SD-WAN 接入服务

访问管理

腾讯云

版权所有：腾讯云计算（北京）有限责任公司

【版权声明】

©2013-2024 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】

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

访问管理
- 访问管理概述
- 可授权策略类型
- 授权策略语法

访问管理
访问管理概述

最近更新时间：2024-09-12 16:53:41

若您需使用 SD-WAN 接入服务、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。

为解决上述问题，您可以通过子账号实现由不同人管理不同服务。默认情况下，子账号没有使用 SD-WAN 接入服务的权利或者 SD-WAN 接入服务相关资源的权限。因此，我们需要创建相关策略允许子账号使用他们所需要的资源或权限。

> **说明：**
> 若您不需要对子账户进行 SD-WAN 接入服务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。

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。
您最初创建的腾讯云主账号，拥有整个账号全部腾讯云服务和资源的完全访问权限，建议您保护好主账号的凭证信息，日常使用子用户或角色进行访问，并开启多因素校验和定时轮换密钥。
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 。

CAM 概念

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：2024-09-12 16:53:42

资源级权限指能够指定用户对哪些资源具有执行操作的能力。SD-WAN 接入服务支持资源级权限，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。
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
Edge 实例相关	qcs::vpc:$region:$account:edge/$edgeId
Edge 防火墙相关	qcs::vpc:$region:$account:firewall/$firewallId

- 所有 `$region` 应为某个 region 的 ID，可以为空。
- 所有 `$account` 应为资源拥有者的 AccountId，或者“*”。
- 所有 `$edgeId` 应为某个 Edge 设备的 ID，或者“*”。
- 所有 `$firewallId` 应为某个防火墙的 ID，或者“*”。

Edge 实例相关

API 操作	资源描述	接口说明
CreateEdge	创建 Edge设备	qcs::vpc:$region:$account:edge/*
DescribeEdges	查询 Edge设备列表	qcs::vpc:$region:$account:edge/*
DowngradeEdgeVersion	降级 Edge 设备版本	qcs::vpc:$region:$account:edge/$edgeId
UpgradeEdgeVersion	升级 Edge 设备版本	qcs::vpc:$region:$account:edge/$edgeId
ResetEdgePassword	设置 Edge 设备本地密码	qcs::vpc:$region:$account:edge/$edgeId
AttachEdgeSN	用户关联 Edge 设备的 SN 码	qcs::vpc:$region:$account:edge/$edgeId
DetachEdgeSN	用户解关联 Edge 设备的 SN 码	qcs::vpc:$region:$account:edge/$edgeId
DescribeEdgeSN	获取可用的设备 SN 号	qcs::vpc:$region:$account:edge/*
DescribeEdgeRoutes	查询 Edge 设备本地路由	qcs::vpc:$region:$account:edge/*

版权所有：腾讯云计算（北京）有限责任公司

CreateEdgeRoute	创建 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
DeleteEdgeRoutes	删除 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
ModifyEdgeRoute	修改 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
EnableEdgeRoutes	启用 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
DisableEdgeRoutes	禁用 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
AdvertiseEdgeRoutes	宣告 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
UndoAdvertiseEdgeRoutes	撤销宣告 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
RecoverEdgeRoutes	恢复删除状态的 Edge 路由	qcs::vpc:$region:$account:edge/$edgeId
CreateEdgeVport	创建逻辑端口	qcs::vpc:$region:$account:edge/$edgeId
RecoverEdgeVport	恢复删除状态的逻辑端口	qcs::vpc:$region:$account:edge/$edgeId
DeleteEdgeVport	删除逻辑端口	qcs::vpc:$region:$account:edge/$edgeId
ModifyEdgeVport	修改逻辑端口	qcs::vpc:$region:$account:edge/$edgeId
DescribeEdgeVports	查询逻辑端口	qcs::vpc:$region:$account:edge/*

Edge 防火墙相关

API 操作	资源描述	接口说明
CreateEdgeFirewall	创建防火墙实例	qcs::vpc:$region:$account:firewall/*
DescribeEdgeFirewalls	查询防火墙实例列表	qcs::vpc:$region:$account:firewall/*

ModifyEdgeFirewall	修改防火墙实例	qcs::vpc:$region:$account:firewall/$firewallId
DeleteEdgeFirewall	删除防火墙实例	qcs::vpc:$region:$account:firewall/$firewallId
AttachEdgeFirewall	用户关联 Edge 设备到防火墙	qcs::vpc:$region:$account:firewall/$firewallId
DetachEdgeFirewall	用户从防火墙解关联 Edge 设备	qcs::vpc:$region:$account:firewall/$firewallId
DescribeFirewallAttachedEdges	查询关联到防火墙的 Edge 设备	qcs::vpc:$region:$account:firewall/$firewallId
DescribeFirewallRules	查询防火墙规则	qcs::vpc:$region:$account:firewall/$firewallId
CreateFirewallRules	创建防火墙规则	qcs::vpc:$region:$account:firewall/$firewallId
DeleteFirewallRules	删除防火墙规则	qcs::vpc:$region:$account:firewall/$firewallId
ModifyFirewallRules	修改防火墙出站和入站规则	qcs::vpc:$region:$account:firewall/$firewallId
ReplaceFirewallRule	替换单条防火墙规则	qcs::vpc:$region:$account:firewall/$firewallId

版权所有：腾讯云计算（北京）有限责任公司

授权策略语法

最近更新时间：2024-09-12 16:53:42

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 **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 permid 前缀描述）。
  1.2 **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。
  1.3 **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。
  1.4 **effect**：影响，必填项，描述声明产生的结果是“允许”还是“显式拒绝”。包括 allow（允许）和 deny（显式拒绝）两种情况。

策略示例

- 若授权 SD-WAN 接入服务的全读写策略，示例如下：
  - 授权子账户的 SD-WAN 接入服务的完全管理权限（创建、管理等全部操作）。
  - 策略名称：EdgeResourceFullAccess。

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

- 若授权 SD-WAN 接入服务的只读权限，示例如下：
  - 授权子账户 SD-WAN 接入服务的只读访问权限，即可以查看 SD-WAN 接入服务所有资源的权限，但子账户无法创建、更新或删除资源。
  - 策略名称：EdgeResourceReadAccess。

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