移动解析 HTTPDNS

访问管理

产品文档

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 腾讯云版权所有

本文档著作权归腾讯云单独所有，未经腾讯云事先书面许可，任何主体不得以任何形式复制、修改、抄袭、传播全部或部分本文档内容。

【商标声明】

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。

【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默示的承诺或保证。

文档目录

访问管理
- 访问控制概述
- 访问控制策略示例

版权所有：腾讯云计算（北京）有限责任公司

访问管理
访问控制概述

最近更新时间：2022-06-22 15:22:45

访问控制（CAM）用于管理腾讯云账户下资源访问权限，通过 CAM，您可以根据身份管理和策略管理控制哪些子账号有哪些资源的操作权限。

例如，您的账户下有多个证书部署在不同项目中，为了加强权限控制，您需要对资源进行授权，您可以给项目 A 的管理员绑定一个授权策略，该策略规定：只有该管理员可操作项目 A 下的负载均衡资源。

如果您不需要对子账户进行 HTTPDNS 证书相关资源的访问控制，您可以跳过此章节。

> 注意：
> 目前仅有控制台支持 CAM 访问授权。

CAM 基本概念

主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/用户组，允许/拒绝，条件]**维度。

1. **账户**

- **主账号**：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**是指用户登录名和密码，**访问证书**是指云 API 密钥（SecretId 和 SecretKey）。

2. **资源与权限**

- **资源**：资源是云服务中被操作的对象，例如一个云服务器实例，COS 存储桶，VPC 实例等。
- **权限**：权限是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**：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/用户组完成授权。

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	策略管理
了解策略的基本结构	策略语法
了解还有哪些产品支持 CAM	支持 CAM 的云服务列表

版权所有：腾讯云计算（北京）有限责任公司

访问控制策略示例

最近更新时间：2022-06-22 15:22:45

HTTPDNS 的全读写策略

- 为子用户或协作者授权完全读写权限（创建、管理等全部操作）。
- 策略名称：QcloudHTTPDNSFullAccess

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

HTTPDNS 的只读策略

- 授权一个子用户只读访问 HTTPDNS 的权限（即可以查看所有 HTTPDNS 下面所有资源的权限），但用户无法创建、更新或删除它们。 在控制台，操作一个资源的前提是可以查看该资源，所以建议您为子账户开通 HTTPDNS 全读权限。
- 策略名称： QcloudHTTPDNSReadOnlyAccess

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