阿里云
微消息队列MQTT版

访问控制（权限管理）

文档版本：20200511

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. 阿里云文档中所有内容，包括但不限于图片、架构设计、页面布局、文字描述，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
	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。	 **禁止：** 重置操作将丢失用户配置数据。
	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。
	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。
	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。	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

微消息队列 MQTT 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 用户在微消息队列 MQTT 版的控制台上管理资源，以及通过 SDK/API 发布与订阅消息。

说明：
微消息队列 MQTT 版目前还不支持跨云账号授权。

应用场景

企业 A 购买了微消息队列 MQTT 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，比如有的负责创建资源，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#unique_5。

   目前，微消息队列 MQTT 版支持实例、Topic 和 Group 粒度的权限设置。详情参见权限策略。

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

  1. 在浏览器中打开 RAM 用户登录入口 。
  2. 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。

  3. 在**子用户用户中心**页面，单击有权限的产品，即可访问控制台。

- 使用 RAM 用户的 AccessKey 调用 API

  在代码中使用 RAM 用户的 AccessKeyId 和 AccessKeySecret 即可。

更多信息

#unique_8

2 权限策略

微消息队列 MQTT 版权限管理是通过阿里云的访问控制 RAM（Resource Access Management）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 AccessKeyId 和 AccessKeySecret），按需为用户分配最小权限。本文介绍微消息队列 MQTT 版在 RAM 中的权限策略。

在 RAM 中，权限策略是用语法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。微消息队列 MQTT 版有以下两类 RAM 的权限策略：

- 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：您可以自主创建、更新和删除，策略的版本更新由您自己维护。

系统策略

微消息队列 MQTT 版目前提供三种系统默认的权限策略。

注意：
微消息队列 MQTT 版目前不支持独立的系统权限策略。您在为 RAM 用户授予以下系统权限策略时，除了对微消息队列 MQTT 版生效外，还会对消息队列 RocketMQ 版生效。

权限策略名称	说明
AliyunMQFullAccess	管理微消息队列 MQTT 版的权限，等同于主账号的权限，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	微消息队列 MQTT 版的发布权限，被授予该权限的 RAM 用户具有使用主账号所有资源通过 SDK 发送消息的权限。
AliyunMQSubOnlyAccess	微消息队列 MQTT 版的订阅权限，被授予该权限的 RAM 用户具有使用主账号所有资源通过 SDK 订阅消息的权限。

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。

微消息队列 MQTT 版的 Resource 与 Action 的对应规则如下所述。

在微消息队列 MQTT 版中，实例、Topic 和 Group 各为一种 Resource，对这些 Resource 授予的权限即为 Action。Topic 和 Group 的 Resource 命名格式因实例是否有命名空间而异。您可在微消息队列 MQTT 版控制台的**实例详情**页面查看实例是否有命名空间。

微消息队列 MQTT 版的 Resource 和 Action 的可选值和对应规则可分为控制台、OpenAPI 和微消息队列 MQTT 版客户端三大类类。针对控制台资源的相关操作，按资源类型又可分为实例、Topic 和 Group 三类。

说明：
如需访问微消息队列 MQTT 版的资源以及 OpenAPI，则需有访问微消息队列 MQTT 版实例的权限，即 mq:MqttInstanceAccess 权限。

MQTT 客户端收发消息权限

消息收发权限涉及 Topic 和 Group ID 的 Resource 命名格式，这些命名格式因微消息队列 MQTT 版实例是否有命名空间而异：

- 有命名空间
  - Topic：acs:mq:*:*:{storeInstanceId}%{topic}
  - Group ID：acs:mq:*:*:{mqttInstanceId}%{groupid}

  注意：
  此处的 **storeInstanceid** 指您为微消息队列 MQTT 版实例绑定的持久化实例的 ID。您可在微消息队列 MQTT 版控制台的**实例详情**页面获取绑定的持久化实例的 ID。
- 无命名空间
  - Topic：acs:mq:*:*:{topic}
  - Group ID：acs:mq:*:*:{groupid}

Action 名称	Action 描述	备注
mq:PUB	消息发布	授予某 RAM 用户 Topic 的相关权限前，需授予该用户 Topic 所在实例的 mq:MqttInstanceAccess 权限。
mq:SUB	消息订阅	

控制台实例操作权限

不论您的微消息队列 MQTT 版实例是否有独立命名空间，Resource 命名格式都统一为 acs:mq:*:*:{mqttInstanceId}。涉及的 Action 及相关说明如下表所示。

Action 名称	Action 说明	备注
mq:MqttInstanceAccess	查询指定实例的基本信息	授予某 RAM 用户 Topic 和 Group 的相关权限前，需授予该用户 Topic 和 Group 所在实例的 mq:MqttInstanceAccess 权限。
mq:DeleteMqttInstance	删除实例	无
mq:UpdateMqttInstance	变更实例的信息	无
mq:BindMqttInstance	绑定实例	如果业务需要绑定实例，需要具备操作指定的微消息队列 MQTT 版实例以及绑定的持久化实例的权限，持久化实例的权限设置，请参见对应产品的权限控制策略。
mq:ListMqttInstance	获取实例列表	无
mq:UpdateMqttInstanceWarn	更新指定实例的报警信息	无

控制台 Topic 操作权限

Topic 的命名格式因微消息队列 MQTT 版实例是否有命名空间而异：

- 有命名空间：acs:mq:*:*:{storeInstanceId}%{topic}

  注意：
  此处的 **storeInstanceid** 指您为微消息队列 MQTT 版实例绑定的持久化实例的 ID。您可在微消息队列 MQTT 版控制台的**实例详情**页面获取绑定的持久化实例的 ID。

- 无命名空间：acs:mq:*:*:{topic}

Action 名称	Action 说明	备注
mq:QueryMqttClientByTopic	根据 Topic 查询订阅的客户端信息	授予某 RAM 用户 Topic 和 Group 的相关权限前，需授予该用户 Topic 和 Group 所在实例的 mq:MqttInstanceAccess 权限。
mq:QueryMqttMsgTransTrend	根据 Topic 查询消息的收发报表	
mq:SendMqttMessageByConsole	控制台发消息测试	

控制台 Group ID 操作权限

Group ID 的命名格式因微消息队列 MQTT 版实例是否有命名空间而异：

- 有命名空间：acs:mq:*:*:{mqttInstanceId}%{groupId}

  注意：
  此处如果是有独立命名空间的实例，则 Group ID 需要拼接微消息队列 MQTT 版实例 ID 作为前缀。

- 无命名空间：acs:mq:*:*:{groupId}

Action 名称	Action 说明	备注
mq:CreateMqttGroupId	创建 Group ID	授予某 RAM 用户 Topic 和 Group 的相关权限前，需授予该用户 Topic 和 Group 所在实例的 “mq:MqttInstanceAccess” 权限。
mq:ListMqttGroupId	获取 Group ID 列表	
mq:QueryMqttClientByClientId	根据 Client ID 查询设备信息	
mq:QueryMqttClientByGroupId	根据 Group ID 查询设备信息	
mq:QueryMqttHistoryOnline	根据 Group ID 查询历史在线设备信息	
mq:DeleteMqttGroupId	删除 Group ID	
mq:QueryMqttDeviceTrace	查询设备轨迹	
mq:QueryMqttDeviceTrace	查询设备的相关消息	

OpenAPI 权限

API	Resource 命名格式（实例无命名空间）	Resource 命名格式（实例有命名空间）	Action 描述
RevokeToken	• 实例：acs:mq:*:*:{mqttInstanceId} • Topic：acs:mq:*:*:{topic} • Group ID：acs:mq:*:*:{groupId}	• 实例：acs:mq:*:*:{mqttInstanceId} • Topic：acs:mq:*:*:{storeInstanceId}%{topic} • Group ID：acs:mq:*:*:{mqttInstanceId}%{groupId}	• mq:MqttInstanceAccess • mq:RevokeToken
QueryToken			• mq:MqttInstanceAccess • mq:QueryToken
ApplyToken			• mq:MqttInstanceAccess • mq:ApplyToken
CreateGroupId			• mq:MqttInstanceAccess • mq:CreateGroupId
DeleteGroupId			• mq:MqttInstanceAccess • mq:DeleteGroupId
ListGroupId			• mq:MqttInstanceAccess • mq:ListGroupId

说明：

API 的更多详情，请参见 #unique_10。

更多信息

- 权限策略示例
- #unique_8
- #unique_12
- 通过 RAM 限制用户的访问 IP 地址

3 权限策略示例

本文介绍在微消息队列 MQTT 版中常见的授权策略示例。

注意事项

在阅读本文前，建议您可先查看在访问控制 RAM 中支持的微消息队列 MQTT 版相关的权限策略。

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。示例中的 {mqttinstanceId}、{storeinstanceId}、{topic} 和 {groupId} 均需替换为您实际的资源信息。例如，{groupId} 替换为 GID_xxx。

注意：

此处的 **{storeInstanceid}** 指您为微消息队列 MQTT 版实例绑定的持久化实例的 ID。您可在微消息队列 MQTT 版控制台的**实例详情**页面获取绑定的持久化实例的 ID。

示例一：授予实例中某 Topic 和 Group 的权限

- 适用于有命名空间的实例

```
{
  "Version":"1",
  "Statement":[
    {   // 授予实例的授权，授予 Topic 和 Group 的权限前请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:MqttInstanceAccess"
      ],
      "Resource":[
        "acs:mq:*:*:{mqttInstanceId}"
      ]
    },
    {   // 授予 Topic 的消息发布和订阅权限
      "Effect":"Allow",
      "Action":[
        "mq:PUB",
        "mq:SUB"
      ],
      "Resource":[
        "acs:mq:*:*:{storeInstanceId}%{topic}"
      ]
    },
    {   // 授予 Group 的权限
      "Effect":"Allow",
      "Action":[
        "mq:SUB"
      ],
      "Resource":[
        "acs:mq:*:*:{mqttInstanceId}%{groupId}"
      ]
    }
  ]
```

```
 }
```

- 适用于无命名空间的实例

```
{
   "Version": "1",
   "Statement": [
      {   //授予实例的授权，授予 Topic 和 Group 的权限前请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:MqttInstanceAccess"
         ],
         "Resource": [
            "acs:mq:*:*:{mqttInstanceId}"
         ]
      },
      {   // 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：授权整个实例的权限（只适用于有命名空间的实例）

若要授予整个实例的权限，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:*:*:{mqttInstanceId}*" //授予该实例的权限，{mqttInstanceId} 用实例 ID 代
替
         ]
      }
   ]
}
```