访问管理

商用案例

产品文档

腾讯云

文档目录

商用案例

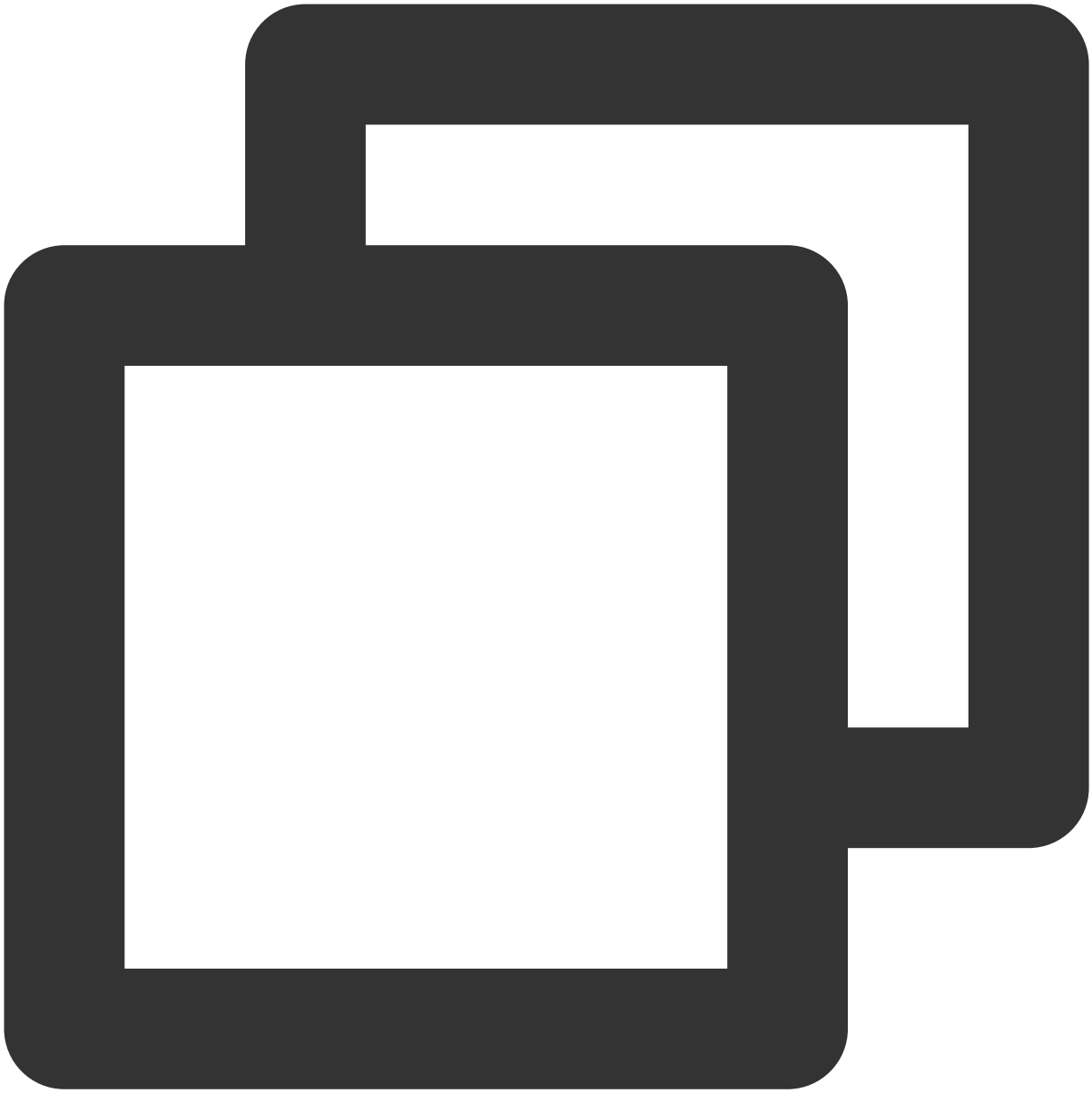
MySQL 相关案例

允许查看指定标签下的 MySQL 实例

最近更新时间：2024-01-23 18:02:53

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。

步骤1：通过策略语法方式创建以下策略。



```
{
    "version": "2.0",
    "statement": [
        {
            "effect": "allow",
            "action": [
                "cdb:Describe*"
            ],
            "resource": "*",
            "condition": {
                "for_any_value:string_equal": {
```

```
                    "qcs:resource_tag": [
                        "game&webpage",
                        "game&app"
                    ]
                }
            }
        }
    ]
}
```

步骤2：将该策略授权给子账号。授权方式请参考 授权管理。

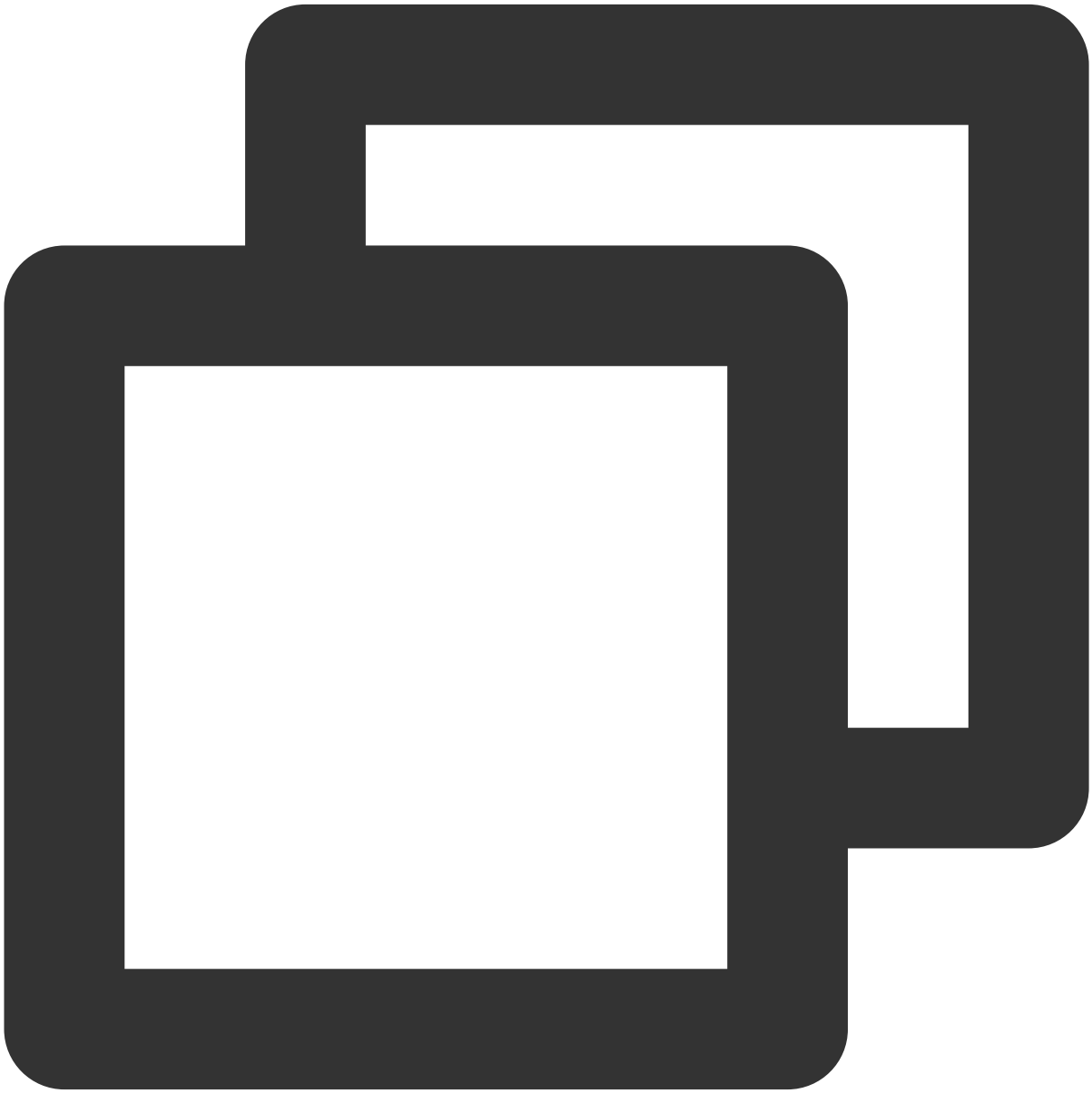
说明：

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。

授权子账号拥有指定 MySQL 实例的查看权限

最近更新时间：2024-01-23 18:02:53

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帐号 CompanyExample 名下的两个 MySQL 实例（实例 ID 分别是 cdb-1 和 cdb-2）的查看权限。
步骤1：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/123
     }
   ]
}
```

步骤2：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 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。

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：2024-01-23 18:02:52

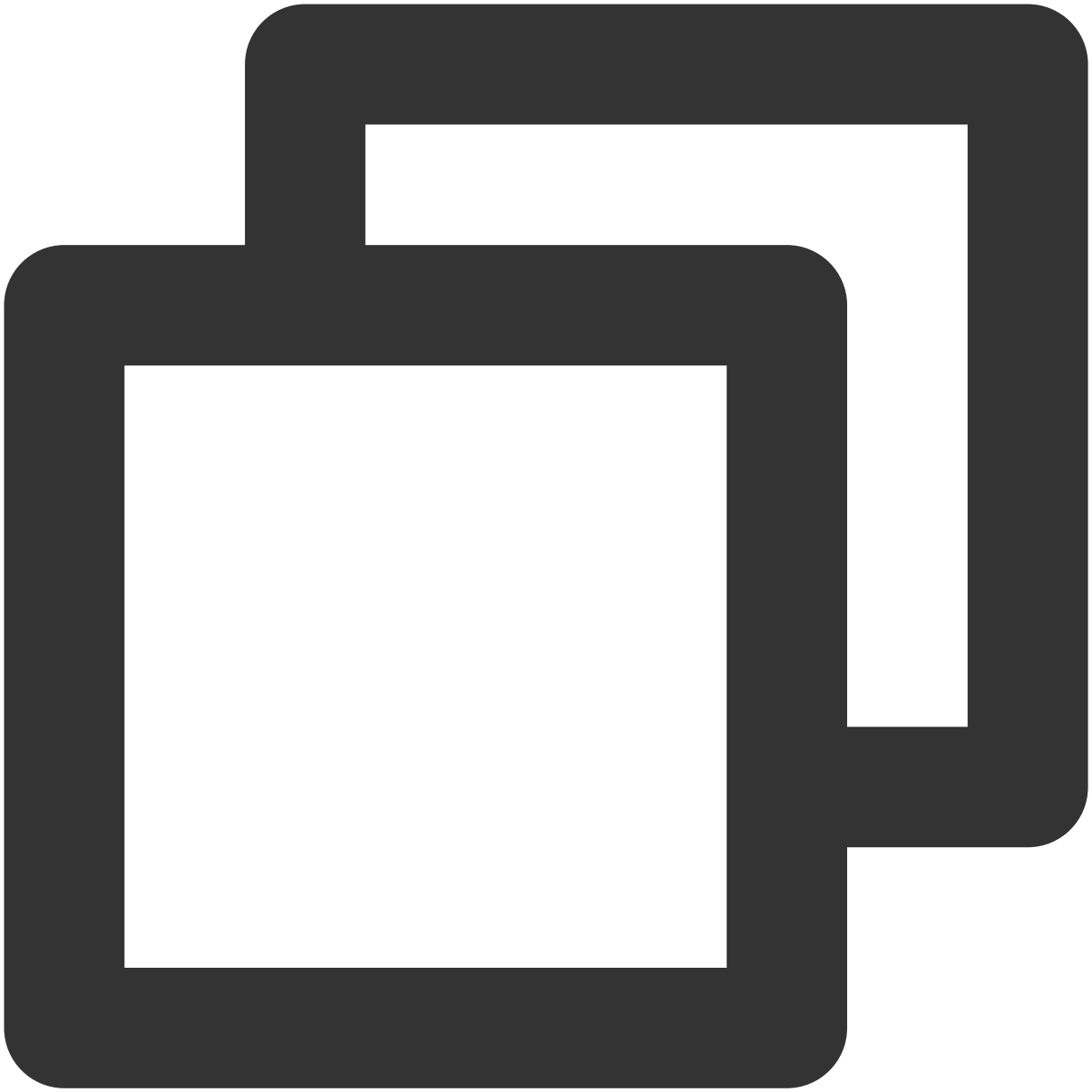
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CLB 服务的完全管理权限（创建、管理、CLB 下单支付等全部操作）。

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：

步骤1：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:::*"
            }
        ]
    }
```

步骤2：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：2024-01-23 18:02:53

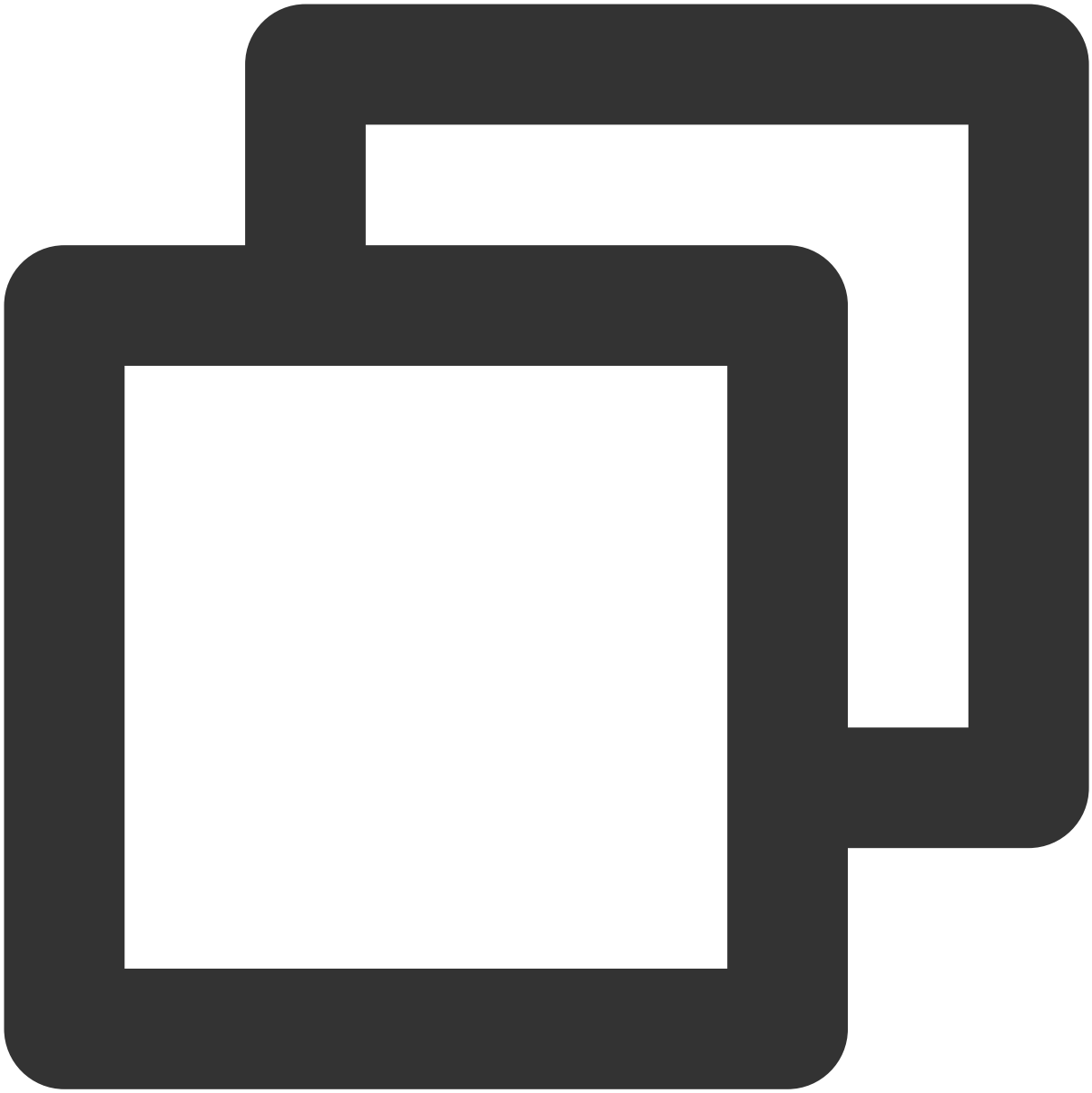
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CLB 服务的所有权限管理权限（创建、管理等全部操作），但不包括支付权限，可以下单但无法支付。

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：

步骤1：通过策略语法方式创建以下策略。



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

步骤2：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：2024-01-23 18:02:52

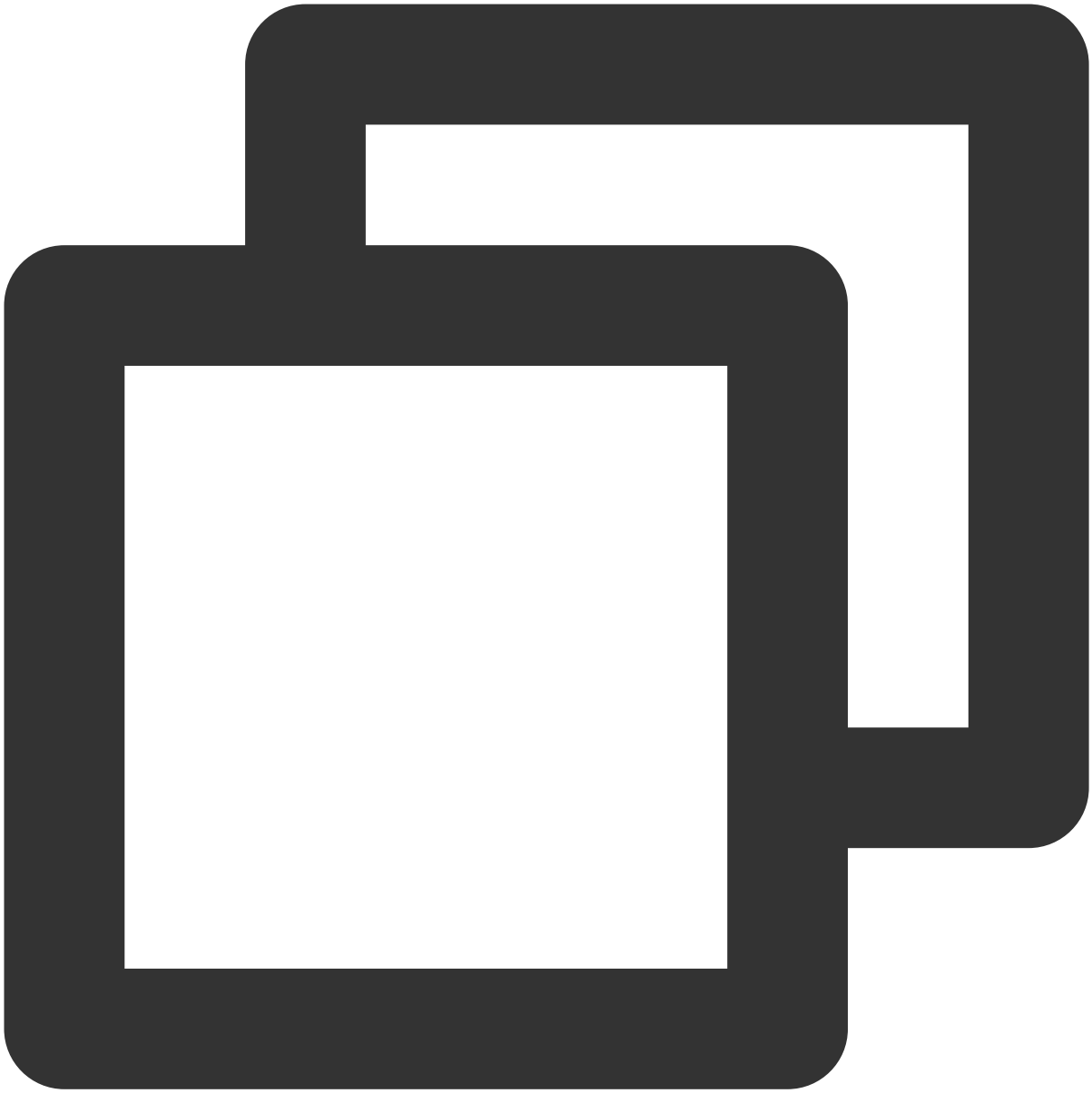
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CLB 服务的查看权限，但子账号无法创建、更新或删除它们。

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：

步骤1：通过策略语法方式创建以下策略。



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

步骤2：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：2024-01-23 18:02:53

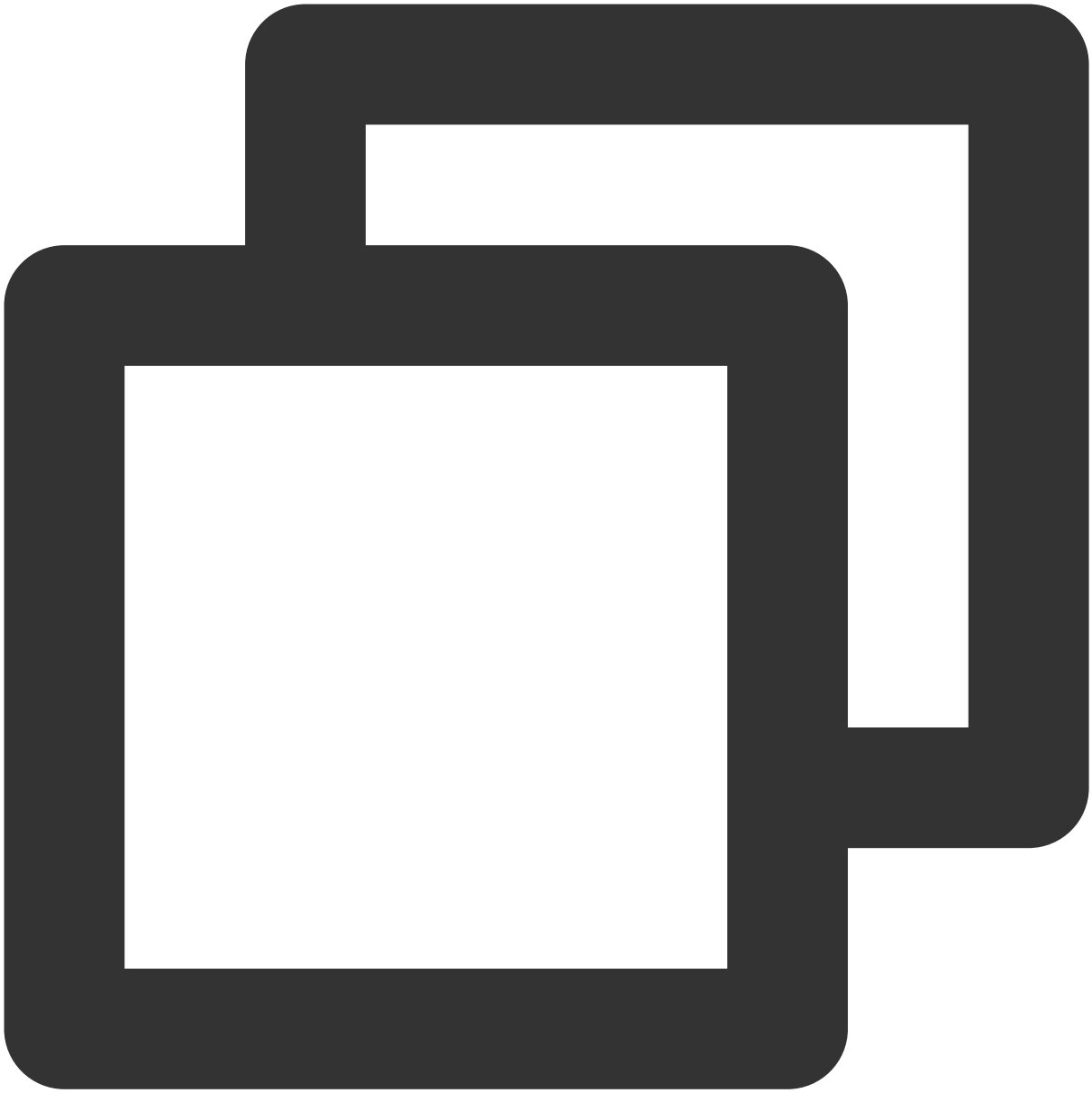
企业帐号 CompanyExample 下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 名下的消息队列的所有权限，无论消息队列是主题模型还是队列模型，都可以被读写。

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：

步骤1：通过策略语法方式创建以下策略。



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

步骤2：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：2024-01-23 18:02:52

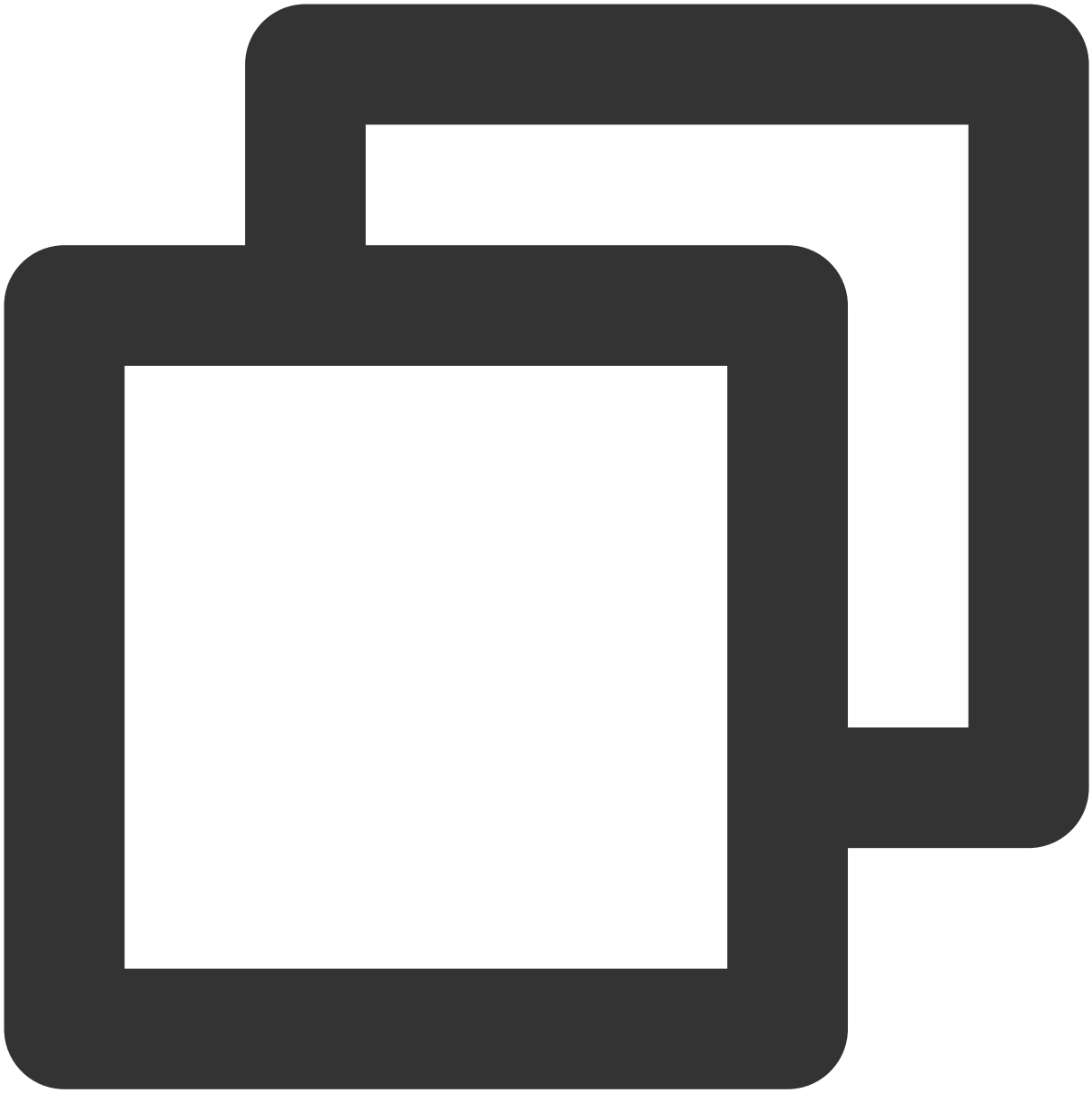
企业帐号 CompanyExample 下有一个子账号 Developer，该子账号希望其可以访问自己创建的消息队列。

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：

步骤1：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",
```

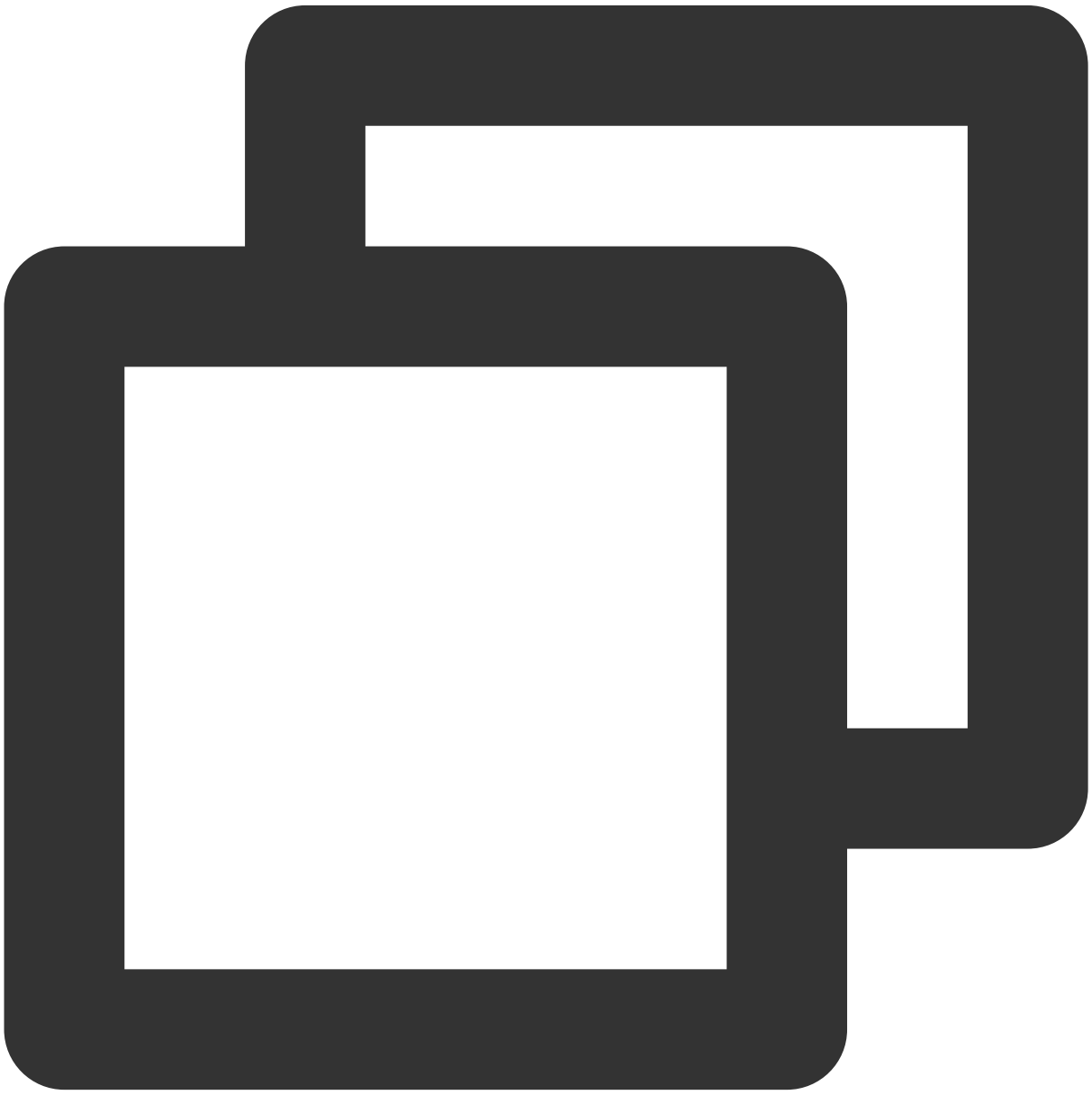
```
            "action": "cmqqueue:*",
            "resource": "qcs::cmqqueue:::queueName/uin/${uin}/*"
        }
    ]
}
```

步骤2：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：2024-01-23 18:02:53

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。
步骤1：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"
     }
     ]
}
```

步骤2：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：2024-01-23 18:02:53

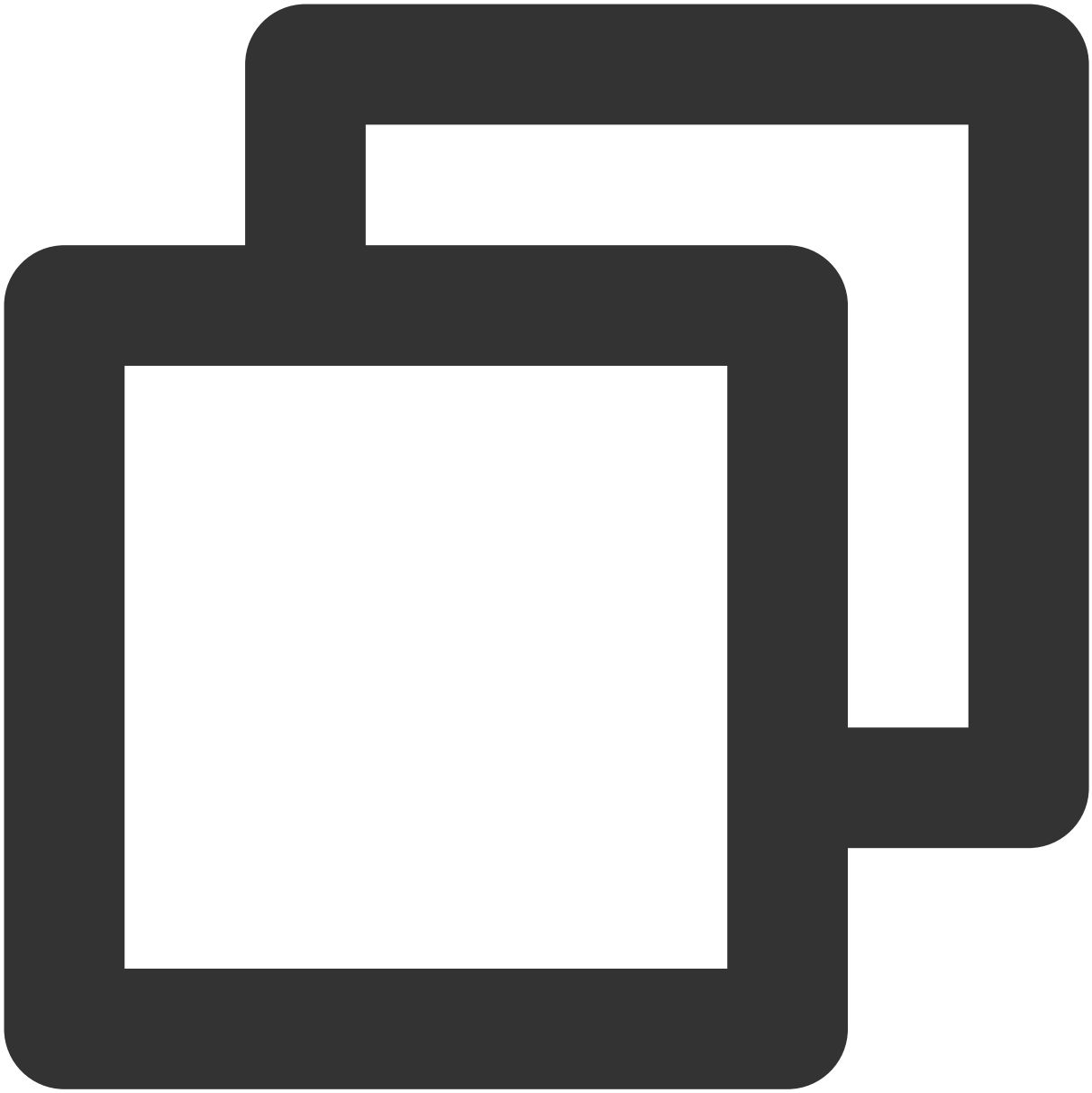
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的完全管理权限（创建、管理、访问 COS 的存储桶或者对象）。

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：

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": "*"
     }
   ]
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

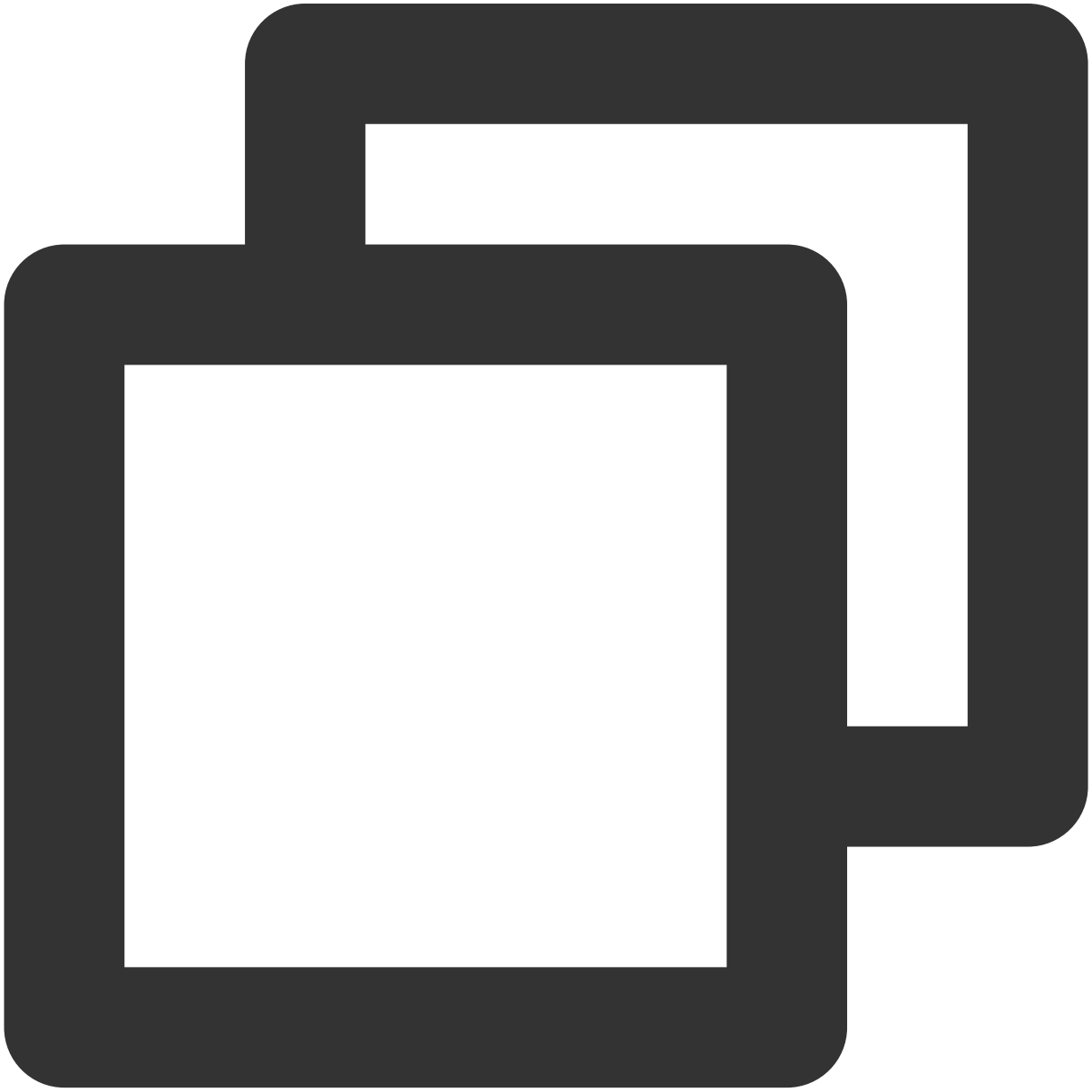
授权子账号对特定目录的所有权限

最近更新时间：2024-01-23 18:02:52

企业帐号 CompanyExample（ownerUin 为12345678，appId 为1250000000）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/1250000000:Bucket1-1250000000/dir1/
                     "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/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。

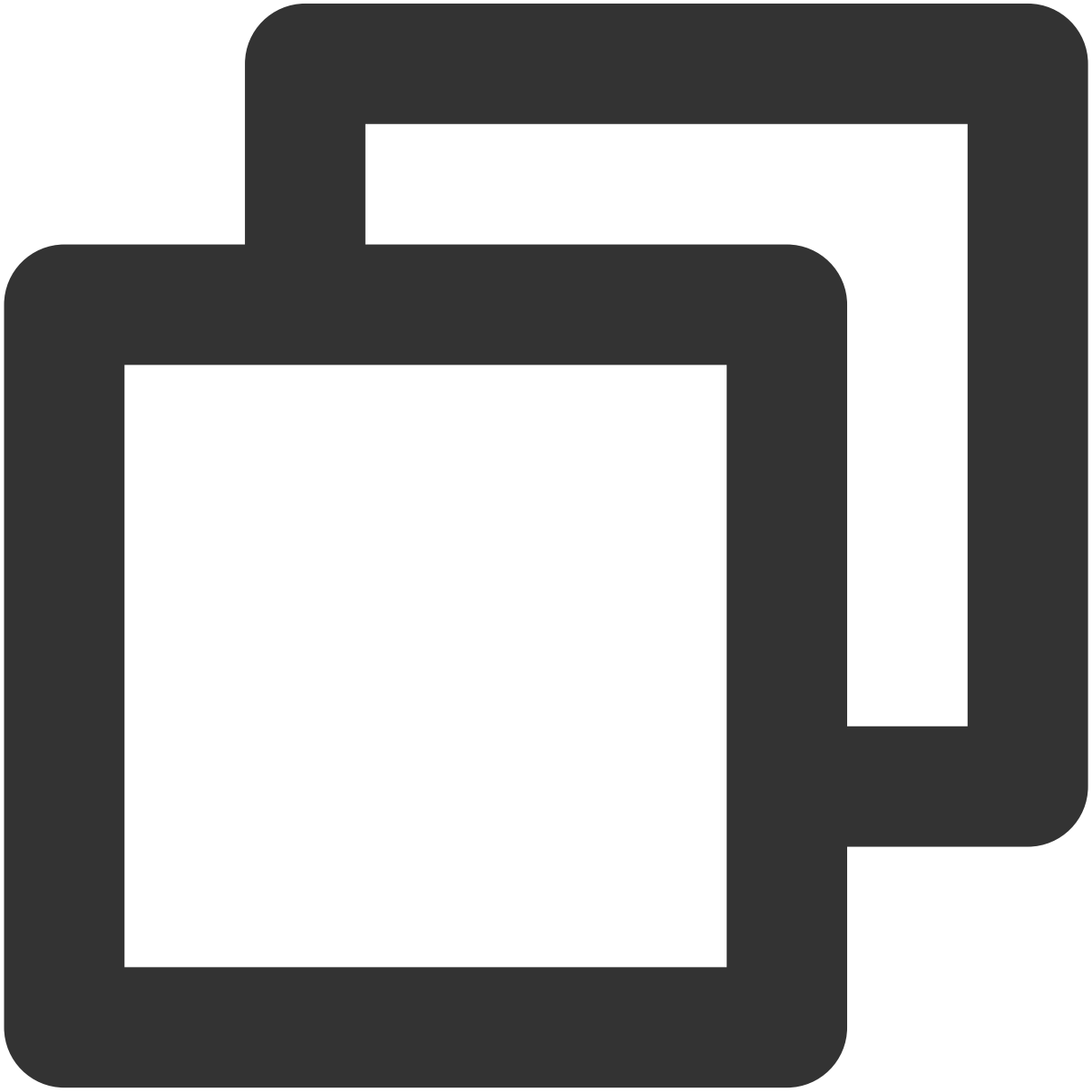
授权子账号对特定目录内文件的读权限

最近更新时间：2024-01-23 18:02:53

企业帐号 CompanyExample（ownerUin 为12345678，appId 为1250000000）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/1250000000:Bucket1-1250000000/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。

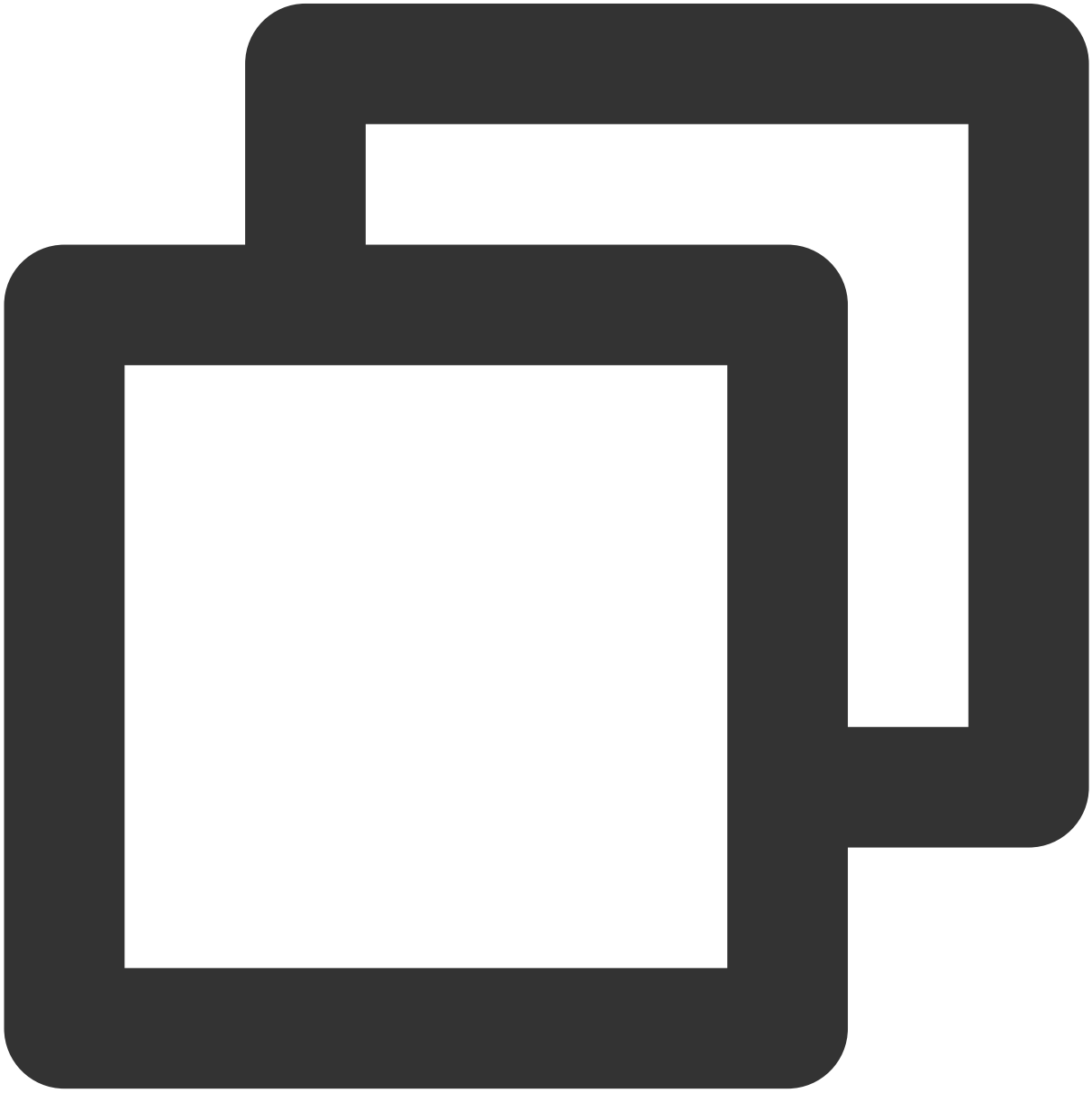
授权子账号对特定文件的读写权限

最近更新时间：2024-01-23 18:02:53

企业帐号 CompanyExample（ownerUin 为12345678，appId 为1250000000）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/1250000000:Bucket1-1250000000/dir1/o
     }
   ]
}
```

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：2024-01-23 18:02:53

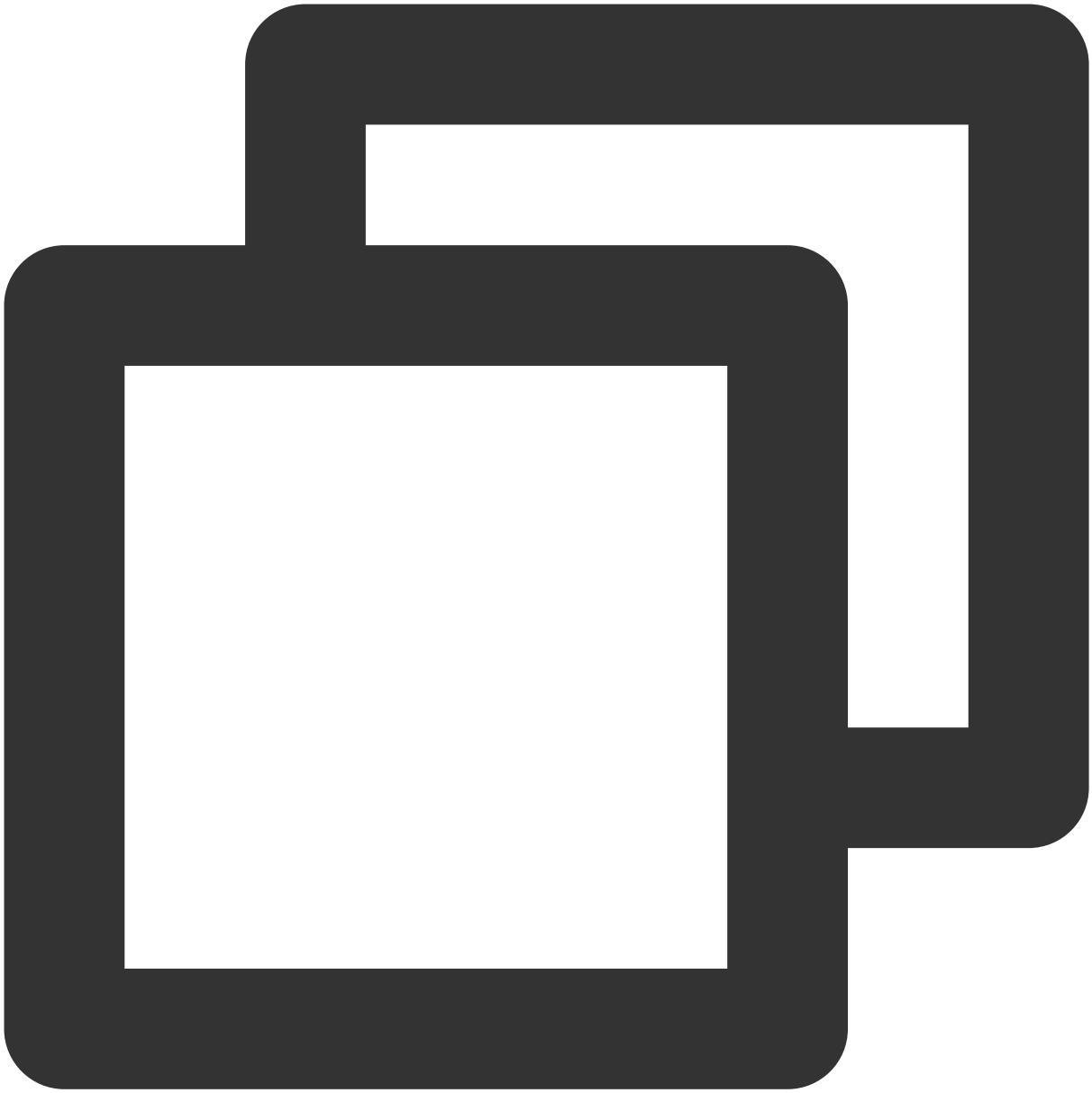
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 COS 服务的只读访问权限（访问 COS 的存储桶或者对象及对象列表等）。

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：

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": "*"
        }
    ]
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

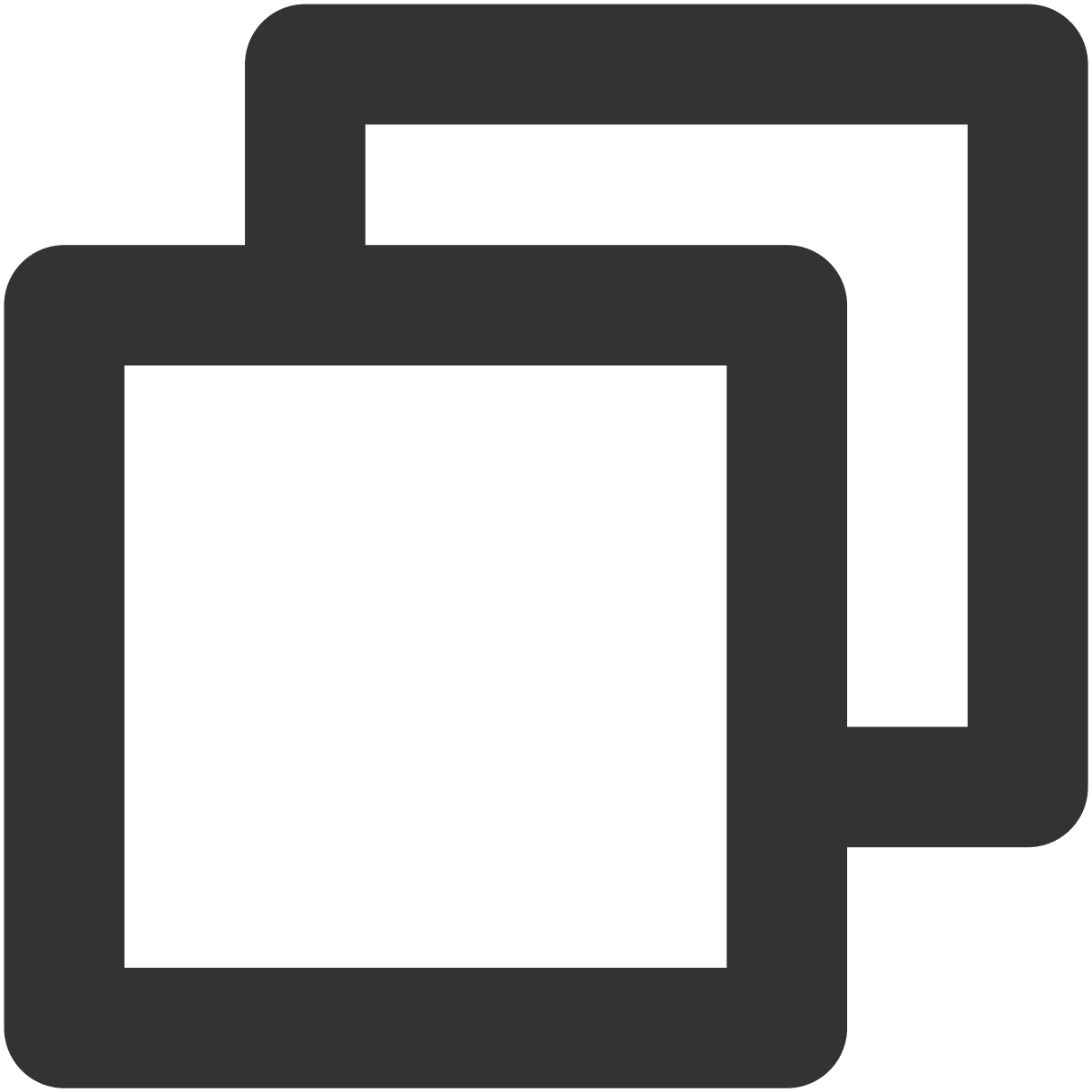
授权子账号对特定目录下所有文件的读写权限并禁止对该目录下指定文件的读写权限

最近更新时间：2024-01-23 18:02:53

企业帐号 CompanyExample（ownerUin 为12345678，appId 为1250000000）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/1250000000:Bucket1-1250000000/dir1/*
     },
     {
          "effect": "deny",
```

```
            "action": "cos:*",
            "resource": "qcs::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/dir1/O
        }
      ]
  }
```

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 ACL 访问控制实践。

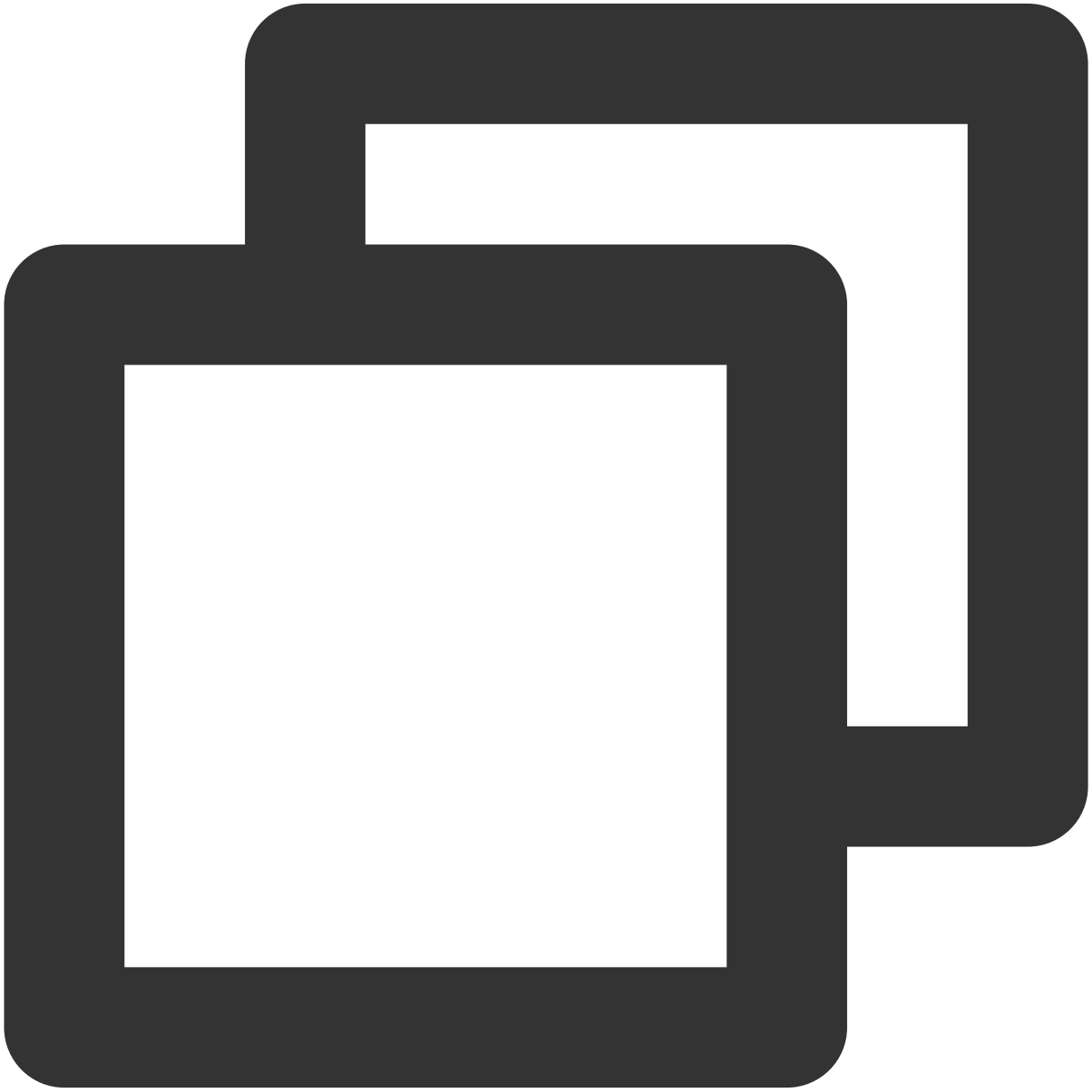
授权子账号对指定前缀的文件的读写权限

最近更新时间：2024-01-23 18:02:53

企业帐号 CompanyExample（ownerUin 为12345678，appId 为1250000000）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/1250000000:Bucket1-1250000000/dir1/t
     }
   ]
}
```

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：2024-01-23 18:02:53

企业帐号 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 ACL 访问控制实践。

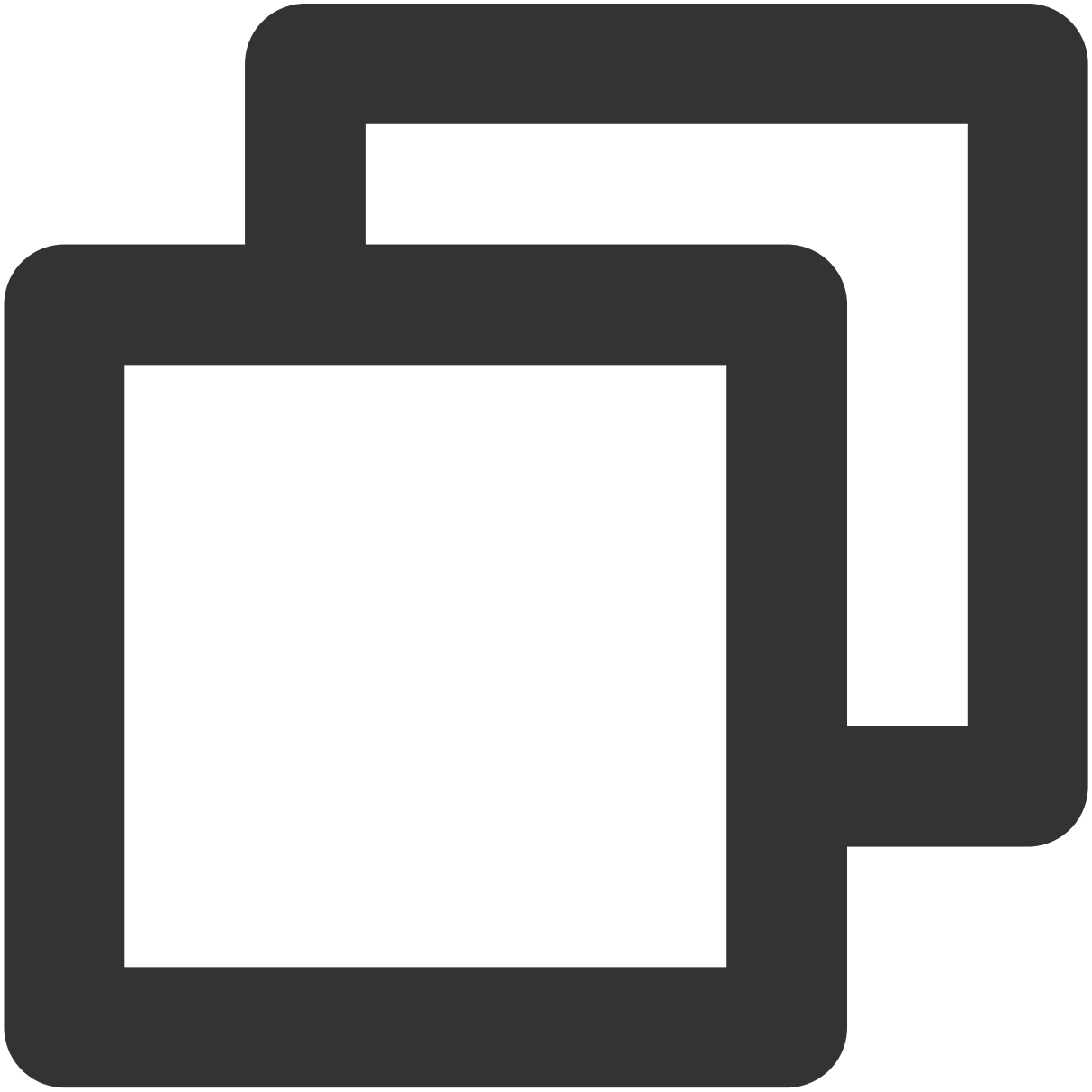
授权跨账号的子账号对指定文件的读写权限

最近更新时间：2024-01-23 18:02:53

企业帐号 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。

步骤 1：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::cos:ap-shanghai:uid/1250000000:Bucket1-1250000000/dir1/O
     }
    ]
}
```

步骤 2：将该策略授权给子账号。授权方式请参考 授权管理。

步骤 3：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：2024-01-23 18:02:53

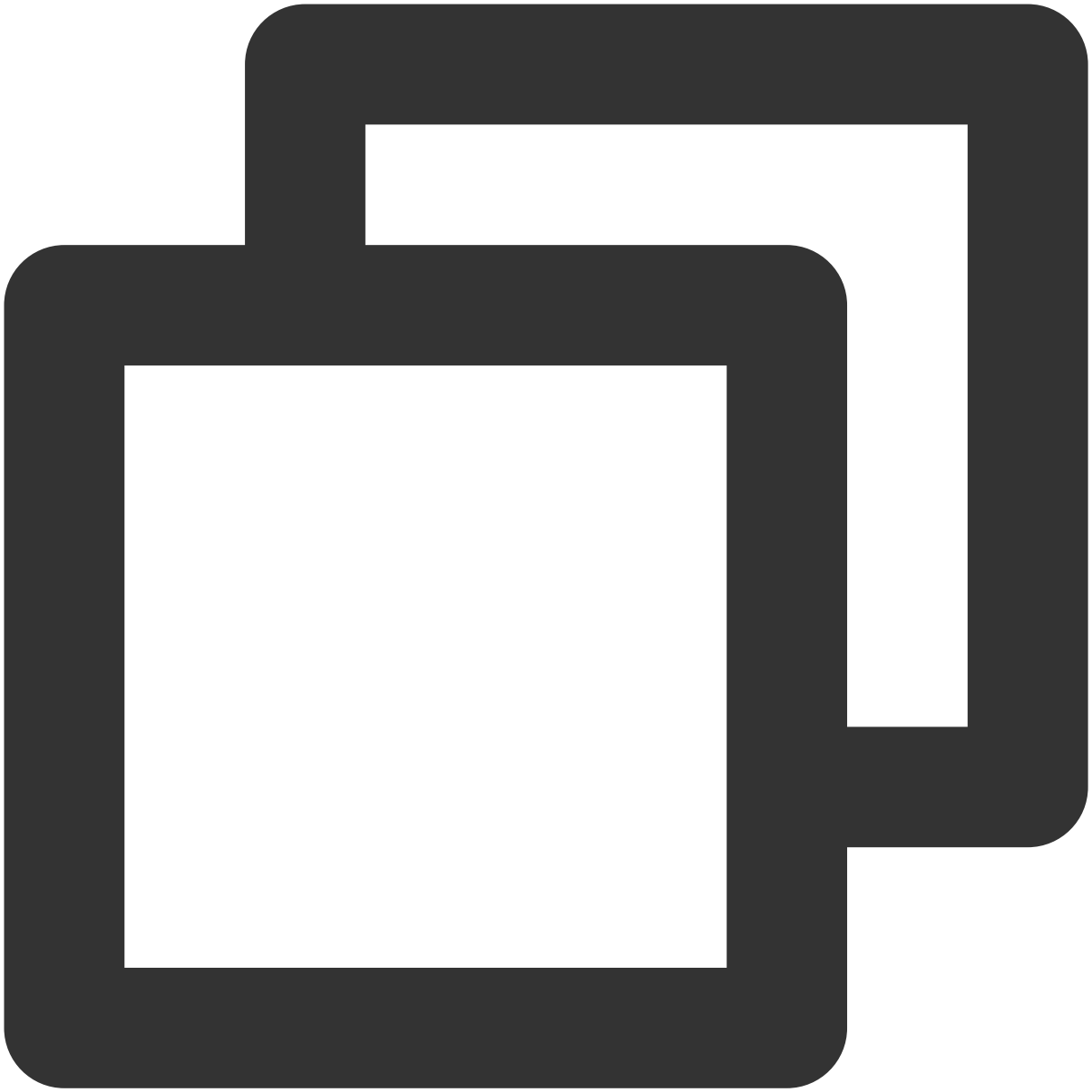
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CVM 服务的完全管理权限（创建、管理、云服务器下单支付等全部操作权限）。

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：

步骤1：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:::*"
            }
        ]
    }
```

步骤2：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：2024-01-23 18:02:53

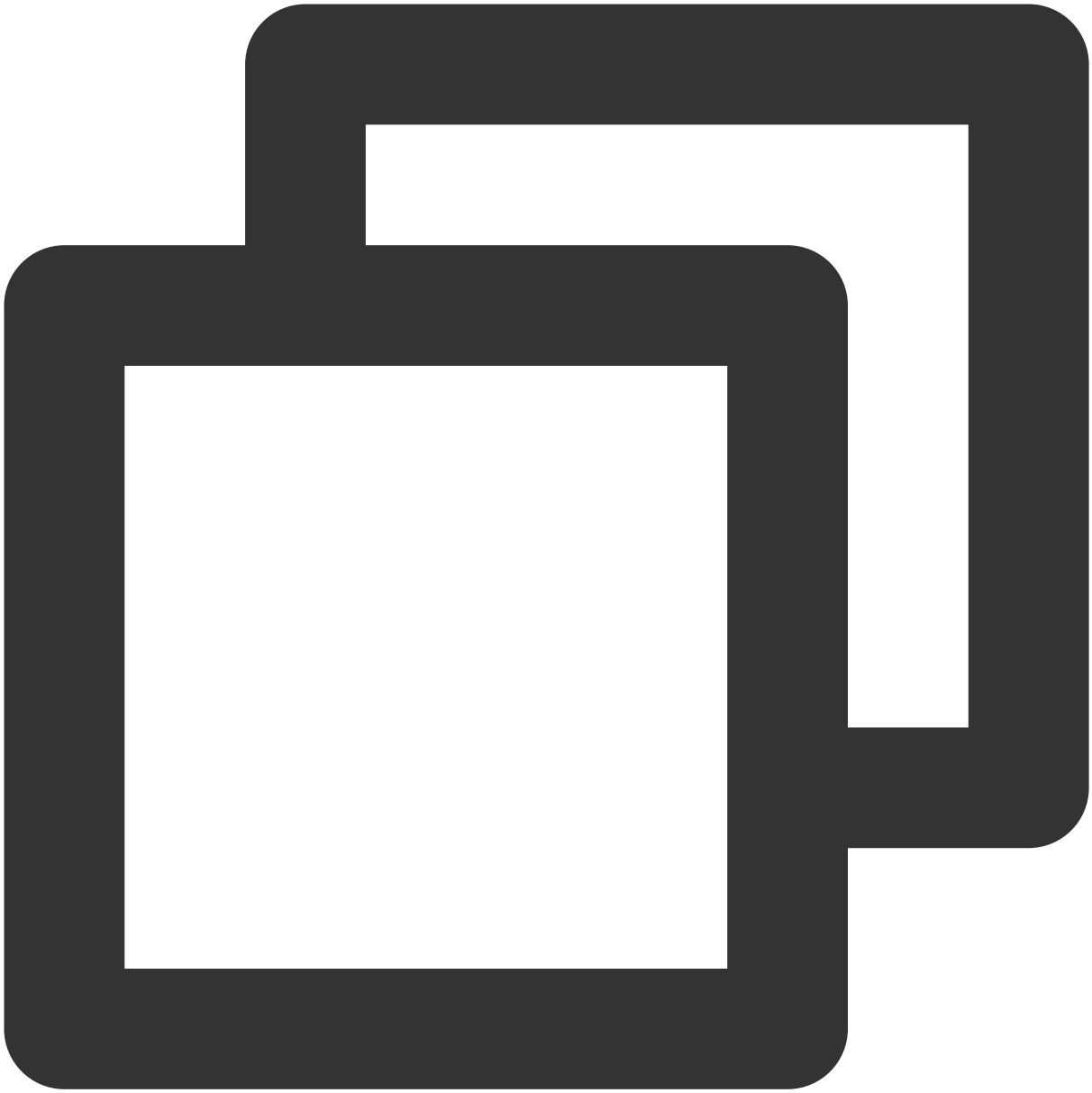
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CVM 服务的查询 CVM 实例的权限，但是不具有创建、删除、开关机的权限。

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：

步骤1：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": "*"
     }
```

```
        ]
    }
```

步骤2：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：2024-01-23 18:02:53

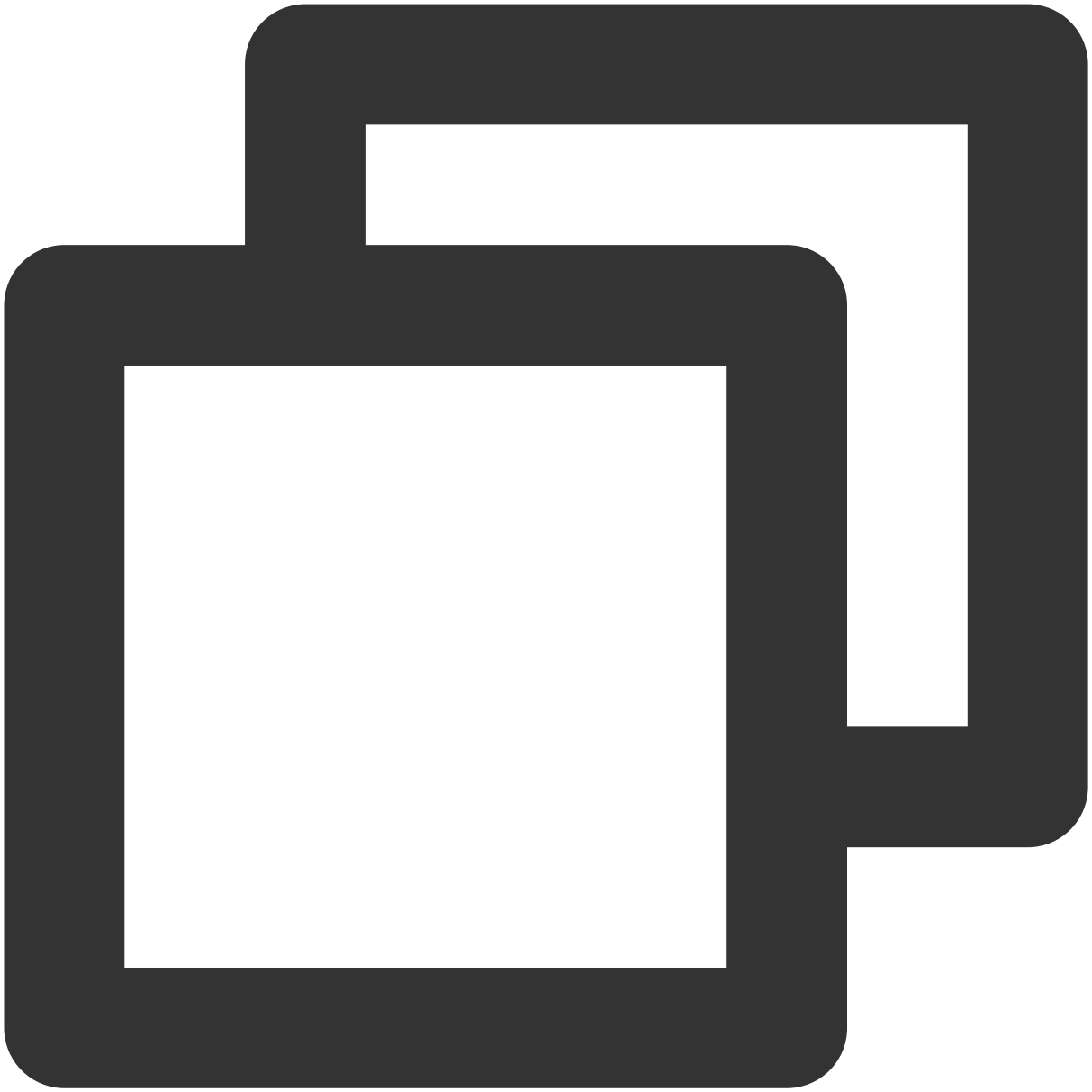
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CVM 服务的查询 CVM 实例及相关资源（VPC 、CLB）的权限，但是不具有创建、删除、开关机的权限。

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：

步骤1：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": "*"
        }
    ]
}
```

步骤2：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：2024-01-23 18:02:53

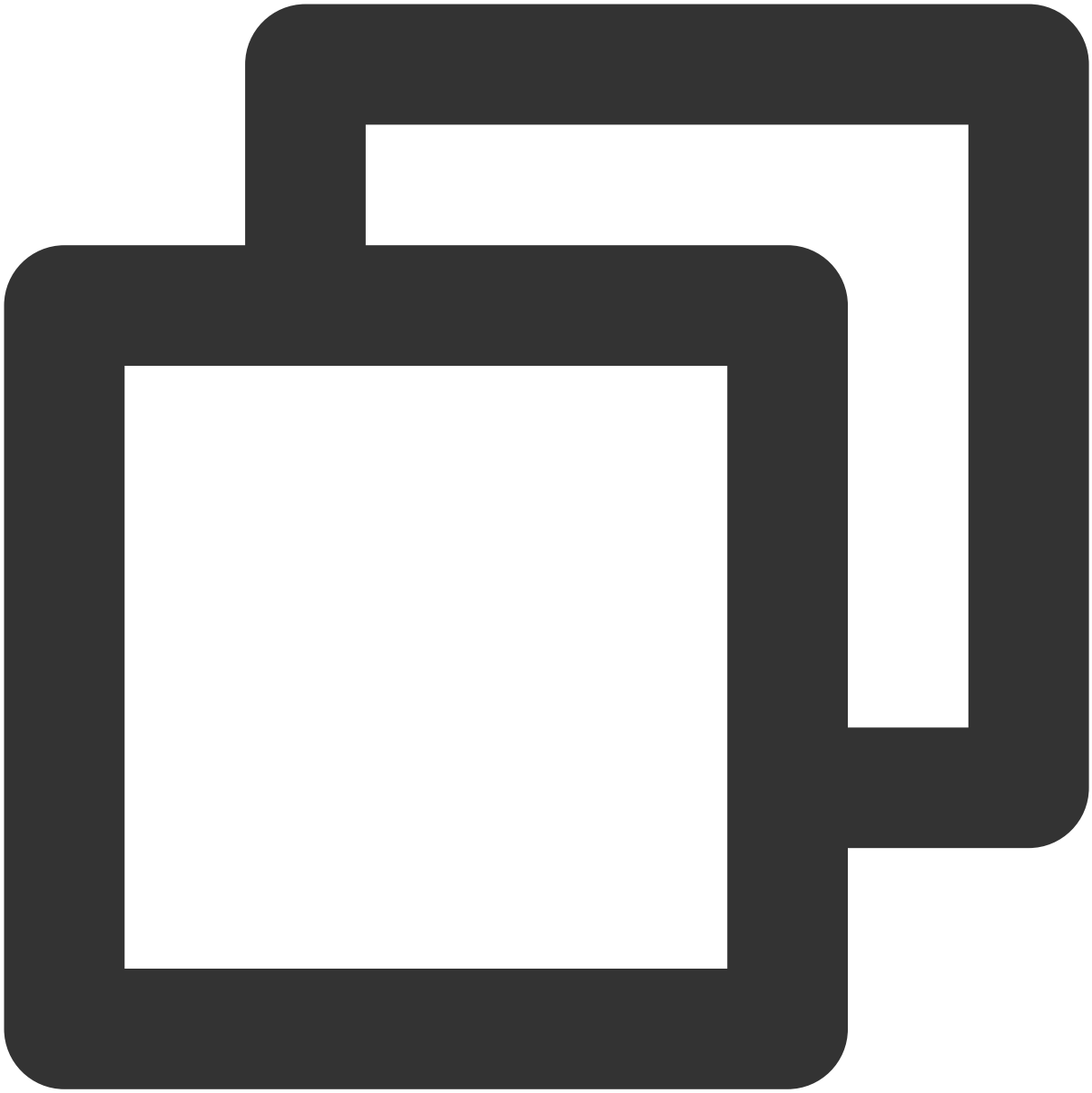
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CVM 服务的查看 CVM 控制台中的云硬盘信息、创建云硬盘、使用云硬盘的权限。

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：

步骤1：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"
        }
    ]
}
```

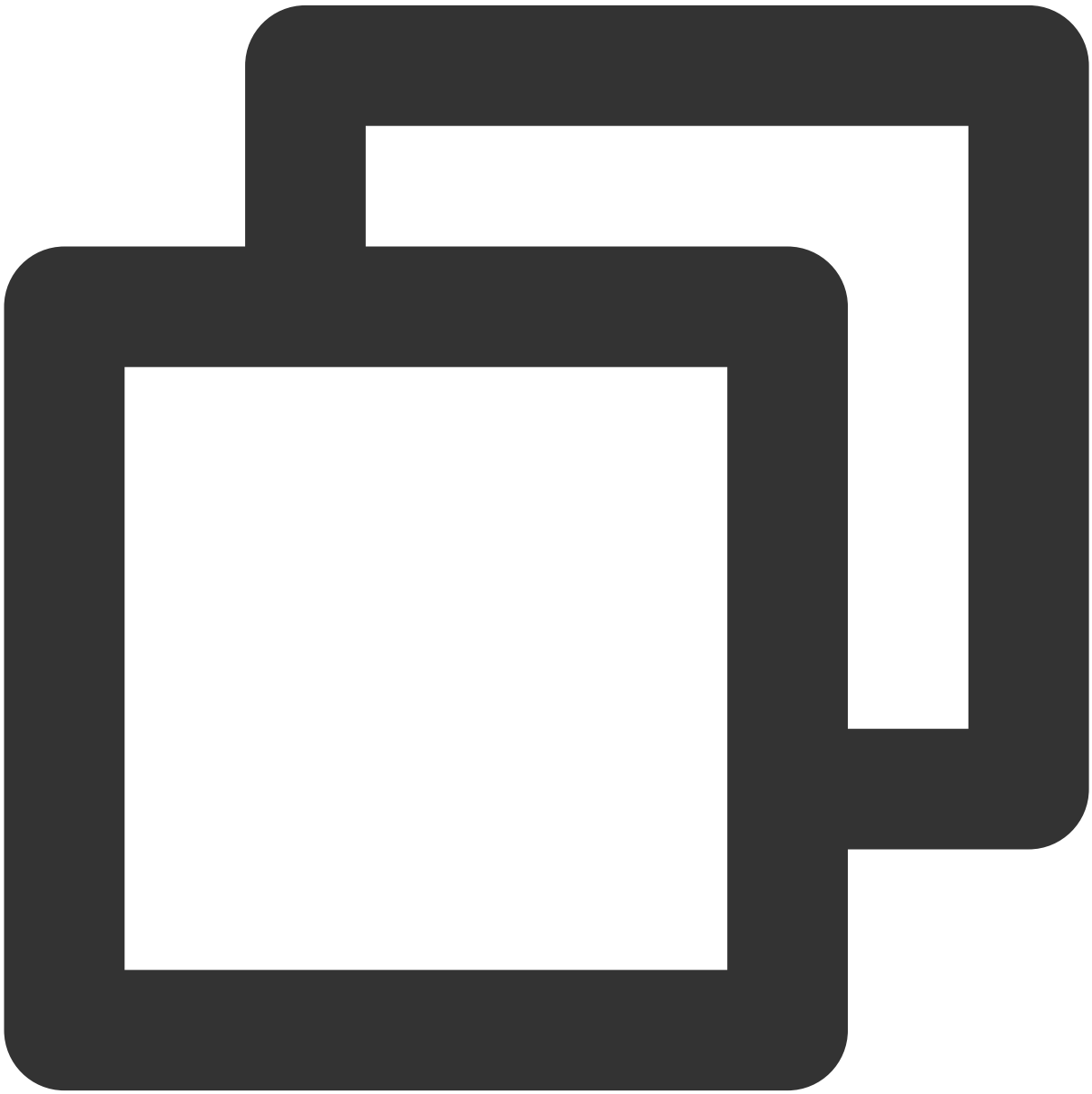
步骤2：将该策略授权给子账号。授权方式请参考 授权管理。

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：2024-01-23 18:02:53

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。



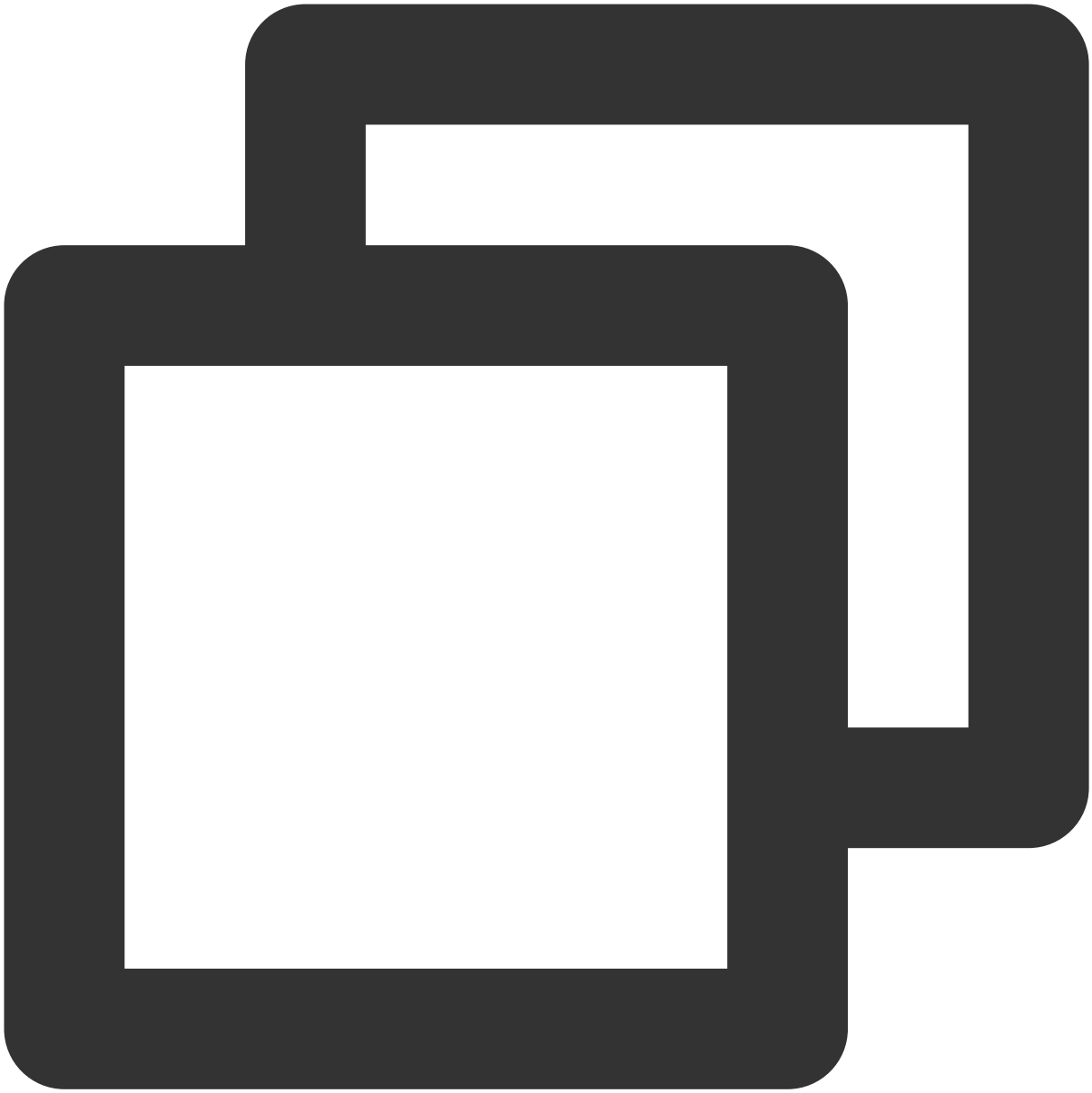
```
{
```

```
    "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。

步骤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"
```

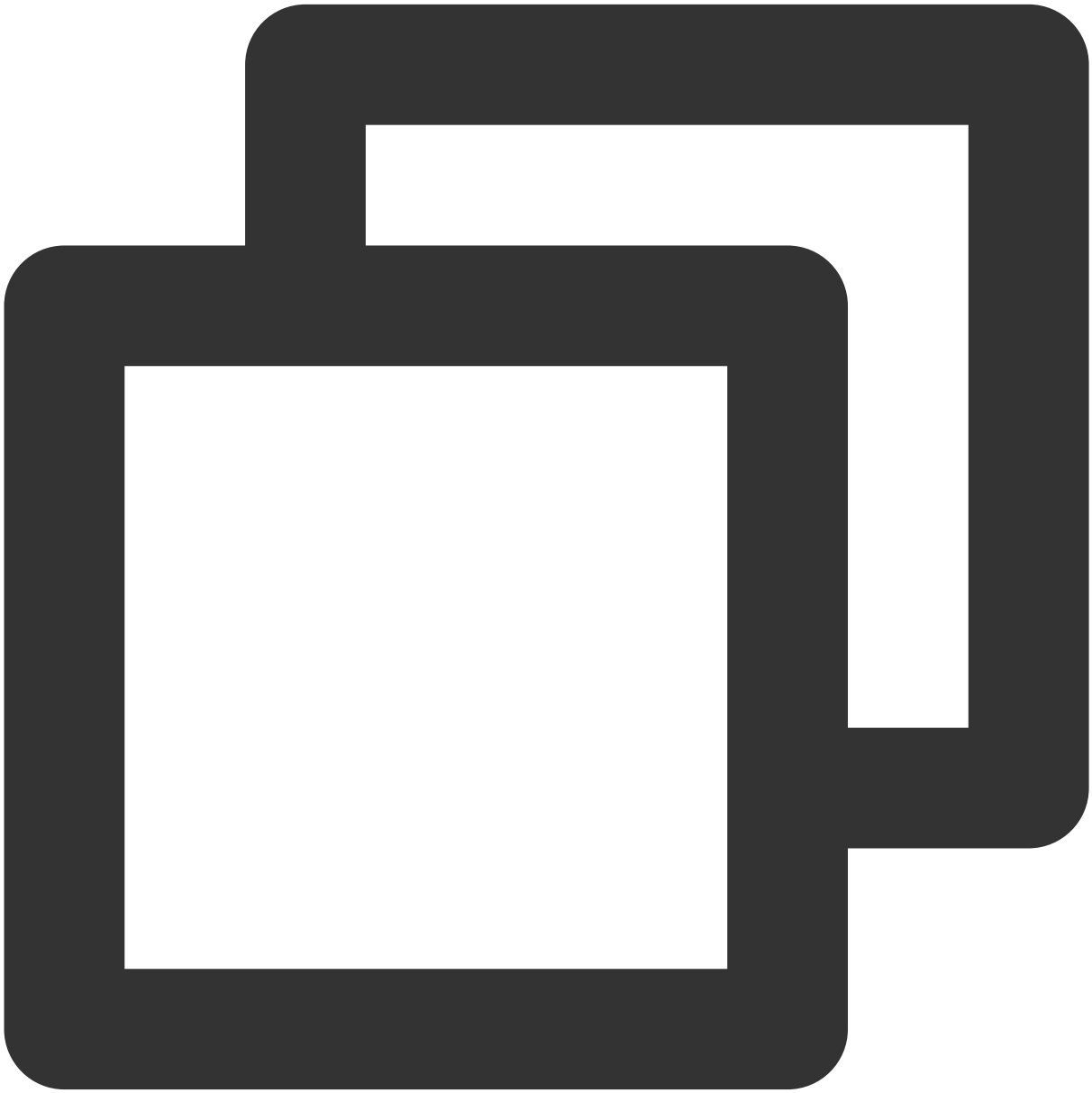
```
            }
        ]
    }
```

步骤2：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：2024-01-23 18:02:53

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 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。
步骤1：通过策略语法方式创建以下策略。



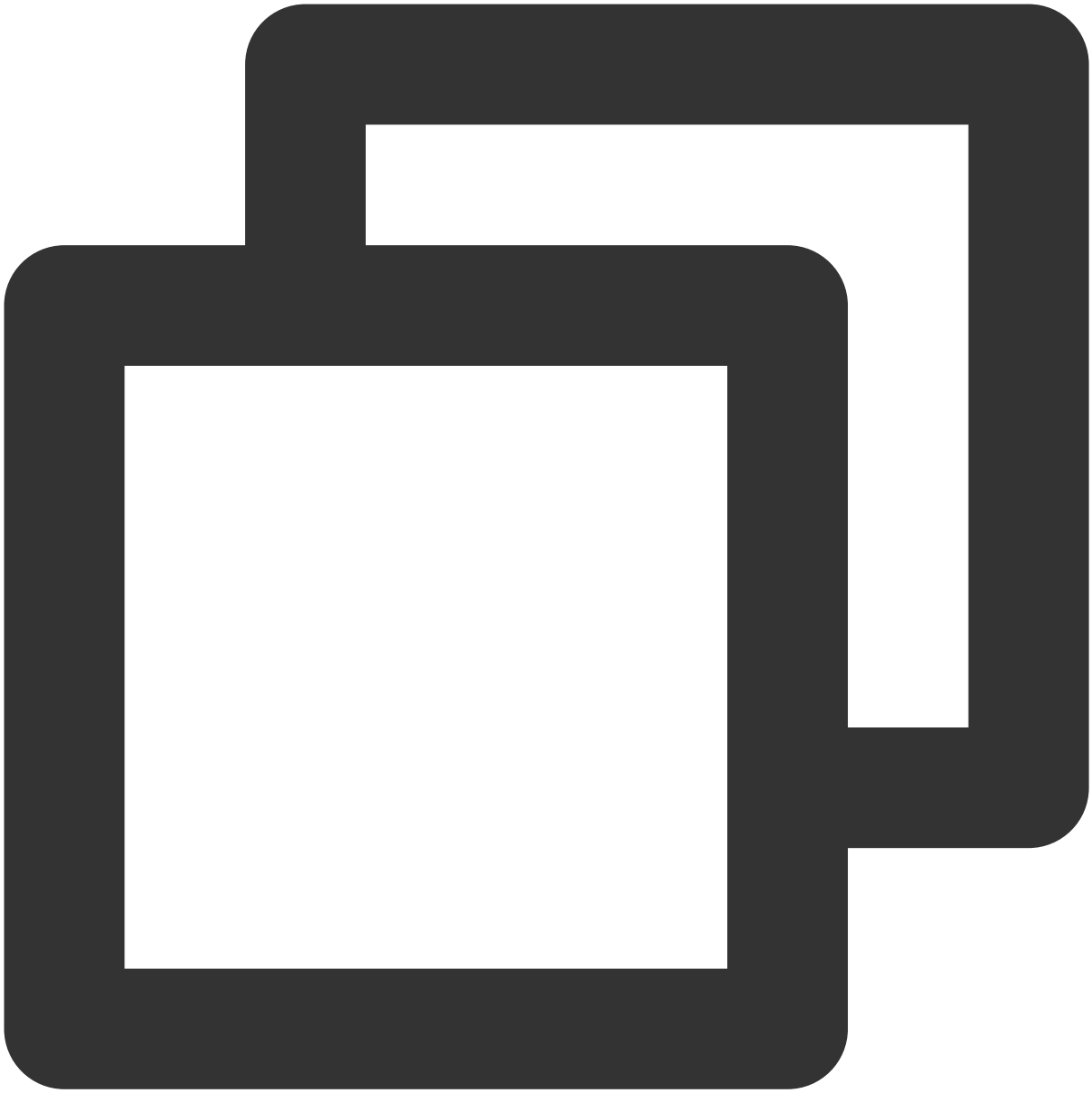
```
{
    "version": "2.0",
```

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

步骤2：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。

步骤1：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"
```

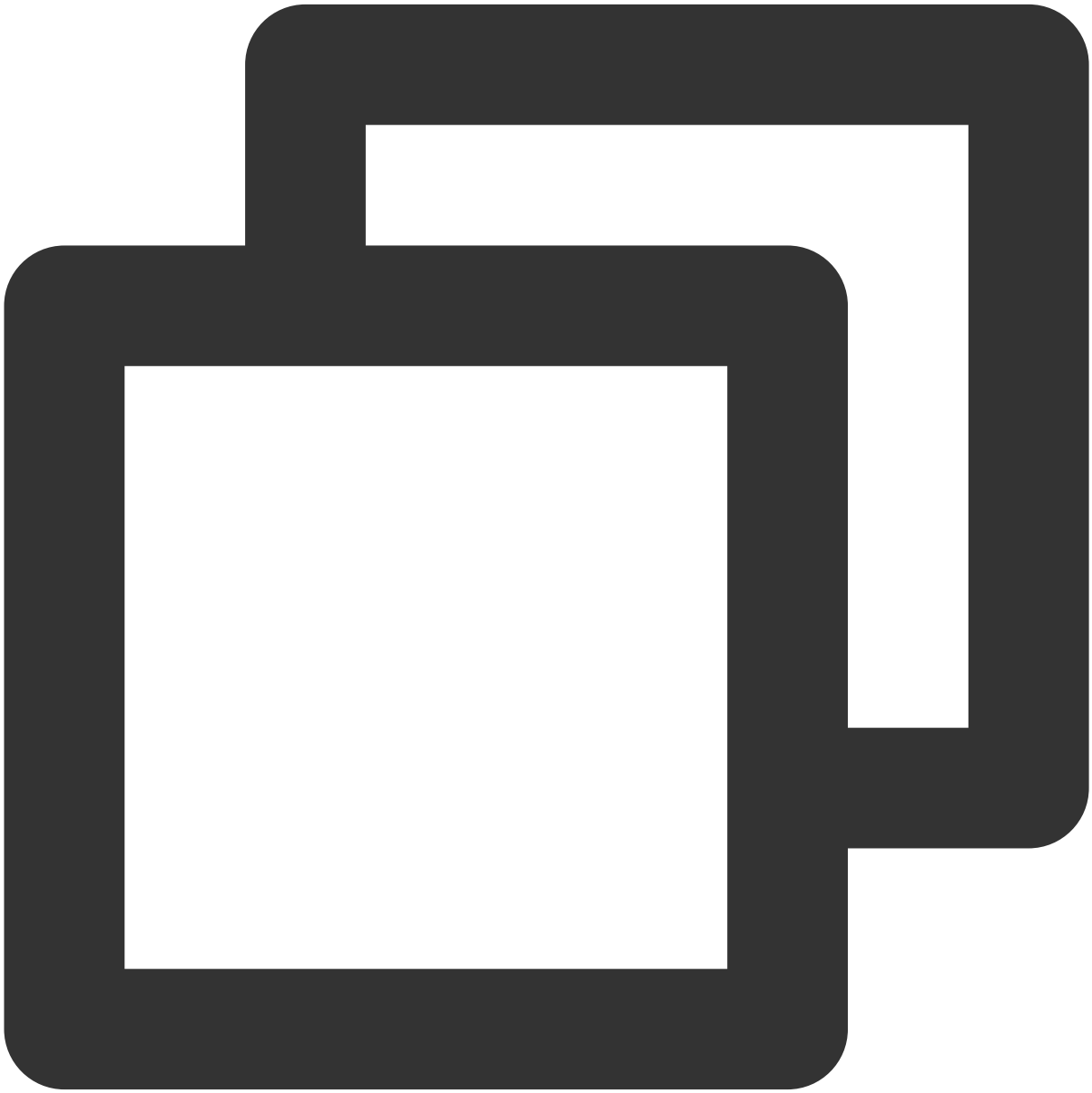
```
            }
        ]
    }
```

步骤2：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：2024-01-23 18:02:53

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 的指定 CVM 机器（id 为 ins-1,广州地域）的操作权限。
步骤1：通过策略语法方式创建以下策略。



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

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

步骤2：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

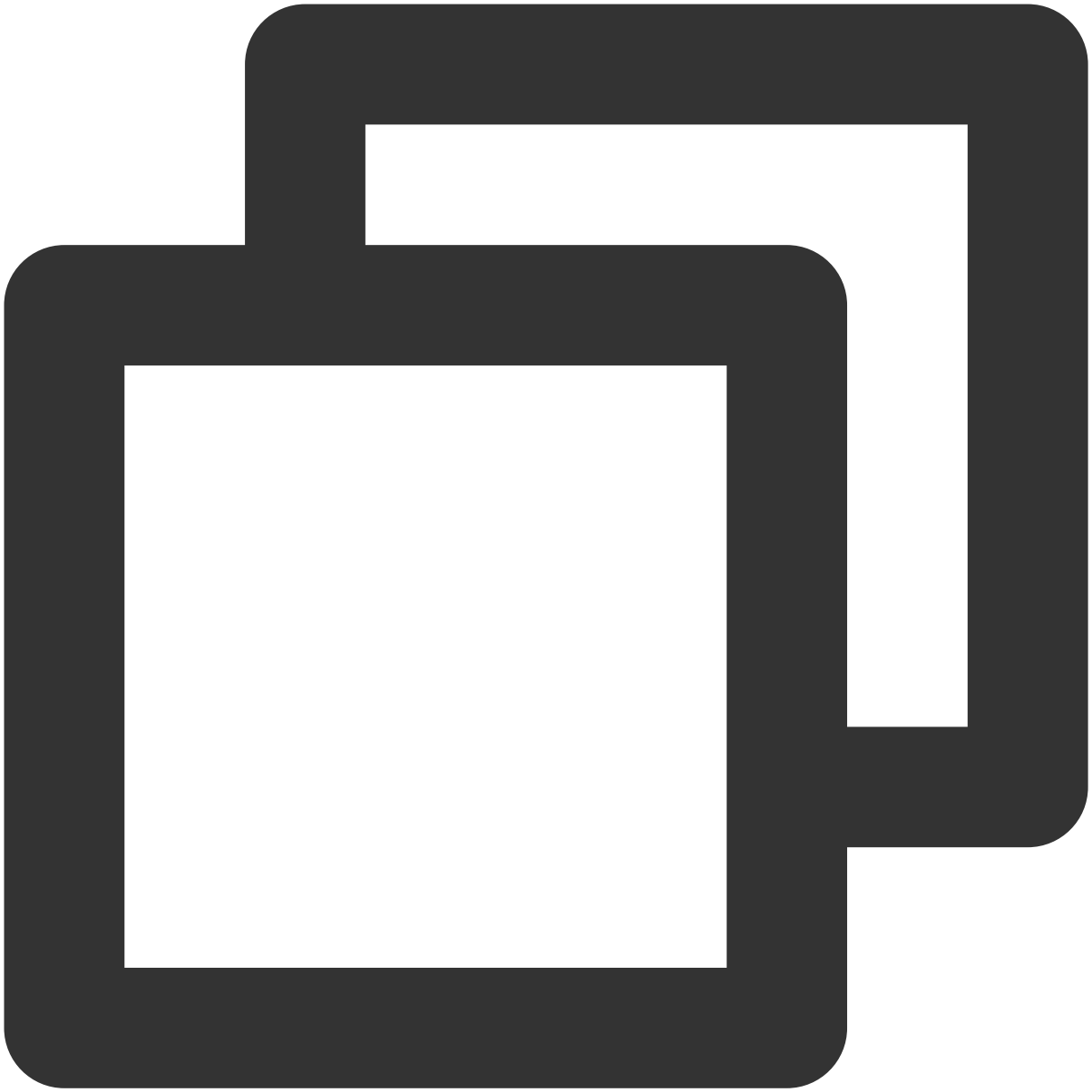
最近更新时间：2024-01-23 18:02:53

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 的广州地域所有机器的操作权限。

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：

步骤 1：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"
        }
    ]
}
```

步骤 2：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：2024-01-23 18:02:53

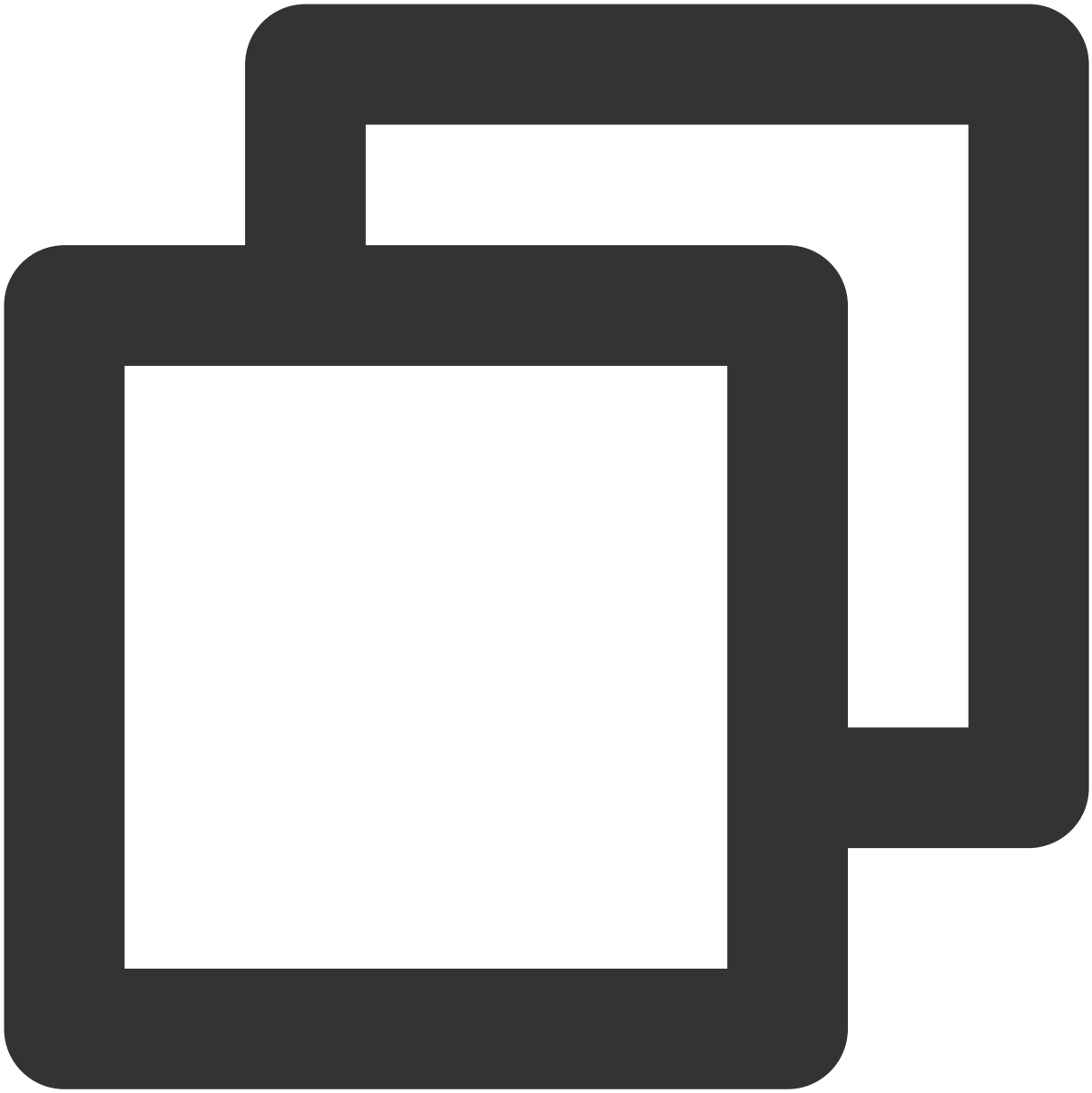
企业帐号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 CVM 服务的所有管理权限（创建、管理等全部操作），但不包括支付权限，可下单但无法支付。

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：

步骤1. 通过策略语法方式创建以下策略。



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

步骤2. 将该策略授权给子账号。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：2024-01-23 18:02:53

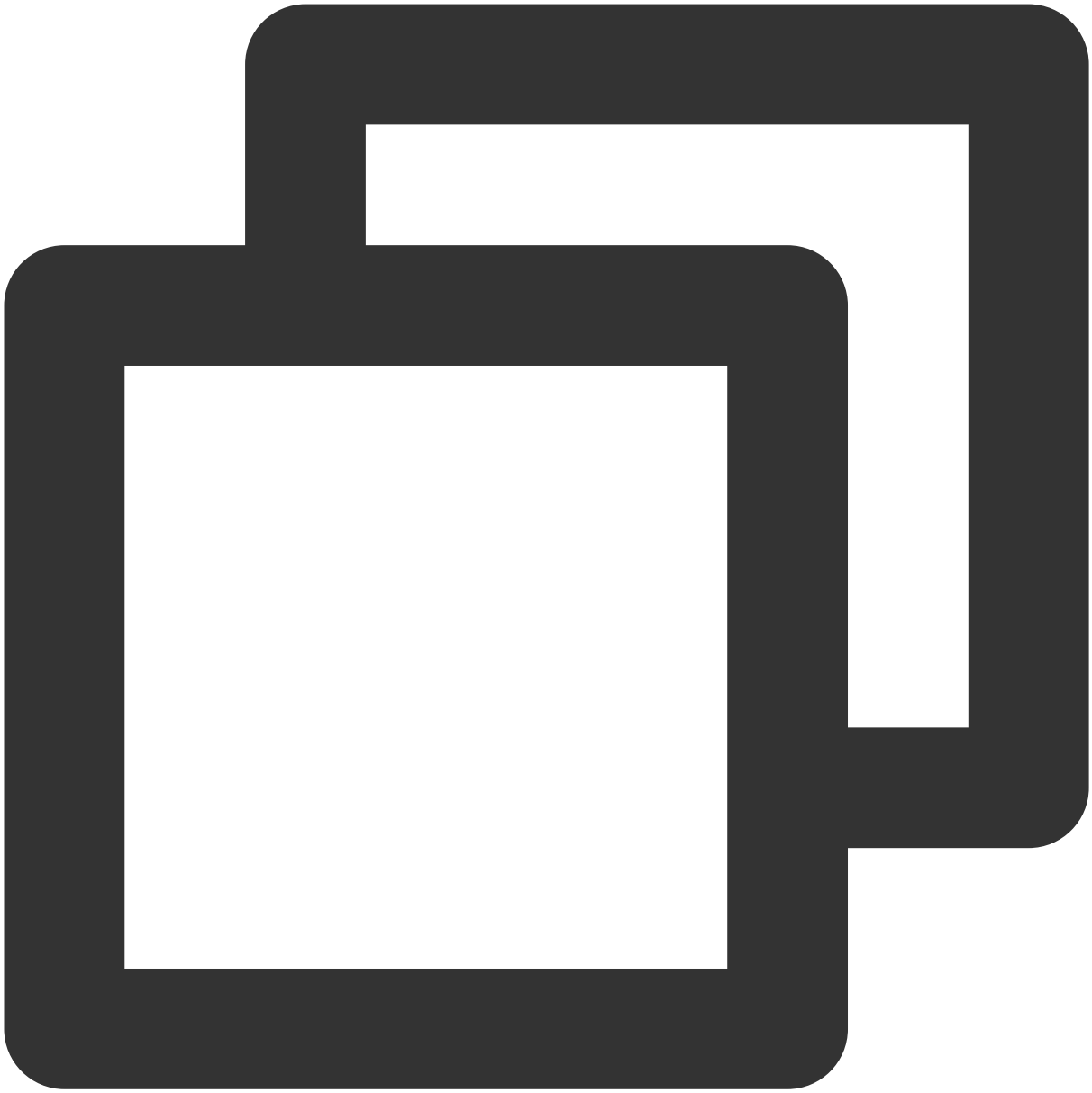
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的VPC 服务的只读权限（查询 VPC 及相关资源，但无法创建、更新或删除它们）。

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：

步骤1：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"
```

```
            }
        ]
    }
```

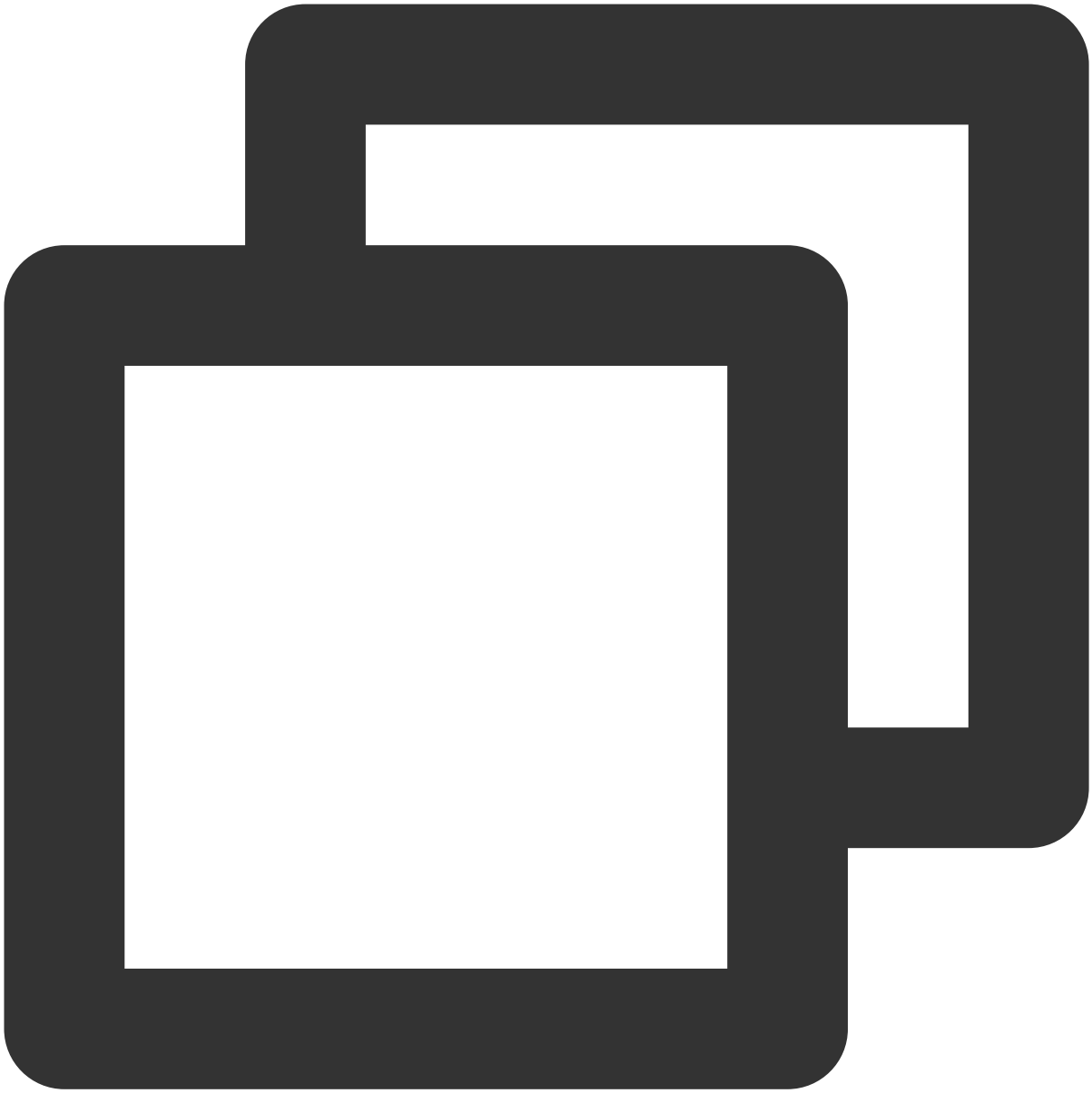
步骤2：将该策略授权给子账号。授权方式请参考 授权管理。

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：2024-01-23 18:02:53

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 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。

步骤1：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"
                        ]
                    }
                }
            }
        ]
    }
```

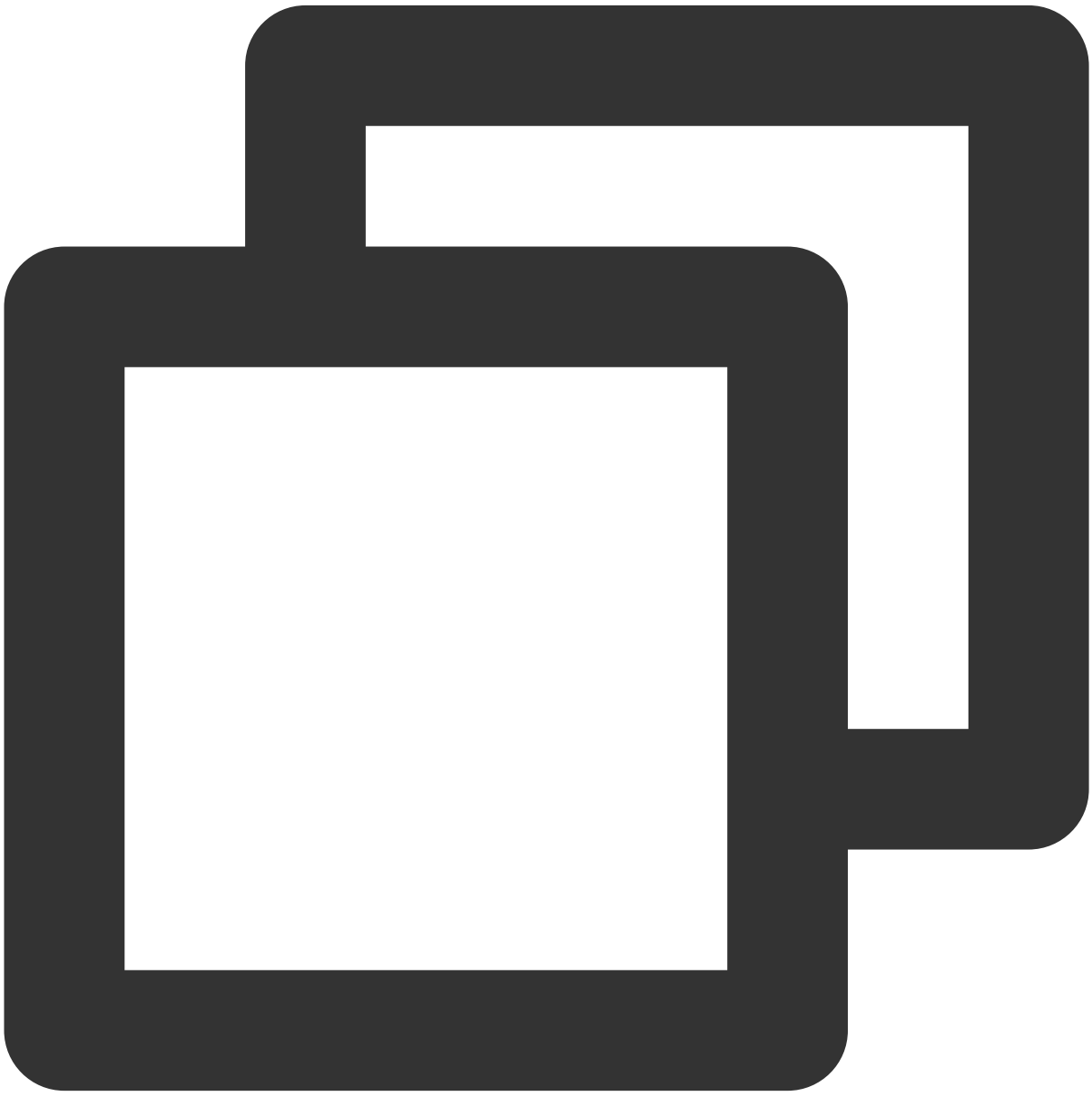
步骤2：将该策略授权给子账号。授权方式请参考 授权管理。

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：2024-01-23 18:02:53

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 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。

步骤1：通过策略语法方式创建以下策略。



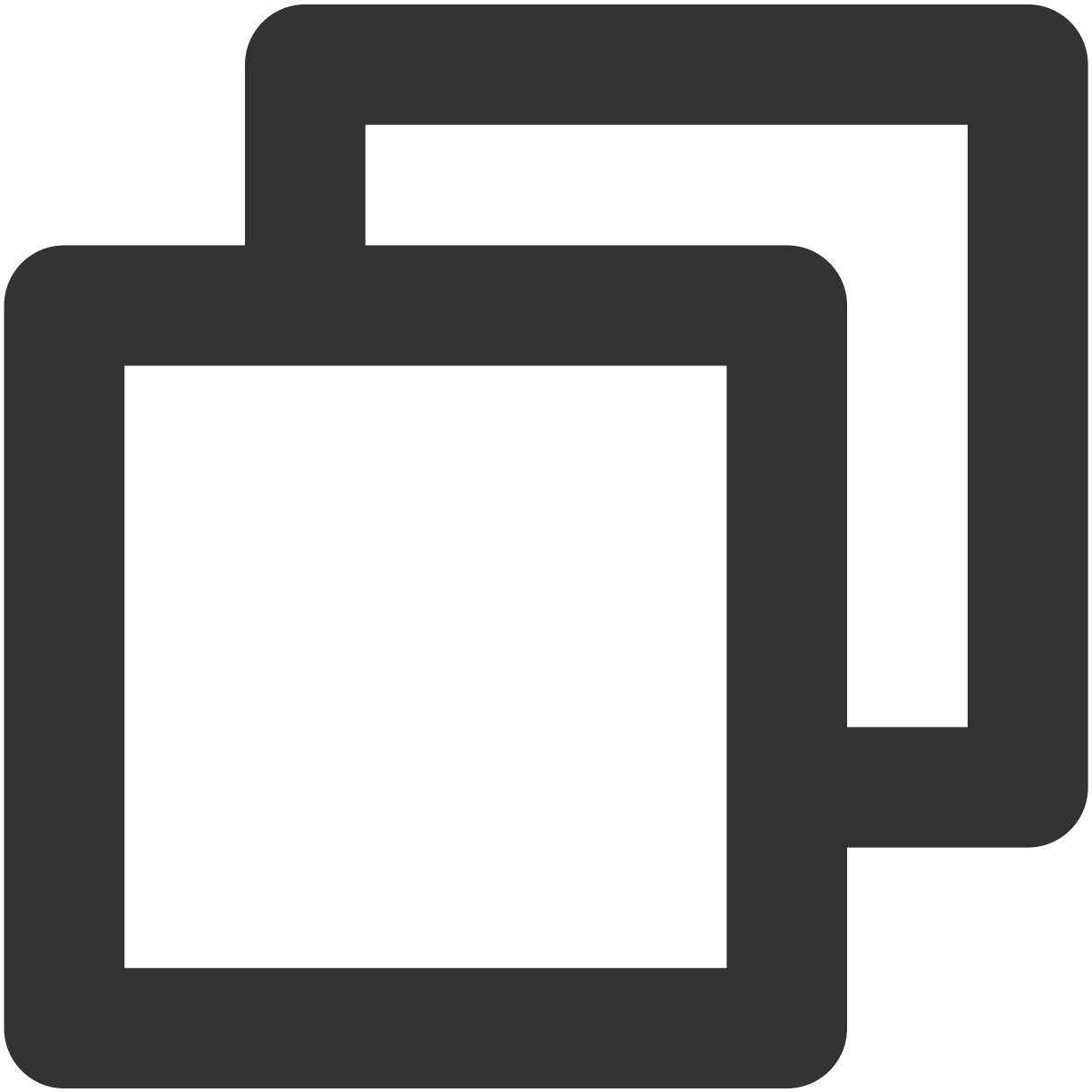
```
{
    "version": "2.0",
    "statement": [
        {
            "action": [
                "vpc:*"
            ],
            "resource": "*",
            "effect": "allow"
        },
        {
            "action": [
                "vpc:AssociateRouteTable",
                "vpc:CreateRoute",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

步骤2：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：2024-01-23 18:02:53

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 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。
步骤1：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"
        }
    ]
}
```

步骤2：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：2024-01-23 18:02:53

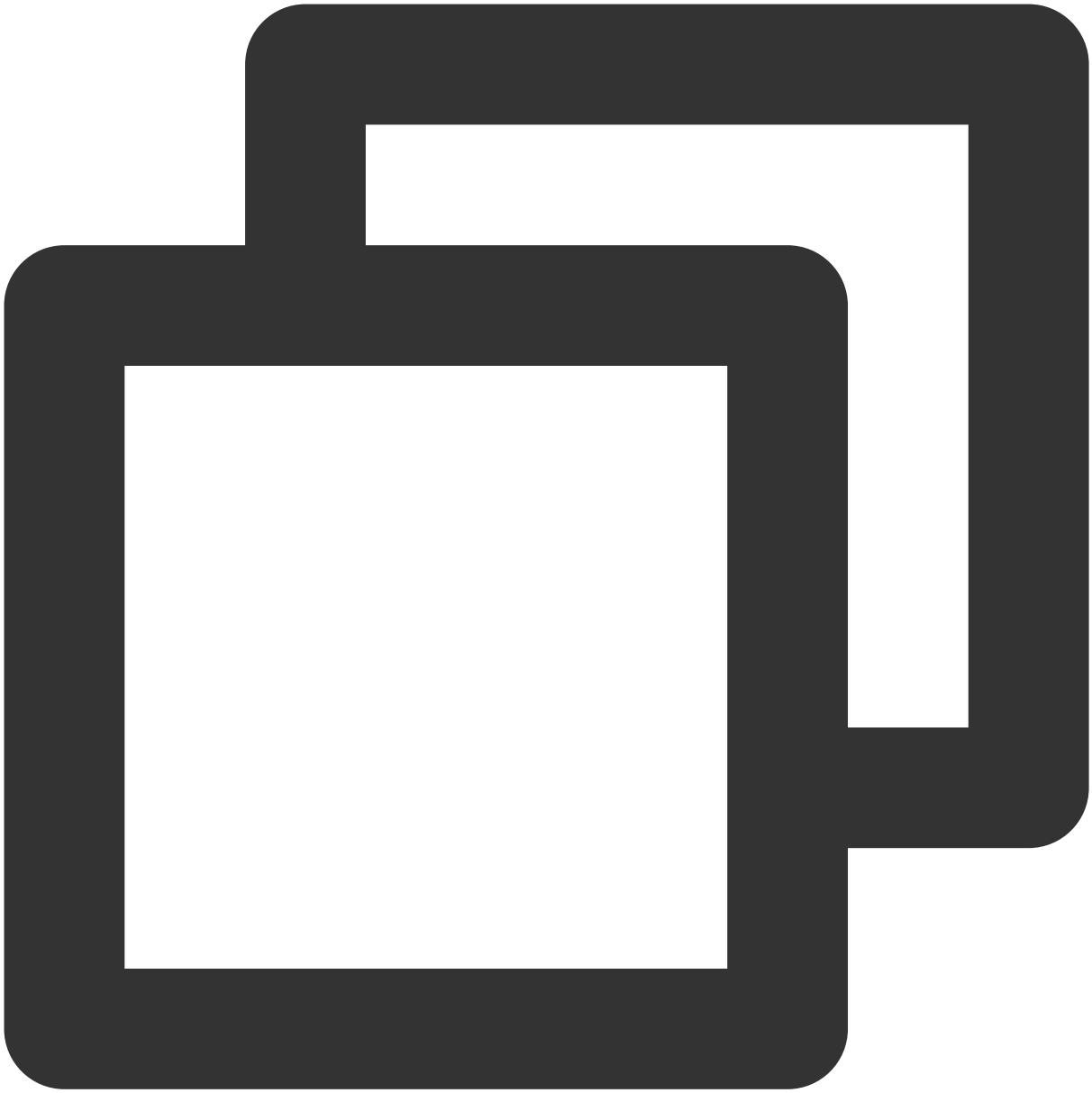
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 VPC 服务的完全管理权限（创建、管理、VPC 下单支付等全部操作）。

方案A：

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

方案B：

步骤1：通过策略语法方式创建以下策略。



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

```
                "resource": "qcs::vpc:::*"
            }
        ]
    }
```

步骤2：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：2024-01-23 18:02:53

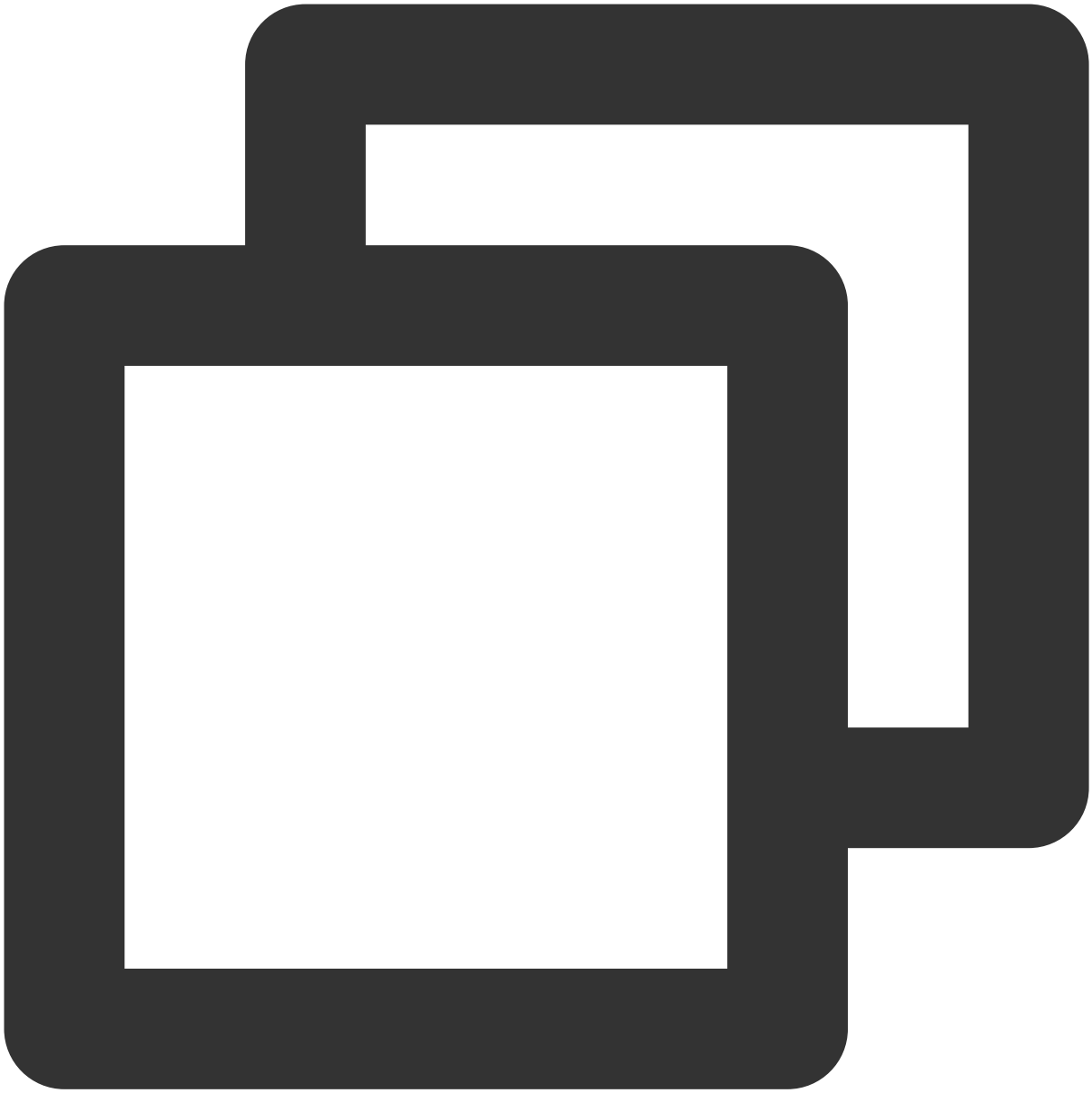
企业帐号 CompanyExample（ownerUin 为 12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的 VPC 服务的所有管理权限（创建、管理等全部操作），但不包括支付权限，可以下单但无法支付。

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：

步骤1：通过策略语法方式创建以下策略。



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

步骤2：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：2024-01-23 18:02:53

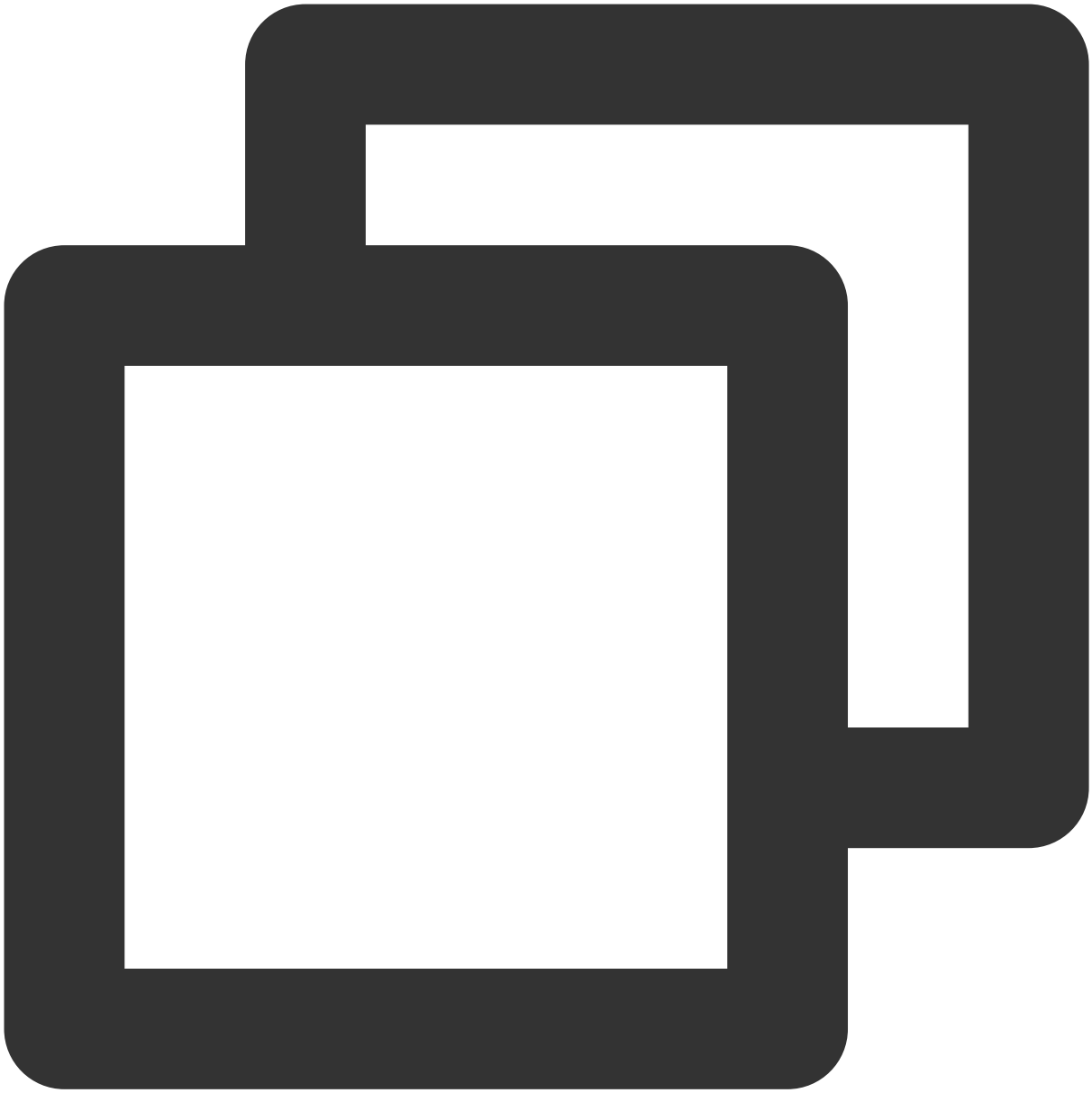
企业帐号 CompanyExample（ownerUin 为12345678）下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 的云点播服务的完全管理权限。

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：

步骤1：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"
        }
    ]
}
```

步骤2：将该策略授权给子账号。授权方式请参考 授权管理。

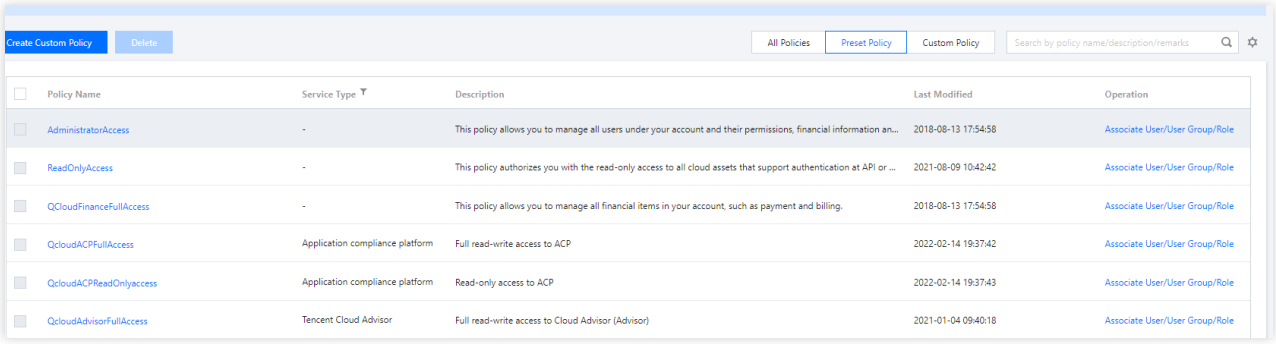
其他案例
授予指定产品的管理权限或只读权限

最近更新时间：2024-01-23 18:02:53

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。

步骤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。

步骤2：

将上述策略授权给 CAM 子账号/用户组。授权方式请参考 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、云服务资产。

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产。

授权子账号拥有所有资源的操作权限

最近更新时间：2024-01-23 18:02:53

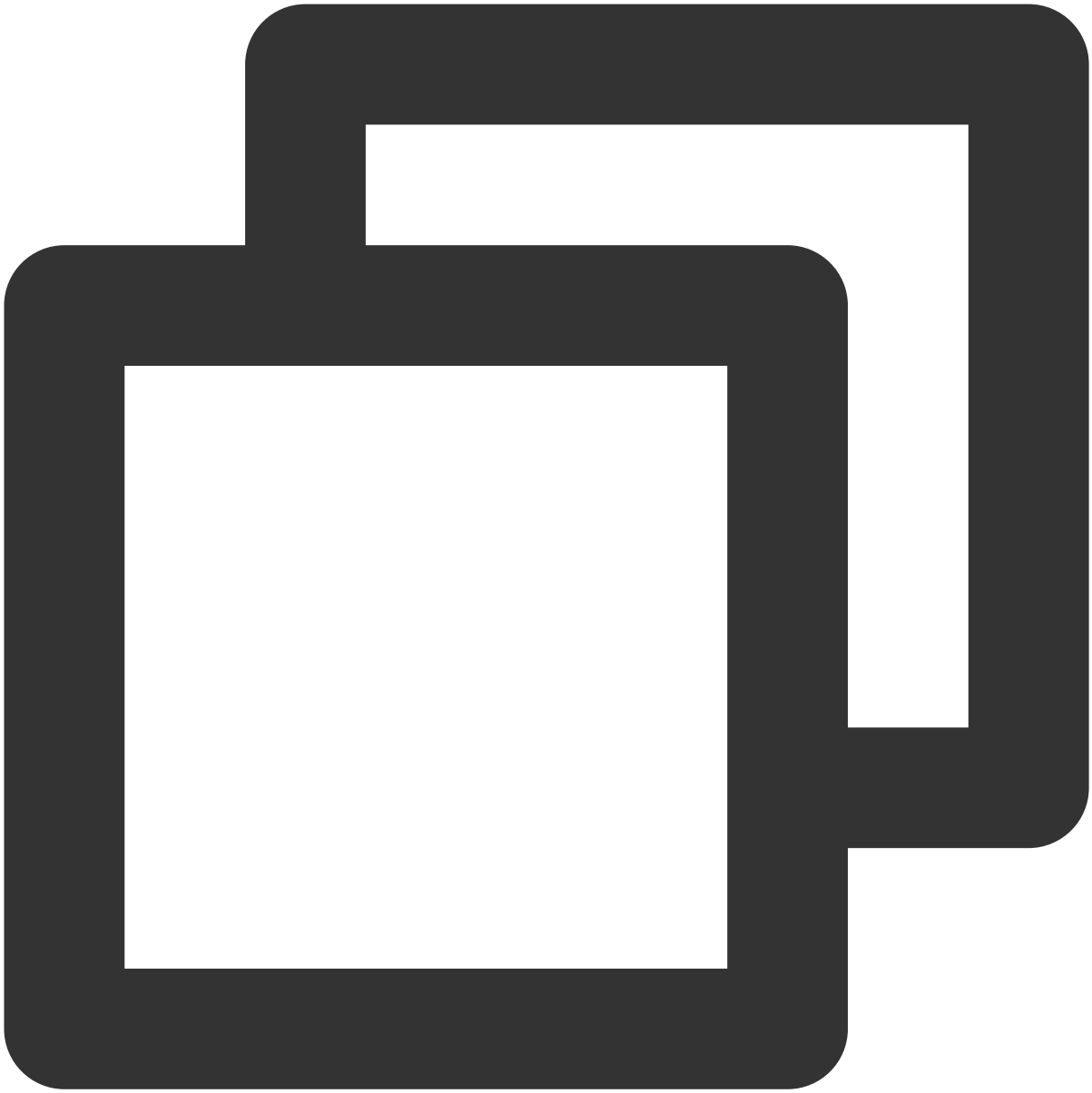
企业帐号 CompanyExample 下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 名下的所有资源都有完全访问权限。

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：

步骤1：通过策略语法方式创建以下策略。



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

步骤2：将该策略授权给子账号。授权方式请参考 授权管理。

授权子账号拥有所有资源的只读权限

最近更新时间：2024-01-23 18:02:53

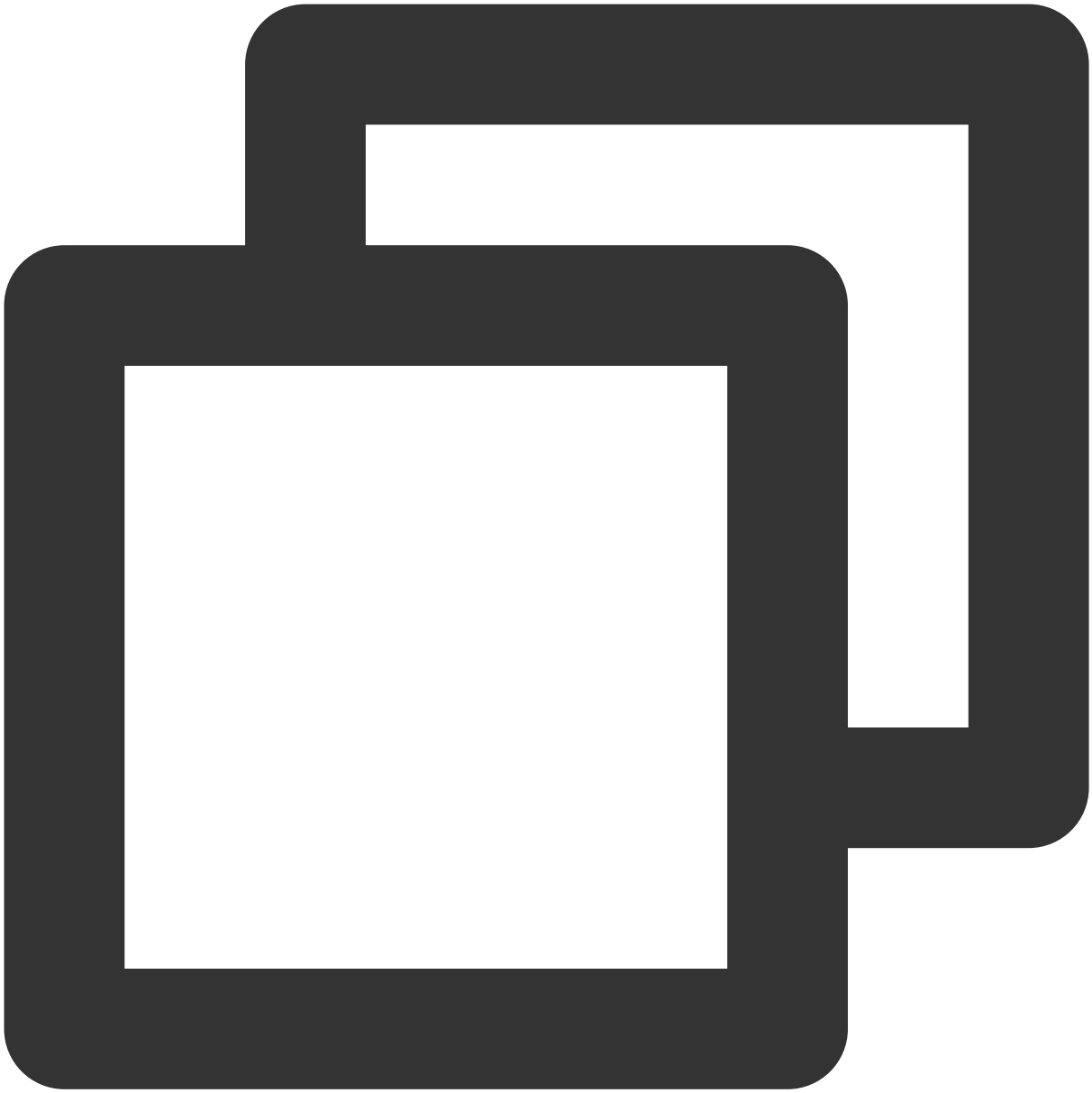
企业帐号 CompanyExample 下有一个子账号 Developer，该子账号需要拥有对企业帐号 CompanyExample 名下的所有资源的只读权限。

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：

步骤1：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:Describe*",
                "monitor:Get*",
                "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*",
                "ccs:Describe*",
                "ccs:Check*",
                "cam:Get*",
                "cam:List*",
                "cam:Describe*",
                "cam:Query*",
                "cdb:Describe*",
                "batch:Describe*",
                "bgpip:BasicGet*",
                "bgpip:BasicCCGet*",
                "bgpip:BasicDDoSGet*",
                "bgpip:BgpGetFpcDeviceList",
                "bgpip:BGPGetInfo",
                "bgpip:BGPGetServiceStatistics",
                "bgpip:BGPGetServicePacks",
                "bgpip:BGPCCGet*",
                "bgpip:BGPWhitelistGet",
                "bgpip:Get*",
                "bgpip:BGPIPWhitelistGet",
                "bgpip:BGPIPGet*",
                "bgpip:BGPIPDDoSGet*",
                "bgpip:BGPIPCCGet*",
                "bgpip:BgpipGetIdByTran",
                "bgpip:BgpipModifyPrice",
                "bgpip:BgpipRenewPrice",
                "bgpip:BgpipCreatePrice",
                "bgpip:BgpipQueryResources",
                "bgpip:BgpipCheckModify",
                "bgpip:BgpipCheckRenew",
                "bgpip:BgpipCheckCreate",
```

```
                "bgpip:BGPDDoSGet*",
                "ccb:ListGitAuth",
                "ccr:pull",
                "ccs:Describe*",
                "ccs:Check*",
                "ckafka:Get*",
                "ckafka:List*",
                "organization:Get*",
                "organization:List*",
                "redis:Describe*",
                "scf:Get*",
                "scf:List*",
                "shield:*Get*",
                "tag:Get*",
                "waf:WafGet*",
                "waf:WAFGetUserInfo",
                "waf:WafDownloadAlerts",
                "waf:WafPackagePrice",
                "waf:WafAreaBanGetAreas",
                "waf:WafFreqGetRuleList",
                "waf:WafAntiFakeGetUrl",
                "waf:WafDNSdetectGet*",
                "waf:BotGet*",
                "wss:CertGetList",
                "cbm:previewProductDetail",
                "cbm:agentInfo",
                "cbm:viewDeals",
                "cbm:rebateInfo",
                "cbm:businessDetail",
                "cbm:inviteClient",
                "cbm:viewClients",
                "cbm:authorize",
                "cbm:viewMessage",
                "cbm:viewMenu",
                "snova:Describe*",
                "gme:Describe*",
                "gme:Download*"
            ],
            "resource": "*",
            "effect": "allow"
        }
    ]
}
```

步骤2：将该策略授权给子账号。授权方式请参考 授权管理。

授权不同子账号拥有独立的云资源管理权限

最近更新时间：2024-01-23 18:02:53

操作场景

若您的公司购买了多种腾讯云资源，您可以通过为资源标记标签的方式来对腾讯云已有资源的进行分类管理，为不同的子账号分配对应的标签管理权限，从而实现子账号独立管理标签下的资源。本文档以一个典型案例让您轻松了解如何通过标签实现子账号拥有独立的云资源权限。

前提条件

假设存在以下条件：
企业帐号 CompanyExample 下有两个子账号 DevA 和 DevB。
已知子账号 DevA 的账号 ID 为 12345。
已知子账号 DevB 的账号 ID 为 67890。
企业帐号 CompanyExample 下有两个云服务器，实例 ID 为 ins-1 和 ins-2。
企业帐号 CompanyExample 下有两个标签键、标签值，分别为test1&test1、test2&test2。

操作步骤

使用标签标记云服务器

您可以通过以下步骤为两个云服务器 ins-1、ins-2标记不同的标签键及标签值，实现分标签管理。

为云服务器 ins-1 标记标签键、标签值为test1&test1

1. 登录进入 资源标签控制台，选择以下信息设置筛选规则筛选出您需要设置的云服务器，单击【查询资源】。
资源类型：需要查询资源所属类型，仅支持标签的产品，详情请参见 支持标签的产品。在本次示例中，选择云服务器实例。
地域：需要查询资源所属地域。在本次示例中，云服务器所属地域为北京。
2. 在资源标签页面下方的筛选结果列表，在左侧勾选需要添加标签的云服务器。在本次示例中，云服务器实例 ID 为 ins-1。
3. 单击**编辑标签值**，进入“编辑已有标签窗口”。
4. 在“编辑已有标签窗口”，填写标签键、标签值信息，本示例标签键、标签值为 test1&test1。
5. 单击**确定**，完成为云服务器 ins-1 标记标签键、标签值为 test1&test1 的操作。

为云服务器 ins-2 标记标签键、标签值为test2&test2

1. 登录进入 资源标签控制台，选择以下信息设置筛选规则筛选出您需要设置的云服务器，单击**查询资源**。
资源类型：需要查询资源所属类型，仅支持标签的产品，详情请参见 支持标签的产品。在本次实例中，选择云服务器实例。
地域：需要查询资源所属地域，在本次示例中，云服务器所属地域为北京。
2. 在资源标签页面下方的筛选结果列表，在左侧勾选需要添加标签的云服务器。在本次示例中，云服务器实例 ID 为 ins-2。
3. 单击**编辑标签值**，进入“编辑已有标签窗口”。
4. 在“编辑已有标签窗口”，填写标签键、标签值信息，本示例标签键、标签值为 test2&test2。
5. 单击**确定**，完成为云服务器 ins-2 标记标签键、标签值为 test2&test2 的操作。

给用户按标签授权

您可以参考以下步骤为子账号 DevA 授予标签键、标签值为test1&test1 管理权限，为子账号 DevB 授予标签键、标签值为test2&test2 管理权限，即两个子账号分别拥有对应标签下资源的独立管理权限。

为子账号 DevA 授予标签键、标签值为 test1&test1 管理权限

1. 进入 策略管理控制台，单击左上角的**新建自定义策略**。
2. 在弹出的选择创建方式窗口中，单击**按标签授权**，进入按标签授权页面。
3. 在按标签授权页面选择以下信息，单击**下一步**，进入检查页面。
赋予用户/用户组：勾选需要授权的用户/用户组。在本次示例中，子账号 DevA 的账号 ID 为 12345。
在标签键：选择需要授权的标签键。在本次示例中，标签键为 test1。
且具有标签值：选择需要授权的标签值。在本次示例中，标签值为 test1。
的资源：默认为管理权限。
4. 在检查页面，填写策略名称、确认策略内容后单击**完成**，完成为子账号 DevA 授予标签键、标签值为test1&test1 管理权限的操作。

为子账号 DevB 授予标签键、标签值为test2&test2 管理权限

1. 进入 策略管理控制台，单击左上角的**新建自定义策略**。
2. 在弹出的选择创建方式窗口中，单击**按标签授权**，进入按标签授权页面。
3. 在按标签授权页面选择以下信息，单击**下一步**，进入检查页面。
赋予用户/用户组：勾选需要授权的用户/用户组。在本次示例中，子账号 DevB 的账号 ID 为 67890。
在标签键：选择需要授权的标签键。在本次示例中，标签键为 test2。
且具有标签值：选择需要授权的标签值。在本次示例中，标签值为 test2。
的资源：默认为管理权限。
4. 在检查页面，填写策略名称、确认策略内容后单击**完成**，完成为子账号 DevB 授予标签键、标签值为 test2&test2 管理权限的操作。

新增资源

如您有新增资源需要管理，请参考 使用标签标记云服务器 为新增资源标记标签键及标签值即可。