访问管理

商用案例

产品文档

腾讯云

文档目录

商用案例
CDB相关案例
授权子账号拥有指定 CDB 实例的查看权限

最近更新时间：2018-06-20 11:32:18

授权子账号拥有指定CDB实例的查看权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample名下的两个cdb实例（实例id分别是cdb-1和cdb-2）的查看权限，

step1：通过策略语法方式创建以下策略

```
{
  "version": "2.0",
  "statement":
   {
      "effect": "allow",
      "action": "cdb:*",
      "resource": ["qcs::cdb::uin/12345678:instanceId/cdb-1", "qcs::cdb::uin/12345678:instanceId/cdb-2"]
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

注：子账号Developer在CDB的查询列表页同样仅能查看到实例id为cdb-1和cdb-2的资源。

CLB 相关案例
授权子账号拥有 CLB 的所有权限

最近更新时间：2018-06-20 11:06:41

授权子账号拥有CLB的所有权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CLB服务的完全管理权限（创建、管理、CLB下单支付等等全部操作）。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCLBFullAccess、QcloudCLBFinanceAccess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": "clb:*",
         "resource": "*"
      },
      {
           "effect": "allow",
           "action": "finance:*",
           "resource": "qcs::clb:::*"
      }
   ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有 CLB 的只读权限

最近更新时间：2018-06-20 11:06:54

授权子账号拥有CLB的只读权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CLB服务的查看权限，但子账号无法创建、更新或删除它们。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCLBReadOnlyAccess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": "clb:Describe*",
      "resource": "*"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有 CLB 的所有权限但不包括支付权限

最近更新时间：2018-06-20 11:07:05

授权子账号拥有CLB的所有权限但不包括支付权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CLB服务的所有权限管理权限（创建、管理等全部操作），但不包括支付权限，可以下单但无法支付。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCLBFullAccess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": "clb:*",
        "resource": "*"
     }
  ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

CMQ 相关案例
授权子账号拥有消息服务的所有权限

最近更新时间：2018-01-08 14:34:54

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": ["cmqtopic:*","camqueue:*"]
      "resource": "*"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有其创建的消息队列的所有权限

最近更新时间：2018-01-08 14:36:01

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

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有特定的主题模型的消息队列的读权限

最近更新时间：2018-01-08 14:36:32

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12345678）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": "cmqqueue:SendMessage",
      "resource":"qcs::cmqqueue:::queueName/uin/12345678/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
授权子账号拥有该账号下 COS 资源的所有权限

最近更新时间：2018-06-20 11:25:53

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的COS服务的完全管理权限（创建、管理、访问COS的存储桶或者对象）。

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": "cos:*",
      "resource": "*"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号对特定目录的所有权限

最近更新时间：2018-05-21 17:19:21

企业帐号 CompanyExample（ownerUin为12345678,appId为8000001）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的上海地域名为 Bucket1 的存储桶的 dir1 目录的完全访问权限。

方案 A：

步骤 1：通过策略语法方式创建以下策略。

```
{
  "version": "2.0",
  "statement":
   {
      "effect": "allow",
      "action": "cos:*",
      "resource": ["qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1/*",
            "qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1"]
   }
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参考 COS 文档。

授权子账号对特定目录内文件的读权限

最近更新时间：2018-05-21 17:19:02

企业帐号 CompanyExample（ownerUin 为 12345678,appId 为 8000001）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的上海地域名为 Bucket1 的存储桶的 dir1 目录下文件的读权限。

方案 A：

步骤 1：通过策略语法方式创建以下策略。

```
{
  "version": "2.0",
  "statement":
   {
      "effect": "allow",
      "action": [
              "cos:List*",
              "cos:Get*",
              "cos:Head*",
              "cos:OptionsObject"
          ],
      "resource": "qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1/*"
   }
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参考 COS 文档。

授权子账号对特定文件的读写权限

最近更新时间：2018-05-21 17:15:51

企业帐号 CompanyExample（ownerUin为12345678,appId为8000001）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的上海地域名为 Bucket1 的存储桶的 dir1 目录下对象 Object1 的读写权限。

方案 A：

步骤 1：通过策略语法方式创建以下策略。

```
{
  "version": "2.0",
  "statement":
   {
      "effect": "allow",
      "action": "cos:*",
      "resource": "qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1/Object1"
   }
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参考 COS 文档。

授权子账号拥有 COS 资源的读权限

最近更新时间：2018-06-20 11:26:04

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的COS服务的只读访问权限（访问COS的存储桶或者对象及对象列表等）。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCOSReadOnlyAccess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": [
              "cos:List*",
              "cos:Get*",
              "cos:Head*",
              "cos:OptionsObject"
          ],
      "resource": "*"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号对特定目录下所有文件的读写权限并禁止对该目录下指定文件的读写权限

最近更新时间：2018-05-21 17:23:18

企业帐号 CompanyExample（ownerUin为12345678,appId为8000001）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的上海地域名为 Bucket1 的存储桶的 dir1 目录下所有对象的读写权限，但没有该目录下对象 Object1 的读写权限。

方案 A：

步骤 1：通过策略语法方式创建以下策略。

```
{
  "version": "2.0",
  "statement":
  [
   {
      "effect": "allow",
      "action": "cos:*",
      "resource": "qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1/*"
   },
   {
      "effect": "deny",
      "action": "cos:*",
      "resource": "qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1/Object1"
   }
  ]
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参考 COS 文档。

授权子账号对指定前缀的文件的读写权限

最近更新时间：2018-05-21 17:25:38

企业帐号 CompanyExample（ownerUin为12345678,appId为8000001）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的上海地域名为 Bucket1 的存储桶的 dir1 目录下以 test 为前缀的对象的读写权限。

方案 A：

步骤 1：通过策略语法方式创建以下策略。

```
{
  "version": "2.0",
  "statement":
   {
      "effect": "allow",
      "action": "cos:*",
      "resource": "qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1/test*"
   }
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参考 COS 文档。

授权所有用户对指定文件的读写权限

最近更新时间：2018-05-21 17:27:58

企业帐号 CompanyExample（ownerUin为12345678,appId为8000001）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的上海地域名为 Bucket1 的存储桶的 dir1 目录下对象 Object1 的读写权限。

方案 A：

步骤 1：通过策略语法方式创建以下策略。

```
{
  "version": "2.0",
  "statement":
   {
      "effect": "allow",
      "action": "cos:*",
      "resource": "qcs::cos:ap-shanghai:uid/8000001:prefix//8000001/Bucket1/dir1/Object1"
   }
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参考 COS 文档。

授权跨账号对指定文件的读写权限

最近更新时间：2018-01-08 17:36:06

企业帐号CompanyGranter（ownerUin为12345678,appId为8000001）,该账号拥有一个对象Object1，在广州地域名为Bucket1的存储桶的dir1目录下。另外一个企业帐号CompanyGrantee（ownerUin为87654321）,需要拥有上述对象的读写权限。

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参考 COS 文档。

授权跨账号的子账号对指定文件的读写权限

最近更新时间：2018-01-08 17:36:21

企业帐号CompanyGranter（ownerUin为12345678,appId为8000001）,该账号拥有一个对象Object1，在广州地域名为Bucket1的存储桶的dir1目录下。另外一个企业帐号CompanyGrantee（ownerUin为87654321）,其子账号需要拥有上述对象的读写权限。

这里涉及权限传递。

step1：企业帐号CompanyGrantee通过策略语法方式创建以下策略

```
{
  "version": "2.0",
  "statement":
   {
      "effect": "allow",
      "action": "cos:*",
      "resource": "qcs::gz:cvm:uid/8000001:prefix//8000001/Bucket1/dir1/Object1"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

step3：企业帐号 CompanyGranter 通过COS控制台进行 Policy 和 ACL 设置，将对象Object1授权给企业帐号CompanyGrantee，具体请参考COS文档。

CVM 相关案例
授权子账号拥有 CVM 的所有权限

最近更新时间：2018-06-20 11:26:29

授权子账号拥有CVM的所有权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的完全管理权限（创建、管理、云服务器下单支付等全部操作权限）。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMFullAccess、QcloudCVMFinanceAccess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": "cvm:*",
         "resource": "*"
      },
      {
           "effect": "allow",
           "action": "finance:*",
           "resource": "qcs::cvm:::*"
      }
   ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有 CVM 的只读权限

最近更新时间：2018-06-20 11:26:39

授权子账号拥有CVM的只读权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查询CVM实例的权限，但是不具有创建、删除、开关机的权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMInnerReadOnlyAccess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": [
           "cvm:Describe*",
           "cvm:Inquiry*"
           ],
      "resource": "*"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有 CVM 相关资源的只读权限

最近更新时间：2018-06-20 11:26:49

授权子账号拥有CVM相关资源的只读权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查询 CVM 实例及相关资源（VPC 、CLB）的权限，但是不具有创建、删除、开关机的权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMReadOnlyAccess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": [
            "cvm:Describe*",
            "cvm:Inquiry*"
         ],
         "resource": "*",
         "effect": "allow"
      },
      {
         "action": [
            "vpc:Describe*",
            "vpc:Inquiry*",
            "vpc:Get*"
         ],
         "resource": "*",
         "effect": "allow"
      },
      {
         "action": [
            "clb:Describe*"
         ],
         "resource": "*",
         "effect": "allow"
      },
```

```
        {
            "effect": "allow",
            "action": "monitor:*",
            "resource": "*"
        }
    ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有弹性云盘的操作权限

最近更新时间：2018-01-08 17:47:24

授权子账号拥有弹性云盘的操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查看CVM控制台中的云硬盘信息，创建云硬盘，使用云硬盘的权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCBSFullAccess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": [
            "cvm:CreateCbsStorages",
            "cvm:AttachCbsStorages",
            "cvm:DetachCbsStorages",
            "cvm:ModifyCbsStorageAttributes",
            "cvm:DescribeCbsStorages",
            "cvm:DescribeInstancesCbsNum",
            "cvm:RenewCbsStorage",
            "cvm:ResizeCbsStorage"
           ],
         "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。

注：如果不允许子账号修改云硬盘属性，请去掉上述策略语法的"cvm:ModifyCbsStorageAttributes"。

授权子账号拥有安全组的操作权限

最近更新时间：2018-01-08 17:47:40

授权子账号拥有安全组的操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的查看CVM控制台中的安全组，并且使用安全组的权限。

以下策略允许子账号在CVM 控制台中具有创建，删除安全组的权限。

step1：通过策略语法方式创建以下策略

```
{
   "version": "2.0",
   "statement": [
      {
         "action": [
            "cvm:DeleteSecurityGroup",
            "cvm:CreateSecurityGroup"
         ],
         "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。

以下策略允许子账号在CVM 控制台中具有创建、删除修改安全组策略的权限。

step1：通过策略语法方式创建以下策略

```
{
   "version": "2.0",
   "statement": [
      {
         "action": [
            "cvm:ModifySecurityGroupPolicy",
            "cvm:CreateSecurityGroupPolicy",
            "cvm:DeleteSecurityGroupPolicy"
         ],
         "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。

授权子账号拥有弹性 IP 地址的操作权限

最近更新时间：2018-06-20 11:27:02

授权子账号拥有弹性IP地址的操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的查看CVM控制台中的弹性IP地址，并且使用弹性IP地址的权限。

step1：通过策略语法方式创建以下策略

```
{
   "version": "2.0",
   "statement": [
      {
         "action": [
            "cvm:AllocateAddresses",
            "cvm:AssociateAddress",
            "cvm:DescribeAddresses",
            "cvm:DisassociateAddress",
            "cvm:ModifyAddressAttribute",
            "cvm:ReleaseAddresses"
         ],
         "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。

以下策略允许子账号查看弹性IP地址并可以将其分配给实例并与之相关联。子账号可以修改弹性IP地址的属性、取消弹性IP地址的关联或释放弹性IP地址。。

step1：通过策略语法方式创建以下策略

```
{
   "version": "2.0",
   "statement": [
      {
         "action": [
            "cvm:DescribeAddresses",
            "cvm:AllocateAddresses",
            "cvm:AssociateAddress"
         ],
```

```
            "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。

授权子账号拥有特定 CVM 的操作权限

最近更新时间：2018-06-20 11:27:15

授权子账号拥有特定CVM的操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的指定CVM机器（id为ins-1,广州地域）的操作权限。

step1：通过策略语法方式创建以下策略

```
{
    "version": "2.0",
    "statement": [
        {
            "action": "cvm:*",
            "resource": "qcs::cvm:gz::instance/ins-1",
            "effect": "allow"
        }
    ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有特定地域的 CVM 的操作权限

最近更新时间：2018-06-20 11:27:25

授权子账号拥有特定地域的CVM的操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的广州地域所有机器的操作权限。

step1：企业帐号CompanyExample直接将预设策略QcloudCVMReadOnlyAccess授权给子账号Developer。授权方式请参考授权管理。

step2：通过策略语法方式创建以下策略

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

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有 CVM 的所有权限但不包括支付权限

最近更新时间：2018-06-20 11:27:40

授权子账号拥有CVM的所有权限但不包括支付权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的CVM服务的所有权限管理权限（创建、管理等全部操作），但不包括支付权限，可以下单但无法支付。

方案A：

企业帐号CompanyExample直接将预设策略QcloudCVMFullAccess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": "cvm:*",
        "resource": "*"
     }
  ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授予子账号拥有项目管理的操作权限

最近更新时间：2018-06-08 14:54:07

企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，需要基于项目授权子账号在控制台管理资源。

Step 1：
按业务权限创建项目管理自定义策略，参考 策略。

Step 2：
给子账号关联创建好的自定义策略，参考 授权管理。

子账号做项目管理时如遇到无权限提示，例如，查看快照、镜像、VPC、弹性公网 IP 等产品时提示无权限，可授权子账号QcloudCVMAccessForNullProject、QcloudCVMOrderAccess 和 QcloudCVMLaunchToVPC 预设策略。授权方式请参考 授权管理。

VPC 相关案例
授权子账号拥有 VPC 的只读权限

最近更新时间：2018-06-20 11:31:33

授权子账号拥有VPC的只读权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的VPC服务的只读权限（查询VPC及相关资源。但无法创建、更新或删除它们）。

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": [
            "vpc:Describe*",
            "vpc:Inquiry*",
            "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。

授权子账号拥有特定 VPC 及该 VPC 内资源的操作权限

最近更新时间：2018-06-20 11:28:07

授权子账号拥有特定VPC及该VPC内资源的操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的VPC服务的特定VPC（id是vpc-id1）及该VPC下的网络资源（如子网、路由表等，不包括云主机、数据库等）的操作权限。

step1：通过策略语法方式创建以下策略

```
{
   "version": "2.0",
   "statement": [
      {
         "action": "vpc:*",
         "resource": "*",
         "effect": "allow",
         "condition": {
            "string_equal_if_exist": {
               "vpc:vpc": [
               "vpc-id1"
               ],
               "vpc:accepter_vpc": [
                "vpc-id1"
               ],
                "vpc:requester_vpc": [
                "vpc-id1"
               ]
            }
         }
      }
   ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有 VPC 的操作权限但无路由表操作权限

最近更新时间：2018-06-20 11:28:19

授权子账号拥有VPC的操作权限但无路由表操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的VPC服务的读写VPC及其相关资源的权限，但是不允许对路由表进行相关操作。

step1：通过策略语法方式创建以下策略

```
{
   "version": "2.0",
   "statement": [
      {
         "action": [
            "vpc:*"
         ],
         "resource": "*",
         "effect": "allow"
      },
      {
         "action": [
            "vpc:AssociateRouteTable",
            "vpc:CreateRoute",
            "vpc:CreateRouteTable",
            "vpc:DeleteRoute",
            "vpc:DeleteRouteTable",
            "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。

授权子账号拥有 VPN 的操作权限

最近更新时间：2018-06-20 11:28:34

授权子账号拥有VPN的操作权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的VPC服务的查看所有VPC资源，但只允许其对VPN进行增、删、改、查操作的权限。

step1：通过策略语法方式创建以下策略

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

授权子账号拥有 VPC 的所有权限

最近更新时间：2018-06-20 11:31:42

授权子账号拥有VPC的所有权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的VPC服务的完全管理权限（创建、管理等全部操作）。

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":
   {
      "effect": "allow",
      "action": "vpc:*",
      "resource": "*"
   }
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权子账号拥有 VPC 的所有权限但不包括支付权限

最近更新时间：2018-06-20 11:29:16

授权子账号拥有VPC的所有权限但不包括支付权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的VPC服务的所有权限管理权限（创建、管理等全部操作），但不包括支付权限，可以下单但无法支付。

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":[
     {
        "effect": "allow",
        "action": "vpc:*",
        "resource": "*"
     }
  ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

云点播相关案例
授权子账号拥有云点播的所有权限

最近更新时间：2018-01-08 15:12:32

授权子账号拥有云点播的所有权限

企业帐号CompanyExample（ownerUin为12345678）下有一个子账号Developer，该子账号需要拥有对企业帐号CompanyExample的云点播服务的完全管理权限。

方案A：

企业帐号CompanyExample直接将预设策略QcloudVODFullAccess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": [
            "vod:*"
         ],
         "resource": "*",
         "effect": "allow"
      },
      {
         "action": "cos:*",
         "resource": "qcs::cos::uid/10022853:*",
         "effect": "allow"
      }
   ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

其他案例
授权子账号拥有所有资源的操作权限

最近更新时间：2018-01-08 17:51:22

授权子账号拥有所有资源的操作权限

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名下的所有资源都有完全访问权限。

方案A：

企业帐号CompanyExample直接将预设策略AdministratorAccess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": "*",
         "resource": "*"
      }
   ]
}
```

step2：将该策略授权给子账号。授权方式请参考授权管理。

授权腾讯云第三方应用访问用户资源

最近更新时间：2018-01-08 17:51:34

授权腾讯云第三方应用访问用户资源

使用腾讯云账户登录腾讯云的第三方应用，通过用户授权之后，第三方应用可以访问被授权的用户云资源

具体请参考第三方应用文档。

授权子账号拥有所有资源的只读权限

最近更新时间：2018-01-08 17:51:48

授权子账号拥有所有资源的只读权限

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名下的所有资源都有完全访问权限。

方案A：

企业帐号CompanyExample直接将预设策略ReadOnlyAccess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": [
                "cvm:Describe*",
                "cvm:Inquiry*",
                "vpc:Describe*",
                "vpc:Inquiry*",
                "vpc:Get*",
                "clb:Describe*",
                "monitor:*",
                "bm:Describe*",
                "bmeip:Describe*",
                "bmlb:Describe*",
                "bmvpc:Describe*",
                "bm:Get*",
                "bmlb:Get*",
                "cos:List*",
                "cos:Get*",
                "cos:Head*",
                "cos:OptionsObject",
                "cas:Describe*",
                "cas:List*",
                "cas:Get*",
                "kms:List*",
                "kms: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。

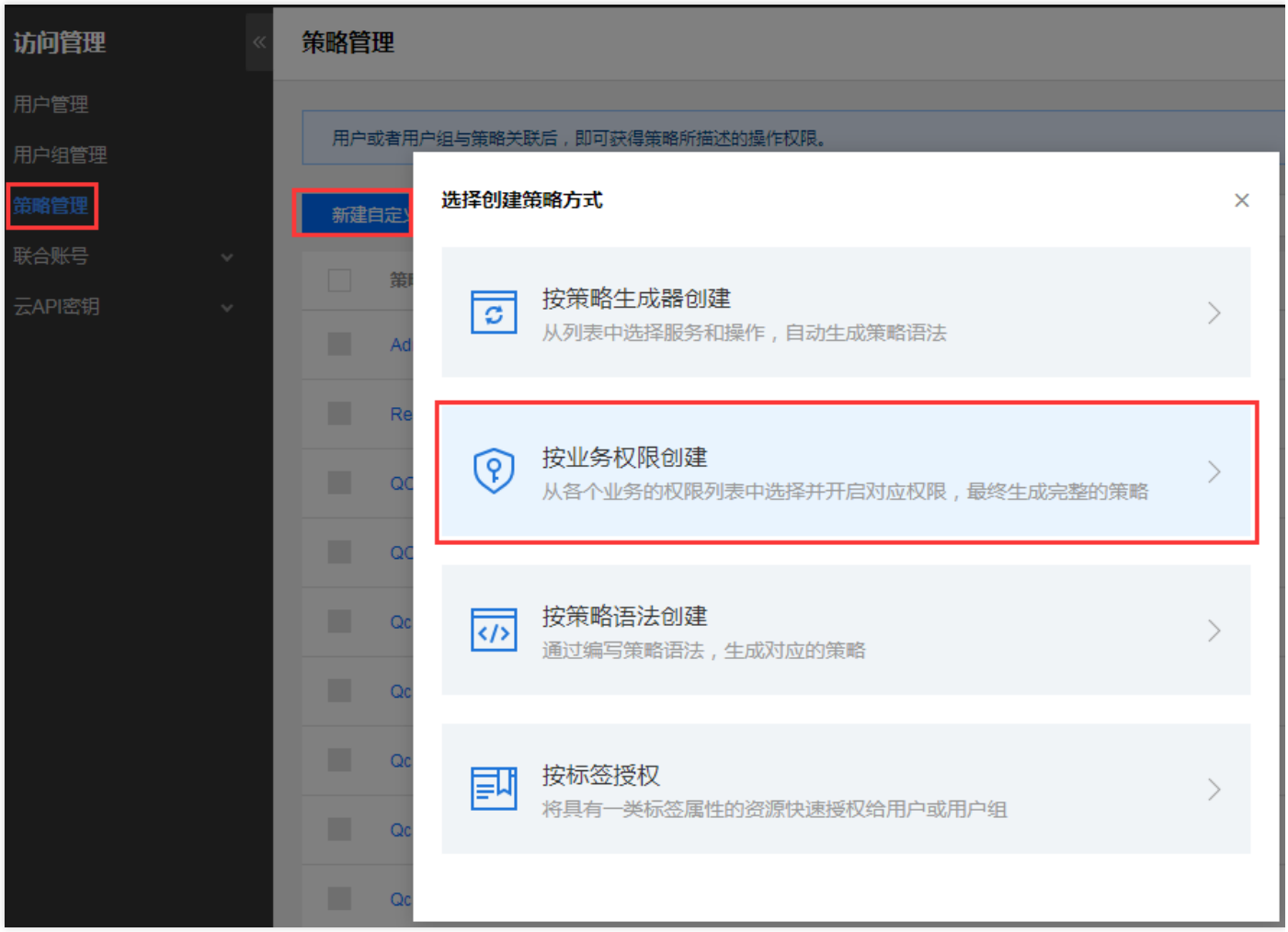
授权子账号管理项目的权限

最近更新时间：2018-06-14 15:04:03

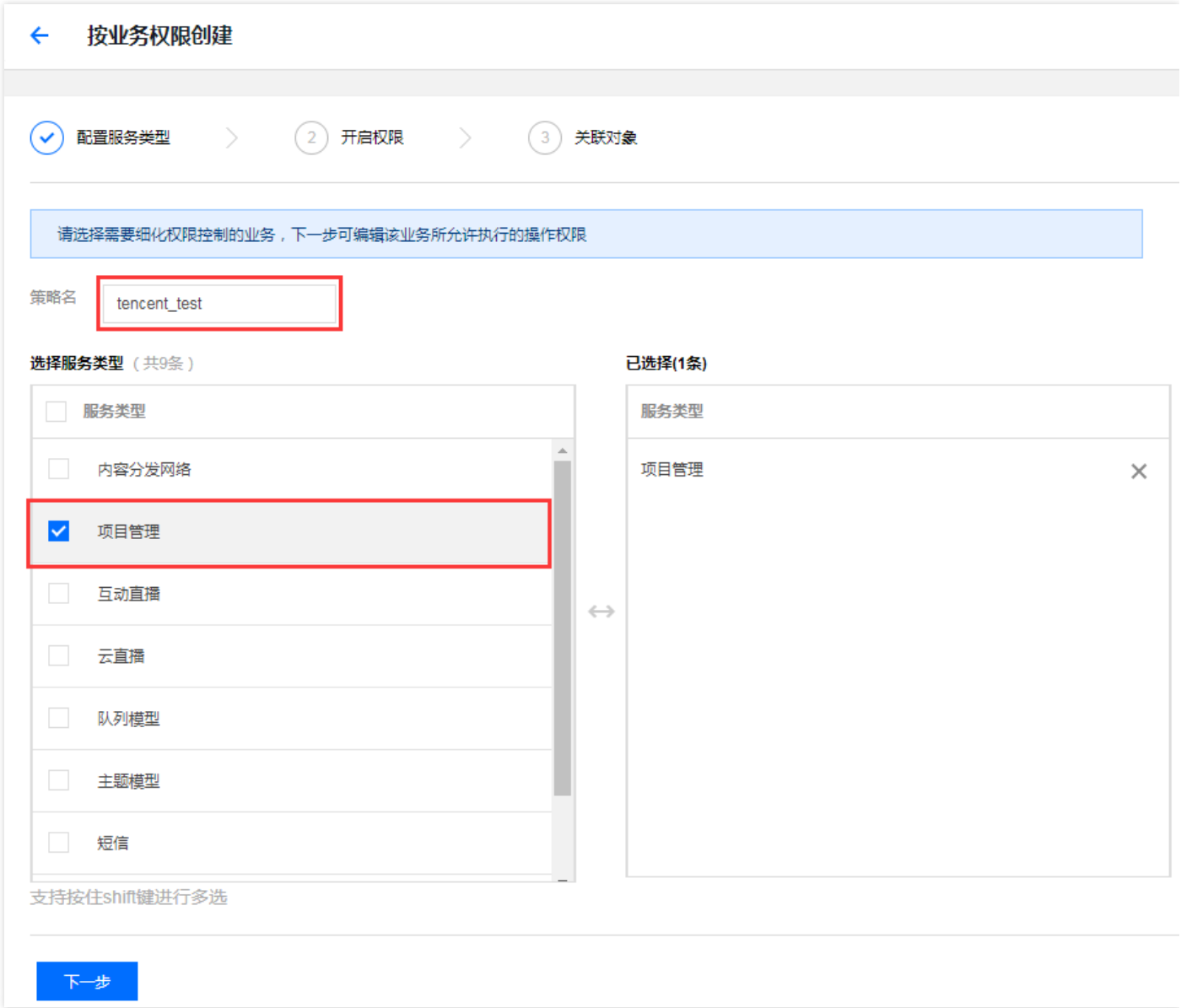
企业帐号 CompanyExample 下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 名下的指定项目有完全访问权限。

1. 登录 腾讯云控制台，将鼠标移动到账号昵称处，此时会弹出下拉列表，单击选项中的【访问管理】进入访问管理控制台。

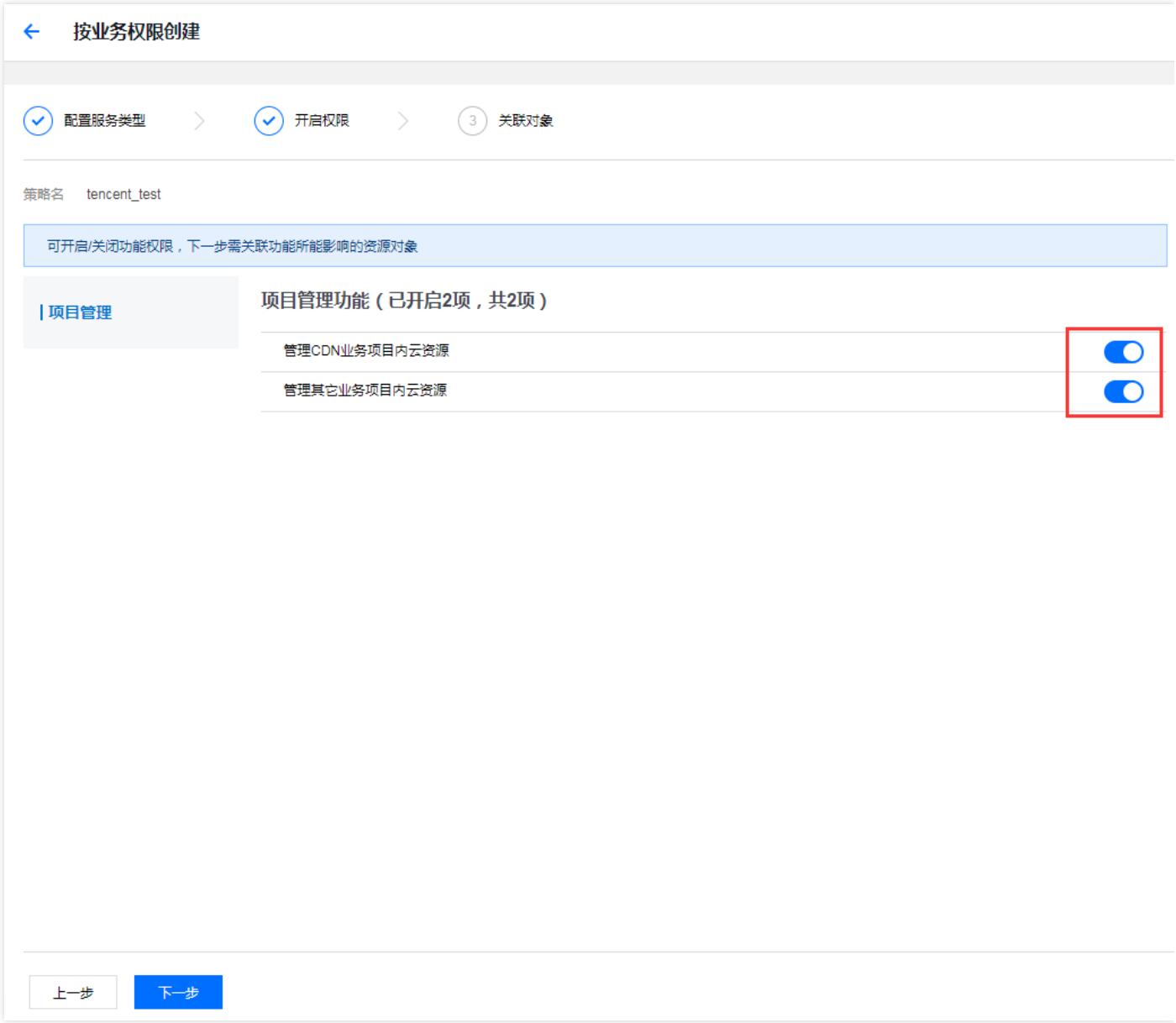
2. 单击左侧导航栏的【策略管理】>【新建自定义策略】>【按业务权限创建】，进入创建页面。



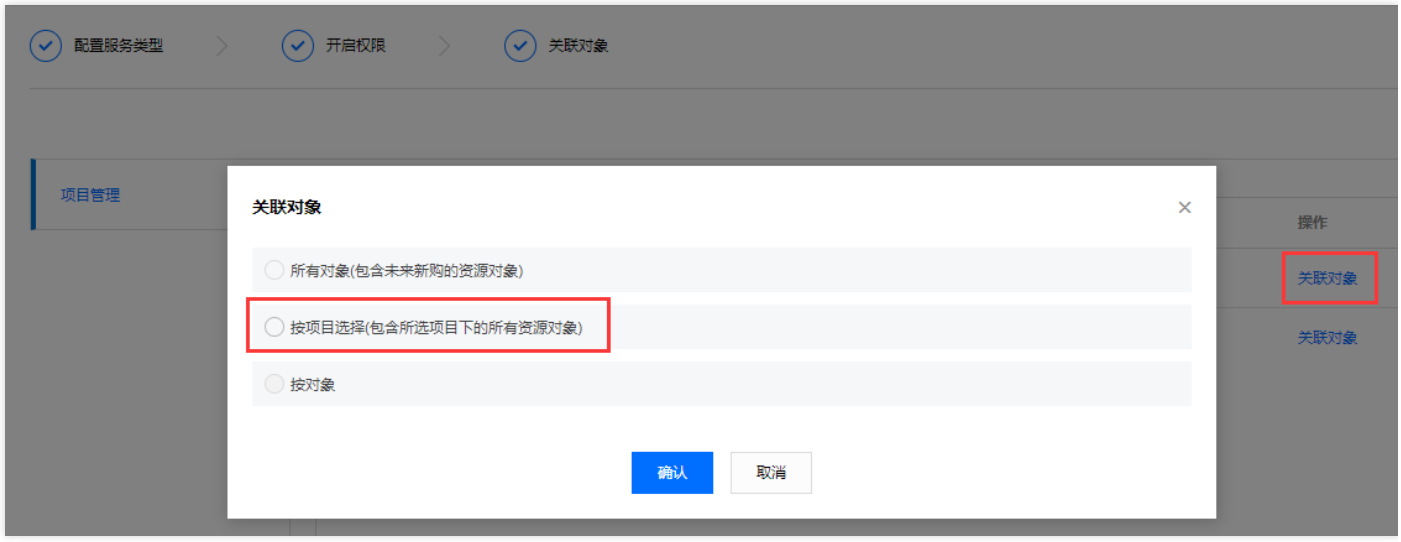
3. 在服务类型中勾选"项目管理"至策略中并命名，单击【下一步】。

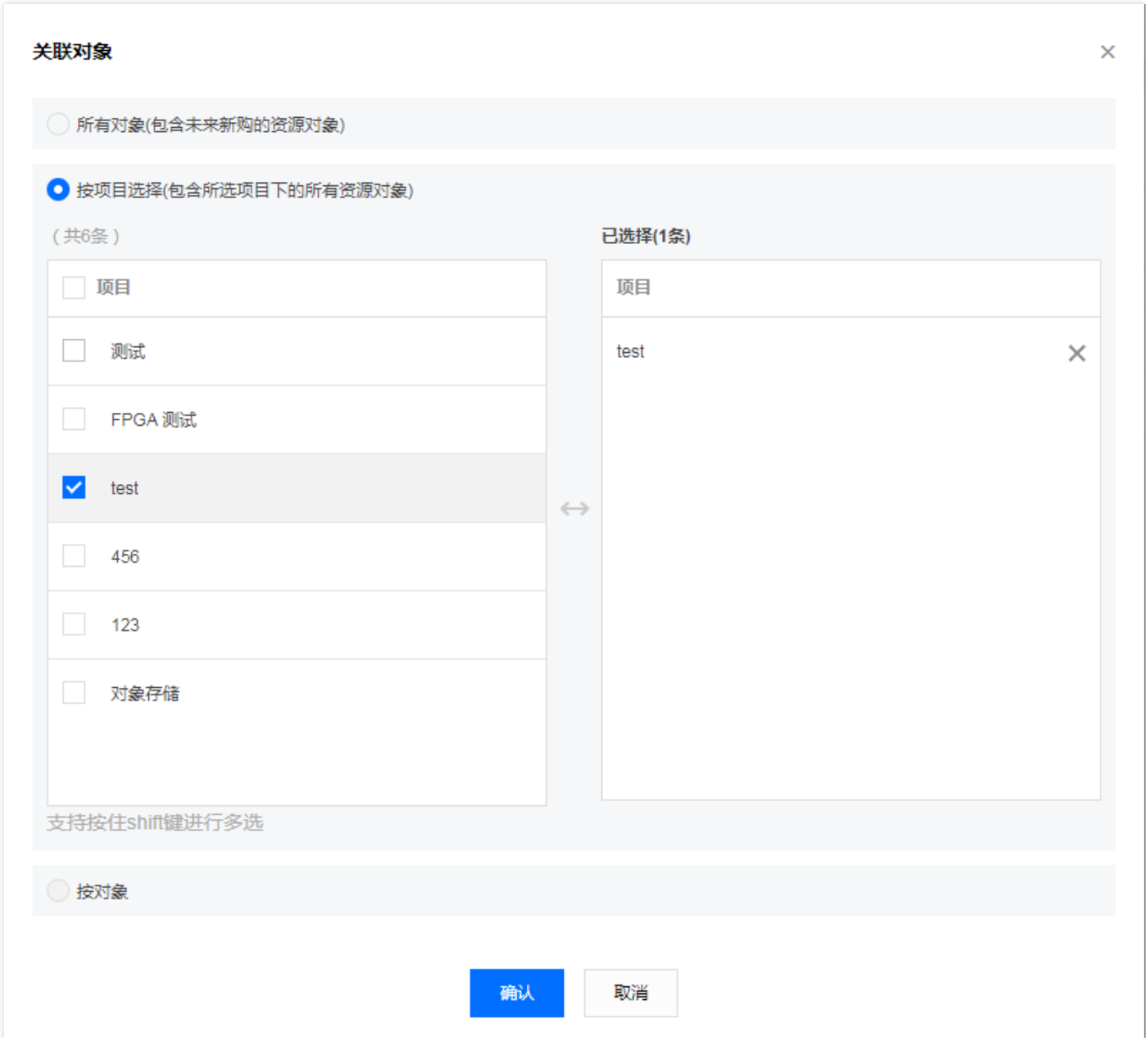


4. 如果要管理 CDN 业务相关项目云资源，将 CDN 的权限开关置为【开】；如果要管理其他业务相关项目云资源，将其他的权限开关置为【开】，并单击【下一步】。



5. 单击【关联对象】>【按项目选择】，选择要关联的项目，单击【确认】>【完成】。


配置服务类型
开启权限
关联对象
项目管理
关联对象
所有对象(包含未来新购的资源对象)
按项目选择(包含所选项目下的所有资源对象)
按对象
确认
取消
操作
关联对象
关联对象


关联对象
所有对象(包含未来新购的资源对象)
按项目选择(包含所选项目下的所有资源对象)
（共6条）
项目
测试
FPGA 测试
test
456
123
对象存储
已选择(1条)
项目
test
支持按住shift键进行多选
按对象
确认
取消

注：目前无法针对项目实施精细化的权限管理。如果要对项目内资源进行差异化的权限管理，建议通过策略语法方式对资源进行单独授权。同时，后续会使用基于标签的方式进行资源的权限管理。