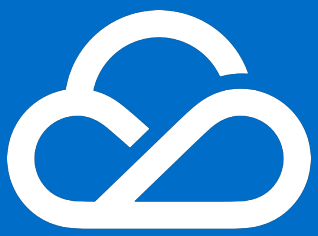
腾讯云云服务器

网络与安全性

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

网络与安全性

网络与安全性概述

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 密钥对登录
。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 地址(Elastic IP, EIP)，又简称弹性 IP 地址或弹性 IP 。是专为动态云计算设计的静态 IP 地址。在以下情境下，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。

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）两种。

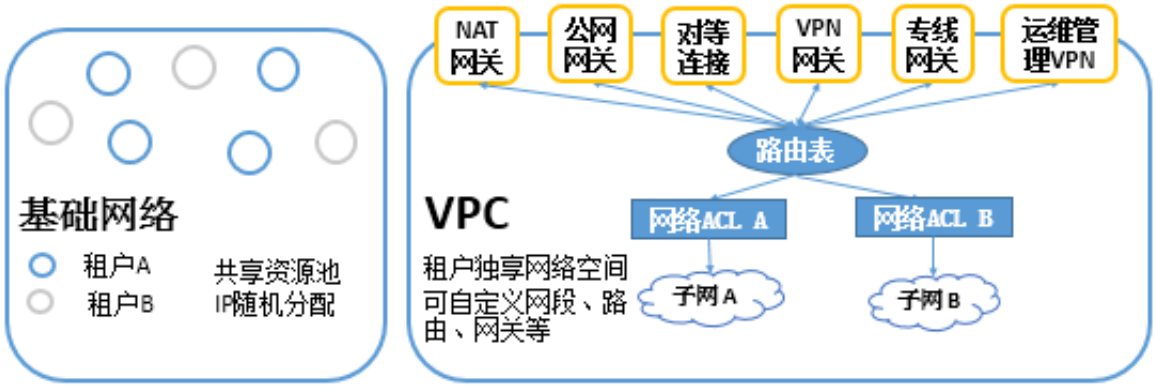
基础网络与私有网络

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。基础网络能满足与实现大部分用户的需求，是刚开始认识和使用腾讯云用户的合适选择。

私有网络：

腾讯云 私有网络（Virtual Private Cloud，VPC）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。



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	安全组	安全组 和 网络 ACL

基础网络与私有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
镜像	可使用镜像在任何网络环境下启动云服务器实例
弹性 IP	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 公网 IP 或 基础网络互通 功能实现相互通信
SSH 密钥	SSH 密钥支持加载至任何网络环境下的云服务器实例
安全组	安全组支持绑定任何网络环境下的云服务器实例

注意：

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

1. 在基础网络云服务器实例中，创建自定义镜像 。
2. （可选）在基础网络云服务器实例数据盘中，创建快照 。
3. 创建私有网络与子网 。
4. 在私有网络内， 购买并启动云服务器实例 。

登录密码

为保证实例的安全可靠，腾讯云提供两种加密登录方式：密码登录和 SSH 密钥对登录。不同操作系统云服务器的用户可以分别参考 自定义配置 Windows 云服务器 与 自定义配置 Linux 云服务器 的设置信息部分，选择加密方式。

本文档介绍密码登录的相关配置内容。

密码是每台云服务器实例专有的登录凭据。任何拥有实例登录密码的人都可以通过被安全组允许的公网地址远程登录云服务器实例。因此，建议您使用较为安全的密码，有效保管并不定期修改。

设置初始密码

- 选择【自动生成密码】的用户，会在控制台 站内信 中收到初始密码。
- 选择【设置密码】的用户，自定义的密码即为初始密码。

1. 选择自定义配置云服务器的用户，在设置主机名及登录方式部分可以选择登录方式，默认为【设置密码】。

2. 按照规定的密码字符限制，输入主机密码和确认密码，单击立即购买，初始密码设置成功，待云服务器实例分配成功。

   设置密码的字符限制：

   - Linux 云服务器密码需 8 到 16 位，

     a-z 和 A-Z 和 0-9 和 ( ) ` ~ ! @ # $ % ^ & * - + = _ | { } [ ] : ; ' < > , . ? /

     中至少包括两项。
   - Windows 云服务器密码需 12 到 16 位，

     a-z 和 A-Z 和 0-9 和 ( ) ` ~ ! @ # $ % ^ & * - + = _ | { } [ ] : ; ' < > , . ? /

     中至少包括三项。

查看密码

自动生成密码，会发送到控制台 站内信 中。单击需要查看的信件即可查看到初始密码。

登录 云服务器控制台 ，单击右上方 信封样式 站内信 图标。

重置密码

注意：

只有关机状态下才可以对云服务器进行重置密码。如果云服务器处于运行中重置密码，将强制关机，可能会导致数据丢失或文件系统损坏。

1. 登录 云服务器控制台 。

2. 关机需要重置密码的云服务器。

3. 打开密码重置框。

   - 对于单个关机的实例，在右侧操作栏中，单击【更多】-【重置密码】。
   - 对于批量实例，勾选所有需要重置密码的主机，在列表顶部，单击【重置密码】，即可批量修改主机登录密码。对于不能重置密码的实例会显示原因。

4. 在重置密码弹出框中输入新密码、确认密码，单击【下一步】。

5. 等待重置成功，您将收到重置成功的 站内信 消息，即可使用新密码开机使用云服务器。

SSH 密钥

为保证实例的安全可靠，腾讯云提供两种加密登录方式： 密码登录 和 SSH 密钥对登录。本文档介绍 SSH 密钥对登录的相关配置内容。不同操作系统云服务器的用户可以分别参考 自定义配置 Windows 云服务器 与 自定义配置 Linux 云服务器 的设置信息部分，选择加密方式。

SSH 密钥概述

腾讯云允许使用公有密钥密码术加密和解密对于 Linux 实例的登录信息。公有密钥密码术使用公有密钥加密某个数据（如一个密码），然后收件人可以使用私有密钥解密数据。公有和私有密钥被称为密钥对。用户可以通过密钥对安全地与云服务器进行连接，是一种比常规密码更安全的登录云服务器的方式。

腾讯云只会存储公有密钥，您需要存储私有密钥。拥有您的私有密钥的任何人都可以解密您的登录信息，因此将您的私有密钥保存在一个安全的位置非常重要。

> 注意：
> Windows 实例不支持 SSH 密钥登录。

创建 SSH 密钥

1. 登录 云服务器控制台 。
2. 单击左侧导航窗格中的【SSH 密钥】。
3. 单击【创建密钥】
   - 若创建方式选择 "创建新密钥对" ，输入密钥名称，单击【确定】；
   - 若创建方式选择 "使用已有公钥"
     ，输入密钥名称，并输入原有的公钥信息，然后单击【确定】。
4. 弹出提示框，单击【下载】（用户需要在 10 分钟内下载私钥）。

密钥绑定/解绑服务器

1. 登录 云服务器控制台 。

2. 单击左侧导航窗格中的【SSH 密钥】。
3. 勾选 SSH 密钥，单击【绑定/解绑云主机】（或在需要修改的密钥名称上右键单击，单击【绑定/解绑云主机】）。
4. 选择地域，勾选需要关联/解绑的服务器（解绑时取消右侧已选择中的服务器），单击【确定】。
5. 后台进行 SSH 密钥下发，下发完成会提示操作成功或操作失败。

修改 SSH 密钥名称/描述

1. 登录 云服务器控制台 。
2. 单击左侧导航窗格中的【SSH 密钥】。
3. 勾选密钥列表中需要修改的密钥，单击上方【修改】（或在需要修改的密钥名称上右键单击，单击【修改】）。
4. 在弹框中输入新的名称及描述信息，单击【确定】。

删除 SSH 密钥

注意：
若 SSH 密钥已关联云服务器或已关联自定义镜像，则不能删除。

1. 登录 云服务器控制台 。
2. 单击导航窗格中的【SSH 密钥】。
3. 勾选所有需要删除的 SSH 密钥，单击【删除】按钮（或在需要删除的密钥名称上右键单击，单击【删除】，在弹出窗口中单击【确认】）。

使用 SSH 密钥登录 Linux 云服务器

使用 SSH 密钥登录 Linux 云服务器前，需要先完成创建 SSH 密钥，并将 SSH 密钥绑定云服务器。

具体操作请参考 登录 Linux 云服务器 。

安全组

概述

简介

安全组是一种有状态的包过滤虚拟防火墙，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。

- 安全组是一个逻辑上的分组，您可以将同一地域内具有相同网络安全隔离需求的基础网络云服务器或弹性网卡实例加到同一个安全组内。
- 您可以通过安全组策略对实例的出入流量进行安全过滤，实例可以是基础网络云服务器或弹性网卡实例。
- 您可以随时修改安全组的规则，新规则立即生效。

安全组模板

安全组支持自定义创建和模板创建，目前提供三个模板：

- 放通 22、80、443、3389 端口和 ICMP，放通 Windows 和 Linux 默认的登录端口和常见的 Web 服务端口到公网，内网端口全通。
- 放通全部端口：暴露全部端口到公网和内网，有一定安全风险。

安全组规则

安全组规则可控制允许到达与安全组相关联的实例的入站流量，以及允许离开实例的出站流量（从上到下依次筛选规则）。默认情况下，新建安全组将 All Drop
（拒绝）所有流量，云服务器绑定一个无规则的安全组拒绝所有流量。

对于安全组的每条规则，您可以指定以下几项内容：

- 协议类型：例如 TCP、UDP 或 ICMP 等。
- 端口：来源或目标的端口范围。
- 授权类型：地址段（ CIDR/IP ）访问，或安全组访问（安全组 ID ）。

- 来源或目标：流量的源（入站规则）或目标（出站规则），请指定以下选项之一：
  - 用 CIDR 表示法，指定的单个 IP 地址。
  - 用 CIDR 表示法，指定的 IP 地址范围（例如： 203.0.113.0/24 ）。
  - 引用安全组 ID ，您可以引用以下安全组的ID之一：
    - 当前安全组：表示与安全组关联的 CVM 可/不可互访。
    - 其他安全组：同一区域中的另一个安全组 ID 。
- 策略：允许或拒绝。

注意：

- 引用安全组 ID
  法作为高阶功能，您可选择使用。引用安全组不会将规则添加到当前安全组。
- 引用安全组 ID 且设置策略为允许时表示：关联来源安全组 ID 的 CVM
  与关联原有安全组的 CVM 可以相互访问。

安全组优先级

- 实例绑定多个安全组时的优先级为：数字越小，优先级越高。
- 安全组内规则的优先级为：位置越上，优先级越高。

实例绑定安全组时，如果该安全组内无任何规则，将默认拒绝所有流量。

安全组与网络 ACL 的区别

对比项	安全组	网络 ACL
操作级别	在实例级别的操作（第一防御层）	在子网级别的操作（第二防御层）
支持的规则	支持允许规则和拒绝规则	支持允许规则和拒绝规则
有无状态	有状态：返回数据流会被自动允许，不受任何规则的影响	无状态：返回数据流必须被规则明确允许
应用实例	只有在启动实例的同时指定安全组、或稍后将安全组与实例关联的情况下，操作才会被应用到实例	自动应用到关联子网内的所有 CVM 实例

限制

- 安全组区分地域和项目，CVM 只能与相同地域、相同项目中的安全组进行绑定。
- 安全组适用于任何（处在 网络环境 的）CVM 实例。
- 每个用户在每个地域每个项目下最多可设置 50 个安全组。
- 一个安全组入站方向或出站方向的访问策略，各最多可设定 100 条。
- 一个 CVM 可以加入多个安全组，一个安全组可同时关联多个 CVM ，数量无限制。
- 基础网络 内云服务器绑定的安全组 无法过滤 来自（或去往）腾讯云上的关系型数据库（CDB）、弹性缓存（ Redis 和 Memcached ）的数据包。如果您需要过滤这类实例的流量，您可以使用 iptables 实现。

功能描述	数量
安全组	50 个/地域
访问策略	100 条/入站方向，100 条/出站方向
实例关联安全组个数	无限制
安全组内实例的个数	无限制

注意：
如果您有大量实例需要互访，可以将他们分配到多个安全组内，并通过安全组 ID 的规则配置进行互相授权，允许互访。

典型场景配置

SSH 远程登录 Linux 实例

为了 SSH 远程登录 Linux 实例，您需要给该实例关联的安全组，添加如下入站规则：

来源	协议端口	策略
0.0.0.0/0	TCP:22	允许

注意：您可在来源处设置 地址段 或 安全组。

MSTSC 登录 Windows 实例

为了 MSTSC 登录 Windows 实例，您需要给该实例关联的安全组，添加如下入站规则：

来源	协议端口	策略
0.0.0.0/0	TCP:3389	允许

注意：您可在来源处设置 地址段 或 安全组。

公网 ping 云主机 实例

为了使用 ping 程序测试 云主机 实例的通讯状况，您需要给该实例关联的安全组，添加如下入站规则：

来源	协议端口	策略
0.0.0.0/0	ICMP	允许

注意：您可在来源处设置 地址段 或 安全组。

云主机实例作 Web 服务器

如果您创建的实例作 Web 服务器用，您需要在实例上安装 Web
服务器程序，并给该实例关联的安全组，添加如下入站规则：

注意：您需要先启动 Web 服务器程序，再查看端口是否设置的是 80 。

来源	协议端口	策略
0.0.0.0/0	TCP:80	允许

使用 FTP 上传或下载文件

如果您需要使用 FTP 软件向
云主机实例上传或下载文件，您需要给该实例关联的安全组，添加如下入站规则：

注意：您需要在实例上先安装 FTP 服务器程序，再查看 20/21 端口是否正常工作。

来源	协议端口	策略
0.0.0.0/0	TCP:22,21	允许

快速入门

安全组是腾讯云提供的实例级别防火墙，可以对任意云服务器进行入/出流量控制。

1. 登录 云服务器控制台 ，在左导航窗格中单击【安全组】。
2. 单击【新建】按钮，输入安全组的名称（例如 my-security-group），选择模板创建或自定义创建，确认出入站规则后，单击【确定】。
3. 在安全组列表右侧单击【加入实例】按钮，勾选需要关联的云主机，即可完成安全组关联云主机的操作。

或者

您还可以进入云主机列表页，查看或修改某云主机已绑定的的安全组。在【云主机】列表页选择需要调整安全组的云主机，右侧单击【更多】>【配置安全组】，选择安全组绑定。

（例如：允许来自您本地计算机（IP：186.23.55.90）通过 HTTP 请求云服务器，可以创建一条类似下图的规则。）

操作指南

您可以使用云服务器控制台进行创建、查看、更新和删除等操作管理安全组及安全组规则。

创建安全组

1. 打开 控制台-安全组 。
2. 在左侧导航窗格中，单击【安全组】。
3. 单击【新建】按钮。
4. 输入安全组的名称（例如：my-security-group）并提供说明。
5. 单击【确定】，完成创建。

向安全组中添加规则

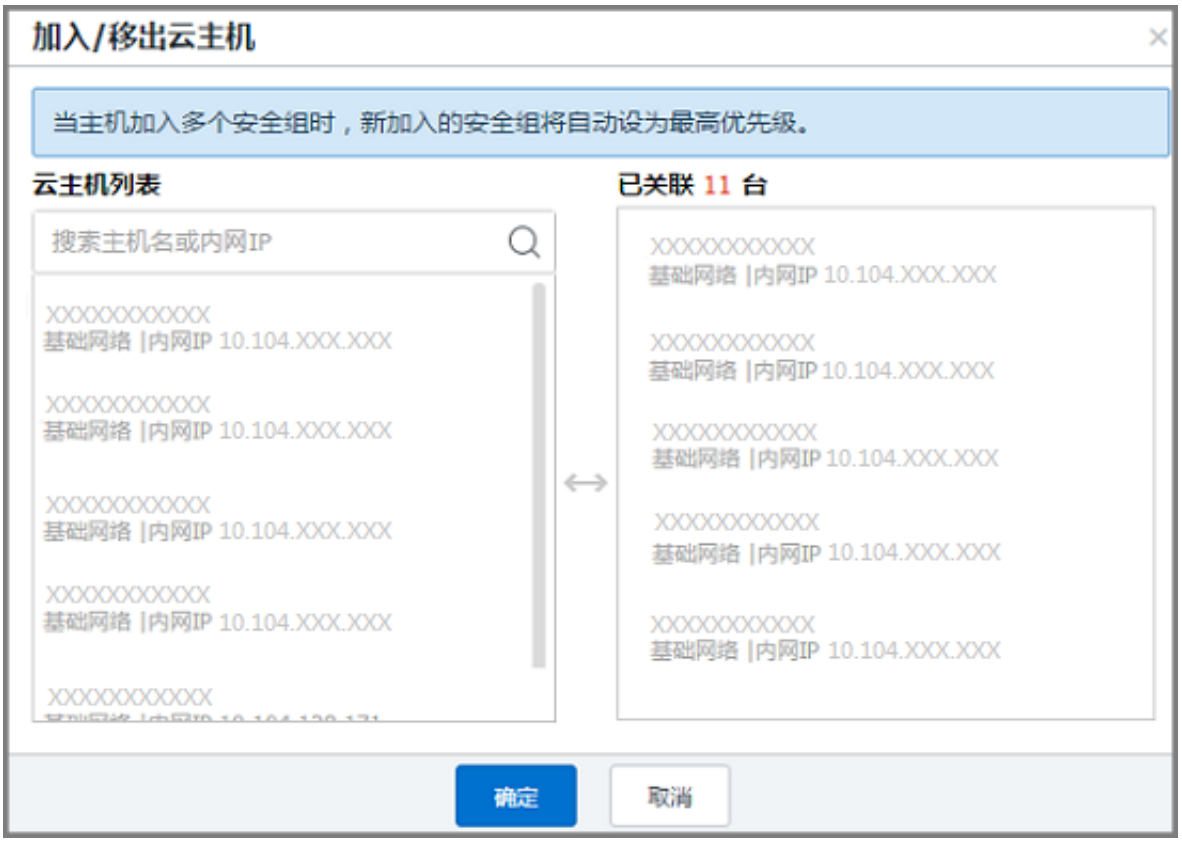
1. 打开 控制台-安全组 。
2. 在左侧导航窗格中，单击【安全组】。
3. 选择需要更新的安全组，单击【安全组ID】。
   详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
4. 在入/出站规则选项卡上，单击【编辑】。从选项卡中选择用于入/出站规则的选项，然后填写所需信息，完成后，单击【保存】。

配置 CVM 实例关联安全组

1. 打开 控制台-云主机 。
2. 在左侧导航窗格中，单击【云主机】。
3. 在需要配置安全组的实例右侧操作栏中，单击【更多】，单击【配置安全组】。
4. 在配置安全组对话框中，从列表中选择一个或多个安全组，单击【确定】。

或者

1. 打开 控制台-安全组。
2. 单击左侧导航窗格中的【安全组】。
3. 选择需要关联的安全组，单击操作栏中的【加入实例】或【移出实例】按钮。
4. 在加入/移出云主机弹出框中，添加或删除需要关联本安全组的云主机，单击【确定】。



导入导出安全组规则

1. 打开 控制台-安全组。
2. 在左侧导航窗格中，单击【安全组】。
3. 选择需要更新的安全组单击【安全组ID】。详细信息窗格内会显示此安全组的详细信息，以及可供您使用入站规则和出站规则的选项卡。
4. 从选项卡中选择用于入/出站规则的选项，然后单击【导入规则】按钮。如原来您已有规则，则推荐您先导出现有规则，新规则导入将覆盖原有规则；如原来为空规则，则可先导出模板，编辑好模板文件后，再将文件导入。

克隆安全组

1. 打开 控制台-安全组。
2. 在左侧导航窗格中，单击【安全组】。
3. 单击列表中安全组对应【克隆】按钮。
4. 在克隆安全组对话框中，选定目标地域、目标项目后，单击【确定】。若新安全组需关联 CVM，请重新进行安全组配置。

删除安全组

1. 打开 控制台-安全组。
2. 在左侧导航窗格中，单击【安全组】。
3. 单击列表中安全组对应【删除】按钮。
4. 在删除安全组对话框中，单击【确定】。若当前安全组有关联的 CVM，则需要先解除安全组才能进行删除。

服务器常用端口

如下是服务器常用端口介绍，关于 Windows 下更多的服务应用端口说明，请参考微软官方文档（Windows 的服务概述和网络端口要求）。

端口	服务	说明
21	FTP	FTP 服务器所开放的端口，用于上传、下载。
22	SSH	22 端口就是 SSH 端口，用于通过命令行模式远程连接 Linux系统服务器。
25	SMTP	SMTP 服务器所开放的端口，用于发送邮件。
80	HTTP	用于网站服务例如 IIS、Apache、Nginx 等提供对外访问。
110	POP3	110 端口是为 POP3（邮件协议 3）服务开放的。
137、138、139	NETBIOS 协议	其中 137、138是 UDP 端口，当通过网上邻居传输文件时用这个端口。而 139 端口：通过这个端口进入的连接试图获得 NetBIOS/SMB 服务。这个协议被用于 Windows 文件和打印机共享和 SAMBA。
143	IMAP	143 端口主要是用于“Internet Message AccessProtocol”v2（Internet 消息访问协议，简称 IMAP），和 POP3 一样，是用于电子邮件的接收的协议。
443	HTTPS	网页浏览端口，能提供加密和通过安全端口传输的另一种 HTTP。
1433	SQL Server	1433 端口，是 SQL Server 默认的端口，SQL Server 服务使用两个端口：TCP-1433、UDP-1434

端口	服务	说明
		。其中 1433 用于供 SQL Server 对外提供服务，1434 用于向请求者返回 SQL Server 使用了哪个 TCP/IP 端口。
3306	MySQL	3306 端口，是 MySQL 数据库的默认端口，用于 MySQL 对外提供服务。
3389	Windows Server Remote Desktop Services（远程桌面服务）	3389 端口是 Windows 2000(2003) Server 远程桌面的服务端口，可以通过这个端口，用“远程桌面”连接工具来连接到远程的服务器。
8080	代理端口	8080 端口同 80 端口，是被用于 WWW 代理服务的，可以实现网页浏览，经常在访问某个网站或使用代理服务器的时候，会加上“:8080”端口号。另外 Apache Tomcat web server 安装后，默认的服务端口就是 8080。

API 概览

安全组相关接口如下：

接口功能	Action ID	功能描述
查询安全组列表	DescribeSecurityGroups	用于查询已经存在的安全组。
创建安全组	CreateSecurityGroup	用于创建新的安全组。
删除安全组	DeleteSecurityGroup	用于删除新的安全组。
修改安全组名称	ModifySecurityGroupAttributes	用于修改已经存在的安全组的属性信息，包括名称和描述。
查询安全组规则	DescribeSecurityGroupPolicy	用于查询已经存在的安全组的规则。
修改安全组规则	ModifySecurityGroupPolicy	用于修改已经存在的安全组的规则。
查询安全组关联的实例列表	DescribeInstancesOfSecurityGroup	用于查询已关联指定的安全组的云服务器。
修改实例关联的安全组	ModifySecurityGroupsOfInstance	用于修改指定云服务器关联的安全组。
查询关联的安全组列表	DescribeAssociateSecurityGroups	查询有哪些安全组的出站或入站规则中包含了输入的安全组 ID。

内网访问

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，且同地域下内网通信完全免费，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）。

> 注意：
> 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 CLB 、 CVM 实例之间内网互访、 CVM 实例与其他云服务（如 CDN、CDB 等）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：初始内网 IP 地址由腾讯云自动在 VPC 网段中任意分配一个地址，用户可在

10.[0 - 255].0.0/8

、

172.[0 - 31].0.0/16

和

192.168.0.0/16

三个网段内为云服务器实例自定义内网 IP
地址，具体的取值范围由实例所在私有网络决定，更多内容可以参考 私有网络和子网 。

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	10.225.30.181 10.225.30.223
	上海	10.236.158.114 10.236.158.106
	北京	10.53.216.182 10.53.216.198
	上海金融	10.48.46.77 10.48.46.27
	深圳金融	100.83.224.91 100.83.224.88

	北美	10.116.19.188 10.116.19.185
	香港	10.243.28.52 10.225.30.178
	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

内网 DNS 设置

当网络解析出现错误时，用户可以手动进行内网 DNS 设置。设置方法如下：

- 对于 Linux 系统用户。在云服务器上，通过编辑

  /etc/resolv.conf

  文件，修改云服务器 DNS 。
  运行命令

  vi /etc/resolv.conf

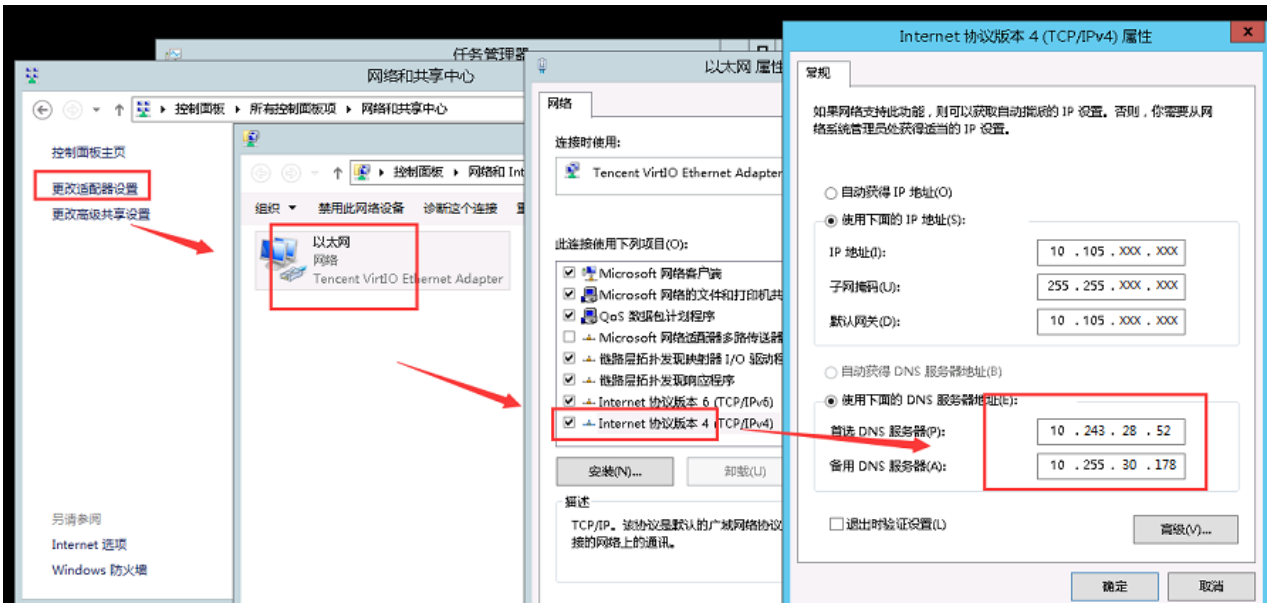
  ，根据上表中对应的不同地域编辑修改 DNS IP。

```
root@VM-90-86-ubuntu:~# vi /etc/resolv.conf
nameserver 10.243.28.52
nameserver 10.225.30.178
options timeout:1 rotate
~
~
```

- 对于 Windows

  系统用户

  。在云服务器上，打开【控制面板】-【网络和共享中心】-【更改适配器设备】，右键单击以太网【属性】，双击【Internet 协议版本4】，修改 DNS 服务器 IP 。



获取实例的内网 IP 地址

使用控制台获取

1. 登录 云服务器控制台 。

2. 云服务器列表中列出了您名下的实例，鼠标移动到云服务器的内网 IP 后，出现复制按钮，单击即可复制内网 IP 。

使用 API 获取

请参考 DescribeInstances 接口 。

使用实例元数据获取

1. 登录云服务器实例。具体登录方法参考 登录 Linux 实例 和 登录 Windows 实例 。

2. 输入命令：

   curl http://metadata.tencentyun.com/meta-data/local-ipv4

   返回值有类似如下结构，即可查看到内网 IP 地址：

```
[root@VM_58_27_centos ~]# curl http://metadata.tencentyun.com/meta-data/local-ipv4
10.XXX.XX.27
```

   有关更多信息，请参阅 实例元数据 。

Internet 访问

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 0 Mbps ，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，此地址不可更改，并且不与您的腾讯云帐号关联。
- 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，请参考 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 私有 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，具体内容可以参考 购买网络带宽 。

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，或包年包月类型实例到期后销毁，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。

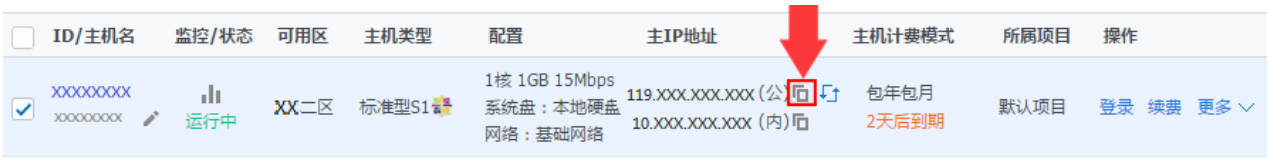
如果您需要一个固定的永久公网 IP 地址，可使用 弹性公网 IP 地址 。

获取实例公网 IP 地址

使用控制台获取

1. 登录 云服务器控制台 。

2. 云服务器列表中列出了您名下的实例，鼠标移动到云服务器的公网 IP
   后，出现复制按钮，单击即可复制该 IP 地址。



注意：
公网 IP 地址通过 NAT 映射到内网 IP 地址。因此，如果在实例内部查看网络接口的属性（例如，通过

ifconfig (Linux)

或

ipconfig (Windows)

命令），则不会显示公网 IP 地址。要从实例内部确定实例的公网 IP 地址，可以参考使用实例元数据获取公网 IP 地址 。

使用 API 获取

请参考 DescribeInstances 接口 。

使用实例元数据获取

1. 登录云服务器实例。具体登录方法参考 登录 Linux 实例 和 登录 Windows 实例 。
2. 输入命令：

   curl http://metadata.tencentyun.com/meta-data/public-ipv4

   返回值有类似如下结构，即可查看到公网 IP 地址：

   有关更多信息，请参阅 实例元数据 。

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。

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 ：弹性网卡的主要内网 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：

云服务器配置	弹性网卡数	网卡绑定 IP 数
CPU: 1核 内存: 1G	2	2
CPU: 1核 内存: > 1G	2	6
CPU: 2核	2	10
CPU: 4核 内存: < 16G	4	10
CPU: 4核 内存: > 16G	4	20
CPU: 8~12核	6	20
CPU: >12核	8	30

配置操作指南

云服务器若需要使用弹性网卡，请参照以下配置步骤完成相应内容：

1. 创建弹性网卡 。
2. 弹性网卡 绑定云服务器 。
3. 配置云服务器和私有网络路由表，参见 私有网络与云主机的路由及安全配置 。
4. 进行 云服务器内的弹性网卡配置 。
5. 分配内网 IP 。可根据需求参见 分配内网 IP（云服务器系统内） 或 分配内网 IP（Qcloud 控制台） 。

更多弹性网卡相关操作请参见 弹性网卡操作指南 。

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	CreateNetworkInterface	创建弹性网卡
弹性网卡申请内网 IP	AssignPrivateIpAddresses	弹性网卡申请内网 IP
弹性网卡绑定云主机	AttachNetworkInterface	弹性网卡绑定云主机

弹性公网IP

弹性公网 IP

弹性公网 IP 地址(EIP)，简称弹性 IP 地址或弹性 IP 。是专为动态云计算设计的静态 IP 地址。它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。

例如，如果您需要将自定义域名重新映射到一个新实例的公网 IP 上，映射关系在 Internet 上传播更新可能需要十几个小时至几十个小时的时间，请求仍然将全部被解析到原有实例上，出现这段时间内新实例无法接收到请求的问题。弹性 IP 可以解决这样的问题，快速将请求指向到新的实例。

弹性公网IP类型

腾讯云有两类账户：

- 第一类账户购买的弹性公网IP只是裸实例，后端资源具备公网能力，即创建CVM实例、NAT网关实例、VPN网关实例时指定这些实例有多少公网能力（带宽上限），用什么计费方式（按流量计费、按带宽计费），公网IP和CLB只作为公网出口。后文统一称为“裸IP”。
- 第二类账户在公网IP和CLB上管理公网能力，后端资源只是裸实例。创建公网IP时指定该IP有多少公网能力（带宽上限），用什么计费方式（按流量计费、按带宽计费）。后端的实例(CVM、NAT网关、VPN网关）使用IP上的公网能力。这类IP有三种类型：小时带宽EIP、包月带宽EIP、按流量计费EIP。（由于此类型正在内测阶段，绝大部分用户属于第一种类型。）

如何识别弹性公网IP的类型？

您进入弹性公网IP控制台。

如果没有“带宽”相关的信息，如下图，即为第一类账户。弹性公网IP的类型为裸IP，无任何公网网络属性，需要后端资源购买公网网络后，再通过公网IP或CLB外访。

如果能看到带宽上限的属性，如下图，即为第二类账户。上面可查询EIP的类型。

ID/名称	状态	弹性IP地址	计费模式	绑定资源	资源类型	申请时间	操作
eip-nzw5lm80 未命名	已绑定	119.29.8.26	计费停止	ins-g5nk0eug 未命名	云服务器	2017-12-04 18:21:23	绑定 | 解绑 | 释放
eip-3u1l4vd6 未命名	已绑定	111.230.148.40	计费停止	ins-dn51j540 1234567890 12...	云服务器	2017-12-01 11:33:31	绑定 | 解绑 | 释放

规则与限制

使用规则：

- 弹性 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 地址与腾讯云账户相关联，而不是与某个具体实例相关联。
- 选择、释放弹性 IP 地址，或欠费超过 26 小时之前，弹性 IP 地址会一直与腾讯云账户保持关联。
- 将弹性 IP 地址与实例绑定时，实例的当前公网 IP 地址会释放到基础网络公网 IP 地址池中。如果将弹性 IP 地址与实例解绑时选择了重新分配公网 IP ，实例会很快自动分配到新的公网 IP 地址（无法保证与绑定前的公网 IP 一致）。此外，销毁实例也会断开与弹性 IP 地址的关联。

使用限制：

- 每个腾讯云账户每个地域每天申购次数为 配额数*2 次。
- 每个腾讯云账户每个地域下最多可创建 20 个弹性公网 IP。
- 解绑EIP时，可免费重新分配公网 IP 的次数为每个腾讯云账户每天 10 次。
- 1 个弹性公网 IP 同一时间只能绑定到 1 个 CVM/NAT 网关实例上，支持动态的绑定和解绑。

计费

费用计算

- 闲置费用：没有绑定云产品实例（CVM 或 NAT 网关）时，裸IP和按流量计费EIP将按下表价格收取少量资源占用费用（不足 1 小时则按比例计费，比如闲置30分钟，则按小时单价* 0.5来算，每小时结算 1 次）。

已经绑定云产品实例（CVM 或 NAT 网关）时，弹性 IP 均免费。
建议您主动及时释放不再使用的弹性公网 IP ，以保证 IP
资源的合理利用，并节省您的费用，操作办法详见 释放弹性公网 IP 。

弹性公网 IP 所在地域	未绑定时价格（不足一个小时按比例收取）
大陆地区、法兰克福	0.20 元/小时
香港地域	0.30 元/小时
北美地域、美西地域（硅谷）	0.25 元/小时
新加坡地域	0.30 元/小时

- 公网网络费用
  ：对
  第二类账
  户（非裸IP），创
  建IP的同时还需要支付公网流量费用
  或公网带宽费用。具体价格见定价中心。计费规则见购买公网网络。

欠费处理

- 对裸IP、小时带宽IP和小时流量IP，若用户账户余额小于 0 元且持续超过 2
  个小时后，会免费保留24小时。这24小时期间所有弹性 IP
  地址将保持为不可操作状态，直至续费后帐号余额大于 0 。若 24 + 2
  小时后余额仍为负，这些弹性公网 IP 将自动释放。

操作指南

以下部分介绍如何使用弹性 IP 地址。

申请弹性公网 IP

1. 登录 云服务器控制台。

2. 在左侧导航窗格中，单击【弹性公网 IP】。

3. 单击【申请】按钮，填写地域与数量后单击【确定】。

4. 申请结束后即可在列表中看到您申请的弹性公网 IP ，此时处于未绑定状态。

弹性公网 IP 绑定云产品

1. 登录 云服务器控制台。

2. 在左侧导航窗格中，单击【弹性公网 IP】。

3. 在需要绑定云产品的 EIP 列表项后，单击【绑定】。（若绑定时， EIP 已绑定了实例，此按钮将为不可用状态，请先解绑。）

4. 在弹出框中选择您需要绑定的云产品类型，并选择相应的云产品实例 ID，单击【绑定】按钮即可完成与云产品的绑定。

弹性公网 IP 解绑云产品

1. 登录 云服务器控制台。

2. 在左侧导航窗格中，单击【弹性公网 IP】。

3. 在已绑定云产品的 EIP 列表项后，单击【解绑】按钮。

4. 点击【确定】。

注意：
解绑后云产品实例可能会被分配新的公网 IP ，可能与绑定前公网 IP 不一致。

释放弹性公网 IP

1. 登录 云服务器控制台。
2. 在左侧导航窗格中，单击【弹性公网 IP】。
3. 在需要释放的 EIP 列表项后，单击【释放】按钮。
4. 单击【确认】完成释放。

异常排查

弹性 IP 地址可能出现网络不通的异常情况，一般有如下原因：

- 弹性 IP 地址没有绑定云产品。具体绑定方法见 弹性公网 IP 绑定云产品 。
- 安全策略无效。查看是否有生效的安全策略（安全组或网络 ACL）。如果绑定的云产品实例有安全策略，例如：禁止 8080 端口访问，那么弹性公网 IP 的 8080 端口也是无法访问的。

EIP 直通

使用场景

用户通过 EIP 访问外网时可选 NAT 模式或 EIP 直通模式，当前默认 NAT 模式。

- NAT 模式下 EIP 在本地不可见。
- EIP 直通后 EIP 在本地可见，在做配置时无须每次手动加入 EIP 地址，可降低开发成本。

注意：
目前 EIP 直通通过白名单控制，仅支持 VPC 内的设备。

操作步骤

一、下载 EIP 配置脚本

由于 EIP 直通过程会导致网络中断，您需先下载 EIP 直通脚本并上传至 CVM。步骤如下：

1. 下载 EIP 直通配置脚本，该步骤可选。下载路径：
   - Linux 脚本下载
   - Windows 脚本下载

   注意：
   Linux 脚本支持系统版本 CentOS 6.x、CentOS 7 和 Ubuntu。

2. 脚本下载到本地后，上传至需要进行 EIP 直通的云主机中。

二、开启 EIP 直通

1. 登录 云服务器控制台。

2. 在左侧导航窗格中，点击【弹性公网IP】。

3. 在选择列表【操作】一列中，单击【EIP 直通】按钮开通即可。

三、运行 EIP 直通脚本

1. 登录到需要 EIP 直通的 CVM 云主机。

2. 运行 EIP 直通脚本。具体方法：

   - Linux 操作系统 CentOS 下：

     eip_direct.sh install XX.XX.XX.XX

     其中，

     XX.XX.XX.XX

     为 EIP 地址，可选填。

   - Windows 操作系统下：

     eip.bat XX.XX.XX.XX

     其中，

     XX.XX.XX.XX

     为 EIP 地址。

注意：

- 脚本仅支持 eth0，暂不支持辅助网卡。
- NAT 网关可绑定开通直通模式的 EIP，但无直通效果。