

# 访问管理

# 操作指南

# 产品文档



腾讯云

**【版权声明】**

©2013-2018 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

## 操作指南

### CAM 概览

#### 身份管理

##### 用户管理

用户管理介绍

子用户

协作者

消息接收人

#### 用户组管理

##### 角色管理

角色概述

基本概念

创建角色

修改角色

使用角色

删除角色

为子账号赋予扮演角色策略

#### 策略管理

权限

策略

授权管理

授权操作指南

#### 策略语法

元素参考

语法结构

评估逻辑

资源描述方式

策略变量

生效条件

#### 联合帐号

企业微信

#### 子账号或协作者安全设置

# 操作指南

## CAM 概览

最近更新时间：2018-08-01 19:53:28

[访问管理控制台](#) 的概览页包括五大模块：[访问管理资源](#)、[登录链接](#)、[敏感操作](#)、[上次登录信息](#)、[安全指引](#)。下文将对各个模块进行介绍。

- 具有权限的用户登录控制台，可查看所有模块的信息，如下图示：

### 概览

<b>用户</b> 4 人 <a href="#">用户管理</a>	<b>用户组</b> 1 组 <a href="#">用户组管理</a>	<b>自定义策略</b> 8 个 <a href="#">策略管理</a>	<b>上次登录信息</b> 上次登录时间 2018-06-14 09:57:50 上次登录IP 14. [REDACTED] (深圳市)																
<b>登录链接</b> 子用户 <a href="https://cloud.tencent.com/login/subAccount/329">https://cloud.tencent.com/login/subAccount/329</a> <a href="#">🔗</a> 企业微信子用户 <a href="https://cloud.tencent.com/login/qywx/329">https://cloud.tencent.com/login/qywx/329</a> <a href="#">🔗</a>			<b>安全指引</b> <a href="#">了解更多</a> ▶ 主账号开启MFA <span>✅ 已完成</span> ▶ 对主账号开启保护 <span>⚠️ 未完成</span> ▶ 创建单独CAM用户 <span>✅ 已完成</span> ▶ 创建组并添加用户 <span>✅ 已完成</span> ▶ 管理授权策略 <span>✅ 已完成</span> ▶ 对子用户启用MFA <span>⚠️ 未完成</span> ▶ 对子用户开启保护 <span>✅ 已完成</span>																
<b>敏感操作</b> <a href="#">查看所有记录</a> <table><thead><tr><th>账号ID</th><th>操作者ID</th><th>敏感操作</th><th>操作时间</th></tr></thead><tbody><tr><td>329 [REDACTED]</td><td>329 [REDACTED]</td><td>绑定TOKEN</td><td>2018-06-12 15:...</td></tr><tr><td>329 [REDACTED]</td><td>329 [REDACTED]</td><td>绑定TOKEN</td><td>2018-06-12 15:...</td></tr><tr><td>329 [REDACTED]</td><td>329 [REDACTED]</td><td>绑定TOKEN</td><td>2018-06-12 15:...</td></tr></tbody></table> <p>共 6 项</p>				账号ID	操作者ID	敏感操作	操作时间	329 [REDACTED]	329 [REDACTED]	绑定TOKEN	2018-06-12 15:...	329 [REDACTED]	329 [REDACTED]	绑定TOKEN	2018-06-12 15:...	329 [REDACTED]	329 [REDACTED]	绑定TOKEN	2018-06-12 15:...
账号ID	操作者ID	敏感操作	操作时间																
329 [REDACTED]	329 [REDACTED]	绑定TOKEN	2018-06-12 15:...																
329 [REDACTED]	329 [REDACTED]	绑定TOKEN	2018-06-12 15:...																
329 [REDACTED]	329 [REDACTED]	绑定TOKEN	2018-06-12 15:...																

- 没有权限的用户登录控制台，只能查看 [登录链接](#) 和 [上次登录信息](#)，如下图示。

主账号可以通过 [QcloudCamSummaryAccess 策略](#) 授权给需要的子用户（或协作者），允许子用户（或协作

者) 查看控制台概览页的信息。

### 概览

#### 访问管理资源

该信息需要授权，请联系您的开发商为您添加权限 [查看权限授权指南](#)

#### 上次登录信息

上次登录时间 2018-06-14 12:55:46

上次登录IP 14. [redacted] (深圳市)

#### 登录链接

子用户 <https://cloud.tencent.com/login/subAccount/329>

企业微信子用户 <https://cloud.tencent.com/login/qywx/329/>

#### 敏感操作 ①

[查看所有记录](#)

账号ID	操作者ID	敏感操作	操作时间
该信息需要授权，请联系您的开发商为您添加权限 <a href="#">查看权限授权指南</a>			

共 0 项

#### 安全指引 [了解更多](#)

该信息需要授权，请联系您的开发商为您添加权限 [查看权限授权指南](#)

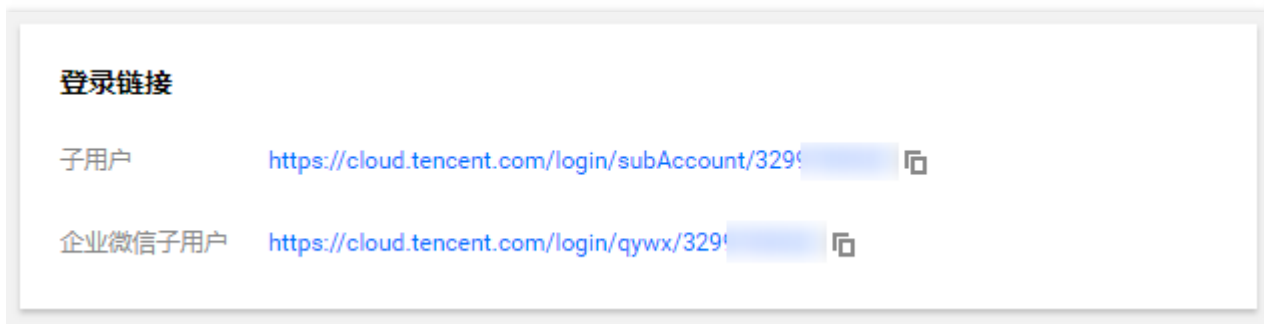
## 访问管理资源

访问管理资源模块展示当前主账号下所创建的用户、用户组和自定义策略数量。同时，用户可通过单击数量下方的按钮，进入对应的管理页面。



## 登录链接

登录链接模块展示了子用户和企业微信子用户的登录链接。主账号和子用户均可通过链接右侧的复制按钮复制链接。



- 子用户登录链接：适用于子用户。
- 企业微信子用户登录链接：适用于通过企业微信创建、关联的子用户。

## 敏感操作

敏感操作模块展示最近 3 天内（最高 50 条），主账号下所有账号的敏感操作记录，展示信息包括：账号 ID，操作者 ID，详细敏感操作和操作时间。

账号ID	操作者ID	敏感操作	操作时间
329[REDACTED]	329[REDACTED]	设置安全保护	2018-06-12 15:13:56

共 1 项

用户还可以通过单击【查看所有记录】，进入云审计控制台，查看更详细的敏感操作记录。

## 上次登录信息

上次登录信息模块展示当前账号的上次登录时间，上次登录 IP 以及地点。

上次登录信息	
上次登录时间	2018-06-14 12:05:05
上次登录IP	14.[REDACTED] (深圳市)

## 安全指引

安全指引模块为用户提供基础 CAM 功能学习和必要的安全操作指引，包括开启 MFA、开启账号保护、创建 CAM 用户和用户组等。

其中，**主账号开启 MFA** 和 **对主账号开启保护** 两项设置只有主账号具有操作权限；其余五项设置，获得授权的所有用户都可以进行操作。

**为了保障您的账户以及云上资产的安全，我们强烈建议您完成安全指引下的所有设置。**

各指引项分为两种状态：**未完成**和**已完成**。主账号用户登录控制台可以看到各指引项的状态，具有权限的非主账号用户无法查看状态。

具有权限的用户可通过单击各指引项左侧的三角符号查看对应的功能介绍和相应的设置入口。下图是主账号登录控制台后的安全指引模块示例。



## 主账号开启 MFA

MFA ( Multi-FactorAuthentication ，多因子认证 ) 是一种简单有效的安全认证方法。MFA 设备又叫动态口令卡或 Token 卡，能够在用户名和密码的基础上，为账号再增加一层保护。目前腾讯云提供两种 MFA 设备：硬件 MFA 设备和虚拟 MFA 设备。

主账号可以单击详细介绍下方的【开启主账号MFA】进入具体设置页面，详细步骤指引参考：

- [硬件 MFA 设备](#)
- [虚拟 MFA 设备](#)



## 对主账号开启保护

主账号可以设置开启登录保护和操作保护。

- 开启登录保护后，在登录腾讯云时需要通过 **MFA 验证** 完成身份验证，这样即使他人盗取您的密码，也无法登录您的账号，能够最大限度地保证您的账号以及账号下资产的安全。
- 开启操作保护后，在进行敏感操作前，需要先通过 **MFA 验证** 或 **手机号验证** 完成身份验证，以确保是您本人操作。

主账号可以单击详细介绍下方的【开启主账号保护】进入具体设置页面，详细步骤指引参考：

- [登录保护](#)
- [操作保护](#)

## 创建单独 CAM 用户

创建 CAM 用户，向他们授予所需的权限。腾讯云主账号可通过用户管理功能对具有不同职责的分类用户进行管理。用户类型包括协作者、消息接收人、子用户。

具有权限的用户可以单击详细介绍下方的【创建用户】进入具体设置页面，详细步骤指引参考：

- [子用户](#)
- [协作者](#)
- [消息接收人](#)

## 创建组并添加用户

创建用户组并且添加 CAM 用户，为该用户组关联适当的策略，以分配不同权限，能够帮助您批量管理、分配账号内的资源，提高工作效率。

具有权限的用户可以单击详细介绍下方的【创建组】进入具体设置页面，详细步骤指引参考：

- [用户组管理](#)

## 管理授权策略

CAM 支持两种类型的策略：预设策略和自定义策略。

- 预设策略是由腾讯云创建和管理的一些常见的权限集合，如超级管理权限和资源管理权限等，粒度比较粗。预设策略不可以编辑。
- 自定义策略是由用户自行创建的策略，允许作细粒度的权限划分。自定义策略允许用户编辑。

给用户组或用户分配权限，可以简化您对账户中 CAM 用户的权限管理和审核。

具有权限的用户可以单击详细介绍下方的【管理自定义策略】进入具体设置页面，详细步骤指引参考：

- [策略管理](#)

## 对子账号启用 MFA

对子账号启用多因子认证（MFA）将加强对您云上资产的安全保护。对 CAM 用户启用 MFA 后，CAM 用户在登录腾讯云或者在腾讯云进行敏感操作时，需要进行二次认证，帮助保护您的资产安全。MFA 的相关设置关系到云上资产安全，子用户或者协作者只能接受主账号或者是具有 CAM 管理权限的用户对这些安全属性的设置。

具有权限的用户可以单击详细介绍下方的【去开启子用户MFA】进入具体设置页面，相关文档参考：

- [MFA 设置指引](#) 的 [为子账号开启 MFA](#) 部分

## 对子账号开启保护

具有权限的用户可以对子账号开启登录保护和操作保护。

- 开启登录保护后，子用户在登录腾讯云时需要通过 **MFA 验证** 完成身份验证，这样即使子用户泄露或遗失密码，也无法登录您的账号，能够最大限度地保障您的资产安全。
- 开启操作保护后，在子用户进行敏感操作前，需要先通过 **MFA 验证** 或 **手机号验证** 完成身份验证，以保障您的资产安全。

对子用户（CAM 用户）开启登录保护和操作保护，有助于对您云上资产的安全保护。

具有权限的用户可以单击详细介绍下方的【去开启子用户保护】进入用户管理页面：

1. 单击需要开启保护的子用户名称，进入该用户的详情信息页面；
2. 单击用户详情信息页面内的【安全设置】；
3. 单击 **MFA设备** 右侧的【管理MFA】即可对选定子用户设置登录保护以及操作保护。

# 身份管理

## 用户管理

### 用户管理介绍

最近更新时间：2018-08-10 17:47:58

腾讯云主账号可通过用户管理功能对具有不同职责的分类用户进行管理。用户类型包括协作者、消息接收人、子用户。

用户类型	登录腾讯云控制台	使用腾讯云 API	策略授权	消息通知	准备条件
协作者	支持	支持	支持	支持	另一个腾讯云账号
消息接收人	不支持	不支持	不支持	支持	用于接收消息的手机号、邮箱
子用户	支持（可选）	支持（可选）	支持	支持	无

# 子用户

最近更新时间：2018-07-31 10:47:27

## 概述

子用户是由根账号创建的实体，有确定的身份 ID 和身份凭证，能够登录并独立设置控制台，且具有 API 访问权限。

## 操作指南

### 新建子用户

1. 登录腾讯云控制台，进入 [用户管理](#) 页面，单击【新建用户】>【子用户】，如下图所示：



2. 填写用户信息。在此过程中，可批量创建子用户，设置访问类型和控制台密码等，如下图所示：

1 填写用户信息 > 2 设定权限 > 3 完成

设置用户信息

用户名	备注	
sample_user	合理设置备注可以更快定位用户	删除

新增用户 (单次最多创建10个用户)

访问类型

- 编程访问  
启用SecretId和SecretKey，支持腾讯云API、SDK和其他开发工具访问
- 腾讯云管理控制台访问  
启用密码、使得用户可以登录到腾讯云管理控制台。

控制台密码

- 自动生成的密码
- 自定义密码

需要重置密码

- 用户必须在下次登录时重置密码

登录保护

- 不开启
- 软件MFA校验

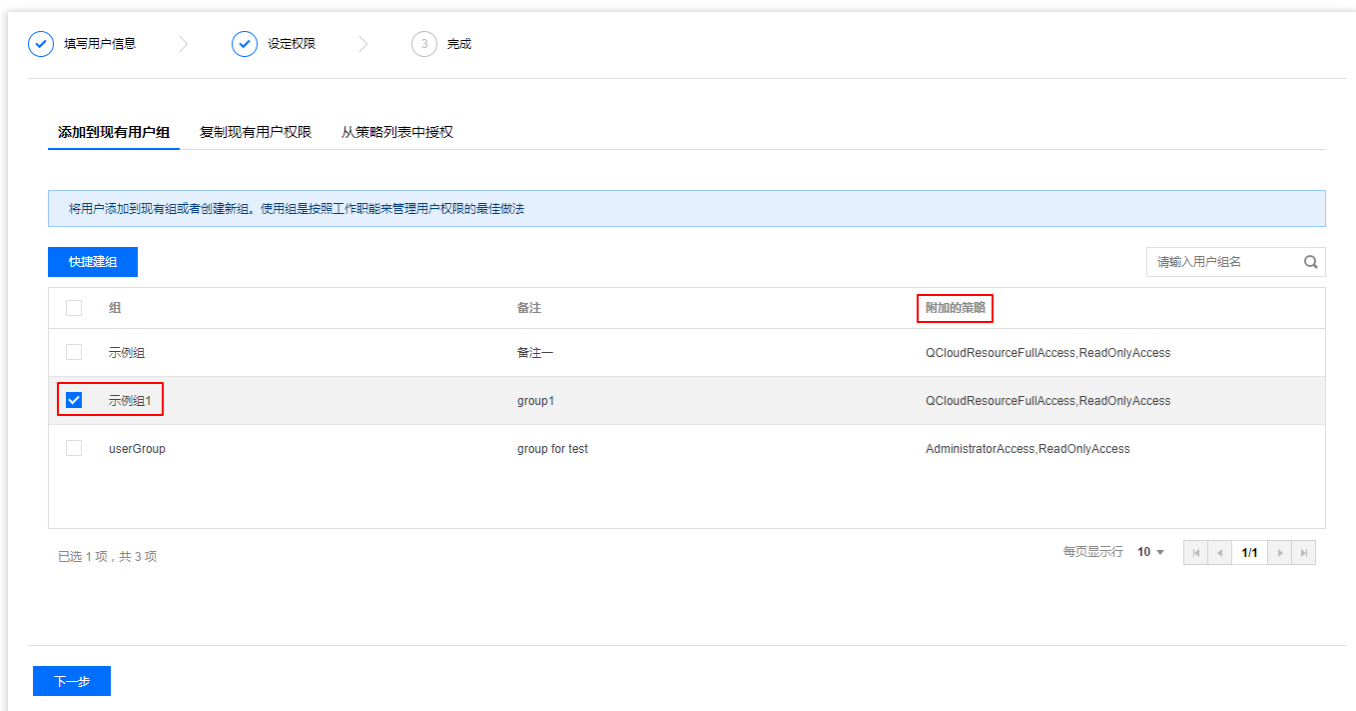
敏感操作保护

- 不开启
- 软件MFA校验

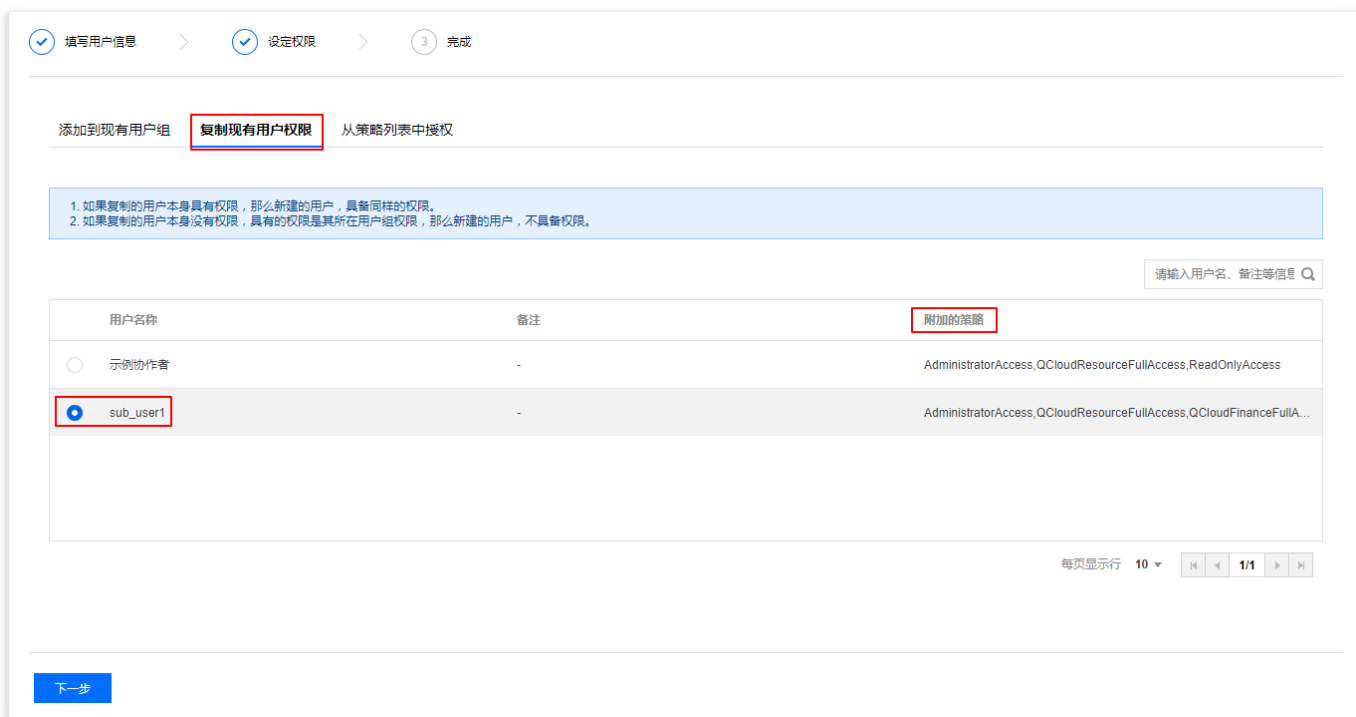
下一步

3. 设定权限。您可以通过以下三种方法为当前新建的子用户设定权限，策略描述了权限，关联策略后子用户即获得策略描述的权限。

- 把子用户添加到组是按工作职能来管理用户权限的最佳做法，您可以通过随组关联获得权限。将子用户添加到现有用户组或新建用户组，子用户可以随组关联到该组附加的策略。



- 通过复制现有用户的权限为子用户关联策略，单击【复制现有用户权限】，勾选需要复制的用户，子用户可以关联到被复制用户附加的策略。



- 通过从策略列表中授权。单击【从策略列表中授权】，勾选需要关联的策略。

✓ 填写用户信息 >
✓ 设定权限 >
3 完成

添加到现有用户组
复制现有用户权限
从策略列表中授权

从策略列表中授权

**策略列表** (共163条)

支持搜索策略名称/描述/备注

策略名	描述	策略...
<input checked="" type="checkbox"/> AdministratorAccess	该策略允许您管理...	预设策略
<input checked="" type="checkbox"/> ReadOnlyAccess	该策略允许您只读...	预设策略
<input checked="" type="checkbox"/> QCloudResourceFu...	该策略允许您管理...	预设策略
<input type="checkbox"/> QCloudFinanceFull...	该策略允许您管理...	预设策略
<input type="checkbox"/> QcloudAAIFullAccess	智能语音 ( AAI ) ...	预设策略
<input type="checkbox"/> QcloudAccessForIO...	物联网解决方案(I...	预设策略

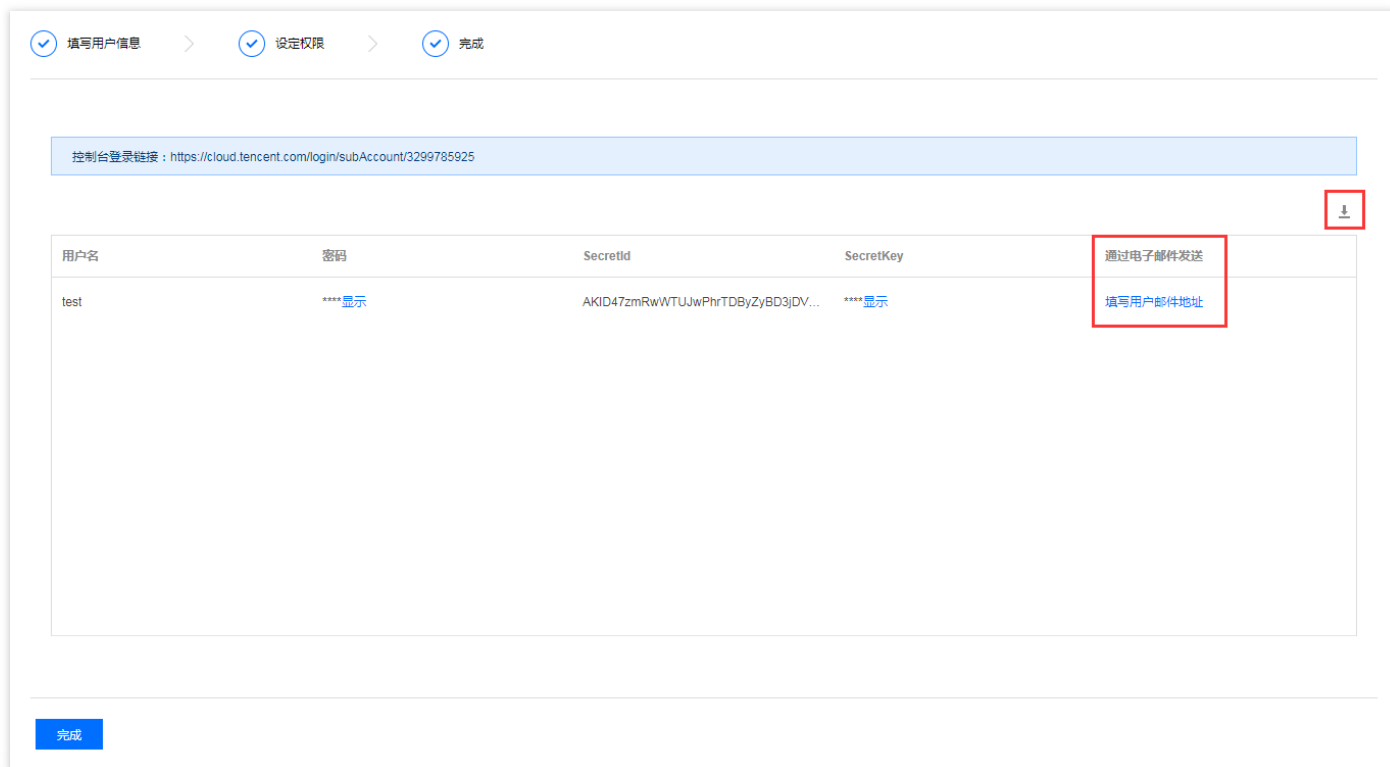
支持按住shift键进行多选

**已选择(3条)**

策略名	描述	策略类型
AdministratorAccess	该策略允许您管理...	预设策略 <span style="float: right;">✕</span>
ReadOnlyAccess	该策略允许您只读...	预设策略 <span style="float: right;">✕</span>
QCloudResourceFull...	该策略允许您管理...	预设策略 <span style="float: right;">✕</span>

下一步

4. 可通过电子邮件将完整信息发送至邮箱，或通过 excel 文件将部分信息保存至本地，如下图所示：

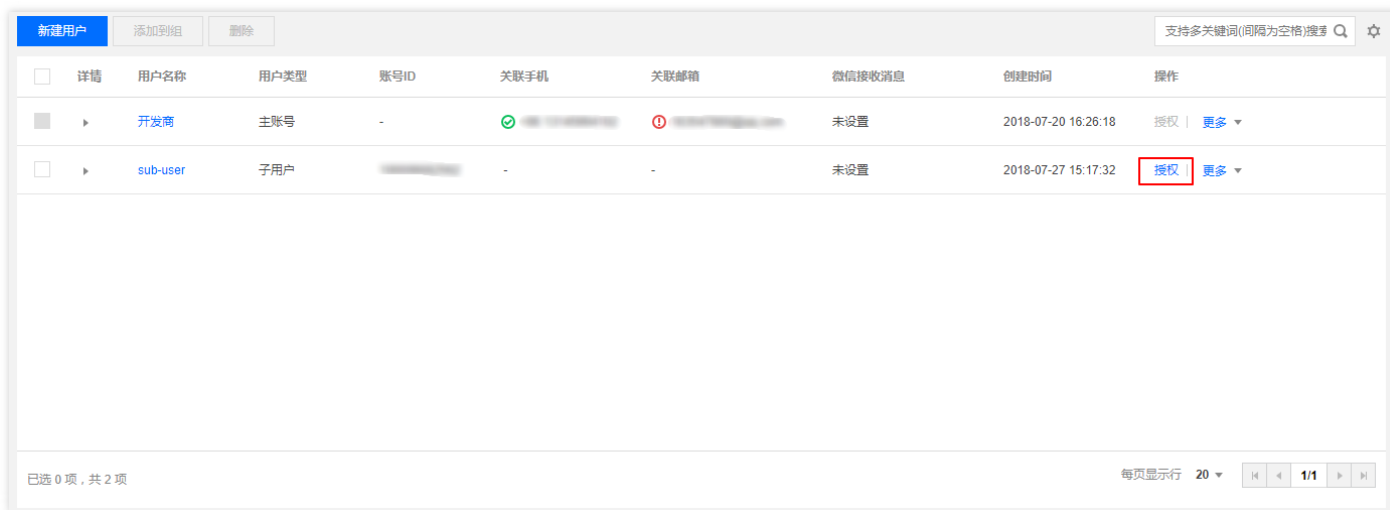


5. 单击【完成】，完成新建子用户操作。

## 为子用户授权关联策略

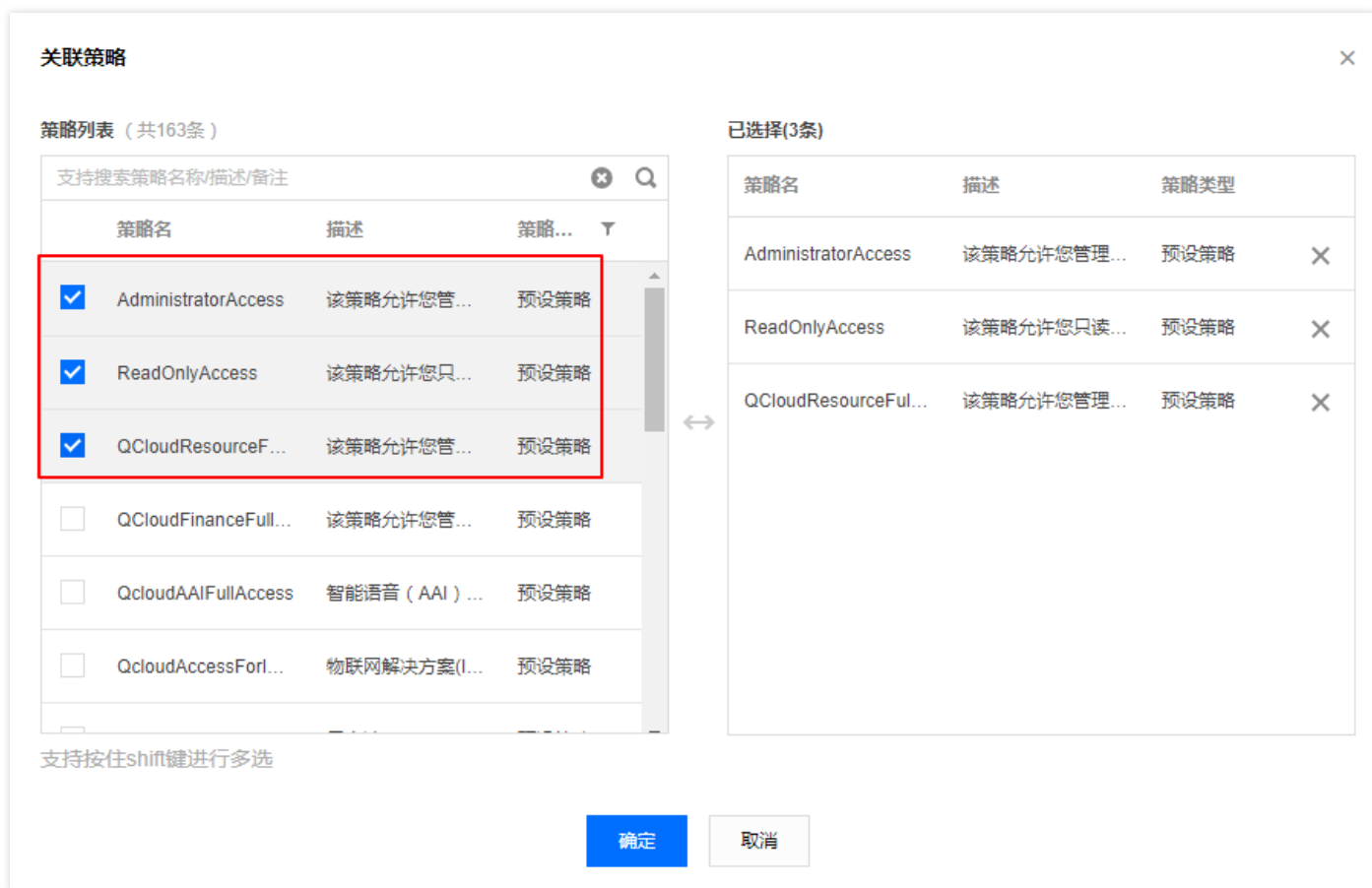
### 直接关联

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要授权关联策略的子用户，单击操作列的【授权】，如图所示：



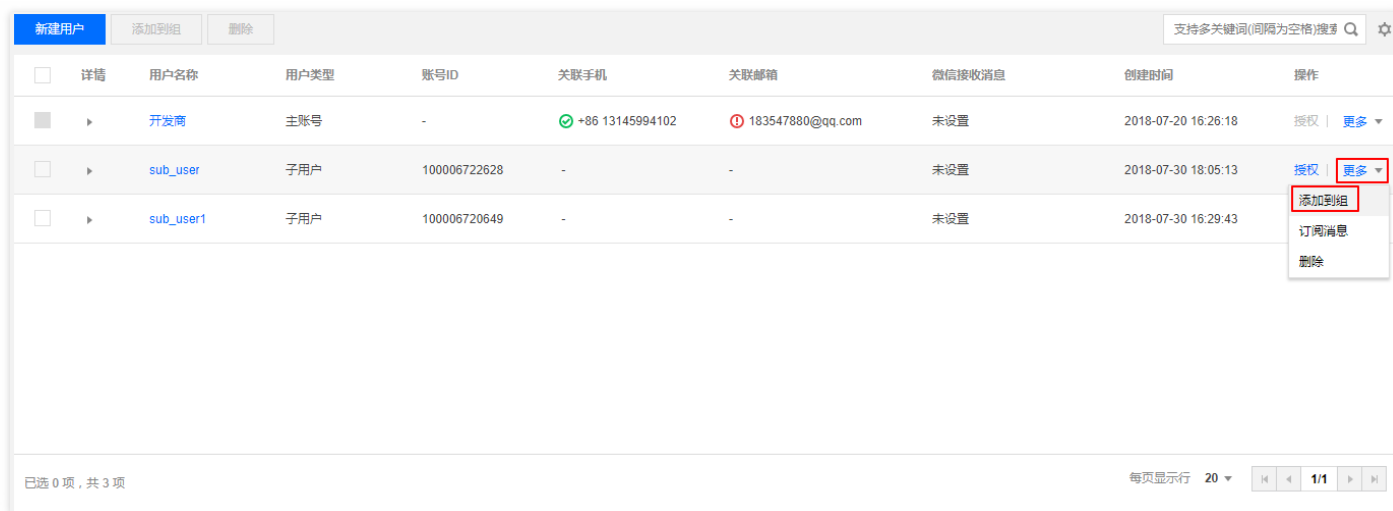


2. 勾选需要授权的策略，单击【确定】，完成为子用户授权关联策略操作。



### 随组关联

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要授权关联策略的子用户，单击操作列的【更多】>【添加到组】。

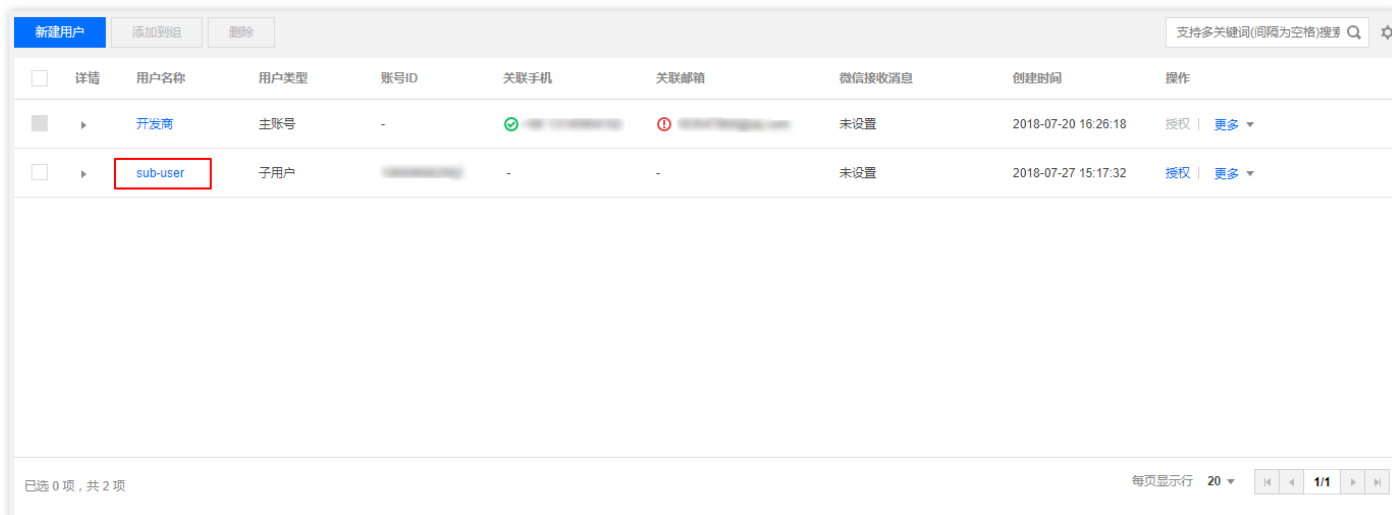


2. 勾选需要添加到的用户组，单击确定，完成通过添加到组进行随组关联策略操作。

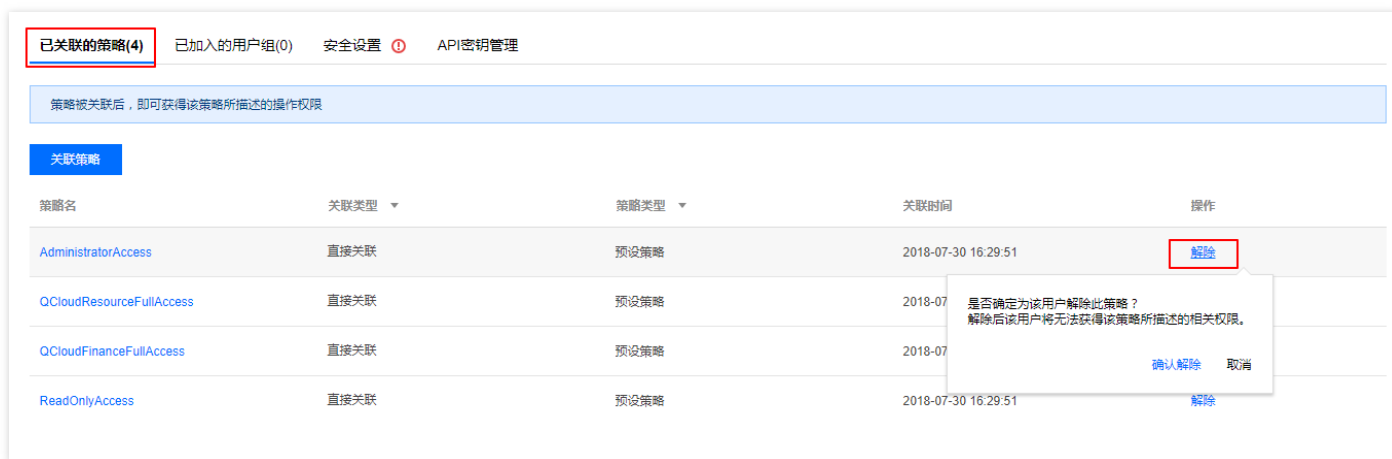
## 为子用户删除关联策略

### 直接解除

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要删除关联策略的子用户，单击子用户名称，进入子用户详情页。



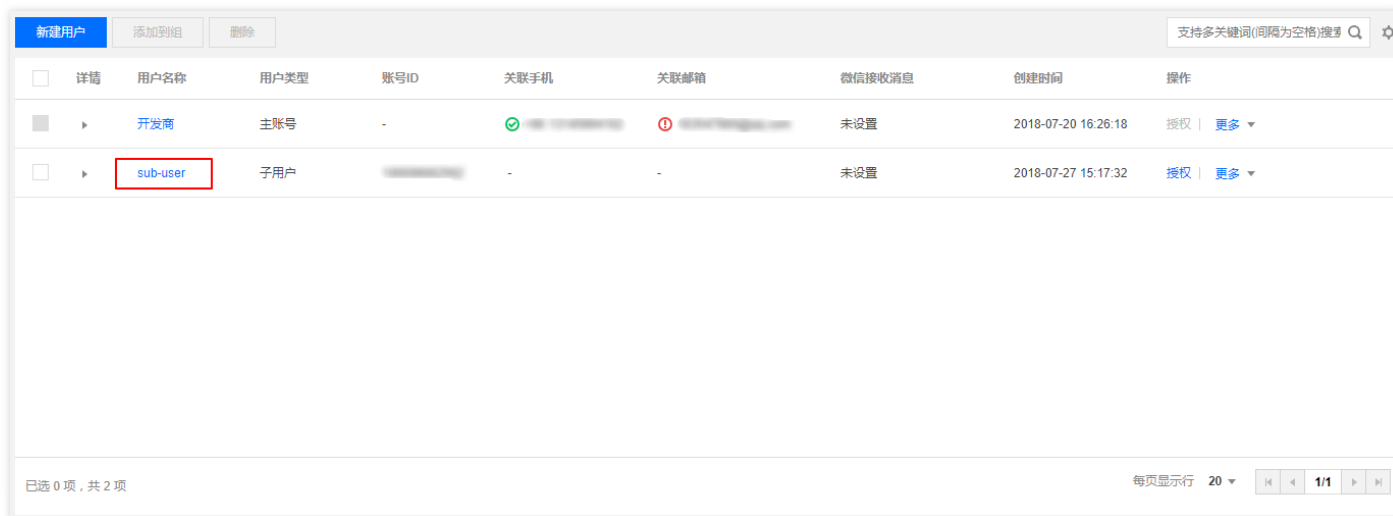
2. 单击【已关联的策略】，在列表中找到需要删除的策略，单击右侧【解除】。



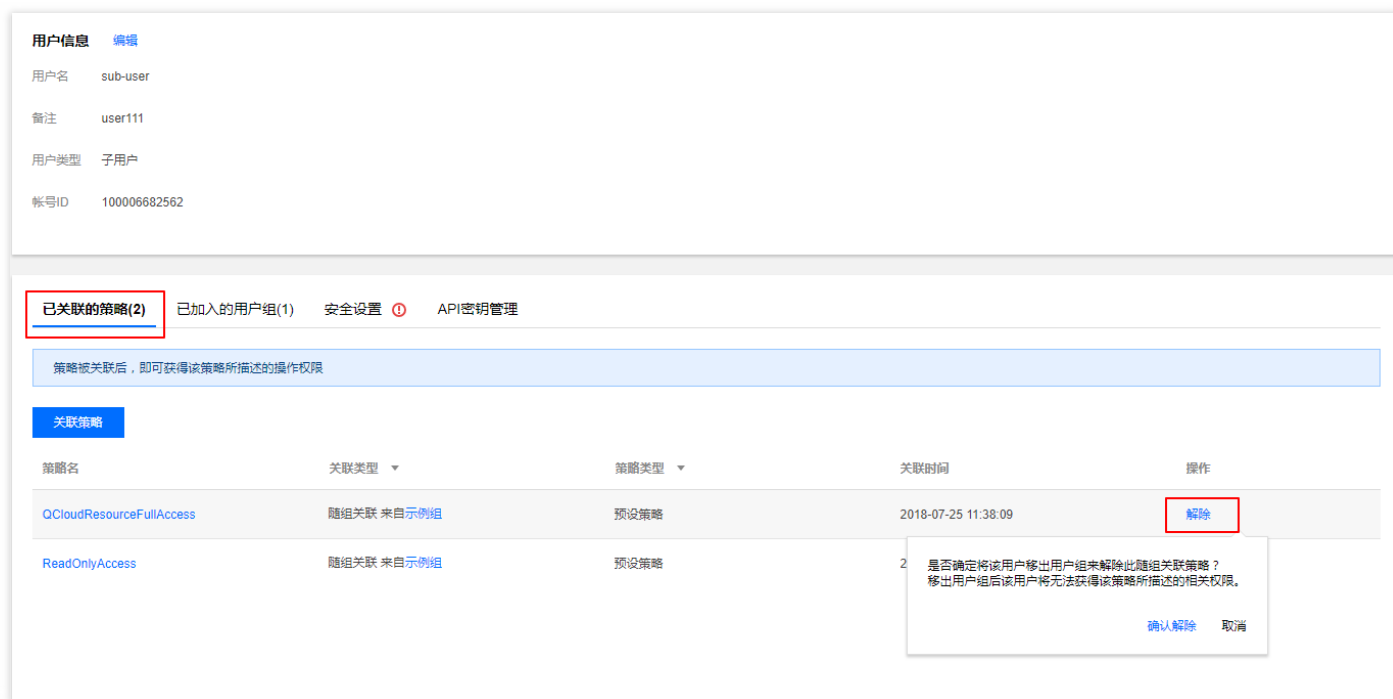
3. 单击【确认解除】，完成为子用户删除关联策略操作。

### 从组中移除

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要删除关联策略的子用户，单击子用户名称，进入子用户详情页。



2. 单击【已关联的策略】，在列表中找到需要删除的随组关联策略，单击右侧【解除】。



3. 单击【确认解除】，将子用户移出用户组，随组关联的策略被解除。

## 为子用户设置订阅消息

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要订阅消息的子用户，单击操作列的【更多】>【订阅消息】，如图所示：

新建用户 添加到组 删除 支持多关键词(间隔为空格)搜索 Q ☆

<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input checked="" type="checkbox"/>	▶	开发商	主账号	-	+86 13145994102	183547880@qq.com	未设置	2018-07-20 16:26:18	授权   更多 ▾
<input type="checkbox"/>	▶	sub-user	子用户	100006682562	-	-	未设置	2018-07-27 15:17:32	授权   更多 ▾

添加到组  
订阅消息  
删除

已选 0 项, 共 2 项 每页显示行 20 ▾ 1/1

2. 勾选需要订阅的消息类型，单击【确定】，完成为子用户设置订阅消息操作。

### 订阅消息 ×

要管理不同消息类型的接收人及接收方式可以前往 [消息中心-消息订阅](#)

消息接收人 **sub-user**

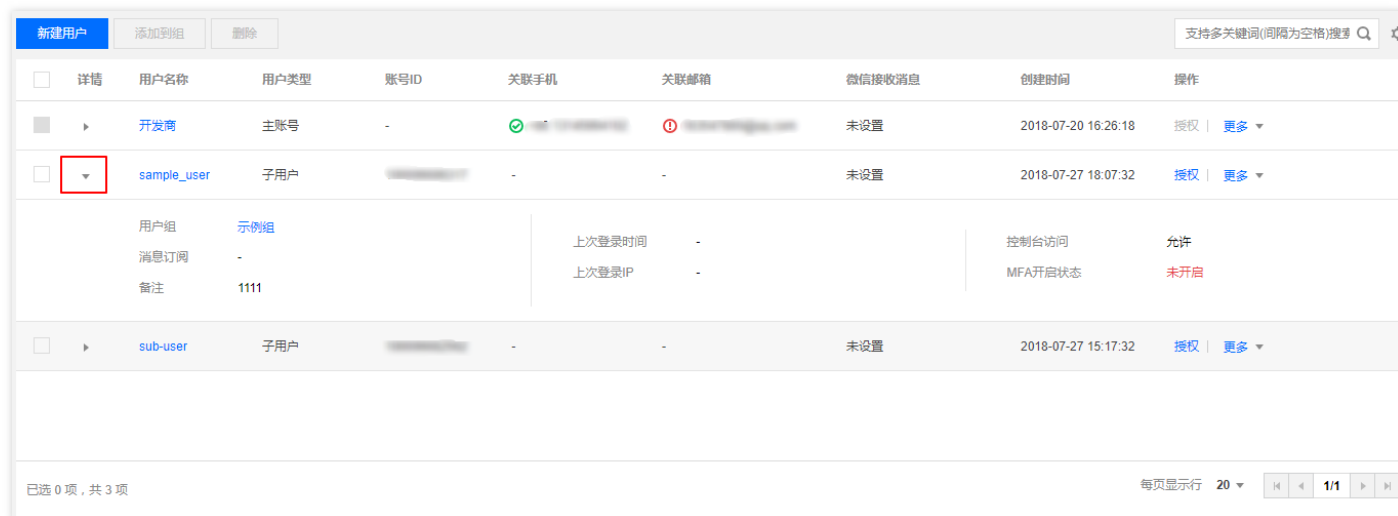
订阅消息类型

<input type="checkbox"/>	全部	
<input type="checkbox"/>	财务消息	^
<input checked="" type="checkbox"/>	账户欠费通知	站内信，邮件，短信，微信
<input checked="" type="checkbox"/>	账户提现通知	站内信，邮件，短信
<input type="checkbox"/>	余额预警通知	站内信，邮件，短信，微信
<input checked="" type="checkbox"/>	产品消息	∨
<input type="checkbox"/>	安全消息	∨
<input type="checkbox"/>	腾讯云动态	∨

**确定** **取消**

## 使用抽屉查看子用户信息

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要查看的子用户，单击左侧的详情图标，如图所示：



详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input type="checkbox"/>	开发者	主账号	-			未设置	2018-07-20 16:26:18	授权   更多
<input type="checkbox"/>	sample_user	子用户	-	-	-	未设置	2018-07-27 18:07:32	授权   更多
用户组 <a href="#">示例组</a> 消息订阅 - 备注 1111		上次登录时间 - 上次登录IP -		控制台访问 允许 MFA开启状态 未开启				
<input type="checkbox"/>	sub-user	子用户	-	-	-	未设置	2018-07-27 15:17:32	授权   更多

已选 0 项，共 3 项 每页显示 20 1/1

您可以在此查看子用户的消息订阅、备注、上次登录时间、上次登录方式、MFA 状态等信息。

## 通过搜索框找到子用户

1. 登录腾讯云控制台，进入 [用户管理](#)，在右上角的搜索框输入关键字，单击搜索图标，可以搜索到相关子用户。



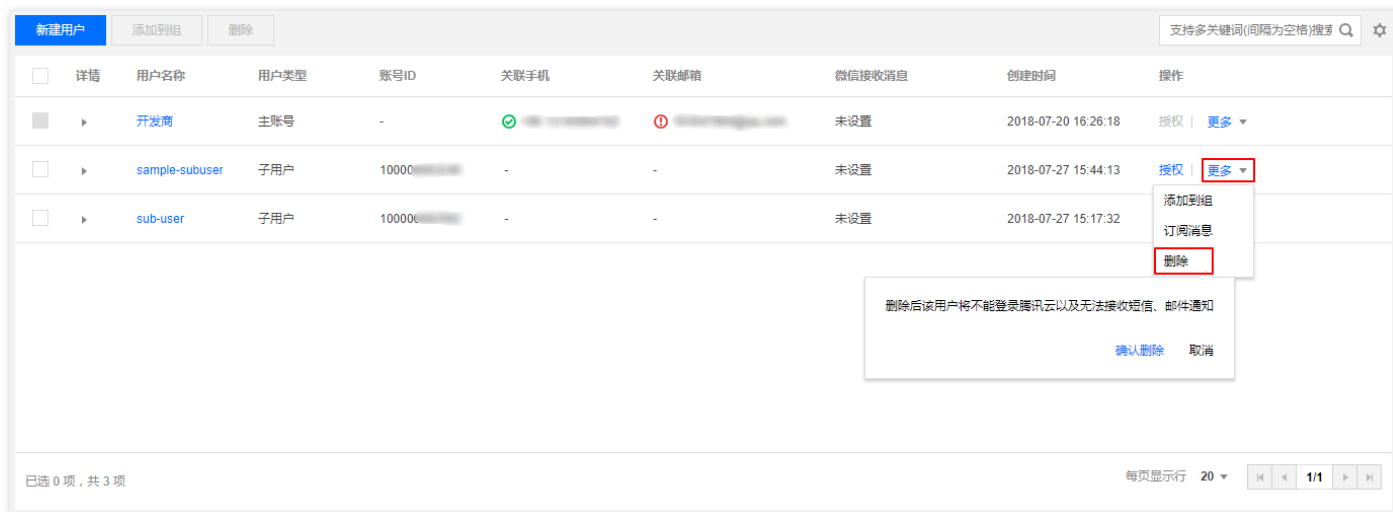
新建用户	添加到组	删除	支持多关键词(间隔为空格)搜索用户名/ID/手机/邮箱/备注						
<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
搜索"s" 找到2条结果。返回原列表									
<input type="checkbox"/>	<input type="checkbox"/>	sub-user	子用户	100006682562	-	-	未设置	2018-07-27 15:17:32	授权   更多
<input type="checkbox"/>	<input type="checkbox"/>	sample_user	子用户	100006686317	-	-	未设置	2018-07-27 18:07:32	授权   更多

搜索框支持多关键词（间隔为空格）搜索。您可以通过用户名、ID、手机、邮箱、备注等关键词搜索相关子用户。

## 删除子用户

### 删除单个子用户

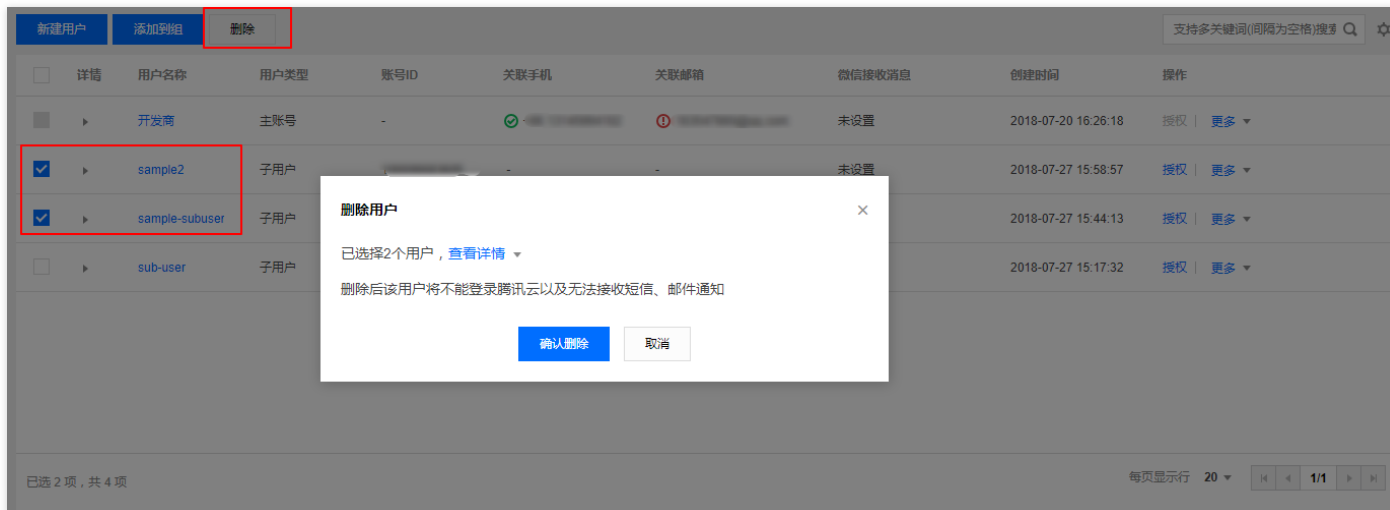
1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要删除的子用户，单击操作列的【更多】>【删除】，如图所示：



2. 单击【确认删除】，完成删除子用户操作。

## 删除多个子用户

1. 登录腾讯云控制台，进入 [用户管理](#)，在用户列表中勾选需要删除的子用户，单击左上方【删除】，如图所示：



2. 单击【确认删除】，完成删除子用户操作。

# 协作者

最近更新时间：2018-07-31 11:38:10

## 概述

协作者是隶属于子账号的一种用户类型，它主要是协作主账号对云上资源以及子账号进行管理，不仅可以登录访问资源也能够接收消息通知。

## 操作指南

### 新建协作者

1. 登录腾讯云控制台，进入 [用户管理](#)，单击【新建用户】，选择【协作者】。

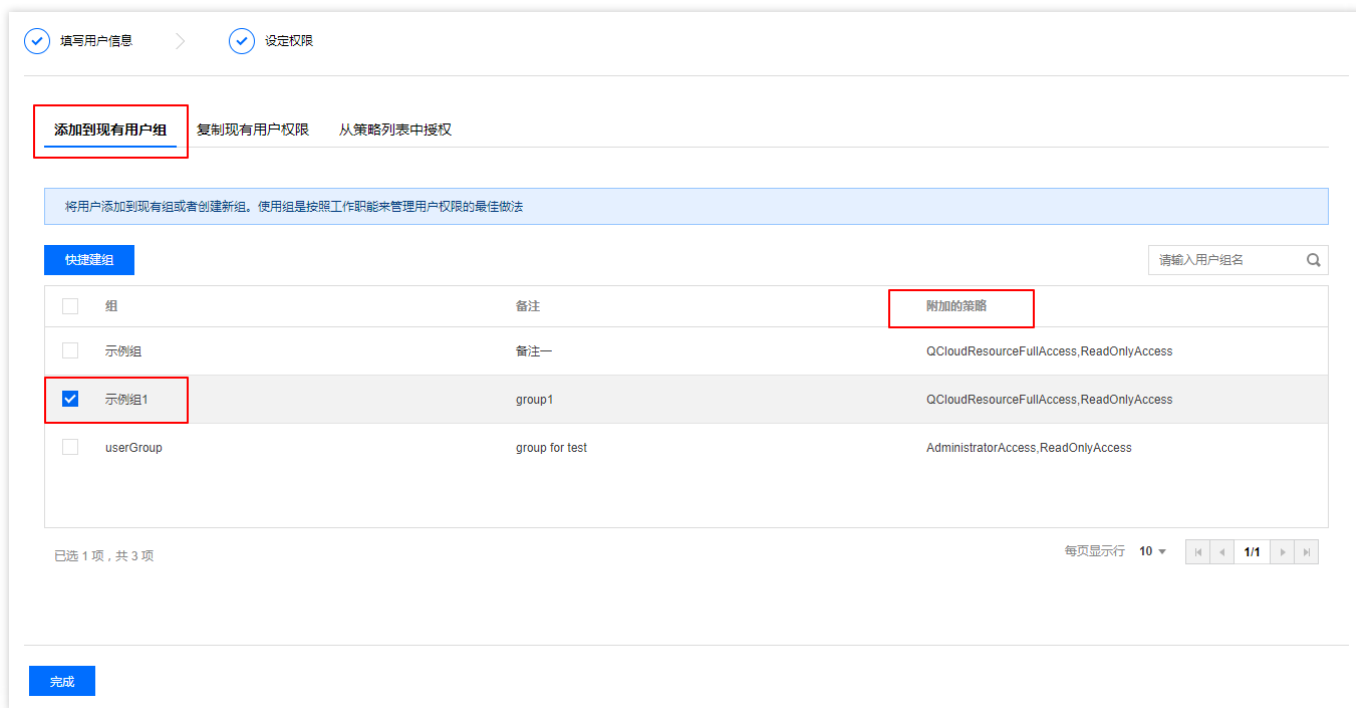


2. 填写相关用户信息，建议您开启登录保护和敏感操作保护。

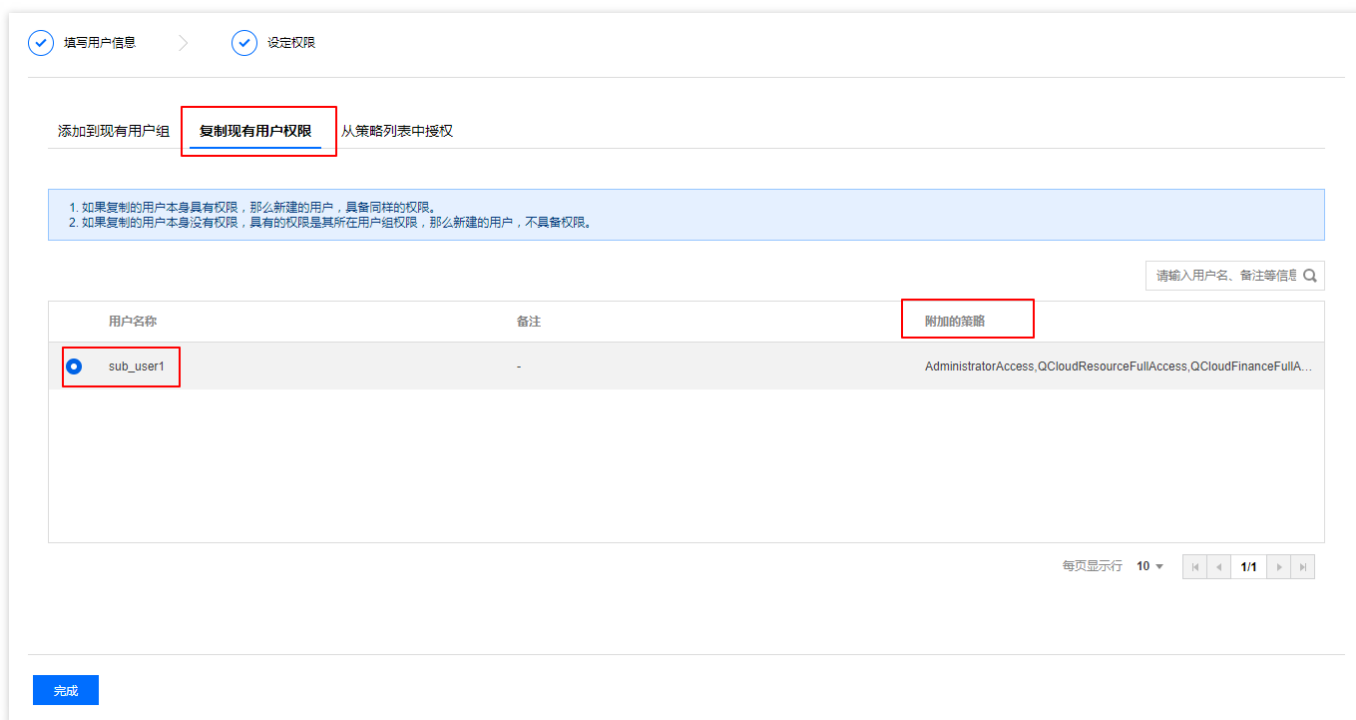


3. 设定权限。您可以通过以下三种方法为当前新建的协作者设定权限，策略描述了权限，关联策略后协作者即获得策略描述的权限。

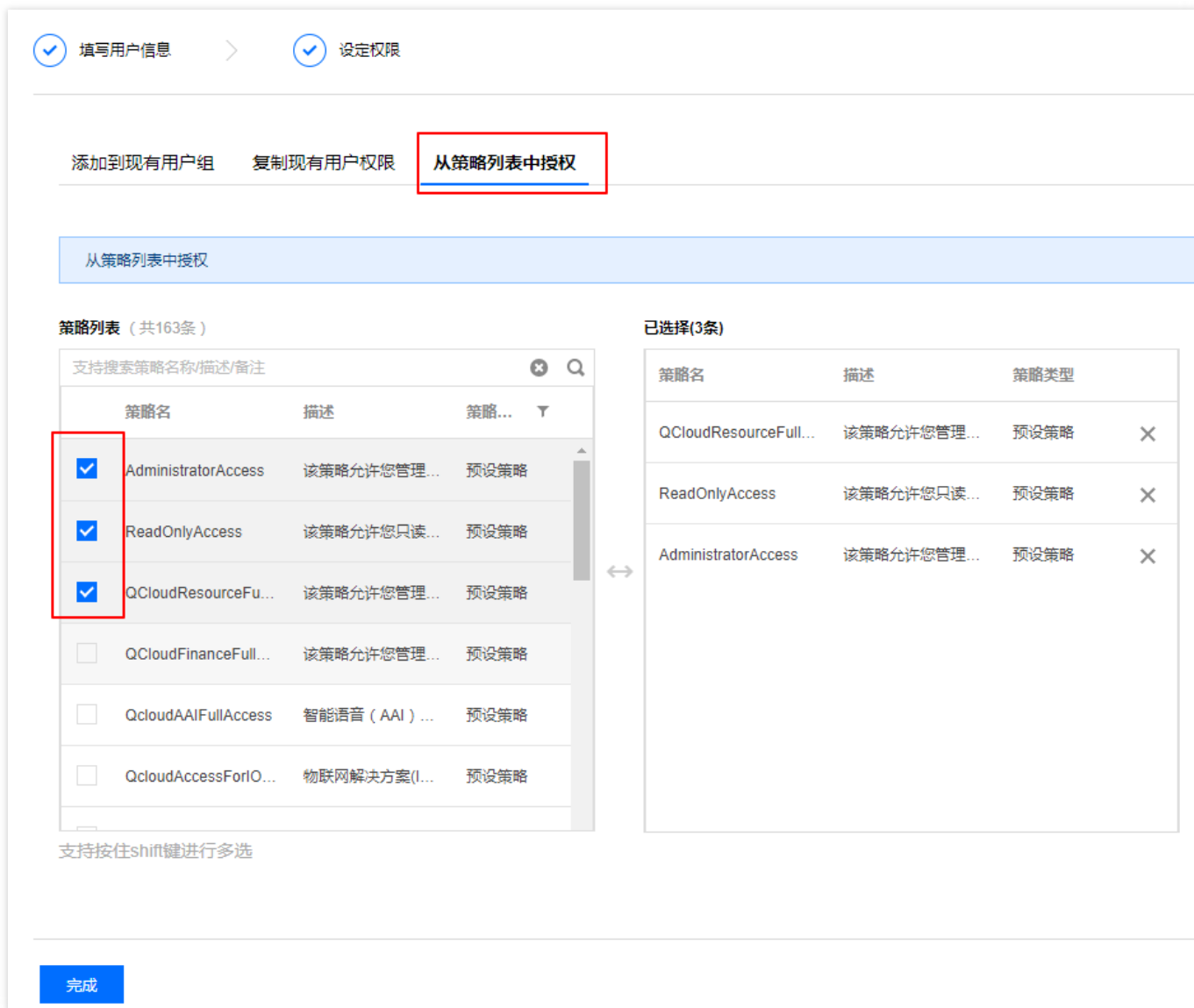
- 使用组是按工作职能来管理用户权限的最佳做法，您可以通过随组关联获得权限。将协作者添加到现有用户组或新建用户组，协作者可以随组关联到该组附加的策略。



- 通过复制现有用户的权限为协作者关联策略，单击【复制现有用户权限】，勾选需要复制的用户，协作者可以关联到被复制用户附加的策略。



- 通过从策略列表中授权。单击【从策略列表中授权】，勾选需要关联的策略。



- 单击【完成】，完成新建协作者操作。

## 为协作者授权关联策略

### 直接关联

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需授权策略的协作者，单击操作列的【授权】。

<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input type="checkbox"/>	▶	开发商	主账号	-	🟢	🔴	未设置	2018-07-20 16:26:18	授权   更多 ▾
<input type="checkbox"/>	▶	示例协作者	协作者	100006686674	🔴	🔴	未验证	2018-07-30 10:30:17	<b>授权</b>   更多 ▾
<input type="checkbox"/>	▶	user	子用户	100006686674	-	-	未设置	2018-07-27 18:36:00	授权   更多 ▾
<input type="checkbox"/>	▶	sample_user	子用户	100006686317	-	-	未设置	2018-07-27 18:07:32	授权   更多 ▾
<input type="checkbox"/>	▶	sub-user	子用户	100006682562	-	-	未设置	2018-07-27 15:17:32	授权   更多 ▾

已选 0 项，共 5 项 每页显示 20 ▾

2. 勾选需要授权的策略，单击【确定】，完成为协作者授权关联策略操作。

### 关联策略 ✕

策略列表 (共163条)

支持搜索策略名称/描述/备注

策略名	描述	策略...
<input checked="" type="checkbox"/> AdministratorAccess	该策略允许您管...	预设策略
<input checked="" type="checkbox"/> ReadOnlyAccess	该策略允许您只...	预设策略
<input type="checkbox"/> QCloudResourceF...	该策略允许您管...	预设策略
<input type="checkbox"/> QCloudFinanceFull...	该策略允许您管...	预设策略
<input type="checkbox"/> QcloudAAIFullAccess	智能语音 (AAI) ...	预设策略
<input type="checkbox"/> QcloudAccessForI...	物联网解决方案(I...	预设策略

支持按住shift键进行多选

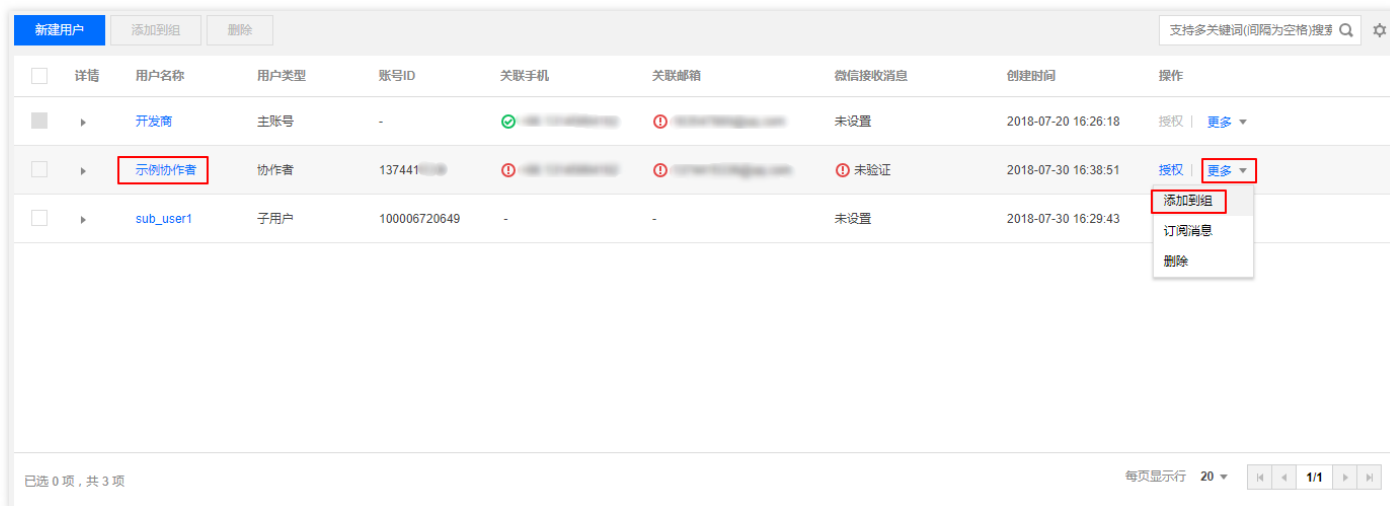
已选择(2条)

策略名	描述	策略类型	
AdministratorAccess	该策略允许您管理...	预设策略	✕
ReadOnlyAccess	该策略允许您只读...	预设策略	✕

确定
取消

## 随组关联

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需授权策略的协作者，单击操作列的【更多】>【添加到组】。



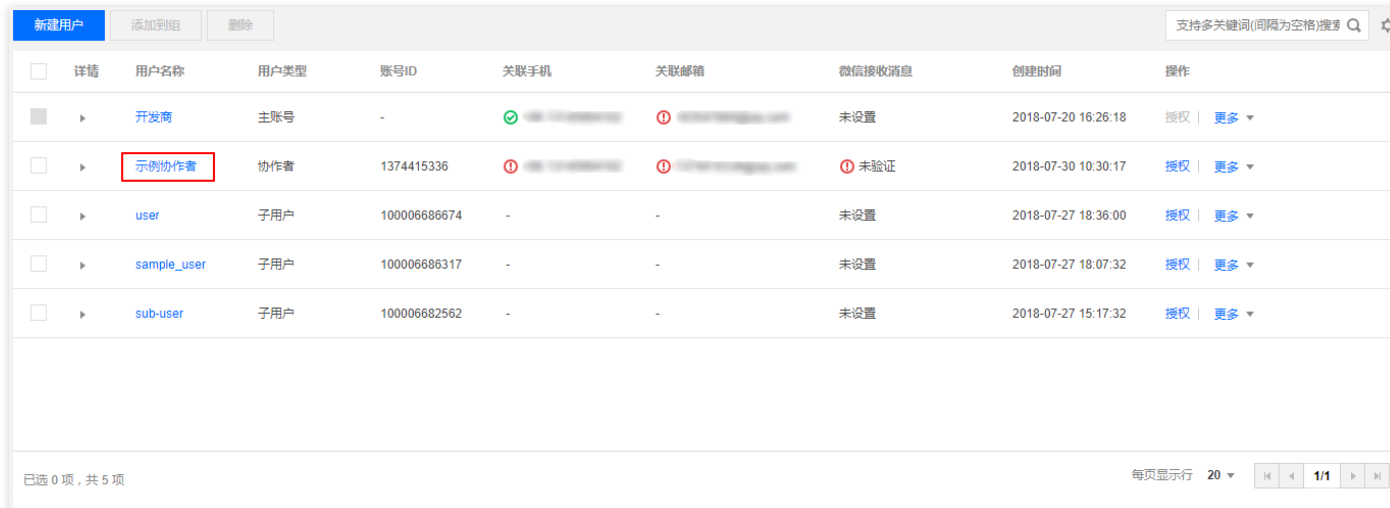
<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input checked="" type="checkbox"/>		开发商	主账号	-			未设置	2018-07-20 16:26:18	授权   更多
<input type="checkbox"/>		示例协作者	协作者	137441			未验证	2018-07-30 16:38:51	授权   更多
<input type="checkbox"/>		sub_user1	子用户	100006720649	-	-	未设置	2018-07-30 16:29:43	授权   更多

2. 勾选需要添加到的用户组，单击【确定】，完成通过添加到组进行随组关联策略操作。

## 为协作者删除关联策略

### 直接解除

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要删除关联策略的协作者，单击协作者名称，进入协作者详情页。



<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input checked="" type="checkbox"/>		开发商	主账号	-			未设置	2018-07-20 16:26:18	授权   更多
<input type="checkbox"/>		示例协作者	协作者	1374415336			未验证	2018-07-30 10:30:17	授权   更多
<input type="checkbox"/>		user	子用户	100006686674	-	-	未设置	2018-07-27 18:36:00	授权   更多
<input type="checkbox"/>		sample_user	子用户	100006686317	-	-	未设置	2018-07-27 18:07:32	授权   更多
<input type="checkbox"/>		sub-user	子用户	100006682562	-	-	未设置	2018-07-27 15:17:32	授权   更多

2. 单击【已关联的策略】，在列表中找到需要删除的策略，单击右侧【解除】。

The screenshot shows the 'User Information' section for a user named '示例协作者'. Below this, there is a section titled '已关联的策略(4)' (4 Associated Strategies). A table lists the strategies with columns for strategy name, association type, strategy type, association time, and actions. A '解除' (Remove) button is highlighted on the 'AdministratorAccess' strategy row. A confirmation dialog box is open, asking '是否确定为该用户解除此策略?' (Are you sure you want to remove this strategy for this user?). The dialog also states '解除后该用户将无法获得该策略所描述的相关权限。' (After removal, the user will no longer be able to obtain the related permissions described by the strategy.) and provides '确认解除' (Confirm Removal) and '取消' (Cancel) buttons.

策略名	关联类型	策略类型	关联时间	操作
AdministratorAccess	直接关联	预设策略	2018-07-30 10:44:09	解除
ReadOnlyAccess	直接关联	预设策略	2018-07-30 10:44:09	解除
QCloudResourceFullAccess	随组关联 来自示例组1	预设策略	2018-07-25 11:29:45	解除
ReadOnlyAccess	随组关联 来自示例组1	预设策略	2018-07-25 11:29:45	解除

3. 单击【确认解除】，完成为协作者删除关联策略操作。

### 从组中移除协作者

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要删除关联策略的协作者，单击协作者名称，进入协作者详情页

The screenshot shows the '新建用户' (New User) page in the Tencent Cloud console. It features a table with columns for user details and actions. The '示例协作者' (Example Collaborator) user is highlighted with a red box. The table includes columns for user name, type, ID, phone, email, WeChat message status, creation time, and actions like '授权' (Authorize) and '更多' (More).

详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
▶	开发者	主账号	-	✓	ⓧ	未设置	2018-07-20 16:26:18	授权   更多
▶	示例协作者	协作者	1374415336	ⓧ	ⓧ	未验证	2018-07-30 10:30:17	授权   更多
▶	user	子用户	100006686674	-	-	未设置	2018-07-27 18:36:00	授权   更多
▶	sample_user	子用户	100006686317	-	-	未设置	2018-07-27 18:07:32	授权   更多
▶	sub-user	子用户	100006682562	-	-	未设置	2018-07-27 15:17:32	授权   更多

2. 单击【已关联的策略】，在列表中找到需要删除的随组关联的策略，单击右侧【解除】。

3. 单击【确认解除】，将协作者移出用户组，随组关联的策略被解除。

## 为协作者订阅消息

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需订阅消息的协作者，单击操作列的【更多】>【订阅消息】，如图所示：

2. 勾选需订阅的消息类型，单击【确定】，完成为协作者订阅消息操作。

### 订阅消息 ✕

要管理不同消息类型的接收人及接收方式可以前往 [消息中心-消息订阅](#)

消息接收人 **示例协作者**

订阅消息类型

<input type="checkbox"/>	全部	
<input checked="" type="checkbox"/>	财务消息	^
<input checked="" type="checkbox"/>	账户欠费通知	站内信，邮件，短信，微信
<input checked="" type="checkbox"/>	账户提现通知	站内信，邮件，短信
<input checked="" type="checkbox"/>	余额预警通知	站内信，邮件，短信，微信
<input type="checkbox"/>	产品消息	v
<input type="checkbox"/>	安全消息	v
<input type="checkbox"/>	腾讯云动态	v

## 使用抽屉查看协作者信息

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需要查看的协作者，单击左侧的详情图标，如图所示：

<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input type="checkbox"/>		开发商	主账号	-			未设置	2018-07-20 16:26:18	授权   更多
<input type="checkbox"/>		示例协作者	协作者	1374415336			未验证	2018-07-30 10:30:17	授权   更多
		用户组	示例组1	上次登录时间		-	控制台访问	允许	
		消息订阅	财务消息	上次登录IP		-	MFA开启状态	未开启	
		备注	合理备注可以快速定位用户						
<input type="checkbox"/>		user	子用户	100006686674	-	-	未设置	2018-07-27 18:36:00	授权   更多
<input type="checkbox"/>		sample_user	子用户	100006686317	-	-	未设置	2018-07-27 18:07:32	授权   更多
<input type="checkbox"/>		sub-user	子用户	100006682562	-	-	未设置	2018-07-27 15:17:32	授权   更多

已选 0 项，共 5 项 每页显示行 20 1/1

您可以在此查看子用户的消息订阅、备注、上次登录时间、上次登录方式、MFA 状态等信息。

## 通过搜索框找到协作者

1. 登录腾讯云控制台，进入 [用户管理](#)，在右上角的搜索框输入关键字，单击搜索图标，可以搜索到相关协作者。

<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
搜索“示例”，找到1条结果。 <a href="#">返回原列表</a>									
<input type="checkbox"/>		示例协作者	协作者	1374415336			未验证	2018-07-30 16:38:51	授权   更多

已选 0 项，共 1 项 每页显示行 20 1/1

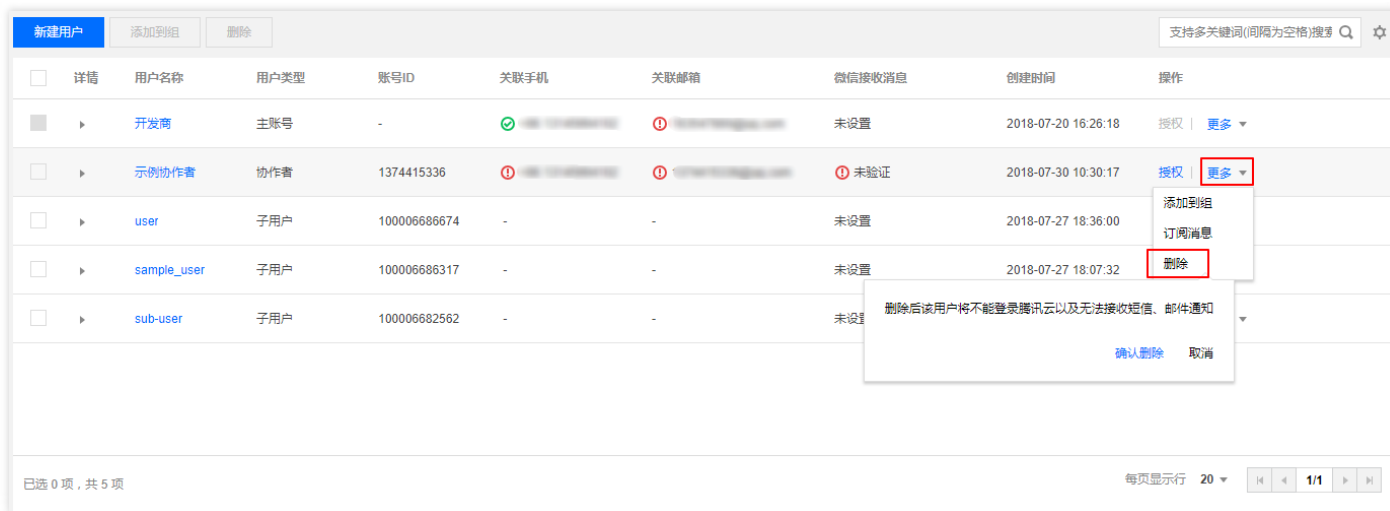
搜索框支持多关键词（间隔为空格）搜索。您可以通过用户名、ID、手机、邮箱、备注等关键词搜索相关协作者。

## 删除协作者



## 删除单个协作者

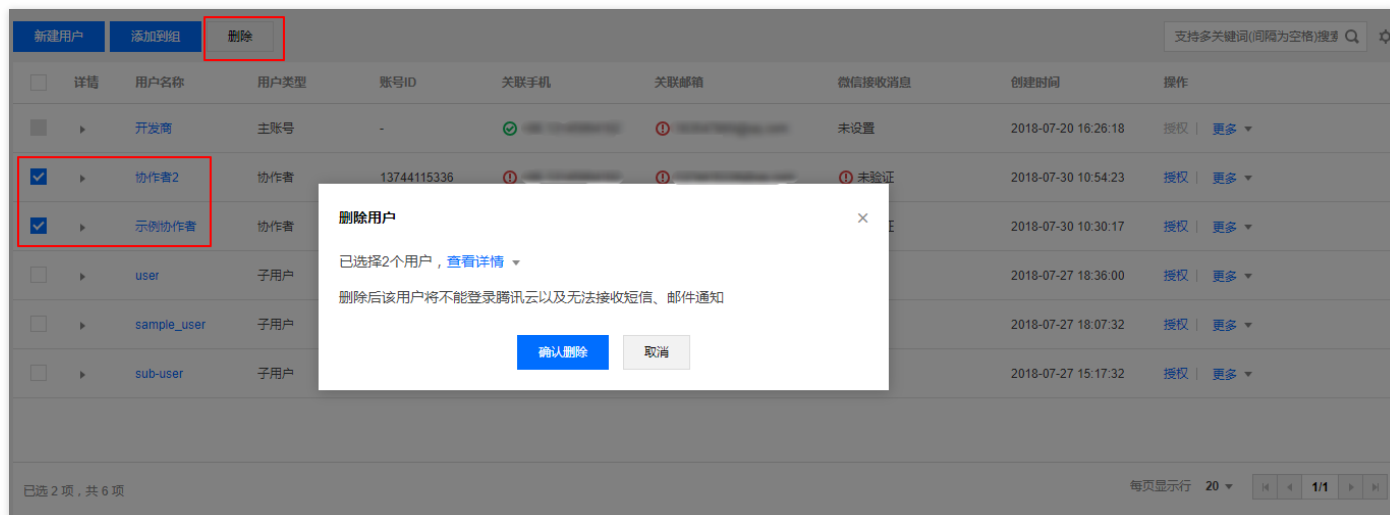
1. 登录腾讯云控制台，进入 [用户管理](#)，找到需删除的协作者，单击操作列的【更多】>【删除】，如图所示：



2. 单击【确认删除】，完成删除协作者操作。

## 删除多个协作者

1. 登录腾讯云控制台，进入 [用户管理](#)，在左侧勾选需删除的协作者，单击左上方的【删除】，如图所示：



2. 单击【确认删除】，完成删除协作者操作。

# 消息接收人

最近更新时间：2018-07-31 11:58:05

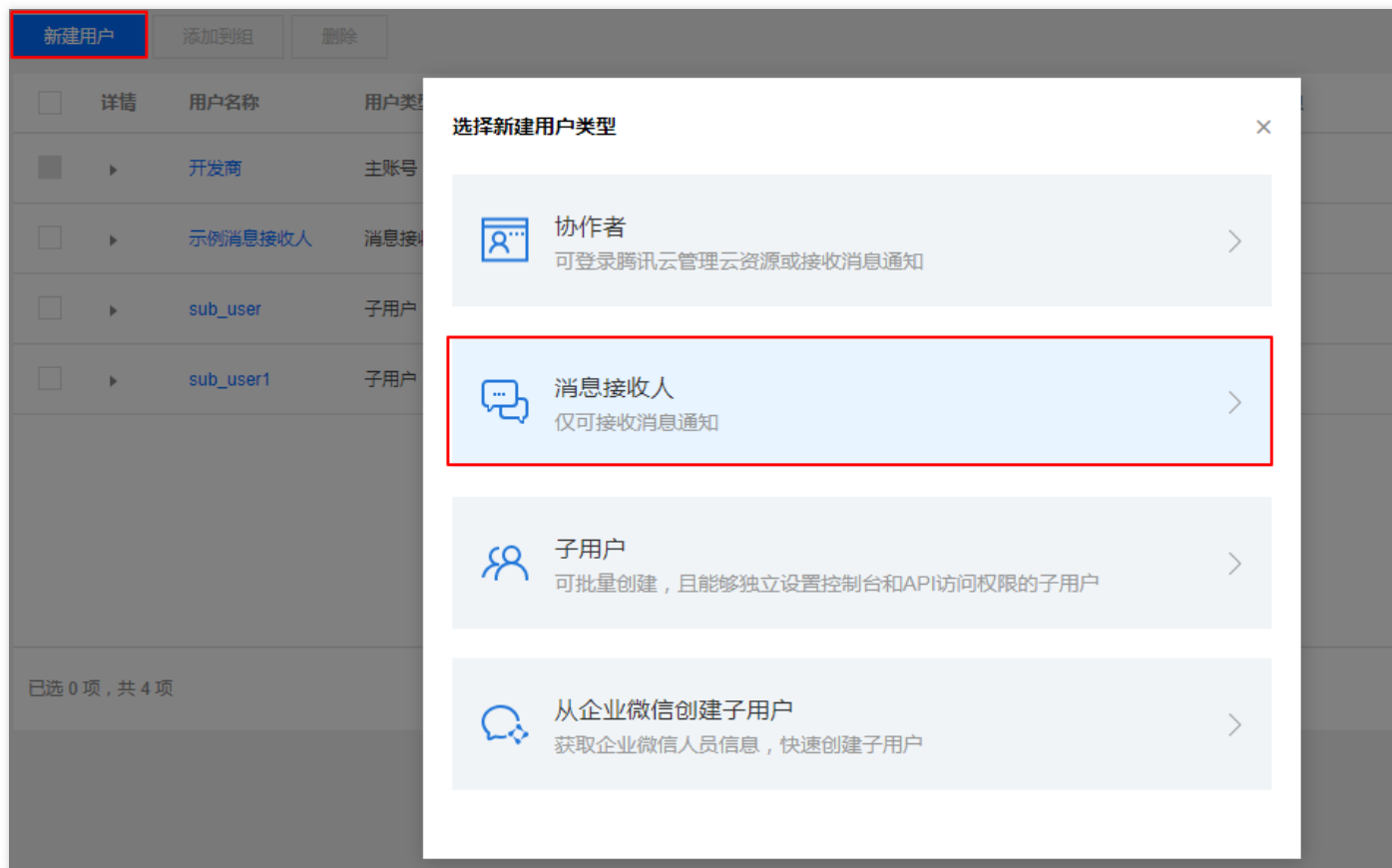
## 概述

消息接收人是隶属于子账号的一种用户类型，它无法编程访问或者登录腾讯云控制台，仅可通过主账号设置的关联联系方式接收消息通知。

## 操作指南

### 新建消息接收人

1. 登录腾讯云控制台，进入 [用户管理](#)，单击【新建用户】，选择【消息接收人】。



2. 填写用户信息，如下图所示：

用户名（必填）

备注 

合理备注可以快速定位用户

联系手机（必填） 中国(+86)

联系邮箱（必填）

是否允许微信接收通知  是  否

1. 联系邮箱将收到一封包含二维码的邮件，微信扫码并关注公众号即可接收通知  
2. 前往 消息中心->消息订阅 设置微信为接收方式后即可接收消息。

[完成](#)

3. 单击【完成】，完成新建消息接收人操作。

## 为消息接收人订阅消息

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需订阅消息的消息接收人，单击操作列的【更多】>【订阅消息】。

新建用户	添加到组	删除	支持多关键词(间隔为空格)搜索						
详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作	
<input type="checkbox"/>	开发者	主账号	-			未设置	2018-07-20 16:26:18	授权   更多	
<input type="checkbox"/>	user_message	消息接收人	-				2018-07-31 11:18:22	授权   更多	
<input type="checkbox"/>	示例消息接收人	消息接收人	-				2018-07-31 10:51:37	授权   更多	
<input type="checkbox"/>	sub_user	子用户	100006722628	-	-	未设置	2018-07-30 18:05:13	添加到组 订阅消息 删除	
<input type="checkbox"/>	sub_user1	子用户	100006720649	-	-	未设置	2018-07-30 16:29:43		

已选 0 项，共 5 项 每页显示行 20 1/1

2. 勾选需订阅的消息类型，单击【确定】，完成为消息接收人订阅消息操作。

### 订阅消息 ×

要管理不同消息类型的接收人及接收方式可以前往 [消息中心-消息订阅](#)

消息接收人 **示例消息接收人**

订阅消息类型

<input type="checkbox"/>	全部	
<input type="checkbox"/>	财务消息	^
<input checked="" type="checkbox"/>	账户欠费通知	站内信，邮件，短信，微信
<input checked="" type="checkbox"/>	账户提现通知	站内信，邮件，短信
<input type="checkbox"/>	余额预警通知	站内信，邮件，短信，微信
<input checked="" type="checkbox"/>	产品消息	v
<input type="checkbox"/>	安全消息	v
<input type="checkbox"/>	腾讯云动态	v

**确定** **取消**

## 添加消息接收人到用户组

1. 登录腾讯云控制台，进入 [用户管理](#)，找到需添加到组的消息接收人，单击操作列的【更多】>【添加到组】。

<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input checked="" type="checkbox"/>		开发商	主账号	-			未设置	2018-07-20 16:26:18	授权   更多
<input type="checkbox"/>		示例消息接收人	消息接收人	-				2018-07-31 10:51:37	授权   更多
<input type="checkbox"/>		sub_user	子用户	100006722628	-	-	未设置	2018-07-30 18:05:13	授权   更多
<input type="checkbox"/>		sub_user1	子用户	100006720649	-	-	未设置	2018-07-30 16:29:43	授权   更多

已选 0 项，共 4 项

每页显示行 20

2. 勾选需要添加到的用户组，单击【确定】，完成添加到组操作。

## 从用户组移出消息接收人

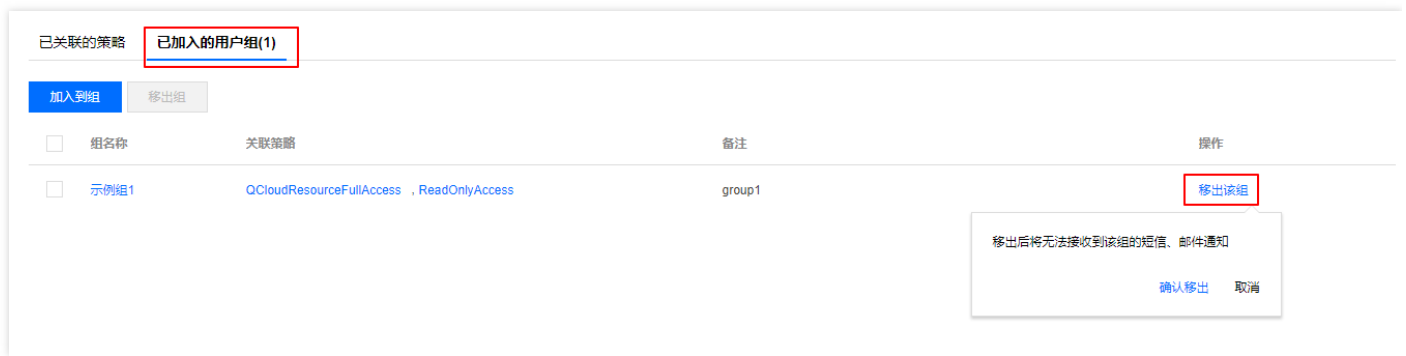
1. 登录腾讯云控制台，进入 [用户管理](#)，找到需从组中移出的消息接收者人，单击消息接收人名称，进入详情页。

<input type="checkbox"/>	详情	用户名称	用户类型	账号ID	关联手机	关联邮箱	微信接收消息	创建时间	操作
<input checked="" type="checkbox"/>		开发商	主账号	-			未设置	2018-07-20 16:26:18	授权   更多
<input type="checkbox"/>		示例消息接收人	消息接收人	-				2018-07-31 10:51:37	授权   更多
<input type="checkbox"/>		sub_user	子用户		-	-	未设置	2018-07-30 18:05:13	授权   更多
<input type="checkbox"/>		sub_user1	子用户		-	-	未设置	2018-07-30 16:29:43	授权   更多

已选 0 项，共 4 项

每页显示行 20

2. 单击【已加入的用户组】，找到需要移出的组，单击【移出该组】。

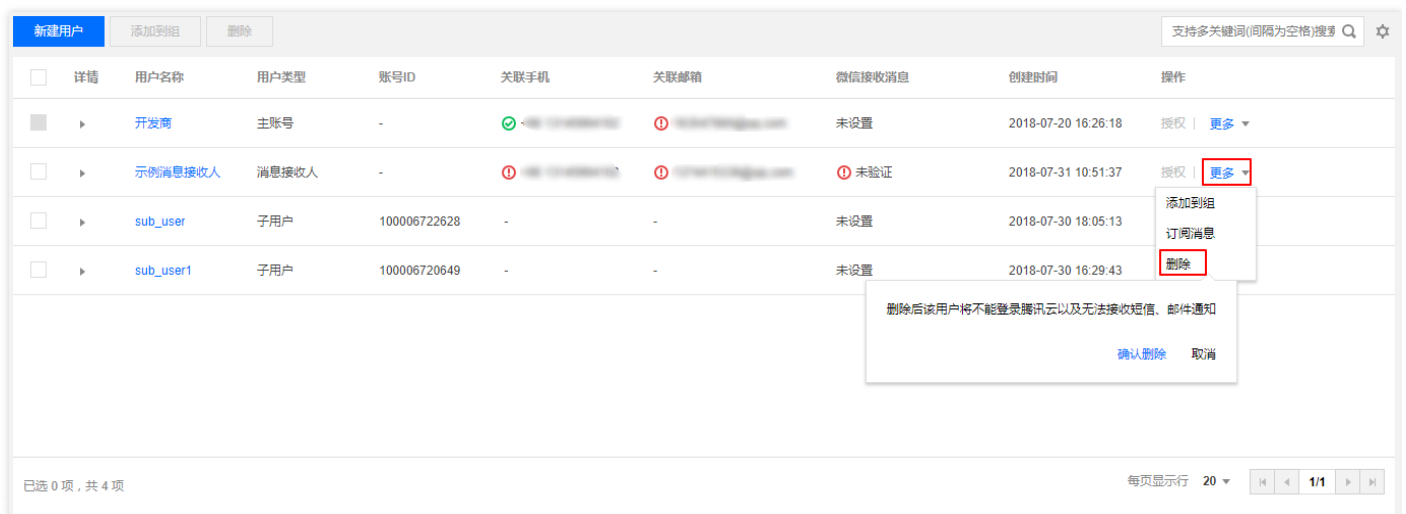


3. 单击【确认移出】，完成从用户组移出消息接收人操作。

## 删除消息接收人

### 删除单个消息接收人

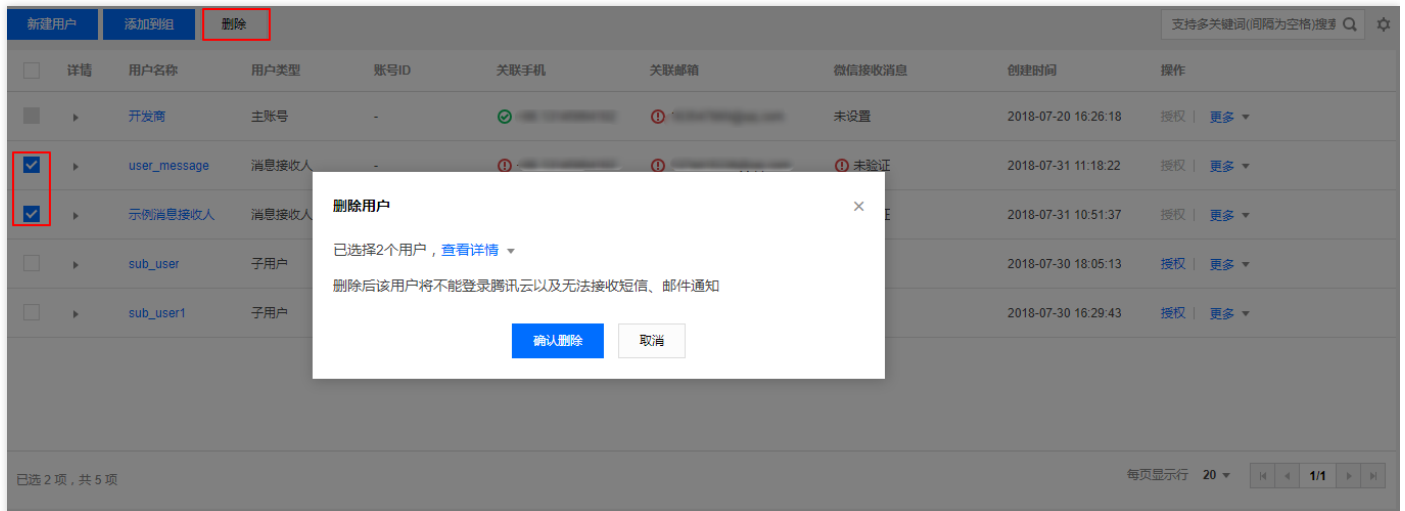
1. 登录腾讯云控制台，进入 [用户管理](#)，找到需删除的消息接收人，单击操作列的【更多】>【删除】。



2. 单击【确认删除】，完成删除消息接收人操作。

### 删除多个消息接收人

1. 登录腾讯云控制台，进入 [用户管理](#)，勾选需删除的消息接收人，单击左上方【删除】。



2. 单击【确认删除】，完成删除消息接收人操作。

# 用户组管理

最近更新时间：2018-08-03 10:16:28

## 概述

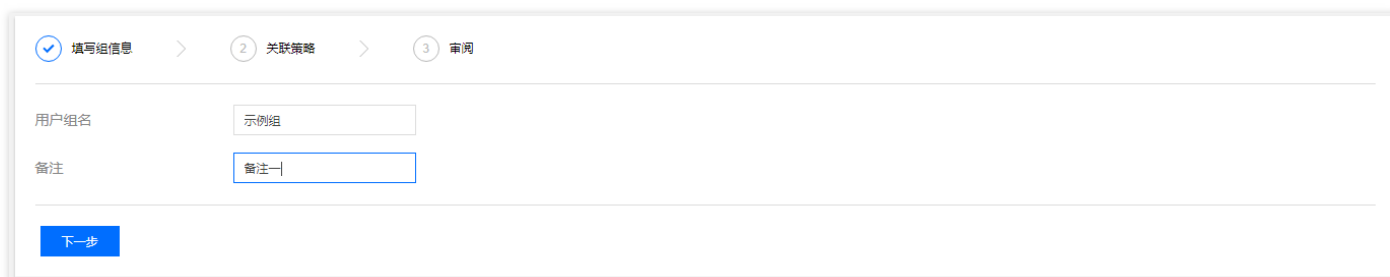
您可以将有相同职能的用户添加在同一用户组，并为该用户组关联适当的策略，以分配不同权限，来提高工作效率。

策略与用户组关联后，用户组内的用户都将获得策略描述的权限，非常适合批量授权的场景

## 操作指南

### 新建用户组

1. 登录 [访问管理控制台](#)，在左侧导航单击进入【用户组管理】。
2. 单击【新建用户组】，填写用户组名和备注。本文以新建一个示例组为例，然后单击【下一步】。



填写组信息 > 2 关联策略 > 3 审阅

用户组名

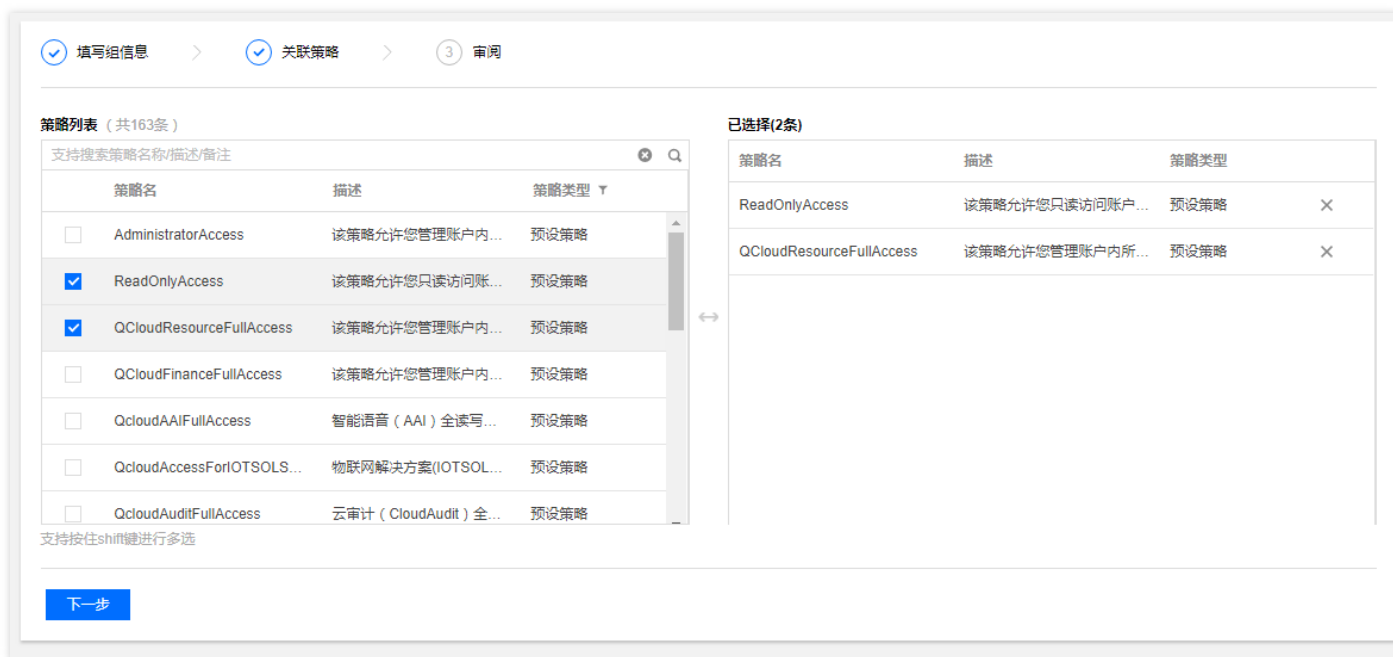
备注

下一步

在用户组列表中您可以搜索用户组名或备注，在众多用户组中快速准确定位到对应的用户组。



3. (可选) 勾选关联策略, 不勾选也可完成新建用户组操作。单击【下一步】, 进入审阅步骤。



4. 在审阅中, 您可以查看用户组的相关设置, 如有误可修改。确认无误后, 单击【完成】, 完成新建用户组操作。



## 为用户组添加用户

### 单个用户组添加用户

1. 登录 [访问管理控制台](#), 在左侧导航单击进入【用户组管理】。在用户组列表中找到要添加用户的用户组, 单击右侧的【添加用户】。

用户组名称	备注	创建时间	操作
<input type="checkbox"/> 示例组	备注一	2018-07-25 11:37:38	<span style="border: 1px solid red; padding: 2px;">添加用户</span> 删除
<input type="checkbox"/> 示例组1	group1	2018-07-25 11:29:41	添加用户 删除
<input type="checkbox"/> userGroup	group for test	2018-07-25 11:10:44	添加用户 删除

已选 0 项，共 3 项

每页显示行 20

2. 勾选要添加的用户，单击【确定】，完成为用户组添加用户操作。

### 添加用户

选择添加的用户 (共4条)

支持多关键词(间隔为空格)搜索用户名/ID/手机/邮箱/备注

用户	用户类型
<input type="checkbox"/> 开发商	主账号
<input checked="" type="checkbox"/> sub-user	子用户
<input checked="" type="checkbox"/> 示例消息接受人	消息接收人
<input type="checkbox"/> 示例协作者	协作者

支持按住shift键进行多选

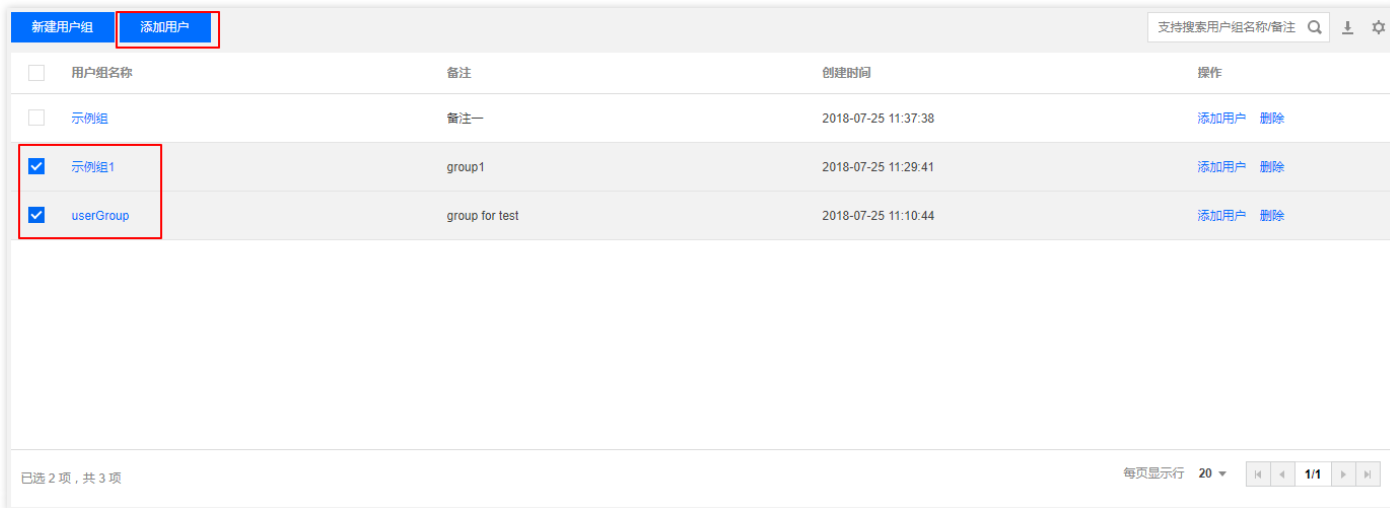
已选择(2条)

用户	用户类型	
sub-user	子用户	×
示例消息接受人	消息接收人	×

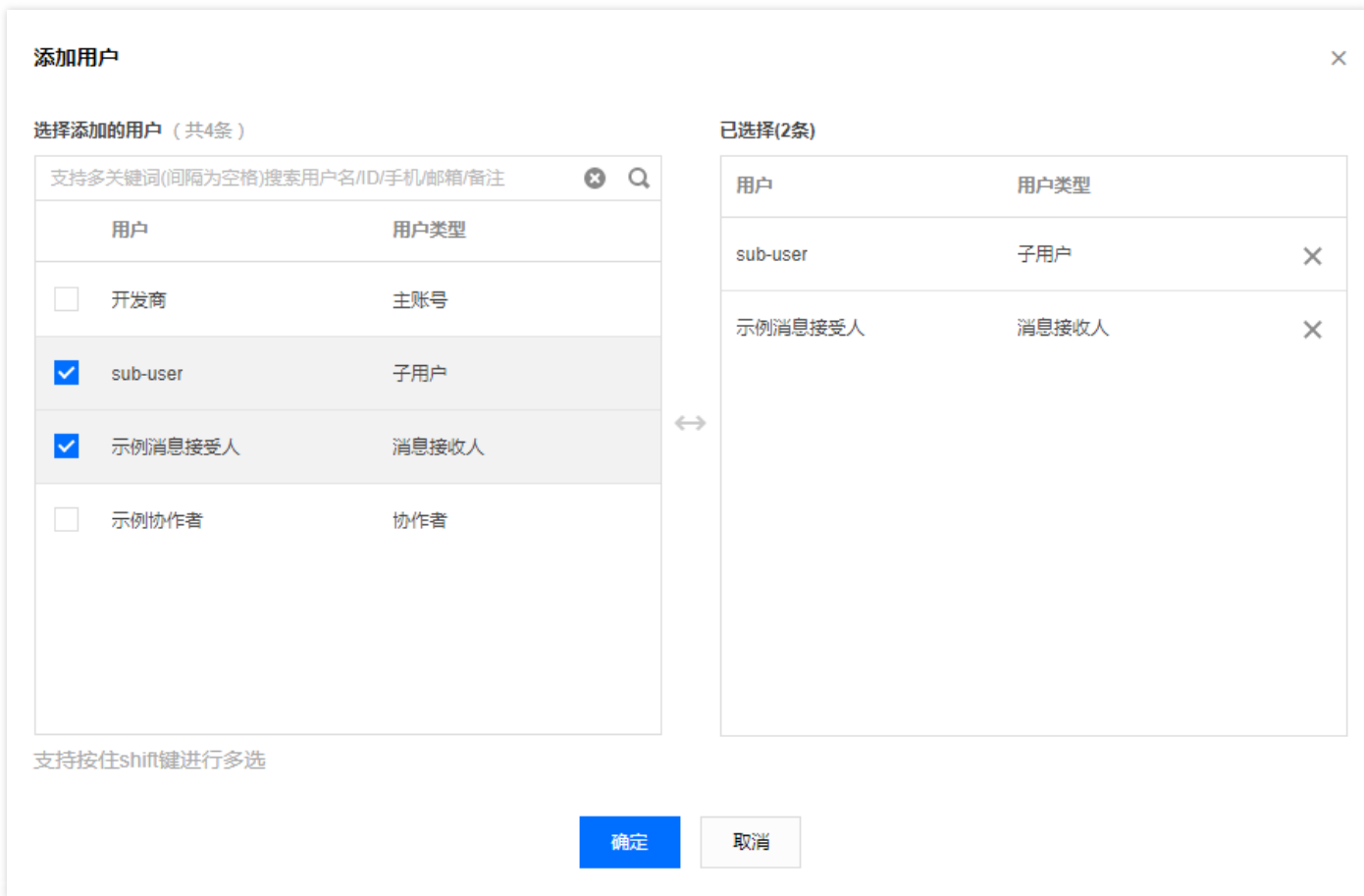
确定
取消

## 多个用户组添加用户

1. 登录 [访问管理控制台](#)，在左侧导航单击进入【用户组管理】。在用户组列表中勾选要添加用户的用户组，单击【添加用户】。



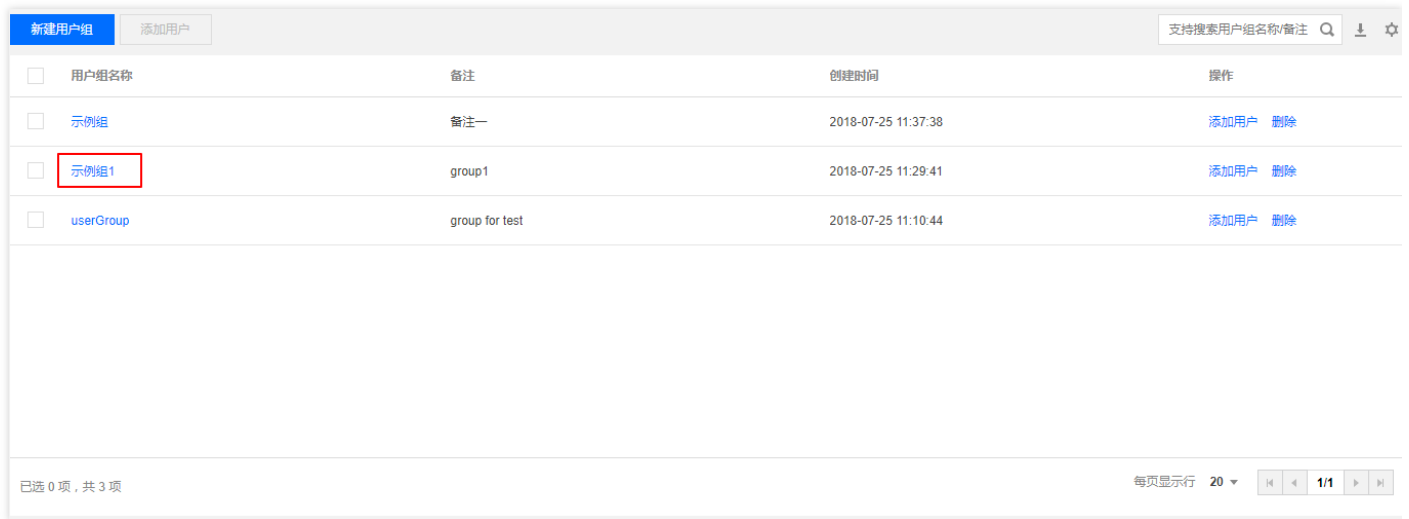
2. 勾选要添加的用户，单击【确定】，完成为用户组添加用户操作。



## 为用户组删除用户

## 为用户组删除单个用户

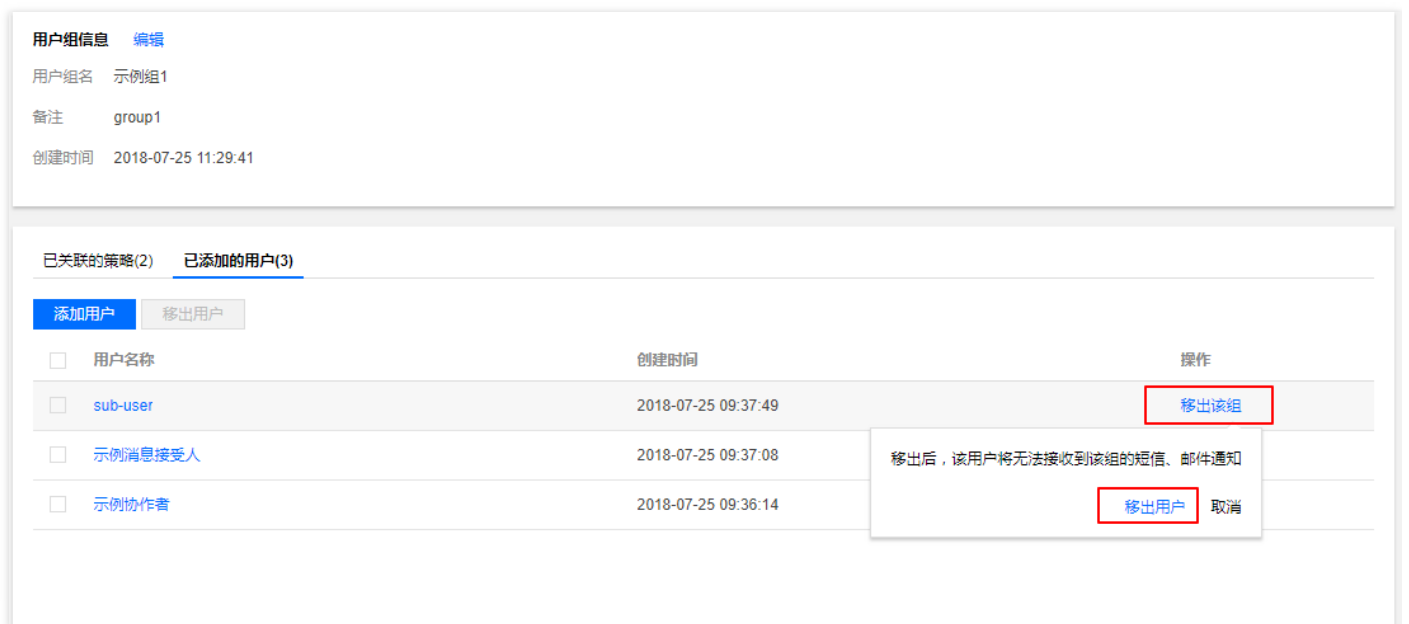
1. 登录 [访问管理控制台](#)，在左侧导航单击进入【用户组管理】。单击用户组名称，进入用户组详情页。



<input type="checkbox"/>	用户组名称	备注	创建时间	操作
<input type="checkbox"/>	示例组	备注一	2018-07-25 11:37:38	<a href="#">添加用户</a> <a href="#">删除</a>
<input type="checkbox"/>	示例组1	group1	2018-07-25 11:29:41	<a href="#">添加用户</a> <a href="#">删除</a>
<input type="checkbox"/>	userGroup	group for test	2018-07-25 11:10:44	<a href="#">添加用户</a> <a href="#">删除</a>

已选 0 项，共 3 项 每页显示行 20 1/1

2. 单击【已添加的用户】，在用户列表中逐个找到要删除的用户，单击右侧的【移出该组】进行删除单个用户。



**用户组信息** [编辑](#)

用户组名 示例组1  
备注 group1  
创建时间 2018-07-25 11:29:41

---

已关联的策略(2) 已添加的用户(3)

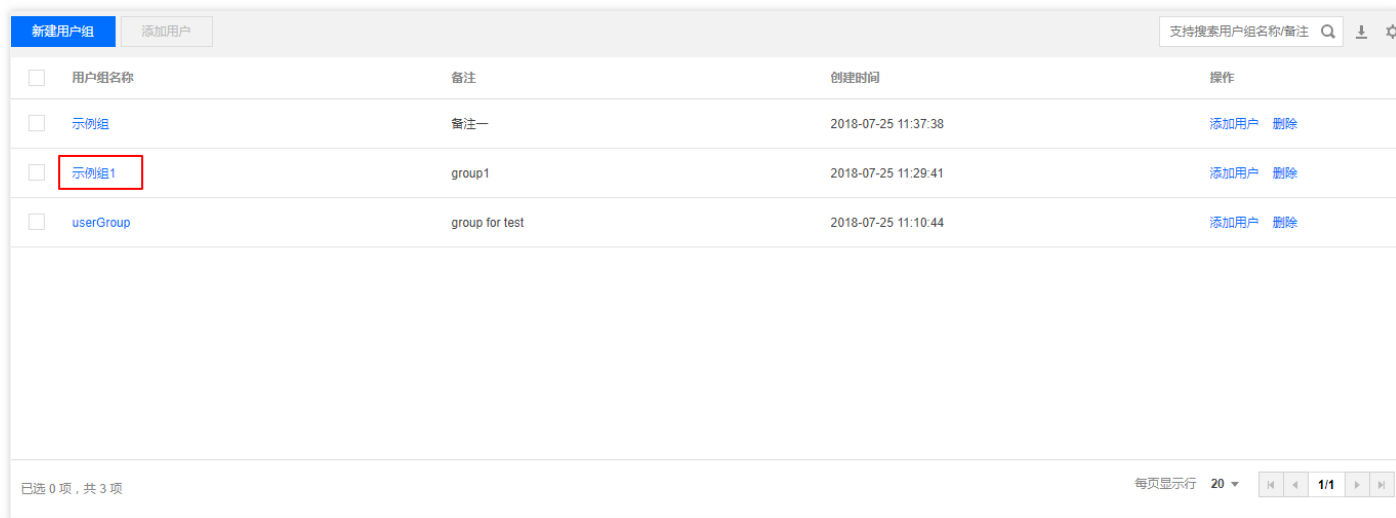
[添加用户](#) [移出用户](#)

<input type="checkbox"/>	用户名称	创建时间	操作
<input type="checkbox"/>	sub-user	2018-07-25 09:37:49	<a href="#">移出该组</a>
<input type="checkbox"/>	示例消息接受人	2018-07-25 09:37:08	移出后，该用户将无法接收到该组的短信、邮件通知
<input type="checkbox"/>	示例协作者	2018-07-25 09:36:14	

3. 单击【移出用户】，完成为用户组删除用户操作。

### 为用户组删除多个用户

1. 登录 [访问管理控制台](#)，在左侧导航单击进入【用户组管理】。单击用户组名称，进入用户组详情页。

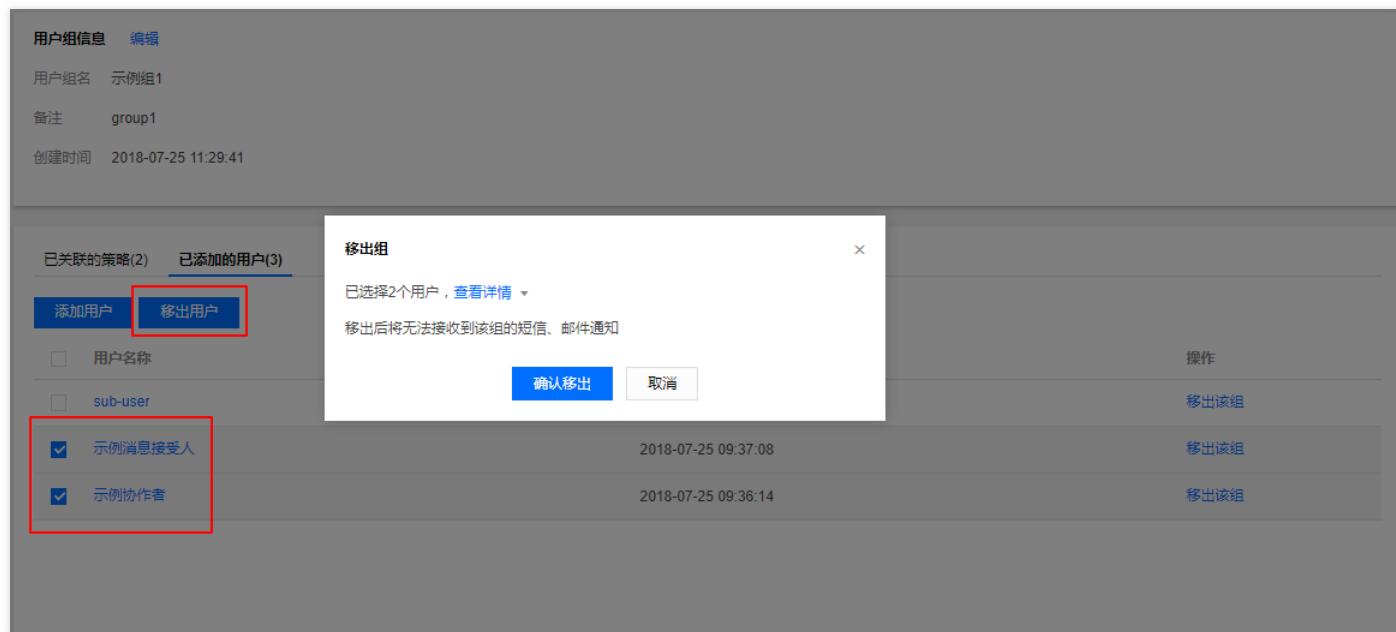


<input type="checkbox"/>	用户组名称	备注	创建时间	操作
<input type="checkbox"/>	示例组	备注一	2018-07-25 11:37:38	<a href="#">添加用户</a> <a href="#">删除</a>
<input type="checkbox"/>	示例组1	group1	2018-07-25 11:29:41	<a href="#">添加用户</a> <a href="#">删除</a>
<input type="checkbox"/>	userGroup	group for test	2018-07-25 11:10:44	<a href="#">添加用户</a> <a href="#">删除</a>

已选 0 项，共 3 项

每页显示行 20

2. 单击【已添加的用户】，勾选多个需要删除的用户，单击左上方的【移出用户】。



**用户组信息** [编辑](#)

用户组名 示例组1

备注 group1

创建时间 2018-07-25 11:29:41

已关联的策略(2) **已添加的用户(3)**

[添加用户](#) [移出用户](#)

<input type="checkbox"/>	用户名称	操作
<input type="checkbox"/>	sub-user	<a href="#">移出该组</a>
<input checked="" type="checkbox"/>	示例消息接受人	2018-07-25 09:37:08 <a href="#">移出该组</a>
<input checked="" type="checkbox"/>	示例协作者	2018-07-25 09:36:14 <a href="#">移出该组</a>

**移出组** ×

已选择2个用户，[查看详情](#)

移出后将无法接收到该组的短信、邮件通知

[确认移出](#) [取消](#)

3. 单击【确认移出】，完成为用户组删除用户操作。

## 为用户组添加策略

1. 登录 [访问管理控制台](#)，在左侧导航单击进入【用户组管理】。单击用户组名称，进入用户组详情页。

用户组名称	备注	创建时间	操作
<a href="#">示例组</a>	备注一	2018-07-25 11:37:38	<a href="#">添加用户</a> <a href="#">删除</a>
<a href="#">示例组1</a>	group1	2018-07-25 11:29:41	<a href="#">添加用户</a> <a href="#">删除</a>
<a href="#">userGroup</a>	group for test	2018-07-25 11:10:44	<a href="#">添加用户</a> <a href="#">删除</a>

2. 单击【已关联的策略】>【关联策略】。

**用户组信息** [编辑](#)

用户组名 [示例组](#)

备注 -

创建时间 2018-07-25 09:24:09

---

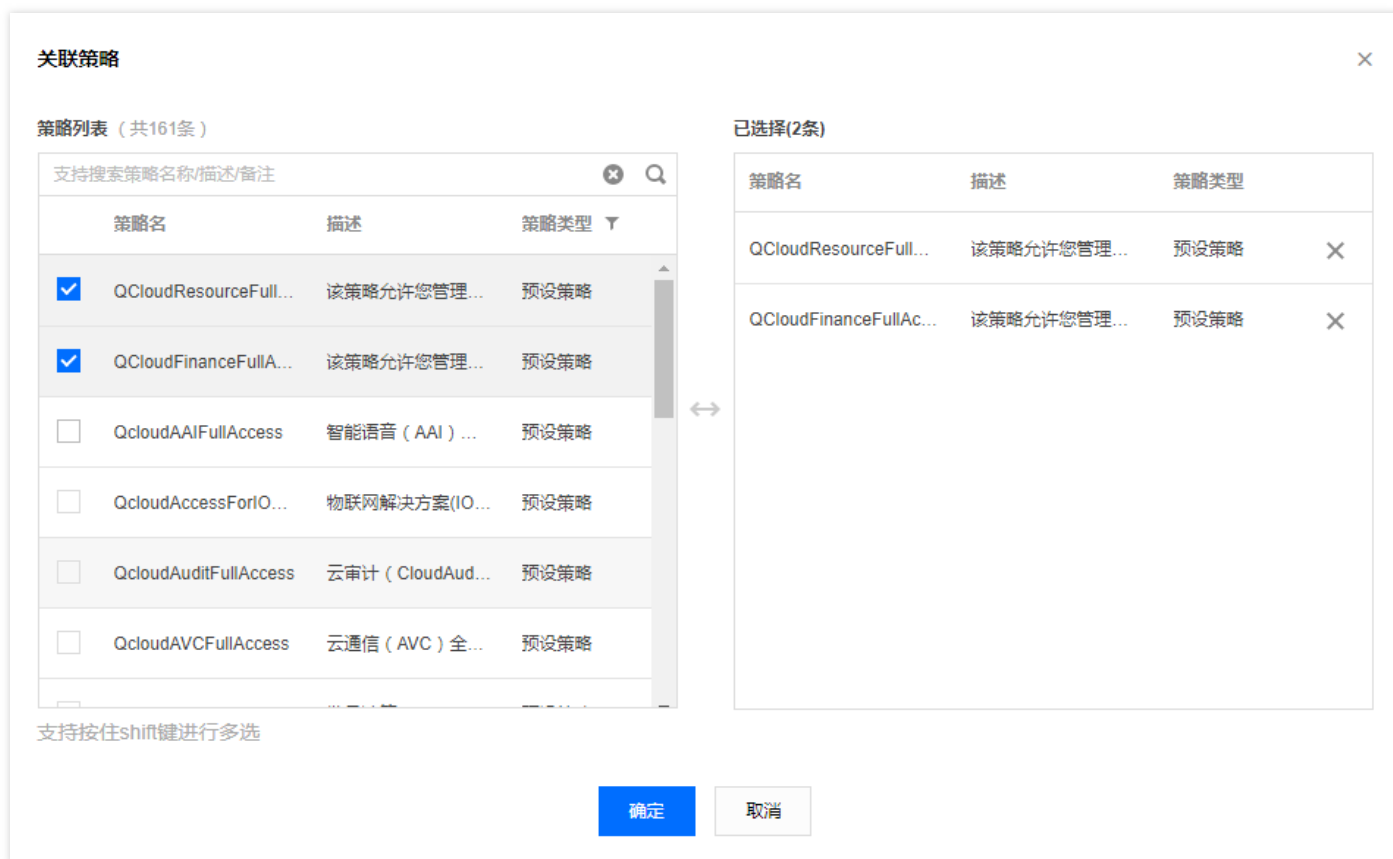
**已关联的策略(0)** 已添加的用户(2)

策略被关联后，该用户组内的所有用户都将获得策略所描述的权限

**关联策略**

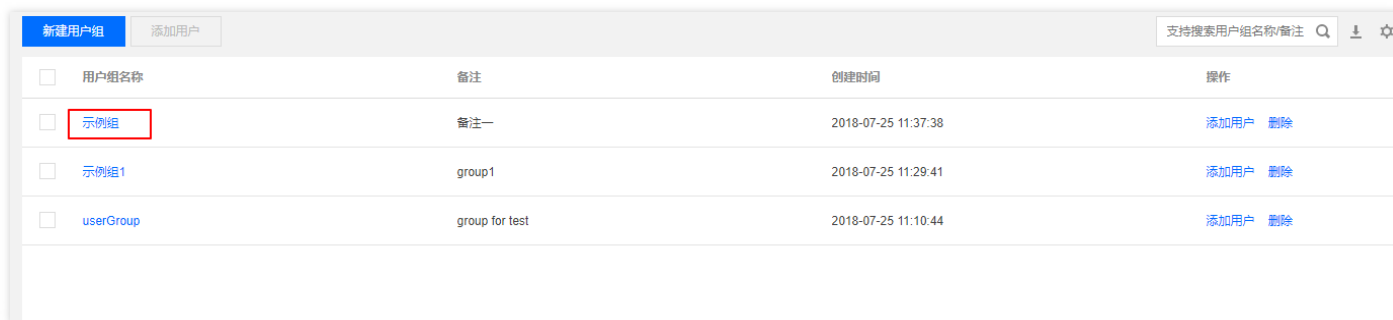
策略名	关联时间	操作
该用户组尚未添加任一策略		

3. 在弹出框勾选要添加的策略，单击【确定】，完成为用户组添加策略操作。



## 为用户组删除策略

1. 登录 [访问管理控制台](#)，在左侧导航单击进入【用户组管理】。单击用户组名称，进入用户组详情页。



2. 在列表中找到需要删除的策略，单击右侧的【解除】，如图所示：

**用户组信息** [编辑](#)

用户组名 示例组

备注 -

创建时间 2018-07-25 09:24:09

---

**已关联的策略(2)** 已添加的用户(2)

策略被关联后，该用户组内的所有用户都将获得策略所描述的权限

**关联策略**

策略名	关联时间	操作
<a href="#">AdministratorAccess</a>	2018-07-25 10:00:37	<a href="#">解除</a>
<a href="#">ReadOnlyAccess</a>	2018-07-25 10:00:37	<a href="#">解除</a>

是否确定为该用户组解除此策略？  
解除后该用户组内用户将无法获得该策略所描述的相关权限。

[确认解除](#) [取消](#)

---

共 2 项

每页显示行 20 « » 1/1 » »

3. 确认无误后单击【确认解除】，完成为用户组删除策略操作。

## 删除用户组

1. 登录 [访问管理控制台](#)，在左侧导航单击进入【用户组管理】。勾选要删除的用户组，单击【删除】，如图所示：



新建用户组		添加用户		支持搜索用户组名称/备注	
用户组名称	备注	创建时间	操作		
<input type="checkbox"/> 示例组	备注一	2018-07-25 11:37:38	添加用户	删除	
<input type="checkbox"/> 示例组1	group1	2018-0	删除该组将不会删除组内的用户，但组内用户将无法接收到该组的短信、邮件通知		
<input type="checkbox"/> userGroup	group for test	2018-0	确认删除	取消	

已选 0 项，共 3 项

每页显示行 20

2. 确认无误后单击【确认删除】，完成删除用户组操作。

# 角色管理

## 角色概述

最近更新时间：2018-08-31 14:42:22

角色类似于腾讯云用户，可以看作是腾讯云的“虚拟账号”，角色同样可被授予策略，拥有在腾讯云中允许执行和拒绝执行的权限。角色可以是任一腾讯云账号代入，并不是唯一地与某个账号绑定关联。角色没有关联的持久证书（密码或访问密钥），主账号仅在申请角色时需要使用持久证书，在用户担任某个角色时，则会动态创建临时证书并为用户进行相应访问时提供该临时证书，即可通过临时密钥签名调用腾讯云基础服务的开放 API 来访问用户的云资源。

能够申请担任角色的对象我们称它为角色载体。目前，腾讯云角色载体分为两类：腾讯云账号、已支持角色功能的产品服务。例如，当您要向您账号中的用户授予临时的资源访问权限，或者是向另一个腾讯云主账号内的用户授予您账户中的资源访问权限。再或者，您可能需要允许腾讯云产品服务对您的资源拥有访问权限，但不希望将长期密钥嵌入在产品服务中，因为这样存在难以轮换密钥以及被截取后泄露导致的安全问题。

# 基本概念

最近更新时间：2018-08-30 18:10:39

在您开始使用角色前需要了解一些基本术语，包括角色、服务角色、自定义角色、角色载体、权限策略等。更多术语介绍请参考 [词汇表](#)。

## 角色

拥有一组权限的虚拟身份。用于对角色载体授予腾讯云中服务、操作和资源的访问权限。这些权限附加到角色，而不附加到具体的用户或者用户组。

CAM 支持以下 2 种类型的角色：

- 服务（预设）角色：由腾讯云服务进行预定义的角色，服务角色需经过用户授权，服务即可通过扮演服务角色对用户资源进行访问操作。
- 自定义角色：由用户自行定义的角色，用户可以自由灵活地决定角色载体和角色权限。

角色可由以下用户使用：

- 可作为角色的腾讯云主账号
- 可作为角色的腾讯云子用户以及协作者

以及，角色还可由支持角色的腾讯云产品服务使用。查询腾讯云产品服务是否支持使用服务角色请参阅 [支持使用 CAM 的云服务](#)。

## 服务角色

服务角色是腾讯云各个产品服务直接提供的独特类型的 CAM 预设角色。服务角色的关联权限由相关产品服务预定义，一旦相关产品服务被您赋予服务角色，即该产品服务能够全权代表您调用服务角色权限范围内的其他腾讯云产品服务。服务角色可以让您更轻松地使用服务，因为在赋予角色的流程中您不必手动添加权限，只需要选择是否给该服务授予服务角色的相关权限。

给相关产品服务赋予服务角色的流程中，服务角色的相关权限和角色载体已经被定义，除非另外定义，否则仅该服务可以代入角色。服务角色的预定义包括角色名称、角色载体、权限策略。

## 自定义角色

自定义角色是用户自行对 CAM 角色进行定义。自定义角色的角色名称、角色载体以及角色权限均由用户决定。自定义角色可以让您更自由灵活地对您云上资源的访问使用权限进行分配。

被您授予角色的对象仅在使用角色的过程中能够获得相关权限，避免给予持久密钥可能带来的安全问题。

## 角色载体

角色载体是被允许承载角色权限的对象。您可以对角色进行角色载体编辑，添加或删除相应对象来允许或者拒绝其扮演角色来访问您的腾讯云资源。目前腾讯云支持的角色载体类型为：腾讯云账号和支持角色的腾讯云服务。查询腾讯云产品服务是否支持使用服务角色，请参阅 [支持使用 CAM 的云服务](#)。

## 权限策略

JSON 格式的权限文档。您可以在权限策略中定义角色可使用的操作和资源。该文档规则依赖于 CAM 策略语言规则。

## 信任策略

JSON 格式的权限文档。您可以在信任策略中定义可扮演角色的对象以及扮演角色时需满足的条件。该文档规则依赖于 CAM 策略语言规则。

# 创建角色

最近更新时间：2018-08-31 14:59:48

创建角色有两种方式：可以使用访问管理控制台或 CAM API。创建角色的具体步骤根据您是为腾讯云账号还是腾讯云产品服务创建角色而稍有不同。

## 通过控制台创建

### 为腾讯云主账号创建角色

1. 登录访问管理（CAM）控制台，进入 [角色管理](#) 页面。单击【新建角色】，进行【选择角色载体】，选择【腾讯云账号】作为角色载体。
2. 在【账户 ID】框中键入您允许其扮演角色来访问您腾讯云资源的主账户 ID，默认键入为您的主账户 ID。如果您想为其他腾讯云子账号授予角色，请参阅 [给予用户赋予角色扮演策略](#)。
3. 在策略列表内勾选您想要给当前创建角色赋予的策略为角色完成权限配置。
4. 输入您的角色名称，审阅您即将创建角色的相关信息，单击【完成】后即完成自定义角色创建。

### 为腾讯云产品服务创建角色

1. 登录访问管理（CAM）控制台，进入 [角色管理](#) 页面。单击【新建角色】，进行【选择角色载体】，选择【腾讯云产品服务】作为角色载体。查询腾讯云产品服务是否支持使用服务角色请参阅 [支持使用 CAM 的云服务](#)。
2. 在已支持角色功能的服务产品列表中勾选您需要的服务作为角色载体。
3. 在策略列表内勾选您想要给当前角色添加的策略为角色配置策略。
4. 输入您的角色名称，审阅您即将创建角色的相关信息，单击【完成】后即完成自定义角色创建。

## 通过 API 创建

腾讯云支持您使用 CAM API 进行新建角色，我们以一个典型案例让您轻松了解如何使用 API 来创建角色。

假设如下场景，公司 A 有一个运维工程师的职位，并且希望将该职位外包给公司 B，该职位需要操作公司 A 广州地域所有云服务器资源。

公司 A 企业账号 CompanyExampleA（ownerUin 为 12345），创建一个角色并将角色载体设置为公司 B 的企业账号 CompanyExampleB（ownerUin 为 67890）。

1. 公司 A 企业账号 CompanyExampleA（ownerUin 为 12345）调用 CreateRole 接口创建一个 roleName 为 DevOpsRole 的角色，policyDocument（角色信任策略）参数设为

```
{
  "version": "2.0",
  "statement": [{
    "action": "name/sts:AssumeRole",
    "effect": "allow",
    "principal": {
      "qcs": ["qcs::cam::uin/67890:root"]
    }
  }]
}
```

2. 公司 A 企业账号 CompanyExampleA ( ownerUin 为 12345 ) 需要为刚才创建的角色附加权限。

i. 公司 A 企业账号 CompanyExampleA ( ownerUin 为 12345 ) 创建策略 DevOpsPolicy , 策略语法如下 :

```
{
  "version": "2.0",
  "statement": [{
    "effect": "allow",
    "action": "cvm:*",
    "resource": "qcs::cvm:ap-guangzhou::*"
  }]
}
```

ii. 公司 A 企业账号 CompanyExampleA ( ownerUin 为 12345 ) 调用 [AttachRolePolicy](#) 将 step1 中创建的策略绑定到角色 DevOpsRole , 入参 policyName=DevOpsPolicy , roleName=DevOpsRole。

经过上面的步骤, 公司 A 企业账号 CompanyExampleA ( ownerUin 为 12345 ) 完成了角色的创建和授权。

# 修改角色

最近更新时间：2018-08-30 17:38:54

## 编辑角色关联策略

1. 登录访问管理（CAM）控制台，进入 [角色管理](#) 页面。
2. 在您账户的角色列表中，单击您要修改的角色名称，进入相应角色详情页。
3. 在角色详情页选择查看【已授权策略】，单击【关联策略】在策略列表内勾选您想要给当前角色添加的策略，单击【确定】完成策略关联。

## 编辑角色载体

1. 登录访问管理（CAM）控制台，进入 [角色管理](#) 页面。
2. 在您账户的角色列表中，单击您要修改的角色名称，进入相应角色详情页。
3. 在角色详情页选择查看【角色载体】，单击【编辑角色载体】：
  - 针对账号的修改：单击【添加账号】添加账号（仅可输入主账号）作为当前角色的角色载体，或者删除相应的账号标签将其从角色载体内移除。
  - 针对服务的修改：勾选产品服务作为当前角色的角色载体，或者取消勾选相应的产品服务将其从角色载体内移除。

# 使用角色

最近更新时间：2018-09-03 10:15:19

腾讯云支持您使用 CAM API 进行使用角色，我们以一个典型案例让您轻松了解如何使用 API 来使用角色。

假设如下场景，公司 A 有一个运维工程师的职位，并且希望将该职位外包给公司 B，该职位需要操作公司 A 广州地域所有云服务器资源。

公司 A 企业账号 CompanyExampleA ( ownerUin 为 12345 )，创建一个角色并将角色载体设置为公司 B 的企业账号 CompanyExampleB ( ownerUin 为 67890 )。公司 A ( CompanyExampleA ) 调用 CreateRole 接口创建一个角色名称 ( roleName ) 为 DevOpsRole 的角色，公司 A 企业账号 CompanyExampleA 为创建的角色附加了权限。上述步骤请参阅 [通过 API 创建](#)。

企业账号 CompanyExampleB 被授权这个角色后，希望由子账号 DevB 来完成这项工作。公司 B ( CompanyExampleB ) 授权 DevB 可以申请扮演 CompanyExampleA 的角色 DevOpsRole。上述步骤请参阅 [为子账号赋予扮演角色策略](#)。

完成上述创建、授权角色，并为子账号赋予扮演角色策略的操作后，子账号 DevB 即可开始使用角色。

1. 需要调用 [AssumeRole](#) 接口申请角色 DevOpsRole 的临时凭证，输入参数如下：

```
roleArn=qcs::cam::uin/12345:roleName/DevOpsRole ,
roleSessionName=DevBAssumeTheRole ,
durationSeconds=7200
```

2. 该接口成功返回了结果如下：

```
{
  "credentials": {
    "sessionToken": "5e776c4216ff4d31a7c74fe194a978a3ff2a42864",
    "tmpSecretId": "AKIDcAZnqgar9ByWq6m7ucln8LNEuY2MkPCI",
    "tmpSecretKey": "VpxrX0IMCpHXWL0Wr3KQNCqJix1uhMqD"
  },
  "expiredTime": 1506433269,
  "expiration": "2018-09-26T13:41:09Z"
}
```

3. DevB 得到了角色的临时凭证后便可以在凭证有效期内执行权限范围内的操作。比如，通过 API 查看云服务器列表，在调用 [DescribeInstances](#) 接口时，将 API 密钥 SecretId 和 SecretKey 的值替换为 tmpSecretId 和 tmpSecretKey 的值，同时，将 [公共参数](#) 中的 Token 设置为 sessionToken 的值。公司 B ( CompanyExampleB ) 也可以直接申请角色的临时凭证操作公司 A ( CompanyExampleA ) 的资源。



**注意：**

公司 A ( CompanyExampleA ) 想终止对公司 B ( CompanyExampleB ) 的授权，删除掉角色 DevOpsRole 即可。

# 删除角色

最近更新时间：2018-08-30 18:23:25

当您不再需要角色时，您可以选择删除角色。操作步骤如下：

## 注意：

当删除的角色是 **服务角色** 时，会一并删除与角色绑定的授权信息。即作为角色载体的产品服务或者账号均无法再使用该角色。

1. 登录访问管理（CAM）控制台，进入 [角色管理](#) 页面。
2. 在您账户的角色列表中，选择您要删除的角色，在【操作】里单击【删除】。
3. 删除服务角色时，需要您再次确认是否删除相关角色。删除角色会一并删除与角色绑定的授权信息，单击【确定】即可删除角色，作为该角色的角色载体的产品服务或者账号均无法再使用该角色。

# 为子账号赋予扮演角色策略

最近更新时间：2018-08-31 14:55:45

作为角色载体的主账号可以允许其子账号对角色进行扮演，这里我们通过一个案例让您轻松了解如何为子账号创建并赋予扮演角色的策略。

假设如下场景，公司 A 有一个运维工程师的职位，并且希望将该职位外包给公司 B，该职位需要操作公司 A 广州地域所有云服务器资源。

公司 A 企业账号 CompanyExampleA ( ownerUin 为 12345 )，创建一个角色并将角色载体设置为公司 B 的企业账号 CompanyExampleB ( ownerUin 为 67890 )。公司 A ( CompanyExampleA ) 调用 CreateRole 接口创建一个角色名称 ( roleName ) 为 DevOpsRole 的角色，公司 A 企业账号 CompanyExampleA 为创建的角色 DevOpsRole 附加了权限。上述步骤请参阅 [通过 API 创建](#)。

公司 B 企业账号 ( CompanyExampleB ) 被授权这个角色后，希望由子账号 DevB 来完成这项工作。公司 B ( CompanyExampleB ) 需要授权子账号 DevB 可以申请扮演公司 A ( CompanyExampleA ) 的角色 DevOpsRole：

1. 创建策略 AssumeRole，示例如下：

```
{
  "version": "2.0",
  "statement": [{
    "effect": "allow",
    "action": ["name/sts:AssumeRole"],
    "resource": ["qcs::cam::uin/12345:roleName/DevOpsRole"]
  }]
}
```

2. 将该策略授权给子账号 DevB。子账号即被赋予了扮演角色 DevOpsRole 的权限。

拥有扮演角色的权限后如何使用角色，请参阅 [使用角色](#)。

# 策略管理

## 权限

最近更新时间：2017-08-24 16:34:49

权限是描述在某些条件下允许或拒绝执行某些操作访问某些资源。

默认情况下，根账号是资源的拥有者，拥有其名下所有资源的访问权限；子账号没有任何资源的访问权限；资源创建者不自动拥有所创建资源的访问权限，需要资源拥有者进行授权。

策略是定义和描述一条或多条权限的语法规则。CAM支持两种类型的策略，预设策略和自定义策略。预设策略是由腾讯云创建和管理的一些常见的权限集合，如超级管理员、云资源管理员等，这类策略只读不可写。自定义策略是由用户创建的更精细化的描述对资源管理的权限集合。预设策略不能具体描述某个资源，粒度较粗，而自定义策略可以灵活的满足用户的差异化权限管理需求。

通过给用户或者用户组绑定一个或多个策略完成授权。被授权的策略既可以是预设策略也可以是自定义策略。

# 策略

最近更新时间：2018-08-01 20:00:03

## 概述

策略是用于定义和描述一条或多条权限的语法规则。腾讯云的策略类型分为预设策略和自定义策略。CAM 从不同角度切入，为您提供多种方法来创建和管理策略。若您需要向 CAM 用户或组添加权限，您可以直接关联预设策略，或创建自定义策略后将自定义策略关联到 CAM 用户或组。每个策略允许包含多个权限，同时您可以将多个策略附加到一个 CAM 用户或组。

## 预设策略

预设策略由腾讯云创建和管理，是被用户高频使用的一些常见权限集合，如资源全读写权限等。操作对象范围广，操作粒度粗。预设策略为系统预设，不可被用户编辑。

在控制台 [策略管理](#) 页面，您可以在搜索框内输入策略名、系统自带的策略描述或您已编辑的备注，快速定位相关策略。

## 自定义策略

由用户创建的策略，允许作细粒度的权限划分。例如为某数据库管理员关联一条策略，使其有权管理云数据库实例，而无权管理云服务器实例。自定义策略根据创建方式的不同分为按策略生成器创建的策略、按业务权限创建的策略、按语法创建的策略和按标签授权的策略：

- 按策略生成器创建的策略，通过从策略向导中选择服务和操作，并定义资源，自动生成策略语法，简单灵活，优先推荐使用；
- 按业务权限创建的策略，由用户设置，权限粒度可由业务接入时控制，解决对权限划分有一定要求，但并不复杂的用户诉求；
- 按语法创建的策略，由用户设置，权限粒度灵活，由用户把控，解决对权限精细划分有较高要求的用户诉求；
- 按标签授权的策略，将具有一类标签属性的资源快速授权给用户或用户组。

## 创建自定义策略

### 按策略生成器创建

1. 登录腾讯云控制台，进入 [策略管理](#) 页面，单击【新建自定义策略】>【按策略生成器创建】，进入创建页面。
2. 选择服务和操作，填写资源描述（参考文档：[资源描述方式说明](#)），完成后单击【添加声明】>【下一步】。

- 部分服务的操作无需关联对象，则不需要填写资源描述。
- 一条策略中可以添加多条声明。

3. 单击【创建策略】即可。其中策略名称和策略内容由控制台自动生成：
  - 策略名称默认为 "policygen"，后缀数字根据创建日期生成。您可进行自定义。
  - 策略内容与第 2 步的服务和操作对应，用户可根据实际需求进行修改。

选择服务和操作 > 编辑策略

---

策略名称 \*

备注

编辑策略内容

```
1 {
2   "version": "2.0",
3   "statement": [
4     {
5       "effect": "allow",
6       "action": [
7         "name/cas:AbortVaultLock"
8       ],
9       "resource": [
10        "*"
11      ]
12    },
13    {
14      "effect": "allow",
15      "action": [
16        "name/consoleSMS:*"
```

[策略语法说明](#) [支持业务列表](#)

上一步 创建策略

## 按业务权限创建

1. 登录腾讯云控制台，进入 [策略管理](#) 页面，单击【新建自定义策略】>【按业务权限创建】，进入创建页面。

2. 选择服务类型并为策略命名，单击【下一步】。

1 配置服务类型 >
2 开启权限 >
3 关联对象

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9条)

- 服务类型
- 内容分发网络
- 项目管理
- 互动直播
- 云直播
- 队列模型
- 主题模型
- 短信

**已选择(1条)**

服务类型

项目管理 ✕

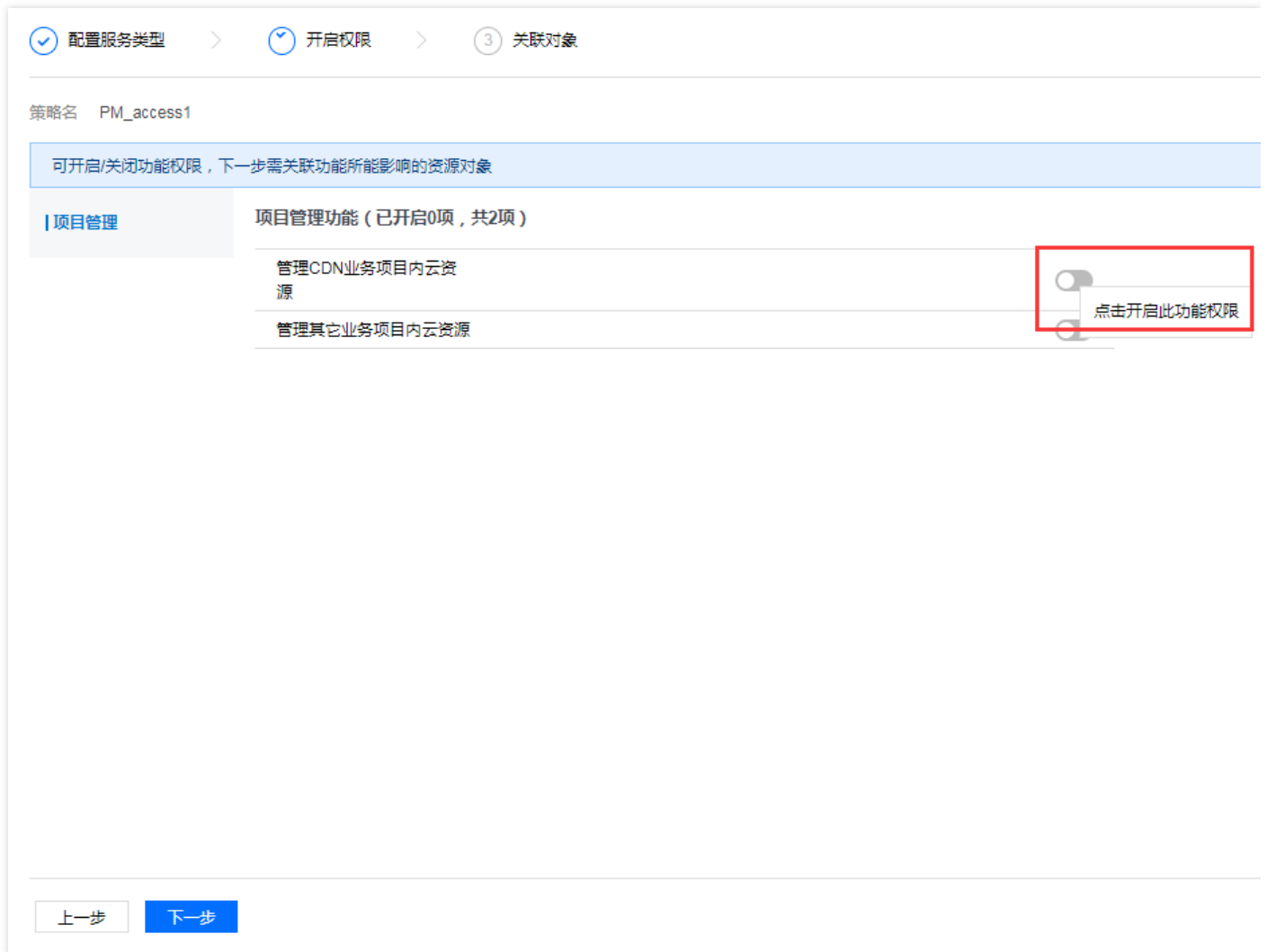
↔

支持按住shift键进行多选

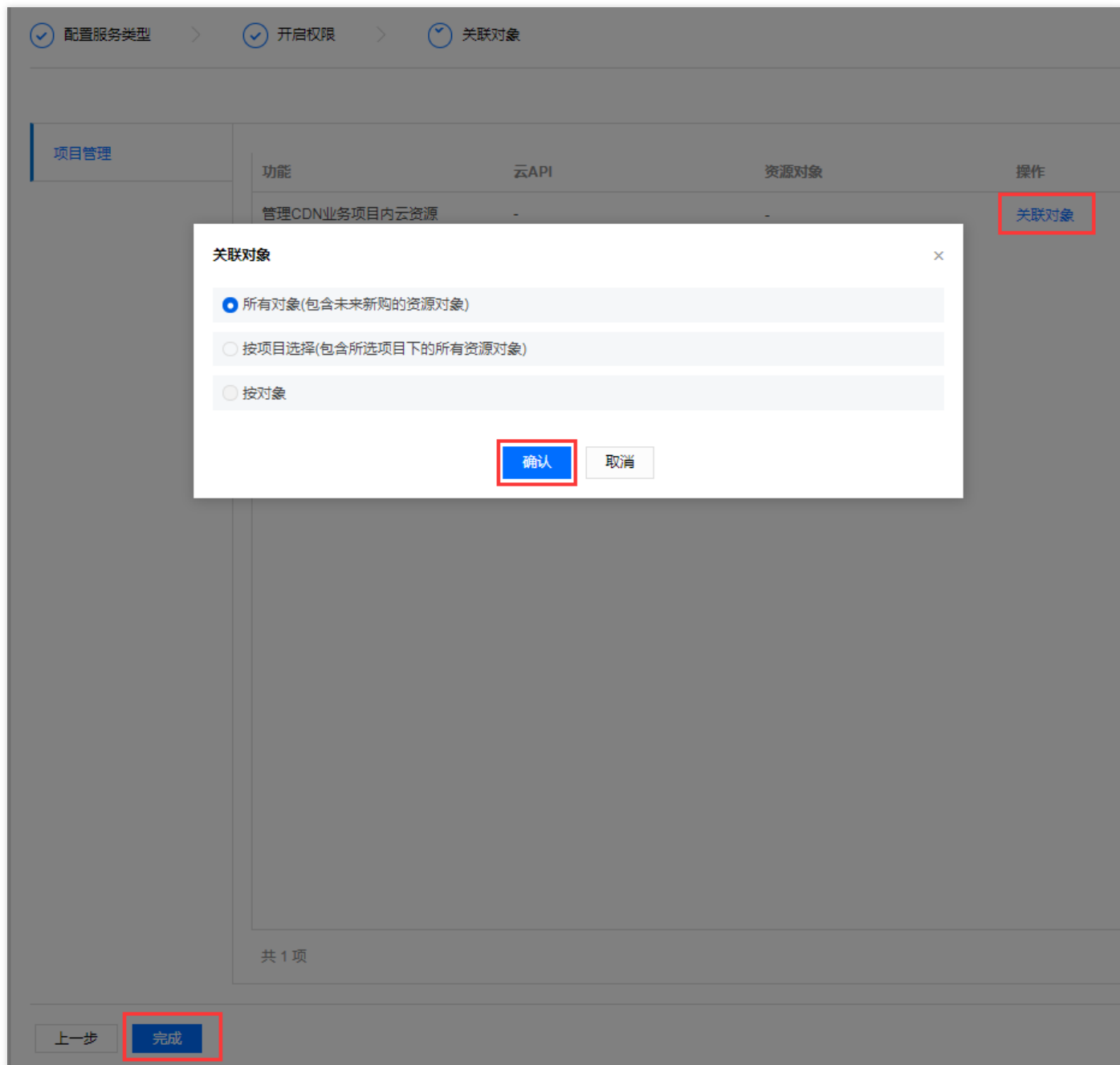
下一步



3. 将需要开启的功能权限开关置为 **开启状态**，并单击【下一步】。

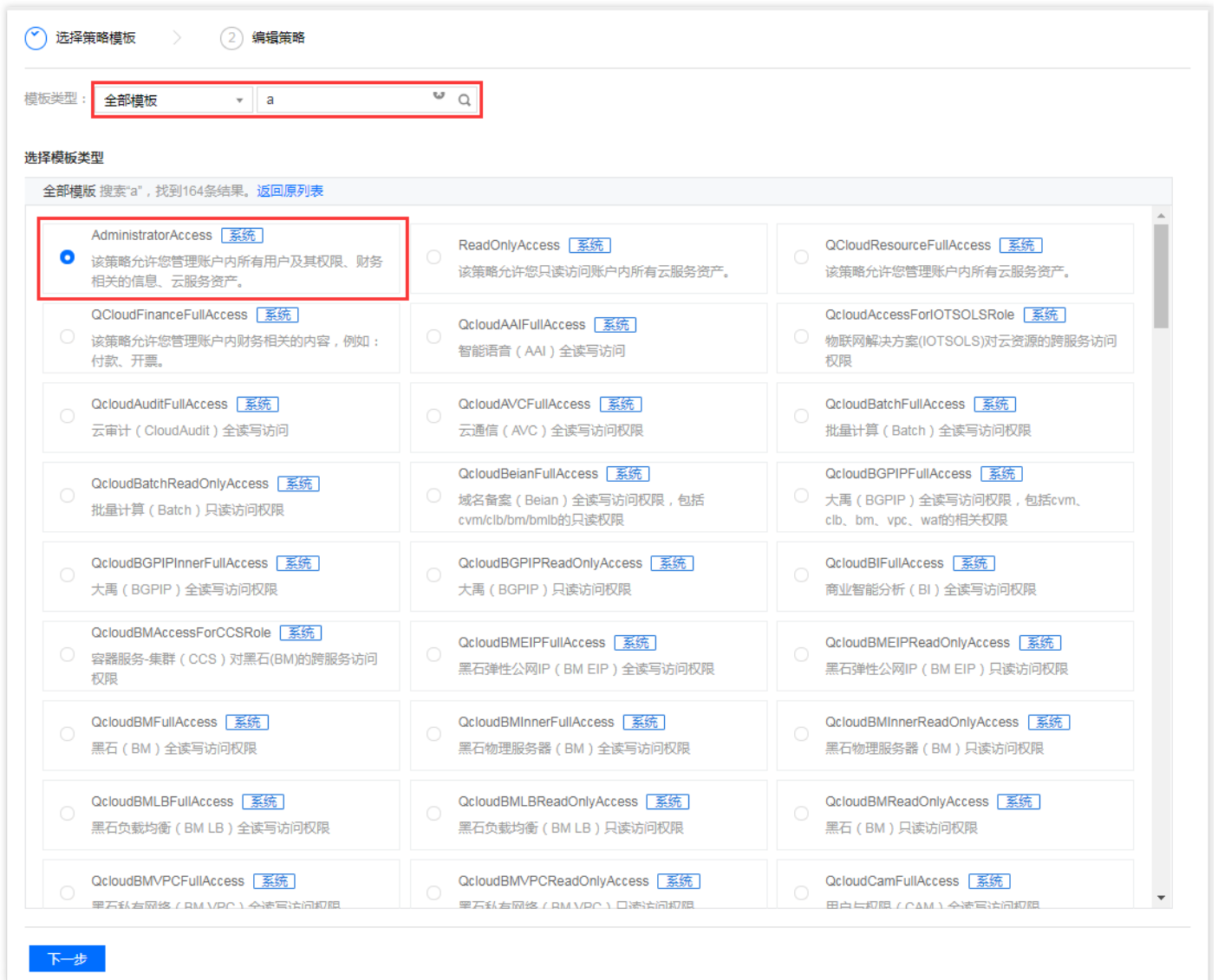


4. 单击【关联对象】，选择要关联的对象，单击【确认】>【完成】。



## 按策略语法创建

1. 登录腾讯云控制台，进入 [策略管理](#) 页面，单击【新建自定义策略】>【按策略语法创建】，进入创建页面。
2. 选择模版类型，可输入关键字进行搜索（如模版类型为全部模版，关键字为 a ），选择 AdministratorAccess 模版，单击【下一步】。



3. 编辑策略内容，单击【创建策略】即可。其中默认的策略名称和策略内容由控制台自动生成，策略名称默认为 "policygen"，后缀数字根据创建日期生成。

选择策略模板 > 编辑策略

策略名称\*

备注

编辑策略内容

```
1 {  
2   "version": "2.0",  
3   "statement": [  
4     {  
5       "effect": "allow",  
6       "action": "*",  
7       "resource": "*"   
8     }  
9   ]  
10 }
```

[策略语法说明](#) [支持业务列表](#)

## 按标签授权

1. 登录腾讯云控制台，进入 [策略管理](#) 页面，单击【新建自定义策略】>【按标签授权】，进入创建页面。

2. 选择各选项信息（如下图），单击【下一步】。

赋予用户	请选择
和用户组	请选择
在标签键 ①	请选择
且具有标签值 ①	请选择
的资源	管理权限

下一步

3. 策略内容可保持为默认，也可根据实际需求编辑策略内容（详见 [策略语法说明](#) 和 [业务支持列表](#)），然后单击【完成】即可。

1 标签策略生成器 >
2 检查并完成

策略名称

将此权限授权给用户

将此权限授权给用户组

**编辑策略内容**

```

1  [
2     "version": "2.0",
3     "statement": [
4         {
5             "effect": "allow",
6             "action": "*",
7             "resource": "*",
8             "condition": {
9                 "for_any_value:string_equal": {
10                  "qcs:tag": [
11                      "test&云"
12                  ]
13              }
14          }
15      ]
16  ]
                    
```

[策略语法说明](#) [支持业务列表](#)

上一步
完成

# 授权管理

最近更新时间：2018-07-23 12:15:03

用户或者用户组可以绑定一个或多个策略完成授权。被授权的策略既可以是预设策略也可以是自定义策略。授权方式可以通过在策略页面选择用户或者在用户页面选择策略来完成。

## 通过策略关联用户/用户组：

### 预设策略关联用户

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏中的【策略管理】，策略管理方式默认为【预设策略】，选择要使用的策略，单击【关联用户/组】。

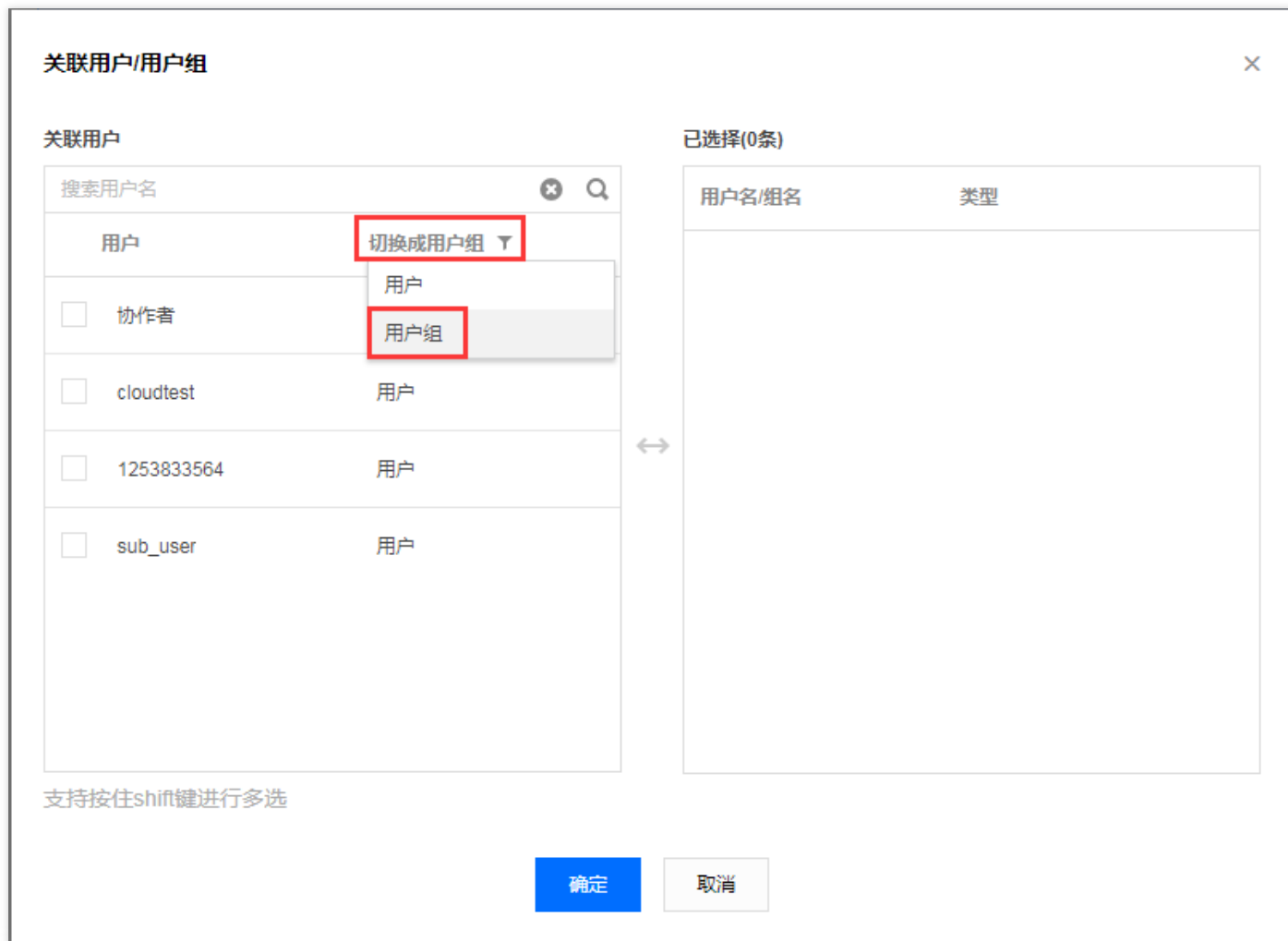


3. 选择要关联的用户，单击【确定】完成关联。

### 预设策略关联用户组

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏中的【策略管理】，策略管理方式默认为【预设策略】，选择要使用的策略，单击【关联用户/组】。

3. 单击【切换成用户组】，在显示的下拉栏中选择【用户组】。



4. 选择要关联的用户组，单击【确定】完成关联。

## 自定义策略关联用户

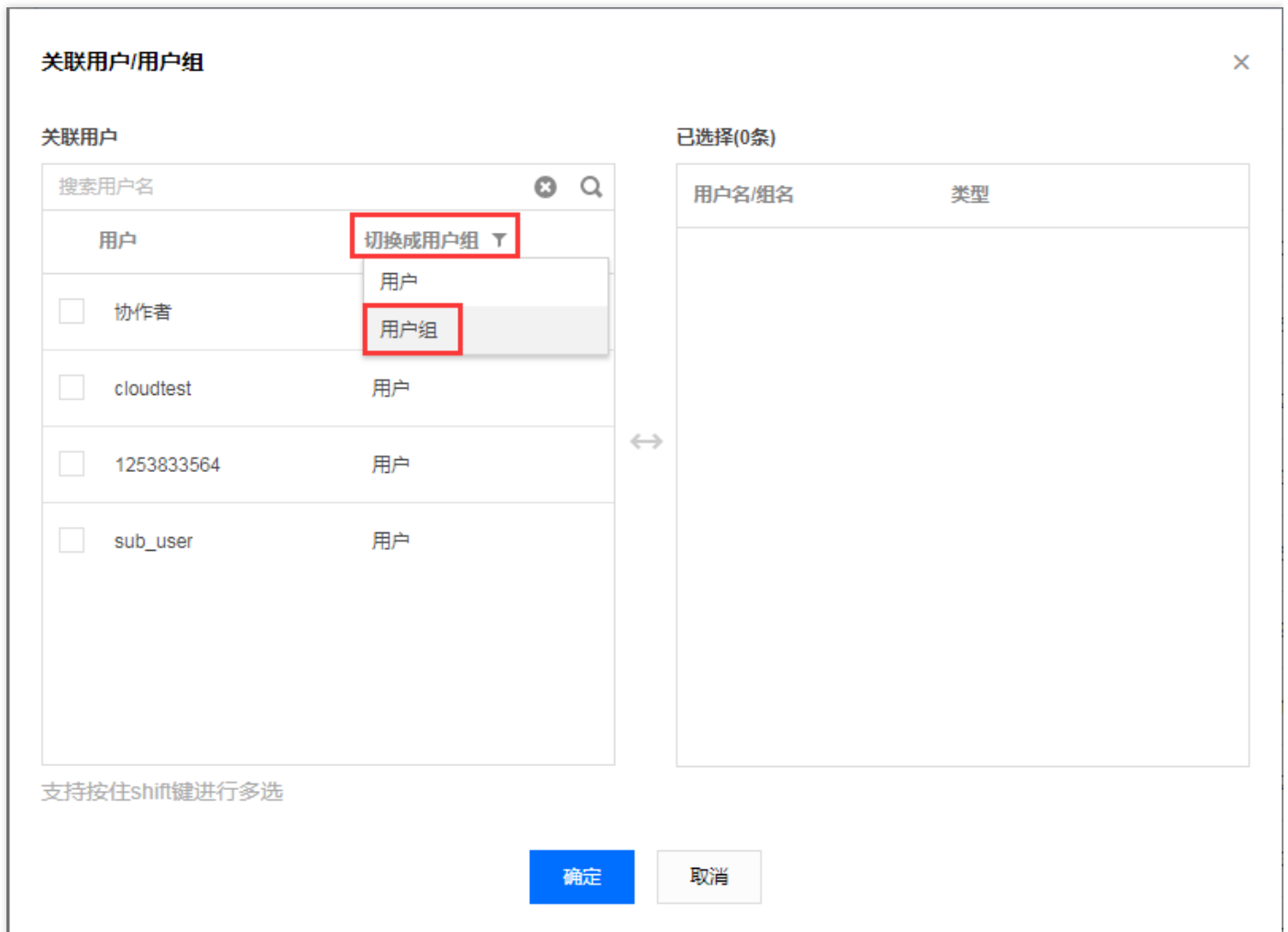
1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏中的【策略管理】，策略管理方式默认为【预设策略】，筛选 **自定义策略**，选择要使用的策略，单击【关联用户/组】。
3. 选择要关联的用户，单击【确定】完成关联。

## 自定义策略关联用户组

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。



- 单击左侧导航栏中的【策略管理】，策略管理方式默认为【预设策略】，筛选 **自定义策略**，选择要使用的策略，单击【关联用户/组】。
- 单击【切换成用户组】，在显示的下拉栏中选择【用户组】。



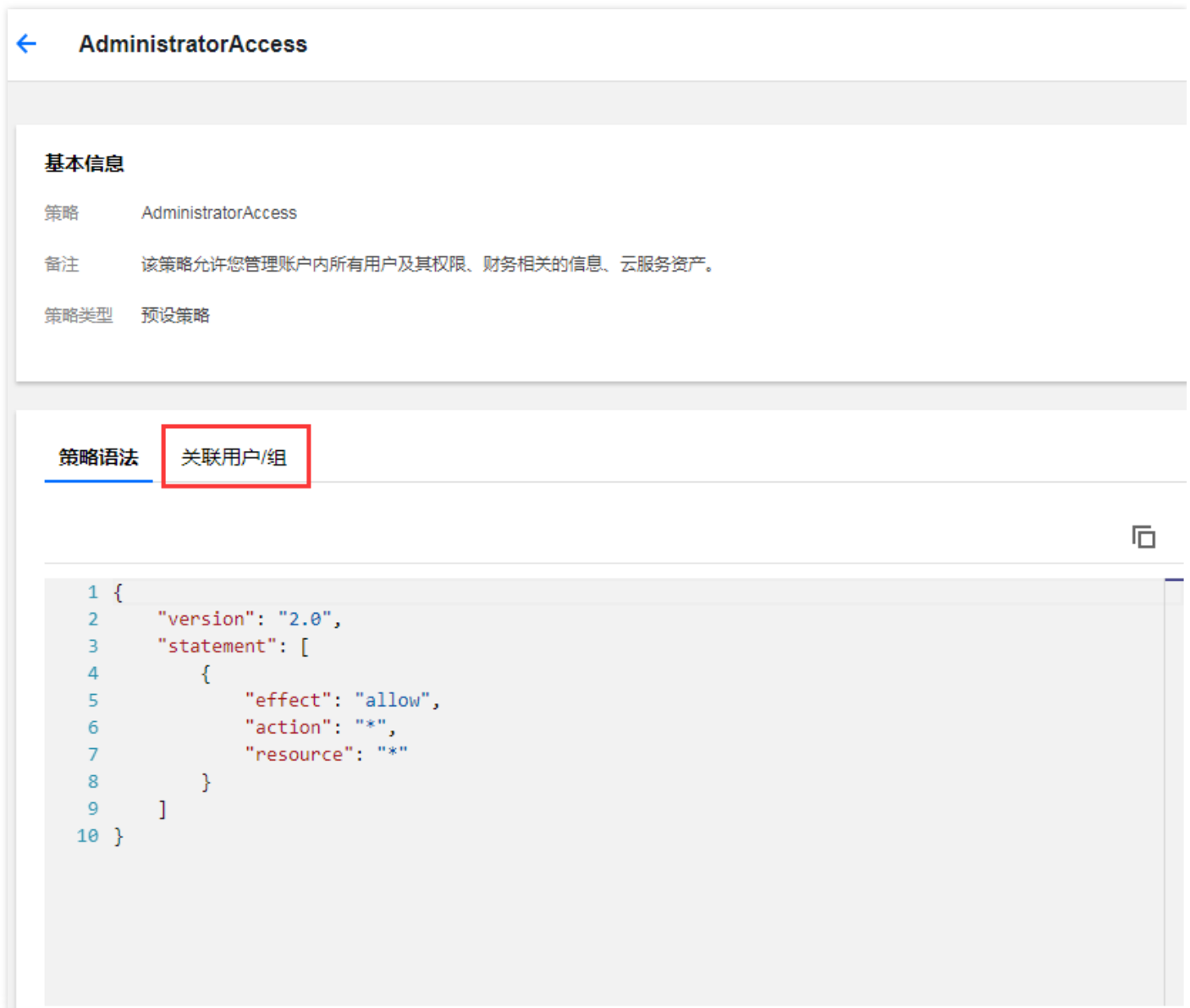
- 选择要关联的用户组，单击【确定】完成关联。

## 通过策略解绑用户/用户组

### 预设策略解绑

- 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
- 单击左侧导航栏中的【策略管理】，策略管理方式默认为【预设策略】，选择要使用的策略，单击该策略的名称。

3. 进入策略详情页面，单击下方【关联用户/组】。



4. 选择要进行操作的用户或者用户组，单击【解除用户/用户组】。

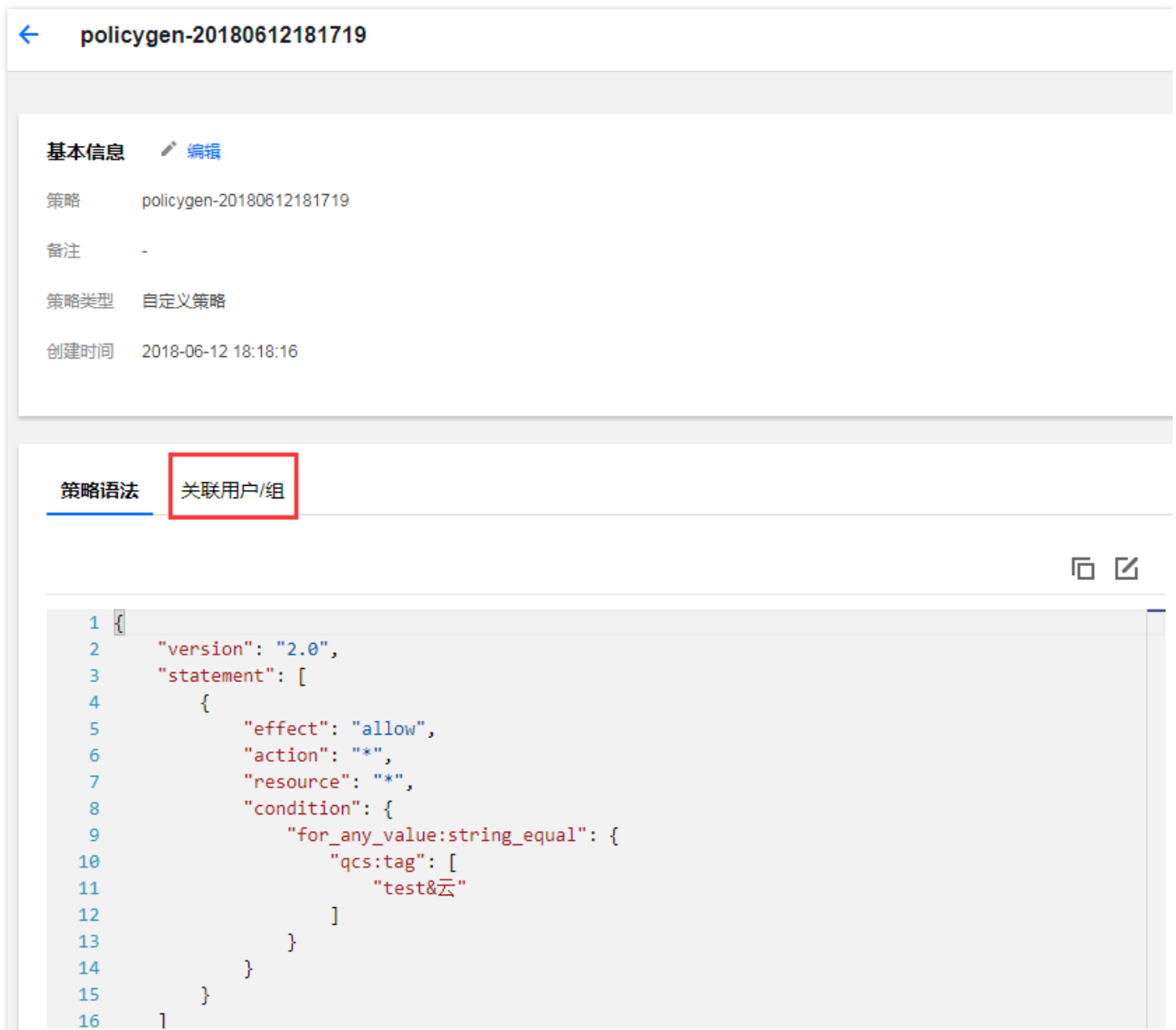
5. 在弹出的提示框中，单击【确认】解除绑定。

## 自定义策略解绑

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。

2. 单击左侧导航栏中的【策略管理】，筛选 **自定义策略**，选择要使用的策略，单击该策略的名称。

3. 进入策略详情页，单击下方【关联用户/组】。



4. 选择要进行解绑的用户或者用户组，单击【解除用户/用户组】。

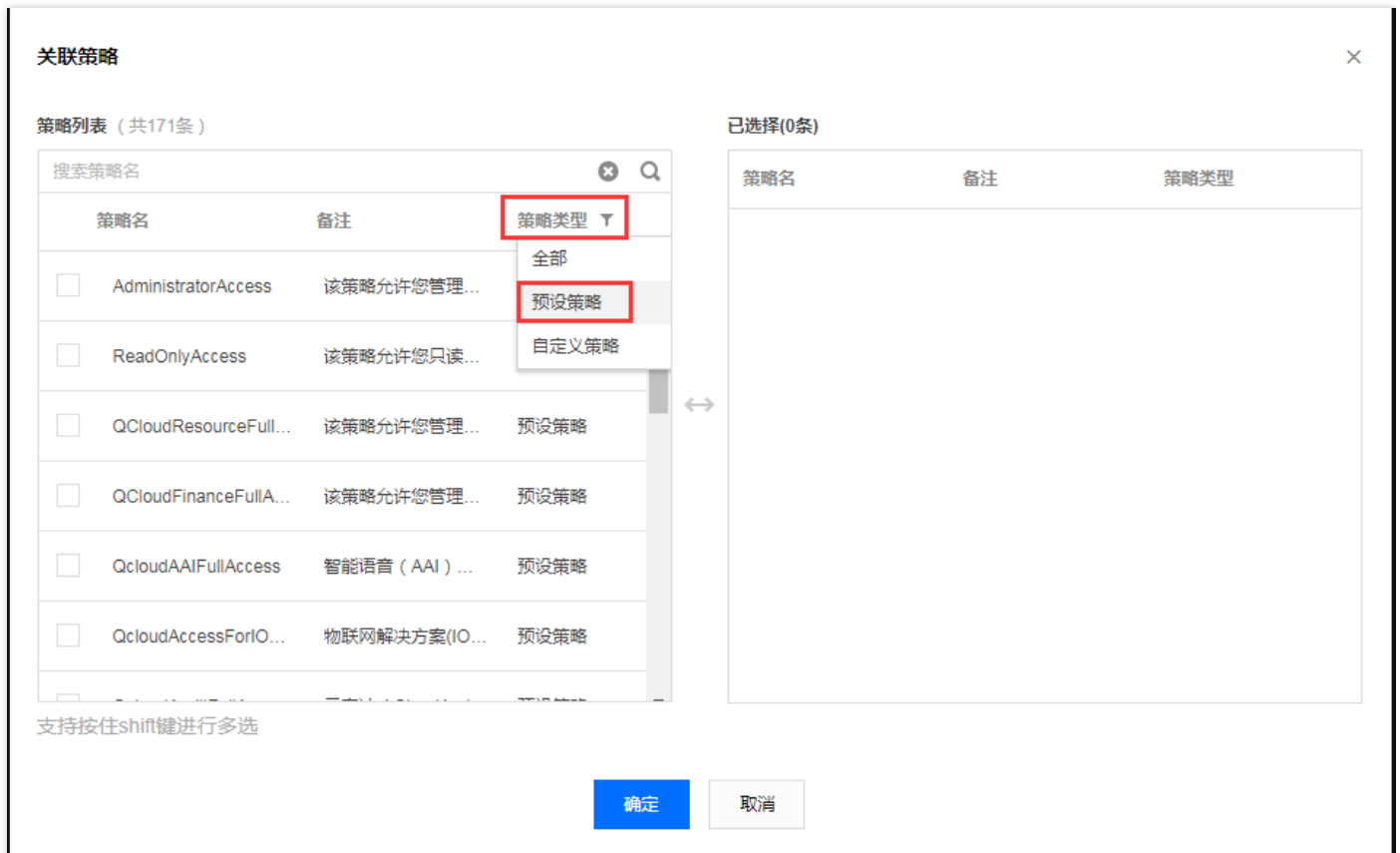
5. 在弹出的提示框中，单击【确认】解除绑定。

## 通过用户/用户组关联策略：

### 用户关联预设策略

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。

2. 单击左侧导航栏【用户管理】> 要操作的用户名称。
3. 进入用户详情页，单击下方的【关联策略】按钮。
4. 筛选 **策略类型**，选择 **预设策略**。

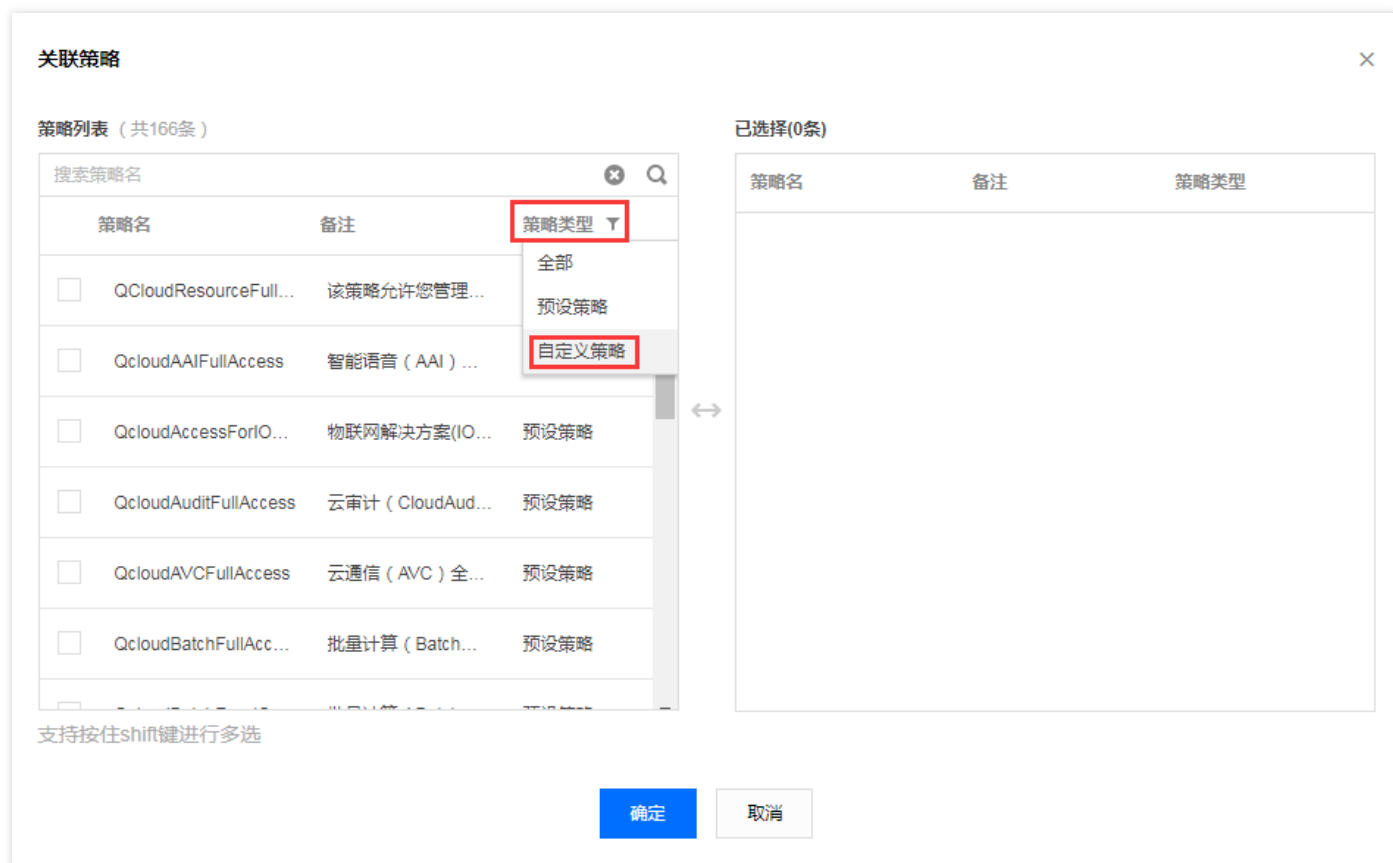


5. 选择要关联的预设策略，单击【确定】完成关联。

## 用户关联自定义策略

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏【用户管理】> 要操作的用户名称。
3. 进入用户详情页，单击下方的【关联策略】按钮。

#### 4. 筛选 策略类型，选择 自定义策略。

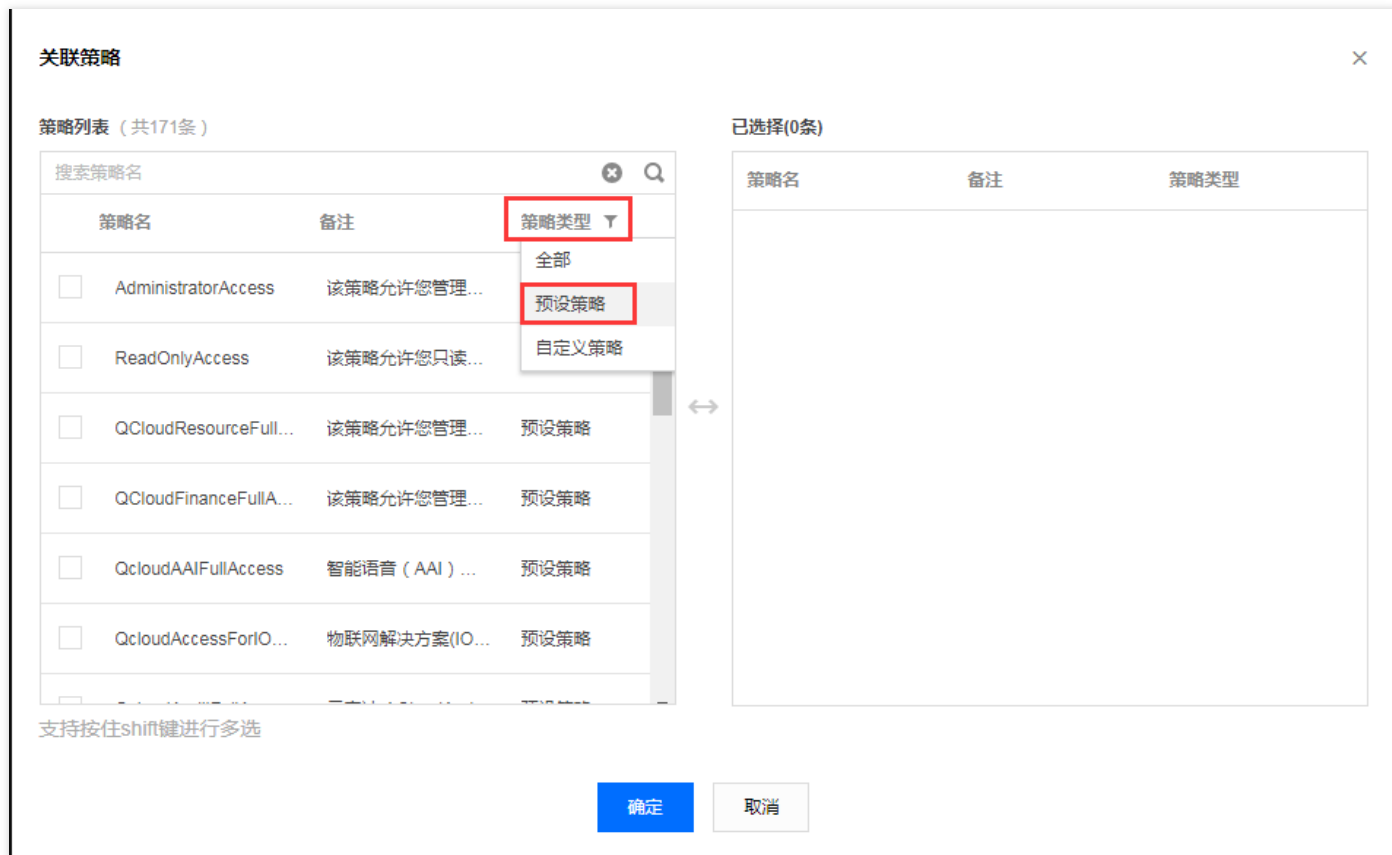


#### 5. 选择要关联的自定义策略，单击【确定】完成关联。

### 用户组关联预设策略

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏【用户组管理】> 要操作的用户名称。
3. 进入用户组详情页，单击下方的【关联策略】按钮。

4. 筛选 **策略类型**，选择 **预设策略**。

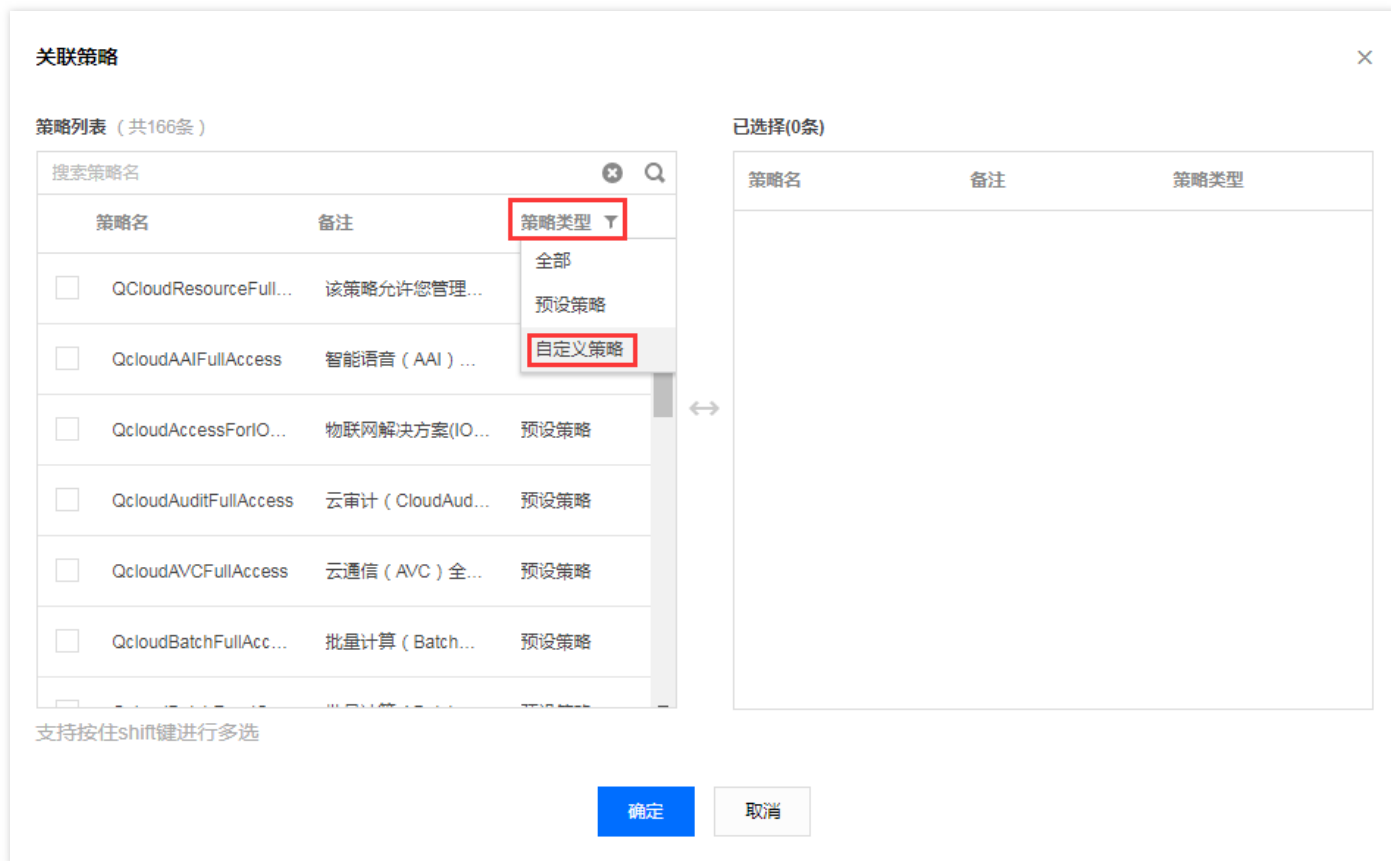


5. 选择要关联的自定义策略，单击【确定】完成关联。

### 用户组关联自定义策略

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏【用户组管理】> 要操作的用户名称。
3. 进入用户组详情页，单击下方的【关联策略】按钮。

#### 4. 筛选 策略类型，选择 自定义策略。



#### 5. 选择要关联的自定义策略，单击【确定】。

## 通过用户/用户组解绑策略

### 用户解绑策略

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏【用户管理】> 要操作的用户名称。
3. 进入用户详情页，选择要解除的策略，单击【解除】。
4. 在弹出来的提示框中，单击【确认解除】解除绑定。

### 用户组解绑策略

1. 登录 [腾讯云控制台](#)，鼠标移动到您的账号昵称处，此时会弹出下拉列表，单击列表选项中的【访问管理】进入访问管理控制台。或者在控制台总览页直接搜索【访问管理】进入访问管理控制台。
2. 单击左侧导航栏【用户组管理】> 要操作的用户名称。
3. 进入用户组详情页，选择要解除的策略，单击【解除】。
4. 在弹出来的提示框中，单击【确认解除】解除绑定。

# 授权操作指南

最近更新时间：2018-07-23 12:16:02

## 限制访问场景

当您访问控制台进行相关云产品操作时，有可能会遇到提示“您没有操作相关资源的权限”，如下图所示：



这种情况，是由于您所登录的子用户或协作者，没有被授予相关的权限，需要主账号授予对应的权限后，才能进行信息查看或者相关操作。

## 授权步骤

### 1. 确认您需要被授予的权限。

在失败信息描述中，指明了您不具备的权限。如上图所示，您不具备 cloudaudit（云审计）这个产品下 LookupEvents 这个接口的权限，导致您无法查看页面上的内容。

### 2. 使用主账号或者具有管理权限的子用户授予相关权限给对应的子用户或协作者。

- i. 登录 [访问管理控制台](#)，进入 **策略管理** 页面，单击【新建自定义策略】>【按策略生成器创建】，授予特定接口权限（如 LookupEvents）。
- ii. 在策略管理页面，查询对应产品的系统策略，将预设系统策略授予子用户，例如本示例中的云审计相关的预设策略。



策略管理

用户或者用户组与策略关联后，即可获得策略所描述的操作权限。

新建自定义策略

删除

全部策略

云审计

<input type="checkbox"/>	策略名	备注	服务类型	创建时间	操作
--------------------------	-----	----	------	------	----

搜索“云审计”，找到1条结果。[返回原列表](#)

<input type="checkbox"/>	<a href="#">QcloudAuditFullAccess</a>	云审计 ( CloudAudit ) 全读写访问	云审计	2017-11-20 10:26:17	<a href="#">关联用户/组</a>
--------------------------	---------------------------------------	--------------------------	-----	---------------------	------------------------

# 策略语法

## 元素参考

最近更新时间：2018-03-22 09:29:20

策略(policy)由若干元素构成，用来描述授权的具体信息。核心元素包括委托人(principal)、操作(action)、资源(resource)、生效条件(condition)以及效力(effect)。元素保留字仅支持小写。它们在描述上没有顺序要求。对于策略没有特定条件约束的情况，condition 元素是可选项。在控制台中不允许写入 principal 元素，仅支持在策略管理 API 中和策略语法相关的参数中使用 principal。

### 1.版本(version)

描述策略语法版本。该元素是必填项。目前仅允许值为"2.0"。

### 2.委托人(principal)

描述策略授权的实体。包括用户（开发商、子账号、匿名用户）、用户组，未来会包括角色、联合身份用户等更多实体。仅支持在策略管理API中策略语法相关的参数中使用该元素。

### 3.语句(statement)

描述一条或多条权限的详细信息。该元素包括 action、resource、condition、effect 等多个其他元素的权限或权限集合。一条策略有且仅有一个statement 元素。

### 4.操作(action)

描述允许或拒绝的操作。操作可以是 API（以name前缀描述）或者功能集（一组特定的 API，以 permid 前缀描述）。该元素是必填项。

### 5.资源(resource)

描述授权的具体数据。资源是用六段式描述。每款产品的资源定义详情会有所区别。有关如何指定资源的信息，请参阅您编写的资源声明所对应的产品文档。该元素是必填项。

### 6.生效条件(condition)

描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息。有些服务允许您在条件中指定其他值。该元素是非必填项。

### 7.效力(effect)

描述声明产生的结果是“允许”还是“显式拒绝”。包括 allow(允许)和deny(显式拒绝)两种情况。该元素是必填项。

### 8.策略样例

该样例描述为：允许属于开发商 ID 1238423 下的子账号 ID 3232523 以及组 ID 18825，对北京地域的 cos 存储桶 bucketA 和广州地域的 cos 存储桶 bucketB 下的对象 object2，在访问 IP 为 10.121.2.\* 网段时，拥有所有 cos 读 API 的权限以及写对象的权限，以及可以发送消息队列的权限。

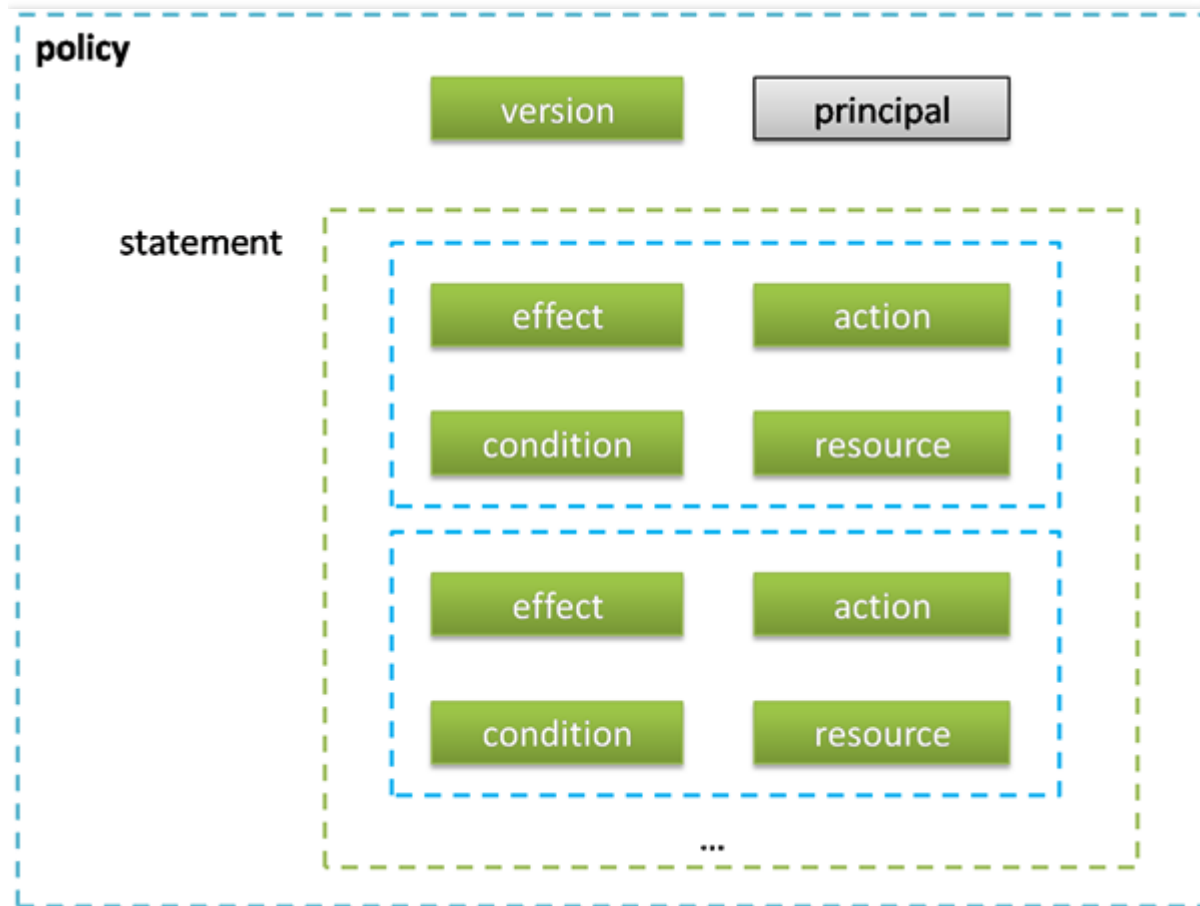
```
{
  "version": "2.0",
  "principal": {"qcs": ["qcs::cam::uin/1238423:uin/3232523",
    "qcs::cam::uin/1238423:groupid/18825"]},
  "statement": [
    {
      "effect": "allow",
      "action": ["name/cos:PutObject", "permid/280655"],
      "resource": ["qcs::cos:bj:uid/1238423:prefix//1238423/bucketA/*",
        "qcs::cos:gz:uid/1238423:prefix//1238423/bucketB/object2"],
      "condition": {"ip_equal": {"qcs:ip": "10.121.2.10/24"}}
    },
    {
      "effect": "allow",
      "action": "name/cmqueue:Sendmessages",
      "resource": "*"
    }
  ]
}
```

# 语法结构

最近更新时间：2017-12-12 15:41:02

整个策略的语法结构如下图所示。策略 policy 由版本 version 和语句 statement 构成，还可以包含委托人信息 principal，委托人仅限于策略管理 API 中策略语法相关的参数中使用。

语句 statement 是由若干个子语句构成。每条子语句包括操作 action、资源 resource、生效条件 condition 以及效力 effect 四个元素，其中 condition 是非必填项。



## JSON 格式

策略语法以 JSON 格式为基础。创建或更新的策略不满足 JSON 格式时，将无法提交成功，所以用户必须要确保 JSON 格式正确。JSON 格式标准在 RFC7159 中定义，您也可以使用在线 JSON 验证程序检查策略格式。

## 语法定义

语法描述中有如下约定：

- 以下字符是包含在策略语法中的 JSON 字符：

```
{ } [ ] " , ;
```

- 以下字符是用于描述策略语法中的特殊字符，不包含在策略中：

```
= < > ( ) |
```

- 当一个元素允许多个值时，使用逗号分隔符和省略号进行表示。例如：

```
[<resource_string>, <resource_string>, ...]  
<principal_map> = { <principal_map_entry>, > <principal_map_entry>, ... }
```

允许多个值时，也可以只包含一个值。当元素只有一个值时，尾部的逗号必须去掉，且中括号"[]"标记可选。例如：

```
"resource": [<resource_string>]  
"resource": <resource_string>
```

- 元素后的问号 (?) 表示该元素是非必填项。例如：

```
<condition_block?>
```

- 元素是枚举值的情况下，枚举值之间用竖线 "|" 表示，并用 "()" 括号定义枚举值的范围。例如：

```
("allow" | "deny")
```

- 字符串元素用双引号包括起来。例如：

```
<version_block> = "version": "2.0"
```

## 语法描述

```
policy = {  
  <version_block>  
  <principal_block?>,  
  <statement_block>  
}
```

```
<version_block> = "version" : "2.0"

<statement_block> = "statement" : [ <statement>, <statement>, ... ]

<statement> = {
  <effect_block>,
  <action_block>,
  <resource_block>,
  <condition_block?>
}

<effect_block> = "effect" : ("allow" | "deny")

<principal_block> = "principal": ("*" | <principal_map>)

<principal_map> = { <principal_map_entry>, <principal_map_entry>, ... }

<principal_map_entry> = "qcs":
[<principal_id_string>, <principal_id_string>, ...]

<action_block> = "action":
("*" | [<action_string>, <action_string>, ...])

<resource_block> = "resource":
("*" | [<resource_string>, <resource_string>, ...])

<condition_block> = "condition" : { <condition_map> }
<condition_map> {
  <condition_type_string> : { <condition_key_string> : <condition_value_list> },
  <condition_type_string> : { <condition_key_string> : <condition_value_list> }, ...
}
<condition_value_list> = [<condition_value>, <condition_value>, ...]
<condition_value> = ("string" | "number")
```

#### 语法说明：

- 一个策略 policy 可以包含多条语句 statement。  
策略的最大长度是 4096 个字符（不包含空格），具体信息请参阅 [限制](#)。  
各个块 block 的显示顺序无限制。例如，在策略中，version\_block 可以跟在 effect\_block 后面等。
- 当前支持的语法版本为 2.0。
- principal\_block 元素在控制台中不允许写入，仅支持在策略管理 API 中和策略语法相关的参数中使用 principal。

- 操作 action 和资源 resource 都支持列表，其中 action 还支持各产品定义的操作集 permid。
- 生效条件可以是单个条件，或者包括多个子条件块的逻辑组合。每个生效条件包括条件操作符 condition\_type、条件键 condition\_key，条件值 condition\_value。
- 每条语句 statement 的效力 effect 为 deny 或 allow。当策略中包含的语句中既包含有 allow 又包含有 deny 时，遵循 deny 优先原则。

## 字符串说明

语法描述的元素字符串说明如下：

### action\_string

由描述作用域、服务类型和操作名称组成。

```
//所有产品所有操作
"action": "*"
"action": "*:*"
// COS 产品所有操作
"action": "cos:*"
// COS 产品的名为 GetBucketPolicy 的操作
"action": "cos:GetBucketPolicy"
// COS 产品部分匹配 Bucket 的操作
"action": "cos:*Bucket*"
//操作集 ID 为 280649 的操作列表
"action": "permid/280649"
// cos 产品，名为 GetBucketPolicy\PutBucketPolicy\DeleteBucketPolicy 的操作列表
"action": ["cos:GetBucketPolicy", "cos:PutBucketPolicy", "cos: DeleteBucketPolicy"]
```

其中，permid 为各产品定义的操作集合 ID，具体信息请参阅各相关产品文档。

### resource\_string

资源通过六段式描述。

```
qcs: project :serviceType:region:account:resource
```

示例如下所示：

```
// COS 产品的 object 资源，上海地域，资源拥有者的 uid 是10001234，资源名是 bucket1/object2，资源前缀是 prefix
qcs::cos:sh:uid/10001234:prefix//10001234/bucket1/object2
// CMQ 产品的队列，上海地域，资源拥有者的 uin 是12345678，资源名是12345678/queueName1,资源前缀是 queueName
```

```
qcs::cmqueue:sh:uin/12345678:queueName/12345678/queueName1
```

// CVM 产品的云服务器，上海地域，资源拥有者的 uin 是 12345678，资源名是 ins-abcdefg，资源前缀是 instance

```
qcs::cvm:sh:uin/12345678:instance/ins-abcdefg
```

具体信息请参阅各产品的 [支持的资源级权限](#) 页面的资源描述方法。

### condition\_type\_string

条件操作符，描述测试条件的类型。例如 string\_equal、string\_not\_equal、date\_equal、date\_not\_equal、ip\_equal、ip\_not\_equal、numeric\_equal、numeric\_not\_equal 等。示例如下所示：

```
"condition":{
  "string_equal":{"cvm:region":["sh","gz"]},
  "ip_equal":{"qcs:ip":"10.131.12.12/24"}
}
```

### condition\_key\_string

条件键，表示将其值采用条件操作符进行操作，以便确定条件是否满足。CAM 定义了一组在所有产品中都可以使用的条件键，包括 qcs:current\_time、qcs:ip、qcs:uin 和 qcs:owner\_uin 等。具体信息请参阅 [生效条件](#)。

### principal\_id\_string

对于 CAM 而言，用户也是它的资源。因此委托人 principal 也采用六段式描述。示例如下，具体信息请参阅 [资源描述方式](#)。

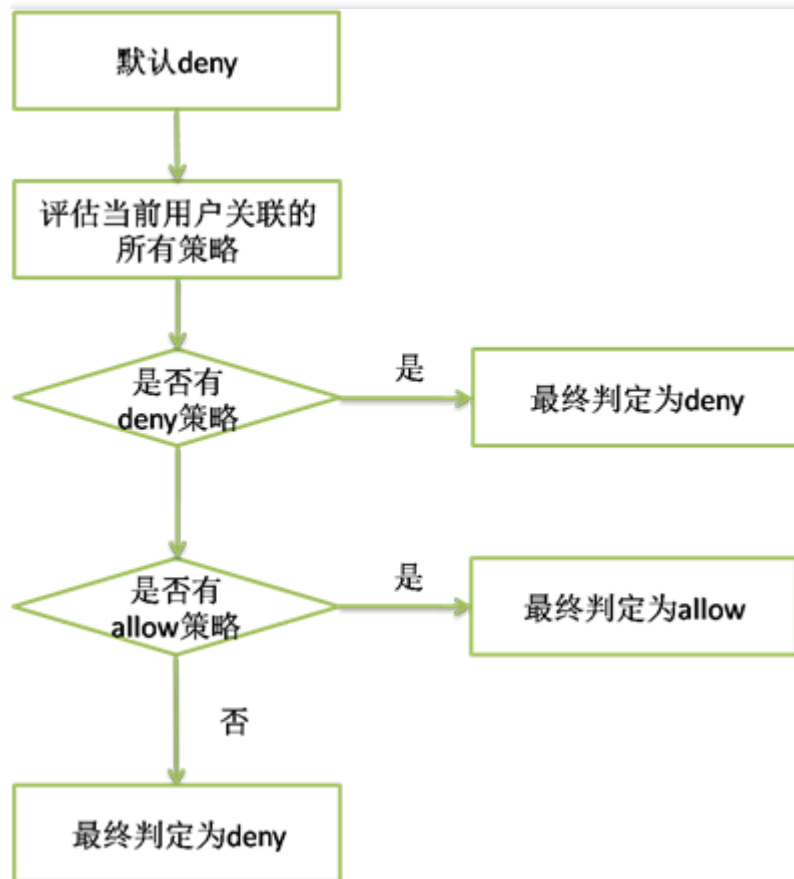
```
"principal":{"qcs":["qcs::cam::uin/1238423:uin/3232",
  "qcs::cam::uin/1238423:groupid/13"]}
```



# 评估逻辑

最近更新时间：2018-01-08 15:38:20

腾讯云用户访问云资源时，CAM 通过以下评估逻辑决定允许或拒绝。



1. 默认情况下，所有请求都将被拒绝。

2. CAM 会检查当前用户关联的所有策略。

- 判断是否匹配策略，是则进行下一步判断；否则最终判断为 deny，不允许访问云资源。
- 判断是否有匹配 deny 策略，是则最终判定为 deny，不允许访问云资源；否则进行下一步判断。
- 判断是否有匹配 allow 策略，是则最终判断为 allow，允许访问云资源；否则最终判定为 deny，不允许访问云资源。

## 注意：

- 对于根账号，默认拥有其名下所有资源的访问权限；且目前仅 COS/CAS 产品支持跨账号的资源访问。
- 有些通用策略，会默认关联所有 CAM 用户。具体请见下文的 [通用策略表](#)。

- 其他策略都必须显式指定，包括 allow 和 deny 策略。
- 对于支持跨帐号资源访问的业务，存在权限传递的场景，即根帐号 A 授权根帐号 B 下的某个子帐号对其资源的访问权限。这个时候 CAM 会同时校验 A 是否授权给 B 该权限以及 B 是否授权给子帐号该权限，两者同时满足的前提下，B 的子帐号才有权访问 A 的资源。

目前支持的通用策略表如下：

策略说明	策略定义
查询密钥需要 MFA 验证	<pre>{   "principal": "",   "action": "account:QueryKeyBySecretId",   "resource": "",   "condition": {"string_equal": {"mfa": "0"}} }</pre>
设置敏感操作需要 MFA 验证	<pre>{   "principal": "",   "action": "account:SetSafeAuthFlag",   "resource": "",   "condition": {"string_equal": {"mfa": "0"}} }</pre>
绑定 token 需要 MFA 验证	<pre>{   "principal": "",   "action": "account:BindToken",   "resource": "",   "condition": {"string_equal": {"mfa": "0"}} }</pre>
解绑 token 需要 MFA 验证	<pre>{   "principal": "",   "action": "account:UnbindToken",   "resource": "",   "condition": {"string_equal": {"mfa": "0"}} }</pre>
修改邮箱需要 MFA 验证	<pre>{   "principal": "",   "action": "account:ModifyMail",   "resource": "",   "condition": {"string_equal": {"mfa": "0"}} }</pre>

策略说明	策略定义
修改手机号需要 MFA 验证	<pre>{   "principal": "",   "action": "account:ModifyPhoneNum",   "resource": "",   "condition": {"string_equal": {"mfa": "0"}} }</pre>

# 资源描述方式

最近更新时间：2017-12-27 10:37:01

资源 resource 元素描述一个或多个操作对象，如 CVM 资源、COS 存储桶等。本文档主要介绍 CAM 的资源描述信息。

## 六段式

所有资源均可采用下述的六段式描述方式。每种产品都拥有其各自的资源和对应的资源定义详情。有关如何指定资源的信息，请参阅对应的产品文档。

六段式定义方式如下所示：

```
qcs:project_id:service_type:region:account:resource
```

其中：

- qcs 是 qcloud service 的简称，表示是腾讯云的云资源。该字段是必填项。
- project\_id 描述项目信息，仅兼容 CAM 早期逻辑。当前策略语法禁止填写该信息。
- service\_type 描述产品简称，如 CVM、CDN 等，产品的检测具体细节请参考对应的产品文档。值为 \* 的时候表示所有产品。该字段是必填项。
- region 描述地域信息。值为空的时候表示所有地域。腾讯云新版地域统一命名方式请参考 [地域和可用区](#)。腾讯云现有的地域命名方式定义如下：

地域缩写	描述
gz	广州
sh	上海
shjr	上海金融区
bj	北京
ca	加拿大
sg	新加坡
hk	香港

地域缩写	描述
cd	成都
de	德国

- account 描述资源拥有者的根账号信息。目前支持两种方式描述资源拥有者，uin 和 uid 方式。
  - uin 方式，即根账号的 QQ 号，表示为 `uin/${uin}`，如 `uin/12345678`；
  - uid 方式，即根账号的 APPID，表示为 `uid/${appid}`，如 `uid/10001234`。
  - 值为空的时候表示创建策略的 CAM 用户所属的根账号。目前 COS 和 CAS 业务的资源拥有者只能用 uid 方式描述，其他业务的资源拥有者只能用 uin 方式描述。
- resource 描述各产品的具体资源详情。
  - 有几种描述方式，该字段是必填项。
    - 表示某个资源子类下的资源 ID。如 VPC 产品的 `instance/ins-abcdefg`。  
`<resource_type>/<resource_id>`
    - 表示某个资源子类下的带路径的资源 ID。如 COS 产品的 `prefix//10001234/bucket1/object2`。该方式下，支持目录级的前缀匹配。如 `prefix//10001234/bucket1/*`，表示 bucket1 下的所有 Object。  
`<resource_type>/<resource_path>`
    - 表示某个资源子类下的所有资源。如 `instance/*`。  
`<resource_type>/*`
    - 表示某产品下的所有资源。  
`*`
  - 在某些场景下，资源 resource 元素也可以用 \* 来描述，含义定义如下，详细信息也请参阅对应的产品文档。
  - 操作 action 是需要关联资源的操作时，resource 定义为 \*，表示关联所有资源。
  - 操作 action 是不需要关联资源的操作时，resource 都需要定义为 \*。

## CAM 的资源定义

CAM 包含了用户、组、策略等资源，CAM 资源的描述方式如下所示：

根账号：

```
qcs::cam::uin/164256472:uin/164256472
```

或

```
qcs::cam::uin/164256472:root
```

子账号：

```
qcs::cam::uin/164256472:uin/73829520
```

组：

```
qcs::cam::uin/164256472:groupid/2340
```

所有用户：

```
qcs::cam::anonymous:anonymous
```

或

```
*
```

策略：

```
qcs::cam:: uin/12345678:policyid/*
```

或

```
qcs::cam:: uin/12345678:policyid/12423
```

## 资源的重要说明

- 资源的拥有者一定是根账号。如果资源是子账号创建的，不会自动拥有资源的访问权限，需要由资源拥有者授权。
- COS、CAS 等业务支持跨帐号授权资源的访问权限。被授权帐号可以通过权限传递方式将资源授权给其子账号。

# 策略变量

最近更新时间：2017-08-31 12:37:18

## 使用场景

场景假设：您希望给每个 CAM 用户授予其创建资源的访问权限。例如您想要设置 COS 资源的创建者默认拥有该资源的访问权限。

如果由资源所有者(根账号)将资源逐个授权给资源创建者，授权成本很高，需要为每种资源都编写策略并授权给创建者。在这种情况下，您可以通过使用策略变量来实现您的需求。在策略的资源定义中增加占位符描述的创建人信息，该占位符即为策略变量。当鉴权时，策略变量将被替换为来自请求本身的上下文信息。

授予创建者资源读权限的策略描述方式如下：

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": "name/cos:Read*",
      "resource": "qcs::cos::uid/1238423:prefix/${uin}/*"
    }
  ]
}
```

- 策略变量在每个资源的路径中带上创建人的 uin。如 uin 为 12356 的用户创建了名为 test 的 bucket，则其对应的资源描述方式为

```
qcs::cos::uid/1238423:prefix/12356/test
```

- uin 为 12356 的用户访问该资源时，鉴权过程中会把对应的策略信息的占位符替换为访问者，即

```
qcs::cos::uid/1238423:prefix/12356/
```

- 策略中的资源 `qcs::cos::uid/1238423:prefix/12356/` 可以通过前缀匹配访问资源 `qcs::cos::uid/1238423:prefix/12356/test`。

## 策略变量的位置

**资源元素位置**：策略变量可以用在[资源六段式](#)的最后一段。

**条件元素位置**：策略变量可以用在条件值中。

以下策略表示 VPC 创建者拥有访问权限。

```
{ "version": "2.0", "statement": { "effect": "allow", "action": "name/vpc:*",  
"resource": "qcs::vpc::uin/12357:vpc/*" "condition": { "string_equal": { "qcs:create_uin": "${uin}"} } } }
```

### 策略变量列表

目前支持的策略变量列表如下：

变量名	变量含义
<code>\${uin}</code>	当前访问者的子账号 uin 。对于访问者是根账号的情况，它和根账号 uin 一致。
<code>\${owner_uin}</code>	当前访问者所属的根账号 uin 。
<code>\${app_id}</code>	当前访问者所属的根账号的 APPID 。



# 生效条件

最近更新时间：2018-01-08 15:38:51

## 使用场景

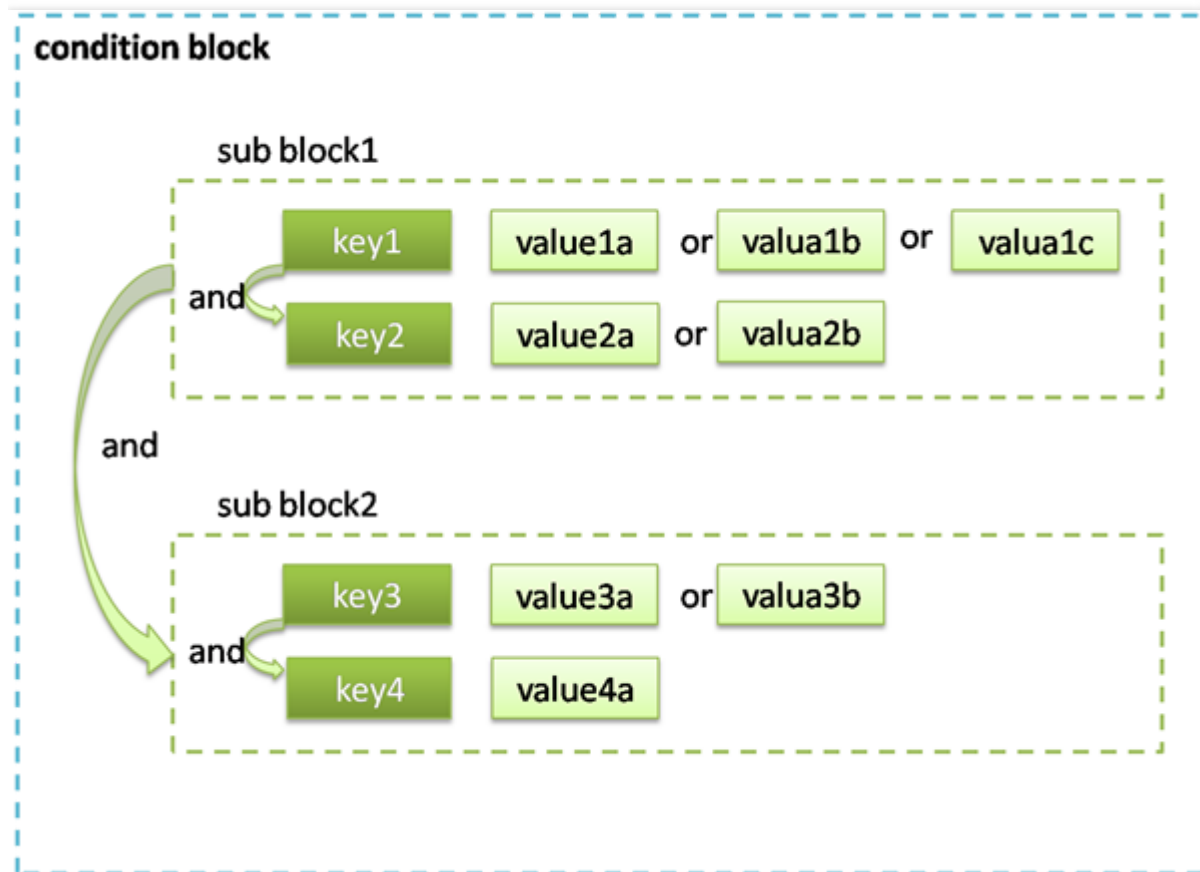
在很多场景下，我们需要对创建的策略进一步约束生效的条件 condition。

场景1：CAM 用户调用云 API 时，需要限制用户访问来源，则要求在现有的策略基础上加上 IP 条件。

场景2：当 CAM 用户在调用 VPC 对等连接 API 时，除了需要判断 CAM 用户是否拥有对等连接 API 和对等连接资源的访问权限外，还需要确认 CAM 用户是否拥有对等连接关联的 VPC 的访问权限。

## 语法结构

生效条件的语法结构如下图所示。一个条件块可以由若干个子条件块 sub block 构成，每个子条件块 sub block 对应一个条件操作符和若干个多个条件键，每个条件键对应了若干个条件值。



## 评估逻辑

条件生效的评估逻辑如下所述：

1. 条件键会对应到多个条件值，只要上下文信息中的对应键值在关联的条件操作符作用下满足其中任意一个条件值，则条件生效。

2. 对于一个子条件块中存在多个条件键的情况下，只有每个条件键对应的条件都生效时，该子条件块才生效。
3. 对于包含多个子条件块的情况，只有每个子条件块都生效时，整个条件才生效。
4. 对于包含 `_if_exist` 后缀的条件操作符，即使上下文信息中不包含条件操作符所关联的条件键，该条件依然生效。
5. 对于 `for_all_value`：限定词约束的条件操作符，适用于上下文信息中的条件键包括多个值的场景。只有当上下文信息中的条件键的每个值在关联的条件操作符作用下生效时，整个条件才生效。
6. 对于 `for_any_value`：限定词约束的条件操作符，适用于上下文信息中的条件键包括多个值的场景。只要上下文信息中的条件键的任意一个值在关联的条件操作符作用下生效时，整个条件就可以生效。

## 使用示例

1. 以下示例表示用户必须在 `10.217.182.3/24` 或者 `111.21.33.72/24` 网段才能调用云 API。

```
{
  "version": "2.0",
  "statement": {
    "effect": "allow",
    "action": "cos:PutObject",
    "resource": "*",
    "condition": {"ip_equal": {"qcs:ip": ["10.217.182.3/24", "111.21.33.72/24"]}}
  }
}
```

2. 以下示例描述允许 VPC 绑定指定的 NAT 网关，VPC 的地域必须是上海。

```
{
  "version": "2.0",
  "statement": {
    "effect": "allow",
    "action": "name/vpc:AcceptVpcPeeringConnection",
    "resource": "qcs::vpc:sh::pcx/2341",
    "condition": {"string_equal_if_exist": {"vpc:region": "sh"}}
  }
}
```

## 条件操作符列表

下表是条件操作符、条件名以及示例的信息。每个产品自定义的条件键，请参阅对应的产品文档。

条件操作符	含义	条件名	举例
-------	----	-----	----

条件操作符	含义	条件名	举例
string_equal	字符串等于(区分大小写)	qcs:tag	<pre>{"string_equal": {"qcs:tag/tag_name1":"tag_value1"}}</pre>
string_not_equal	字符串不等于(区分大小写)	qcs:tag	<pre>{"string_not_equal": {"qcs:tag/tag_name1":"tag_value1"}}</pre>
string_equal_ignore_case	字符串等于(不区分大小写)	qcs:tag	<pre>{"string_equal_ignore_case": {"qcs:tag/tag_name1":"tag_value1"}}</pre>
string_not_equal_ignore_case	字符串不等于(不区分大小写)	qcs:tag	<pre>{"string_not_equal_ignore_case": {"qcs:tag/tag_name1":"tag_value1"}}</pre>
string_like	字符串匹配(区分大小写)	qcs:tag	<pre>{"string_like": {"qcs:tag/tag_name1":"tag_value1"}}</pre>
string_not_like	字符串不匹配等于(区分大小写)	qcs:tag	<pre>{"string_not_like": {"qcs:tag/tag_name1":"tag_value1"}}</pre>
date_not_equal	时间不等于	qcs:current_time	<pre>{"date_not_equal": {"qcs:current_time":"2016-06-01T00:01:00Z"}}</pre>
date_greater_than	时间大于	qcs:current_time	<pre>{" date_greater_than ": {"qcs:current_time":"2016-06-01T00:01:00Z"}}</pre>
date_greater_than_equal	时间大于等于	qcs:current_time	<pre>{" date_greater_than_equal ": {"qcs:current_time":"2016-06-01T00:01:00Z"}}</pre>
date_less_than	时间小于	qcs:current_time	<pre>{" date_less_than ": {"qcs:current_time":"2016-06-01T00:01:00Z"}}</pre>

条件操作符	含义	条件名	举例
date_less_than_equal	时间小于等于	qcs:current_time	{"date_less_than ": {"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_less_than_equal	时间小于等于	qcs:current_time	{"date_less_than_equal ": {"qcs:current_time":"2016-06-01T00:01:00Z"}}
ip_equal	ip等于	qcs:ip	{"ip_equal":{"qcs:ip ":"10.121.2.10/24"}}
ip_not_equal	ip不等于	qcs:ip	{"ip_not_equal":{"qcs:ip ": ["10.121.2.10/24", "10.121.2.20/24"]}}
numeric_not_equal	数值不等于	qcs:mfa	{"numeric_not_equal":{"mfa":1}}
numeric_greater_than	数值大于		{"numeric_greater_than ": {"cvm_system_disk_size":10}}
numeric_greater_than_equal	数值大于等于		{"numeric_greater_than_equal ": {"cvm_system_disk_size":10}}
numeric_less_than	数值小于		{"numeric_less_than ": {"cvm_system_disk_size":10}}
numeric_less_than_equal	数值小于等于		{"numeric_less_than_equal ": {"cvm_system_disk_size":10}}
numeric_equal	数值等于	qcs:mfa	{"numeric_equal":{"mfa":1}}
numeric_greater_than	数值大于		{"numeric_greater_than ": {"some_key":11}}
bool_equal	布尔值匹配	-	-
null_equal	条件键为空匹配	-	-

说明：

1. 日期格式按照 ISO8601 标准表示，并需要使用 UTC 时间。

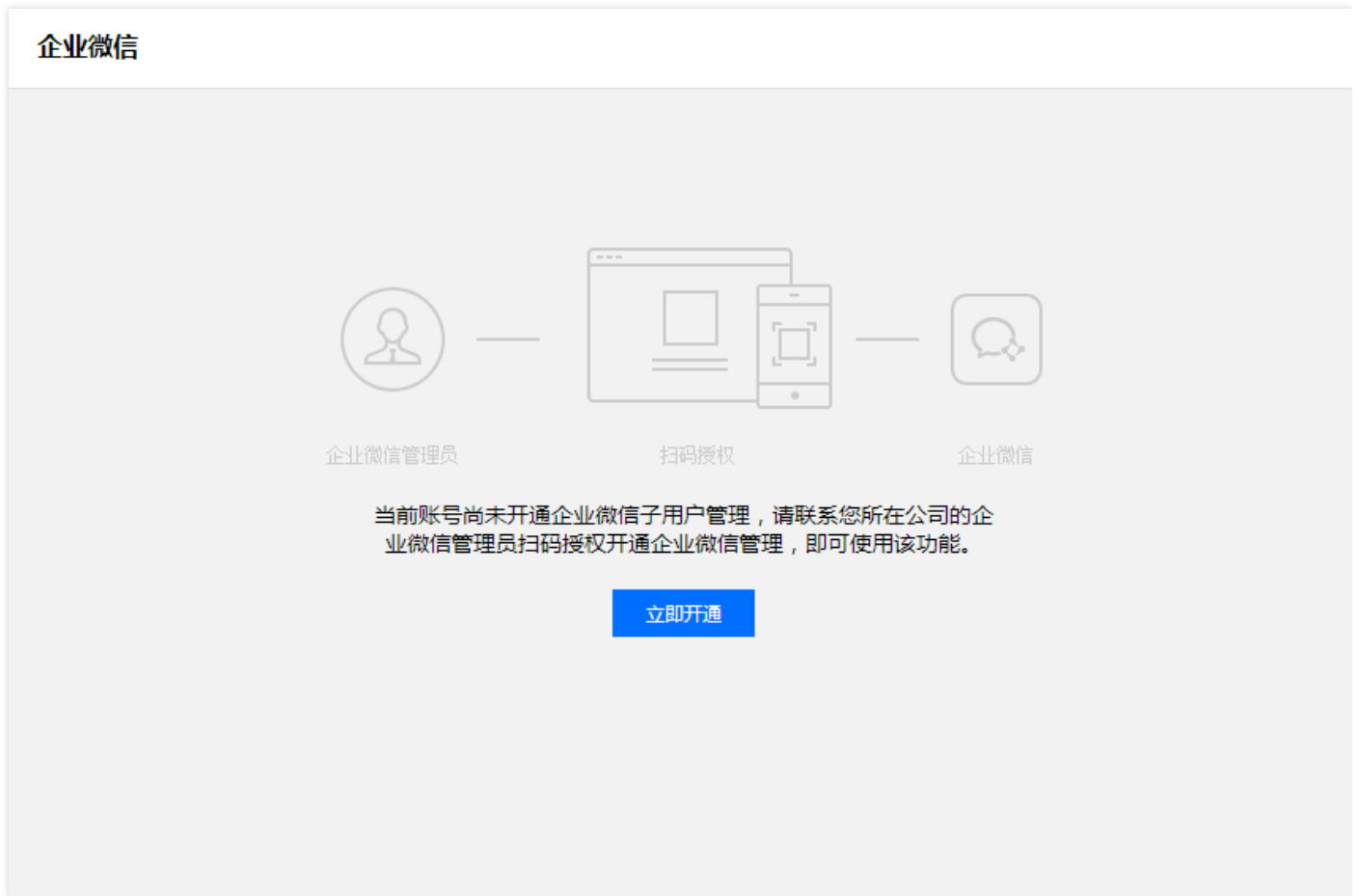
- 
2. IP 格式要符合 CIDR 规范。
  3. 条件操作符 ( `null_equal` 除外 ) 加上后缀 `_if_exist` , 表示上下文信息中即便不包含对应的键值依然生效。
  4. `for_all_value` : 限定词搭配条件操作符使用 , 表示上下文信息中条件键的每个值都满足要求时才生效。
  5. `for_any_value` : 限定词搭配条件操作符使用 , 表示上下文信息中条件键的任意一个值满足要求时就可以生效。
  6. 部分业务不支持条件 , 或仅支持部分条件。具体信息参考业务文档说明。

# 联合帐号 企业微信

最近更新时间：2018-08-10 15:26:51

您可以授权腾讯云访问您所在企业微信的通讯录。授权后，在 CAM 新建用户时可以选择从企业微信通讯录中拉取相应的用户，方便您创建子用户。具体步骤如下：

1. 登录 [企业微信控制台](#) 页面，单击【立即开通】。



2. 企业微信管理员通过扫描二维码授权腾讯云获取企业微信通讯录。
3. 授权成功后，会在企业微信列表看到授权记录。企业微信列表，只记录您的授权行为，不会主动去访问您的企业微信通讯录，除非您手动从新建用户中选择需要从企业微信中添加子用户。

### 企业微信

1. 此处为关联企业微信账号，从企业微信架构的人员信息中添加到腾讯云子用户，请进入用户管理->新建用户->从企业微信创建子用户；
2. 只能从激活的企业微信中添加人员，如果您的企业信息已经过期，请重新授权；
3. 企业微信子账号登录链接：<https://cloud.tencent.com/login/qywx/100006584512>

添加

企业名称	添加时间
test	2018-08-09 16:32:49

共 1 项

每页显示行 20 ▾

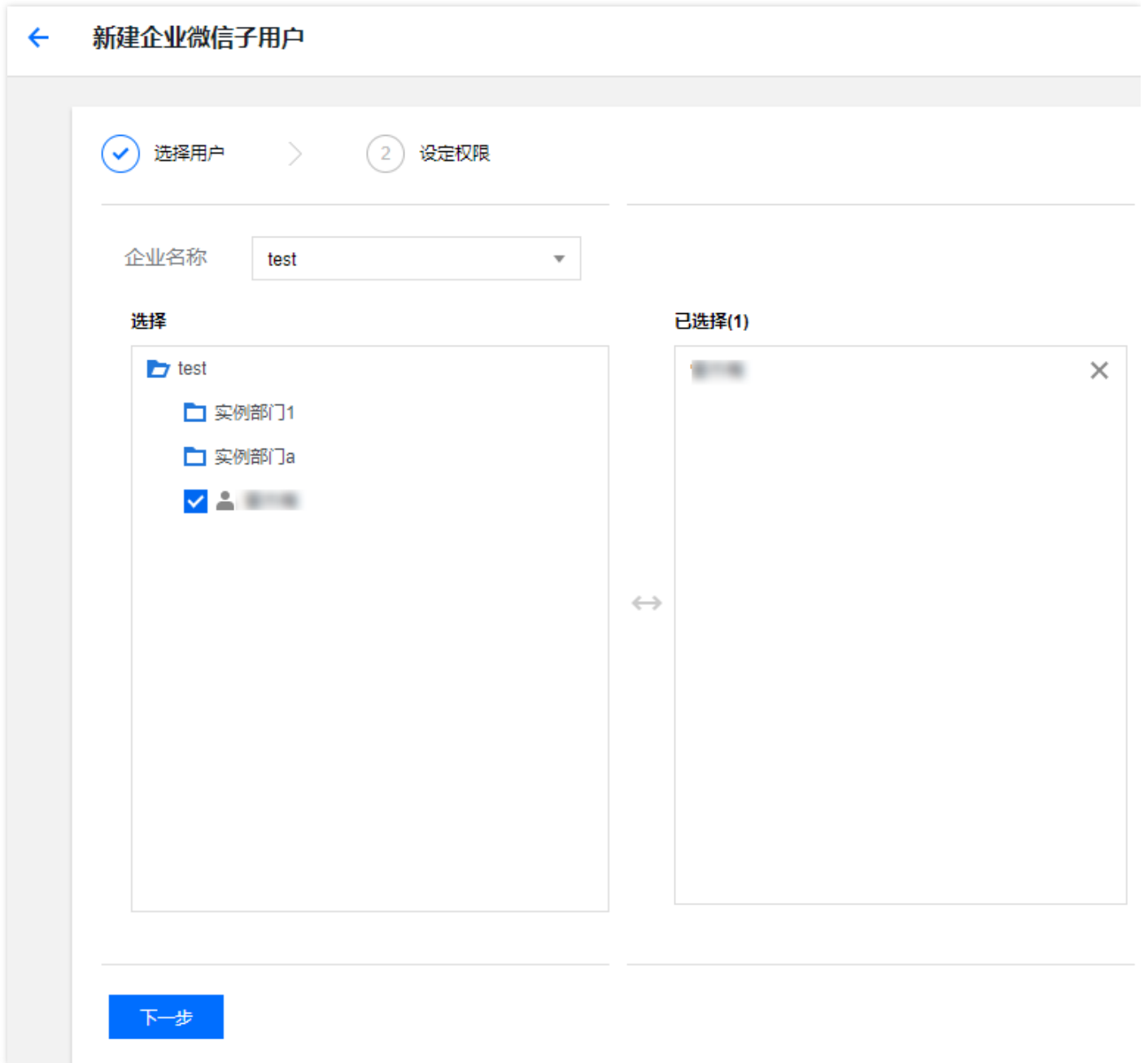


4. 单击【用户管理】 > 【新建用户】 > 【从企业微信创建子用户】。



5. 拉取授权过的企业微信通信录。若授权还在有效期，则可以拉取到您的通信录；若授权超过有效期或者在企业微信后台解除授权，则需要重新授权。勾选需要新建子用户的企业微信，单击【下一步】。





6. 为子用户设定权限。您可以通过【添加到现有组】、【复制现有用户权限】或【从策略列表中授权】来为子用户设定权限。

✓ 选择用户 >
✓ 设定权限

添加到现有用户组
复制现有用户权限
从策略列表中授权

将用户添加到现有组或者创建新组。使用组是按照工作职能来管理用户权限的最佳做法

快捷建组

请输入用户组名 Q

<input type="checkbox"/> 组	备注	附加的策略
<input type="checkbox"/> 示例组	备注一	QCloudResourceFullAccess,ReadOnlyAccess
<input type="checkbox"/> 示例组1	group1	QCloudResourceFullAccess,ReadOnlyAccess
<input type="checkbox"/> userGroup	group for test	AdministratorAccess,ReadOnlyAccess

已选 0 项，共 3 项
每页显示行 10 ▼

⏪ ⏩ 1/1 ⏪ ⏩

下一步

如果您在设定权限遇到问题，可参考 [新建子用户](#) 中【设定权限】部分内容

7. 设定权限后，单击【下一步】，完成新建子用户操作。

# 子账号或协作者安全设置

最近更新时间：2018-09-30 15:42:48

您可以在创建或管理子用户过程中，设置子用户需要进行二次认证，才可登录腾讯云或者在腾讯云进行敏感操作。由于这些设置关系到您账号的安全性，如果您是子账号或者协作者，只能接受主账号或者是具有 CAM 管理权限的用户对这些安全属性的设置。

CAM 子用户可以设置的操作属性如下：

设置内容	设置项
操作保护	手机验证码
	MFA
	不开启
登录保护	手机验证码
	MFA
	不开启

CAM 协作者可以设置的操作属性如下：

设置内容	设置项
操作保护	手机验证码
	MFA
	不开启
登录保护	手机验证码
	MFA
	不开启

您在安全设置中只能看到主账号看到的状态展示，如果您需要变更设置，可以请求主账号或者是具有 CAM 管理权限的子用户，在 CAM - 用户管理中，设置相关内容。

## 开启 MFA 相关设置

1. 新建子用户时，可以在选择用户具备控制台登录权限后，设置相关内容；
2. 如果设置子用户开启 MFA 校验，那么子用户在下一次登录时，需要进行 MFA 设备关联，才可以进入控制台进行操作。

## 重置 MFA

1. 进入子用户（协作者）详情页面，进入安全设置，找到 MFA 设置项；
2. 在管理 MFA 设置项中，可以对子用户（协作者）的 MFA 设置内容进行管理和配置；
3. 如果子用户（协作者）已经开启 MFA 校验，您可以重置该用户的设备状态。完成重置后，子用户（协作者）下一次登录将进入重新绑定 MFA 的流程。当子用户（协作者）丢失设备时，可以通过这个设置进行重新关联。

## 常见问题

### 忘记 MFA 设备怎么办？

请主账号或具有管理权限的用户在 CAM 访问管理中重置 MFA，具体操作请参考为 [重置 MFA](#)。