

Alibaba Cloud MQTT

Access control

Issue: 20190916

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK.
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>switch {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 Grant permissions to RAM users.....	1
2 Permission policies.....	4

1 Grant permissions to RAM users

Message Queue for MQTT supports granting permissions to Resource Access Management (RAM) users at the topic level using an Alibaba Cloud account (primary account) to prevent security risks caused by exposing the AccessKey of your primary account. Only authorized RAM users are allowed to manage resources on the MQTT console and publish and subscribe to messages through SDKs and API operations.

**Note:**

Currently, Message Queue for MQTT does not support authorization across Alibaba Cloud accounts.

Scenarios

Company A purchases Message Queue for MQTT and the employees of Company A need to perform operations on the resources of this service, such as instances, topics, and groups. For example, different employees are responsible for different jobs, including creating resources, publishing messages, and subscribing to messages. Employees with different roles require different permissions.

The scenario is described in detail, as follows:

- For security and trust purposes, Company A wants to create RAM users for its employees, instead of directly giving them the AccessKey of the Alibaba Cloud account.
- A RAM user can only use resources under authorization. Resource usage and costs are not calculated separately for that RAM user account. All expenses are billed to the Alibaba Cloud account of Company A.
- Company A can revoke the permissions of RAM users at any time, or delete the RAM user accounts it creates at any time.

In this scenario, the Alibaba Cloud account of Company A can allow fine-grained separation of permissions on resources that need to be operated by employees.

Procedure

1. Create a RAM user by using the Alibaba Cloud account of Company A.

For more information, see [#unique_4](#).

2. (Optional) Create custom policies for the RAM user as needed.

For more information, see [#unique_5](#).

Currently, Message Queue for MQTT supports setting permissions at the instance, topic, and group level. For more information, see [#unique_6](#).

3. Grant permissions to the RAM user with the Alibaba Cloud account of Company A.

For more information, see [#unique_7](#).

Next steps

After creating RAM users with an Alibaba Cloud account (primary account), you can distribute the logon names and passwords of the RAM user accounts or AccessKey information to other employees. Other employees can log on to the console or call an API operation with a RAM user account through the following steps.

- Log on to the console

1. Open the [RAM user logon portal](#) in the browser.
2. On the RAM user logon page, enter the RAM user name and click Next, enter the RAM user password, and then click Log on.



Note:

The RAM user name is in the format of <\$ username >@<\$ AccountAli as > or <\$ username >@<\$ AccountAli as >. onalibun . com .<\$ AccountAli as > is the account alias. If no account alias is set, the value defaults to the ID of the Alibaba Cloud account (primary account).

3. On the RAM User Center page, click products with permissions to access the console.

- Call an API operation with the RAM user's AccessKey

Use the AccessKey ID and AccessKey Secret of the RAM user in the code.

More information

- [#unique_8](#)
- [#unique_9](#)
- [#unique_10](#)
- [#unique_5](#)
- [#unique_4](#)

- [#unique_7](#)

2 Permission policies

Alibaba Cloud offers Resource Access Management (RAM), which allows you to manage permissions for Message Queue for MQTT. With RAM, you can avoid sharing the key of your Alibaba Cloud account (the AccessKey that contains AccessKey ID and AccessKey Secret) with other users. Instead, you can grant them only the necessary permissions. This topic describes the permission policies of Message Queue for MQTT in RAM.

In RAM, a policy is a collection of permissions described by using [syntax structure](#). A policy can accurately describe the authorized resource sets, action sets, and authorization conditions. Message Queue for MQTT has the following two types of RAM policies:

- **System policies:** Policies that are created by Alibaba Cloud. You can use but not modify these policies. Version updates of the policies are maintained by Alibaba Cloud.
- **Custom policies:** Policies that you can create, update, and delete. You also maintain the version updates of these policies.

System policies

Message Queue for MQTT now provides three system policies by default.



Notice:

At present, Message Queue for MQTT does not support independent system policies. When you grant the following system permission policies to RAM users, they also apply to Message Queue in addition to Message Queue for MQTT.

Policy name	Description
AliyunMQFullAccess	The permission to manage Message Queue for MQTT. It is the equivalent of the permission that the primary account has. A RAM user granted with this permission can send and receive all messages and use all functions of the console.

Policy name	Description
AliyunMQPubOnlyAccess	This permission provides the publish permission of Message Queue for MQTT. A RAM user granted with this permission can use all resources of the primary account to send messages through SDKs.
AliyunMQSubOnlyAccess	This permission provides the subscribe permission to Message Queue for MQTT. A RAM user granted with this permission can use all resources of the primary account to subscribe to messages through SDKs.

Custom policies

With custom policies, you can grant fine-grained access to users.

Mapping between resources and actions in Message Queue for MQTT

In Message Queue for MQTT, instances, topics, and groups are different types of resources, and the permissions granted for these resources are actions. The naming formats of topics and groups vary depending on whether the instance has a namespace. You can check if an instance has a namespace on the Instance Details page in the MQTT console.

The following table lists mapping between resources and actions in Message Queue for MQTT.

Resource	Naming format (with namespace)	Naming format (no namespace)	Action name	Action description	Note
Instance	acs:mq:*:*:{mqttInstanceId}	acs:mq:*:*:{mqttInstanceId}	mq:OnsMqttInstanceBaseInfo	Query the basic information of a specified instance.	Before granting permissions to a RAM user for topics and groups, you must grant the "mq:OnsMqttInstanceBaseInfo" permission of the instance to which the topics and groups belong.
			mq:OnsMqttInstanceDelete	Delete an instance	None

Resource	Naming format (with namespace)	Naming format (no namespace)	Action name	Action description	Note
			mq: OnsMqttInstanceUpdate	Update instance information	None
			mq: OnsMqttInstanceBind	Bind an instance	If you need to bind a Message Queue instance , you must have the permissions to operate on the specified Message Queue for MQTT instance and the bound Message Queue instance . For the permission settings of the Message Queue instances, see its permission policies.
			mq: OnsMqttInstanceList	Obtain the list of instances	None
			mq: OnsMqttInstanceUpdateWarn	Update the alerting information of a specified instance	None

Resource	Naming format (with namespace)	Naming format (no namespace)	Action name	Action description	Note
Topic	acs:mq:*:*:{storeId}%{topic}	acs:mq:*:*:{topic}	mq:OnsMqttQueryClientByTopic	Query the clients that subscribed to a topic	Before granting permissions to a RAM user for topics and groups, you must grant the "mq:OnsMqttInstanceBaseInfo" permission of the instance to which the topics and groups belong.  Notice: - If it is an instance with independent namespace, the topic must use the ID of the bound Message Queue for MQTT instance as the prefix. - The <code>storeId</code> here is the ID of the Message Queue instance that is bound to the Message Queue for MQTT instance. You can find the ID of the Message Queue instance on the Instance Details page in the MQTT console.
			mq:OnsMqttQueryMsgTrend	Query statistics on sending and receiving messages by topic	
			mq:OnsMqttMessageSend	Test the function of sending messages in the MQTT console	

Resource	Naming format (with namespace)	Naming format (no namespace)	Action name	Action description	Note
Group ID	acs:mq:*:*:{mqttInstanceId}%{groupId}	acs:mq:*:*:{groupId}	mq:OnsMqttGroupIdCreate	Create a group ID	Before granting permissions to a RAM user for topics and groups, you must grant the "mq:OnsMqttInstanceBaseInfo" permission of the instance to which the topics and groups belong.  Notice: If it is an instance with independent namespace, the group ID must use the ID of the bound Message Queue for MQTT instance as the prefix.
			mq:OnsMqttGroupIdList	Obtain the list of group IDs	
			mq:OnsMqttQueryClientByClientId	Query MQTT client information by client ID	
			mq:OnsMqttQueryClientByGroupId	Query MQTT client information by group ID	
			mq:OnsMqttQueryHistoryOnline	Query historical online MQTT client information by group ID	
			mq:OnsMqttGroupIdDelete	Delete a group ID	
			mq:OnsMqttDeviceTrace	Query MQTT device traces	
			mq:OnsMqttQueryClientTrace	Query messages related to an MQTT client	

Examples of common policies

To directly copy the sample code, delete the comments ("//" and the text description that follows).

- Example 1: Grant permissions to query message statistics by a specific topic and query historical online connections by group ID in a specific instance.
- For instances with namespaces

```
{
  "Version ":" 1 ",
  "Statement ":[
    {
      // Grant permission s for an instance .
      Before granting permission s for topics and groups
      , you must grant permission for the correspond ing
      instance ( applicable to instances with namespaces )
      " Effect ":" Allow ",
    }
  ]
}
```



```

        " Action ":[
            " mq : OnsMqttIns tanceBaseI nfo "
        ],
        " Resource ":[
            " acs : mq :*:*:{ mqttInstan ceId }"
        ]
    },
    { // Grant the permission to query statistics by
      topic
        " Effect ":" Allow ",
        " Action ":[
            " mq : OnsMqttQue ryMsgTrans Trend "
        ],
        " Resource ":[
            " acs : mq :*:*:{ storeInsta nceId }%{ topic }"
        ]
    },
    { // Grant permission s for a group
        " Effect ":" Allow ",
        " Action ":[
            " mq : OnsMqttQue ryHistory0 nline "
        ],
        " Resource ":[
            " acs : mq :*:*:{ mqttInstan ceId }%{ groupId }"
        ]
    }
  ]
}

```

- For instances without namespaces

```

{
  " Version ": " 1 ",
  " Statement ": [
    { // Grant permission s for an instance . Before
      granting permission s for topics and groups ,
      grant permission s for the correspond ing instance (
      applicable to instances without namespaces )
        " Effect ": " Allow ",
        " Action ": [
            " mq : OnsMqttIns tanceBaseI nfo "
        ],
        " Resource ": [
            " acs : mq :*:*:{ mqttInstan ceId }"
        ]
    },
    { // Grant the permission to query
      statistics by topic
        " Effect ":" Allow ",
        " Action ":[
            " mq : OnsMqttQue ryMsgTrans Trend "
        ],
        " Resource ":[
            " acs : mq :*:*:{ topic }"
        ]
    },
    { // Grant permission for a group
        " Effect ":" Allow ",
        " Action ":[
            " mq : OnsMqttQue ryHistory0 nline "
        ],
        " Resource ":[
            " acs : mq :*:*:{ groupId }"
        ]
    }
  ]
}

```

```

    ]
  }
}

```

- **Example 2: Grant permission for an entire instance (only applicable to instances with namespaces)**

To grant the permission for the entire instance, which means the permission to operate on all the resources in the instance, set the policy as follows.

```

{
  // Only applicable to instances with namespaces
  "Version ": " 1 ",
  "Statement ": [
    {
      "Effect ": " Allow ",
      "Action ": [
        " mq :*"
      ],
      "Resource ": [
        " acs : mq :*:*:{ mqttInstan ceId }*" // Grant
        permission for the instance . Replace { mqttInstan ceId }
        with the ID of your instance .
      ]
    }
  ]
}

```

Next steps

- [#unique_13](#)

More information

- [#unique_8](#)
- [#unique_9](#)
- [#unique_10](#)
- [#unique_5](#)
- [#unique_4](#)
- [#unique_7](#)
- [#unique_14](#)