访问管理

商用案例

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2025 腾讯云版权所有

本文档（含所有文字、数据、图片等内容）完整的著作权归腾讯云计算（北京）有限责任公司单独所有，未经腾讯云事先明确书面许可，任何主体不得以任何形式复制、修改、使用、抄袭、传播本文档全部或部分内容。前述行为构成对腾讯云著作权的侵犯，腾讯云将依法采取措施追究法律责任。

【商标声明】

腾讯云

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。未经腾讯云及有关权利人书面许可，任何主体不得以任何方式对前述商标进行使用、复制、修改、传播、抄录等行为，否则将构成对腾讯云及有关权利人商标权的侵犯，腾讯云将依法采取措施追究法律责任。

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。
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默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

商用案例
MySQL 相关案例
允许查看指定标签下的 MySQL 实例
授权子账号拥有特定地域的cdb操作权限
CLB 相关案例
授权子账号拥有 CLB 的所有权限（包含支付权限）
授权子账号拥有 CLB 的所有权限但不包括支付权限
CMQ 相关案例
授权子账号拥有消息服务的所有权限
授权子账号拥有其创建的消息队列的所有权限
授权子账号拥有特定的主题模型的消息队列的读权限
COS 相关案例
授权子账号对特定目录的所有权限
授权子账号对特定目录内文件的读权限
授权子账号对特定文件的读写权限
授权子账号拥有 COS 资源的读权限
授权子账号拥有特定目录下除指定文件之外的其他所有文件的读写权限
授权子账号对指定前缀的文件的读写权限
跨账号访问：授权主账号访问其他主账号的指定文件
跨账号访问：授权子账号访问其他主账号的指定文件
CVM 相关案例
授权子账号拥有 CVM 的所有权限
授权子账号拥有 CVM 的只读权限
授权子账号拥有 CVM 相关资源的只读权限
授权子账号拥有弹性云盘的操作权限
授权子账号拥有安全组的操作权限
授权子账号拥有弹性IP地址的操作权限
授权子账号拥有特定 CVM 的操作权限
授权子账号拥有特定地域的 CVM 的操作权限
授权子账号拥有 CVM 的所有权限但不包括支付权限
授予子账号拥有项目管理的操作权限
VPC 相关案例
授权子账号拥有特定 VPC 的操作权限
授权子账号拥有 VPC 的操作权限但无路由表操作权限
授权子账号拥有 VPN 的操作权限
授权子账号拥有 VPC 的所有权限
授权子账号拥有 VPC 的所有权限但不包括支付权限
云点播相关案例
授权子账号拥有云点播的所有权限
其他案例
授予指定产品的管理权限或只读权限
授权子账号管理项目的权限

商用案例
MySQL 相关案例
允许查看指定标签下的 MySQL 实例

最近更新时间：2024-09-30 16:59:44

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有对企业账号 CompanyExample 名下的两个 MySQL 实例（实例 ID 分别是 cdb-1，标签为：game&webpage 和 cdb-2，标签为：game&app）的查看权限。

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cdb:Describe*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "game&webpage",
                        "game&app"
                    ]
                }
            }
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

> **说明**
> 子账号 Developer 在 MySQL 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。

授权子账号拥有特定地域的cdb操作权限

最近更新时间：2024-09-20 10:10:29

企业账号 CompanyExample（ownerUin 为 12345678）下有一个子账号 cdb，它授予特定地域（gz）下的所有 CDB 实例的全部操作权限（*）给子账号。具体而言，该子账号将可以对这些 CDB 实例执行任何操作。

1. 通过策略语法方式创建策略。

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

- action：表示被允许的操作。`cdb:*` 表示允许所有 CDB 操作。
- effect：表示该声明所描述的许可是允许还是拒绝。`allow` 表示允许。
- resource：表示该声明适用的资源范围。`qcs::cdb:gz::*` 表示授权子账号拥有特定地域（gz）下的所有 CDB 实例的全部操作权限。`*` 表示通配符，表示对所有实例授权。

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

CLB 相关案例
授权子账号拥有 CLB 的所有权限（包含支付权限）

最近更新时间：2024-09-30 16:59:44

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

方案A：

企业账号 CompanyExample 直接将预设策略 QcloudCLBFullAccess、QcloudCLBFinanceAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 15:34:18

企业账号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业账号 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：

企业账号 CompanyExample 直接将预设策略 QcloudCLBFullAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:45

企业账号 CompanyExample 下有一个子账号 Developer，该子账号需要拥有企业账号 CompanyExample 名下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：

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

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:45

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

方案A：

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

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-08-16 21:18:22

企业账号 CompanyExample（ownerUin 为 12345678）有一个基于主题模型的消息队列，同时它有一个子账号 Developer，希望其可以访问该消息队列。

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement": [
     {
        "action": "cmqqueue:SendMessage",
        "resource":"qcs::cmqqueue:::queueName/uin/12345678/test-caten",
        "effect": "allow"
     }
     ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

COS 相关案例
授权子账号对特定目录的所有权限

最近更新时间：2024-09-30 16:59:45

企业账号 CompanyExample（ownerUin 为12345678，appId 为1250000000）下有一个子账号 Developer，该子账号需要拥有企业账号 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：

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement":[
     {
         "effect": "allow",
         "action": "cos:*",
         "resource": ["qcs::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/dir1/*",
                      "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/dir1"]
     }
   ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参见 COS 产品文档 。

授权子账号对特定目录内文件的读权限

最近更新时间：2024-09-30 16:59:45

企业账号 CompanyExample（ownerUin 为12345678，appId 为1250000000）下有一个子账号 Developer，该子账号需要拥有企业账号 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：

1. 通过策略语法方式创建策略。

```
{
   "version": "2.0",
   "statement":[
    {
        "effect": "allow",
        "action":  [
                   "cos:List*",
                   "cos:Get*",
                   "cos:Head*",
                   "cos:OptionsObject"
               ],
        "resource": "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/dir1/*"
    }
  ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参见 COS 产品文档 。

授权子账号对特定文件的读写权限

最近更新时间：2024-09-30 16:59:45

企业账号 CompanyExample（ownerUin 为12345678，appId 为1250000000）下有一个子账号 Developer，该子账号需要拥有企业账号 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：

1. 通过策略语法方式创建策略。

```
 {
    "version": "2.0",
    "statement":[
     {
         "effect": "allow",
         "action": "cos:*",
         "resource": "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-
1250000000/dir1/object1"
     }
   ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参见 COS 产品文档 。

授权子账号拥有 COS 资源的读权限

最近更新时间：2024-09-30 16:59:45

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有对企业账号 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：

企业账号 CompanyExample 直接将预设策略 QcloudCOSReadOnlyAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

```
{
   "version": "2.0",
   "statement":[
    {
        "effect": "allow",
        "action":  [
                   "cos:List*",
                   "cos:Get*",
                   "cos:Head*",
                   "cos:OptionsObject"
               ],
        "resource": "*"
    }
  ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

授权子账号拥有特定目录下除指定文件之外的其他所有文件的读写权限

最近更新时间：2024-09-30 16:59:45

企业账号 CompanyExample（ownerUin 为12345678，appId 为1250000000）下有一个子账号 Developer，该子账号需要拥有企业账号 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：

1. 通过策略语法方式创建策略。

```
 {
    "version": "2.0",
    "statement":
    [
     {
         "effect": "allow",
         "action": "cos:*",
         "resource": "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/dir1/*"
     },
     {
         "effect": "deny",
         "action": "cos:*",
         "resource": "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-
1250000000/dir1/Object1"
     }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

方案 B：

通过 COS 控制台进行 Policy 和 ACL 设置。具体请参见 ACL 访问控制实践 。

授权子账号对指定前缀的文件的读写权限

最近更新时间：2024-09-30 16:59:45

企业账号 CompanyExample（ownerUin 为12345678，appId 为1250000000）下有一个子账号 Developer，该子账号需要拥有企业账号 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：

1. 通过策略语法方式创建策略。

```
{
   "version": "2.0",
   "statement":[
    {
        "effect": "allow",
        "action": "cos:*",
        "resource": "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/dir1/test*"
    }
  ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

方案 B：

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

跨账号访问：授权主账号访问其他主账号的指定文件

最近更新时间：2024-09-30 16:59:45

企业账号 CompanyGranter（ownerUin 为12345678，appId 为1250000000），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。另外一个企业账号 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。详情请参见 ACL 访问控制实践 。

跨账号访问：授权子账号访问其他主账号的指定文件

最近更新时间：2024-09-30 16:59:46

企业账号 CompanyGranter（ownerUin 为12345678，appId 为1250000000），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。另外一个企业账号 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。

1. 企业账号 CompanyGrantee 通过策略语法方式创建策略。

```
 {
    "version": "2.0",
    "statement":[
     {
         "effect": "allow",
         "action": "cos:*",
         "resource": "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-
1250000000/dir1/Object1"
     }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。
3. 企业账号 CompanyGranter 通过 COS 控制台进行 Policy 和 ACL 设置，将对象 Object1 授权给企业账号 CompanyGrantee，具体请参见 COS 产品文档 。

CVM 相关案例
授权子账号拥有 CVM 的所有权限

最近更新时间：2024-08-16 21:18:22

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有对企业账号 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：

企业账号 CompanyExample 直接将预设策略 QcloudCVMFullAccess、QcloudCVMFinanceAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

授权子账号拥有 CVM 的只读权限

最近更新时间：2024-09-30 16:59:46

企业账号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 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：

企业账号 CompanyExample 直接将预设策略 QcloudCVMInnerReadOnlyAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:46

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有对企业账号 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：

企业账号 CompanyExample 直接将预设策略 QcloudCVMReadOnlyAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略，

```
{
    "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": "*"
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:46

企业账号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 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：

企业账号 CompanyExample 直接将预设策略 QcloudCBSFullAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:CreateCbsStorages",
                "cvm:AttachCbsStorages",
                "cvm:DetachCbsStorages",
                "cvm:ModifyCbsStorageAttributes",
                "cvm:DescribeCbsStorages",
                "cvm:DescribeInstancesCbsNum",
                "cvm:RenewCbsStorage",
                "cvm:ResizeCbsStorage"
                ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

> **说明**
> 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：2024-09-30 16:59:46

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 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。

1. 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"
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 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。

1. 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"
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:46

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 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。

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:AllocateAddresses",
                "cvm:AssociateAddress",
                "cvm:DescribeAddresses",
                "cvm:DisassociateAddress",
                "cvm:ModifyAddressAttribute",
                "cvm:ReleaseAddresses"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 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。

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "cvm:DescribeAddresses",
                "cvm:AllocateAddresses",
                "cvm:AssociateAddress"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 11:27:41

企业账号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 CompanyExample 的指定 CVM 机器的操作权限，我们将这些 CVM 机器统一使用标签 game&webpage 标记。

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cvm:*",
                "vpc:DescribeNetworkInterfaces"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
                    "qcs:resource_tag": [
                        "game&webpage"
                    ]
                }
            }
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:46

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

方案 A:

企业账号 CompanyExample 直接将预设策略 QcloudCVMReadOnlyAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案 B:

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:47

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

方案A：

企业账号 CompanyExample 直接将预设策略 QcloudCVMFullAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:47

企业账号 CompanyExample（主账号 ID 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。

1. 按业务权限创建项目管理自定义策略，详情请参见 创建项目策略 。
2. 给子账号关联创建好的自定义策略，详情请参见 授予项目策略 。

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。授权方式请参见 授权管理 。

VPC 相关案例
授权子账号拥有特定 VPC 的操作权限

最近更新时间：2024-09-30 16:59:47

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 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，不包括云服务器、数据库等）的操作权限。

1. 通过策略语法方式创建策略。

```
{
    "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"
                    ]
                }
            }
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:47

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 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。

1. 通过策略语法方式创建策略。

```
{
    "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"
        }
    ]
}
```

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

授权子账号拥有 VPN 的操作权限

最近更新时间：2024-09-30 16:59:47

企业账号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 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。

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 授权管理 。

授权子账号拥有 VPC 的所有权限

最近更新时间：2024-09-30 16:59:47

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

方案A：

企业账号 CompanyExample 直接将预设策略 QcloudVPCFullAccess、QcloudVPCFinanceAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:47

企业账号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有企业账号 CompanyExample 的 VPC 服务的所有管理权限（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：

企业账号 CompanyExample 直接将预设策略 QcloudVPCFullAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

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

2. 将该策略授权给子账号。授权方式请参见 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：2024-09-30 16:59:47

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

方案A：

企业账号 CompanyExample 直接将预设策略 QcloudVODFullAccess 授权给子账号 Developer。授权方式请参见 授权管理 。

方案B：

1. 通过策略语法方式创建策略。

```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "vod:*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "action": "cos:*",
            "resource": "qcs::cos::uid/10022853:*",
            "effect": "allow"
        }
    ]
}
```

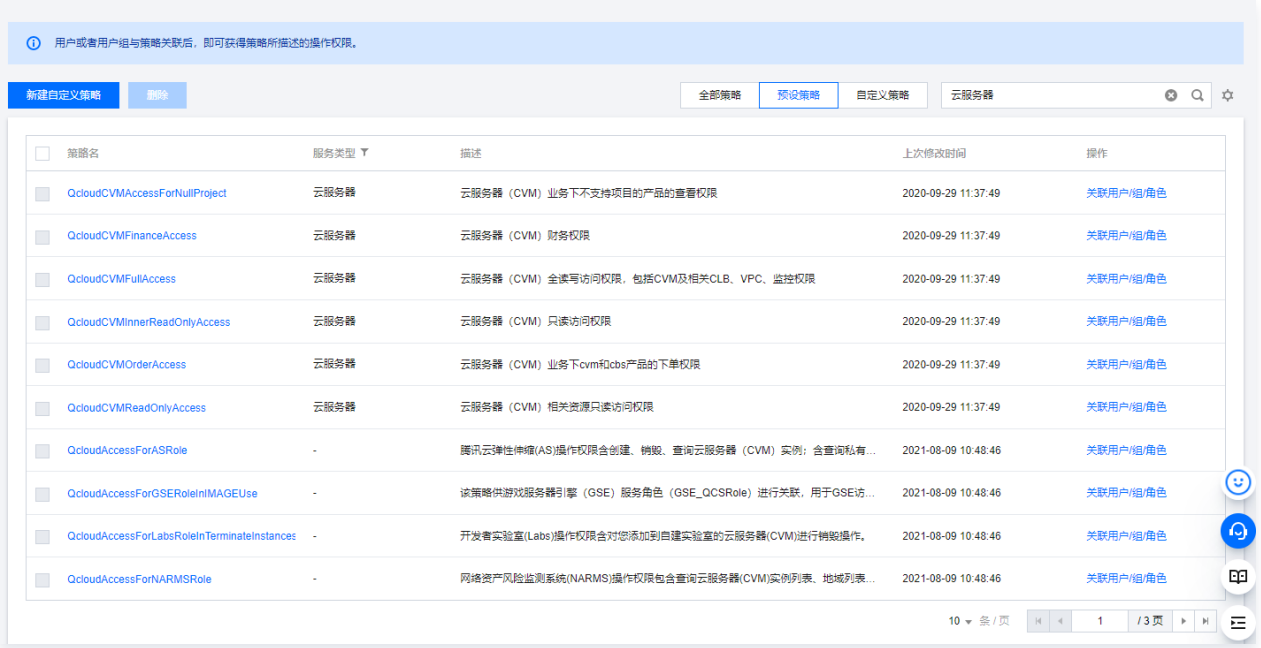
2. 将该策略授权给子账号。授权方式请参见 授权管理 。

其他案例
授予指定产品的管理权限或只读权限

最近更新时间：2024-08-16 21:18:22

为简化客户权限的配置操作，腾讯云的产品在接入访问管理时，会提供默认的授权策略，客户可以直接使用这些策略来关联 CAM 子账号或用户组，实现控制对应产品服务访问权限的目的。这类策略属于 CAM 预设策略，每类产品服务通常至少提供管理策略和只读策略。

1. 进入**访问管理** > **策略** 控制台，在搜索框中输入产品名称（如云服务器），即可查看对应产品的预设策略列表。



其中，QcloudCVMFullAccess为管理策略，QcloudCVMInnerReadOnlyAccess为只读策略。

> **注意**
> 部分产品的管理策略是不包含支付权限的，您可以同步为需要授权的 CAM 子用户/用户组管理支付所需的默认策略，如 CVM 的 QcloudCVMFullAccess。

2. 将上述策略授权给 CAM 子账号/用户组。授权方式请参见 授权管理 。
   - 如果您需要为子用户授予腾讯云账号的全部管理权限，您可以使用预设策略 AdministratorAccess。
     AdministratorAccess ：该策略允许您管理账户内所有用户及其权限、财务相关的信息、云服务资源。
   - 如果您需要为子用户授予腾讯云账号的只读权限，您可以使用预设策略 ReadOnlyAccess。
     ReadOnlyAccess：该策略允许您只读访问账户内所有支持接口级鉴权或资源级鉴权的云服务资源。

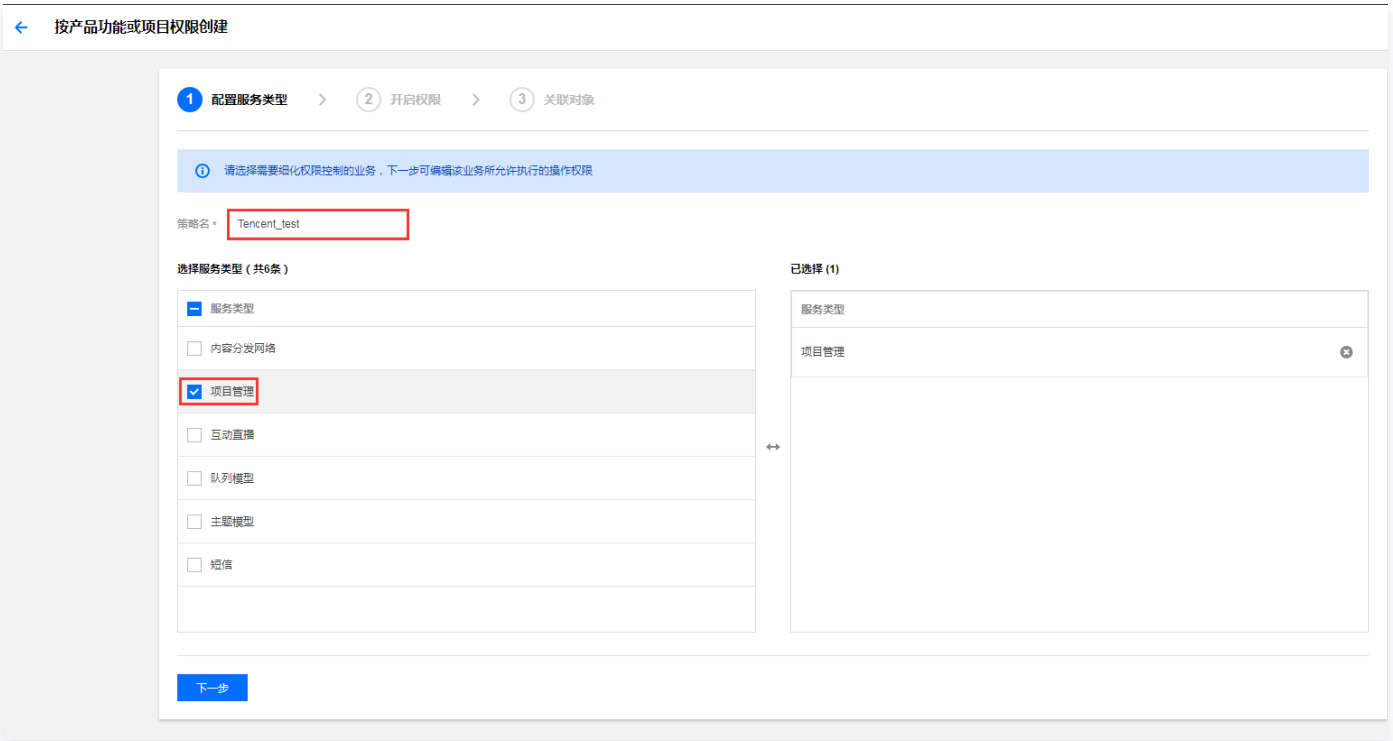
授权子账号管理项目的权限

最近更新时间：2024-09-30 16:59:48

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

1. 进入 访问管理 控制台，在左侧导航栏中，单击 策略，进入策略管理页面。
2. 在策略管理页面，单击**新建自定义策略**。
3. 在弹出的**选择创建策略方式**窗口中，选择 按产品功能或项目权限创建 。如下图所示：

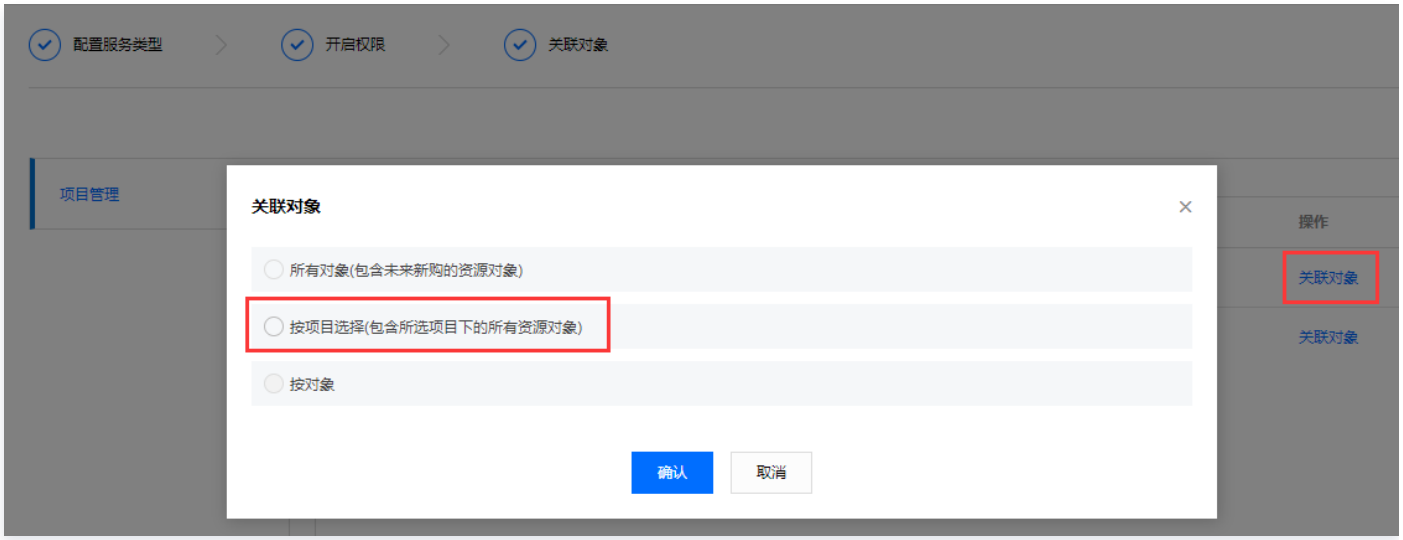
4. 在**按产品功能或项目权限创建**页面，输入策略名，并在**选择服务类型**中勾选 **项目管理**，单击**下一步**。



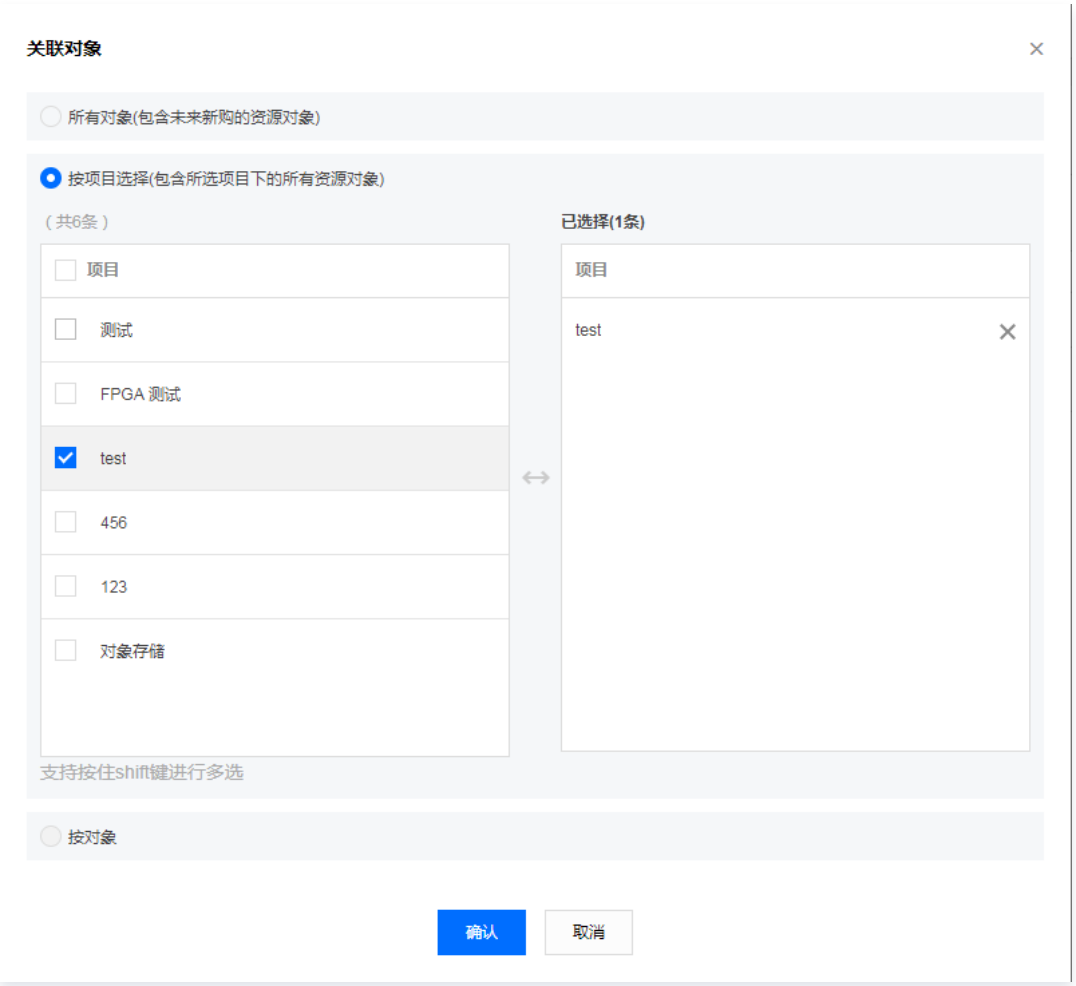
5. 根据实际需求，配置项目管理功能。如下图所示：

- 如果要管理 CDN 业务相关项目云资源，将 CDN 的权限开关置为**开启**。
- 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**开启**。

6. 单击**下一步**。
7. 单击**关联对象**，选择**按项目选择**。如下图所示：



8. 选择要关联的项目，单击**确认**。如下图所示：



9. 单击**完成**。

> **说明**
> 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。