ALIBABA CLOUD

阿里云

消息队列 MQ
访问控制（权限管理）

文档版本：20220117

阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。

2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。

3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。

4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。

5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。

6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	危险 重置操作将丢失用户配置数据。
警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	警告 重启操作将导致业务中断，恢复业务时间约十分钟。
注意	用于警示信息、补充说明等，是用户必须了解的内容。	注意 权重设置为0，该服务器不会再接受新请求。
说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击**设置**> **网络**> **设置网络类型**。
粗体	表示按键、菜单、页面名称等UI元素。	在**结果确认**页面，单击**确定**。
`Courier字体`	命令或代码。	执行 `cd /d C:/window` 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	`bae log list --instanceid` *Instance_ID*
[] 或者 [a|b]	表示可选项，至多选择一个。	`ipconfig [-all|-t]`
{} 或者 {a|b}	表示必选项，至多选择一个。	`switch {active|stand}`

目录

1.RAM主子账号授权 05
2.通过RAM角色实现跨云账号授权 07
3.服务关联角色 12
4.权限策略和示例 15

1.RAM主子账号授权

消息队列RocketMQ版

支持云账户（主账号）给RAM用户（子账号）授予Topic资源级别的权限，避免因暴露阿里云账号（主账号）密钥造成的安全风险。仅限有权限的RAM用户在

消息队列RocketMQ版

的控制台上管理资源，以及通过SDK/API发布与订阅消息。

应用场景

企业A购买了

消息队列RocketMQ版

服务，企业A的员工需要操作这些服务所涉及的资源，例如实例、Topic或Group资源，有的员工负责创建资源，有的负责发布消息，还有的负责订阅消息。由于每个员工的工作职责不一样，需要的权限也不一样。

具体场景说明如下：

- 出于安全或信任的考虑，企业A不希望将云账号密钥直接透露给员工，而希望能给员工创建相应的用户账号。
- 用户账号只能在授权的前提下操作资源，不需要对用户账号单独计量计费，所有开销都计入企业A云账号名下。
- 企业A随时可以撤销用户账号的权限，也可以随时删除其创建的用户账号。

此种场景下，A的云账号可以将需要员工进行操作的资源进行细粒度的权限分隔。

操作步骤

1. 企业A云账号创建RAM用户。

   具体步骤参见创建RAM用户。

2. （可选）企业A云账号可根据需求为刚创建的RAM用户创建自定义的策略。

   具体步骤参见创建自定义权限策略。

   目前，

   消息队列RocketMQ版

   支持实例、Topic和Group粒度的权限设置。详情参见权限策略和示例。

3. 企业A云账号为RAM用户授权。

   具体步骤参见为RAM用户授权。

后续步骤

使用阿里云账号（主账号）创建好RAM用户后，即可将RAM用户的登录名称及密码或者AccessKey信息分发给其他用户。其他用户可以按照以下步骤使用RAM用户登录控制台或调用API。

- 登录控制台。
  i. 在浏览器中打开RAM用户登录入口。
  ii. 在**RAM用户登录**页面上，输入RAM用户登录名称，单击**下一步**，并输入RAM用户密码，然后单击**登录**。

> **说明** RAM用户登录名称的格式为 `<$username>@<$AccountAlias>` 或 `<$username>@<$AccountAlias>.onaliyun.com` 。 `<$AccountAlias>` 为账号别名，如果没有设置账号别名，则默认值为阿里云账号（主账号）的ID。

iii. 在阿里云控制台首页顶部，找到搜索文本框输入并单击**消息队列for Apache RocketMQ**，即可访问

消息队列RocketMQ版

的控制台。

- 使用RAM用户的AccessKey调用API。

  在代码中使用RAM用户的AccessKey ID和AccessKey Secret即可。

更多信息

- 通过RAM角色实现跨云账号授权
- 权限策略和示例
- 什么是RAM

2.通过RAM角色实现跨云账号授权

使用企业A的阿里云账号（主账号）创建RAM角色并为该角色授权，并将该角色赋予企业B，即可实现使用企业B的主账号或其RAM用户（子账号）访问企业A的阿里云资源的目的。

背景信息

企业A购买了

消息队列RocketMQ版

服务来开展业务，并希望将部分业务授权给企业B。

需求说明：

- A希望能专注于业务系统，仅作为资源Owner；而消息发布和订阅等任务委托或授权给企业B。
- 企业A希望当企业B的员工加入或离职时，无需做任何权限变更。企业B可以进一步将A的资源访问权限分配给B的RAM用户（员工或应用），并可以精细控制其员工或应用对资源的访问和操作权限。
- 企业A希望如果双方合同终止，企业A随时可以撤销对企业B的授权。

解决方案

企业A需要授予企业B的员工对

消息队列RocketMQ版

的资源进行操作。假设企业A和企业B分别有一个阿里云账号A和阿里云账号B，需要完成以下操作完成企业A和企业B的跨云账号授权及资源访问：

1. 步骤一：创建RAM角色并授权

   阿里云账号A创建一个RAM角色，并根据业务范围和需求为RAM角色授予对应的权限，并允许阿里云账号B下的RAM用户扮演该角色。

2. 步骤二：跨云账号访问资源

   RAM角色授权完成后，阿里云账号B下的RAM用户通过扮演RAM角色可获取该角色对应的权限。RAM用户可通过以下方式访问阿里云账号A的资源：

   - 通过SDK访问资源
   - 通过控制台访问资源
   - 通过API访问资源

步骤一：创建RAM角色并授权

1. 首先需要使用企业A的阿里云账号（主账号）登录RAM控制台并为企业B的云账号创建RAM角色。

   具体步骤，请参见创建可信实体为阿里云账号的RAM角色。

2. （可选）企业A为刚创建的RAM角色创建自定义策略。

   具体步骤，请参见创建自定义权限策略。

   目前，

   消息队列RocketMQ版

   支持实例、Topic和Group粒度的权限设置。更多信息，请参见权限策略和示例。

3. 新创建的角色没有任何权限，因此企业A必须为该角色添加权限。可添加系统权限策略或自定义权限策略。

具体步骤，请参见为RAM角色授权。

4. 使用企业B的阿里云账号（主账号）登录RAM控制台并创建RAM用户。

   具体步骤，请参见为企业B创建RAM用户。

5. 企业B为RAM用户添加AliyunSTSAssumeRoleAccess权限。

   具体步骤，请参见为RAM用户授权。

   企业B必须为其主账号下的RAM用户添加AliyunSTSAssumeRoleAccess权限，RAM用户才能扮演企业A创建的RAM角色。

步骤二：跨云账号访问资源

- **通过SDK访问资源**

  企业B的RAM用户可通过SDK访问企业A的

  消息队列RocketMQ版

  资源，完成消息收发功能。SDK访问有以下两种配置方式：

- **配置STS Token**：使用STS Token方式，您必须在SDK代码中提供RAM用户的AccessKey ID、AccessKey Secret和SecurityToken（临时安全令牌），但是SecurityToken有时效性需要不断更新。使用STS获取临时安全令牌的方法，请参见AssumeRole。

> **注意** STS方式只适用于
>
> 消息队列RocketMQ版
>
> 的Java SDK 1.7.8.Final及以上版本。

STS Token配置示例

- 初始化

  消息队列RocketMQ版

  的客户端时，您只需将获取到的AccessKey ID、AccessKey Secret和SecurityToken填入到以下属性中即可：

```
Properties properties = new Properties();
// STS的AccessKey ID。
properties.put(PropertyKeyConst.AccessKey, "STS.XXX");
// STS的AccessKey Secret。
properties.put(PropertyKeyConst.SecretKey, "XXX");
// STS的SecurityToken。
properties.put(PropertyKeyConst.SecurityToken, "XXX");
// 其他属性。
properties.put(PropertyKeyConst.NAMESRV_ADDR, "XXX");
......
Producer client = ONSFactory.createProducer(properties);
client.start();
```

- 当SecurityToken过期时，调用updateCredential方法动态更新。

```
Properties properties = new Properties();
// STS的AccessKey ID。
properties.put(PropertyKeyConst.AccessKey,"STS.XXX");
// STS的AccessKey Secret。
properties.put(PropertyKeyConst.SecretKey, "XXX");
// STS的SecurityToken。
properties.put(PropertyKeyConst.SecurityToken, "XXX");
client.updateCredential(properties);
```

- **配置ECS实例RAM角色**：使用ECS实例RAM角色的方式，您无需在SDK中配置RAM用户的AccessKey ID、AccessKey Secret和SecurityToken信息，只需要输入创建的RAM角色名称即可，提高了代码配置的便利性。但是您需要先将创建的RAM角色与应用程序所部署的ECS实例完成绑定，将RAM角色权限授予ECS实例，具体步骤，请参见为实例授予RAM角色。

  > **注意** ECS实例RAM角色方式只适用于
  >
  > 消息队列RocketMQ版
  >
  > 的Java SDK 1.8.7.3.Final及以上版本。

  ECS实例RAM角色配置示例

  ```
  Properties properties = new Properties();
  // 您创建的RAM角色的名称，并且已将该RAM角色授予ECS实例。
  properties.put(PropertyKeyConst.RAM_ROLE_NAME,"XXX");
  ```

- **通过控制台访问资源**

  企业B的RAM用户可按照以下步骤登录控制台访问企业A的

  消息队列RocketMQ版

  资源。

  i. 在浏览器中打开RAM用户登录入口。

  ii. 在**RAM用户登录**页面上，输入RAM用户登录名称，单击**下一步**，并输入RAM用户密码，然后单击**登录**。

  > **说明** RAM用户登录名称的格式为 `<$username>@<$AccountAlias>` 或 `<$username>@<$AccountAlias>.onaliyun.com` 。 `<$AccountAlias>` 为账号别名，如果没有设置账号别名，则默认值为阿里云账号（主账号）的ID。

  iii. 在阿里云控制台登录页面，将鼠标指针移到右上角头像上，并在浮层中单击**切换身份**。

  iv. 在**阿里云 - 角色切换**页面，输入企业A的**企业别名**、**默认域名**或**主账号UID**中的任意一种，以及**角色名**，然后单击**提交**。

  v. 对企业A的

  消息队列RocketMQ版

  资源进行操作。

- **通过API访问资源**

  企业B的RAM用户可通过调用

  消息队列RocketMQ版

  提供的API接口访问企业A的资源。调用API的方法，请参见API调用方式。

更多信息

- RAM主子账号授权
- 权限策略概览
- 什么是RAM
- 基本概念

- 创建自定义权限策略
- 创建RAM用户
- 为RAM用户授权
- 授予实例RAM角色

3.服务关联角色

本文介绍

消息队列Rocket MQ版

服务关联角色的背景信息、策略内容、注意事项和常见问题。

背景信息

服务关联角色是某个云服务在某些情况下，为了完成自身的某个功能，需要获取其他云服务的访问权限而提供的RAM角色。您在该云服务的控制台首次使用该功能时，系统会提示您完成服务关联角色的自动创建。更多关于服务关联角色的信息，请参见服务关联角色。

消息队列Rocket MQ版

提供服务关联角色AliyunServiceRoleForOns，通过扮演该RAM角色，

消息队列Rocket MQ版

可获取如下权限：

- 访问云监控的权限，以实现监控报警相关功能。
- 访问阿里云ARMS Prometheus的权限，以实现Dashboard相关功能。

策略内容

AliyunServiceRoleForOns

服务关联角色AliyunServiceRoleForOns被授予的权限策略AliyunServiceRolePolicyForOns的策略内容如下：

```
{
    "Version": "1",
    "Statement": [
        {
            "Action": [
                "cms:DescribeMetricRuleList",
                "cms:DescribeMetricList",
                "cms:DescribeMetricData"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "arms:OpenVCluster",
                "arms:ListDashboards"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": "ram:DeleteServiceLinkedRole",
            "Resource": "*",
            "Effect": "Allow",
            "Condition": {
                "StringEquals": {
                    "ram:ServiceName": "ons.aliyuncs.com"
                }
            }
        }
    ]
}
```

注意事项

如果您删除了自动创建的服务关联角色，该服务关联角色相关的功能由于权限不足将无法再被使用，请谨慎操作。如需重新创建该服务关联角色并为其授权，请参见创建可信实体为阿里云服务的RAM角色和为RAM角色授权。

删除服务关联角色的更多信息，请参见删除服务关联角色。

常见问题

为什么我的RAM用户无法自动创建消息队列RocketMQ版服务关联角色AliyunServiceRoleForOns?

如果阿里云账号已经创建了服务关联角色，RAM用户就会继承该阿里云账号的服务关联角色。如果没有继承，请登录RAM控制台为其添加以下权限策略。

```
{
    "Statement": [
        {
            "Action": [
                "ram:CreateServiceLinkedRole"
            ],
            "Resource": "acs:ram:*:阿里云账号ID:role/*",
            "Effect": "Allow",
            "Condition": {
              "StringEquals": {
                "ram:ServiceName":  "ons.aliyuncs.com"
                }
            }
        }
    ],
    "Version": "1"
}
```

说明 请将 `阿里云账号ID` 替换为您实际的阿里云账号ID。

如果您的RAM用户被授予该权限策略后，仍然无法自动创建服务关联角色，请为该RAM用户授予以下任一权限策略：

- AliyunMQFullAccess
- AliyunMQPubOnlyAccess
- AliyunMQSubOnlyAccess

以上权限策略的更多信息，请参见系统策略。

4.权限策略和示例

消息队列Rocket MQ版

的权限管理是通过阿里云的访问控制RAM（Resource Access Management）产品实现的。使用RAM可以让您避免与其他用户共享云账号密钥，即AccessKey（包含AccessKey ID和AccessKey Secret），按需为用户分配最小权限。本文介绍

消息队列Rocket MQ版

在RAM中的权限策略和示例。

背景信息

在RAM中，权限策略是用权限策略语法和结构描述的一组权限的集合，可以精确地描述被授权的Resource（资源集）、Action（操作集）以及授权条件。更多信息，请参见权限策略基本元素。

消息队列Rocket MQ版

有以下RAM的权限策略：

- 系统策略

  系统策略统一由阿里云创建，您只能使用不能修改，策略的版本更新由阿里云维护。

- 自定义策略

  自定义策略可由您自主创建、更新和删除，策略的版本更新由您自行维护。您需到RAM控制台编辑相应权限策略，再给相应用户授予该权限。具体的权限策略示例，请参见下文中的权限策略示例。

> **说明**
>
> 消息队列Rocket MQ版
>
> 提供的消息收发服务和管控服务的每次请求都有安全访问控制。

系统策略

消息队列Rocket MQ版

提供以下系统默认的权限策略。

权限策略名称	说明
AliyunMQFullAccess	消息队列Rocket MQ版 的管理权限，等同于阿里云账号的权限，被授予该权限的RAM用户具有所有消息收发权限且有控制台所有功能操作权限。
AliyunMQPubOnlyAccess	消息队列Rocket MQ版 的发布权限，被授予该权限的RAM用户具有使用阿里云账号所有资源通过SDK发送消息的权限。

权限策略名称	说明
AliyunMQSubOnlyAccess	消息队列RocketMQ版 的订阅权限，被授予该权限的RAM用户具有使用阿里云账号所有资源通过SDK订阅消息的权限。
AliyunMQReadOnlyAccess	消息队列RocketMQ版 的只读权限，被授予该权限的RAM用户仅有通过访问控制台或调用管控API读取资源信息的权限。

自定义策略

自定义权限策略（Policy）可以满足您更细粒度的授权需求。

在

消息队列RocketMQ版

中，实例、Topic和Group等各为不同的Resource，对这些Resource授予的操作即为Action。包含{groupId}和{topic}的Resource，命名格式因实例是否有命名空间而异。您可以登录

消息队列RocketMQ版

控制台的**实例详情**页面，根据**命名空间**字段判断实例是否有命名空间。

消息队列RocketMQ版

的Resource和Action的可选值和对应规则可分为

消息队列RocketMQ版

服务、

消息队列RocketMQ版

客户端、控制台和OpenAPI。其中，针对控制台的相关操作，按资源类型又可分为实例、Group、Topic和标签。

> **注意**
>
> - 如需访问
>
> 消息队列RocketMQ版
>
> 的资源以及OpenAPI，则需要有访问
>
> 消息队列RocketMQ版
>
> 实例的权限，对应的Action为 `mq:QueryInstanceBaseInfo` 。
> - {instanceId}、{topic}和{groupId}均需替换为您实际的资源信息。例如，{groupId}替换为GID_test。

消息队列RocketMQ版

服务开通权限

Resource	命名格式	Action	
		Action名称	说明
消息队列RocketMQ版服务	*	ons:OpenOnsService	开通消息队列RocketMQ版服务

消息队列RocketMQ版

客户端收发消息权限

> **说明** 授予某RAM用户Topic和Group的相关权限前，需先授予该用户Topic和Group所在实例的 `mq:QueryInstanceBaseInfo` 权限。

Resource	命名格式		Action	
	有命名空间	无命名空间	Action名称	说明
Group	acs:mq:*:*:{instanceId}%{groupId} 示例：acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%GID_test *	acs:mq:*:*:{groupId} 示例：acs:mq:*:*:GID_test	mq:SUB	订阅消息
Topic	acs:mq:*:*:{instanceId}%{topic} 示例：acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%Topic-test	acs:mq:*:*:{topic} 示例：acs:mq:*:*:Topic-test	mq:PUB	发布消息
			mq:SUB	订阅消息

消息队列RocketMQ版

控制台实例操作权限

> **说明** 授予某RAM用户实例的相关操作权限前，需授予该用户实例的 `mq:QueryInstanceBaseInfo` 权限。

Resource	命名格式	Action	
		Action名称	说明
实例	acs:mq:*:*:*	mq:CreateInstance	创建实例
	acs:mq:*:*:{instanceId} 示例：acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k	mq:QueryInstanceBaseInfo	查询实例基本信息
		mq:UpdateInstance	更新实例
		mq:DeleteInstance	删除实例（慎用）

消息队列Rocket MQ版

控制台Group操作权限

> **说明** 授予某RAM用户Topic和Group的相关权限前，需先授予该用户Topic和Group所在实例的 `mq:QueryInstanceBaseInfo` 权限。

Resource	命名格式		Action	
	有命名空间	无命名空间	Action名称	说明
Group	acs:mq:*:*:{instanceId} 示例：acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k		mq:CreateGroup	创建Group ID
	acs:mq:*:*:{instanceId}%{groupId} 示例：acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%GID_test	acs:mq:*:*:{groupId} 示例：acs:mq:*:*:GID_test	mq:DeleteGroup	删除Group ID（慎用）
			mq:QueryGroupSubDetail	查询Group ID订阅的Topic
			mq:UpdateGroupConsumer	配置Group ID对应的消费集群的消息读写权限
			mq:QueryConsumerAccumulate	查询Group ID下的消息堆积数据
			mq:QueryConsumerStatus	查询Group ID的详细状态数据
			mq:QueryConsumerConnection	查询Group ID下客户端的连接信息

Resource	命名格式		Action	
	有命名空间	无命名空间	Action名称	说明
			mq:QueryTrendGroupOutputTps	查询Group ID下消息消费的统计数据
			mq:ResendDLQMessage	重发死信消息
			mq:QueryDLQMessage	查询死信消息

消息队列RocketMQ版

控制台Topic操作权限

> **说明** 授予某RAM用户Topic和Group的相关权限前，需先授予该用户Topic和Group所在实例的 `mq:QueryInstanceBaseInfo` 权限。

Resource	命名格式		Action	
	有命名空间	无命名空间	Action名称	说明
Topic	acs:mq:*:*:{instanceId}%{topic} 示例：acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%Topic-test	acs:mq:*:*:{topic} 示例：acs:mq:*:*:Topic-test	mq:CreateTopic	创建Topic
			mq:DeleteTopic	删除Topic（慎用）
			mq:UpdateTopic	更新Topic
			mq:QueryTopicStatus	查询Topic的消息总量和最近更新时间
			mq:QueryTopicSubDetail	查看订阅Topic的Group ID
			mq:ResetConsumerOffset	重置Group ID在指定Topic中的消费位点
			mq:QueryConsumerTimeSpan	查询Group ID订阅的Topic可重置的时间范围
			mq:QueryMessageTrace	查询消息的消费状态
			mq:QueryMessage	查询消息的详细信息
			mq:QueryDLQMessage	查询死信消息

Resource	命名格式		Action	
	有命名空间	无命名空间	Action名称	说明
			mq:QueryTrendTopicInputTps	查询Topic写入消息的统计数据
			mq:QueryTrace	获取查询消息轨迹的任务ID。获取任务ID后调用OnsTraceGetResult接口传入任务ID即可收到消息轨迹的查询结果。调用OnsTraceGetResult接口不需要获取授权。

消息队列RocketMQ版

控制台标签操作权限

> **说明** 授予某RAM用户标签的相关权限前，需先授予该用户标签资源所属实例的 `mq:QueryInstanceBaseInfo` 权限。

Resource	命名格式	Action	
		Action名称	说明
标签	acs:mq:*:*:*	mq:TagResources	为资源绑定标签
		mq:ListTagResources	查询标签
		mq:UntagResources	解绑并删除标签（慎用）

OpenAPI权限

消息队列RocketMQ版

提供的OpenAPI及其授权操作如下表所示。

> **说明** 授予某RAM用户API的操作权限前，需先授予该用户API调用的资源所属实例的 `mq:QueryInstanceBaseInfo` 权限，资源的命名格式为 `acs:mq:*:*:{instanceId}` 。

API	命名格式		Action
	有命名空间	无命名空间	
OnsRegionList	不涉及	不涉及	无需授权。
OpenOnsService	*		ons:OpenOnsService

<table>
<tr><th rowspan="2">API</th><th colspan="2">命名格式</th><th rowspan="2">Action</th></tr>
<tr><th>有命名空间</th><th>无命名空间</th></tr>
<tr><td>OnsInstanceDelete</td><td colspan="2">acs:mq:*:*:*</td><td>• mq:QueryInstanceBaseInfo
• mq:CreateInstance</td></tr>
<tr><td>OnsInstanceBaseInfo</td><td colspan="2" rowspan="3">acs:mq:*:*:{instanceId}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k</td><td>mq:QueryInstanceBaseInfo</td></tr>
<tr><td>OnsInstanceDelete</td><td>• mq:QueryInstanceBaseInfo
• mq:DeleteInstance</td></tr>
<tr><td>OnsInstanceUpdate</td><td>• mq:QueryInstanceBaseInfo
• mq:UpdateInstance</td></tr>
<tr><td>OnsInstanceInServiceList</td><td>acs:mq:*:*:{instanceId}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k</td><td>不涉及</td><td>mq:QueryInstanceBaseInfo

说明
• 若API访问资源所属的实例有命名空间，则RAM用户调用接口时必须先授予实例的 `mq:QueryInstanceBaseInfo` 权限，否则调用该接口查询不到任何信息。
• 若实例无命名空间，则RAM用户调用该接口无需授予任何权限。</td></tr>
</table>

<table>
<tr><th rowspan="2">API</th><th colspan="2">命名格式</th><th rowspan="2">Action</th></tr>
<tr><th>有命名空间</th><th>无命名空间</th></tr>
<tr><td>OnsTopicCreate</td><td rowspan="5">acs:mq:*:*:{instanceId}%{topic}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%Topic-test</td><td rowspan="5">acs:mq:*:*:{topic}
示例：
acs:mq:*:*:Topic-test</td><td>• mq:QueryInstanceBaseInfo
• mq:CreateTopic</td></tr>
<tr><td>OnsTopicDelete</td><td>• mq:QueryInstanceBaseInfo
• mq:DeleteTopic</td></tr>
<tr><td>OnsTopicStatus</td><td>• mq:QueryInstanceBaseInfo
• mq:QueryTopicStatus</td></tr>
<tr><td>OnsTopicUpdate</td><td>• mq:QueryInstanceBaseInfo
• mq:UpdateTopic</td></tr>
<tr><td>OnsTopicSubDetail</td><td>• mq:QueryInstanceBaseInfo
• mq:QueryTopicSubDetail</td></tr>
<tr><td>OnsTopicList</td><td colspan="2">acs:mq:*:*:{instanceId}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k</td><td>mq:QueryInstanceBaseInfo
说明 RAM用户调用该接口时，仅返回有对应发布和订阅权限的Topic信息。</td></tr>
<tr><td>OnsGroupCreate</td><td colspan="2">acs:mq:*:*:{instanceId}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k</td><td>• mq:QueryInstanceBaseInfo
• mq:CreateGroup</td></tr>
<tr><td>OnsGroupDelete</td><td rowspan="2">acs:mq:*:*:</td><td rowspan="2"></td><td>• mq:QueryInstanceBaseInfo
• mq:DeleteGroup</td></tr>
<tr><td></td><td></td></tr>
</table>

API	有命名空间 命名格式 acs:mq:*:*:{instanceId}%{groupId} 示例： acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%GID_test	无命名空间 acs:mq:*:*:{groupId} 示例： acs:mq:*:*:GID_test	Action
OnsGroupSubDetail			• mq:QueryInstanceBaseInfo • mq:QueryGroupSubDetail
OnsGroupConsumerUpdate			• mq:QueryInstanceBaseInfo • mq:UpdateGroupConsumer
OnsGroupList	acs:mq:*:*:{instanceId} 示例： acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k		mq:QueryInstanceBaseInfo 说明 RAM用户调用该接口时，仅返回有对应发布和订阅权限的Group信息。
TagResources	acs:mq:*:*:*		• mq:QueryInstanceBaseInfo • mq:TagResources
ListTagResources			• mq:QueryInstanceBaseInfo • mq:ListTagResources
UntagResources			• mq:QueryInstanceBaseInfo • mq:UntagResources
OnsConsumerAccumulate	acs:mq:*:*:{instanceId}%{groupId}	acs:mq:*:*:{groupId} 示例： acs:mq:*:*:GID_test	• mq:QueryInstanceBaseInfo • mq:QueryConsumerAccumulate
OnsConsumerStatus			• mq:QueryInstanceBaseInfo • mq:QueryConsumerStatus

API	有命名空间	无命名空间	Action
OnsConsumerGetConnection	示例： 命名格式 acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%GID_test		• mq:QueryInstanceBaseInfo • mq:QueryConsumerConnection
OnsConsumerResetOffset	acs:mq:*:*:{instanceId}%{topic} 示例： acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%Topic-test	acs:mq:*:*:{topic} 示例： acs:mq:*:*:Topic-test	• mq:QueryInstanceBaseInfo • mq:ResetConsumerOffset
OnsConsumerTimeSpan			• mq:QueryInstanceBaseInfo • mq:QueryConsumerTimeSpan
OnsMessagePush			• mq:QueryInstanceBaseInfo • mq:SUB
OnsMessageTrace	acs:mq:*:*:{instanceId}%{topic} 示例： acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%Topic-test	acs:mq:*:*:{topic} 示例： acs:mq:*:*:Topic-test	• mq:QueryInstanceBaseInfo • mq:QueryMessageTrace
OnsMessageGetByMsgId			• mq:QueryInstanceBaseInfo • mq:QueryMessage
OnsMessageGetByKey			• mq:QueryInstanceBaseInfo • mq:QueryMessage
OnsMessagePageQueryByTopic			• mq:QueryInstanceBaseInfo • mq:QueryMessage
OnsTrendTopicInputTps	acs:mq:*:*:{instanceId}%{topic} 示例： acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%Topic-test	acs:mq:*:*:{topic} 示例： acs:mq:*:*:Topic-test	• mq:QueryInstanceBaseInfo • mq:QueryTrendTopicInputTps

<table>
<tr><th rowspan="2">API</th><th colspan="2">命名格式</th><th rowspan="2">Action</th></tr>
<tr><th>有命名空间</th><th>无命名空间</th></tr>
<tr><td>OnsTrendGroupOutputTps</td><td>acs:mq:*:*:{instanceId}%{groupId}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%GID_test</td><td>acs:mq:*:*:{groupId}
示例：
acs:mq:*:*:GID_test</td><td>• mq:QueryInstanceBaseInfo
• mq:QueryTrendGroupOutputTps</td></tr>
<tr><td>OnsTraceGetResult</td><td colspan="2">acs:mq:*:*:{instanceId}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k</td><td>mq:QueryInstanceBaseInfo</td></tr>
<tr><td>OnsTraceQueryByMsgId</td><td rowspan="2">acs:mq:*:*:{instanceId}%{topic}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%Topic-test</td><td rowspan="2">acs:mq:*:*:{topic}
示例：
acs:mq:*:*:Topic-test</td><td>• mq:QueryInstanceBaseInfo
• mq:QueryTrace</td></tr>
<tr><td>OnsTraceQueryByMsgKey</td><td>• mq:QueryInstanceBaseInfo
• mq:QueryTrace</td></tr>
<tr><td>OnsDLQMessageGetById</td><td rowspan="3">acs:mq:*:*:{instanceId}%{groupId}
示例：
acs:mq:*:*:MQ_INST_138015630679****_BcZwWZ9k%GID_test</td><td rowspan="3">acs:mq:*:*:{groupId}
示例：
acs:mq:*:*:GID_test</td><td>• mq:QueryInstanceBaseInfo
• mq:ResendDLQMessage</td></tr>
<tr><td>OnsDLQMessagePageQueryByGroupId</td><td>• mq:QueryInstanceBaseInfo
• mq:QueryDLQMessage</td></tr>
<tr><td>OnsDLQMessageResendById</td><td>• mq:QueryInstanceBaseInfo
• mq:QueryDLQMessage</td></tr>
</table>

权限策略示例

注意 如需直接复制示例代码，使用时请删除注释内容，即“//”及以后的文字说明。

- 示例一：授予实例中某Topic和Group的权限

  授予使用实例下某Topic和Group消息发布和订阅的权限，请按以下示例设置。

- 适用于有命名空间的实例

```
{
        "Version":"1",
        "Statement":[
            {    // 授予实例的权限，授予Topic和Group的权限前须先授予相应实例的权限（适用于有命名空间的实例）。
                "Effect":"Allow",
                "Action":[
                    "mq:QueryInstanceBaseInfo"
                ],
                "Resource":[
                    "acs:mq:*:*:{instanceId}"
                ]
            },
            {   // 授予Topic的消息发布和订阅权限。
                "Effect":"Allow",
                "Action":[
                    "mq:PUB",
                    "mq:SUB"
                ],
                "Resource":[
                    "acs:mq:*:*:{instanceId}%{topic}"
                ]
            },
            {     // 授予Group的权限。
                "Effect":"Allow",
                "Action":[
                    "mq:SUB"
                ],
                "Resource":[
                    "acs:mq:*:*:{instanceId}%{groupId}"
                ]
            }
        ]
    }
```

- 适用于无命名空间的实例

```
{
    "Version":"1",
    "Statement":[
        {    // 授予实例的权限，授予Topic和Group的权限前须先授予相应实例的权限（适用于无命名空间的实例）。
            "Effect":"Allow",
            "Action":[
                "mq:QueryInstanceBaseInfo"
            ],
            "Resource":[
                "acs:mq:*:*:{instanceId}"
            ]
        },
        {   // 授予Topic的消息发布和订阅权限。
            "Effect":"Allow",
            "Action":[
                "mq:PUB",
                "mq:SUB"
            ],
            "Resource":[
                "acs:mq:*:*:{topic}"
            ]
        },
        {    // 授予Group的权限。
            "Effect":"Allow",
            "Action":[
                "mq:SUB"
            ],
            "Resource":[
                "acs:mq:*:*:{groupId}"
            ]
        }
    ]
}
```

- 示例二：授予用户某实例下的所有权限（只适用于有命名空间的实例）

  若要授予用户整个实例的权限，即该实例中所有资源的所有操作权限，请按以下示例设置。

```
{   // 仅适用于有命名空间的实例。
    "Version": "1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "mq:*"
            ],
            "Resource": [
                "acs:mq:*:*:{instanceId}*" // 授予用户该实例下的所有权限，{instanceId}用实例ID代替。
            ]
        }
    ]
}
```

更多信息

- 创建自定义权限策略
- 创建RAM用户
- 为RAM用户授权
- 通过RAM限制用户访问的IP地址