ID	Click to navigate to client management and locate the client
Topic	Subscribed topic
QoS	Subscription QoS
Source	Subscription source
Status	Subscription status
Node	Subscription node
Actions	Delete

7.2.3 Operations

Toolbar

- **Add:** Manually add subscription.
- **Sync:** Opens "Subscription Sync Preview", showing add/update/delete differences, syncs after confirmation.

Manual Add Subscription (Drawer)

Field	Type	Required	Description
Client ID	Text	Yes	Target client
Topic	Text	Yes	Subscription topic
QoS	Dropdown	Yes	QoS 0 / 1 / 2
Description	Multi-line text	No	Remarks

Delete Note: If the subscription still exists on the cluster, deleting it will also cancel the client's subscription.

7.3 Message Management

Corresponding menu: *Resource Management* → *Message Management*

Message Management is a container page with three tabs: **Retained Messages**, **Topic Rewrite**, and **Auto Subscribe**.

7.3.1 Retained Messages

Tab: *Message Management* → *Retained Messages*

Displays retained messages stored on the Broker, with the ability to view decoded content and delete.

Top Filtering: Search Topic.

List

Column	Description
Topic	Topic name
Client ID	Client that published the retained message
QoS	Message QoS
Retain	Retained flag
Actions	View Content / Delete

- **View Content:** Fetches retained message details and decodes Payload, displayed in a popup (title "Retained Message Content - {topic}"), supports copy.
- **Delete:** Deletes the retained message. Sending an empty retained message can also clear it.

7.3.2 Topic Rewrite

Tab: Message Management → Topic Rewrite

Manages topic rewrite rules, redirecting or transforming topics during subscribe/publish/all actions.

Top Filtering: Action type (Subscribe / Publish / All), source topic / destination topic search.

List

Column	Description
Action	Subscribe / Publish / All
Source Topic	Matching source topic
Destination Topic	Rewritten destination topic
Regex	Matching regular expression
Order	Rule matching order
Actions	Edit / Delete

Toolbar: Add, Sync to MQTT.

Add / Edit Rule (Drawer)

Field	Type	Required	Description
Action	Dropdown	Yes	Subscribe / Publish / All
Source Topic	Text	Yes	Source topic
Destination Topic	Text	Yes	Destination topic
Regex	Text	Yes	Matching regex
Order	Number	No	≥0, smaller value matches first

7.3.3 Auto Subscribe

Tab: Message Management → Auto Subscribe

Manages auto-subscribe rules. Clients automatically subscribe to specified topics after connecting.

Top Filtering: QoS (0 / 1 / 2), topic search.

List

Column	Description
Topic	Auto-subscribe topic
QoS	Subscription QoS
No Local	Whether to not receive messages published by itself
Retain As Published	Whether to retain the Retain flag as published
Retain Handling	Retained message handling strategy
Order	Matching order
Actions	Edit / Delete

Toolbar: Add, Sync to MQTT.

Add / Edit Rule (Drawer)

Field	Type	Required	Description
Topic	Text	Yes	Auto-subscribe topic
QoS	Dropdown	Yes	QoS 0 / 1 / 2

No Local	Dropdown	Yes	No(0) / Yes(1)
Retain As Published	Dropdown	Yes	No(0) / Yes(1)
Retain Handling	Dropdown	Yes	0-Send retained message / 1-Do not send retained message / 2-Do not send and do not receive subsequent
Order	Number	No	≥0

7.4 Client Management

Corresponding menu: *Resource Management* → *Client Management*

Manages online MQTT client connections, displaying client ID, username, IP, connection time, Keepalive, clean session, and protocol. Supports single/batch disconnect and viewing connection details.

7.4.1 Top Filtering

- **Search Client ID:** Search by client ID.
- **Search Username:** Search by username.

7.4.2 Client List

Column	Description
Client ID	Client identifier
Username	Login username
IP Address	Client IP (shown as IP:port when port is included)
Connection Time	Connection establishment time
Keepalive	Heartbeat keepalive interval
Clean Session	Clean Session / Clean Start
Protocol	Protocol name and version
Actions	Details / Disconnect

7.4.3 Operations

Toolbar

- **Batch Disconnect (N):** Available after checking multiple rows, disconnects selected connections in batch.

Row-level Operations

- **Details:** Opens connection details drawer (see below).
- **Disconnect:** Disconnects the connection.

7.4.4 Connection Details

Clicking "Details" opens a drawer (title "Connection Details - {clientId}"), containing four tabs:

- **Connection Details:** Read-only display of client ID, username, IP, connection time, Keepalive, clean session, protocol, etc.; provides a **Clear Authorization Cache** button (forces refresh of the client's authorization cache).
- **Subscription Management:** Client's current subscription list (columns: Topic, QoS, NL, RAP, RH, Actions). Provides **Add Subscription** (Topic, QoS, No Local, Retain As Published, Retain Handling), row-level **Unsubscribe**.
- **Inflight Messages:** Messages currently being delivered (columns: ID, Topic, QoS, Payload, Send Time), supports "Load More".
- **Message Queue:** Messages queued for delivery (columns: ID, Topic, QoS, Payload, Send Time), supports "Load More".

8 Monitoring and Operations

Corresponding menu: *Monitoring and Operations*

This chapter covers three functions: *Monitoring Dashboard*, *Resource Monitoring*, and *Logs and Alerts*.

8.1 Monitoring Dashboard

Corresponding menu: *Monitoring and Operations → Monitoring Dashboard*

Cluster-wide metrics monitoring dashboard, displaying metric trends in chart form by dimension.

- **Time Range:** Top time selector, default shows the last 1 hour, customizable (auto-selects minute/hour/day granularity).
- **Dimension Tabs:** Tabs are dynamically generated by backend configuration (e.g., cluster, node, client dimensions). Some dimensions require selecting a variable (dropdown filter) first to display corresponding charts.
- Empty state shown when no configuration; skeleton screen shown during loading.

The specific dimensions and charts of the monitoring dashboard are determined by the cluster monitoring configuration. The actual interface display may vary.

8.2 Resource Monitoring

Corresponding menu: *Monitoring and Operations → Resource Monitoring*

Resource Monitoring is a container page with three tabs: **Topic Monitoring**, **Node Monitoring**, and **Slow Subscriptions**.

8.2.1 Topic Monitoring

Tab: *Resource Monitoring → Topic Monitoring*

Monitors message traffic metrics for specified topics.

List

Column	Description
Topic	Monitored topic
Incoming Messages	Number of messages flowing into the topic

Outgoing Messages	Number of messages flowing out of the topic
Dropped Messages	Number of dropped messages (displayed in red when greater than 0)
Actions	Stop Monitoring

Toolbar: Refresh, Add.

- **Add:** Popup "Add Monitoring Topic", enter Topic name to add monitoring. Note: MQTT supports a maximum of 100 Topic Metrics by default; it is recommended to only monitor critical business topics.
- **Stop Monitoring:** Removes monitoring for that topic.

8.2.2 Node Monitoring

Tab: Resource Monitoring → Node Monitoring

Displays the operational status of each cluster node.

Toolbar: Refresh.

List

Column	Description
Node	Node name
Status	Running (green) or abnormal status (red)
Version	Node version
Uptime	Time since started
Connections	Current connection count
Memory Usage	Memory utilization
Role	Node role
Actions	View Details

Node Details (Drawer, title "Node Details - {node name}") contains three tabs:

- **Node Details:** Displays node, status, role, version, system description, OTP version, uptime, connections, active connections, available/used processes, 1/5/15 minute load, max file descriptors, total/used memory, etc. in description list format.
- **Metrics:** Metric name / value.
- **Statistics:** Statistic name / value.

8.2.3 Slow Subscriptions

Tab: Resource Monitoring → Slow Subscriptions

Lists slow subscription records with long delivery times, and allows configuring the detection threshold.

Top Filtering: Search Client ID.

Toolbar

- **Clear All Records:** Clears all slow subscription records after confirmation.
- **Settings:** Opens slow subscription settings drawer.

List

Column	Description
Client ID	Client identifier
Topic	Subscribed topic
Node	Node where the record was generated
Latency (ms)	Delivery latency in milliseconds
Creation Time	Record time

Slow Subscription Settings (Drawer)

Field	Type	Required	Description
Enable Slow Subscription	Toggle	—	Whether to enable detection
Top K Count	Number	Yes	1~1000
Stat Type	Dropdown	Yes	whole / internal / response
Threshold	Text	Yes	e.g., 500ms, 5s, 1m
Expiry Interval	Text	Yes	e.g., 300s

When enabled, a slow subscription record will be generated when the message delivery time from Broker to subscriber exceeds the threshold.

8.3 Logs and Alerts

Corresponding menu: Monitoring and Operations → Logs and Alerts

Logs and Alerts is a container page with two tabs: **Log Trace** and **Alerts**.

8.3.1 Log Trace

Tab: Logs and Alerts → Log Trace

Creates and manages cluster trace tasks (trace logs by client, topic, or IP), views and downloads logs.

Top Filtering: Search task name.

Toolbar: Add.

List

Column	Description
Name	Task name
Type	Client / Topic / IP Address
Target	Trace target value
Start Time	Trace start time
End Time	Trace end time
Content Encoding	Default text
Status	Running (green) / Stopped / Pending (blue)
Actions	View Log / Stop (running) / Delete (not running)

Add Trace Task (Drawer)

Field	Type	Required	Description
Task Name	Text	Yes	Task name
Trace Type	Dropdown	Yes	Client / Topic / IP Address
Target Value	Text	Yes	Label changes by type (Client ID / Topic / IP Address)
Time Range	Date-time range	—	Default from now to 30 minutes later
Log Format	Dropdown	—	Text / JSON
Content Encoding	Dropdown	—	Text / Hex / Hidden

View Log (Drawer, title "Log Content - {name}"): Read-only text area displaying logs, supports **Copy**, **Download** (downloaded as .zip).

8.3.2 Alerts

Tab: Logs and Alerts → Alerts

Displays active and resolved alerts in the cluster.

Top Filtering: Search alert name.

Toolbar: Clear All Alerts (clears all alerts after confirmation).

List

Column	Description
Node	Node that triggered the alert
Alert Name	Alert name
Alert Info	Alert details (expandable)
Activation Time	Alert activation time
Status	Active (red) / Resolved

9 System Configuration

Corresponding menu: System Configuration

This chapter covers five functions: Authenticator Management, Authorization Source Management, Listeners, System Configuration, and Data Backup.

9.1 Authenticator Management

Corresponding menu: System Configuration → Authenticator Management

Manages the MQTT client authentication chain, supporting multiple authentication mechanisms and data sources. Authenticators can be sorted, enabled/disabled, and synced to the cluster.

9.1.1 Top Filtering

- **Authentication Method:** Password Based / JWT / SCRAM.
- **Data Source:** Dynamically changes with authentication method (Built-in Database, MySQL, PostgreSQL, Redis, HTTP, Static JWT, JWKS Endpoint, etc.).
- **Query** button.

9.1.2 List

Column	Description
Authenticator ID	Authenticator identifier
Authentication Method	Password Based / JWT / SCRAM
Data Source	Backend data source type
User Count	Number of users under this authenticator
Enabled	Enable/disable toggle
Order	Authentication chain matching order
Creation Time	Creation time
Actions	View / Edit / Move Up / Move Down / Delete

9.1.3 Add Authenticator (Three-step Wizard, Full Page)

Adding/editing an authenticator is a **full-page wizard**, not a drawer:

1. **Select Authentication Method:** Password Based (username/password), JWT (Token), SCRAM (challenge-response).
2. **Select Data Source:**
 - Password Based: Built-in Database, MySQL, PostgreSQL, Redis, HTTP
 - JWT: Static JWT, JWKS Endpoint
 - SCRAM: Built-in Database
3. **Fill Configuration** (varies by combination):

Password Based + Built-in Database: Account type (username/clientid), password encryption method (plain/md5/sha/sha256/sha512/bcrypt/pbkdf2), salting method (prefix/suffix/disable).

Password Based + MySQL/PostgreSQL: Server address, database, username, password, password encryption method, salting method, enable TLS, SQL.

Password Based + Redis: Deployment mode (single/sentinel/cluster), server address, Sentinel master name (for sentinel), database, password, password encryption method, salting method, enable TLS, command.

Password Based + HTTP: Request method (GET/POST), URL, request headers, enable TLS, request body (for POST).

JWT (Static): JWT from (password/username), encryption method (HMAC / public key), secret or public key, key Base64 encoded, disconnect after expiry, Payload validation.

JWT + JWKS Endpoint: JWT from, JWKS Endpoint, refresh interval, request headers, enable TLS, disconnect after expiry, Payload.

SCRAM + Built-in Database: Algorithm (sha256/sha512), Iteration Count (default 4096).

9.1.4 Other Operations

- **Enable/Disable:** Toggle switch in the list.
- **Move Up/Move Down:** Adjust authentication chain order (buttons disabled at boundaries).
- **Sync to MQTT:** Push authenticator configuration to cluster.
- **View:** Drawer displaying JSON configuration.
- **Certificate Files:** TLS-related fields support uploading .crt/.key/.pem/.txt files.

9.2 Authorization Source Management

Corresponding menu: System Configuration → Authorization Source Management

Manages MQTT authorization/ACL data sources, controlling access permissions through multiple backends. File type supports direct editing of ACL files.

9.2.1 Top Filtering

- **Authorization Source Type:** Built-in Database / File / HTTP / MySQL / PostgreSQL / Redis.
- **Query** button.

9.2.2 List

Column	Description
Authorization Source Type	Backend type
Enabled	Enable/disable toggle
Permission Rule Count	Number of rules under this source
Order	Matching order
Creation Time	Creation time
Actions	View / Edit / Manage acl.conf (File type) / Move Up / Move Down / Delete

9.2.3 Add Authorization Source (Two-step Wizard, Full Page)

1. Select **Authorization Source Type**: Built-in Database, File, HTTP, MySQL, PostgreSQL, Redis.
2. Fill Configuration (varies by type):
 - **Built-in Database**: Maximum rule count (default 100).
 - **File**: ACL rule content (supports uploading .conf/.txt).
 - **HTTP**: Request method (GET/POST), URL, request headers, enable TLS, request body (for POST).
 - **MySQL/PostgreSQL**: Server address, database, username, password, auto-reconnect, enable TLS, SQL.
 - **Redis**: Redis type (single/sentinel/cluster), server address, database, password, auto-reconnect, enable TLS, command.

9.2.4 Other Operations

- **Enable/Disable, Move Up/Move Down, Sync to MQTT, View** (JSON) same as authenticator.
- **Manage acl.conf** (File type only): Opens a drawer for direct editing of ACL file content.

*Tip: Specific ACL rules for built-in database authorization source are maintained in **Users and Permissions** → **Permission Management**.*

9.3 Listeners

*Corresponding menu: **System Configuration** → **Listeners***

Manages MQTT Broker network listeners, supporting TCP, SSL, WS, WSS protocols.

9.3.1 List

Column	Description
Listener ID	Composed of "type:name", e.g., <code>tcp:default</code>
Type	TCP / SSL / WS / WSS
Bind Address	Listen address and port
Enabled	Enable status
Running Status	Running status
Connections	Current connection count
Actions	View / Edit / Start / Stop / Restart / Delete

9.3.2 Add / Edit Listener

Basic Configuration (all types):

Field	Description
Listener Type	TCP / SSL / WS / WSS, locked after creation
Name	Combined with type to form Listener ID, locked after creation
Bind Address	e.g., <code>0.0.0.0:1883</code> or <code>:1883</code>
Acceptor Count	Number of Acceptors
Max Connections	Supports "Unlimited"
Mount Point	Mount point

Tabs by Type:

Type	Tabs
TCP	Proxy & Rate Limiting, TCP Options
SSL	Proxy & Rate Limiting, TCP Options, TLS Certificate, TLS Advanced
WS	Proxy & Rate Limiting, TCP Options, WebSocket, Compression
WSS	Proxy & Rate Limiting, TCP Options, TLS Certificate, TLS Advanced, WebSocket, Compression

Key points per tab:

- **Proxy & Rate Limiting:** Proxy protocol switch and timeout, listener max connection rate, single client max publish rate/traffic.
- **TCP Options:** ActiveN, Backlog, Buffer, High Watermark, Send Timeout, Keepalive, TCP_NODELAY, SO_REUSEADDR, etc.
- **TLS Certificate:** TLS Cert, TLS Key, CA Cert (all support file upload).
- **TLS Advanced:** TLS version, cipher suites, handshake parameters, OCSP Stapling, etc.
- **WebSocket:** Path, idle timeout, max frame size, MQTT piggyback mode, Origin check and CORS, proxy headers, sub-protocols, etc.
- **Compression:** Context takeover, window bits, memory level, compression strategy.

9.3.3 Other Operations

- **Start / Stop / Restart:** All require confirmation.
- **View:** Opens a read-only drawer, only provides "Close".

9.4 System Configuration

Corresponding menu: *System Configuration* → *System Configuration*

Manages various Broker system configurations in tab form. Each tab corresponds to a configuration section, supporting save, reset, and JSON preview.

9.4.1 Configuration Sections (Tabs)

Tab	Description	Key Configuration Items
Alarm (alarm)	Alert settings	Alert actions (log/publish), max history alert storage, alert validity period
Broker	Broker settings	Global session registry, session history retention time
Dashboard	Console settings	CORS support, Swagger support, Token expiration time, default password, HTTP/HTTPS listening
Log (log)	Log settings	Console/File log (enable, level, path, rotation, formatting), rate limit time window
Global Zone (global_zone)	MQTT global behavior	Keepalive, max packet size, session expiry, max QoS, Inflight, wildcard/shared subscription, persistent session, jitter detection, forced GC, etc.
System Topics (sys_topics)	System topic events	Connect/disconnect/subscribe/unsubscribe events, heartbeat interval, message interval

System Monitoring (sysmon)	System monitoring thresholds	Broker/OS/VM water level lines and check intervals
----------------------------	------------------------------	--

9.4.2 Operations

Top-right corner of each tab provides:

- **Save:** Saves the current section configuration (merged with original config before submission).
- **Reset:** Restores MQTT defaults after confirmation and reloads.
- **View Current Config JSON:** Read-only popup displaying the current configuration as JSON.

*Tip: After saving, the cluster will reload the relevant configuration, usually taking effect immediately. Some network-related configurations (such as listeners) may need a listener restart. **Reset will overwrite all custom configurations**, please proceed with caution.*

9.5 Data Backup

Corresponding menu: *System Configuration → Data Backup*

Manages MQTT Broker data backup files, supporting creation, import, upload, download, and deletion.

9.5.1 List

Column	Description
File Name	Backup file name
Node	Node where the file resides
Size	File size (B/KB/MB)
Creation Time	Creation time
Actions	Download / Delete

9.5.2 Operations

Toolbar

- **Create Backup:** Generates a new backup file on the cluster.
- **Import:** Opens "Import Backup" drawer, selects and imports from existing backup files.
- **Upload:** Uploads a backup file from local to the cluster.
- **Refresh:** Refreshes the list.

Row-level Operations

- **Download:** Downloads the backup file to local.
- **Delete:** Deletes the backup file (requires confirmation).

10 Frequently Asked Questions

Questions in this chapter are categorized by function. Page references use the actual left menu path.

10.1 I. Connection and Authentication

10.1.1 Q1: Client connection shows authentication failure. How to troubleshoot?

1. Confirm the username and password used by the client are correct.
2. Go to **System Configuration → Authenticator Management**, confirm that the built-in database authenticator or corresponding external authenticator is enabled.
3. Go to **Users and Permissions → User Management**, confirm the user exists and belongs to the correct authenticator.
4. Check **Monitoring and Operations → Logs and Alerts → Alerts** and node logs for authentication-related errors.

10.1.2 Q2: Why can the client still connect after changing the user password?

After modifying the user, you need to click "Sync to MQTT" in **Users and Permissions → User Management**, otherwise the new password will not take effect. If the user is already online, go to **Resource Management → Client Management** to manually disconnect and force the client to reconnect.

10.1.3 Q3: What is the difference between a super user and a regular user?

Super users bypass all ACL checks and have publish and subscribe permissions for all topics. Regular users need to explicitly configure ACL rules in **Users and Permissions → Permission Management** to access specified topics.

10.2 II. Topics and Subscriptions

10.2.1 Q4: Subscribed to a topic but not receiving messages. How to troubleshoot?

1. Confirm the client is successfully connected and the subscription relationship is established (**Resource Management → Client Management → Details → Subscription Management**).
2. Go to **Resource Management → Subscription Management**, confirm the subscribed Topic and QoS are correct.
3. Check **Users and Permissions → Permission Management**, confirm the user/client ID has `Subscribe` or `All` permission for the corresponding topic.
4. Check **Resource Management → Message Management → Topic Rewrite / Auto Subscribe**, confirm no accidental rewriting of subscription relationships.

5. Check **Monitoring and Operations** → **Resource Monitoring** → **Topic Monitoring**, confirm messages are flowing in.

10.2.2 Q5: What is the purpose of retained messages? How to clear them?

Retained messages are immediately received when a new subscriber subscribes, commonly used for status synchronization. Clear methods:

- Send an empty retained message to the topic.
- Manually delete in **Resource Management** → **Message Management** → **Retained Messages** page.

10.2.3 Q6: Will QoS 0 and QoS 1 subscribers receive the same message?

Yes. QoS is a negotiated result between the publisher and subscriber. Messages are delivered according to the subscriber's specified QoS level, not the publisher's specified QoS.

10.3 III. Authentication and Authorization

10.3.1 Q7: ACL rules are configured but still shows no permission. What to do?

1. In **Users and Permissions** → **Permission Management**, confirm the `built_in_database` authorization source is selected.
2. Confirm the rules have been clicked "Sync to MQTT".
3. Check the authorization source order in **System Configuration** → **Authorization Source Management** to ensure preceding authorization sources do not have conflicting rules.
4. In **Resource Management** → **Client Management** → **Details**, click "Clear Authorization Cache" to force refresh the cache.

10.3.2 Q8: How are multiple authorization sources matched?

Multiple authorization sources are matched sequentially according to their order in **System Configuration** → **Authorization Source Management**. Matching stops upon first success. Rules within the same authorization source are also matched in order. It is recommended to place more specific rules first.

10.4 IV. Monitoring and Operations

10.4.1 Q9: How to view the real-time operational status of the MQTT cluster?

Go to **Monitoring and Operations** → **Resource Monitoring** → **Node Monitoring** to view each node's status; go to **Monitoring and Operations** → **Monitoring Dashboard** to view overall cluster metric trends.

10.4.2 Q10: How are slow subscription records generated?

After enabling detection in **Monitoring and Operations** → **Resource Monitoring** → **Slow Subscriptions** → **Settings**, when the message delivery time from Broker to subscriber exceeds the set threshold, a slow subscription record is generated. Records can be viewed and thresholds adjusted on the same page.

10.4.3 Q11: Why can only 100 topics be added to Topic Monitoring?

The MQTT cluster has a limit on the number of Topic Metrics, with a default maximum of 100. It is recommended to only monitor critical business topics (**Monitoring and Operations** → **Resource Monitoring** → **Topic Monitoring**).

10.4.4 Q12: Where can I view log traces and alerts?

Go to **Monitoring and Operations** → **Logs and Alerts**: the **Log Trace** tab allows creating trace tasks by client/topic/IP and downloading logs; the **Alerts** tab displays active and resolved alerts in the cluster.

10.5 V. System Configuration

10.5.1 Q13: How long does it take for system configuration changes to take effect?

After saving in **System Configuration** → **System Configuration**, the cluster reloads the relevant configuration, usually taking effect immediately. Some network-related configurations (such as listener addresses) may require restarting the corresponding listener in **System Configuration** → **Listeners**.

10.5.2 Q14: What impact does resetting system configuration have?

Resetting restores the configuration to MQTT defaults, overwriting all custom configurations. Please confirm important configurations have been backed up in **System Configuration** → **Data Backup** before proceeding.

10.6 VI. Other

10.6.1 Q15: What is the relationship between MQTT and ADMQ MQTT mentioned in the documentation?

ADMQ MQTT (Open MQTT / EMQX) is the unified management module for MQTT clusters on the ADMQ Manager platform. In the documentation, the terms are used interchangeably based on context, both referring to the MQTT management capability within the platform.

UNIFIED SERVICE HOTLINE

4008-555-800

Kingdee Apusic Cloud Computing Co., Ltd. (referred to as “Kingdee Apusic”) was founded in 2000. Its predecessor was “Kingdee Middleware Company.” It is a basic software platform provider under Kingdee Group, a national standards-setting enterprise for cloud computing, and a core software enterprise in the national IT application innovation industry. Kingdee Apusic is an enterprise undertaking the National 863 Key R&D Program and the National Major Science and Technology Project for Core Electronic Components, High-end General-purpose Chips and Fundamental Software, and is also a basic platform provider for the national key projects of “Two Networks, One Website, Four Databases, and Twelve Golden Projects.” Its products are widely used in key industries such as government, military, finance, and energy, and it has cumulatively served more than 100,000 customers.



National standard setter for cloud computing
Basic software enterprise under Kingdee Group
Core enterprise for IT application innovation
Website: www.apusic.com

