

# 云服务器

## 安全与合规

### 产品文档



**【版权声明】**

©2013–2026 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】**

及其他腾讯云服务相关的商标均为腾讯集团下的相关公司主体所有。另外，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

## 安全与合规

### 访问管理

访问管理概述

可授权的资源类型

授权策略语法

支持访问管理的 CVM API 接口

访问管理示例

### 网络

网络概述

网络环境

内网服务

公网服务

弹性公网 IP

弹性网卡

配置巨型帧能力

主机安全

DDoS 基础防护

# 安全与合规

## 访问管理

### 访问管理概述

最近更新时间：2024-01-08 09:12:28

如果您在腾讯云中使用到了云服务器（Cloud Virtual Machine, CVM）、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，您就可以通过子账号实现不同的人管理不同的服务，来规避以上的问题。默认情况下，子账号没有使用 CVM 的权利或者 CVM 相关资源的权限。因此，我们就需要创建策略来允许子账号使用他们所需要的资源或权限。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](#)。

若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。跳过这些部分不会影响您对文档中其余部分的理解和使用。

## 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 操作不支持资源级权限，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
了解策略基本结构	<a href="#">策略语法</a>
在策略中定义操作	<a href="#">CVM 的操作</a>
在策略中定义资源	<a href="#">CVM 的资源路径</a>
使用条件来限制策略	<a href="#">CVM 的条件密钥</a>
CVM 支持的资源级权限	<a href="#">CVM 支持的资源级权限</a>
控制台示例	<a href="#">控制台示例</a>



# 可授权的资源类型

最近更新时间：2024-01-08 09:12:28

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。云服务器（Cloud Virtual Machine, CVM）部分支持资源级权限，即表示针对支持资源级权限的 CVM 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。例如，您 [授权用户拥有广州地域的 CVM 操作权限](#)。

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
<a href="#">云服务器实例相关</a>	<code>qcs::cvm:\$region::instance/*</code>
<a href="#">云服务器密钥相关</a>	<code>qcs::cvm:\$region::keypair/*</code>
<a href="#">云服务器镜像相关</a>	<code>qcs::cvm:\$region:\$account:image/*</code>

[云服务器实例相关](#)、[云服务器密钥相关](#) 和 [云服务器镜像相关](#) 分别介绍了当前支持资源级权限的 CVM API 操作，以及每个操作支持的资源和条件密钥。**设置资源路径时**，您需要将 `$region`、`$account` 等变量参数修改为您实际的参数信息，同时您也可以使用 `*` 通配符。相关操作示例可参见 [访问管理示例](#)。

## 说明：

表中未列出的 CVM API 操作即表示该 CVM API 操作不支持资源级权限。针对不支持资源级权限的 CVM API 操作，您仍可以向用户授予使用该操作的权限，但是策略语句的资源元素必须指定为 `*`。

## 云服务器实例相关

API 操作	资源路径	条件密钥
<code>DescribeInstanceInternetBandwidthConfigs</code>	<code>qcs::cvm:\$region:\$account:instance/*</code> <code>qcs::cvm:\$region:\$account:instance/\$instanceId</code>	<code>cvm:region</code> <code>cvm:zone</code> <code>cvm:instance_type</code>
<code>ModifyInstanceInternetChargeType</code>	<code>qcs::cvm:\$region:\$account:instance/*</code> <code>qcs::cvm:\$region:\$account:instance/\$instanceId</code>	<code>cvm:region</code> <code>cvm:zone</code> <code>cvm:instance_type</code>
<a href="#">ModifyInstancesAttribute</a>	<code>qcs::cvm:\$region:\$account:instance/*</code> <code>qcs::cvm:\$region:\$account:instance/\$instanceId</code>	<code>cvm:region</code> <code>cvm:zone</code> <code>cvm:instance_type</code>

ModifyInstancesProject	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
ModifyInstancesRenewFlag	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
RebootInstances	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
RenewInstances	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
ResetInstance	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId 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:systemdisk/*</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
ResetInstancesInternetMaxBandwidth	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
ResetInstancesPassword	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>

ResetInstancesType	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
ResizeInstanceDisks	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
RunInstances	<pre>qcs::cvm:\$region:\$account:instance/* 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</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
StartInstances	<pre>qcs::cvm:\$region:\$account:instance/* qcs::cvm:\$region:\$account:instance/\$instanceId</pre>	<pre>cvm:region cvm:zone cvm:instance_type</pre>
StopInstances	<pre>qcs::cvm:\$region:\$account:instance/*</pre>	<pre>cvm:region cvm:zone</pre>

	<code>qcs::cvm:\$region:\$account:instance/\$instanceId</code>	<code>cvm:instance_type</code>
<a href="#">TerminateInstances</a>	<code>qcs::cvm:\$region:\$account:instance/*</code> <code>qcs::cvm:\$region:\$account:instance/\$instanceId</code>	<code>cvm:region</code> <code>cvm:zone</code> <code>cvm:instance_type</code>

## 云服务器密钥相关

API 操作	资源路径	条件密钥
<a href="#">AssociateInstancesKeyPairs</a>	<code>qcs::cvm:\$region:\$account:instance/*</code> <code>qcs::cvm:\$region:\$account:instance/\$instanceId</code> <code>qcs::cvm:\$region:\$account:keypair/*</code> <code>qcs::cvm:\$region:\$account:keypair/\$keyId</code>	-
<a href="#">CreateKeyPair</a>	<code>qcs::cvm:\$region:\$account:keypair/*</code>	-
<a href="#">DeleteKeyPairs</a>	<code>qcs::cvm:\$region:\$account:keypair/*</code> <code>qcs::cvm:\$region:\$account:keypair/\$keyId</code>	-
<a href="#">DescribeKeyPairs</a>	<code>qcs::cvm:\$region:\$account:keypair/*</code>	-
<a href="#">DescribeKeyPairsAttribute</a>	<code>qcs::cvm:\$region:\$account:keypair/*</code> <code>qcs::cvm:\$region:\$account:keypair/\$keyId</code>	-
<a href="#">DisassociateInstancesKeyPairs</a>	<code>qcs::cvm:\$region:\$account:instance/*</code> <code>qcs::cvm:\$region:\$account:instance/\$instanceId</code> <code>qcs::cvm:\$region:\$account:keypair/*</code>	-

	<code>qcs::cvm:\$region:\$account:keypair/\$keyId</code>	
<a href="#">ImportKeyPair</a>	<code>qcs::cvm:\$region:\$account:keypair/*</code>	-
<a href="#">ModifyKeyPairAttribute</a>	<code>qcs::cvm:\$region:\$account:keypair/*</code> <code>qcs::cvm:\$region:\$account:keypair/\$keyId</code>	-

## 云服务器镜像相关

API 操作	资源路径	条件密钥
<a href="#">CreateImage</a>	<code>qcs::cvm:\$region:\$account:instance/*</code> <code>qcs::cvm:\$region:\$account:instance/\$instanceId</code> <code>qcs::cvm:\$region:\$account:image/*</code>	<code>cvm:region</code>
<a href="#">DeleteImages</a>	<code>qcs::cvm:\$region:\$account:image/*</code> <code>qcs::cvm:\$region:\$account:image/\$imageId</code>	<code>cvm:region</code>
<a href="#">DescribeImages</a>	<code>qcs::cvm:\$region:\$account:image/*</code>	<code>cvm:region</code>
<a href="#">DescribeImagesAttribute</a>	<code>qcs::cvm:\$region:\$account:image/*</code> <code>qcs::cvm:\$region:\$account:image/\$imageId</code>	<code>cvm:region</code>
<a href="#">DescribeImageSharePermission</a>	<code>qcs::cvm:\$region:\$account:image/*</code>	<code>cvm:region</code>
<a href="#">ModifyImageAttribute</a>	<code>qcs::cvm:\$region:\$account:image/*</code> <code>qcs::cvm:\$region:\$account:image/\$imageId</code>	<code>cvm:region</code>
<a href="#">ModifyImageSharePermission</a>	<code>qcs::cvm:\$region:\$account:image/*</code> <code>qcs::cvm:\$region:\$account:image/\$imageId</code>	<code>cvm:region</code>
<a href="#">SyncImages</a>	<code>qcs::cvm:\$region:\$account:image/*</code> <code>qcs::cvm:\$region:\$account:image/\$imageId</code>	<code>cvm:region</code>

# 授权策略语法

最近更新时间：2024-03-21 20:08:19

## 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。
  - 1.1 **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。
  - 1.2 **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 **permit** 前缀描述）。该元素是必填项。
  - 1.3 **资源 resource** 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。
  - 1.4 **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。

## 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**：资源拥有者的根账号信息，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。

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:subnet/\$subnetId
镜像	qcs::cvm:\$region:\$account:image/*
CBS	qcs::cvm:\$region:\$account:volume/\$diskId
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= instance_type • 其中 instance_type 指代的是实例类型（例如 S1.SMALL1）。

cvm:image_type	String	<p>cvm:image_type= <code>image_type</code></p> <ul style="list-style-type: none"><li>其中 <code>image_type</code> 指的是镜像类型（例如 IMAGE_PUBLIC）。</li></ul>
vpc:region	String	<p>vpc:region= <code>region</code></p> <ul style="list-style-type: none"><li>其中 <code>region</code> 指的是地域（例如 ap-guangzhou）。</li></ul>
cvm:disk_size	Integer	<p>cvm:disk_size= <code>disk_size</code></p> <ul style="list-style-type: none"><li>其中 <code>disk_size</code> 指的是磁盘大小（例如 500）。</li></ul>
cvm:disk_type	String	<p>cvm_disk_type= <code>disk_type</code></p> <ul style="list-style-type: none"><li>其中 <code>disk_type</code> 指的是磁盘类型（例如 CLOUD_BASIC）。</li></ul>
cvm:region	String	<p>cvm:region= <code>region</code></p> <ul style="list-style-type: none"><li>其中 <code>region</code> 指的是地域（例如 ap-guangzhou）。</li></ul>

# 支持访问管理的 CVM API 接口

最近更新时间：2024-01-08 09:12:28

## 基本信息

CAM 中产品名	CAM 中简称	授权粒度
云服务器	cvm	资源级

### ! 说明：

云产品的授权粒度按照粒度粗细分为服务级、操作级和资源级三个级别。

- **服务级**：定义对服务的整体是否拥有访问权限，分为允许对服务拥有全部操作权限或者拒绝对服务拥有全部操作权限。服务级授权粒度的云产品，不支持对具体的接口进行授权。
- **操作级**：定义对服务的特定接口（API）是否拥有访问权限，例如：授权某账号对云服务器服务进行只读操作。
- **资源级**：定义对特定资源是否有访问权限，这是最细的授权粒度，例如：授权某账号仅读写操作某台云服务器实例。能支持资源级接口授权的产品，则会被认定为资源级授权粒度。

## 接口授权粒度

- **资源级接口**：此类型接口支持对某一个具体特定的资源进行授权。
- **操作级接口**：此类型接口不支持对某一个特定的资源进行授权。

资源级接口在鉴权时，云产品会将具体的资源六段式传给 CAM 鉴权，故支持对某一个具体特定的资源进行授权和鉴权。

操作级接口在鉴权时，云产品不会将具体的资源六段式传给 CAM 鉴权，只会传递任意资源 `*`。因此授权时策略语法若限定了具体的资源，鉴权时此接口不传递该资源，CAM 会判断此接口不在授权范围，会判断为无权限。

# 访问管理示例

最近更新时间：2024-01-06 18:00:25

## 操作场景

您可以通过使用访问管理（Cloud Access Management, CAM）策略让用户拥有在云服务器（Cloud Virtual Machine, CVM）控制台中查看和使用特定资源的权限。本文档提供了查看和使用特定资源的权限示例，指导用户如何使用控制台的特定部分的策略。

## 操作示例

### CVM 的全读写策略

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

具体操作步骤如下：

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

### CVM 的只读策略

如果您希望用户拥有查询 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。该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。具体操作步骤如下：

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

### CVM 相关资源的只读策略

如果您希望用户只拥有查询 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。该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 中以单词“Describe”开头的所有操作、以单词“Inquiry”开头的所有操作和以单词“Get”开头的所有操作。
- CLB 中以单词“Describe”开头的所有操作。
- Monitor 中所有的操作。

具体操作步骤如下：

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

## 弹性云盘的相关策略

如果您希望用户可以查看 CVM 控制台中的云硬盘信息，并具有创建云硬盘，使用云硬盘等的权限，可先将以下操作添加到您策略中，再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服务器上。
- **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。
- **DescribeInstancesCbsNum**: 查询云服务器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。

具体操作步骤如下：

1. 根据 [策略](#)，创建一个可以查看 CVM 控制台中的云硬盘信息，具有创建云硬盘，使用云硬盘等其他权限的自定义策略。

策略内容可参考以下策略语法进行设置：

```
{
  "version": "2.0",
  "statement": [
    {
      "effect": "allow",
      "action": [
        "name/cvm:CreateCbsStorages",
        "name/cvm:AttachCbsStorages",
        "name/cvm:DetachCbsStorages",
        "name/cvm:ModifyCbsStorageAttributes",
        "name/cvm:DescribeCbsStorages"
      ],
      "resource": [
        "qcs::cvm::uin/1410643447:*"
      ]
    }
  ]
}
```

2. 找到创建的策略，在该策略行的操作列中，单击关联用户/组。
3. 在弹出的关联用户/用户组窗口中，选择您需要授权的用户/组，单击确定。

## 安全组的相关策略

如果您希望用户可以查看并使用 CVM 控制台中的安全组，可将以下操作添加到您策略中，再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。

具体操作步骤如下：

1. 根据 [策略](#)，创建一个允许用户在 CVM 控制台中具有创建、删除、修改安全组等其他权限的自定义策略。策略内容可参考以下策略语法进行设置：

```
{
  "version": "2.0",
  "statement": [
    {
      "action": [
        "name/cvm:ModifySecurityGroupPolicys",
        "name/cvm:ModifySingleSecurityGroupPolicy",
        "name/cvm:CreateSecurityGroupPolicy",
        "name/cvm>DeleteSecurityGroupPolicy"
      ],
      "resource": "*",
      "effect": "allow"
    }
  ]
}
```

2. 找到创建的策略，在该策略行的操作列中，单击**关联用户/组**。
3. 在弹出的**关联用户/用户组**窗口中，选择您需要授权的用户/组，单击**确定**。

## 弹性 IP 地址的相关策略

如果您希望用户可以查看并使用 CVM 控制台中的弹性 IP 地址，可先将以下操作添加到您策略中，再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。

具体操作步骤如下:

1. 根据 [策略](#), 创建一个自定义策略。

该策略允许用户在 CVM 控制台具有查看弹性 IP 地址并可以将其分配给实例并与之相关联, 但不可以修改弹性 IP 地址的属性、取消弹性 IP 地址的关联或释放弹性 IP 地址的权限。策略内容可参考以下策略语法进行设置:

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

2. 找到创建的策略, 在该策略行的操作列中, 单击**关联用户/组**。
3. 在弹出的**关联用户/用户组**窗口中, 选择您需要授权的用户/组, 单击**确定**。

## 授权用户拥有特定 CVM 的操作权限策略

如果您希望授权用户拥有特定 CVM 操作权限, 可将以下策略关联到该用户。具体操作步骤如下:

1. 根据 [策略](#), 创建一个自定义策略。

该策略允许用户用于对 ID 为 ins-1, 地域为广州的 CVM 实例的操作权限, 策略内容可参考以下策略语法进行设置:

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

```
}  
]  
}
```

2. 找到创建的策略，在该策略行的操作列中，单击**关联用户/组**。
3. 在弹出的**关联用户/用户组**窗口中，选择您需要授权的用户/组，单击**确定**。

## 授权用户拥有特定地域 CVM 的操作权限策略

如果您希望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。具体操作步骤如下：

1. 根据 [策略](#)，创建一个自定义策略。

该策略允许用户拥有对广州地域的 CVM 机器的操作权限，策略内容可参考以下策略语法进行设置：

```
{  
  "version": "2.0",  
  "statement": [  
    {  
      "action": "cvm:*",  
      "resource": "qcs::cvm:ap-guangzhou::*",  
      "effect": "allow"  
    }  
  ]  
}
```

2. 找到创建的策略，在该策略行的操作列中，单击**关联用户/组**。
3. 在弹出的**关联用户/用户组**窗口中，选择您需要授权的用户/组，单击**确定**。

## 授权子账号拥有 CVM 的所有权限但不包括支付权限

假设，企业账号（CompanyExample，ownerUin 为12345678）下有一个子账号（Developer），该子账号需要对企业账号的 CVM 服务拥有所有管理权限（例如创建、管理等全部操作），但不包括支付权限（可下单但无法支付）。

我们可通过以下两种方案进行实现：

- **方案 A**

企业账号 CompanyExample 直接将预设策略 QcloudCVMFullAccess 授权给子账号 Developer。授权方式请参见 [授权管理](#)。

- **方案 B**

1. 根据以下策略语法，创建一个 [自定义策略](#)。

```
{
```

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

2. 将该策略授权给子账号。授权方式请参见 [授权管理](#)。

## 授予子账号拥有项目管理的操作权限

假设，企业账号（CompanyExample，ownerUin 为12345678）下有一个子账号（Developer），需要基于项目授权子账号在控制台管理资源。

具体操作步骤如下：

1. 根据业务权限创建一个项目管理的自定义策略。

详情请参见 [策略](#)。

2. 参见 [授权管理](#)，将创建好的自定义策略授权给子账号。

子账号做项目管理时如遇到无权限提示，例如查看快照、镜像、VPC、弹性公网 IP 等产品时提示无权限，可授权子账号 QcloudCVMAccessForNullProject、QcloudCVMOrderAccess 和 QcloudCVMLaunchToVPC 预设策略。授权方式请参见 [授权管理](#)。

## 自定义策略

如果您觉得预设策略不能满足您的要求，您可以通过创建自定义策略达到目的。

具体操作步骤请参见 [策略](#)。

更多 CVM 相关的策略语法请参见 [授权策略语法](#)。

# 网络

## 网络概述

最近更新时间：2024-01-08 09:12:28

腾讯云提供网络和安全功能，保障您的实例安全、高效、自由地对外对内提供服务。

### 加密登录方式

腾讯云提供两种加密登录方式：[密码登录](#) 和 [SSH 密钥登录](#)。用户可以自由选择两种方式安全的与云服务器进行连接。Windows 系统实例不支持 SSH 密钥登录。

### 网络访问

同处于腾讯云上的云产品可以经由 [Internet 访问](#)，也可经由 [内网访问](#)。

- [Internet 访问](#)：Internet 访问是腾讯云提供给实例进行公开数据传输的服务。实例被分配 公网 IP 地址以实现与网络上其他计算机进行通信。
- [内网访问](#)：内网访问即局域网（LAN）服务，是腾讯云通过提供给实例内网 IP 地址，以实现同地域下完全免费的内网通信服务。

### 网络环境

腾讯云的 [网络环境](#) 可以分为：基础网络和私有网络（VPC）。

- [基础网络](#)：基础网络是腾讯云上所有用户的公共网络资源池。适合刚开始认识和使用腾讯云的用户。
- [私有网络](#)：私有网络是一块您在腾讯云上自定义的逻辑隔离网络空间。私有网络下的实例可被启动在预设的、自定义的网段下，与其他用户相互隔离。适合熟悉网络管理的用户。

### 安全组

[安全组](#) 是一种有状态的包过滤功能虚拟防火墙，用于设置单台或多台云服务器的网络访问控制，是腾讯云提供的重要的网络安全隔离手段。

您可以使用以下方法来控制您的实例的访问权限：

- 创建多个安全组，并给每个安全组指定不同的规则。
- 每个实例分配一个或多个安全组，腾讯云将按照这些规则确定：哪些流量可访问实例、实例可以访问哪些资源。
- 配置安全组，以便只有特定的 IP 地址或特定的安全组可以访问实例。

### 弹性公网 IP

[弹性公网 IP](#)（Elastic IP，简称 EIP），是可以独立购买和持有的、某个地域下固定不变的公网 IP 地址。

在以下场景下，推荐使用弹性公网 IP：

- 实例可能会因为不可控原因宕机，需要相同 IP 地址的替代实例以保证访问。
- 实例没有公网 IP 地址，需要一个静态 IP 地址。

## 弹性网卡

**弹性网卡**（Elastic Network Interface, ENI）是绑定私有网络内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移。弹性网卡在配置管理网络、搭建高可靠网络方案时有较大帮助。

## 主机安全

**主机安全** 基于腾讯安全积累的海量威胁数据，利用机器学习为用户提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异地登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系，防止数据泄露。

## DDoS 基础防护

**DDoS 基础防护** 是腾讯云免费为云服务器、负载均衡等资源提供的基础 DDoS 防护能力，满足日常安全运营需求。腾讯云会根据用户的安全信誉状态，动态调整封堵阈值。DDoS 基础防护默认开启，实时监控网络流量，发现攻击立即清洗，为腾讯云上公网 IP 秒级开启防护。

# 网络环境

最近更新时间：2024-01-08 09:12:28

腾讯云的网络环境可以分为 **私有网络**（Virtual Private Cloud, VPC）和基础网络两种。

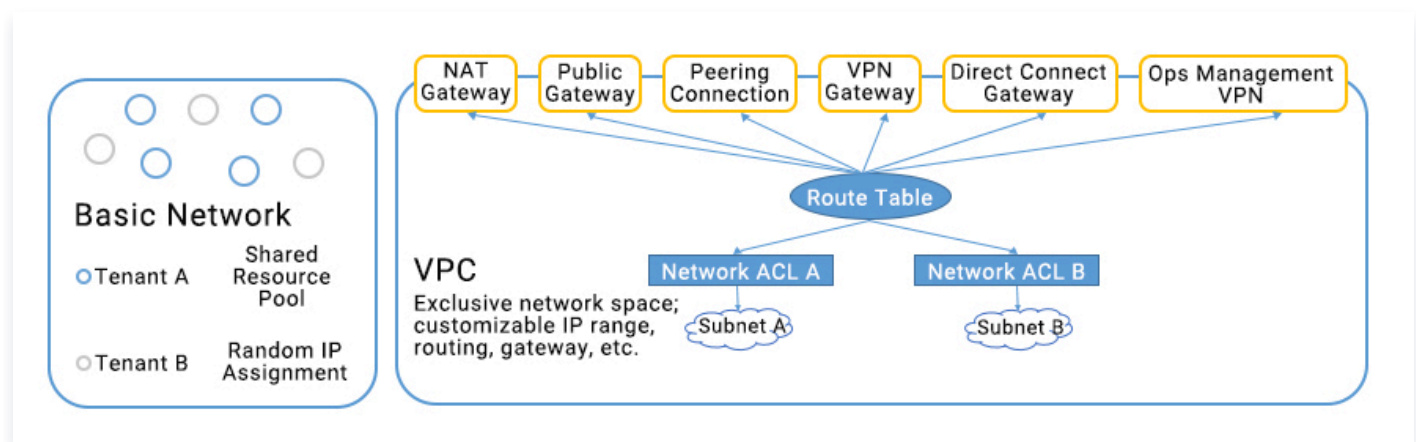
2017年6月13日后，新注册的账号已不支持基础网络，推荐您使用私有网络。其原因如下：

- 功能完备性：基础网络功能均可通过私有网络满足，且私有网络提供更多灵活的网络服务。例如自定义网段、路由、支持专线接入、VPN、NAT 等。
- 迁移平滑性：业界均无完全平滑的迁移方案（需关机，变更内网 IP 等）。如果您后续因业务发展需使用私有网络，迁移过程可能影响您的业务。

## 私有网络与基础网络

### 私有网络

腾讯云 **私有网络** 是一块您在腾讯云上自定义的逻辑隔离网络空间。即使在相同地域下，不同的私有网络之间默认无法互相通信。与您在数据中心运行的传统网络相似，托管在腾讯云私有网络内的是您在腾讯云上的服务资源，包括 **云服务器**、**负载均衡**、**云数据库** 等云服务资源。用户可以完全掌握私有网络环境，更多详细配置与应用场景详见 **私有网络产品概述**。私有网络能构建较为复杂的网络架构，是熟悉网络管理用户的合适选择。



### 基础网络

基础网络是腾讯云上所有用户的公共网络资源池。用户所有云上的资源都由腾讯云统一管理，管理简单、快捷。

### 功能区别

功能	基础网络	私有网络
租户关联	租户关联	基于 GRE 封装的逻辑隔离网络
网络自定义	不支持	支持
路由自定义	不支持	支持

自定义 IP	不支持	支持
互通规则	同租户同地域互通	支持跨地域跨账号互通
安全控制	<a href="#">安全组</a>	<a href="#">安全组</a> 和 <a href="#">网络 ACL</a>

## 私有网络与基础网络间资源共享与访问

腾讯云上一些云资源和功能可以在同时支持两种网络环境，可在不同网络之间共享或访问。

资源	说明
<a href="#">镜像</a>	可使用镜像在任何网络环境下启动云服务器实例
<a href="#">弹性 IP</a>	弹性 IP 可以绑定任何网络环境下的云服务器实例
实例	基础网络下实例和私有网络内实例可以通过 <a href="#">公网 IP</a> 或 <a href="#">基础网络互通</a> 功能实现相互通信
<a href="#">SSH 密钥</a>	SSH 密钥支持加载至任何网络环境下的云服务器实例
<a href="#">安全组</a>	安全组支持绑定任何网络环境下的云服务器实例

### ⓘ 说明：

[负载均衡](#) 无法在基础网络与私有网络之间共享。即使已建立网络互通连接，同样不支持负载均衡同时绑定私有网络内实例和基础网络实例。

## 基础网络内实例迁移至私有网络

参见 [切换私有网络服务](#)，将基础网络内实例迁移至私有网络。

# 内网服务

最近更新时间：2025-10-31 19:13:10

内网服务即局域网（LAN）服务，云服务之间经由内部链路互相访问。腾讯云上的云产品可以经由 [Internet 访问](#)，也可经由腾讯云内网互相访问。腾讯云机房均由底层万兆/千兆互联，提供带宽高、时延低的内网通信服务，帮助您灵活构建网络架构。

## 内网 IP 地址

### 概述

内网 IP 地址是无法通过 Internet 访问的 IP 地址，是腾讯云内网服务的实现形式。每个实例都具有分配内网 IP 的默认网络接口（即 eth0），内网 IP 地址可由腾讯云自动分配也可由用户自定义（仅在 [私有网络](#) 环境下）。

#### ⓘ 说明：

在操作系统内部自行变更内网 IP 会导致内网通讯中断。

### 属性

- 内网服务具有用户属性，不同用户间相互隔离，即默认无法经由内网访问另一个用户的云服务。
- 内网服务具有地域属性，不同地域间相互隔离，即默认无法经由内网访问同账户下不同地域的云服务。

### 适用场景

内网 IP 可以用于负载均衡、云服务器实例之间内网互访、云服务器实例与其他云服务（如 TencentDB）之间内网互访。

### 地址分配

每个云服务器实例在启动时都会被分配一个默认的内网 IP 地址。针对不同的 [网络环境](#)，内网 IP 也有所不同：

- 基础网络：内网 IP 地址由腾讯云自动分配，不可更改。
- 私有网络：目前腾讯云私有网络 CIDR 支持使用三大私有网段中的任意一个，IP 地址范围如下：
  - 10.0.0.0 – 10.255.255.255 （掩码范围需在12 – 28之间）
  - 172.16.0.0 – 172.31.255.255 （掩码范围需在12 – 28之间）
  - 192.168.0.0 – 192.168.255.255 （掩码范围需在16 – 28之间）

## 内网 DNS

### DNS 服务器地址

内网 DNS 服务负责域名解析，如果 DNS 配置有误会造成域名无法访问。

腾讯云在不同地域均提供了可靠的内网 DNS 服务器。具体配置如下：

网络环境	地域	内网 DNS 服务器
基础网络	广州	广州一区： 10.112.65.31 10.112.65.32
		广州三区： 10.59.218.193 10.59.218.194
		广州四区： 100.121.190.140 100.121.190.141
	上海	9.193.104.247 11.122.34.35
	北京	10.53.216.182 10.53.216.198
	北美	10.116.19.188 10.116.19.185
	中国香港	10.243.28.52 10.164.55.3
	新加坡	100.78.90.19 100.78.90.8
	广州 Open	10.59.218.18 10.112.65.51
	成都	100.88.222.14 100.88.222.16
	硅谷	100.102.22.21 100.102.22.30
	法兰克福	100.120.52.60 100.120.52.61
首尔	10.165.180.53 10.165.180.62	
私有网络	所有地域	183.60.83.19 183.60.82.98

## 操作指南

您可以进行查看或修改实例内网 IP 地址等操作，详细指引请参考：

- [获取实例内网 IP 地址和设置 DNS](#)
- [修改实例内网 IP 地址](#)

# 公网服务

最近更新时间：2024-01-08 09:12:28

当用户在云服务器实例上部署的应用需要公开提供服务时，必须经由 Internet 传输数据，且必须具备一个 Internet 上的 IP 地址（亦称公网 IP 地址）。腾讯云提供的 Internet 访问均经由腾讯云数据中心高速互联网。国内多线 BGP 网络覆盖超过二十家网络运营商，BGP 公网出口秒级跨域切换，保证您的用户无论使用哪种网络，均能享受高速、安全的网络质量。

## 公网 IP 地址

- **概述：**公网 IP 地址是 Internet 上的非保留地址，有公网 IP 地址的云服务器可以和 Internet 上的其他计算机互相访问。
- **获取：**在创建云服务器时，在网络中设置带宽大于 0Mbps，完成后腾讯云系统会自动从腾讯云公有 IP 地址池中为该实例分配一个公有 IP 地址，此地址可更改，操作详情请参见 [更换公网 IP](#)。
- **配置：**您可以在 Internet 上登录有公网 IP 地址的云服务器实例对其进行相应配置，有关登录云服务器实例的更多内容，请参见 [登录 Linux 实例](#) 和 [登录 Windows 实例](#)。
- **转换：**公有 IP 地址通过网络地址转换（NAT）映射到实例的 [内网 IP 地址](#)。
- **维护：**腾讯云的所有公网接口统一由 Tencent Gateway (TGW) 进行处理。腾讯云云服务器实例的公网网卡在统一接口层 TGW 上配置，云服务器无感知。所以，用户在云服务器中通过 `ifconfig` (Linux) 或 `ipconfig` (Windows) 命令查看网络接口信息时，只能查看到 [内网](#) 的信息。公网信息需要由用户自行登录 [云服务器控制台](#) 云服务器列表/详情页进行查看。
- **费用：**实例通过公网 IP 地址提供服务需要支付相应的费用，具体内容可以参见 [公网计费模式](#)。

## 公网 IP 地址释放

用户无法主动关联或释放与实例关联的公网 IP 地址。

出现下列情况下时，公网 IP 地址会被释放或重新分配：

- **销毁实例时。**用户主动销毁按量计费类型实例，腾讯云将释放它的公网 IP 地址。
- **弹性公网 IP 地址 与实例关联和取消关联时。**实例关联弹性公网 IP 地址时，腾讯云将释放实例原有的公网 IP 地址。取消实例与弹性 IP 地址的关联时，实例会被自动分配一个新的公网 IP 地址，原有被释放的公网 IP 地址将返回到公网 IP 地址池中，并且您无法重新使用它。

如果您需要一个固定的永久公网 IP 地址，可使用 [弹性公网 IP 地址](#)。

## 操作指南

您可以进行获取和更换公网 IP 地址等操作，详细指引请参考：

- [获取实例公网 IP 地址](#)
- [更换实例公网 IP 地址](#)

# 弹性公网 IP

最近更新时间：2024-04-10 14:19:43

## 简介

弹性公网 IP 地址（EIP），简称弹性 IP 地址或弹性 IP。它是专为动态云计算设计的静态 IP 地址，是某地域下一个固定不变的公网 IP 地址。借助弹性公网 IP 地址，您可以快速将地址重新映射到账户中的另一个实例或 NAT 网关实例，从而屏蔽实例故障。

弹性公网 IP 未进行释放前，您可以将其一直保留于您的账号中。相较于公网 IP 仅可跟随云服务器一起申请释放，弹性公网 IP 可以与云服务器的生命周期解耦，作为云资源单独进行操作。例如，若您需要保留某个与业务强相关的公网 IP，可以将其转为弹性公网 IP 保留在您的账号中。

## EIP 的 IP 地址类型

腾讯云支持常规 BGP IP、精品 BGP IP、加速 IP 和静态单线 IP 等多种类型的弹性公网 IP。

- 常规 BGP IP：国内多线 BGP 网络覆盖超过二十家网络运营商（三大运营商、教育网、广电等），BGP 公网出口支持秒级跨域切换，保证您的用户无论使用哪种网络，均能享受高速、安全的网络质量。
- 精品 BGP IP：专属线路，避免绕行国际运营商出口网络；延时更低，可有效提升境外业务对中国大陆用户覆盖质量。
- 加速 IP：采用 Anycast 加速，使公网访问更稳定、可靠、低延迟。
- 静态单线 IP：通过单个网络运营商访问公网，成本低且便于自主调度。
- 高防 EIP：云原生 DDoS 防护 BGP IP，需配合企业版高防包使用，提供 Tbps 级别 DDoS 全力防护。高防 EIP 分别与业务资源、高防资源绑定后，便可拥有 DDoS 防护能力。

## IP 资源池

- 如您的业务需要预留连续 IP 地址，或分配特定网段的 IP 地址，可 [提交工单](#) 咨询，我们将为您分配独有的 IP 资源池。
- 目前支持独有资源池的线路类型有：常规 BGP、静态单线、精品 BGP。
- 具体费用请咨询商务经理。

## EIP 和普通公网 IP 的区别

公网 IP 地址是 Internet 上的非保留地址，有公网 IP 地址的云服务器可以和 Internet 上的其他计算机互相访问。普通公网 IP 和 EIP 均为公网 IP 地址，二者均可为云资源提供访问公网和被公网访问的能力。

- 普通公网 IP：仅能在 CVM 购买时分配且无法与 CVM 解绑，如购买时未分配，则无法获得。
- EIP：可以独立购买和持有的公网 IP 地址资源，可随时与 CVM、NAT 网关、弹性网卡和高可用虚拟 IP 等云资源绑定或解绑。

! 说明：

当前普通公网 IP 仅支持常规 BGP IP 线路类型。

与普通公网 IP 相比，EIP 提供更灵活的管理方式，如下表所示，详情请参见 [公网 IPv4 地址](#)。

对比项	普通公网 IP	EIP
访问公网/被公网访问	✓	✓
独立购买与持有	×	✓
自由绑定与解绑	×	✓
实时调整带宽 <sup>1</sup>	✓	✓
IP 资源占用费	×	✓

#### ❗ 说明：

[公网 IP 控制台](#) 仅支持调整 EIP 的带宽，普通公网 IP 的带宽调整请参见 [调整普通公网 IP 网络配置](#)。

EIP 可以与云资源的生命周期解耦合，单独进行操作。例如，若您需要保留某个与业务强相关的公网 IP 地址，可以将普通公网 IP 转换为 EIP 保留在您的账号中。

## 规则与限制

### 使用规则

- 弹性公网 IP 地址同时适用于基础网络和私有网络的实例，以及私有网络中的 [NAT 网关](#) 实例。
- 弹性 IP 地址与 CVM 实例绑定时，实例的当前公网 IP 地址会被释放。
- 销毁 CVM/NAT 网关实例，会断开与弹性 IP 地址的关联。
- 弹性公网 IP 计费规则请参见 [弹性公网 IP 计费](#)。
- 弹性公网 IP 操作步骤请参见 [弹性公网 IP](#)。

### 配额限制

资源	限制
每个腾讯云账户每个地域 (Region) 配额弹性公网 IP 个数	20个
每个腾讯云账户各个地域每天申购次数	配额数 * 2次
解绑 EIP 时，每个账户每天可免费重新分配公网 IP 的次数	10次

#### ❗ 说明：

- 弹性公网 IP 配额默认不支持调整，可通过 [NAT 网关](#)、[负载均衡](#) 进行 IP 收敛。
- 如有特殊情况需调整，则需账号存在对应量级的云服务资源，且合理使用。

## 云服务器绑定公网 IP 限制

### 说明：

在2019年9月18日零点前购买的云服务器不受此限制，其支持绑定的公网 IP 数量等于您的服务器支持的 [内网 IP 数量](#)。

云服务器的 CPU 数	支持绑定的公网 IP 数量上限（含普通公网 IP 和弹性公网 IP）
CPU: 1 – 5	2
CPU: 6 – 11	3
CPU: 12 – 17	4
CPU: 18 – 23	5
CPU: 24 – 29	6
CPU: 30 – 35	7
CPU: 36 – 41	8
CPU: 42 – 47	9
CPU: $\geq$ 48	10

# 弹性网卡

最近更新时间：2024-01-08 09:12:28

**弹性网卡**（Elastic Network Interface, ENI）是绑定私有网络内云服务器的一种弹性网络接口，可在多个云服务器间自由迁移。弹性网卡在配置管理网络、搭建高可靠网络方案时有较大帮助。

弹性网卡具有私有网络、可用区和子网属性，只可以绑定相同可用区下的云服务器。一台云服务器可以绑定多个弹性网卡，具体绑定数量将根据云服务器规格而定。

## 相关概念

- **主网卡与辅助网卡**：私有网络的云服务器创建时联动创建的网卡为主网卡，用户自行创建的网卡为辅助网卡，其中主网卡不支持绑定和解绑，辅助网卡支持绑定解绑。
- **主内网 IP**：弹性网卡的主内网 IP，在弹性网卡创建时由系统随机分配或用户自行制定，主网卡的主内网 IP 支持修改，辅助网卡的主内网 IP 不支持修改。
- **辅助内网 IP**：弹性网卡主 IP 以外绑定的辅助内网 IP，由用户在创建弹性网卡或编辑弹性网卡时自行配置，支持绑定和解绑。
- **弹性公网 IP**：与弹性网卡上的内网 IP 一一绑定。
- **安全组**：弹性网卡可以绑定一个或多个安全组。
- **MAC 地址**：弹性网卡有全局唯一的 MAC 地址。

## 应用场景

- **内网、外网、管理网隔离**：  
重要业务的网络部署一般会要求数据传输内网、外网和管理网三网隔离，通过不同的路由策略和安全组策略保证网络之间的数据安全和网络隔离。您可以像物理服务器一样，为云服务器绑定三个位于不同子网的弹性网卡来实现三网隔离。
- **高可靠应用部署**：  
系统架构中的关键组件，都需要通过多机热备来保证系统的高可用性。腾讯云提供了可以灵活绑定和解绑的弹性网卡及内网 IP，您可以配置 Keepalived 的容灾设置实现关键组件的高可用部署。

## 使用限制

根据 CPU 和内存配置不同，云服务器可以绑定的弹性网卡数和单网卡绑定内网 IP 数有较大不同，网卡和单网卡 IP 配额数如下表所示：

### ⚠ 注意：

单个网卡绑定 IP 数量仅代表网卡可以绑定的 IP 数量上限，不承诺按照上限提供 EIP 配额，账号的 EIP 配额按照 EIP 使用限制 提供。

## 云服务器支持绑定的弹性网卡配额

机型	实例类型	弹性网卡配额									
		CPU : 1核	CPU : 2核	CPU : 4核	CPU : 6核	CPU : 8核	CPU : 10核	CPU : 12核	CPU : 14核	CPU : 16核	CPU : >16核
标准型	标准型 S5	2	4	4	-	6	-	-	-	8	8
	标准存储增强型 S5se	-	-	4	-	6	-	-	-	8	8
	标准型 SA2	2	4	4	-	6	-	-	-	8	8
	标准型 S4	2	4	4	-	6	-	-	-	8	8
	标准网络优化型 SN3ne	2	4	4	-	6	-	8	-	8	8
	标准型 S3	2	4	4	-	6	-	8	-	8	8
	标准型 SA1	2	2	4	-	6	-	-	-	8	8

	标准型 S2	2	4	4	-	6	-	8	-	8	8
	标准型 S1	2	4	4	-	6	-	8	-	8	8
高 IO 型	高 IO 型 IT5	-	-	-	-	-	-	-	-	8	8
	高 IO 型 IT3	-	-	-	-	-	-	-	-	8	8
内存型	内存型 M5	2	4	4	-	6	-	8	-	8	8
	内存型 M4	2	4	4	-	6	-	8	-	8	8
	内存型 M3	2	4	4	-	6	-	8	-	8	8
	内存型 M2	2	4	4	-	6	-	8	-	8	8
	内存型 M1	2	4	4	-	6	-	8	-	8	8
计算型	计算型 C4	-	-	4	-	6	-	-	-	8	8
	计算网络增强型 CN3	-	-	4	-	6	-	-	-	8	8
	计算型 C3	-	-	4	-	6	-	-	-	8	8

	计算型 C2	-	-	4	-	6	-	-	-	8	8
GPU 机型	GPU 计算型 GN2	-	-	-	-	-	-	-	-	-	8
	GPU 计算型 GN6	-	-	-	-	-	-	-	-	-	8
	GPU 计算型 GN6 S	-	-	4	-	6	-	-	-	-	-
	GPU 计算型 GN7	-	-	4	-	6	-	-	-	-	8
	GPU 计算型 GN8	-	-	-	4	-	-	-	8	-	8
	GPU 计算型 GN10 X	-	-	-	-	6	-	-	-	-	8
	GPU 计算型 GN10 Xp	-	-	-	-	-	6	-	-	-	8
FPGA	FPGA 加速型 FX4	-	-	-	-	-	6	-	-	-	8

机型												
大数据型	大数据型 D3	-	-	-	-	6	-	-	-	8	8	
	大数据型 D2	-	-	-	-	6	-	-	-	8	8	
	大数据型 D1	-	-	-	-	6	-	-	-	-	8	
裸金属云服务器	不支持绑定弹性网卡											

## 云服务器单网卡支持绑定的内网IP配额

机型	实例类型	单网卡绑定内网 IP 配额									
		CPU : 1 核	CPU : 2 核	CPU : 4 核	CPU : 6 核	CPU : 8 核	CPU : 10 核	CPU : 12 核	CPU : 14 核	CPU : 16 核	CPU : >16 核
标准型	标准型 S5	6	10	10	-	20	-	-	-	30	30
	标准存储增强型 S5se	-	-	20	-	20	-	-	-	30	30

标准型 SA2	6	10	10	-	20	-	-	-	30	30
标准型 S4	6	10	10	-	20	-	-	-	30	30
标准网络优化型 SN3ne	6	10	10	-	20	-	30	-	30	30
标准型 S3	6	10	10	-	20	-	30	-	30	30
标准型 SA1	内存=1G : 2 内存>1G : 6	10	内存=8G : 10 内存=16G : 20	-	20	-	-	-	30	30
标准型 S2	6	10	10	-	20	-	30	-	30	30

	标准型 S1	6	10	10	-	20	-	30	-	30	30
高 IO 型	高 IO 型 IT5	-	-	-	-	-	-	-	-	30	30
	高 IO 型 IT3	-	-	-	-	-	-	-	-	30	30
内存型	内存型 M5	6	10	10	-	20	-	30	-	30	30
	内存型 M4	6	10	10	-	20	-	30	-	30	30
	内存型 M3	6	10	10	-	20	-	30	-	30	30
	内存型 M2	6	10	10	-	20	-	30	-	30	30
	内存型 M1	6	10	10	-	20	-	30	-	30	30
计算型	计算型 C4	-	-	10	-	20	-	-	-	30	30
	计算	-	-	10	-	20	-	-	-	30	30

	网络增强型 CN 3											
	计算型 C3	-	-	10	-	20	-	-	-	30	30	
	计算型 C2	-	-	10	-	20	-	-	-	30	30	
GPU 机型	GPU 计算型 GN 2	-	-	-	-	-	-	-	-	-	30	
	GPU 计算型 GN 6	-	-	-	-	-	-	-	-	-	30	
	GPU 计算型 GN 6S	-	-	10	-	20	-	-	-	-	-	
	GPU 计算型	-	-	10	-	20	-	-	-	-	30	

	GN 7											
	GPU 计算型 GN 8	-	-	-	10	-	-	-	30	-	30	
	GPU 计算型 GN 10X	-	-	-	-	20	-	-	-	-	30	
	GPU 计算型 GN 10X p	-	-	-	-	-	20	-	-	-	30	
FP GA 机型	FP GA 加速型 FX 4	-	-	-	-	-	20	-	-	-	30	
大数据型	大数据型 D3	-	-	-	-	20	-	-	-	30	30	
	大数据	-	-	-	-	20	-	-	-	30	30	

	型 D2											
	大数据型 D1	-	-	-	-	20	-	-	-	-		30
裸金属云服务器	不支持绑定弹性网卡											

## API 概览

此处展示弹性网卡与云服务器相关的 API 接口，如下表所示。更多弹性网卡相关操作请参见 [弹性网卡 API 概览](#)。

接口功能	Action ID	功能描述
创建弹性网卡	<a href="#">CreateNetworkInterface</a>	创建弹性网卡
弹性网卡申请内网 IP	<a href="#">AssignPrivateIpAddresses</a>	弹性网卡申请内网 IP
弹性网卡绑定云服务器	<a href="#">AttachNetworkInterface</a>	弹性网卡绑定云服务器

# 配置巨型帧能力

最近更新時間：2025-06-24 16:02:22

本文介绍云服务器 CVM 实例巨型帧功能的使用方式，包括新购买云服务器时开启巨型帧功能，已经购买的云服务器开启巨型帧功能。

## 前提条件

参考云服务器 [实例规格文档](#)，查看当前云服务器机型是否支持巨型帧功能。

## 操作步骤

### 新购买云服务器开启巨型帧功能

1. 登录 [腾讯云官网](#)，选择产品 > 计算和容器 > 计算 > [云服务器](#)，单击**立即选购**，进入云服务器购买页面。
2. 按照 [通过购买页创建实例](#) 指导，完成基础配置。
3. 在设置网络和主机步骤中开启巨型帧功能。

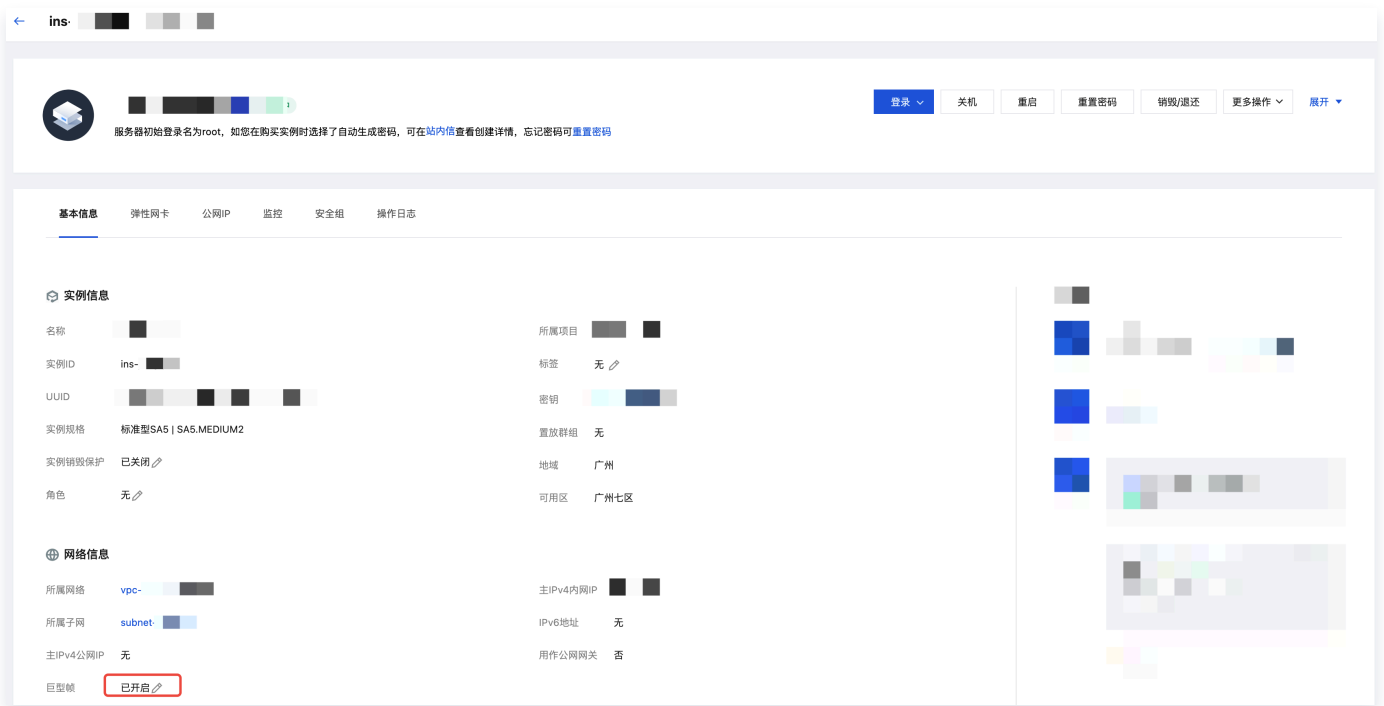
选择高级设置 > 巨型帧，勾选**免费开通**，开启巨型帧功能，完成后，单击**下一步：确认配置信息**

The screenshot shows the 'Advanced Settings' step in the Tencent Cloud console. The 'Giant Frames' section is highlighted with a red box, showing the 'Free Activation' checkbox checked. Other sections like 'Host Name', 'CAM Role', and 'Custom Data' are also visible.

4. 参考 [通过购买页创建实例](#)，完成云服务器购买。

### 已经购买的云服务器开启/关闭巨型帧功能

1. 登录 [云服务器控制台](#)，进入云服务器页面。
2. 单击对应云服务器实例名称，跳转到云服务器详情页。
3. 在网络信息中，找到巨型帧开关。



4. 单击**编辑**图标，修改巨型帧功能状态，选择**启用/关闭**后，单击**确定**。

#### ⚠ 注意：

修改云服务器巨型帧配置需要重启服务器，重启期间将无法提供服务，请您做好相关准备，以免造成影响。

## 修改巨型帧配置



**i** 注意：修改巨型帧配置需要重启实例，重启期间将无法提供服务，请您做好相关准备，以免造成影响。

您已选择1台实例 [收起](#)

ID/名称	实例类型	实例配置
	标准型SA5	2核 2GB 0Mbps 系统盘：通用型SSD云硬盘 网络：vpc-

巨型帧配置  启用  关闭

确定

取消

# 主机安全

最近更新时间：2024-01-08 09:12:28

## 简介

主机安全基于腾讯安全积累的海量威胁数据，利用机器学习为用户提供黑客入侵检测和漏洞风险预警等安全防护服务，主要包括密码破解拦截、异地登录提醒、木马文件检测、高危漏洞检测等安全功能，解决当前服务器面临的主要网络安全风险，帮助企业构建服务器安全防护体系，防止数据泄露。

主机安全分为基础防护及专业防护两个版本，腾讯云云服务器在创建时可选择默认免费开通主机安全基础防护。

### 说明：

主机安全基础防护及专业防护功能介绍与比较，请参见 [功能介绍与版本比较](#)。

## 计费方式

主机安全基础防护不收取服务费用。

## 安装主机安全基础防护

您可结合实际情况，通过以下方式安装主机安全基础防护：

### 创建云服务器时自动安装

腾讯云云服务器在创建时，可选择默认免费开通主机安全基础防护。在云服务器实例购买页面的“安全加固”中，勾选“免费开通”即可自动安装主机安全。如下图所示：



Security  Enable for Free  
Reinforcement Free Anti-DDoS Protection and CWP Basic (component installation required) [Details](#)

### 为已有云服务器手动安装

若您需为已有实例安装主机安全，请对应实例操作系统通过以下方式进行安装：

- [Windows 云服务器环境](#)
- [Linux 云服务器环境](#)

成功安装后，您可在 [主机安全控制台](#) 查看云服务器的安全状态。

## 相关文档

- 主机安全基础防护及专业防护 [功能介绍与版本比较](#)
- [安全概览](#)

# DDoS 基础防护

最近更新时间：2024-01-08 09:12:28

## 简介

DDoS 基础防护是腾讯云免费为云服务器、负载均衡等资源提供的基础 DDoS 防护能力，满足日常安全运营需求。腾讯云会根据用户的安全信誉状态，动态调整封堵阈值。DDoS 基础防护默认开启，实时监控网络流量，发现攻击立即清洗，为腾讯云上公网 IP 秒级开启防护。

## 计费方式

DDoS 基础防护为免费服务，若您需其他 DDoS 防护解决方案，请参见 [DDoS 防护解决方案对比](#)。

## 开通 DDoS 基础防护

腾讯云云服务器在创建时可选择默认免费开通 DDoS 基础防护。在云服务器实例购买页面的“安全加固”中，勾选“免费开通”即可开通 DDoS 基础防护。

开通后，您可在 [云服务器控制台概览页](#) 或 DDoS 防护控制台的 [DDoS 基础防护](#) 页面查看云服务器的防护配置。