

腾讯云消息队列 CMQ

用户与权限

产品文档



腾讯云

【版权声明】

©2013-2017 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】



及其它腾讯云服务相关的商标均为腾讯云计算（北京）有限责任公司及其关联公司所有。本文档涉及的第三方主体的商标，依法由权利人所有。

【服务声明】

本文档意在向客户介绍腾讯云全部或部分产品、服务的当时的整体概况，部分产品、服务的内容可能有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或模式的承诺或保证。

文档目录

文档声明.....	2
用户与权限.....	4
用户与权限概述	4
通过控制台设置权限.....	6
通过API设置权限	11

用户与权限

用户与权限概述

腾讯云的 CMQ 消息服务可通过 用户与权限 实现权限管理与控制，支持对指定 用户 或 用户组，通过策略管理 设置权限，粒度到<接口>或<接口集>。

本文将先指引您了解权限设置相关内容，并介绍 CMQ 的权限设置维度。

1. 设置策略

腾讯云用户与权限通过 策略

来控制用户或用户组的相关权限。所以您可以先建立成熟的策略，再将指定的用户或用户组关联到该策略。

- [策略的作用 >>](#)
- [了解策略类型 >>](#)
- [了解策略组成 >>](#)

2. 用户及用户组

做权限设置时，您需要确定要指定权限的用户或用户组；设置用户或用户组时，即可将其关联到相关策略。

用户

- [了解用户的作用 >>](#)
- [学习如何新建子用户 >>](#)
- [将用户关联到策略 >>](#)

用户组

- [了解用户组的作用 >>](#)
- [如何新建用户组 >>](#)
- [将用户组关联到策略 >>](#)

3. CMQ 权限维度

本小节将在近期补充。

4. CMQ 权限设置示例

[通过API设置权限 >>](#)

[通过控制台设置权限 >>](#)

通过控制台设置权限

本文以指定某用户拥有 CMQ 队列模型的消费消息及批量消费消息 写权限为例，演示如何设置 CMQ 权限。CMQ 的 CAM 权限管理能力，目前处于灰度阶段，您可联系我们的一线技术支持寻求帮助。

注意：

CAM 上线前，原协作者账户、子账户均可以登录 CMQ 控制台，并看到根账户的资源列表（即 list 接口权限，原先用的是根账户密钥）。接入 CAM

后，子账户默认是没有获取根账户资源列表权限的（登录控制台用的是子账户的密钥），需要根账户通过 CAM 授权，才有访问权限。

控制台操作指南如下：

一、创建用户

1. 访问[用户与权限控制台](#)，并点击【新建用户】。
2. 如果该用户需要登录腾讯云控制台或者调用云 API，则需要选择【允许该用户登录腾讯云】、并填写【QQ帐号】作为登录凭证。

注意：

子账户的 QQ 号，建议使用未在腾讯云注册的 QQ 号（子账户无需充值费用，CMQ 费用会在主账户扣除）

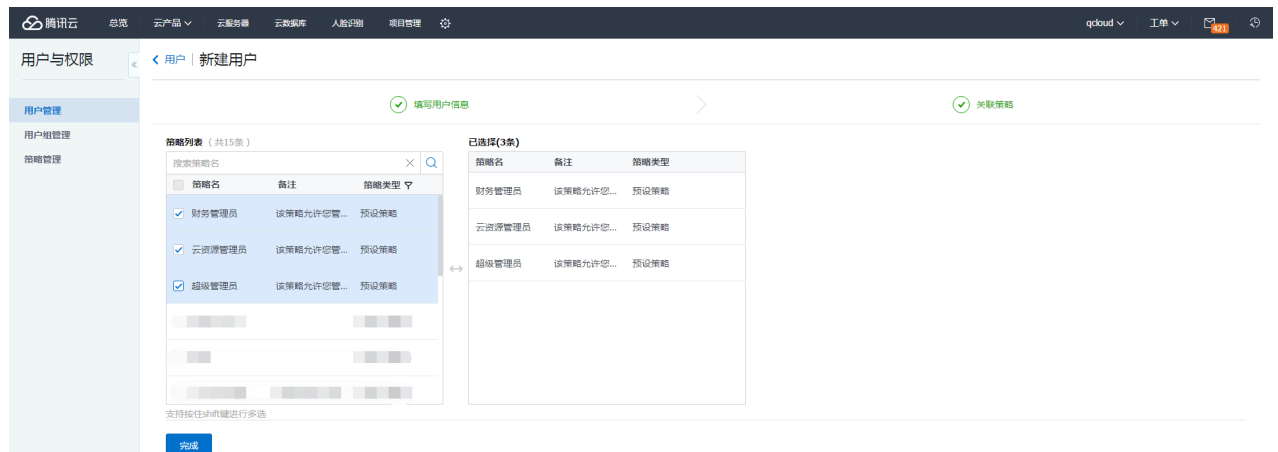
[免费申请 QQ号 >>](#)

The screenshot shows the 'Create User' interface in the Tencent Cloud IAM console. The form is titled '填写用户信息' (Fill in user information). It includes the following fields:

- 姓名 (必填) (Name, required): walletye
- 备注 (Nickname): 平台产品组员工
- 是否允许登录腾讯云 (必填) (Allow user to log in to Tencent Cloud, required): 是 (checked)
- 登录QQ号 (必填) (Login QQ number, required): 2732034714 (highlighted with a red box)
- 手机号码 (必填) (Mobile number, required): 15920550099
- 邮箱 (必填) (Email, required): 2732034714@qq.com

A '下一步' (Next step) button is located at the bottom of the form.

3. 为该用户关联策略（策略描述了权限，关联策略后用户即获得策略描述的权限）。



4. 在【用户管理】列表中，即可查看刚刚添加的子用户。



二、新建自定义策略

我们可以创建某自定义策略指定开启具体 API 接口的权限，如指定 CMQ Queue 的写权限（消费消息、批量消费消息）。

1. 配置服务类型，勾选【队列模型】。

[策略](#) | 新建自定义策略

1 配置服务类型

2 开启权限

请选择需要细化权限控制的业务，下一步可编辑该业务所允许执行的操作权限

策略名

选择服务类型 (共8条)

服务类型

☐ 用户与权限
 ☐ 互动直播
 ☐ 云直播
 ☐ 云点播
 ☒ 队列模型
 ☐ 主题模型

已选择(1条)

服务类型

队列模型

支持按住shift键进行多选

下一步

2. 指定具体 API 接口。

[返回](#) | Queue消费权限

基本信息
 [编辑](#)

策略

Queue消费权限

备注

-

策略类型

自定义策略

创建时间

2017-03-09 21:35:05

策略权限

关联用户/组

队列模型

+ 配置服务类型

功能	云API	对象数	操作
获取队列列表	ListQueue ListQueueDetail	该权限不需要关联对象	关联对象 ☐
创建队列	CreateQueue	该权限不需要关联对象	关联对象 ☐
批量删除消息	BatchDeleteMessage	该权限需要关联对象	关联对象 ☐
删除消息	DeleteMessage	该权限需要关联对象	关联对象 ☐
批量消费消息	BatchReceiveMessage	1个	关联对象 ☒
消费消息	ReceiveMessage	1个	关联对象 ☒

3. 指定资源对象。

示例中，我们指定该策略，将该根账户下存量的，新增的（包括该子账户创建的）的所有 Queue

作为关联对象。

注意：

子账户默认没有 CMQ 的 list 接口权限（即登录 CMQ

的控制台，无法在控制台看到具体的资源列表，可根据您的情况，考虑是否对子账户添加 list 权限）



三、关联子用户

将创建的策略关联到子用户，这样，该子用户将对该子用户内的所有 Queue 资源拥有消费消息、批量消费消息的权限。

[返回](#) | horacezhang_cmptest

用户信息 [编辑](#)

姓名 horacezhang_cmptest
备注 -
是否允许登录腾讯云 是
登录QQ号 [REDACTED]
联系手机 [REDACTED]
联系邮箱 [REDACTED]@tencent.com

已关联的策略

[已加入的用户组](#)

策略被关联后，即可获得该策略所描述的操作权限

关联策略

策略名	关联时间	操作
Queue消费权限	2017-03-09 21:35:28	解除

四、子用户登录

使用子账户登录后，若找不到对应的资源，请在控制台右上角，点击切换协作者开发商帐号。



通过API设置权限

前提：子用户的密钥

使用子账户的账户及密码登录，在控制台的【云产品】 -

[【云API密钥】](#)，找到子用户的密钥。密钥用于生成签名，认证通过后可访问相关腾讯云资源。

签名的作用：

- 验证请求用户身份：通过用户密钥来确认。
- 防止内容被篡改：通过对请求内容使用 hash 算法进行签名，通过签名的一致性来判定内容是否被篡改。
- 防止重放攻击：
签名内容中包括请求时间、签名时间及有效期，可避免过期请求重放。同时云服务也可以通过请求时间来拒绝过期请求。

API调用简单示例

1. 接口协议

编码类型：utf8

编码格式：json

传输方式：post

请求协议：http

调用规范示例如下：

```
{
  "version": 1,
  "componentName": "MC",
  "eventId": 123456,
  "interface": {
    "interfaceName": "接口名"
  },
  "para": {
```

接口对应参数

```
}  
}  
}
```

返回结果：各返回结果如果出错则 returnCode 不为0，returnMessage 内容为出错信息。

```
{  
  "version" : 1,  
  "eventId" : 123456,  
  "componentName" : "CONSOLE_LOGICAL_SERVER",  
  "returnValue" : 0,  
  "returnCode" : 0,  
  "returnMessage" : "OK",  
  "data" : {  
    "ownerUin":123,  
    "uin":124,  
    "ownerAppid":323  
  }  
}
```

注：后续对输入参数中的 interfaceName、para 和输出参数中的 data 进行说明。

2. 接口说明

有关用户与权限 CAM 的详细 API 接口介绍，可 [点击此处查阅 >>](#)

3. 调用示例

新增策略：CreateCamStrategy

策略示例：

设置某个子用户（Uin 为 3232）具有 list 账户下所有 queue 的权限，且对北京 region 的 horacetest1 有消费消息、批量删除消息的权限。

字段解析：

参数	描述	示例取值
strategyName	策略名称。	strategy1
strategyInfo	策略描述的内容。（注意，这里要传一个json字符串）	见示例代码
remark	策略的备注。	horace test
resource设置*	如果操作是需要关联资源的，它表示所有对象。如果操作是不需要关联资源的（比如 list 操作），它表示空对象。	*

示例代码：

```
{
  "strategyName": "strategy1",
  "strategyInfo": {
    "version": "2.0",
    "principal": {
      "qcs": [
        "qcs::cam::uin/1238423:uin/3232",
        "qcs::cam::uin/1238423:groupid/13"
      ]
    },
    "statement": [
      {
        "effect": "allow",
        "action": "name/cmqueue:ListQueue",
        "resource": "*"
      },
      {
        "effect": "allow",
        "action": "name/cmqueue:ReceiveMessage",
        "resource": "name/cmqueue:BatchDeleteMessage"
      }
    ]
  },
  "qcs::cmqueue:bj:uin/1238423:queueName/3232/horacetest1",
  "qcs::cmqueue:bj:uin/1238423:queueName/3232/horacetest1"
],
  "remark": "horace test"
}
```

子账户关联/移除策略：OperateCamStrategy

此接口可给用户或者用户组联/移除策略。

策略示例：将 UIN 为 123456 的用户关联到策略 ID 为 666 的策略。

字段解析：

参数	描述	示例取值
groupId	如果是关联用户，则groupId传-1； 如果是关联用户组，则groupId传具体组id。	-1
relateUin	如果是关联用户，则relateUin传具体用户uin；如果是关联用户组，则relateUin传-1。	123456
strategyId	需要关联的策略id。	666
actionType	值为“1”表示关联策略；值为“2”表示移除策略。	1

示例代码：

```
{  
  "groupId":-1,  
  "relateUin":123456,  
  "strategyId":666,  
  "actionType":1  
}
```

调用说明

注：该小节内容适用于各种业务的用户与权限管理，在设置 CMQ 业务时，请根据以下说明判断 CMQ 的相关取值。

1. principal 可以不填，后续通过关联策略接口去关联用户；

2. principal、action、resource，当只有一个元素时，可以不加[]。

3. 资源(resource)描述格式通常采用六段式，格式为"qcs:project:serviceType:region:account:resource"

- project可以用id/0, ""或者"id/"表示所有项目。授权时 project 为空表示 id/0，鉴权时project 为空表示可在任意项目中出现。默认为空。
- serviceType为cos、cdn、vpc等，"*"表示所有业务。不可以为空。
- region为地域，值为空，表示所有地域，其他地域分别是"gz", "st", "tj", "sh", "hk", "ca", "shjr", "bj"。默认为空。
- account，表示为"uin/{uin}"或者"uid/{uid}"。为空时，对于CDN业务和VPC业务等的资源，填充为"uin/{uin}"，对于COS业务的资源，填充化为"uid/{uid}"，"{uin}"或"{uid}"表示访问者的uin或者uid。默认为空。（还有一种特殊情况，“uin/-1”，一般是预设策略才出现，扩展表展开后会把-1变成开发商的uin，另外预设策略只允许子账户或角色的授权，所以可以直接用子账户或角色所属的根账户uin来替换-1。）
- resource由name/value构成。name表示业务对资源的定义。如cmq的为queueName和topicName。cos是用prefix描述，cdn用host描述等。""表示所有资源，归一化为"/"的形式。不可以为空。
- 用户、策略也是一种资源。CAM 根账户描述为 qcs::cam::uin/1238423:uin/1238423，CAM子账户描述为qcs::cam::uin/1238423:uin/3236671，匿名用户描述为qcs::cam::anonymous:anonymous。
- resource 为空时表示操作不需要关联对象。在系统中归一化为*。
- 对资源描述中uin或uid是否真的是该资源的拥有者，需要由业务来校验。强制要求业务在鉴权通过后必须校验，建议在授权时也进行校验。