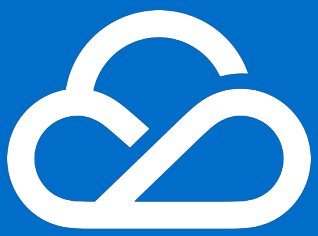
腾讯云云服务器

访问管理

产品文档



腾讯云

【版权声明】

【商标声明】

【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模式的承诺或保证。

文档目录

访问管理

概述

如果您在腾讯云中使用到了云服务器（CVM，Cloud Virtual Machine）、私有网络、数据库等服务，这些服务由不同的人管理，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。

这个时候，您就可以通过子帐号实现不同的人管理不同的服务，以避免以上的问题。默认情况下，子帐号没有使用CVM的权利或者CVM相关资源的的权限。因此，我们就需要创建策略来允许子帐号使用他们所需要的资源或者权限。

访问管理（CAM，Cloud Access Management）是腾讯云提供的一套Web服务，它主要用于帮助客户安全管理腾讯云账户下的资源的访问权限。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的时候，可以将策略与一个用户或者一组用户关联起来，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，请参照策略语法。有关CAM策略的更多相关使用信息，请参照策略。

如果您不需要对子账户进行CVM相关资源的访问管理，您可以跳过此章节。跳过这些部分并不影响您对文档中其余部分的理解和使用。

该功能目前处于灰度中，可提工单申请。

入门

CAM 策略必须授权使用一个或多个 CVM 操作或者必须拒绝使用一个或多个 CVM 操作。同时还必须指定可以用于操作的资源（可以是全部资源，某些操作也可以是部分资源），策略还可以包含操作资源所设置的条件。

CVM 部分 API 操作支持资源级权限，意味着，对于该类
API操作，您不能在使用该类操作的时候指定某个具体的资源来使用，而必须要指定全部资源来使用。

任务	链接

任务	链接
了解策略基本结构	策略语法
在策略中定义操作	CVM的操作
在策略中定义资源	CVM的资源路径
使用条件来限制策略	CVM的条件密钥
CVM支持的资源级权限	CVM支持的资源级权限
控制台示例	控制台示例

策略结构

策略语法

CAM 策略：

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

- 版本 version 是必填项，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. 操作 action 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）。该元素是必填项。
    2. 资源 resourcce 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。该元素是必填项。
    3. 生效条件 condition
       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。该元素是非必填项。
    4. 影响 effect 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。该元素是必填项。

CVM 的操作

在 CAM 策略语句中，您可以从支持 CAM 的任何服务中指定任意的 API 操作。对于 CVM，请使用以 name/cvm: 为前缀的 API 。例如： name/cvm:RunInstances 或者 name/cvm:ResetInstancesPassword 。如果您要在单个语句中指定多个操作的时候，请使用逗号将它们隔开，如下所示:

"action":["name/cvm:action1","name/cvm:action2"]

您也可以使用通配符指定多项操作。例如，您可以指定名字以单词" Describe "开头的所有操作，如下所示：

"action":["name/cvm:Describe*"]

如果您要指定 CVM 中所有操作，请使用 * 通配符，如下所示：

"action"：["name/cvm:*"]

CVM 的资源路径

每个 CAM 策略语句都有适用于自己的资源。
资源路径的一般形式如下：

qcs:project_id:service_type:region:account:resource

project_id：描述项目信息，仅为了兼容CAM早期逻辑，无需填写。
service_type：产品简称，如 CVM。

region：地域信息，如 bj。
account：资源拥有者的根帐号信息，如 uin/164256472。
resource：各产品的具体资源详情，如 instance/instance_id1 或者 instance/*。

例如，您可以使用特定实例 (i-15931881scv4) 在语句中指定它，如下所示：

"resource":["qcs::cvm:bj:uin/164256472:instance/i-15931881scv4"]

您还可以使用 * 通配符指定属于特定账户的所有实例，如下所示：

"resource":["qcs::cvm:bj:uin/164256472:instance/*"]

您要指定所有资源，或者如果特定 API 操作不支持 资源级权限，请在 Resource 元素中使用 *
通配符，如下所示：

"resource": ["*"]

如果您想要在在一条指令中同时指定多个资源，请使用逗号将它们隔开，如下所示为指定两个资源的例子：

"resource":["resource1","resource2"]

下表描述了 CVM 能够使用的资源和对应的资源描述方法。

table th:nth-of-type(1){
width:250px;
}
table th:nth-of-type(2){
width:500px;
}

在下表中，$为前缀的单词均为代称。

- 其中，project指代的是项目ID。
- 其中，region指代的是地域。
- 其中，account指代的是账户ID。

资源	授权策略中的资源描述方法
实例	qcs::cvm:$region:$account:instance/$instanceId
密钥	qcs::cvm:$region:$account:keypair/$keyId
VPC	qcs::vpc:$region:$account:vpc/$vpcId
子网	qcs::vpc:$region:$account:vpc/$vpcId
系统磁盘	qcs::cvm:$region:$account:systemdisk/*
镜像	qcs::cvm:$region:$account:image/*
子网	qcs::vpc:$region:$account:subnet/$subnetId
数据盘	qcs::cvm:$region:$account:datadisk/*
安全组	qcs::cvm:$region:$account:sg/$sgId
EIP	qcs::cvm:$region:$account:eip/*

CVM 的条件密钥

在策略语句中，您可以选择性指定控制策略生效时间的条件。每个条件都包含一个或多个密钥值对。条件密钥不区分大小写。

- 如果您指定了多个条件或在单一条件中指定了多个密钥，我们将通过逻辑 AND 操作对其进行评估。
- 如果您在单一条件中指定了一个具有多个值的密钥，我们将通过逻辑 OR 操作对其进行评估。必须匹配所有条件才能授予权限。

下表描述了 CVM 用于特定于服务的条件键。

条件键	参考类型	键值对
cvm:instance_type	String	cvm:instance_type=

条件键	参考类型		键值对	
				instance_type • 其中 instance_type 指代的是实例类型（例如 S1.SMALL1）。
		cvm:image_type	String	cvm:image_type=image_type • 其中 image_type

条件键	参考类型		键值对	
				指代的是镜像类型（例如 IMAGE_PUBLIC）
		vpc:region	String	vpc:region=region • 其中 region 指代的是地域（例如 ap-guangzhou）

条件键	参考类型		
	cvm:disk_size	Integer	cvm:disk_size= disk_size • 其中 disk_size 指代的是磁盘大小（例如500）
	cvm:disk_type	String	cvm_disk_type= disk_type • 其中 disk_type 指代的是磁盘类型

条件键	参考类型		键值对	
				（例如 CLOUD_BASIC）
		cvm:region	String	cvm:region=region • 其中 region 指代的是地域（例如 ap-guangzhou）

支持的资源级权限

资源级权限指的是能够指定允许用户对哪些资源具有执行操作的能力。 CVM 部分支持资源级权限，这意味着对于某些 CVM 操作，您可以控制何时允许用户执行操作(基于必须满足的条件)或是允许用户使用的特定资源。下表将向您介绍一下， CVM 可授权的资源类型。

CAM 中可授权的资源类型：

资源类型	授权策略中的资源描述方法
云服务器实例相关	qcs::cvm:$region::instance/*
云服务器密钥相关	qcs::cvm:$region::keypair/*
云服务器镜像相关	qcs:t:cvm:$region:$account:image/*

下表将介绍当前支持资源级权限的 CVM （ Cloud Virtual Machine,云服务器） API 操作，以及每个操作支持的资源和条件密钥。指定资源路径的时候，您可以在路径中使用 * 通配符。

> 注意：
> 如果某一个 CVM API 操作在下表中没有列出，则它不支持资源级权限。如果 CVM API 操作不支持资源级权限，那么您还是可以向用户授予使用该操作的权限，但是必须为策略语句的资源元素指定 * 。

云服务器实例相关：

API 操作	资源路径	条件密钥
DescribeInstanceInternetBandwidthConfigs	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ModifyInstanceInternetChargeType	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type

API 操作	资源路径	条件密钥
ModifyInstancesAttribute	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ModifyInstancesProject	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ModifyInstancesRenewFlag	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RebootInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RenewInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResetInstance	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:image/*	cvm:region cvm:zone cvm:instance_type

API 操作	资源路径	条件密钥
	qcs::cvm:$region:$account:image/$imageId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId qcs:::cvm:$region:$account:systemdisk/*	
ResetInstancesInternetMaxBandwidth	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResetInstancesPassword	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResetInstancesType	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
ResizeInstanceDisks	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
RunInstances	qcs::cvm:$region:$account:instance/*	cvm:region cvm:zone

API 操作	资源路径	条件密钥
	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId qcs::cvm:$region:$account:sg/* qcs::cvm:$region:$account:sg/$sgId qcs::vpc:$region:$account:subnet/* qcs::vpc:$region:$account:subnet/$subnetId qcs:::cvm:$region:$account:systemdisk/* qcs::cvm:$region:$account:datadisk/* qcs::vpc:$region:$account:vpc/* qcs::vpc:$region:$account:vpc/$vpcId	cvm:instance_type

API 操作	资源路径	条件密钥
StartInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
StopInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type
TerminateInstances	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId	cvm:region cvm:zone cvm:instance_type

云服务器密钥相关：

API 操作	资源路径	条件密钥
AssociateInstancesKeyPairs	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-
CreateKeyPair	qcs::cvm:$region:$account:keypair/*	-
DeleteKeyPairs	qcs::cvm:$region:$account:keypair/*	-

API 操作	资源路径	条件密钥
	qcs::cvm:$region:$account:keypair/$keyId	
DescribeKeyPairs	qcs::cvm:$region:$account:keypair/*	-
DescribeKeyPairsAttribute	qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-
DisassociateInstancesKeyPairs	qcs::cvm:$region:$account:instance/* qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-
ImportKeyPair	qcs::cvm:$region:$account:keypair/*	-
ModifyKeyPairAttribute	qcs::cvm:$region:$account:keypair/* qcs::cvm:$region:$account:keypair/$keyId	-

云服务器镜像相关：

API 操作	资源路径	条件密钥
CreateImage	qcs::cvm:$region:$account:instance/*	cvm:region

API 操作	资源路径	条件密钥
	qcs::cvm:$region:$account:instance/$instanceId qcs::cvm:$region:$account:image/*	
DeleteImages	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId	cvm:region
DescribeImages	qcs::cvm:$region:$account:image/*	cvm:region
DescribeImagesAttribute	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId	cvm:region
DescribeImageSharePermission	qcs::cvm:$region:$account:image/*	cvm:region
ModifyImageAttribute	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId	cvm:region
ModifyImageSharePermission	qcs::cvm:$region:$account:image/* qcs::cvm:$region:$account:image/$imageId	cvm:region
SyncImages	qcs::cvm:$region:$account:image/*	cvm:region

API 操作	资源路径	条件密钥
	qcs::cvm:$region:$account:image/$imageId	

控制台示例

CVM 访问管理策略示例

您可以通过使用 CAM（Cloud Access Management，访问管理）策略让用户拥有在 CVM（Cloud Virtual Machine，云服务器）控制台中查看和使用特定资源的权限。该部分的示例能够使用户使用控制台的特定部分的策略。

CVM 的全读写策略

如果您想让用户拥有创建和管理 CVM 实例的权限，您可以对该用户使用名称为：QcloudCVMFullAccess 的策略。
您可以进入 策略管理界面，并在右边的全部服务中选择【云服务器】，就可以在图中位置找到该策略。

策略语法如下：

```
{
  "version": "2.0",
  "statement": [
  {
  "action": [
  "name/cvm:*"
  ],
  "resource": "*",
```

"effect": "allow"
},
{
"action": [
"name/vpc:*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/clb:*"
],
"resource": "*",
"effect": "allow"
},
{
"effect": "allow",
"action": "name/monitor:*",
"resource": "*"
}
]
}

以上策略是通过让用户分别对 CVM、VPC（Virtual Private Cloud）、CLB（Cloud Load Balance）和 MONITIOR 中所有资源都具有操作的权限来达到目的。

CVM 的只读策略

如果您只想让用户拥有查询 CVM 实例的权限，但是不具有创建、删除、开关机的权限，您可以对该用户使用名称为：QcloudCVMInnerReadOnlyAccess 的策略。

建议：请配置 CVM 的只读策略。

您可以进入 策略管理界面，并在右边的全部服务中选择【云服务器】，就可以在图中位置找到该策略。

策略语法如下：

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

以上策略是通过让用户分别对如下操作 CVM 中所有以单词" Describe "开头的所有操作和所有以单词" Inquiry "开头的所有操作具有操作的权限来达到目的。

CVM 相关资源的只读策略

如果您想要让用户只拥有查询 CVM 实例及相关资源（VPC 、CLB ）的权限，但不允许该用户拥有创建、删除、开关机等操作的权限，您可以对该用户使用名称为：QcloudCVMReadOnlyAccess 的策略。
您可以进入 策略管理界面,并在右边的全部服务中选择【云服务器】，就可以在图中位置找到该策略。

策略语法如下：

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

```
"name/vpc:Describe*",
"name/vpc:Inquiry*",
"name/vpc:Get*"
],
"resource": "*",
"effect": "allow"
},
{
"action": [
"name/clb:Describe*"
],
"resource": "*",
"effect": "allow"
},
{
"effect": "allow",
"action": "name/monitor:*",
"resource": "*"
}
]
}
```

以上策略是通过让用户分别对如下操作具有操作权限来达到目的：

- CVM 中所有以单词" Describe "开头的所有操作和所有以单词" Inquiry "开头的所有操作。
- VPC 中所有以单词" Describe "开头的所有操作、所有以单词" Inquiry "开头的所有操作和所有以单词" Get "开头的所有操作。
- CLB 中所有以单词" Describe "开头的所有操作。
- Monitor 中所有的的操作。

弹性云盘的相关策略

如果您想要让用户能够查看 CVM 控制台中的云硬盘信息，创建云硬盘，使用云硬盘，可将以下操作添加到您

策略中，然后将该策略关联到该用户。

- CreateCbsStorages ：创建云硬盘。
- AttachCbsStorages ：挂载指定的弹性云盘到指定的云主机上。
- DetachCbsStorages ：解挂指定的弹性云盘。
- ModifyCbsStorageAttributes ：修改指定云硬盘的名称或项目 ID。
- DescribeCbsStorages ：查询云硬盘的详细信息性。
- DescribeInstancesCbsNum ：查询云主机已挂载的弹性云盘数量和可挂载的弹性云盘的总数。
- RenewCbsStorage ：续费指定的弹性云盘。
- ResizeCbsStorage ：扩容指定的弹性云盘。

以下策略不允许用户修改云硬盘属性。

```
{
  "version": "2.0",
  "statement": [
  {
  "action": [
  "name/cvm:ModifyCbsStorageAttributes",
  ],
  "resource": [
  "qcs::cvm::uin/1410643447:*"
  ],
  "effect": "deny"
  }
  ]
}
```

安全组的相关策略

如果您想要让用户能够查看 CVM
控制台中的安全组，并且使用安全组，可将以下操作添加到您策略中，然后将该策略关联到该用户。

- DeleteSecurityGroup ：删除安全组。
- ModifySecurityGroupPolicys ：替换安全组所有策略。
- ModifySingleSecurityGroupPolicy ：修改安全组单条策略。
- CreateSecurityGroupPolicy ：创建安全组策略。
- DeleteSecurityGroupPolicy ：删除安全组策略。
- ModifySecurityGroupAttributes ：修改安全组属性。

以下策略允许用户在 CVM 控制台中具有创建，删除安全组的权限。

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

以下策略可以让用户在 CVM 控制台中具有创建、删除修改安全组策略的权限。

```
{
  "version": "2.0",
  "statement": [
  {
  "action": [
  "name/cvm:ModifySecurityGroupPolicys",
  "name/cvm:ModifySingleSecurityGroupPolicy",
  "name/cvm:CreateSecurityGroupPolicy",
```

```
  "name/cvm:DeleteSecurityGroupPolicy"
  ],
  "resource": "*",
  "effect": "allow"
  }
  ]
}
```

弹性 IP 地址的相关策略

如果您想要让用户能够查看 CVM 控制台中的弹性 IP 地址，并且使用弹性 IP 地址，可将以下操作添加到您策略中，然后将该策略关联到该用户。

- AllocateAddresses ：分配地址给 VPC 或者 CVM。
- AssociateAddress ：将弹性 IP 地址与实例或者与网络接口关联。
- DescribeAddresses ：查看 CVM 控制台中的弹性 IP 地址。
- DisassociateAddress ：取消弹性 IP 地址与实例或者与网络接口关联。
- ModifyAddressAttribute ：修改弹性 IP 地址的属性。
- ReleaseAddresses ：解除弹性 IP 地址。

以下策略允许用户查看弹性 IP 地址并可以将其分配给实例并与之相关联。用户不可以修改弹性 IP 地址的属性、取消弹性 IP 地址的关联或释放弹性 IP 地址。

```
{
  "version": "2.0",
  "statement": [
  {
  "action": [
  "name/cvm:DescribeAddresses",
  "name/cvm:AllocateAddresses",
  "name/cvm:AssociateAddress"
  ],
  "resource": "*",
```

```
  "effect": "allow"
  }
  ]
}
```

授权用户拥有特定 CVM 的操作权限策略

如果您想要授权用户拥有特定 CVM 操作权限，可将以下策略关联到该用户。
以下策略允许用户拥有对 id 为 ins-1,广州地域的 CVM 机器的操作权限。

```
{
  "version": "2.0",
  "statement": [
  {
  "action": "cvm:*",
  "resource": "qcs::cvm:gz::instance/ins-1",
  "effect": "allow"
  }
  ]
}
```

授权用户拥有特定地域 CVM 的操作权限策略

如果您想要授权用户拥有特定地域的 CVM 的操作权限，可将以下策略关联到该用户。
以下策略允许用户拥有对广州地域的 CVM 机器的操作权限。

```
{
  "version": "2.0",
  "statement": [
  {
  "action": "cvm:*",
  "resource": "qcs::cvm:gz::*",
```

```
  "effect": "allow"
  }
  ]
}
```

自定义策略

如果您觉得预设策略不能满足您所想要的要求，您也可以创建自定义策略。
自定义的策略语法如下：

```
{
  "version": "2.0",
  "statement": [
  {
  "action": [
  "Action"
  ],
  "resource": "Resource",
  "effect": "Effect"
  }
  ]
}
```

Action中换成您要进行允许或拒绝的操作。
Resource中换成您要授权的具体资源。
Effect中换成允许或者拒绝。