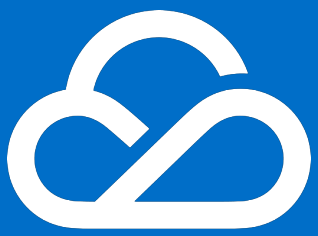
腾讯云账号相关

访问控制

产品文档



腾讯云

【版权声明】

【商标声明】

【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
什么是访问控制? 4
CAM概述 4
CAM术语 5
产品功能 7
应用场景 8
支持CAM的云服务列表 9
购买指导 11
用户指南 12
概述 12
身份管理 13
用户管理 13
用户组管理 16
策略管理 18
权限 18
策略 19
授权管理 26
策略语法 31
元素参考 31
语法结构 34
评估逻辑 40
资源描述方式 43
策略变量 46
生效条件 48
限制 53
限制 53
最佳实践 54
商用案例 56
CMQ相关案例 56
COS相关案例 59
VPC相关案例 60

什么是访问控制?

CAM概述

访问控制（CAM）是腾讯云提供的一套Web服务，它主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。通过CAM，您可以创建、管理和销毁用户(组)，并通过身份管理和策略管理控制哪些人可以使用哪些腾讯云资源。

CAM术语

1.根账号

根账号又被称为开发商。创建腾讯云账号时，会创建一个用于登陆腾讯云服务的根账号身份。根账号是腾讯云资源归属、资源使用计量计费的基本主体。根账号默认拥有其名下所拥有的资源的完全访问权限，包括访问该账号的账单信息，修改用户密码，创建用户和用户组以及访问其他云服务资源等。默认情况下，资源只能被根账号所访问，任何其他用户访问都需要获得根账号的授权。

2.子账号（用户）和用户组

子账号是由根账号创建的实体，有确定的身份ID和身份凭证，且能登录到腾讯云控制台。根账号可以创建多个子账号(用户)。子账号默认不拥有资源，必须由所属根账号进行授权。一个子账号可以归属于多个根账号，分别协助多个根账号管理各自的云资源，但同一时刻，一个子账号只能登录到一个根账号下，管理该根账号的云资源。子账号可以通过控制台切换开发商从一个根账号切换到另外一个根账号。子账号在控制台登陆时会自动切换到默认根账号上，并拥有该根账号所授予的访问权限。当切换开发商之后，会拥有切换后根账号授权的访问权限，而切换前根账号授予的访问权限会立即失效。

有相同职能的用户可以被添加在同一用户组，为该用户组关联适当的策略，以分配不同权限。

3.身份凭证

身份凭证是用于证明用户真实身份的凭据，用户必须要确保身份凭证的安全。它包括登陆凭证和访问证书两种。

登陆凭证是指用户登陆名和密码。通过使用登录名和密码登入腾讯云控制台，便可以通过控制台进行权限范围内的访问。

访问证书是指云API密钥(SecretId和SecretKey)，包括个人API密钥和项目密钥。大多数业务使用个人API密钥访问腾讯云API。少数业务使用项目密钥访问腾讯云API，包括万象优图、优图人脸识别、COS等服务。

多因素认证（Multi-Factor Authentication, MFA）是在上述身份凭证的基础上增加的一项安全保护功能。当安全信息设置里绑定了MFA设备后，可以选择开启登陆保护和操作保护。当开启 MFA登陆保护后，用户登陆腾讯云网站时，系统在用户输入的用户名和密码验证通过后还要求输入来自其MFA设备的动态安全码进行二次

验证。当开启MFA操作保护后，用户在一些敏感操作时必须要通过输入MFA设备的动态安全码完成二次验证。

4.资源

资源是云服务中被操作的对象，如COS存储桶或对象，VPCID，消息队列等。根账号、子账号甚至策略也是一种资源。

5.权限和策略

权限是指允许或拒绝某些用户执行某些操作，访问某些资源。。默认情况下，根账号拥有其名下所有资源的访问权限，而子账号没有所属根账号下任何资源的访问权限。

策略是定义和描述一条或多条权限的语法规范。根账号通过将策略关联到用户或用户组完成授权。超级管理员或者被授权拥有策略管理权限的子账号也可以创建、更新、删除策略以及进行策略的授权。

策略都可以在控制台的用户和权限页面进行操作。部分业务支持在业务控制台相关页面定义策略，如COS控制台等。

产品功能

CAM提供以下功能支持：

1) 根账号资源的授权访问

可以将根账号的资源授权给其他人员，包括子账号或者是其他根账号，而不需要分享根账号相关的身份凭证。

2) 精细化的权限管理

可以针对不同的资源授权给不同的人员不同的访问权限。例如可以允许某些子账号拥有某个COS存储桶的读权限，而另外一些子账号或者根账号可以用户某个COS存储对象的写权限等。这里的资源、访问权限、用户都可以批量打包。

3) 身份认证

对访问者的身份进行确认。

4) 最终一致性

CAM目前支持腾讯云的多个地域，通过复制策略数据实现在跨地域的数据同步，虽然CAM策略的修改会及时提交，不过跨地域的策略同步会导致策略生效的延迟；同时CAM使用缓存来提高性能（目前是一分钟缓存），更新需要在缓存过期后生效。

应用场景

1.企业子账号权限管理

企业内不同岗位的员工需要拥有该企业云资源的最小化访问权限。

场景：某个企业拥有很多云资源，包括CVM、VPC实例、CDN实例、COS存储桶和对象等。该企业拥有很多员工，包括开发人员、测试人员、运维人员等。部分开发人员需要拥有其所在项目相关的开发机云资源的读写权限，测试人员需要拥有其所在项目的测试机云资源的读写权限，运维人员负责机器的购买和日常运营。当企业员工职责或参与项目发生变更，将终止对应的权限。

2.不同企业之间的权限管理

不同企业间需要进行云资源的共享。

场景：某企业拥有很多云资源，该企业希望能专注产品研发，而将云资源运维工作授权给其他运营企业来实施。当运营企业的合同终止时，将收回对应的管理权限。

支持CAM的云服务列表

支持CAM的云服务列表如下：

服务	业务权限	策略语法	云API	控制台	授权粒度	条件	临时证书
CDN	支持	不支持	支持	支持	操作级	不支持	不支持
消息队列CMQ	支持	支持	支持	支持	资源级	不支持	不支持
密钥管理服务KMS	支持	支持	支持	支持	资源级	不支持	不支持
互动直播	支持	支持	不支持	支持	服务级	不支持	不支持
云点播	支持	支持	不支持	支持	服务级	不支持	不支持
云直播	支持	支持	不支持	支持	服务级	不支持	不支持
短信	支持	支持	不支持	支持	服务级	不支持	不支持
对象存储COS	不支持	支持	支持	不支持	资源级	部分支持	支持
归档存储CAS	不支持	支持	支持	支持	资源级	部分支持	支持
私有网络VPC(灰度)	不支持	支持	支持	支持	资源级	部分支持	不支持
存储网关CSG(灰度)	不支持	支持	支持	支持	资源级	不支持	支持
云数据库CDB(灰度)	不支持	支持	支持	不支持	资源级	不支持	不支持
数据传输DTS(灰度)	不支持	支持	支持	不支持	资源级	不支持	不支持
负载均衡CLB(灰度)	不支持	支持	支持	支持	资源级	部分支持	不支持
云服务器CVM(灰度)	不支持	支持	支持	支持	资源级	部分支持	不支持
安全组DFW(灰度)	不支持	支持	支持	支持	资源级	部分支持	不支持
云硬盘CBS(灰度)	不支持	支持	支持	支持	资源级	部分支持	不支持

说明：

1）“业务权限”是指按业务权限方式创建策略，“策略语法”是指按策略语法方式创建策略。

2)“云API”是指云API是否接入了CAM，“控制台”是指控制台是否接入了CAM。

3)授权粒度按照粒度粗细分为服务级、操作级和资源级三个级别。服务级粒度下仅支持定义某个服务是否拥有访问权限；操作级粒度下支持某个服务下的某个操作是否拥有访问权限；资源级粒度下支持针对某个资源是否拥有访问权限，是最细粒度的授权。

4)条件语法仅在部分业务支持。已支持条件的业务的条件列表请参考具体的业务文档说明。

5)临时证书目前仅对象存储COS和归档存储CAS支持。

6)对象存储COS仅支持xml协议的API接口；私有网络VPC等云服务均在灰度期，具体信息请参考业务文档说明。

购买指导

1、开通简介

CAM服务不需要开通，仅需要申请注册一个腾讯云帐号即可。该服务为免费服务。

2、开通方法

开通CAM服务需要申请注册一个腾讯云帐号。申请方法请参考相关文档。

用户指南

概述

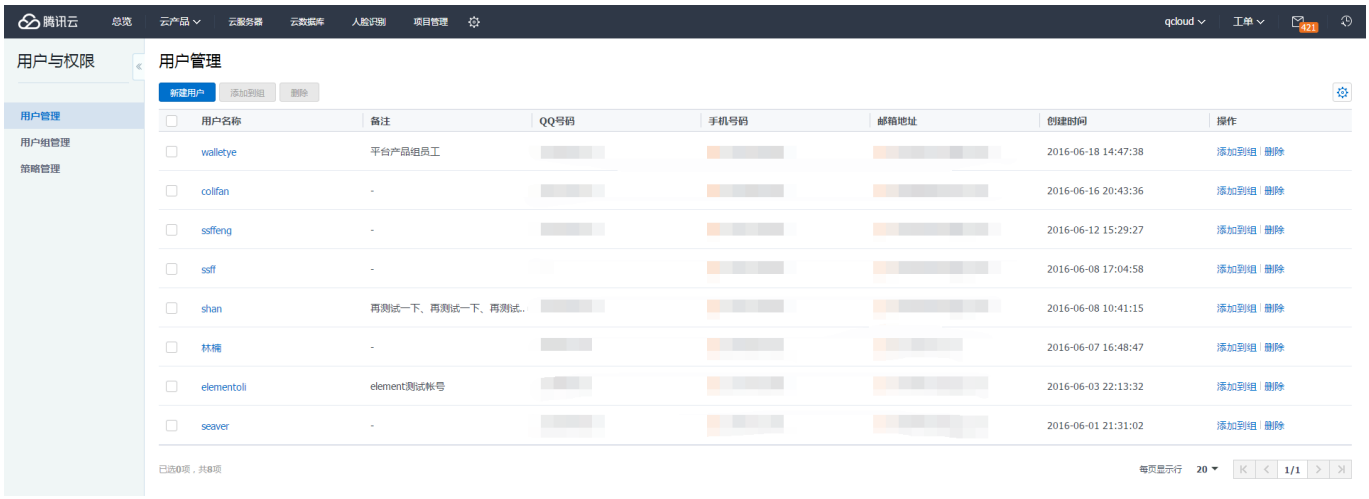
详细描述了CAM的核心能力以及使用方法。包括身份管理、策略管理和策略语法这几部分，并对CAM的一些使用限制进行了说明。

身份管理

用户管理

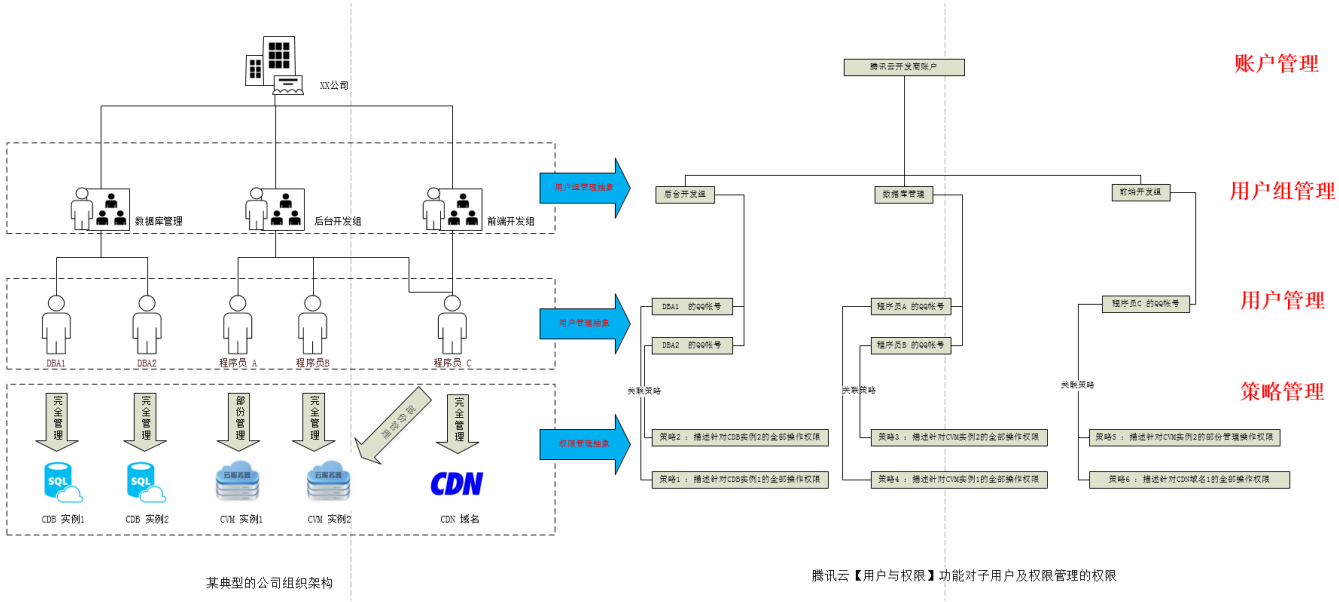
访问入口

请访问[用户与权限控制台]

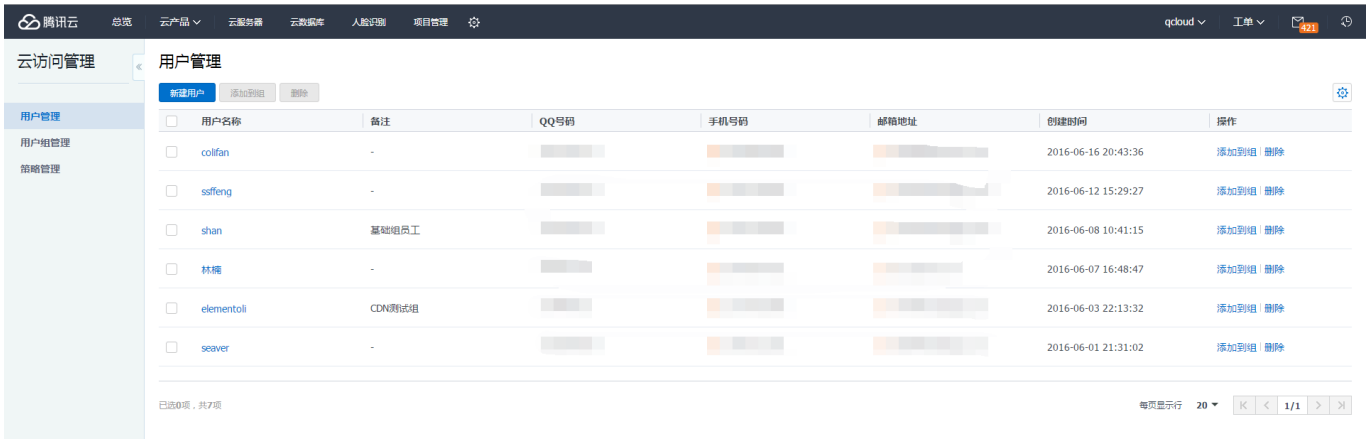


用户管理的作用

你可以将需要管理账户内云资源的员工(以QQ帐号为登录凭证)添加为你账户的子用户，可以为子用户关联适当的策略，以分配不同权限。



类比于公司组织架构，子用户即公司员工。

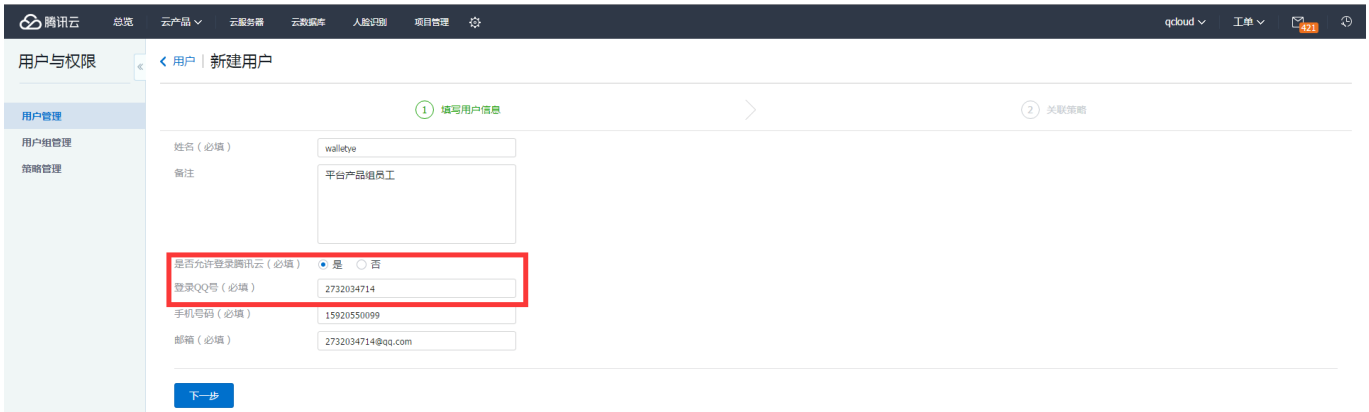


【用户管理】即是对组织架构中员工管理的抽象。

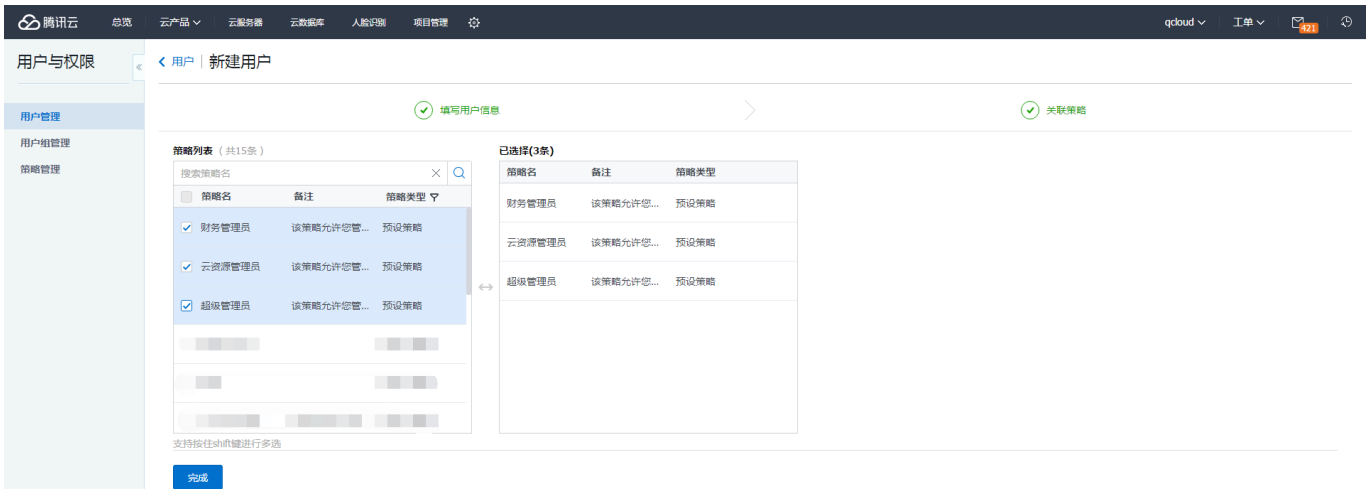
如何新建子用户

step1:访问用户与权限控制台，并点击【新建用户】

step2: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



step3:请为该用户关联策略(策略描述了权限，关联策略后用户即获得策略描述的权限）

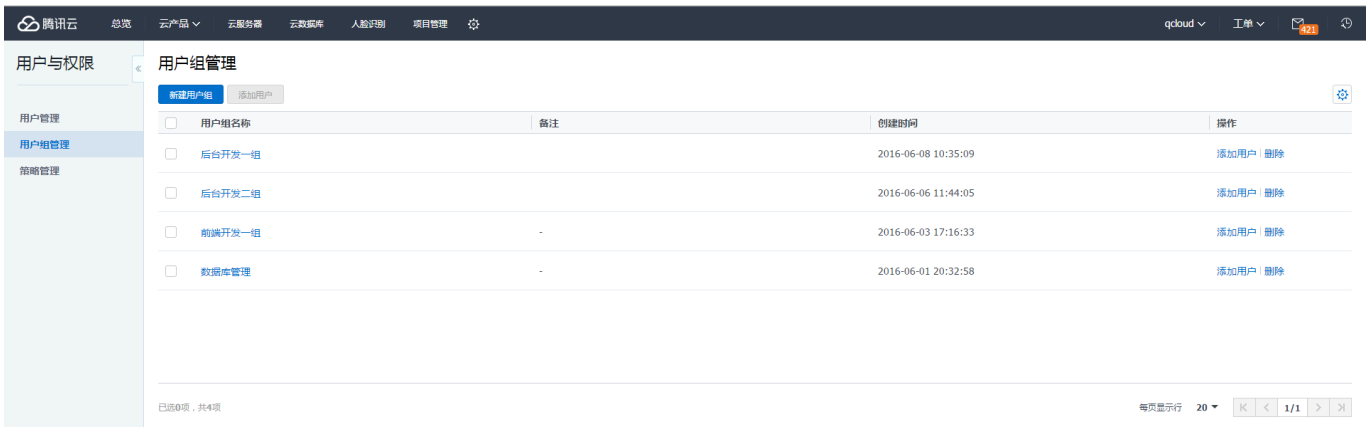


step4: 在【用户管理】列表中，即可查看刚刚添加的子用户。

用户组管理

访问入口

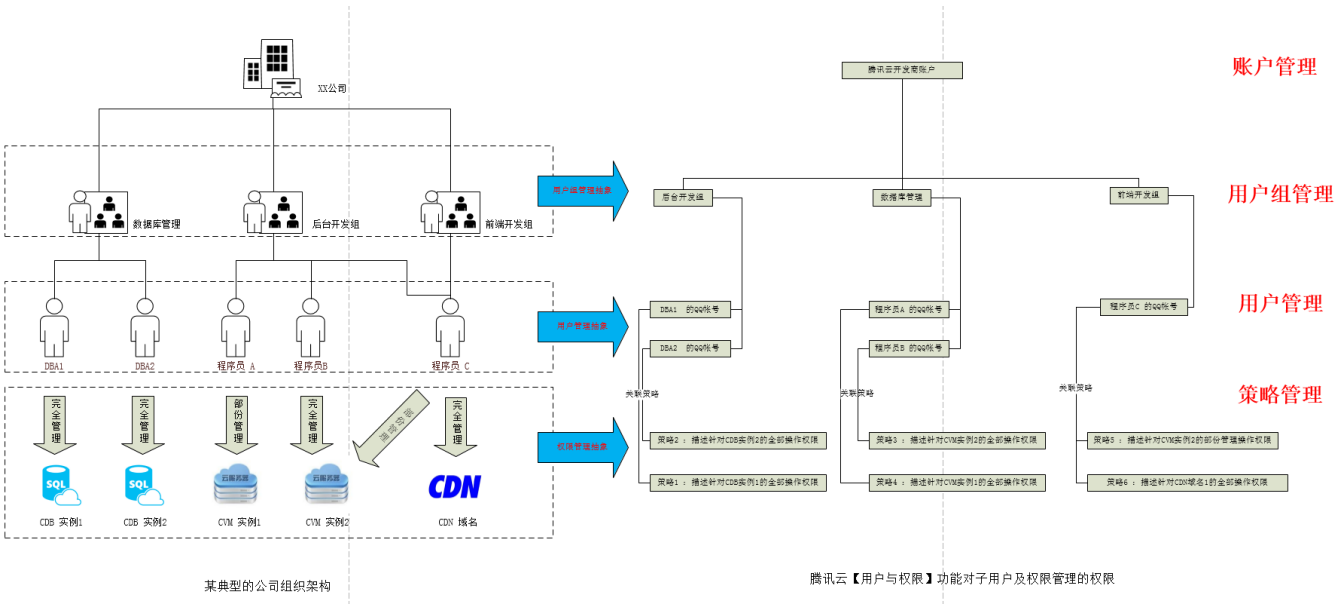
请访问[用户与权限控制台]



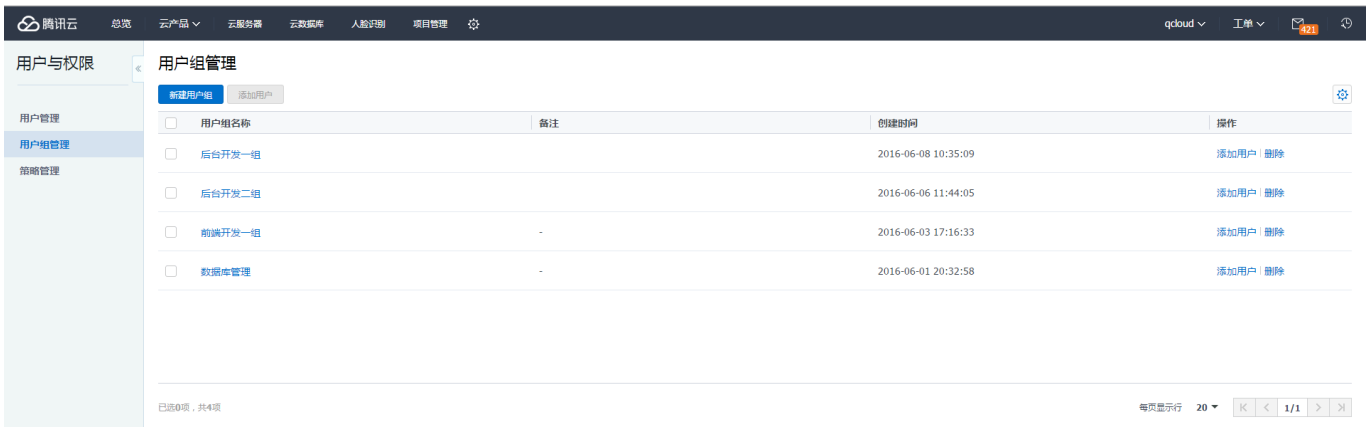
用户组的作用

你可以将有相同职能的用户添加在同一用户组，为该用户组关联适当的策略，以分配不同权限。

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，非常适合作批量授权。



类比于公司组织架构，用户组管理即部门管理。

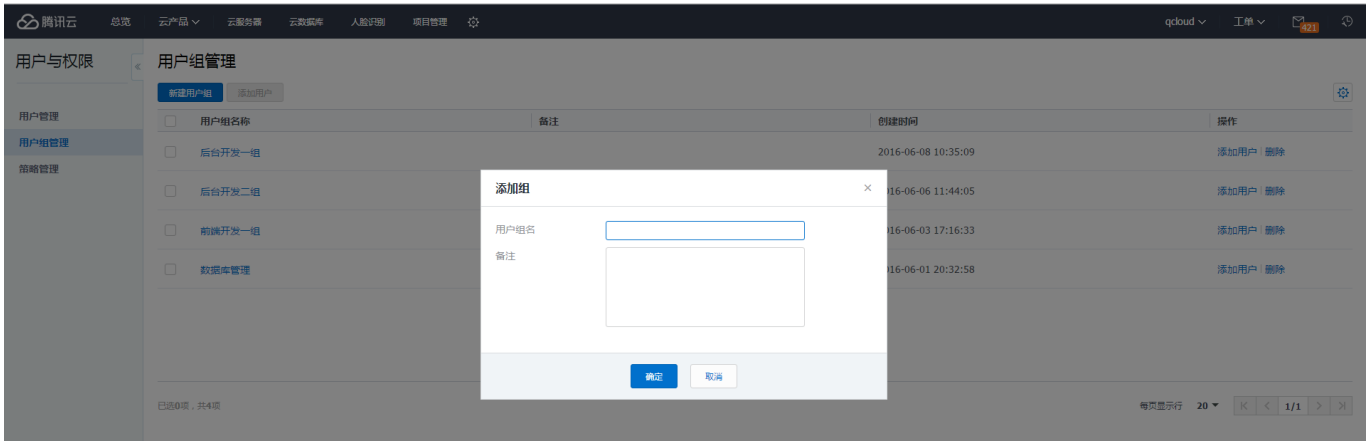


【用户组管理】即是对组织架构中部门管理的抽象。

如何新建用户组

step1:请访问用户与权限控制台

step2: 点击【新建用户组】，填写用户组名和备注，即可创建



策略管理

权限

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范。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

策略是定义和描述一条或多条权限的语法规范。CAM支持两种类型的策略，预设策略和自定义策略。

1.预设策略

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。这类策略不可以编辑。

在预设策略的界面中，我们可以通过服务类型还有关键字来进行搜索。这里我们以服务类型为全部服务，关键字为ad进行搜索：

2.自定义策略

由用户创建的策略，允许你作各细粒度的权限划分。比如为某DBA关联一条策略，让他只能管理CDB实例，而无权管理CVM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和按语法创建的策略。

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。

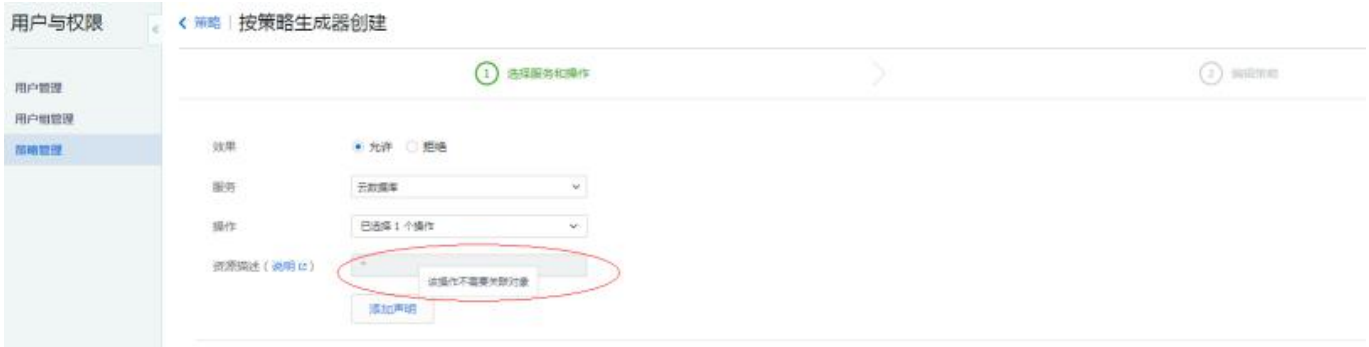
3.创建自定义策略

3.1按策略生成器创建

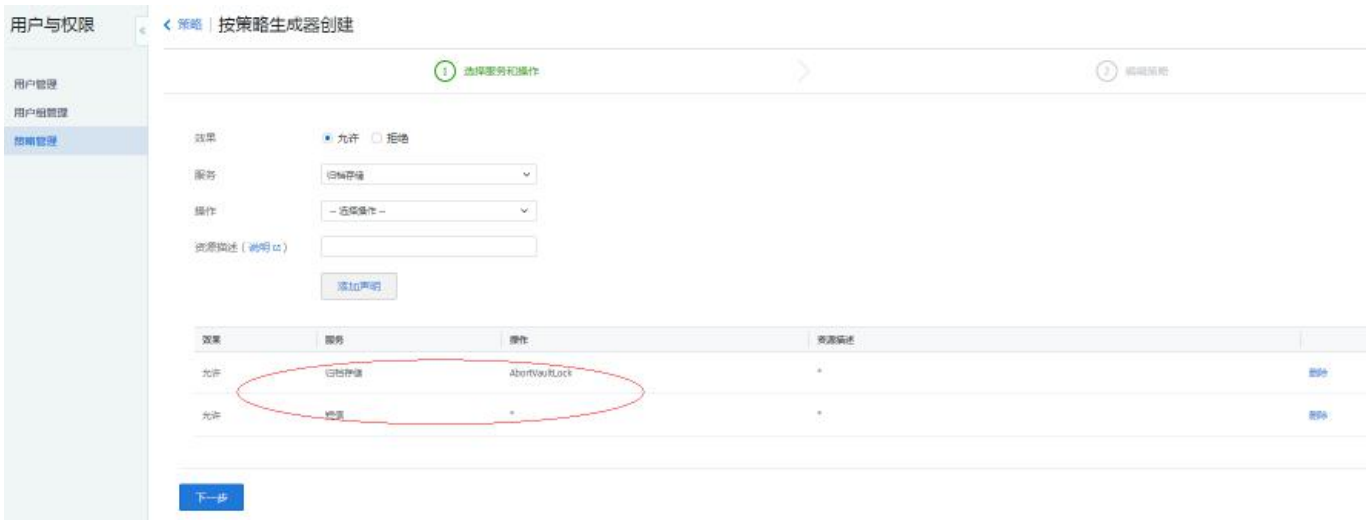
step1: 访问策略管理控制台，则点击【创建自定义策略】,并选择按策略生成器创建。

step2: 从列表中选择想要的服务以及操作, 然后点击添加声明，接着点击下一步。其中,有一些服务的操作是需要关联对象的,则需要填写资源描述。下图就是需要关联对象的操作，其中资源描述的具体定义和示例可以点击左侧的“说明”链接。

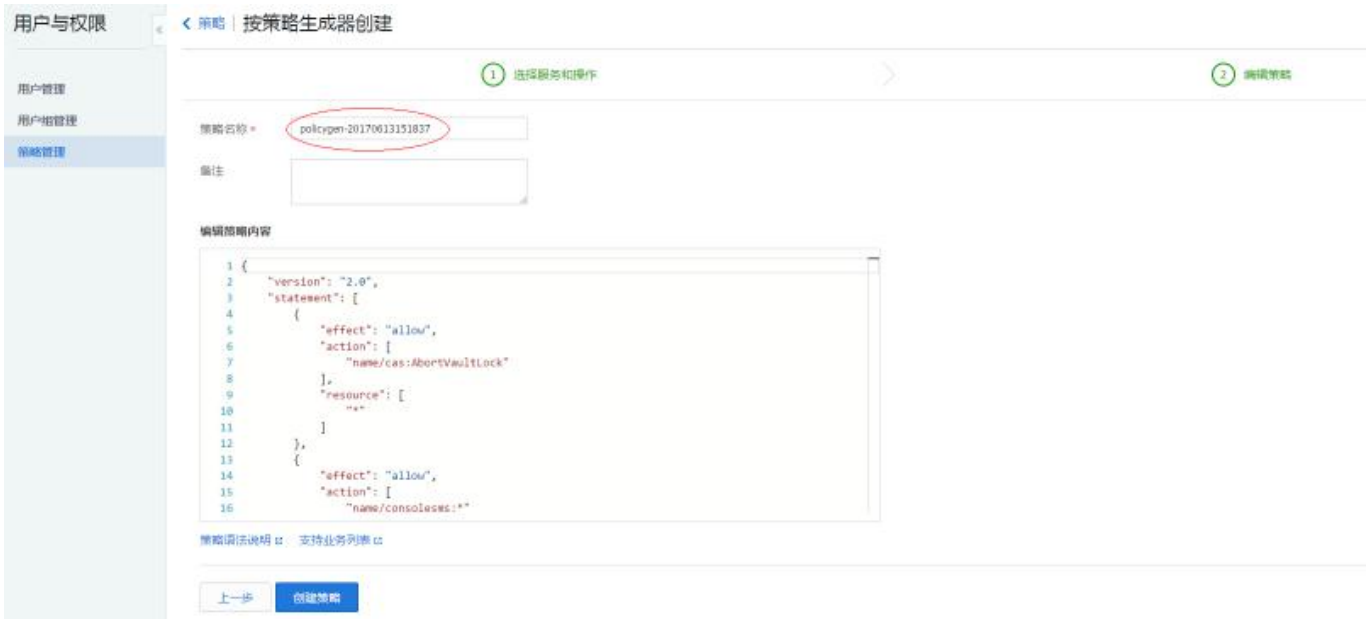
有一些服务的操作是不需要关联对象的，也就是不需要资源描述。下图就是不需要关联对象的操作。你会发现资源描述那一栏不可填。



其中，我们可以在一条策略中添加多条声明，这里我们选择的是归档存储里面的AboutVaultLock还有短信里面的SmsQcloudcom。



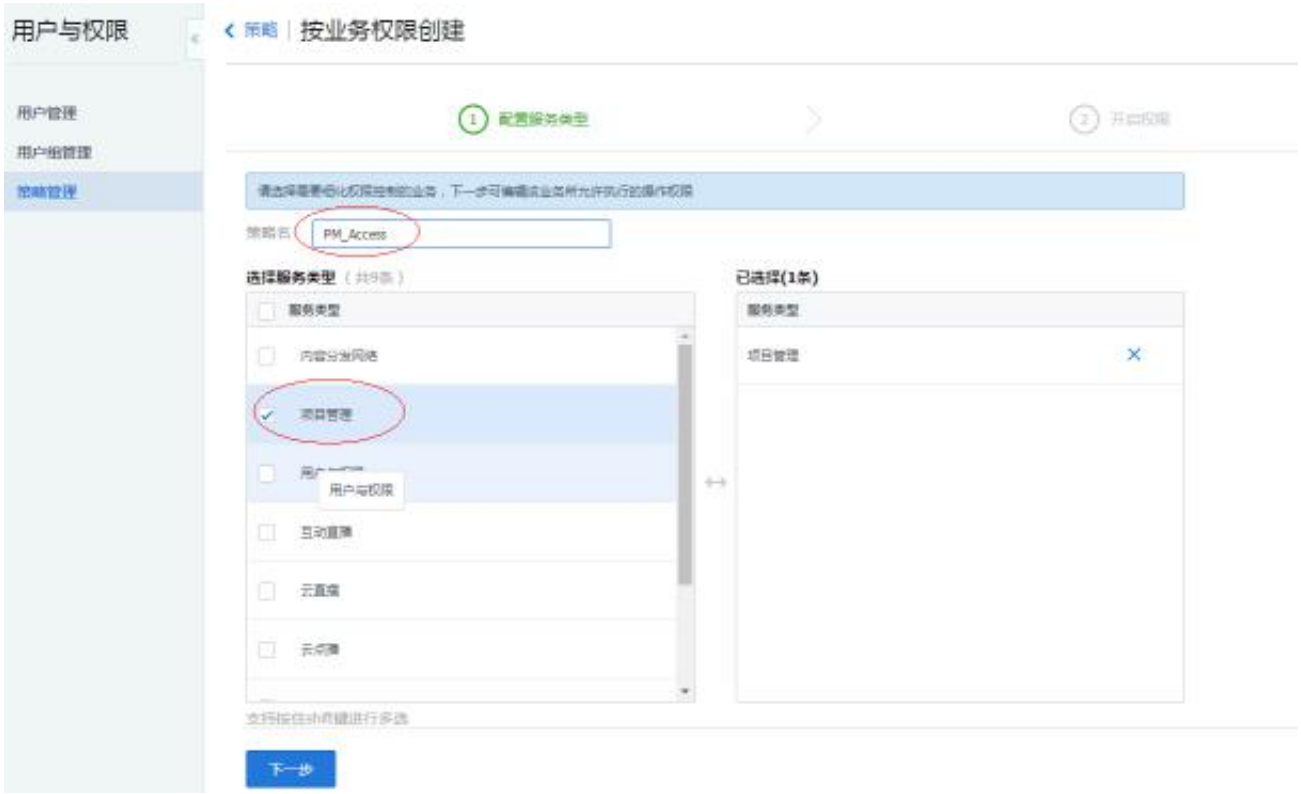
step3：点击创建策略。其中策略名称是自动生成的，其中前面的policygen是前缀，后面的数字是根据创建的时间来确定的，策略内容也是自动生成的，是我们之前选择的服务和操作所对应的，我们可以在策略内容里面进行微调，有相关问题的话，可以点击左下方策略语法说明和支持业务列表。



3.2按业务权限创建：

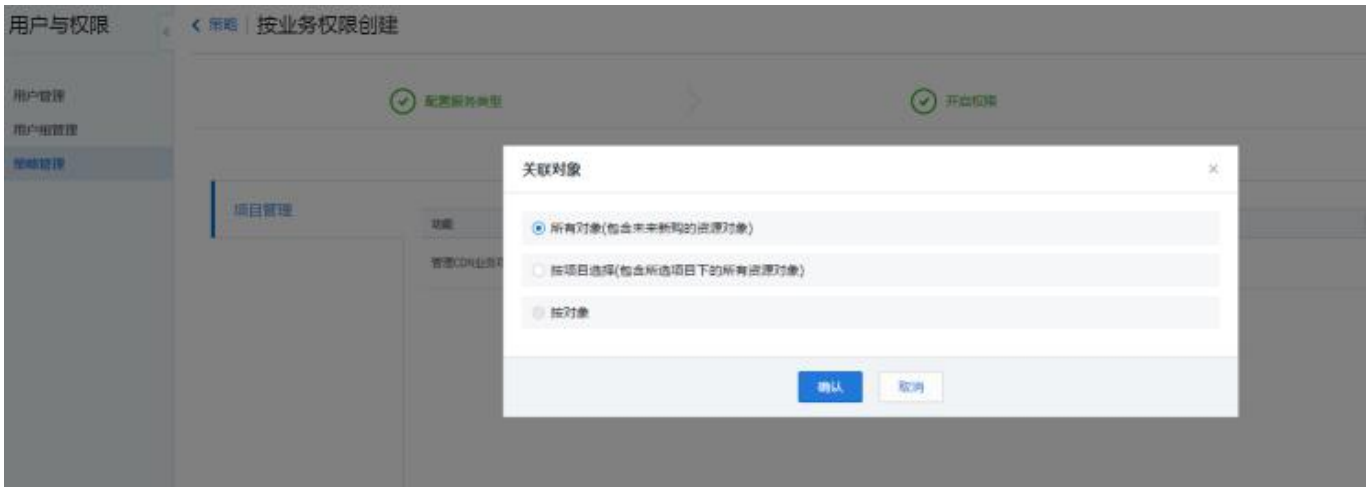
step1: 访问策略管理控制台，则点击【创建自定义策略】,并选择按业务权限创建。

step2: 添加业务至策略中并命名，点击下一步。

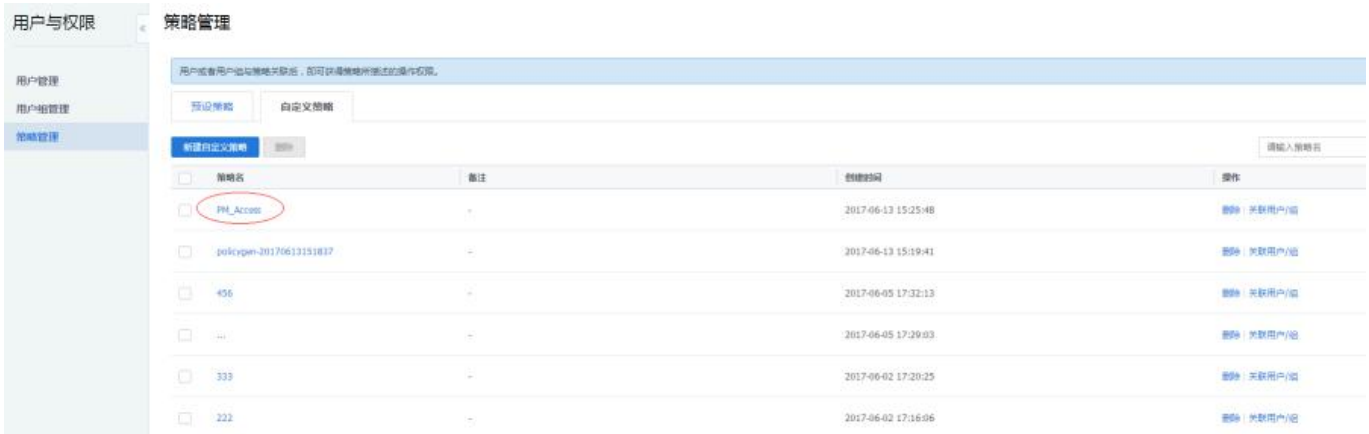


step3: 将某些功能的权限开关置为【开】，并点击下一步。

step4: 如果功能需要指定作用域，则需要添加相关的资源，然后点击保存。



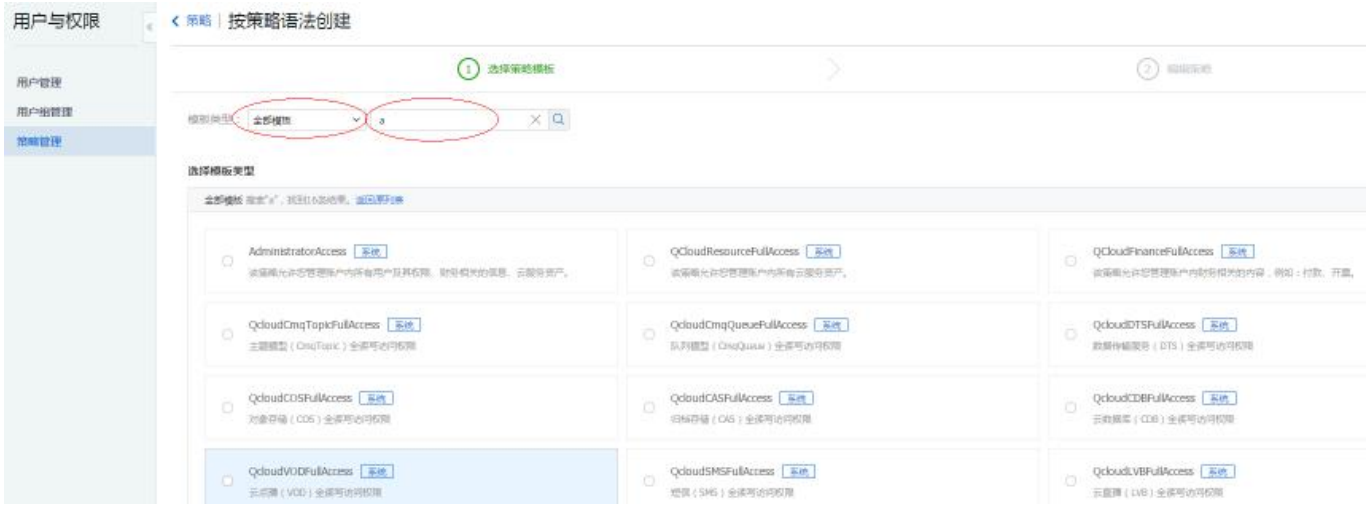
step5: 可以在策略列表中查看到策略。



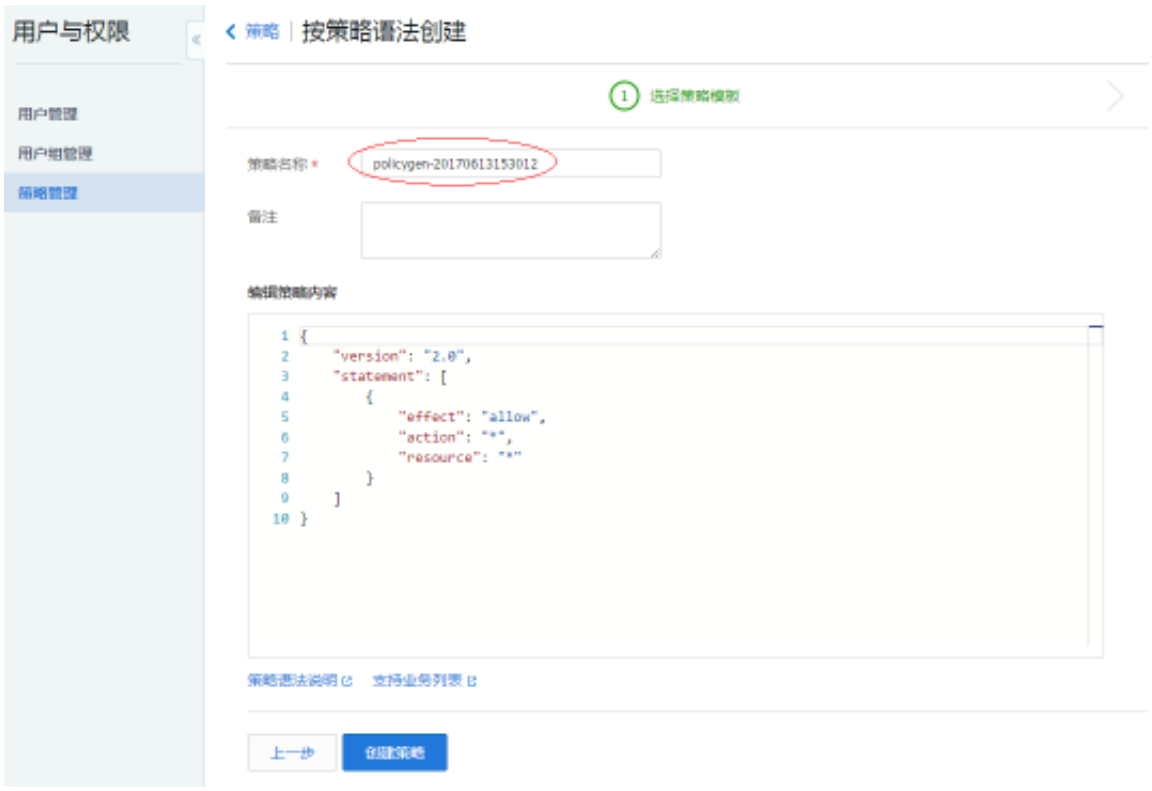
3.3按策略语法创建：

step1: 访问策略管理控制台，则点击【创建自定义策略】,并选择按策略语法创建。

step2:在这里可以选择模版类型，并且可以在确定模版类型之后，通过关键字搜索，搜索成功后，选择其中一个模版，然后点击下一步。在这里我们以模版类型为全部模版，关键字为a搜索，并选择AdministratorAccess模版。



step3：在这里会出现相应的模版的策略内容，我们可以在里面进行修改，修改完成后，点击创建策略。其中策略名称是自动生成的，其中前面的policygen是前缀，后面的数字是根据创建的时间来确定的，有相关问题的话，可以点击左下方策略语法说明和支持业务列表。


用户与权限
用户管理
用户组管理
策略管理
策略 | 按策略语法创建
1 选择策略模板
策略名称 *
policygen-20170613153012
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
上一步
创建策略

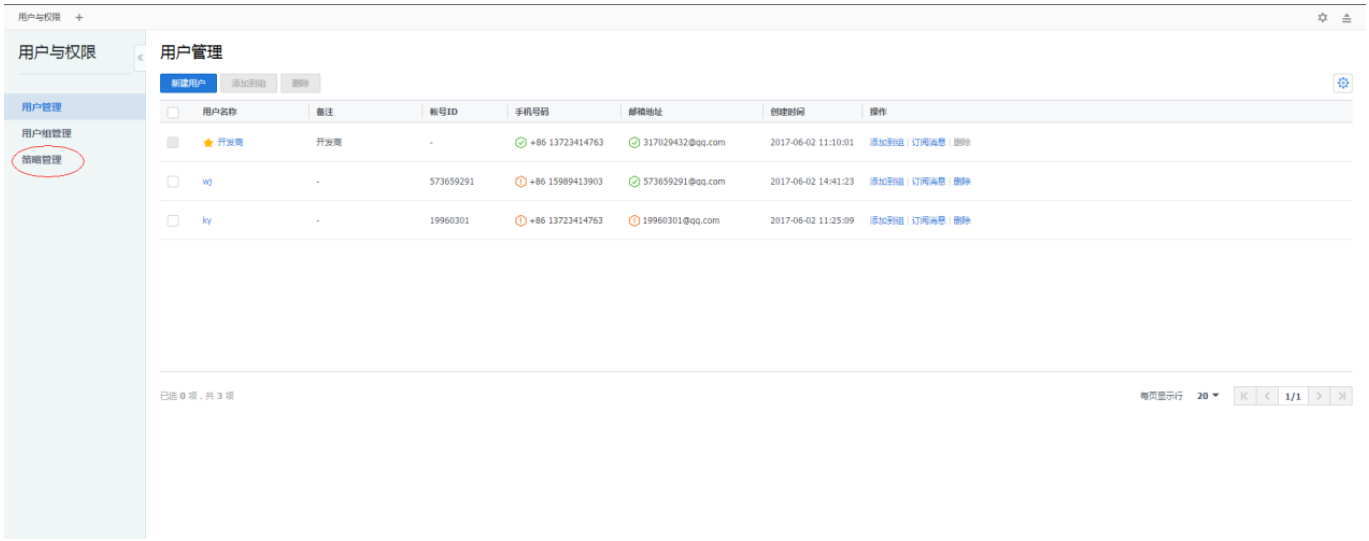
授权管理

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。

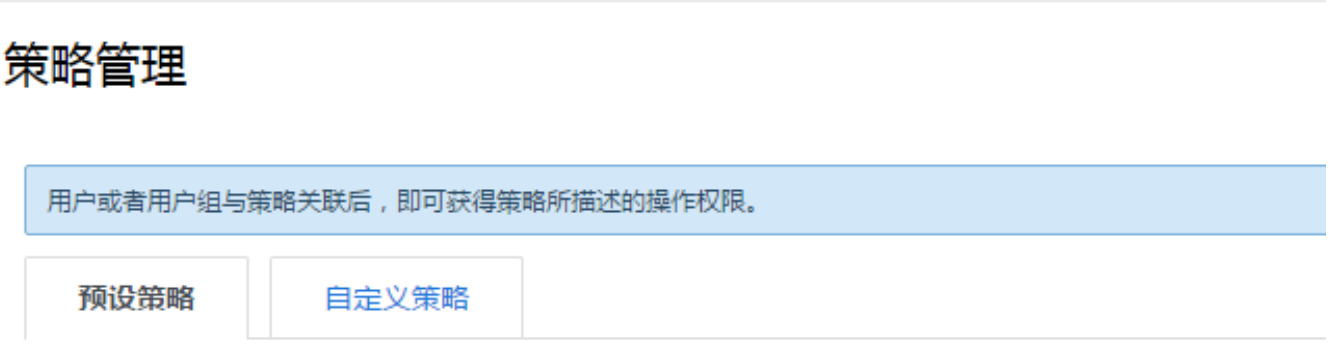
授权方式可以通过在策略页面选择用户或者在用户页面选择策略来完成。

通过策略关联用户/用户组：

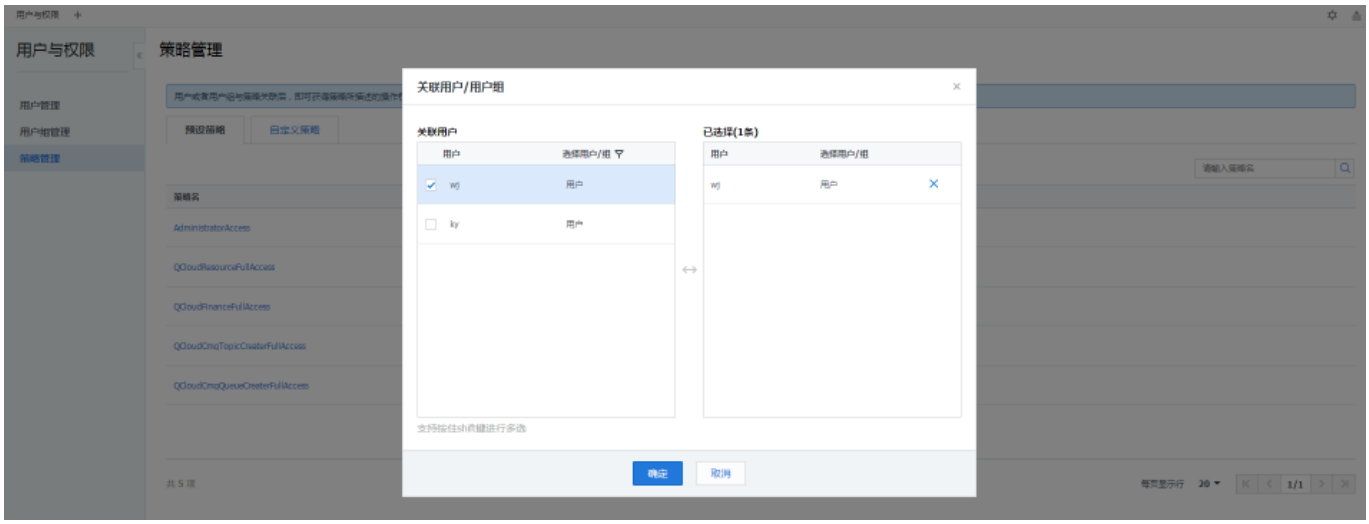
step1: 访问用户与权限控制台，并点击策略管理



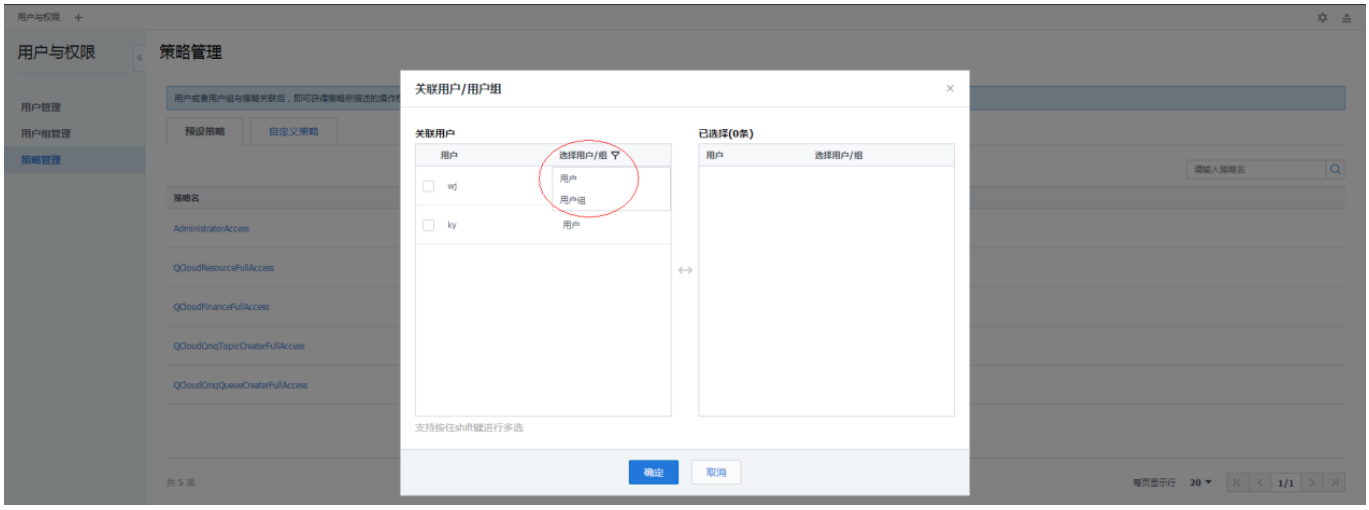
step2: 选择不同的策略方式去管理，预设策略和自定义策略管理，点击预设策略。



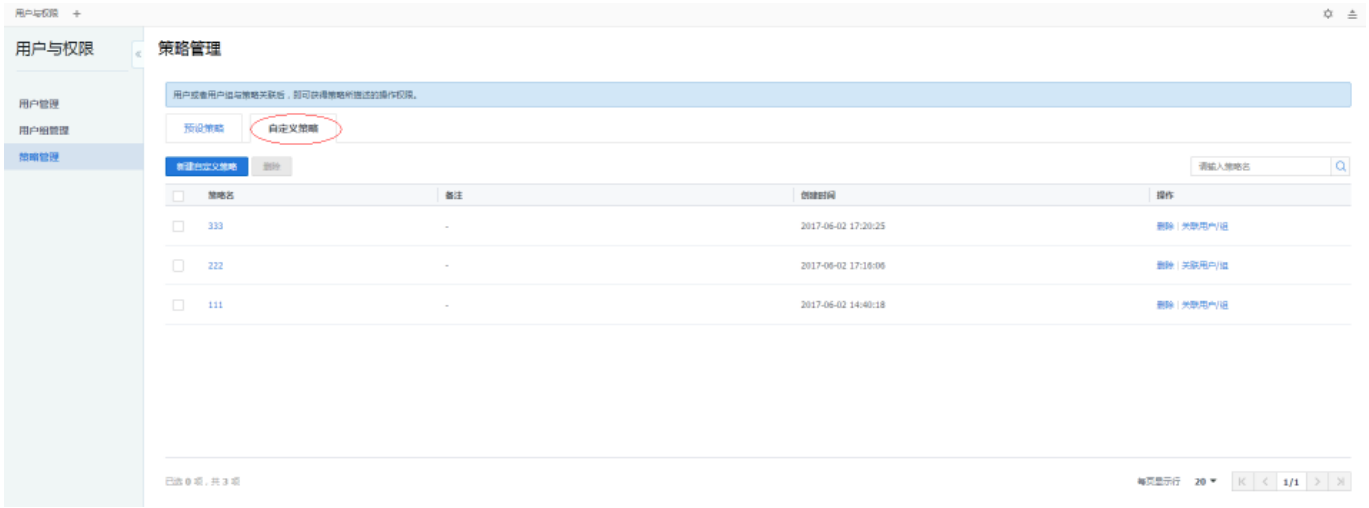
step3: 选择其中一项策略，点击关联用户/组，默认是用户界面，如果要关联用户，则勾选出要关联的对象，点击确定。



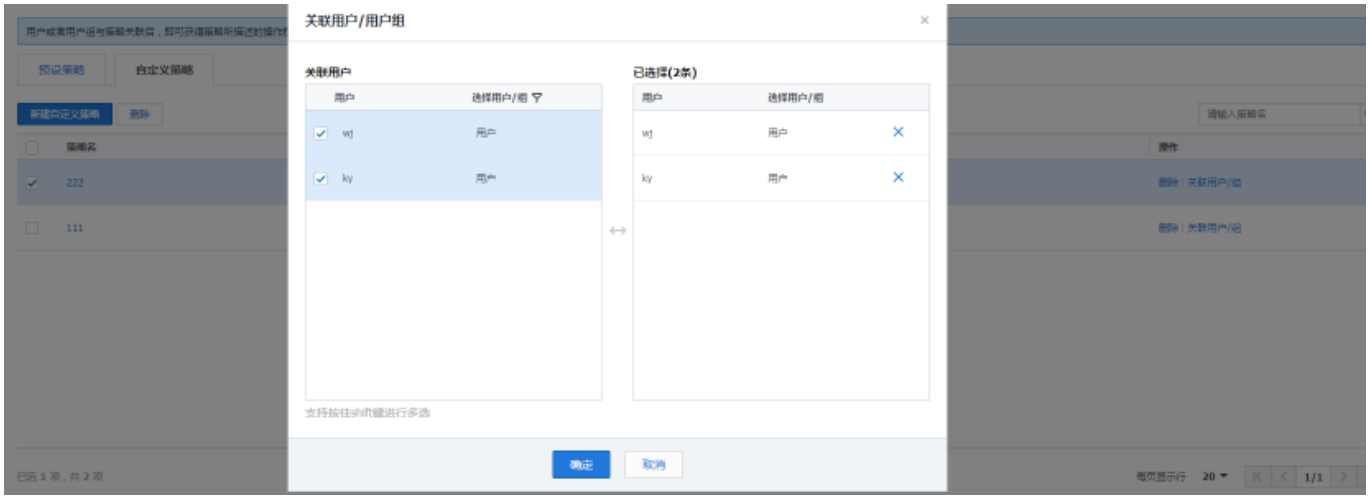
如果要关联组的话，点击选择用户/组，选择用户组，然后勾选出要关联的组，点击确定。



step4:如果按自定义策略管理，点击自定义策略。



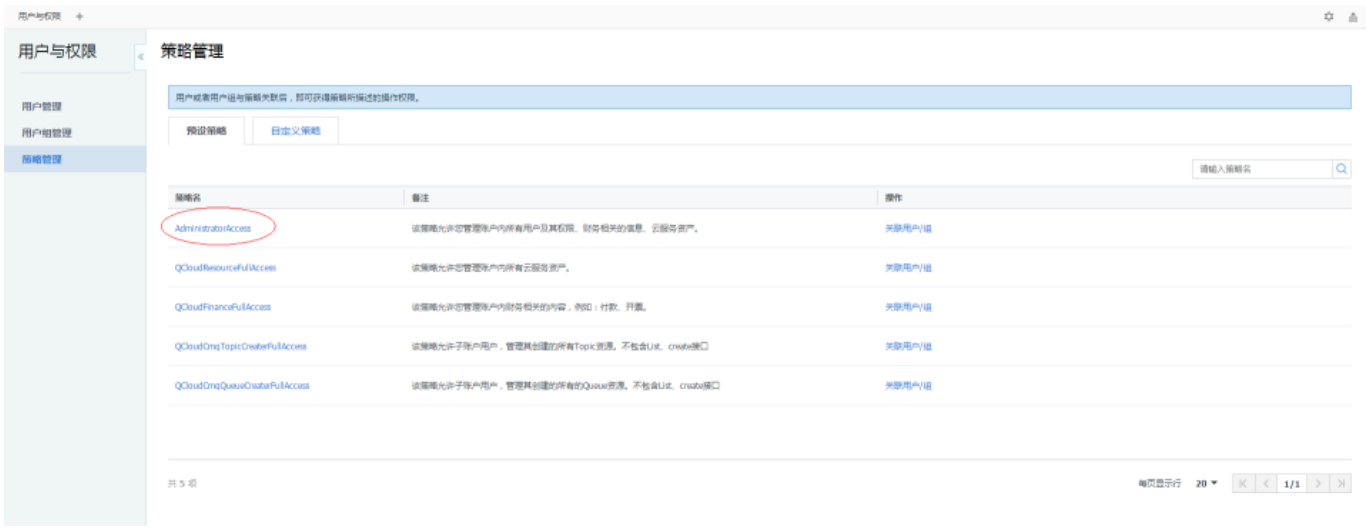
Step5：则勾选出要使用的自定义策略，并点击关联用户/组，默认是用户界面，如果要关联用户，则勾选出要关联的用户，点击确定。



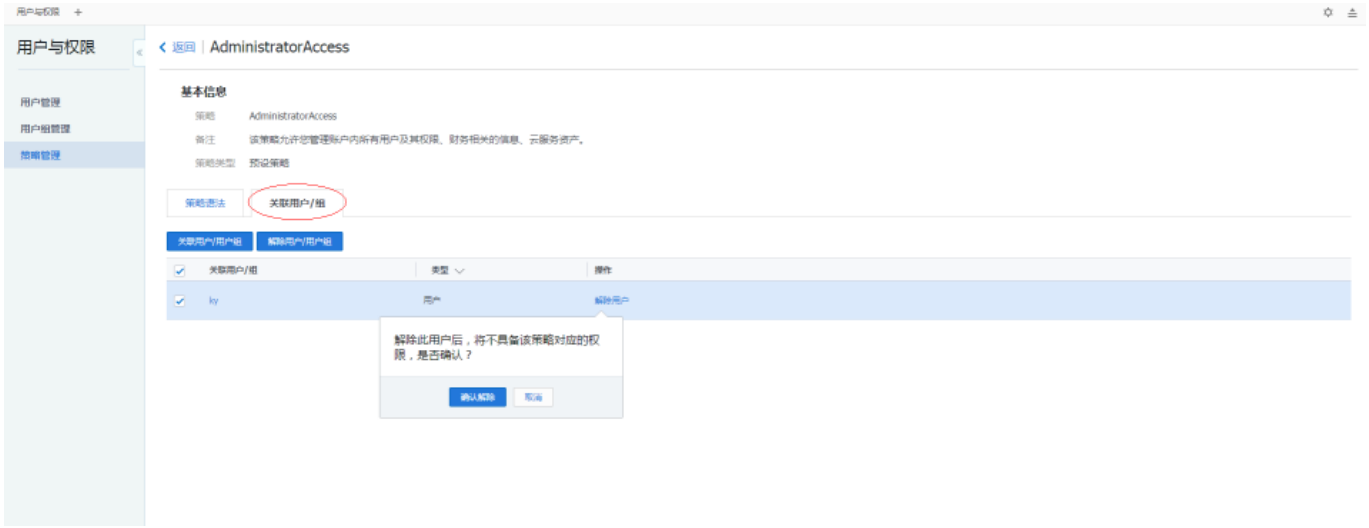
如果要关联组的话，点击选择用户/组，选择用户组，然后勾选出要关联的组，点击确定。

如果没有已经定义好的自定义策略，则参照https://www.qcloud.com/document/product/378/8955 去创建自定义策略。

如果想要解除关联的话，点击你想要解除关联的策略的策略名。

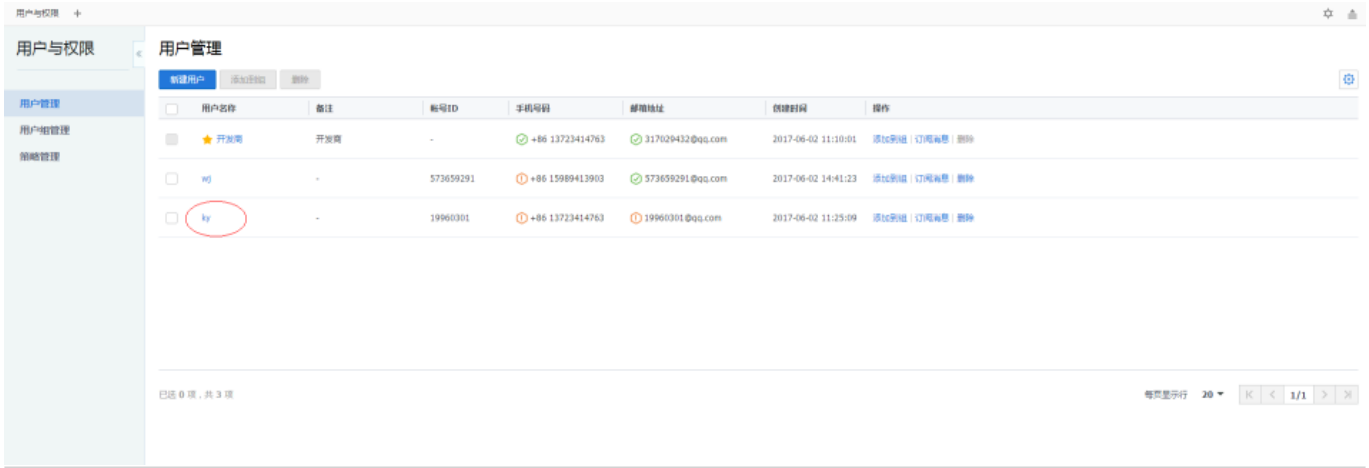


进入界面后，点击关联用户/组，勾选出你想解除关联的用户/用户组，点击解除用户/用户组。



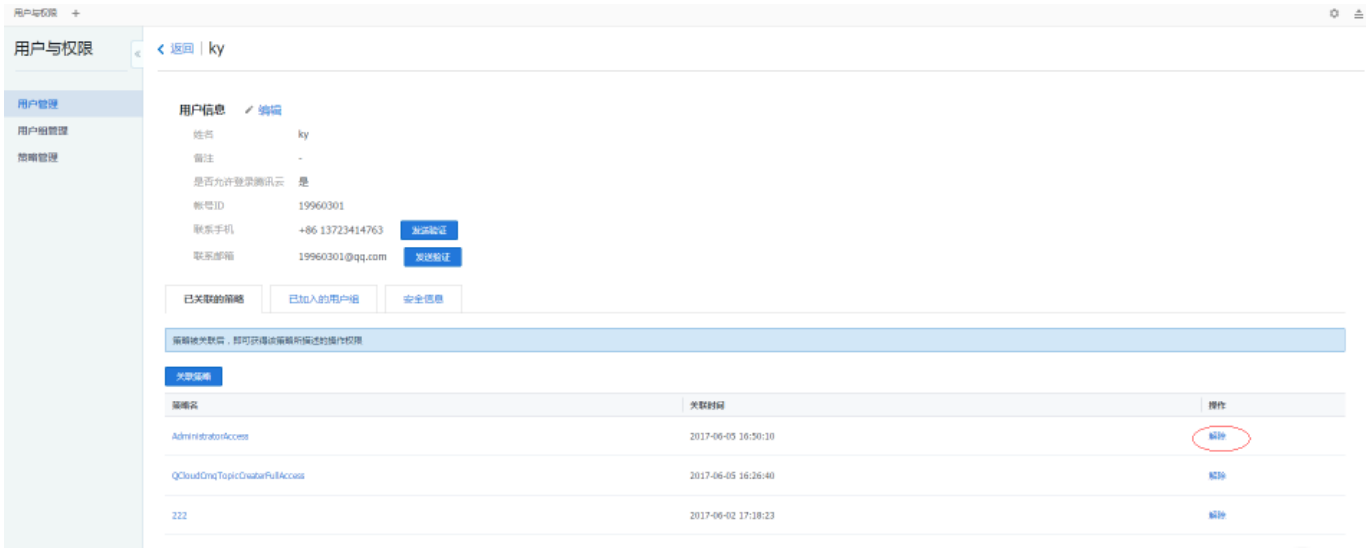
通过用户关联策略：

Step1：访问用户与权限控制台，点击用户管理，选择其中的一名用户，点击用户名称。



Step2：进入界面后，点击关联策略，然后在弹出的页面中勾选出一条或多条策略，可以是预设策略也可以是自定义策略。

如果想要解除关联的话，则在想解除关联的策略的那一栏上点击解除。



策略语法

元素参考

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)

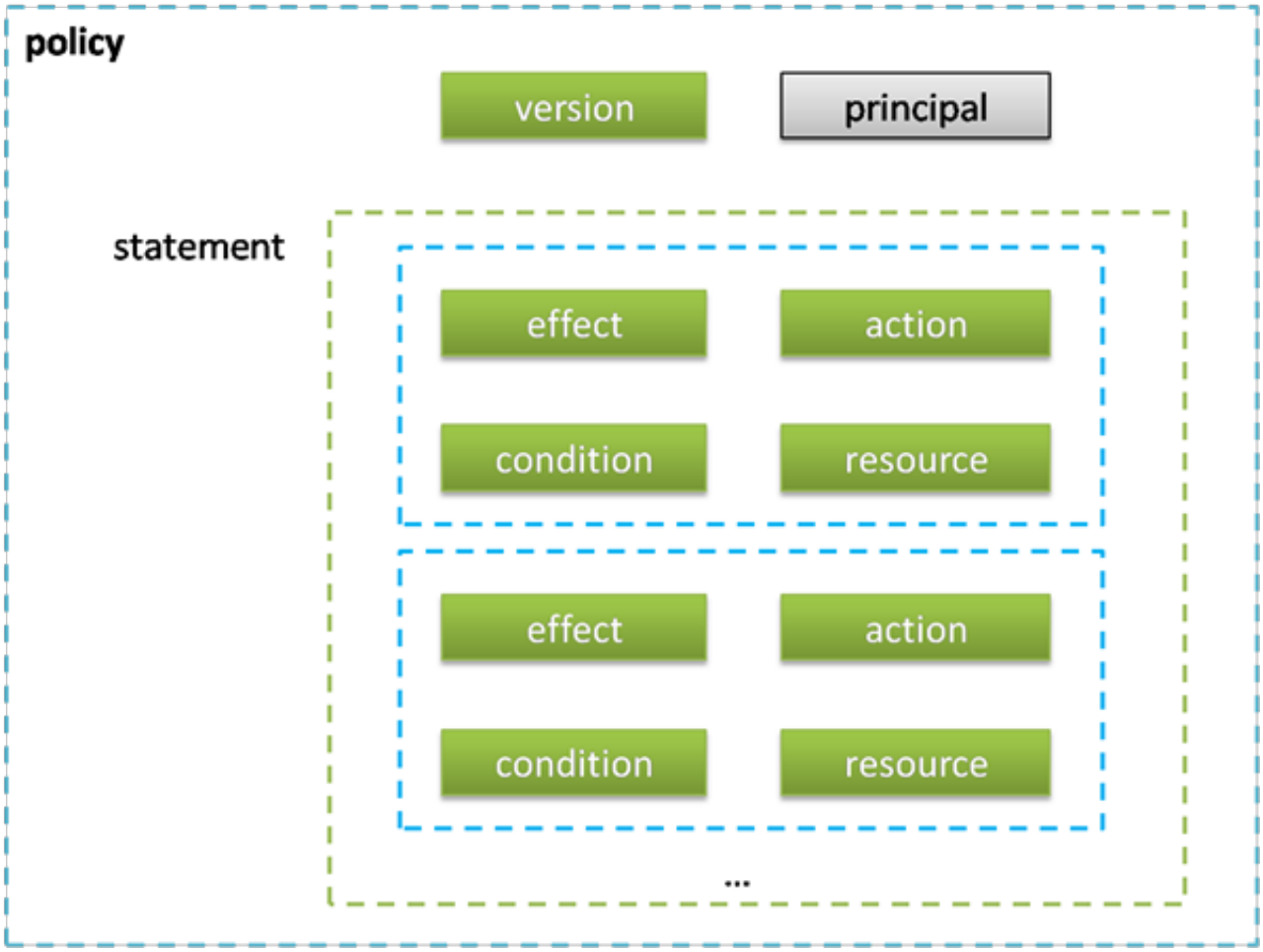
描述声明产生的结果是“允许”还是“显式拒绝”。包括allow(允许)和deny(显式拒绝)两种情况。该元素是必填项。

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/bucketA/*",
  "qcs::cos:gz:uid/1238423:prefix/bucketB/object2"],
  "condition": {"ip_equal":{"qcs:ip":"10.121.2.10/24"}}
  },
  {
  "effect":"allow",
  "action":"name/cmqqueue:Sendmessages",
  "resource":"*"
  }
  ]
}
```

语法结构



整个策略的语法结构如上图所示。

策略(policy)由版本(version)和语句(statement)构成，还可以包含委托人(principal)信息，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)这四个元素，其中condition是非必填项。

1.JSON格式

策略语法是以 JSON 格式为基础。创建或更新的策略不满足JSON格式时，无法提交成功，用户必须要确保 JSON 格式正确。JSON格式标准在 RFC 7159 中定义。您也可以使用在线 JSON 验证程序检查策略格式。

2.语法约定

语法描述中有如下约定：

1) 以下字符是包含在策略语法中的json字符：

{ } [ ] " , :

2) 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：

= < > ( ) |

3) 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>

4) 元素后的问号 (?) 表示该元素是非必填项。例如：

<condition_block?>

5) 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")

6) 字符串元素用双引号包括起来。例如：

<version_block> = "version" : "2.0"

3.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：

1) 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。

2) 当前支持的语法版本为2.0。

3) 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。

4) 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)。

5) 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 ）构成。

6) 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，我们遵循deny优先原则。

4.字符串说明

语法描述的元素字符串的一些说明。

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":"name/*:*"
//cos产品所有操作
"action":"name/cos:*"
//cos产品的名为GetBucketPolicy的操作
"action":"name/cos:GetBucketPolicy"
//cos产品部分匹配Bucket的操作
"action":"name/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":["name/cos:GetBucketPolicy","name/cos:PutBucketPolicy","name/cos: DeleteBucketPolicy"]

permid为各产品定义的操作集合ID。具体信息请参阅各产品的帮助文档。

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obje
ct资源，上海地域，资源拥有者的uid是1238423，资源名是bucket1/object2，资源前缀是prefix
qcs::cos:sh:uid/1238423:prefix/bucket1/object2
//cmq产品的队列，上
海地域，资源拥有者的uin是6887234，资源名是6887234/queueName1,资源前缀是queueName
qcs::cmqqueue:sh:uin/6887234:queueName/6887234/queueName1

condition_type_string:

条件操作符，描述测试条件的类型。例如string_equal、string_notequal、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":{"qcs:tag":["dev1","dev3"],
  "mfa":"1"]},
  "ip_equal":{"qcs:ip":"10.131.12.12/24"}
}
```

condition_key_string:

条件键，描述将对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。具体细节请参阅生效条件。

principal_id_string:

对于cam产品而言，用户也是它的资源。因此委托人(principal)也是用六段式描述。示例如下，具体细节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

腾讯云用户访问云资源时，CAM通过以下评估逻辑决定是否允许或拒绝给定。

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。

a.对于根账号，默认拥有其名下所有资源的访问权限；目前仅COS产品支持跨账号的资源访问。

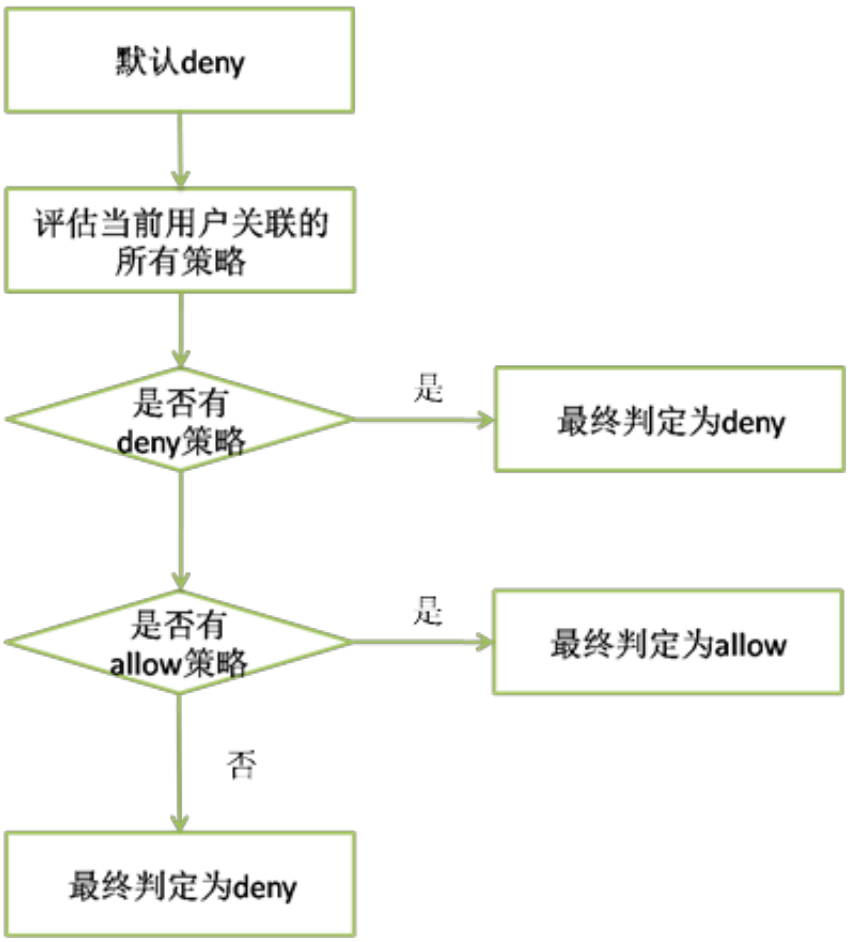
b.有些通用策略，会默认关联所有CAM用户。具体请见下文的通用策略表。

c.其他策略都必须显式指定，包括allow和deny策略。

3）如果有匹配deny策略，则最终判定为deny，不允许访问云资源。

4）如果有匹配allow策略，则最终判断为allow，允许访问云资源。

5）如果没有匹配任何策略，则最终判断为deny，不允许访问云资源。



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	{
	"principal":"",
	"action":"name/account:QueryKeyBySecretId",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

设置敏感操作需要MFA验证	{
	"principal":"",
	"action":"name/account:SetSafeAuthFlag",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

绑定token需要MFA验证	{ "principal":"",

策略说明	策略定义
	"action":"name/account:BindToken", "resource":"", "condition":{"string_equal":{"mfa":"0"}} }

解绑token需要MFA验证	{
	"principal":"",
	"action":"name/account:UnbindToken",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

修改邮箱需要MFA验证	{
	"principal":"",
	"action":"name/account:ModifyMail",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

修改手机号需要MFA验证	{
	"principal":"",
	"action":"name/account:ModifyPhoneNum",
	"resource":"",
	"condition":{"string_equal":{"mfa":"0"}}
	}

资源描述方式

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。

1.六段式

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：

1) qcs是qcloud service的简称，表示是腾讯云的云资源。该字段是必填项。

2) project_id描述项目信息，仅为了兼容CAM早期逻辑。这里请不填。

3) service_type描述产品简称，如cvm、cdn等，产品的检测具体细节请对应的产品文档。对于CAM产品简称是cam。值为"*"的时候表示所有产品。该字段是必填项。

4) region描述地域信息。值为空的时候表示所有地域。目前支持的地域列表如下所示：

地域缩写	描述
gz	广州IDC
sh	上海IDC
shjr	深圳金融IDC
bj	北京IDC
ca	加拿大IDC
sg	新加坡IDC

5)account描述资源拥有者的根账号信息。目前支持两种方式描述的资源拥有者。一种方式是uin方式，即根账号的qq号，表示为uin/${uin}，如uin/164256472；另外一种方式是uid方式，即根账号的appid，表示为uid/

${appid}如uid/1000382392。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。

6) 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。

a.<resource_type>/<resource_id>

表示某个资源子类下的资源ID。如VPC产品的vpc/vpc_id1

b. <resource_type>/<resource_path>

表示某个资源子类下的带路径的资源ID。如COS产品的prefix/1228934/bucketName1/object2。该方式下，支持目录级的前缀匹配。如prefix/1228934/bucketName1/*，表示bucketName1下的所有object。
c. <resource_type>/*
表示某个资源子类下的所有资源。如vpc/*。
d.*
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。

a.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。

b.操作(action)是不需要关联资源的操作时，resource都需要定义为"*"。

c.操作(action)中同时包含需要关联资源的操作和不需要关联资源的操作时，resource定义为"*"时，有两种含义，一方面描述需要关联资源的操作，都会关联所有资源；另外一方面描述不需要关联资源的操作。

2.CAM资源定义

CAM是腾讯云的一个产品，包含了用户、组、策略等资源。这里列出了CAM资源的描述方式。

根账号：

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

或者qcs::cam::uin/164256472:root

子账号：

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

组：

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

匿名用户：

qcs::cam::anonymous:anonymous

或者*

策略：

qcs::cam:: uin/164256472:policyid/*

qcs::cam:: uin/164256472:policyid/12423

3.资源的一些重要说明

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。

策略变量

1.使用场景

考虑下面这种场景：您希望给每个CAM用户授予其创建资源的访问权限。比如COS资源的创建者默认拥有该资源的访问权限。如果由资源拥有者(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。在策略的资源定义中包含占位符描述的创建人信息，该占位符即使策略变量。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。

创建者拥有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}/*"
  }
}
```

给每个资源的路径中带上创建人的uin。比如uin为12356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uin
12356)，即"qcs::cos::uid/1238423:prefix/12356/
"。策略中的资源"qcs::cos::uid/1238423:prefix/123
56/"可以通过前缀匹配访问的资源"qcs::cos::uid/1238423:prefix/12356/test"。

2.使用策略变量的位置

1）资源元素位置

策略变量可以用在资源六段式的最后一段。

2）条件元素位置

策略变量可以用在条件值中。

下述策略描述了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}"}}
  }
}
```

3.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
${uin}	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。
${owner_uin}	当前访问者所属的根账号uin。
${app_id}	当前访问者所属的根账号的appid。

生效条件

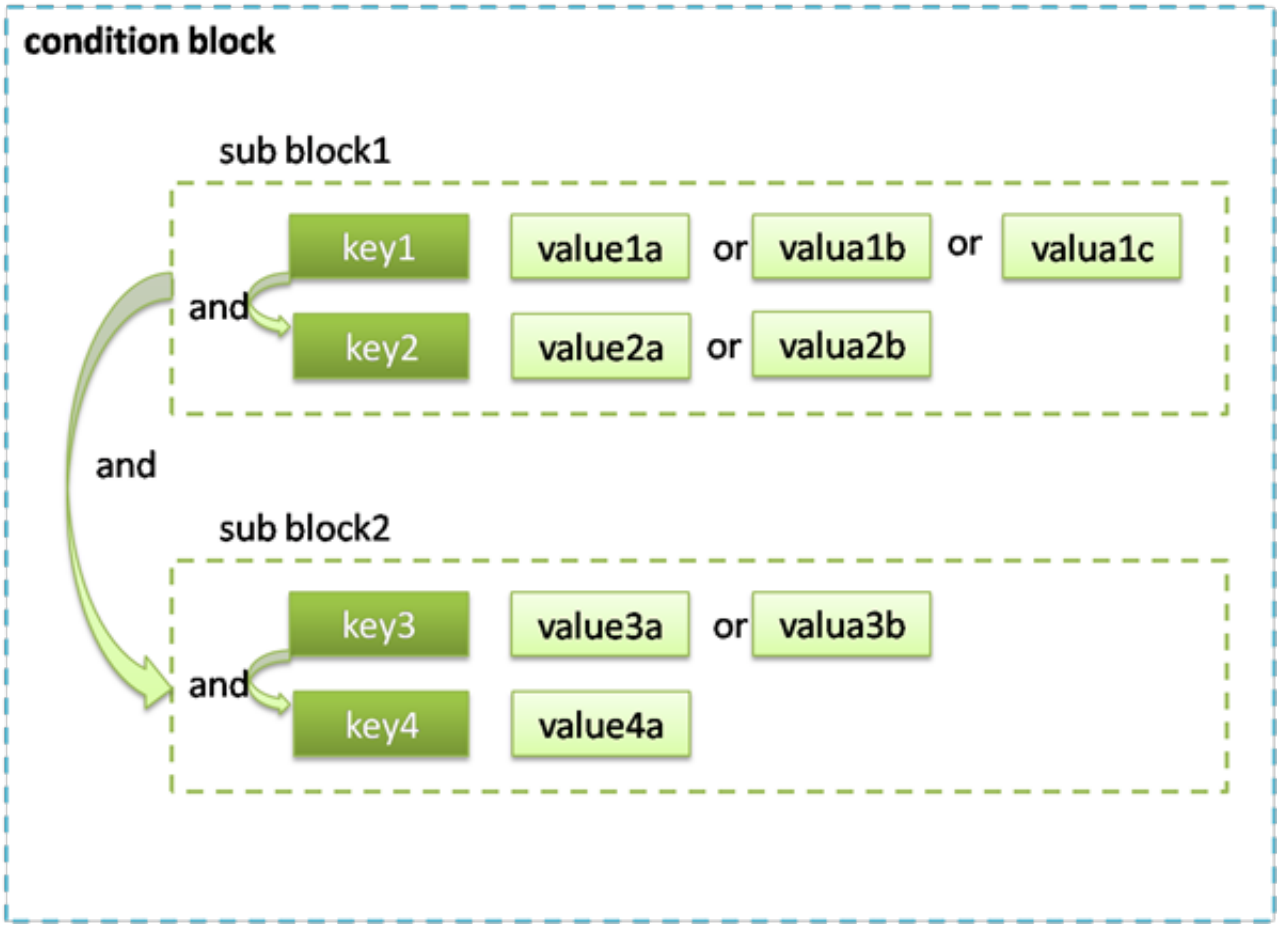
1.概念和使用场景

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。

2.语法结构



生效条件的语法结构如上图所示。

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。

3.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的条件键，如果上下文信息中不包含对应的键值，该条件依然生效。

4.使用示例

1)
该示例描述了允许给指定队列发送
消息，限制条件是用户必须在10.217.182. 或者111.21.33.的网段调用云API。

```
{
  "version": "2.0",
  "statement": {
  "effect": "allow",
  "action": "name/cmqqueue:Sendmessages",
  "resource": "qcs::cmq:sh::queueName/123877/test",
  "condition": {"ip_equal": {"qcs:ip": ["10.217.182.3/24", "111.21.33.72/24"]}}
  }
}
```

2) 该示例描述了允许VPC绑定指定的NAT网关，限制条件是VPC的地域是上海，且VPCID值为324238。

```
{
  "version": "2.0",
```

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

5.条件操作符列表

下面列出了目前支持的条件操作符列表以及通用的条件键和示例等信息。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
string_equal	字符串等于	qcs:tag	{"string_equal":{"qcs:tag/tag_name1":"tag_value1"}}
string_not_equal	字符串不等于	qcs:tag	{"string_not_equal":{"qcs:tag/tag_name1":"tag_value1"}}
date_not_equal	时间不等于	qcs:current_time	{"date_not_equal":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_greater_than	时间大于	qcs:current_time	{" date_greater_than ":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_greater_than_equal	时间大于等于	qcs:current_time	{" date_greater_than_equal ":{"qcs:current_time":"2016-06-01T00:01:00Z"}}
date_less_than	时间小于	qcs:current_time	{" date_less_than ":{"qcs:current_time":"2016-06-01T 00:01:00Z"}}

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":"2016-06-01T 00:01:00Z"}}
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}}

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) 条件键加上后缀_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) 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。

限制

限制

限制项	限制值
一个账号中的组数	20
一个账号中的用户数	1000
一个用户可加入的组的数量	10
一个组中的用户数	100
一个账号的策略数	1000
附加到一个CAM用户、组的策略数	20
自定义策略字符数	4096

最佳实践

基本指导原则

1.开启MFA保护

建议您为所有帐号绑定MFA；为根帐号开启登陆保护和敏感操作保护；为所有子账号都开启敏感操作保护。对于支持邮箱登陆或者微信登陆的强烈推荐进行MFA二次验证。

2.使用子账号访问腾讯云

请尽量不要使用根帐号的身份凭证访问腾讯云，更不要将身份凭证共享给他人。一般情况下，应该为所有访问腾讯云的用户创建子账号，同时授权该子帐号相应的管理权限。

3.使用组给子帐号分配权限

按照工作职责定义好组，并给组分配相应的管理权限。然后把用户分配到对应的组里。这样，当您修改了组的权限时，组里相关用户的权限随即发生了变更。另外，当组织架构发生调整时，只需要更新用户和组的关系即可。

4.最小权限原则

最小权限原则是一项标准的安全原则。即仅授予执行任务所需的最小权限，不要授予更多无关权限。例如，一个用户仅是CDN服务的使用者，那么不需要将其他服务的资源访问权限（如COS读写权限）授予给该用户。

5.分子帐号管理用户、权限和资源

建议同一个子账号不同时管理用户、权限和资源。应该让部分子账户管理用户，部分子账号管理权限，部分子账号管理其他云资源。

6.定期轮转身份凭证

建议您或CAM用户要定期轮换登录密码或云API密钥。这样可以让身份凭证绣楼情况下的影响时间受限。

7.删除不需要的证书和权限

删除用户不需要的证书以及用户不再需要的权限。尽量减少访问凭证泄漏后带来的安全风险。

8.使用策略条件来增强安全性

尽可能的为策略定义更精细化的条件，约束策略生效的场景，强化安全性。如约束用户必须在指定的时间，指定的服务器上执行某些操作等。

商用案例

CMQ相关案例

授权子帐号拥有消息服务的所有权限

企业帐号CompanyExample下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample名下的消息队列的所有权限，无论消息队列是主题模型还是队列模型，都可以被读写。

方案A：

企业帐号CompanyExample直接将预设策略QCloudCmqQueueFullAccess和QCloudCmqTopicFullAccess授权给子账号Developer。授权方式请参考授权管理。

方案B：

step1：通过策略语法方式创建以下策略

```
{
 "version": "2.0",
 "statement":
 {
 "effect": "allow",
 "action": ["name/cmqtopic:*","name/camqueue:*"]
 "resource": "*"
 }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子帐号拥有其创建的消息队列的所有权限

企业帐号CompanyExample下有一个子账号Developer，该子账号希望其可以访问自己创建的消息队列。

方案A：

企业帐号CompanyExample直接将预设策略QCloudCmqQueueCreaterFullAccess和QCloudCmqTopicCreaterFullAccess授权给子账号Developer。授权方式请参考授权管理。

方案B：

step1：通过策略语法方式创建以下策略

```
{
  "version": "2.0",
  "statement":
  [
  {
  "effect": "allow",
  "action": "name/cmqtopic:*",
  "resource": "qcs::cmqtopic:::topicName/uin/${uin}/*"
  },
  {
  "effect": "allow",
  "action": "name/cmqqueue:*",
  "resource": "qcs::cmqqueue:::queueName/uin/${uin}/*"
  }
  ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子帐号拥有特定的主题模型的消息队列的读权限

企业帐号CompanyExample（ownerUin为1234）有一个基于主题模型的消息队列，同时他有一个子账号Developer，希望其可以访问该消息队列。

step1：通过策略语法方式创建以下策略

```
{
  "version": "2.0",
  "statement":
  {
  "action": "name/cmqqueue:SendMessage",
  "resource":"qcs::cmqqueue:::queueName/uin/1234/test-caten",
  "effect": "allow"
  }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

COS相关案例

授权子帐号拥有COS资源的所有权限

企业帐号CompanyExample下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample名下的COS资源的所有权限

方案A：

企业帐号CompanyExample直接将预设策略QcloudCOSFullAccess授权给子账号Developer。授权方式请参考授权管理。

方案B：

step1：通过策略语法方式创建以下策略

```
{
  "version": "2.0",
  "statement":
  {
  "effect": "allow",
  "action": "name/cos:*"
  "resource": "*"
  }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

跨帐号访问权限和公有读写权限

请参考COS文档说明。

VPC相关案例

授权子帐号拥有VPC所有权限

企业帐号CompanyExample下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample名下所有VPC资源的读写权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudVPCFullAccess授权给子账号Developer。授权方式请参考授权管理。

方案B：

step1：通过策略语法方式创建以下策略

```
{
  "version": "2.0",
  "statement":
  {
  "action": "name/vpc:*",
  "resource": "*",
  "effect": "allow"
  }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子帐号拥有VPC只读权限

企业帐号CompanyExample下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample名下所有VPC资源的只读权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudVPCReadOnlyAccess授权给子账号Developer。授权方式请参考授权管理。

方案B：

step1：通过策略语法方式创建以下策略

```
{
  "version": "2.0",
  "statement": [
  {
  "action": [
  "name/vpc:Describe*",
  "name/vpc:Inquiry*",
  "name/vpc:Get*"
  ],
  "resource": "*",
  "effect": "allow"
  }
  ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子帐号管理VPC，但不能操作路由表

企业帐号CompanyExample下有一个子账号Developer，该子账号需要管理企业帐号CompanyExample名下所有VPC资源，但不能操作CompanyExample名下的路由表。

step1：通过策略语法方式创建以下策略

```
{
  "version": "2.0",
```

```
 "statement": [
 {
 "action": [
 "name/vpc:*"
 ],
 "resource": "*",
 "effect": "allow"
 },
 {
 "action": [
 "name/vpc:AssociateRouteTable",
 "name/vpc:CreateRoute",
 "name/vpc:CreateRouteTable",
 "name/vpc:DeleteRoute",
 "name/vpc:DeleteRouteTable",
 "name/vpc:ModifyRouteTableAttribute"
 ],
 "resource": "*",
 "effect": "deny"
 }
 ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。