私有网络

常见问题

产品文档

腾讯云

【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。

文档目录

常见问题
通用类
概念相关

最近更新时间：2020-08-24 16:41:29

如何实现私有网络不同子网内的通信?

- 每个私有网络默认内网互通，您可以在对应路由表中看到一条默认路由，该路由即表示该私有网络下所有资源内网互通。
- 如果是不同私有网络的子网，则内网不互通，需要使用 对等连接 或 云联网 才能实现通信。

能否将服务器部署在同一私有网络下的不同可用区中?

可以。VPC 具有地域属性（如广州、北京、首尔），VPC 内子网具有可用区属性（如广州一区、广州二区），同一 VPC 内的子网可以部署在同一地域的不同可用区中。而云服务器的可用区属性继承自其所属子网，在可用区的子网下购买服务器，即可实现将服务器部署在不同可用区。

如何实现不同可用区中云服务器和数据库的通信?

- 相同 VPC：默认互通，如果不通，请优先排查 安全组 及 网络 ACL 等防火墙策略。
- 不同 VPC：默认隔离，如需互通，您可以通过 对等连接 或 云联网，实现两个 VPC 的内网互通。

每个私有网络最多可为云产品实例提供多少个内网 IP 地址?

每个私有网络最多可为云产品实例提供65533个内网 IP 地址。

什么是 CIDR?

CIDR（Classless Inter-Domain Routing）即无类别域间路由，由您指定的独立网络空间地址块，通过 IP 和掩码结合，实现对网络的整体划分。它消除了传统的 A 类、B 类和 C 类地址以及划分子网的概念，更加有效地分配了 IP 的地址空间。在创建私有网络和子网时，需要以 CIDR 的形式创建对应的网段，例如，需创建范围为 `10.0.16.0 - 10.0.17.255` 的网段，则：
`10.0.16.0 - 10.0.17.255` 转换为二进制为 `00001010.00000000.00010000.00000000 - 00001010.00000000.00010001.11111111`，前23位相同，转换成 CIDR 的形式为 `10.0.16.0/23`。

网段和 IP 相关

最近更新时间：2020-05-27 09:52:28

VPC 和子网的网段有什么限制?

腾讯云 VPC CIDR 支持使用以下私有网段中的任意一个：

- 10.0.0.0 - 10.255.255.255（掩码范围需在16 - 28之间）
- 172.16.0.0 - 172.31.255.255（掩码范围需在16 - 28之间）
- 192.168.0.0 - 192.168.255.255（掩码范围需在16 - 28之间）

子网的 CIDR 必须在私有网络的 CIDR 内或相同。

VPC 和子网的网段可以修改吗?

- 您在创建私有网络和子网时，需要指定其 CIDR，一旦创建即不可更改。
- 如果您因为私有网络网段重叠而无法建立对等连接，推荐您使用限制粒度更小的 云联网（子网网段不重叠即可），或对私有网络下实例进行迁移。VPC 间迁移请参考 切换私有网络服务。

如何处理因 VPC 网段冲突而无法建立对等连接的问题?

建立对等连接时，要求两端 VPC 的 CIDR 不可以重叠，否则无法建立对等连接。

- 如果您两端 VPC 中，需要通信的子网网段不重叠，可以使用 云联网 来实现通信。云联网可以将 VPC 通信时的网段限制缩小到子网层面。
  例如，您需要通信的两个 VPC 网段均为10.0.0.0/16，但子网分别为10.0.1.0/24和10.0.2.0/24，则可以通过云联网实现通信。更多信息，请参考 云联网产品文档。
- 如果云联网仍不能满足您的需求，则需要将重叠子网内的资源进行迁移。
  - 云服务器更换子网，请参考 更换实例子网。
  - VPC 间迁移，请参考 切换私有网络服务。

VPC 内资源（CVM、数据库等）是否支持修改内网 IP?

- 云服务器主网卡的主内网 IP 支持修改，辅助网卡的主内网 IP 不支持修改，详情请参见 修改内网 IP 地址。
- 内网负载均衡（CLB）/ 云数据库（TencentDB）不支持修改内网 IP。

VPC 内的云服务器或数据库能否切换到其它 VPC?

- 目前支持云服务器、云数据库 MySQL的迁移，暂不支持其他数据库的迁移。
- 云服务器可从当前 VPC 迁移至同账户下的其他 VPC 内，详细操作步骤和注意事项，请参见 切换私有网络服务。

- 云数据库 MySQL 可从当前 VPC 迁移至同账户下的其他 VPC 内，详细操作步骤和注意事项，请参见 切换网络。

弹性公网 IP 有什么作用?

弹性公网 IP 适用于以下场景：

1. **容灾**
   我们强烈建议您使用弹性公网 IP 来容灾。当您的某台服务器无法正常提供服务时，您可以将这台机器上的弹性公网 IP 解绑，并重新绑定到健康的机器上，帮您快速恢复服务。
2. **保留特定公网 IP**
   当您需要保留账户中的某个特定公网 IP 时，可将其转换为弹性公网 IP，绑定设备后，即可使用该 IP 进行公网访问。只要您不进行“释放”操作，该弹性公网 IP 便一直保留在您的账户中。
3. **其他特殊场景**
   当您有其他特殊情况需要替换 IP 时，可通过普通公网 IP 转换为弹性公网 IP，并绑定/解绑弹性公网 IP 的方式来实现。但弹性公网 IP 资源宝贵，单个账号下每个地域会有配额限制，建议您合理规划与使用。

如何保持公网 IP 地址不变?

当您需要保留账户中的某个特定公网 IP 时，可将其转换为弹性公网 IP，绑定设备后，即可使用该 IP 进行公网访问。只要您不进行“释放”操作，该弹性公网 IP 便一直保留在您的账户中。
相关操作指引，请参见 普通公网 IP 转 EIP。

弹性公网 IP 能否再转换为普通公网 IP?

弹性公网 IP 无法再次转换为普通公网 IP。

基础网络相关

最近更新时间：2020-12-14 19:19:34

基础网络和私有网络的区别是?

- 私有网络是用户在腾讯云上建立的一块逻辑隔离的网络空间。
- 私有网络较基础网络而言，拥有更多功能。二者的详细区别与选择，请参见 管理基础网络。

基础网络属性的云服务器能否修改为私有网络属性?

可以，我们提供单台和批量云服务器的基础网络切换至私有网络的服务。详细操作步骤和注意事项，请参见 切换私有网络服务。

> ⚠ 注意：
> 该操作不可逆，请您在操作前务必仔细阅读文档。

私有网络属性的云服务器能否修改为基础网络属性?

不能，我们暂不支持私有网络属性云服务器变更为基础网络属性。私有网络支持的功能更多、更灵活，建议您将基础网络迁移上私有网络。

如何实现基础网络中云服务器与 VPC 中云服务器的通信?

您可以通过 基础网络互通 来实现基础网络和 VPC 的通信。
使用基础网络互通服务，有以下限制：

1. 需要通信的基础网络和 VPC 必须在同一区域（可以在不同可用区，如广州一区和广州二区）。
2. 需要 VPC 的 CIDR（网段范围）为`10.[0-47].0.0/16`（含子集），否则会产生冲突。

如果您的基础网络和 VPC 符合上述条件，可以到控制台对应 VPC 详情页中的基础网络互通处进行配置，关联上需要互通的基础网络云服务器即可。

基础网络中的负载均衡、数据库等资源可以和 VPC 通信吗?

- 终端连接可帮助您实现 VPC 内实例通过内网与基础网络实例通信的功能，其原理是将基础网络实例 IP 与 VPC 内 IP 建立映射，访问该 VPC IP 即访问基础网络实例，支持的基础网络产品包括：传统型 CLB、TencentDB、CMEM、REDIS、MongoDB，不支持跨地域/跨账号。
- 方向：单向（VPC 访问基础网络）。
- 如果有需要，欢迎提供 工单申请。

不同账号的基础网络与 VPC 间能否通信?

暂不支持不同账号的基础网络和 VPC 间资源的（云服务器、数据库等）通信，VPC 支持的功能更多、更灵活，建议您将基础网络迁移上私有网络。

如何解除私有网络与基础网络内云服务器的关联?

您好，解关联步骤如下：

1. 登录 私有网络控制台。
2. 单击需要与基础网络互通的 VPC ID，进入私有网络详情页。
3. 单击【基础网络互通】，在基础网络云服务器列表中选择需要解关联的云服务器，并单击【解除关联】。
4. 单击【确认】，即可完成解关联操作。

详细操作说明，请参见 解除私有网络与基础网络内云服务器关联。

产品配额相关

最近更新时间：2020-12-01 09:38:36

VPC 有配额限制吗？每个账号可创建多少 VPC？

VPC 部分资源有使用配额限制。默认每个账号每个地域可以创建20个私有网络。

申请弹性 IP 失败？每个账号可以申请多少个弹性 IP？

- 每个腾讯云账户在每个地域（Region）可以申请的弹性公网 IP 个数为20个。
- 每个腾讯云账户各个地域每天申购次数为配额数 × 2次（即默认为40次）。解绑 EIP 时，每个账户每天可免费重新分配公网 IP 的次数为10次。

连接类
连接公网

最近更新时间：2020-05-27 10:03:29

如果云服务器在购买时没有分配公网 IP，应该如何申请?

如果您在购买云服务器时没有分配公网 IP，那么无法为该云服务器再申请普通公网 IP，但可以通过 弹性公网 IP 来实现相同功能，操作详情请参见 申请 EIP。

- 弹性公网 IP 是公网 IP 的一种，是某地域下一个固定不变的公网 IP 地址。与普通公网 IP 不同的是，它是与您的账户绑定，即：您可以将一个弹性公网 IP 根据需要与不同的云服务器绑定、解绑（一次仅能绑定一个）。
- 由于弹性公网 IP 的特殊性，如果您申请了弹性公网 IP 但并未绑定实例，需要收取一定的 IP 资源费用，详情请参见 弹性公网 IP 计费说明。

没有公网 IP 地址的实例（云服务器、数据库）如何访问公网?

没有公网 IP 的实例可以申请弹性公网 IP（请参见上一个问题），或者通过 NAT 网关访问公网。
NAT 网关 能够为私有网络内的云服务器提供 SNAT 和 DNAT 功能，如果您有多台云服务器需要通过一个公网 IP 访问公网，可以使用 NAT 网关。

能否为云服务器更换公网 IP?

可以。

- 如果您的云服务器是在购买时分配的普通公网 IP，请参见 更换公网 IP 地址。
- 如果您的云服务器绑定的是弹性公网 IP，您需要 解绑该弹性公网 IP，重新 申请一个弹性公网 IP 或为其绑定已有弹性公网 IP。

> ⚠ 注意：
> 普通公网 IP 转换成弹性公网 IP 后，建议您立即释放，否则，未绑定实例的弹性公网 IP 将会收取一定 IP 资源费用。

能否找回之前使用的公网 IP? 能否申请指定的弹性公网 IP?

- 公网 IP 释放后不能找回。
- 支持找回您使用过、且当前未分配给其它用户的弹性公网 IP，详情请参见 找回公网 IP 地址。

弹性公网 IP 数量达到上限后能否申请增加配额?

由于弹性公网 IP 资源的有限性，每个账号每个地域仅能申请20个，不能申请增加配额。对于无公网 IP 的云服务器，您可以使用 NAT 网关等方式访问公网。

如果云服务器有公网 IP 或弹性公网 IP，所在子网又关联了 NAT 网关，将如何实现公网的访问？

如果一台云服务器有公网 IP 或弹性公网 IP，同时，子网又关联了 NAT 网关，即路由表中设置了该子网访问公网流量的下一跳是 NAT 网关，那么，默认该云服务器访问公网的流量会全部通过 NAT 网关实现。

如果您需要修改优先级，使得云服务器访问公网的流量通过公网IP实现，请参见 调整 NAT 网关和公网 IP 的优先级。

当云服务器通过公网网关或 NAT 网关访问公网时，网络费用是否会收取双份？

不会，网络费用只收取一份。通过公网网关或 NAT 网关访问公网，收取的是公网网关或 NAT 网关的网络费用。

VPC 间通信

最近更新时间：2020-08-25 11:25:31

云服务器/数据库如何内网通信?

VPC 中云服务器与数据库的内网通信在网络层面均为内网 IP 通信，因此无差异。内网 IP 不同场景的通信方式如下：

通信场景	通信方案
不同地域	不同地域的云服务器或数据库属于不同 VPC，通过 对等连接 / 云联网 （同/跨账号均支持）通信
不同可用区	同 VPC： 默认互通 不同 VPC： 通过 对等连接 / 云联网 （同/跨账号均支持）通信
不同VPC	通过 对等连接 / 云联网 （同/跨账号均支持）通信
不同子网	同 VPC：默认互通 不同 VPC： 通过 对等连接 / 云联网 （同/跨账号均支持）通信
跨账号	跨账号 通过 对等连接 / 云联网 （同/跨地域均支持）通信

⚠ 注意：

- 当您通过对等连接或云联网实现跨账号 VPC 间的互联时，需注意如下两点：
  - 资源均属于主账号，因此您创建跨账号对等连接或云联网互通时，请填写对方的主账号。
  - 子账号仅有操作权限，所以如果您的子账号不具备创建对等连接或云联网权限，请向主账号申请权限。
- 同 VPC 下不同子网间（不论是否在同一可用区），**内网默认互通**，如果不通，请优先排查 安全组 及 网络 ACL 等防火墙策略。

如何处理因 VPC 网段冲突而无法建立对等连接的问题?

建立对等连接时，要求两端 VPC 的 CIDR 不可以重叠，否则无法建立对等连接。

- 如果您需要通信的两个 VPC 网段有重叠，但具体的子网网段不重叠，可以使用 云联网 来实现通信。云联网可以将 VPC 通信时的网段限制缩小到子网层面。
  例如，您需要通信的两个 VPC 网段均为 `10.0.0.0/16`，但子网分别为 `10.0.1.0/24` 和 `10.0.2.0/24`，则可以通过云联网实现通信。详情请参见 云联网。
- 如果云联网仍不能满足您的需求，则需要将重叠子网内的资源进行迁移。
  - 云服务器更换子网，详情请参见 更换实例子网。

- VPC 间迁移，详情请参见 切换私有网络服务。

若 VPC1 分别和 VPC2、VPC3 建立了对等连接，那 VPC2 和 VPC3 能互通吗?

不能，对等连接能使 VPC 两两建立互联，但是这种互通关系不发生传递。即当 VPC1 与 VPC2 建立了对等连接，VPC1 和 VPC3 也建立了对等连接时，由于对等连接的不传递性，VPC2 和 VPC3 的流量不能互通。

基础网络互通相关

最近更新时间：2020-09-10 09:51:30

什么是基础网络互通?

基础网络互通指将基础网络内的云服务器关联至指定私有网络，使基础网络中的云服务器可以与私有网络内的云服务器、数据库等云服务通信。更多信息，请参见 管理基础网络。

如何实现基础网络中云服务器与 VPC 中云服务器的通信?

您可以通过 基础网络互通 来实现基础网络和 VPC 的通信。
使用基础网络互通服务，有以下限制：

1. 需要通信的基础网络和 VPC 必须在同一区域（可以在不同可用区，如广州一区和广州二区）。
2. 需要 VPC 的 CIDR（网段范围）为`10.0.0.0/16 – 10.47.0.0/16`（含子集），否则会产生冲突。

如果您的基础网络和 VPC 符合上述条件，可以到控制台对应 VPC 详情页中的基础网络互通处进行配置，关联上需要互通的基础网络云服务器即可。

基础网络中的负载均衡、数据库等资源可以和 VPC 通信吗?

- 终端连接可帮助您实现 VPC 内实例通过内网与基础网络实例通信的功能，其原理是将基础网络实例 IP 与 VPC 内 IP 建立映射，访问该 VPC IP 即访问基础网络实例，支持的基础网络产品包括：传统型CLB、TencentDB、CMEM、REDIS、MongoDB，不支持跨地域/跨账号。
- 方向：单向（VPC 访问基础网络）。
- 如有需要，请提交 工单申请。

不同账号的基础网络与 VPC 间能否通信?

暂不支持不同账号的基础网络和 VPC 间资源的（云服务器、数据库等）通信，VPC 支持的功能更多、更灵活，建议您将基础网络迁移上私有网络。

安全类
VPC 安全相关

最近更新时间：2020-06-29 16:58:10

如何确保 VPC 中云服务器的安全?

VPC 本身是一个逻辑隔离的网络环境，可以通过设置安全组和网络 ACL 来进行流量控制：

- 安全组：提供 CVM 实例级别的网络流量控制，没有允许进出实例的流量将自动被拒绝。
- 网络 ACL：提供子网级别的网络流量控制。

端口与安全组相关

最近更新时间：2020-09-25 14:57:16

端口相关

登录实例前，需要放通什么端口?

一般而言，对于 Linux 实例要放通22号端口，对于 Windows 实例需要放通3389号端口。更多适用于其他实例类型的端口请参考 安全组应用案例。

为什么要开启端口? 如何开启某个端口?

您需要在安全组中开启端口后，才可以使用端口对应的服务。示例：
若想要使用 8080 端口访问网页，需要在安全组开启、放通该端口的情况下，才能实现。
放通某个端口的操作步骤如下：

1. 登录 安全组控制台，单击该实例绑定的安全组，进入详情页。
2. 选择入站规则/出站规则，单击【添加规则】。
3. 填写您的 IP 地址（段）及需要放通的端口信息，选择允许放通。
   详细操作步骤，请参见 添加安全组规则。

为什么修改端口后服务无法使用?

修改服务端口后，还需在对应的安全组开放对应的端口，否则服务不可用。

腾讯云不支持哪些端口?

如下端口存在安全隐患，出于安全因素考虑，运营商将其拦截，导致无法访问。建议您更换端口，不要使用如下端口监听：

协议	不支持端口
TCP	42、135、137、138、139、445、593、1025、1434、1068、3127、3128、3129、3130、4444、5554、5800、5900、9996
UDP	1026、1027、1434、1068、5554、9996、1028、1433、135 - 139

为什么无法使用 TCP 25 端口连接外部地址，如何解禁?

- 为了提升腾讯云 IP 地址发邮件的质量，将默认限制云服务器使用 TCP 25 端口连接外部地址。您可以登录 控制台，将鼠标移动至顶部导航账号处，单击【安全管控】即可看到25端口解封入口。
- 每个账号支持解封5次云服务器，且仅支持预付费包年包月的云服务器，暂不支持按量付费云服务器。

更多端口说明，请参见 服务器常用端口。

安全组相关

为什么安全组中会默认有一条拒绝规则?

安全组规则，是从上至下依次筛选生效的，之前设置的允许规则通过后，其他的规则会默认被拒绝。若是规则放通全部端口，则最后这条拒绝规则是不生效的。出于安全考虑，我们提供该默认设置。

选择安全组不正确，会对绑定该安全组的实例有何影响？该如何解决?

- **问题隐患**
  - 远程连接(SSH) Linux 实例、远程登录桌面 Windows 实例可能失败。
  - 远程 Ping 该安全组下的 CVM 实例的公网 IP 和内网 IP 可能失败。
  - HTTP 访问该安全组下的实例暴露的 Web 服务可能失败。
  - 该安全组下实例访问 Internet 服务可能失败。
- **解决方案**
  - 若发生以上问题，可以在控制台的安全组管理中，重新设置安全组规则，例如：只绑定默认全通安全组。
  - 安全组具体设置规则，请参见 安全组 - 安全组规则。

安全组的方向和策略是什么?

- 安全组策略方向分为出和入，出方向是指过滤云服务器的出流量，入方向是指过滤云服务器的入流量。
- 安全组策略分为**允许**和**拒绝**流量。

安全组策略的生效顺序是什么?

安全组策略的生效顺序是从上至下的。流量经过安全组的策略匹配顺序是从上至下，一旦匹配成功则策略生效。

为什么端口在安全组中放通了，但依然无法访问?

- 实例绑定的其他安全组中拒绝了该端口，且优先级高
- 设置了网络ACL或防火墙

为什么安全组未允许的 IP 仍然能访问云服务器？

可能有以下原因：

- CVM 可能绑定了多个安全组，特定 IP 在其他安全组中被允许。
- 特定 IP 属于审批过的腾讯云公共服务。

使用了安全组是否意味着不可以使用 iptables?

不是。安全组和 iptables 可以同时使用，您的流量会经过两次过滤，流量的走向如下：

- 出方向：实例上的进程 > iptables > 安全组。
- 入方向：安全组 > iptables > 实例上的进程。

云服务器已经全部退还，为什么安全组无法删除？

请查看回收站内是否还有云服务器。安全组绑定了回收站内的云服务器时，同样无法被删除。

安全组克隆时命名能否与目标区域的安全组相同？

不行。命名需保持与目标地域现有安全组名称不同。

安全组跨项目跨地域克隆是否有云 API 支持？

为了方便使用控制台的客户，我们目前提供了控制台支持，暂无直接云 API 支持。您可通过原有的批量导入导出安全组规则的云 API ，间接达到安全组的跨项目跨地域克隆。

安全组跨项目跨地域克隆会否将安全组管理的云服务器一起复制过去？

不会，安全组跨地域克隆，只将原安全组出入口规则克隆，云服务器需另行关联。