

# 私有域解析 Private DNS

## 访问管理



腾讯云

## 【 版权声明 】

©2013–2024 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 】



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

### 访问管理

访问控制概述

可授权资源类型

访问控制策略示例

# 访问管理

## 访问控制概述

最近更新时间：2024-04-24 10:20:11

**访问管理（Cloud Access Management, CAM）**可以帮助您安全、便捷地管理对腾讯云服务和资源的访问。您可以使用 CAM 创建子用户、用户组和角色，并通过策略控制其访问范围。CAM 支持用户和角色 SSO 能力，您可以根据具体管理场景针对性设置企业内用户和腾讯云的互通能力。

### CAM 基本概念

主账户通过给予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则。**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	<a href="#">策略管理</a>
了解策略的基本结构	<a href="#">策略语法</a>
了解还有哪些产品支持 CAM	<a href="#">支持 CAM 的云服务列表</a>

# 可授权资源类型

最近更新时间：2023-08-29 14:42:43

资源级权限指的是能够指定用户对哪些资源具有执行操作的能力。Private DNS 大部分接口支持资源级授权，允许用户对特定私有域进行操作。

## Private DNS 在访问管理中支持的授权类型

资源类型	资源六段式格式
私有域	<code>qcs::privatedns::\$accountid:zone/\$zoneid</code>

其中：

- 所有 `$accountid` 应为资源拥有者的 AccountId，或者留空。
- 所有 `$zoneid` 应为特定私有域的 ID。如果授权所有的私有域，可以填写 “\*”。

## Private DNS 在访问管理支持授权的操作

API 操作	API 说明	资源路径
DescribeUserConfig	获取当前用户配置	*
DescribeAuditLog	获取操作日志列表	<code>qcs::privatedns::zone/\${Zoneid}</code>
DescribePrivateZoneList	获取私有域列表	<code>qcs::privatedns::zone/\${Zoneid}</code>
ModifyPrivateZoneVpc	修改私有域关联的 VPC	<code>qcs::privatedns::zone/\${Zoneid}</code>
DeletePrivateZoneRecord	删除私有域解析记录	<code>qcs::privatedns::zone/\${Zoneid}</code>
ModifyPrivateZoneRecord	修改私有域解析记录	<code>qcs::privatedns::zone/\${Zoneid}</code>
DeletePrivateZone	删除私有域	<code>qcs::privatedns::zone/\${Zoneid}</code>
DescribeRequestData	获取私有域解析请求量	<code>qcs::privatedns::zone/\${Zoneid}</code>
DescribePrivateZone	获取私有域信息	<code>qcs::privatedns::zone/\${Zoneid}</code>
DescribePrivateZoneRecordList	获取私有域记录列表	<code>qcs::privatedns::zone/\${Zoneid}</code>
ModifyPrivateZone	修改私有域	<code>qcs::privatedns::zone/\${Zoneid}</code>

CreatePrivateZoneRecord	添加私有域解析记录	qcs::privatedns::zone/\${ZoneId}
DescribeDashboard	获取私有域解析概览	*
DescribePrivateZoneService	查询私有域解析开通状态	*
SubscribePrivateZoneService	开通私有域解析	*
ModifyUserConfig	修改当前用户配置	*
CreatePrivateZone	创建私有域	*

# 访问控制策略示例

最近更新时间：2023-08-29 14:42:43

## 操作场景

访问控制（CAM）用于管理腾讯云账户下资源访问权限，通过 CAM，您可以通过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。本文档指导您如何使用控制台的特定部分的策略。

## 操作示例

### Private DNS 的全读写策略

如果您希望用户拥有创建和管理私有域解析 Private DNS 的全部权限，您可以为该用户配置策略名称为：**QcloudPrivateDNSFullAccess**。

请参见 [授权管理](#)，将预设策略 **QcloudPrivateDNSFullAccess** 授权给用户。

策略语法如下：

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

### Private DNS 的只读策略

如果您希望用户只拥有查询 Private DNS 私有域相关的权限，但不允许该用户拥有创建、删除等操作的权限，您可以对该用户配置策略名称为：**QcloudPrivateDNSReadOnlyAccess**。

请参见 [授权管理](#)，将预设策略 **QcloudPrivateDNSReadOnlyAccess** 授权给用户。

策略语法如下：

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

```
    "privatedns:Describe*",
  ],
  "resource": "*",
  "effect": "allow"
}
]
```