专线接入

访问管理

产品文档

腾讯云

文档目录

访问管理

访问管理概述

最近更新时间：2024-01-13 16:02:36

若您需使用专线接入、私有网络、云服务器等服务，且这些服务由不同人进行管理，但都共享您的云账号密钥，将存在以下问题：
您的密钥由多人共享，泄密风险高。
您无法限制其它人的访问权限，易产生误操作造成安全风险。
专线接入的专用通道支持资源级授权，您可以通过 CAM 服务实现由不同人管理不同服务，来解决上述问题。默认情况下，子账号不可以操作专用通道相关资源。因此需要创建相关策略允许子账号使用所需要的资源或权限。
说明：
若您不需要对子账户进行专用通道相关资源的访问管理，您可以跳过此章节。跳过此章节不会影响您对文档中其余部分的理解和使用。

授权支持列表

专线接入服务中包含物理专线、专用通道、专线网关等资源，对资源的授权详情如下：

资源名	是否支持授权	授权粒度
物理专线	是	接口级
专用通道	是	资源级
专线网关	是	资源级

CAM 概念

访问管理（Cloud Access Management，CAM）是腾讯云提供的一套 Web 服务，它主要用于帮助您安全管理腾讯云账户下的资源访问权限。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。
当您使用 CAM 时，可以将策略与一个用户或一组用户关联起来，策略能够授权或者拒绝用户使用指定资源完成指定任务。有关 CAM 策略的更多相关基本信息，请参见 策略语法。有关 CAM 策略的更多相关使用信息，请参见 策略。
根账户通过给子账户绑定策略实现授权，策略设置可精确到 API、资源、用户或用户组、允许或拒绝，条件等维度。
账户
根账号：腾讯云资源归属、资源使用计量计费的基本主体，可登录腾讯云服务。

子账号：由根账号创建账号，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。**

身份凭证：包括登录凭证和访问证书两种，**登录凭证**指用户登录名和密码，**访问证书**指云 API 密钥（SecretId 和 SecretKey）。

资源与权限

资源：指云服务中被操作的对象，如一个云服务器实例，COS 存储桶，VPC 实例等。

权限：指允许或拒绝某些用户执行某些操作。默认情况下，**根账号拥有其名下所有资源的访问权限**，而**子账号没有根账号下任何资源的访问权限**。

策略：指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。

说明：

更多相关信息，请参见 CAM 概述。

相关文档

目标	链接
了解策略和用户之间关系	策略
了解策略的基本结构	元素参考
了解还有哪些产品支持 CAM	支持 CAM 的产品

可授权策略类型

最近更新时间：2024-01-13 16:02:36

专用通道支持资源级权限，即表示针对支持资源级权限的操作，控制何时允许用户执行操作或是允许用户使用的特定资源。

可授权策略介绍

在访问管理（Cloud Access Management，CAM）中可授权的资源类型如下：

资源类型	授权策略中的资源描述方法
专用通道相关操作	qcs::dc::uin/${Uin}/dcx/${DirectConnectTunnelId}

所有 `${Uin}` 为资源拥有者的 AccountId，或者“*”。
所有 `${DirectConnectTunnelId}` 为专用通道 ID，或者“*”。

专用通道相关操作

接口名称	接口描述	六段式定义
CreatePublicDirectConnectTunnel	创建互联网专用通道	qcs::dc::uin/:dcx/*
DescribeDirectConnectTunnels	获取专用通道列表	qcs::dc::uin/:dcx/*
AcceptDirectConnectTunnel	接受专用通道	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
DeleteDirectConnectTunnel	删除专用通道	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
ModifyDirectConnectTunnelAttribute	修改专用通道属性	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
CreateDirectConnectTunnel	创建专用通道	qcs::dc::uin/:dcx/*
RejectDirectConnectTunnel	拒绝专用通道申请	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
DescribePublicDirectConnectTunnelRoutes	查询互联网通道路由表	qcs::dc::uin/:dcx/${DirectConnectTunnelId}

DescribeDirectConnectTunnelExtra	查询专用通道扩展信息	qcs::dc::uin/:dcx/${DirectConnectTunnelId}
ModifyDirectConnectTunnelExtra	修改专用通道扩展信息	qcs::dc::uin/:dcx/${DirectConnectTunnelId}

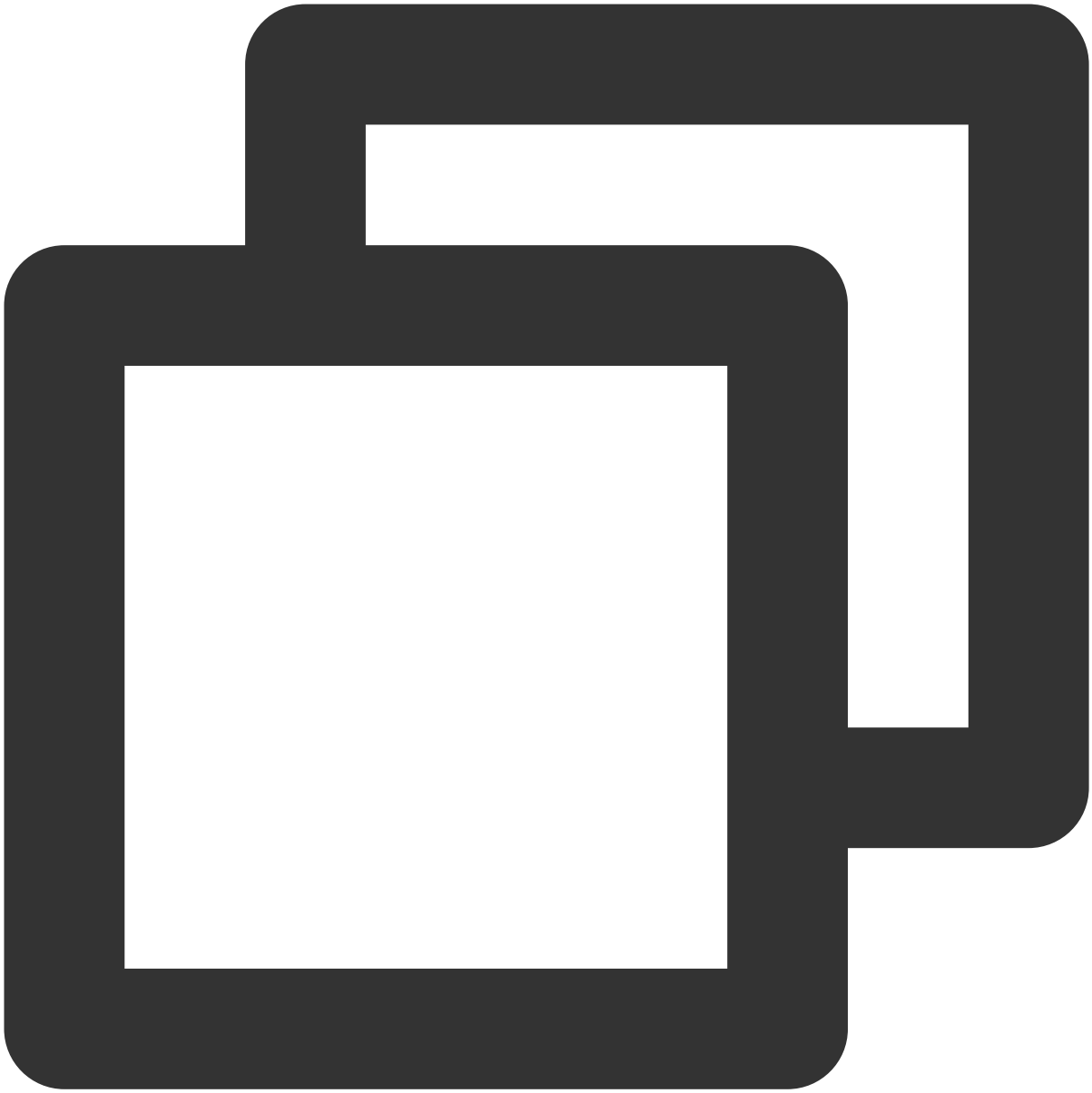
授权策略语法

最近更新时间：2024-01-13 16:02:36

本文列出了 CAM 授权策略语法及使用示例。

CAM 策略语法

CAM 策略语法如下：



```
{
        "version":"2.0",
        "statement":
        [
            {
                "effect":"effect",
                "action":["action"],
                "resource":["resource"],
                 "condition": {"key":{"value"}}
            }
        ]
```

```
}
```

version：版本，必填项，目前仅允许值为"2.0"。

语句 statement 是用来描述一条或多条权限的详细信息。该元素包括 effect、action、resource，condition 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。

1.1 **effect**：影响，必填项，描述声明产生的结果是“允许”还是显示“拒绝”。包括 allow （允许）和 deny （显式拒绝）两种情况。

1.2 **action**：操作，必填项，用来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 permit 前缀描述）。

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

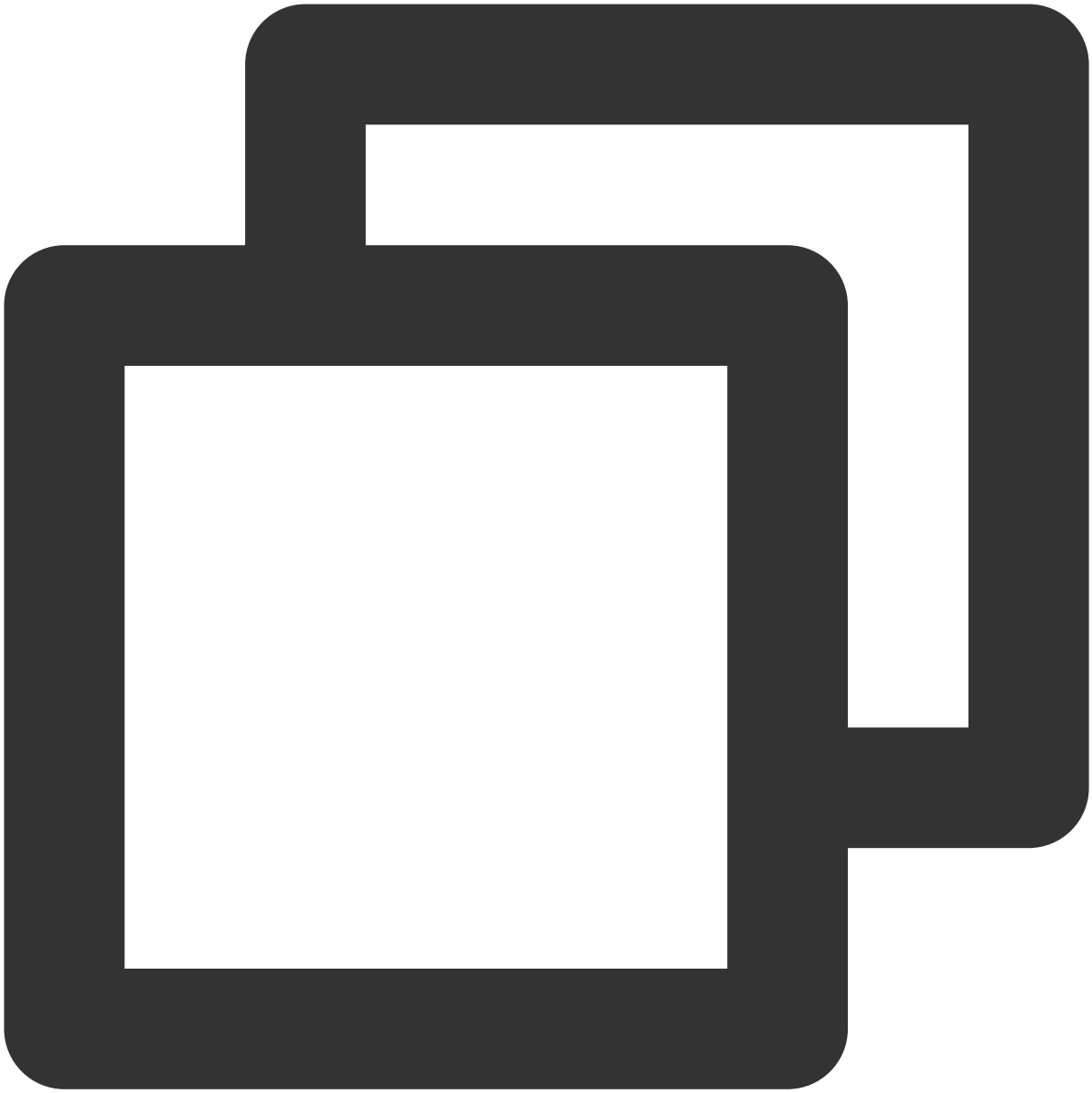
1.4 **condition**：生效条件，非必填项，描述策略生效的约束条件。条件包括操作符、操作键和操作值组成。条件值可包括时间、IP 地址等信息。有些服务允许您在条件中指定其他值。

策略示例

若授权专用通道的全读写策略，示例如下：

授权子账户的专用通道的完全管理权限（创建、管理等全部操作）。

策略名称：QcloudDCFullAccess。



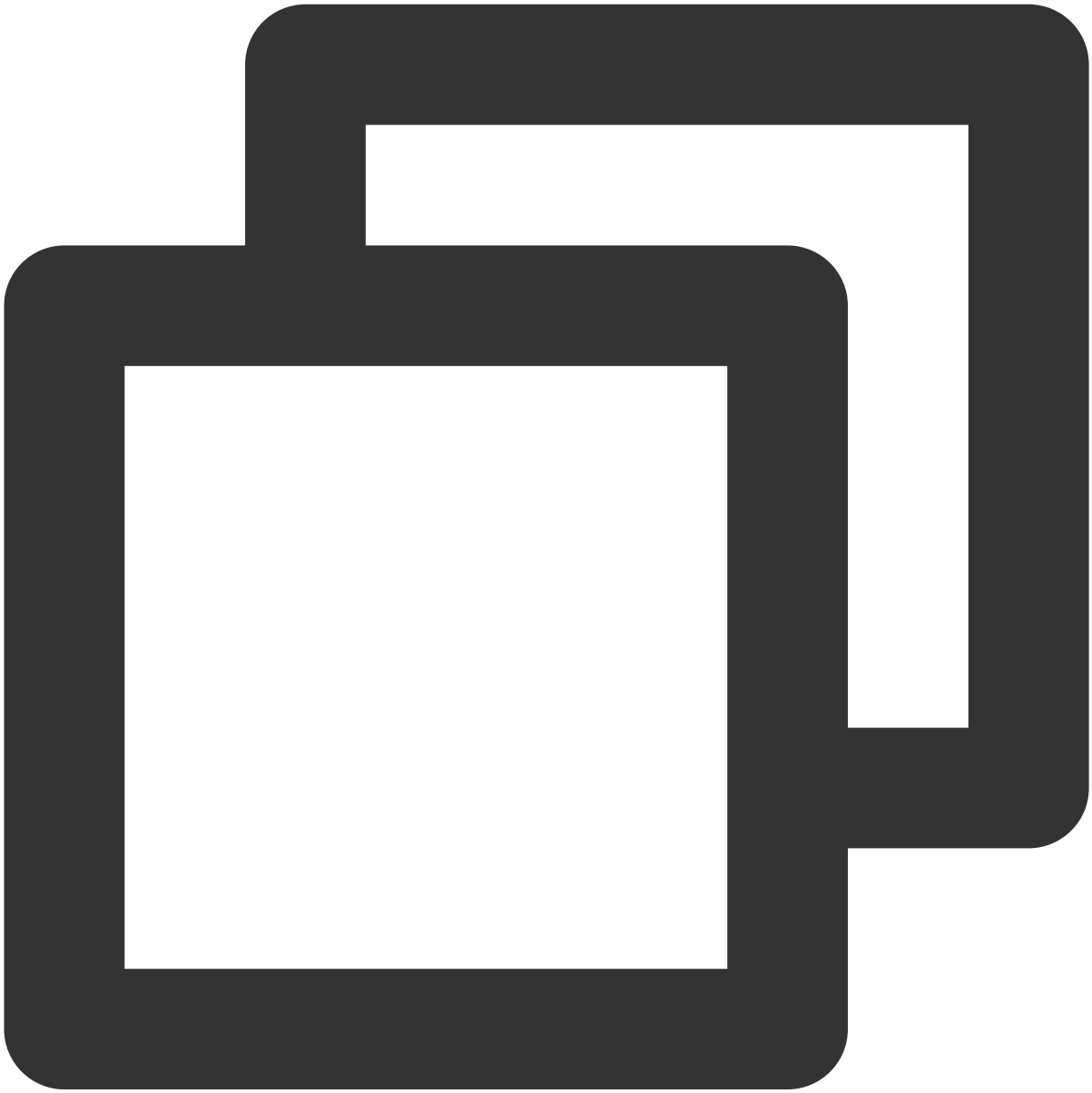
```
{
"version": "2.0",
"statement": [
    {
        "action": [
            "dc:*"
        ],
        "resource": "*",
        "effect": "allow"
    }
]
```

```
}
```

若授权专用通道的只读权限，示例如下：

授权子账户专用通道的只读访问权限，即可以查看专用通道所有资源的权限，但子账户无法创建、更新或删除资源。

策略名称：QcloudDCReadOnlyAccess。



```
{
"version": "2.0",
"statement": [
    {
```

```
        "action": [
            "dc:Describe*",
            "dc:Is*"
        ],
        "resource": "*",
        "effect": "allow"
    }
]
```