专线接入

操作指南

产品文档

腾讯云

文档目录

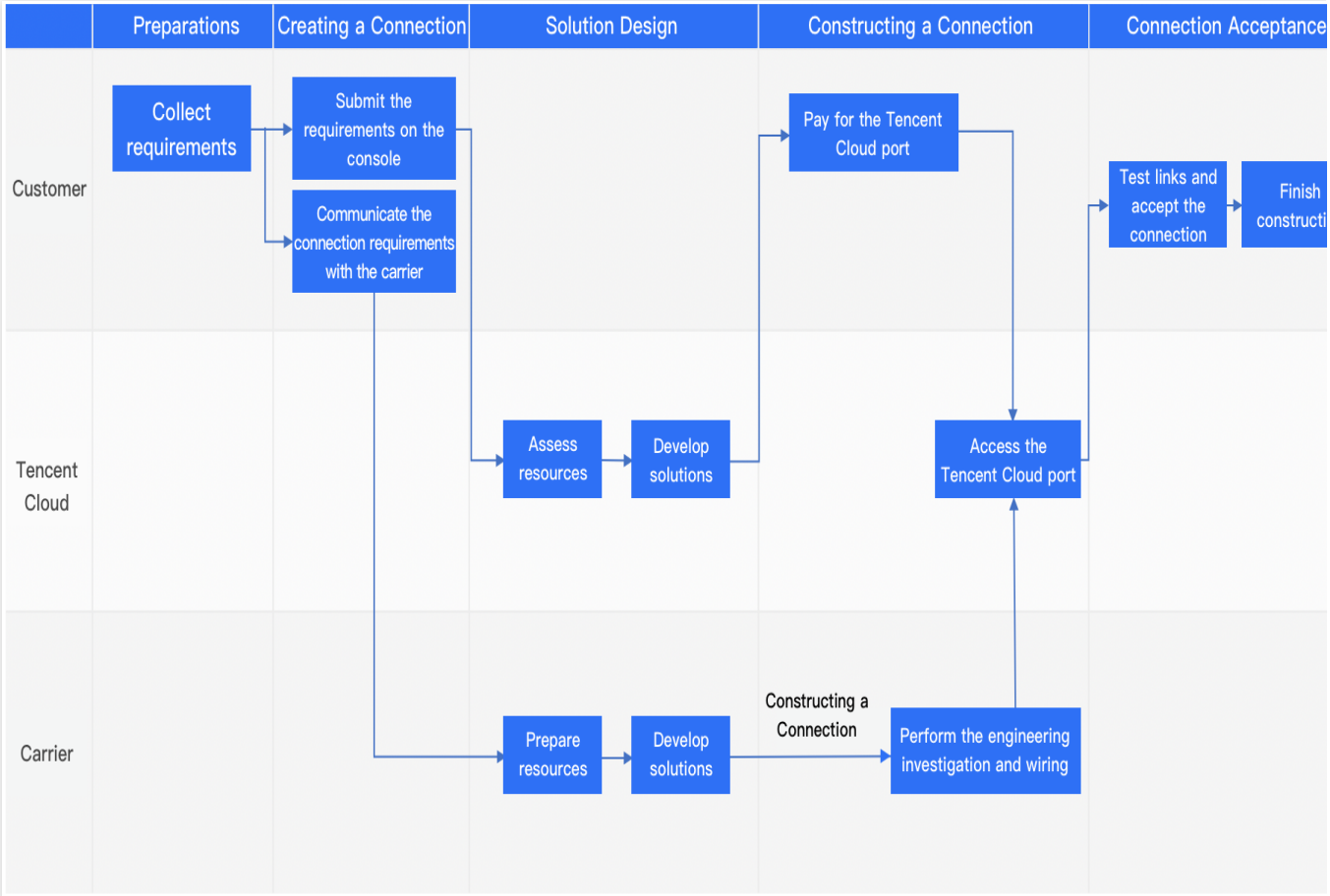
操作指南
物理线路
物理专线接入概述

最近更新时间：2024-11-05 11:05:18

物理线路用于连接本地 IDC 和腾讯云。创建物理线路包括接入前信息确认、控制台申请、运营商工勘铺设专线等工作，整个施工周期约为 2~3 个月。为避免影响您的上云进度，请您提前做好专线上云计划。

创建流程

创建物理线路的流程如下：



1. 准备工作：创建物理专线前，您需要进行接入点信息确认、腾讯云需求和运营商需求整理。
2. 创建物理专线：若您的本地 IDC 与腾讯云接入点不在同一个机房内，则需在腾讯云控制台提交创建申请，并联系符合《专线接入审核标准》的运营商进行需求沟通。若您的本地 IDC 与腾讯云接入点在同一个机房内，则无需联系运营商，待腾讯云设计方案后直接进行专线建设。

3. 方案设计：腾讯云收到您的专线申请后，将进行资源评估和方案设计，并与您确认。同时运营商需要进行资源准备和方案设计，相关费用请咨询运营商。
4. 专线建设：若您的本地 IDC 与腾讯云接入点不在同一个机房内，运营商将根据方案进行工勘、铺设专线。同时您需要在腾讯云控制台支付腾讯云端口费用，完成后腾讯云将进行接入端口配置，配合运营商将物理专线接入腾讯云。若您的本地 IDC 与腾讯云接入点在同一个机房内，则直接联系腾讯云专线经理协调相关资源协助专线建设。

说明：

2021-02-01 起，腾讯云对所有新增接入的物理专线永久减免初装费。

5. 专线验收：专线施工完成后，您需要进行链路测试和验收。

准备工作

创建物理专线前，您需要进行接入点信息确认。

接入点即腾讯云物理专线的网络服务提供点，在保证网络质量的同时减少物理专线成本，建议选择就近接入。腾讯云支持的地域一般具备2个以上接入点，可实现多线容灾。每个接入点的具体地址请 提交工单 咨询。选择接入点时，需要了解以下信息：

地域：地域（Region）是指物理的数据中心的地理区域。腾讯云不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。为了降低访问时延、提高下载速度，建议您就近选择。

运营商：即提供物理专线的资源供应方，如中国移动、中国联通、中国电信等，或者其他符合专线接入审核标准的运营商。

说明：

根据国家相关法律法规和工业和信息化部颁发的[《关于清理规范互联网网络接入服务市场的通知》（信管函2017]32号），使用专线接入服务时，请选择具有相应资质的专线服务商实施专线接入建设。

使用不合规的专线您可能面临国家监管部门的行政处理，导致线路不可用，且您需自行承担相关责任，腾讯云不承担任何责任。

端口：您可以根据实际需要选择光口或者电口。

光口：即用来连接光纤线缆的物理接口。腾讯云提供1G、10G、100G三种端口规格的光口。

电口：即服务器和网络中对 RJ45 等各种双绞线接口的统称，即普通网线。腾讯云提供千兆电口（10/100/1000BASE-T），适用于低带宽的场景。

说明：

100G端口需要提 工单申请。

物理专线建设时，请务必确保 IDC 侧接口模块规格与腾讯云侧接口模块规格一致，模块规格不一致将可能无法正常通信。

如果当前 IDC 侧接口规格与腾讯云侧接口规格不一致，建议更换 IDC 侧模块；如需要更换腾讯云侧端口，请废弃已有接入流程，重新申请新的物理专线端口，发起新的物理专线接入流程。

端口类型		规格
光口	1G光口	SFP - GE - LX - Sm1310，10KM

		SFP - GE - LH80 - SM1550，80KM
	10G光口	SFP - XG - LX - SM1310，10KM
		SFP - XG - LH80 - SM1550，80KM
	100G光口	QSFP - 100G - LR4 - WDM1300，10KM
电口		10/100/1000BASE - T

创建物理专线

场景	操作
IDC 与腾讯云接入点不在同一机房	在腾讯云控制台申请物理专线，具体操作请参见 申请物理专线。同时，您需要联系符合专线接入审核标准的运营商进行需求沟通。
IDC 与腾讯云接入点在同一机房	在腾讯云控制台申请物理专线，具体操作请参见 申请物理专线。

专线建设

本地 IDC 与腾讯云接入点不同机房

专线建设阶段包含运营商的建设和腾讯云的专线建设两个流程并行，具体如下：

运营商建设

1.1.1 运营商工勘。

1.1.2 确认施工方案和相关费用。

1.1.3 运营商发起物理专线建设。

说明：

专线接入至专线接入点机房时，可能会存在入楼光纤或楼内线缆租赁费用，详情请咨询运营主体或线路提供商。

1.1.4 接入机房。

1.1.1 联系专线经理申请进入接入点机房操作，并提供入室工勘人员的姓名、身份证和联系方式。

1.1.2 审批通过后，专线经理会协助工勘人员在2个工作日完成入室。

腾讯云建设

当您在控制台支付腾讯云端口费用后，腾讯云将进行接入端口配置，并配合运营商将物理专线接入腾讯云。

本地 IDC 与腾讯云接入点同机房

本地 IDC 与接入点同机房时，则直接联系腾讯云专线经理协调相关资源协助专线建设。

说明：

专线接入至专线接入点机房时，可能会存在入楼光纤或楼内线缆租赁费用，详情请咨询运营主体或线路提供商。

专线验收

进行专线验收时，您需要完成创建整个专线接入线路，具体请参见 快速入门。然后分别进行压测验收测试、时延测试、和可靠性测试。

压测验收测试：使用网络测试工具 Iperf3 验证 IDC 与腾讯云是否网络互通。

时延测试：使用网络测试工具 Iperf3 验证任意端到端的时延。

可靠性测试：使用网络测试工具 Iperf3 验证端到端通信的丢包情况。

测试项分别为 size1500、count2000 和 size5000、count2000。

说明：

size1500 表示发包表量，即1500个数据包；count2000 表示发包次数，即发包2000次。

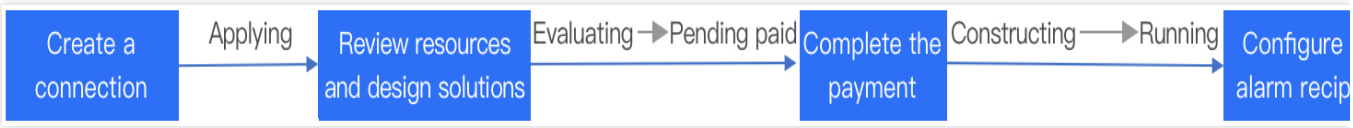
Iperf3 工具相关操作指导请参见 Iperf3 官网 用户指导书。

申请接入物理专线

最近更新时间：2024-11-05 11:05:18

本文将介绍如何在腾讯云控制台创建物理专线。

操作流程



说明：

物理专线新建完成后，请及时联系您在腾讯侧的商务经理，配合您完成物理专线建设工作。如果您在腾讯侧没有商务经理，可提交 工单申请。

1. 创建物理专线：在控制台同步您的物理专线需求，完成后专线状态为“申请中”。
2. 资源评估和方案设计：腾讯云收到您的专线需求后，将进行资源评估，专线状态流转为“评估中”；随后专线经理与您同步确认专线设计方案，完成后专线状态为“待付款”。
3. 支付费用：在控制台完成付款后，专线状态流转为“建设中”。您还需要联系运营商和腾讯云共同完成专线建设和专线验收，并在控制台确认验收，完成后专线状态为“运营中”。

说明：

2021-02-01 起，腾讯云对所有新增接入的物理专线永久减免初装费。申请流程中将取消“待付款”状态，从“评估中”直接流转为“建设中”。

操作步骤

步骤一：创建物理专线

建设申请发起后，物理专线状态将转换为“申请中”，腾讯云将在3个工作日内进行资源评估和方案设计。

1. 登录 专线接入控制台，在“物理专线”页面上方单击 **+新建**。
2. 在“确认接入信息”页面填写以下信息，然后单击**确定**。

参数	描述	备注
专线名称	请自定义您的物理专线的名称。	支持更改。
地域	物理的数据中心的地理区域。腾讯云不同地域之间完全隔离，保证不同地域间最大程度的稳定性和容错性。	为了降低访问时延、提高下载速度，建议您就近选择。

接入点	腾讯云物理专线的网络服务提供点，建议选择就近接入，具体接入点请参见 专线接入点。	腾讯云支持的地域一般具备2个以上接入点，可实现双线容灾。
物理线路提供商	具有合规电信业务经营资质的运营商。	中国电信、中国移动、中国联通、本地线路、中国其他、境外其他。
端口规格	腾讯云提供1G、10G和100G的端口规格。	100G的端口规格需要提 工单申请。
端口类型	若选择端口规格为 1G，您可以根据实际需要选择光口或者电口类型。若选择端口规格为 10G，端口类型仅可选择光口类型。	按带宽选择对应的接口类型，可咨询您的专线服务商或腾讯云架构师 / 售后经理提供技术支持。
带宽上限	若端口规格选择 1G，则可设置的带宽上限范围为 1Mbps-1000Mbps。 若端口规格选择 10G，则可设置的带宽上限范围为 1Mbps-10000Mbps。	-
IDC 地址	用户 IDC 具体地址。	-
联系人	申请物理专线的客户侧联系人。	张三。
联系方式	申请物理专线的客户侧联系人的联系方式。	-
申请者 Email	物理专线申请者电子邮件。	XXXX@XXXX.com。

步骤二：资源评估和方案设计

腾讯云专线经理接到您的专线需求后，将综合评估专线资源，物理专线状态流转为“评估中”；随后通过电话和您沟通专线接入服务细节，确认物理专线可以接入后，物理专线状态流转为“待付款”。当出现以下几种情况时，物理专线可能出现申请驳回：

信息不准确 ：接入信息不完整，请根据专线经理反馈，更新申请信息，重新发起申请。

资源不足： 接入端口或上连带宽资源不满足，请根据专线经理反馈，在专线资源具备后，重新发起申请。

不具备资格 ：物理专线仅对规模型企业客户提供服务，请更新企业资质后，重新发起专线申请。

步骤三：支付费用

物理专线申请评估通过后，您需要在控制台完成付款。控制台付款成功后，专线经理将立即受理接入请求，并协调相关资源协助建设接入，物理专线状态流转为“建设中”。付款步骤如下：

1. 登录 专线接入控制台 。
2. 在物理专线列表中找到待付款的物理专线，单击**去付款**。
3. 在弹窗内再次确认专线接入信息后，单击**确认**。
4. 进入计费平台完成付款。

步骤四：配置告警接收对象

创建物理专线后，腾讯云将自动为该物理专线配置以下针对带宽利用率的指标告警，帮助您监控、运维物理专线。

指标项	统计周期	条件	条件数值	持续周期	策略
带宽利用率	一分钟	>=	80%	5个周期	每天告警一次

自动创建的默认告警策略未配置接受人信息，仅支持控制台告警，您可以自行配置告警接收对象，详情请参见 配置告警。

后续操作

运营商完成物理专线建设后，您需要同时创建专线网关、专用通道来测试并验收，完成验收后物理专线状态进入“运营中”状态。

创建专线网关

创建专用通道

配置路由表

管理物理专线

最近更新时间：2024-11-05 11:05:18

专线运行后，您可在控制台进行查看专线信息、修改带宽、删除专线、添加标签等操作。

查看专线信息

1. 登录 专线接入控制台 ，并在左侧导航栏单击**物理专线**。
2. 在物理专线列表中单击待查看的专线名称。
3. 在专线信息详情页面查看该物理专线的基本信息，包含专线供应商、接口类型、接入点、带宽等信息。

修改专线带宽

若当前物理专线带宽不能满足您的业务需求时，可以在控制台修改物理专线带宽。
1. 登录 专线接入控制台，并在左侧导航栏单击**物理专线**。
2. 在目标专线的“带宽”列单击

。
3. 在编辑框中修改带宽值，然后单击**确定**。
说明：
若当前物理专线下没有创建专用通道，则调整带宽不小于1Mbps，且不超过其端口带宽值。
若当前物理专线下已创建专用通道，则调整带宽不低于所有通道的最大带宽值，且不超过其端口带宽值。
目前物理专线的各规格端口带宽上限分别为：
1G 电口：1000Mbps
1G 光口：1000Mbps
10G 光口：10000Mbps
100G 光口：100000Mbps

添加标签

为方便对您账户中物理专线的查找和管理，您可以为物理专线添加标签，具体操作如下：
1. 登录 专线接入控制台，并在左侧导航栏单击**物理专线**。
2. 在物理专线列表中单击目标物理专线右侧“操作”列的**编辑标签**。

3. 在“编辑标签”页面分别在下拉菜单中选择标签键和标签值。若现有标签不符合您的需要，请单击**标签管理**以新建标签。
4. 使用标签查找物理专线。
5. 在“物理专线”页面上方单击放大镜图标左侧的编辑框，并在下拉菜单中选择**标签**。
6. 在编辑框中输入标签信息，单击放大镜图标。
7. 使用标签管理物理专线。
8. 在“物理专线”页面上方单击

图标。
9. 在“自定义列表字段”页面勾选目标标签，并单击**确定**。
完成后，标签键会出现在物理专线列表。

删除专线

当您不需要再使用物理专线时，可以裁撤物理专线。
1. 登录 专线接入控制台，并在左侧导航栏单击**物理专线**。
2. 在物理专线列表中单击待裁撤专线右侧“操作”列的**删除**。
3. 在“确认删除”对话框中勾选**确认删除**，并单击确认。

说明：
发起裁撤申请后，该物理专线将停止计算端口月租费用。

共享物理专线

最近更新时间：2024-01-13 16:40:45

您可共享其他账号的物理专线建设专用通道，也可将自己账号下的物理专线共享给其他腾讯云客户。
如果您是向腾讯云合作伙伴购买物理专线服务，一般是共享物理专线模式，您需向合作伙伴获得合作伙伴物理专线账号的 UIN、物理专线实例 ID 以及 VLANID。操作详情请参见 申请通道 。

专线网关
专线网关概述

最近更新时间：2024-11-05 11:05:18

专线网关用于连接腾讯云 VPC 与物理专线（专用通道），是专线网络的流量入口。专线网关分为私有网络专线网关和云联网专线网关，您可以根据不同的场景进行选择。

使用限制

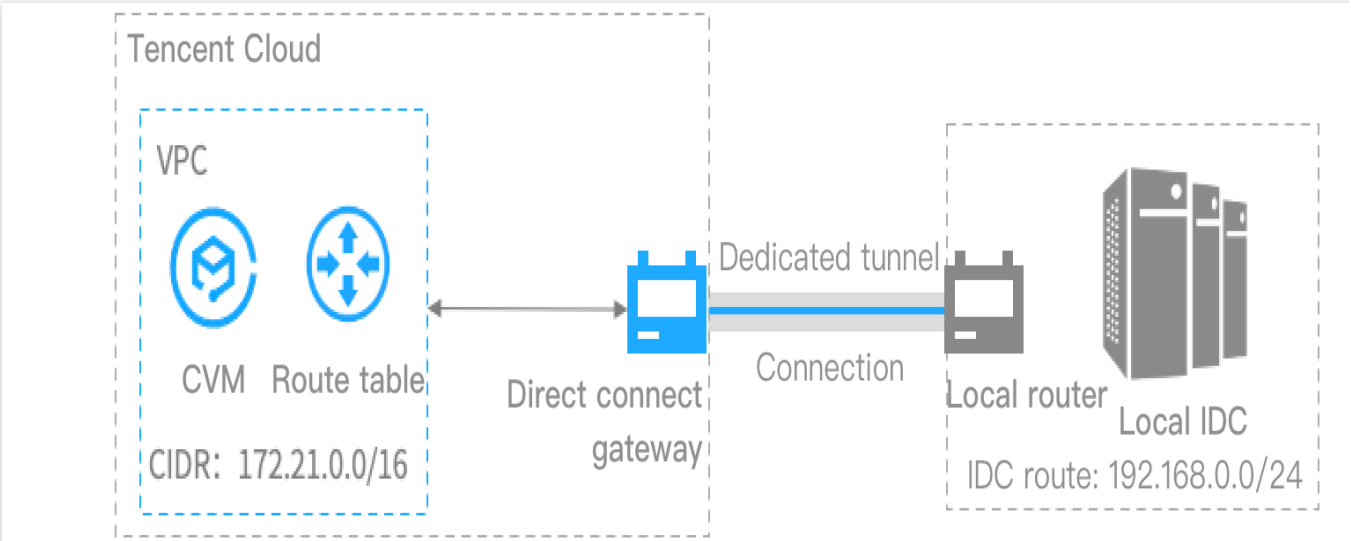
标准型专线网关支持传递辅助 CIDR，但需要遵循如下限制：
标准型专线网关支持传递10个辅助 CIDR。
NAT 型专线网关不支持传递辅助 CIDR。
长时间无业务的专线网关（即同时满足以下条件），将会被系统清理：
创建超过180天
持续90天未绑定专用通道
持续90天内无业务流量

私有网络专线网关

在专线网络架构中，专用通道的模式对 IDC 到腾讯云 VPC 方向的路由目的网段有影响，具体如下表所示：

专用通道模式	IDC 侧上云路由
静态	IDC 到腾讯云 VPC 方向的路由规则，由用户在本地路由器配置。
BGP	IDC 侧通过 BGP 协议学习到 VPC CIDR。

例如某专线网络架构中，使用私有网络专线网关实现腾讯云 VPC 与一个数据中心连接，不同模式的专用通道下路由配置如下：
若专用通道为静态模式，IDC 到腾讯云 VPC 方向的路由目的网段，由用户在本地路由器配置，如 VPC CIDR（172.21.0.0/16）。



VPC route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway	Configured in the Tencent Cloud console

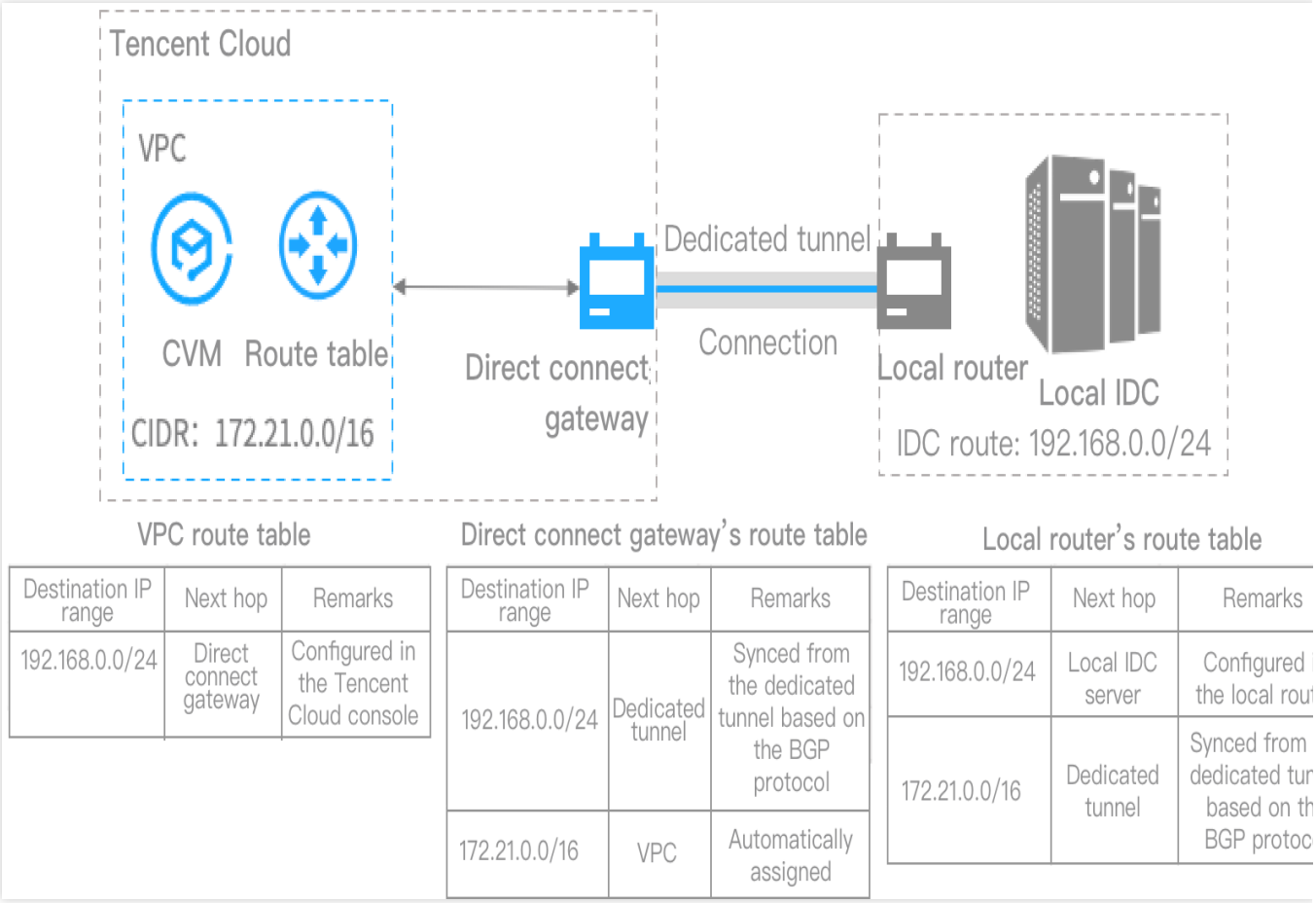
Direct connect gateway's route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Dedicated tunnel	Configured through the **CPE IP Range** parameter when the dedicated tunnel is created via the console
172.21.0.0/16		Automatically assigned

Local router's route table

Destination IP range	Next hop	Remark
192.168.0.0/24	Local IDC server	Configu in the lo route
172.21.0.0/16	Dedicated tunnel	Configure the loc router

若专用通道为 BGP 模式，IDC 到腾讯云 VPC 方向的路由目的网段，为本地路由器通过 BGP 协议学习到的 VPC CIDR（172.21.0.0/16）。



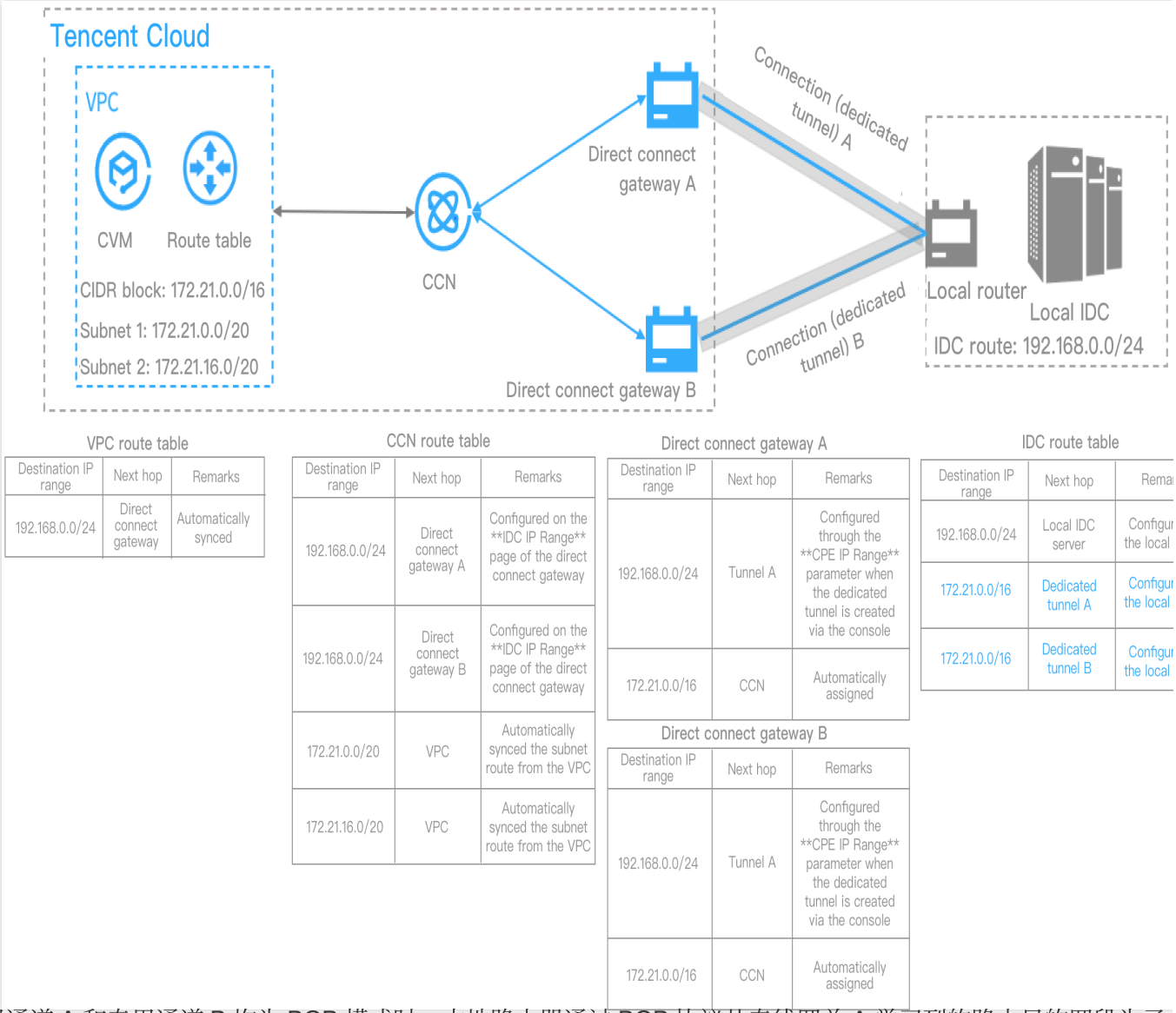
云联网专线网关

一个云联网专线网关可以关联一个云联网和多个专用通道，实现云联网内的多个 VPC 与不同的 IDC 互联。在专线网络架构中，创建云联网专线网关的时间、专用通道的模式均对 IDC 到腾讯云 VPC 方向的路由目的网段有影响，具体如下表所示：

创建时间	专用通道模式	IDC 侧上云路由
2020 年 9 月 15 日零点前	静态	IDC 到腾讯云 VPC 方向的路由规则，由用户在本地路由器配置。
	BGP	IDC 侧通过 BGP 协议学习到 VPC 子网 CIDR。
2020 年 9 月 15 日零点后	静态	IDC 到腾讯云 VPC 方向的路由规则，由用户在本地路由器配置。
	BGP	IDC 侧通过 BGP 协议学习到 VPC CIDR。

例如在某专线网络架构中，专线网关 A 为 2020 年 9 月 15 日零点前创建，专线网关 B 为 2020 年 9 月 15 日零点后创建。不同专用通道模式的路由流转如下：

当专用通道 A 和专用通道 B 均为静态模式时，IDC 到腾讯云 VPC 方向的路由目的网段为用户在本地路由器配置的 VPC CIDR（172.21.0.0/16）。专线网关 A 和专线网关 B 的路由完全一致，因此本地 IDC 的流量均匀发送至两个专线网关。



VPC route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway	Automatically synced

CCN route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway A	Configured on the **IDC IP Range** page of the direct connect gateway
192.168.0.0/24	Direct connect gateway B	Configured on the **IDC IP Range** page of the direct connect gateway
172.21.0.0/20	VPC	Automatically synced the subnet route from the VPC
172.21.16.0/20	VPC	Automatically synced the subnet route from the VPC

Direct connect gateway A

Destination IP range	Next hop	Remarks
192.168.0.0/24	Tunnel A	Configured through the **CPE IP Range** parameter when the dedicated tunnel is created via the console
172.21.0.0/16	CCN	Automatically assigned

Direct connect gateway B

Destination IP range	Next hop	Remarks
192.168.0.0/24	Tunnel A	Configured through the **CPE IP Range** parameter when the dedicated tunnel is created via the console
172.21.0.0/16	CCN	Automatically assigned

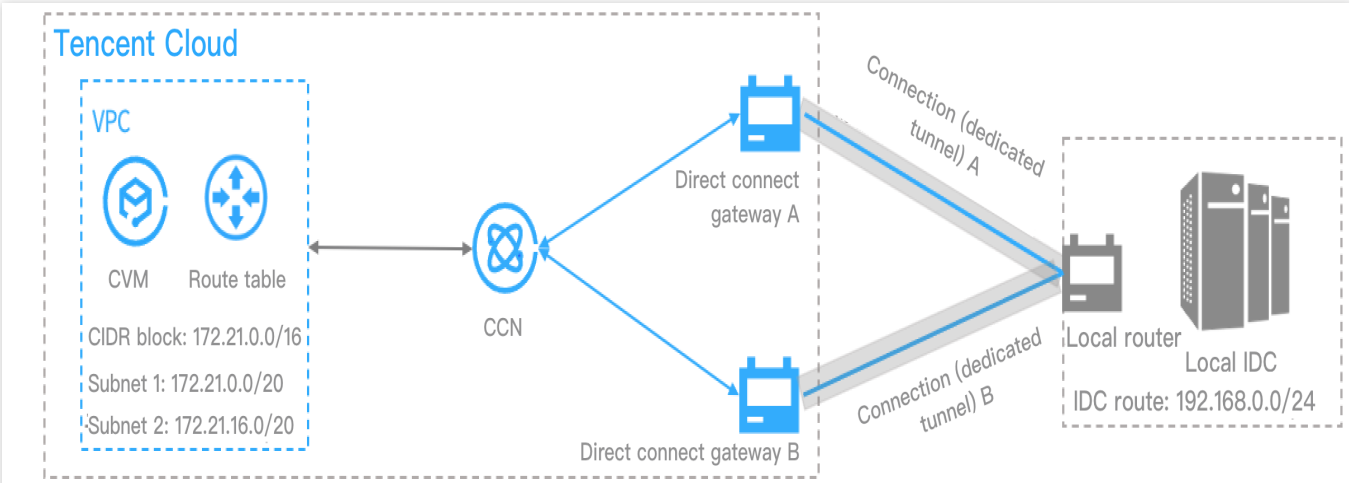
IDC route table

Destination IP range	Next hop	Rema
192.168.0.0/24	Local IDC server	Configur the local
172.21.0.0/16	Dedicated tunnel A	Configur the local
172.21.0.0/16	Dedicated tunnel B	Configur the local

当专用通道 A 和专用通道 B 均为 BGP 模式时，本地路由器通过 BGP 协议从专线网关 A 学习到的路由目的网段为子网 CIDR（172.21.0.0/20、172.21.16.0/20），从专线网关 B 通过 BGP 路由协议学习到目的网段为 VPC CIDR（172.21.0.0/16）。由于本地路由器按最长掩码匹配原则进行转发，因此流量将全部转发至专线网关 A。当专用通道 A 故障时，IDC 侧去往专线网关A 的路由条目消失，上云流量才会转发至专线网关 B。

说明：

如果您的专线网关在 2020年9月15日零点前所创建，请提交 工单申请 将专线网关对外发布路由规则更改为 VPC CIDR。



VPC route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway	Automatically synced

CCN route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway A	Configured on the **IDC IP Range** page of the direct connect gateway
192.168.0.0/24	Direct connect gateway B	Configured on the **IDC IP Range** page of the direct connect gateway
172.21.0.0/20	VPC	Automatically synced the subnet route from the VPC
172.21.16.0/20	VPC	Automatically synced the subnet route from the VPC

Direct connect gateway A

Destination IP range	Next hop	Remarks
192.168.0.0/24	Tunnel A	Synced from the dedicated tunnel based on the BGP protocol
172.21.0.0/20	CCN	Automatically assigned
172.21.16.0/20	CCN	Automatically assigned

Direct connect gateway B

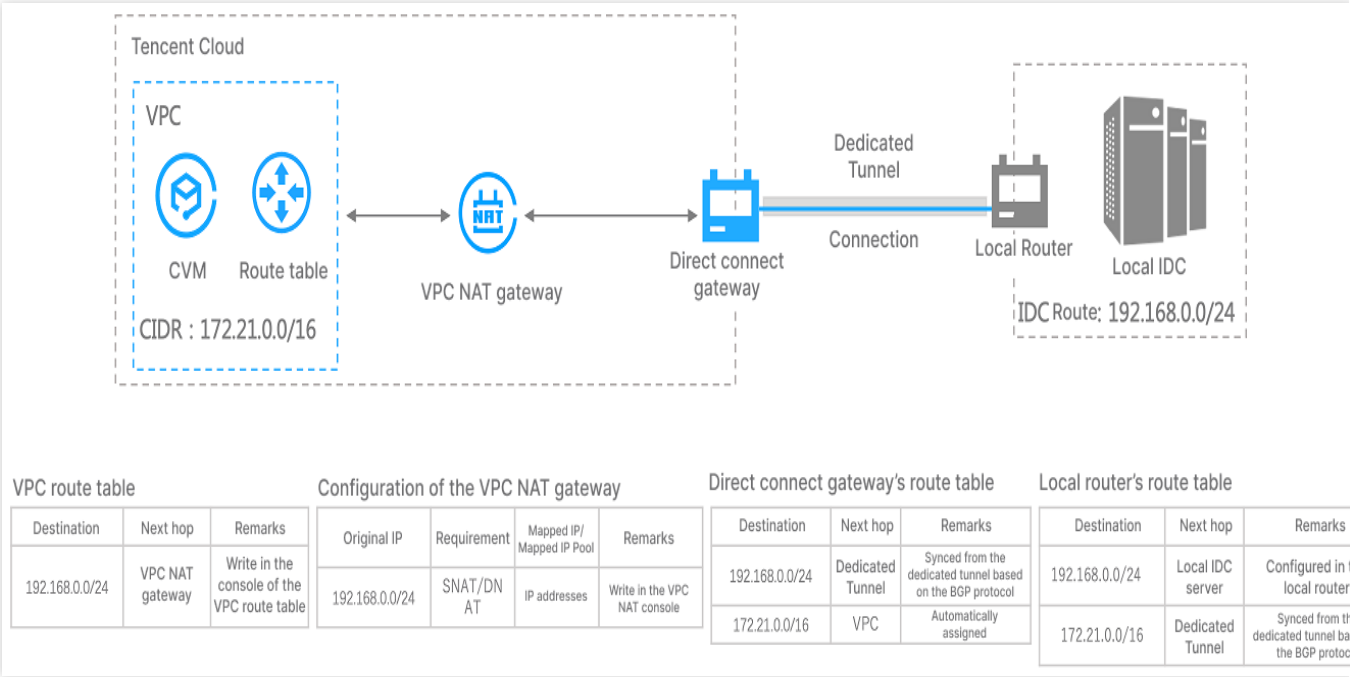
Destination IP range	Next hop	Remarks
192.168.0.0/24	Tunnel A	Synced from the dedicated tunnel based on the BGP protocol
172.21.0.0/16	CCN	Automatically assigned

IDC route table

Destination IP range	Next hop	Rema
192.168.0.0/24	Local IDC server	Configur the local
172.21.0.0/20	Dedicated tunnel A	Synced fr dedicated based o BGP pro
172.21.16.0/20	Dedicated tunnel A	Synced fr dedicated based o BGP pro
172.21.0.0/16	Dedicated tunnel B	Synced fr dedicated based o BGP pro

NAT 网络专线网关

在专线网关架构中，可以通过 NAT 网络型专线网关（后简称 NAT 型专线网关）进行 IP 地址转换，从而解决云上云下 IP 冲突问题。



VPC route table

Destination	Next hop	Remarks
192.168.0.0/24	VPC NAT gateway	Write in the console of the VPC route table

Configuration of the VPC NAT gateway

Original IP	Requirement	Mapped IP/ Mapped IP Pool	Remarks
192.168.0.0/24	SNAT/DNAT	IP addresses	Write in the VPC NAT console

Direct connect gateway's route table

Destination	Next hop	Remarks
192.168.0.0/24	Dedicated Tunnel	Synced from the dedicated tunnel based on the BGP protocol
172.21.0.0/16	VPC	Automatically assigned

Local router's route table

Destination	Next hop	Remarks
192.168.0.0/24	Local IDC server	Configured in local router
172.21.0.0/16	Dedicated Tunnel	Synced from the dedicated tunnel based on the BGP protocol

专用通道建议优先使用 BGP 模式，可以自动学习 IDC 到腾讯云 VPC 方向的目的网段。

在私网 NAT 中配置的 SNAT 本端三层、SNAT 本端四层和 DNAT 对端四层会自动产生映射关系；对端三层不会产生 NAT 映射关系。同时由于默认不发布 VPC CIDR，因此不能单独配置对端三层使用，需要与本端搭配使用。

2023年03月对 NAT 型专线网关进行了优化。网络地址转换配置内容标准化，由原来的专线侧配置映射关系，优化为 NAT 侧配置映射关系，专线侧绑定 NAT 实例。新旧版配置对应关系如下：

原配置参数名称	新参数名称	
本端IP转换	映射方向：本端	映射类型：三层
对端IP转换	映射方向：对端	映射类型：三层
本端源IP端口转换	映射方向：本端	映射类型：四层
本端目的IP端口转换	映射方向：对端	映射类型：四层

本端：对 VPC 内网 IP 地址转换。对端：对 VPC 对端网络的内网 IP 地址进行转换，如对端为 IDC 网络，则可转换 IDC 内的 IP 地址。三层：仅转换 IP 地址。四层：将 IP 和端口映射为指定 IP 池内随机端口。

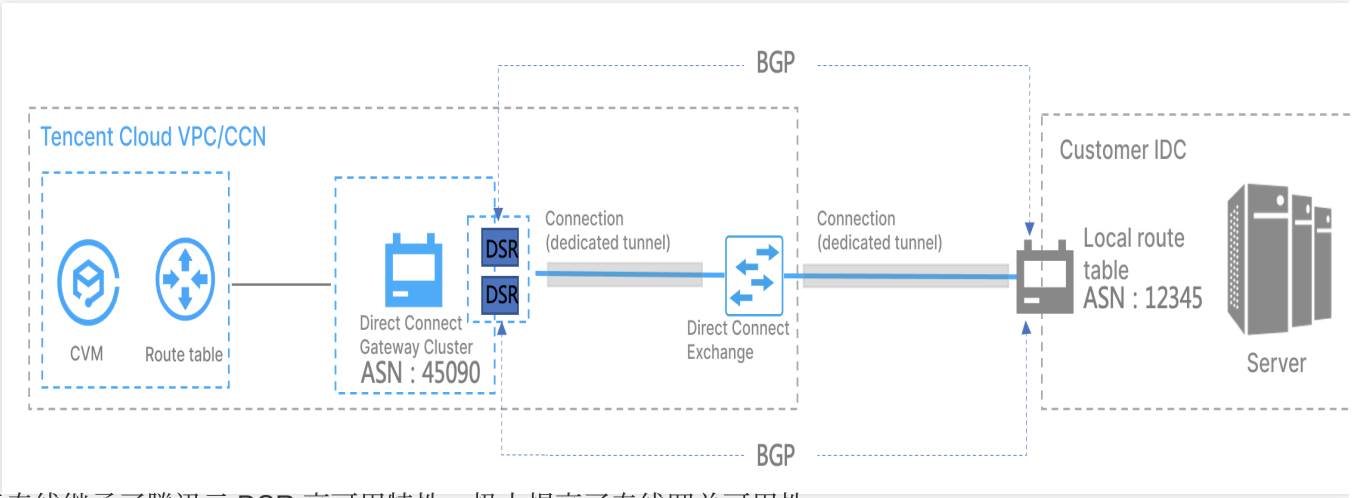
高可用概述

专线网关是连接云上网络和云下用户 IDC 的桥梁，其服务的高可用性对业务稳定运行至关重要。

DSR概述

腾讯自研分布式 SDN 路由系统（Disaggregated Software-Defined Router， DSR），是腾讯基于 SDN、NFV 和微服务技术自助研发的新一代软件路由系统，从系统架构、路由控制、数据转发等层面避免单点故障，用于替代传统的商业路由器，目前广泛的部署在腾讯超大规模、高性能、高弹性的云网络系统。
与传统的网络物理设备相比，腾讯云 DSR 系统支持 NFV、微服务等多种云计算虚拟技术，通过分布式架构有效的避免了单一组件故障对整体系统的影响，实现组件级故障自动发现、隔离和恢复。

专线网关高可用设计



腾讯云专线继承了腾讯云 DSR 高可用特性，极大提高了专线网关可用性。
在路由转发平面，DSR 通过多活技术为每个专用通道提供2个双活的路由系统，每个路由系统独立分布在不同的 DSR 集群上，同时 DSR 集群对外提供了2个腾讯云边界 IP 地址来实现控制面路由双活机制（active-active system），这样 IDC 侧本地路由器通过 BGP 协议分别与两个 DSR 集群分别建立了 BGP 邻居关系，有效的保证了 DSR 集群升级或者单集群故障时业务的高可用，避免因单 BGP 邻居中断导致路由收敛而对业务产生的影响。
在数据转发面，DSR 系统通过大规模集群控制和自研集群扩展技术，实现海量数据和流量的分布式转发。在集群内通过实时监测机制动态调整并剔除异常服务节点，保证了单集群的可用性；集群间通过大规模集群扩展技术，实现用户业务在多个集群间横向扩容，确保了跨集群的可用性。

推荐配置

1. 腾讯云侧：DSR 通过 BGP 协议学习腾讯云到用户 IDC 的路由，下一跳为用户本地路由器。
2. 用户 IDC 侧：用户本地路由器通过 BGP 协议学习到腾讯云 VPC 的路由，下一跳为 2个 DSR 集群的 IP 地址。

创建专线网关

最近更新时间：2024-11-05 11:05:18

本文将介绍如何创建专线网关，以及入方向路由说明。

前提条件

您已申请物理专线，具体操作请参见 申请接入物理专线。
如果使用 VPC，请确保您已创建腾讯云 VPC，具体操作请参见 快速搭建 IPv4 私有网络。
如果使用云联网 CCN，请确保您已创建云联网实例，具体操作请参见 新建云联网实例。
如果您使用 NAT 型专线网关，请您确保已创建私网 NAT。
说明：
NAT 型专线网关需要开白使用，如需使用，请 提交工单；NAT 型专线网关网络地址映射配置参数新旧版本对应关系请参见 专线网关概述。

使用限制

标准型专线网关支持传递辅助 CIDR，但需要遵循如下限制：
标准型专线网关支持传递10个辅助 CIDR。
NAT 型专线网关不支持传递辅助 CIDR。

操作步骤

1. 登录 专线接入控制台，并在左侧导航栏单击**专线网关**。
2. 在“专线网关”页面上方选择地域和私有网络，然后单击**+新建**。

3. 在**新建专线网关**对话框中配置网关详情，完成后单击**确定**。

字段	含义
名称	专线网关的名称。
可用区	选择地域所在可用区。
关联网络	选择云联网类型、私有网络或 NAT 类型的专线网关。
所在网络	所选的专线网关网络类型不同，则需关联相应网络类型的实例。
网关类型	若创建私有网络类型的专线网关，不具备网络地址转换功能。 若创建 NAT 型专线网关，具备网络地址转换功能，需要您在 NAT 侧配置转换规则。

入方向路由说明

在专线网络架构中，创建专线网关的时间、专用通道的模式均对入方向（IDC 到腾讯云 VPC 方向）的路由目的网段有影响，更多详细说明请参见 专线网关概述。

网关类型	创建时间	专用通道模式	IDC 侧上云路由
私有网络专线网关	无限制	静态	入方向路由的路由规则，由用户在本地路由器配置。
		BGP	IDC 侧通过 BGP 协议学习到 VPC CIDR。
云联网专线网	2020 年 9 月 15 日	静态	入方向路由的路由规则，由用户在本地路由器配置。

关	零点前	BGP	IDC 侧通过 BGP 协议学习到子网 CIDR。
	2020 年 9 月 15 日零点后	静态	入方向路由的路由规则，由用户在本地路由器配置。
		BGP	IDC 侧通过 BGP 协议学习到 VPC CIDR。
NAT 型专线网关	无限制	静态	入方向路由的路由规则，由用户在本地路由器配置。 VPC 路由下一跳需指向私网 NAT 网关。
		BGP	VPC 路由下一跳需指向私网 NAT 网关

后续操作

若您创建的云联网专线网关，则还需在专线网关添加 IDC 网段才可以实现网络通信，详情请参见 发布网段至云联网。

若您创建的 VPC 专线网关，还需配置 VPC 路由表信息，才能实现网络通信，详情请参见 配置路由表。

云联网专线网关发布网段至云联网

最近更新时间：2024-11-05 11:05:18

当云联网与专线网关关联时，需为云联网配置下一跳为专线网关、目的端为 IDC 网段的路由策略，才可以实现网络通信。配置云联网路由策略有自定义手动填写（静态）和自动学习传递自动学习（BGP）两种方式，详情请参见 路由概述。本文将介绍如何在专线网关上发布网段至云联网。

说明：

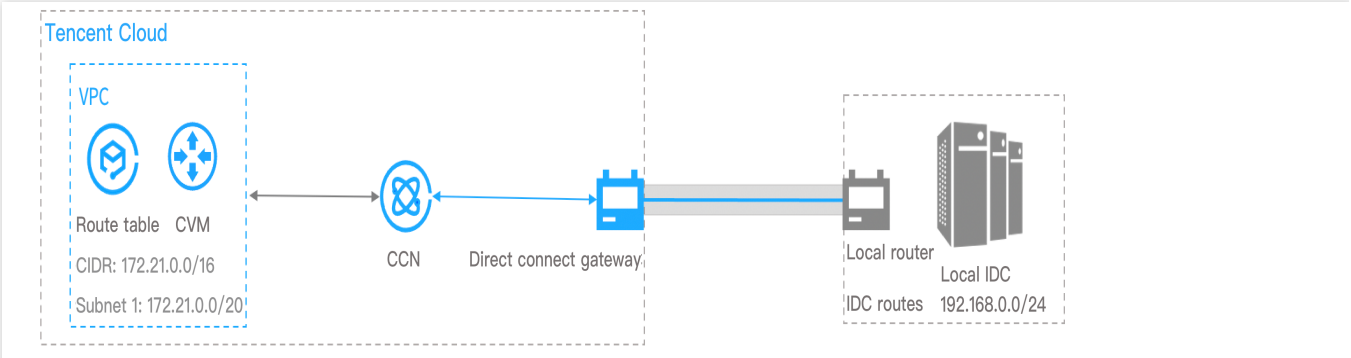
专线网关发往云联网的路由条目数小于等于20条，如需提升额度请提交 工单申请。

背景信息

在下图所示的专线网络架构中，本地 IDC 通过关联云联网专线网关、云联网实现与腾讯云 VPC 通信，云上 VPC 到 IDC 方向的目的网段为 `192.168.0.0/24` 。在专线网关上配置 IDC 网段后，云联网的路由表中将增加一条下一跳为专线网关、目的网段为 `192.168.0.0/24` 的路由策略，实现路由传递。

说明：

若您在专线网关上配置多个 IDC 网段，云联网将根据最长掩码匹配原则进行路由转发，详情请参见 云联网路由概述。



VPC route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	CCN	Automatically synced

CCN route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Direct connect gateway	Configured on the "IDC IP Range" page of the direct connect gateway or synced based on the BGP protocol
172.21.0.0/20	VPC	Automatically syncs the subnet route from the VPC

Direct connect gateway's route table

Destination IP range	Next hop	Remarks
192.168.0.0/24	Dedicated tunnel	Configured through the "CPE IP Range" parameter when the dedicated tunnel is created in the console
172.21.0.0/16	CCN	Automatically assigned

IDC route table

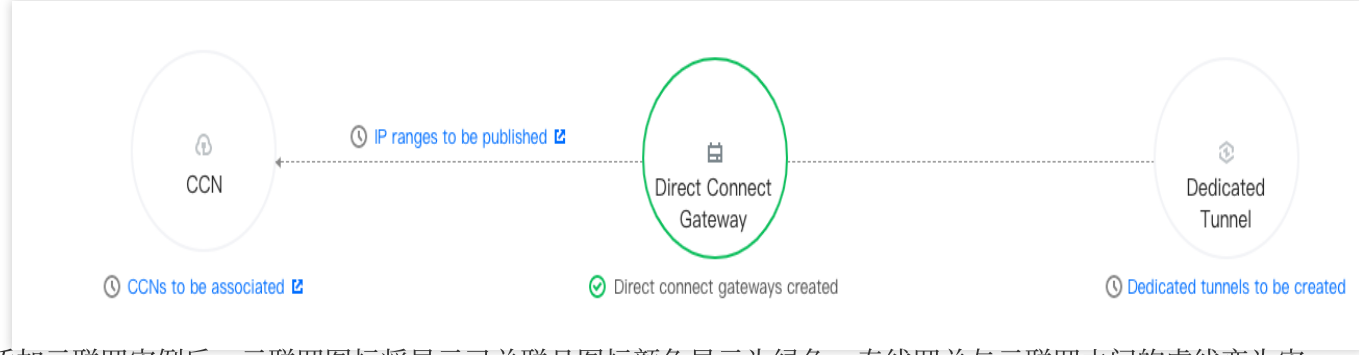
Destination IP range	Next hop	Remarks
192.168.0.0/24	Local IDC server	Configured in local router
172.21.0.0/16	Dedicated Tunnel	Configured in local router

前提条件

您已创建云联类型的专线网关，详情请参见 创建专线网关。

操作步骤

1. 登录 专线接入控制台 ，并在左侧导航栏单击**专线网关**。
2. 在“专线网关”页面上方选择地域和私有网络，然后在专线网关列表中单击目标实例 ID。
3. 在专线网关详情页面单击**发布网段**页签。
专线网关上的发布网段（即 IDC 网段）是指专线网关发送至云联网的路由。云联网收到该路由后，将自动新增一条下一跳为此专线网关、目的端为 IDC 网段的路由。
4. （可选）关联云联网。
如果 创建专线网关 时没有指定具体的云联网实例，请单击**关联云联网**，然后在弹出的对话框中选择待关联的云联网实例并单击**确定**。



成功添加云联网实例后，云联网图标将显示已关联且图标颜色显示为绿色，专线网关与云联网之间的虚线变为实线。即专线网关与云联网已互联。
5. 创建专用通道。
专用通道是物理专线的网络链路划分，提供了用户 IDC 和腾讯云之间的网路链路。
在与专线网关相连的专用通道图标下，单击**创建专用通道**。自动跳转至专用通道创建页面，您可在该页面配置专用通道信息。

专用通道创建详情请参见 申请专用通道。
成功创建专用通道后，专用通道图标将显示已创建且图标颜色显示为绿色，专线网关与云联网之间的虚线变为实线。即已为专线网关配置专用通道。

6. 发布 IDC 网段至云联网。

发布 IDC 网段到云联网，专线网关可以学习到云联网路由；云联网是否学习到的专线网关路由，由 IDC 网段发布方式决定。

自定义方式：用户手动配置模式，云联网学会指定的专线网关路由。

自动传递方式：即 BGP 模式，云联网自动获取专用通道发来的网关路由，但取决于专用通道的发布时间。

自定义方式

自动传递方式

模式切换须知

即原静态/手动配置模式。

1. （可选）在**发布规则**区域选择云联网实例。

当前专线网关未配云联网或者更换云联网情况下可执行本步骤。

说明：

发布方式系统自动填充，默认**自定义**方式，如果需要**自动传递**方式请提交 工单申请。

2. 在**网段详情**页面的**自定义**页签中单击**新建**，并填写发往云联网的网段信息，然后单击**保存**。

单击**保存**后，专线网关将配置的 IDC 网段发送给云联网。

说明：

发布的 IDC 网段数须小于等于100个。如需超额请提交 工单申请。

即原BGP模式。如需使用请提交 工单申请。

1. （可选）在**发布规则**区域选择云联网实例。

当前专线网关未配云联网或者更换云联网情况下可执行本步骤。

说明：

开启本功能后系统勾选**自动传递**。如果有自定义使用场景，请勾选**自定义**进行配置。

自定义模式和自动传递模式二者只能生效其一。

2. 配置 IDC 网段。

在**自动传递**方式下专线网关自动学习 IDC 网段信息，无须配置。

说明：

更新时间存在一分钟延时，若当前 IDC 网段有更新，请手动刷新页面。

发送网关的 IDC 网段到云联网的两种方式支持互相切换。

自定义切换为自动传递

需要提交 工单申请 开启自动传递发布发布功能。

自定义方式切换为自动传递方式后，当前已发布到云联网的自定义 IDC 网段信息将被撤回，专线网关自动学习 IDC 网段信息并将其传递给云联网。

自动传递切换为自定义

自动传递方式切换为自定义方式后，需要在**网段详情**页面的**自定义**页签中配置待发布的网段。

7. 查看发布的 IDC 网段。

在**网段详情**区域的网段列表中可查看发布的 IDC 网段信息。

查看专线网关路由表

最近更新时间：2024-11-05 11:05:18

若您的专线网络架构中使用云联网专线网关，则可以在控制台查看专线网关 IDC 方向和云联网方向的路由表信息。

使用限制

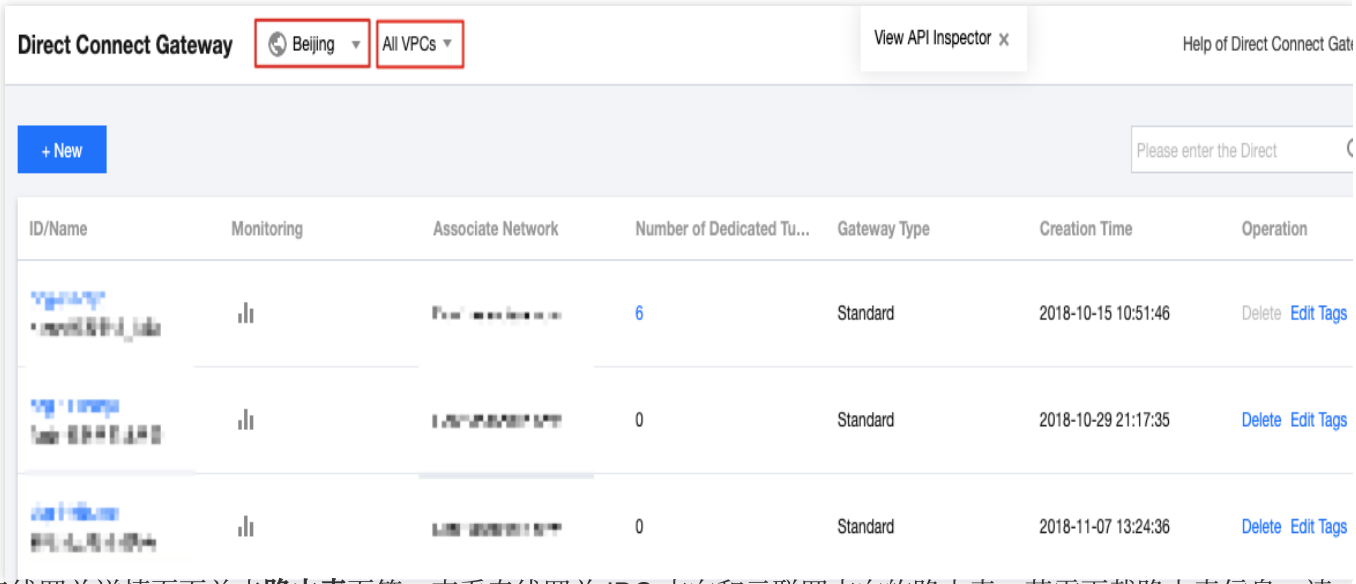
专线网关支持路由表功能灰度发布中，若需使用请提 工单申请。
中国台湾地域暂不支持此功能。

前提条件

您已创建云联网类型的专线网关，并关联云联网，详情请参见 创建专线网关。
创建专用通道， 并关联该专线网关，详情请参见 申请通道。
已为专线网关添加 IDC 网段，详情请参见专线网关添加 IDC 网段。

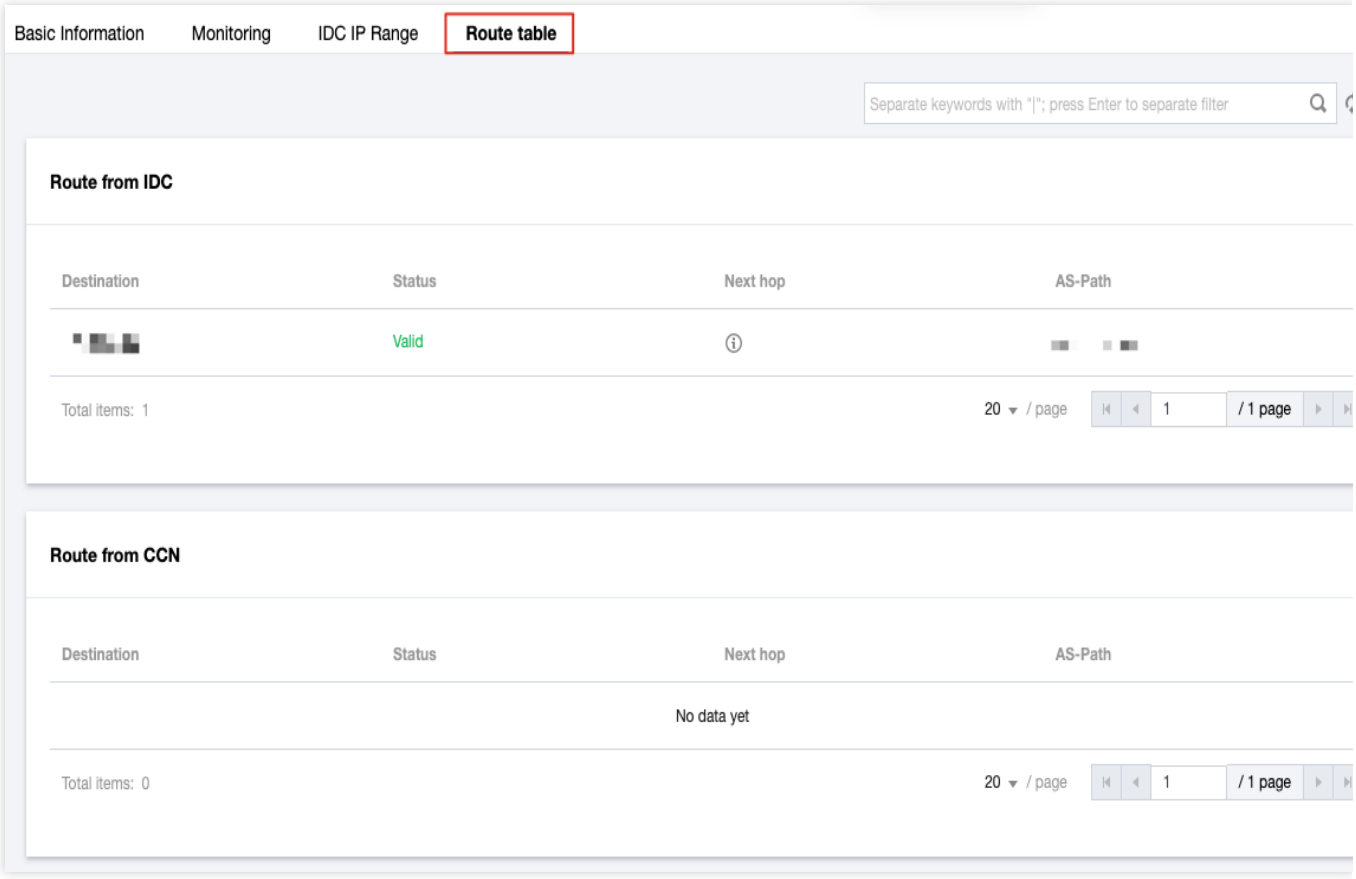
操作步骤

1. 登录 专线接入控制台 ，并在左侧导航栏单击**专线网关**。
2. 在“专线网关”页面上方选择地域和私有网络，然后在专线网关列表中单击目标实例 ID。



3. 在专线网关详情页面单击**路由表**页签，查看专线网关 IDC 方向和云联网方向的路由表，若需下载路由表信息，请单击

-


Basic Information
Monitoring
IDC IP Range
Route table
Separate keywords with "|"; press Enter to separate filter
Route from IDC
Destination
Status
Next hop
AS-Path
Valid
Total items: 1
20 / page
1
/ 1 page
Route from CCN
Destination
Status
Next hop
AS-Path
No data yet
Total items: 0
20 / page
1
/ 1 page

VPC 专线网关
配置网络地址转换（NAT）

最近更新时间：2024-11-05 11:05:18

您可为网关类型为 NAT 型的专线网关配置 IP 转换和配置 IP 端口转换，具体可参考如下操作：

说明：

本文仅是 V3R1 版本的 NAT 网络型专线网关网络地址转换指导，升级后的 V3R2 版本专线侧仅需在 创建专线网关 时绑定相应的私有 NAT 实例即可，其中 IP 映射关系需要在 NAT 侧进行配置

配置 IP 转换

配置 IP 端口转换

配置示例

配置 IP 转换

配置本端 IP 转换

规则限制

原 IP 必须在私有网络 CIDR 范围内。

映射 IP 不可以在专线网关所在私有网络 CIDR 范围内。

原 IP 唯一不可以重复，即私有网络内1个 IP 只能唯一映射为1个 IP。

映射 IP 唯一不可以重复，即多个 VPC IP 不可映射为同一个 IP。

原目的 IP 不支持广播地址（255.255.255.255）、D 类地址（224.0.0.0 - 239.255.255.255）、E 类地址（240.0.0.0 - 255.255.255.254）。

专线网关的本端 IP 转换最大支持100个 IP 映射，每个 IP 映射最大支持20条 ACL 规则（如需提升配额，请提交 工单申请）。

操作步骤

1. 登录 私有网络控制台。
2. 在左侧导航栏中，单击**专线网关**，进入管理页面。
3. 单击网关类型为 NAT 型专线网关 ID，进入详情页。
4. 在专线网关详情页中，选择**本端 IP 转换**选项卡，进行本端 IP 转换配置。
5. 在 IP 映射页左上角，单击**新增**，新增本端 IP 映射。
6. 在弹框中，输入原 IP、映射 IP 及备注，单击**确定**即可。
7. （可选）新增本端 IP 映射时，默认添加了允许所有进出流量通过的 ACL 规则，即本端 IP 转换对所有专用通道生效，您可以编辑本端 IP 转换的 ACL 规则，以改变本端 IP 转换的适用范围。

说明：

当专线网关同时配置对端 IP 转换时，本端 IP 转换 ACL 规则的**目的 IP** 需要填写**对端 IP 转换的映射 IP**，而不是原 IP。
本端 IP 转换 ACL 规则支持配置协议（支持 TCP 或 UDP）、源端口、目的 IP、目的端口，其中，端口、IP 不填代表 ALL；当协议选择 ALL 时，端口和 IP 默认均选择 ALL。
8. 在 IP 映射页中，单击 IP 映射所在行右侧的**编辑 ACL 规则**，进入 ACL 规则编辑状态。
9. 在已有的 ACL 规则底部，单击**新增一行**，完成 ACL 规则的新增后，单击**保存**即可。
10. （可选）在 ACL 规则编辑状态下，您可对已有的 ACL 规则进行修改或删除，完成操作后，单击**保存**即可。
11. （可选）您也可在 IP 映射页中，直接单击

展开 IP 映射规则，单击规则所在行右侧的**修改**或**删除**，操作完成后，确认操作即可。
12. （可选）如果您需修改本端 IP 映射，可在 IP 映射页中，单击 IP 映射所在行右侧的**修改 IP 映射**，即可修改本端 IP 映射的原 IP、映射 IP 和备注，单击**确定**后，IP 映射生效。
13. （可选）如果您需删除本端 IP 映射，可在 IP 映射页中，单击 IP 映射所在行右侧的**删除**，并确认操作即可，IP 映射删除后将联动删除该 IP 映射下的 ACL 规则。

配置对端 IP 转换

规则限制

映射 IP 不可以在专线网关所在私有网络 CIDR 范围内。
原 IP 唯一不可以重复，即专线对端1个 IP 只能唯一映射为1个 IP。
映射 IP 唯一不可以重复，即不支持多个专线对端 IP 映射为同1个 IP。
原目的 IP 不支持广播地址（255.255.255.255）、D 类地址（224.0.0.0 - 239.255.255.255）、E 类地址（240.0.0.0 - 255.255.255.254）。
专线网关的对端 IP 转换最大支持100个 IP 映射（如需提升配额，请提交 工单申请）。

操作步骤

1. 登录 私有网络控制台。
2. 在左侧导航栏中，单击**专线网关**，进入管理页面。
3. 单击网关类型为 NAT 型专线网关 ID，进入详情页。
4. 在专线网关详情页中，选择**对端 IP 转换**选项卡，进行对端 IP 转换配置。
5. 在 IP 映射页左上角，单击**新增**，新增对端 IP 映射。
6. 在弹框中，输入原 IP、映射 IP 及备注，单击**确定**即可。
7. （可选）如果您需修改对端 IP 映射，可在 IP 映射页中，单击 IP 映射所在行右侧的**修改 IP 映射**，即可修改对端 IP 映射的原 IP、映射 IP 和备注，单击**确定**后，对端 IP 映射生效。
8. （可选）如果您需删除对端 IP 映射，可在 IP 映射页中，单击 IP 映射所在行右侧的**删除**，并确认操作即可。

配置 IP 端口转换

配置本端源 IP 端口转换

说明：

当本端 IP 转换和本端源 IP 端口转换冲突时，优先匹配本端 IP 转换。

规则限制

映射 IP 池不可以在专线网关所在私有网络的 CIDR 范围内。

多个映射 IP 池的 ACL 规则不可以重叠，否则会导致网络地址转换冲突。

多个映射 IP 池之间 IP 不可以重叠。

映射 IP 池仅支持单 IP 或连续 IP，且连续 IP 的 /24 网段需保持一致，即支持“192.168.0.1 - 192.168.0.6”，不支持“192.168.0.1 - 192.168.1.2”。

映射 IP 池不支持广播地址（255.255.255.255）、D 类地址（224.0.0.0 - 239.255.255.255）、E 类地址（240.0.0.0 - 255.255.255.254）。

本端源 IP 端口转换最大支持100个映射 IP 池，每个映射 IP 池支持最大20条 ACL 规则（如需提升配额，请提交 工单申请）。

操作步骤

1. 登录 私有网络控制台。
2. 在左侧导航栏中，单击**专线网关**，进入管理页面。
3. 单击网关类型为 NAT 型专线网关 ID，进入详情页。
4. 在专线网关详情页中，选择**本端源 IP 端口转换**选项卡，进行本端源 IP 端口转换配置。
5. 在映射 IP 池页左上角，单击**新增**，新增映射 IP 池。
6. 在弹框中，输入映射 IP 池（支持 IP 或 IP 段，IP 段格式为 “A - B”）和备注，单击**确定**即可。
7. 新增映射 IP 池的 ACL 规则为拒绝所有进出流量通过，需要额外编辑 ACL 规则才可以实现网络转换。

说明：

当专线网关同时配置对端 IP 转换时，本端源 IP 端口转换 ACL 规则的**目的 IP** 需要填写**对端 IP 转换的映射 IP**，而不是原 IP。

本端源 IP 端口转换 ACL 规则支持配置协议（支持 TCP 或 UDP）、源 IP、源端口、目的 IP、目的端口。

8. 在映射 IP 池页中，单击映射 IP 池所在行右侧的**编辑 ACL 规则**，进入 ACL 规则编辑状态。
9. 在已有 ACL 规则底部，单击**新增一行**，完成 ACL 规则的新增后，单击**保存**即可。
10. （可选）在 ACL 规则编辑状态下，您可对已有的 ACL 规则进行修改或删除，完成操作后，单击**保存**即可。
11. （可选）您也可在映射 IP 池页中，单击

展开映射 IP 池规则，单击规则所在行右侧的**修改**或**删除**，操作完成后，确认操作即可。

12. （可选）如果您需修改映射 IP 池，可在映射 IP 池页中，单击映射 IP 池所在行右侧的**修改映射 IP 池**，即可修改该映射 IP 池的 IP 和备注。
13. （可选）如果您需删除映射 IP 池，可在映射 IP 池页中，单击映射 IP 池所在行右侧的**删除**并确认操作，即可删除该映射 IP 池，映射 IP 池删除后，将自动删除映射 IP 池关联的 ACL 规则。

配置本端目的 IP 端口转换

规则限制

原 IP 必须在专线网关所在私有网络 CIDR 范围之内。
原 IP 端口唯一，即私有网络内同一 IP 端口只能唯一映射为一个 IP 端口。
映射 IP 端口不可以在私有网络 CIDR 范围之内。
映射 IP 端口不可以重复，即不存在一个 IP 端口映射多个私有网络 IP 端口。
原 IP 和映射 IP 不支持广播地址（255.255.255.255）、D 类地址（224.0.0.0 - 239.255.255.255）、E 类地址（240.0.0.0 - 255.255.255.254）。
本端目的 IP 端口转换最大支持100个 IP 端口映射（如需提升配额，请提交 工单申请）。

操作步骤

1. 登录 私有网络控制台。
2. 在左侧导航栏中，单击**专线网关**，进入管理页面。
3. 单击网关类型为 NAT 型专线网关 ID，进入详情页。
4. 在专线网关详情页，选择**本端目的 IP 端口转换**选项卡，进行本端目的 IP 端口转换配置。
5. 在 IP 端口映射页左上角，单击**新增**，新增本端目的 IP 端口映射。
6. 在弹框中，选择协议，输入原 IP 端口、映射后 IP 端口及备注，单击**确定**即可。
7. （可选）如果您需修改本端目的 IP 端口映射，可在 IP 端口映射页中，单击 IP 端口映射所在行右侧的**修改 IP 端口映射**，即可修改该 IP 端口映射的映射关系及备注。
8. （可选）如果您需删除本端目的 IP 端口映射，可在 IP 端口映射页中，单击 IP 端口映射所在行右侧的**删除**并确认操作，即可删除该映射。

配置示例

配置本端 IP 转换示例

若私有网络内的 IP A `192.168.0.3` 作为原 IP，通过本端 IP 转换，映射为 IP B `10.100.0.3`，则：
IP A 对专线对端的主动访问网络包原 IP 将自动修改为 `10.100.0.3`。
所有专线对端访问的 `10.100.0.3` 的网络包将自动指向 IP A `192.168.0.3`。

配置对端 IP 转换示例

专线对端 IP D `10.0.0.3` 作为原 IP，通过对端 IP 转换，映射为 IP C `172.16.0.3`，则：
IP D `10.0.0.3` 主动访问私有网络的网络包原 IP，并自动修改为 IP C `172.16.0.3`。
所有私有网络访问 IP C `172.16.0.3` 的网络包，将自动指向专线对端 IP D `10.0.0.3`。

配置本端源 IP 端口转换示例

私有网络 C 网段为 `172.16.0.0/16`，通过专线连接第三方银行 A 和 B，其中银行 A 对端网段为 `10.0.0.0/28`，要求对接网段为 `192.168.0.0/28`；银行 B 对端网段为 `10.1.0.0/28`，要求对接网段为 `192.168.1.0/28`。则可以按照下面配置 A、B 两条本端源 IP 端口转换：

配置		本端源 IP 端口转换 A	本端源 IP 端口转换 B
映射 IP 池		192.168.0.1 - 192.168.0.15	192.168.1.1 - 192.168.1.15
ACL 规则	协议	ALL	ALL
	源 IP	172.16.0.0/16	172.16.0.0/16
	源端口	—	—
	目的 IP	10.0.0.0/28	10.1.0.0/28
	目的端口	—	—

完成配置后，私有网络 C 内主动访问银行 A、B 的网络请求，会根据对应的 ACL 规则分别转换为对应映射 IP 池的随机端口，访问对应的专用通道。

配置本端目的 IP 端口转换示例

私有网络 C 的网段为 `172.16.0.0/16`，仅希望开放部分端口给专线对端主动访问，则可以按照下面方案配置 A、B 两条本端目的 IP 端口映射：

本端目的 IP 端口映射 A：原 IP 端口 `172.16.0.1:80`，映射后 IP 端口 `10.0.0.1:80`。

本端目的 IP 端口映射 B：原 IP 端口 `172.16.0.1:8080`，映射后 IP 端口 `10.0.0.1:8080`。

完成配置后，专线对端可以主动访问 `10.0.0.1:80`、`10.0.0.1:8080` 端口，实现对私有网络 C 内 `172.16.0.1:80`、`172.16.0.1:8080` 两个端口的主动访问。

配置路由表

最近更新时间：2024-11-05 11:05:18

创建专线网关并完成专用通道建设后，即可在控制台配置私有网络的路由表，将需要通向专线的流量引导到专线网关。

1. 登录 私有网络控制台。
2. 在左侧目录中，单击**路由表**，进入管理页面。
3. 单击需要关联专线网关的路由表 ID， 进入详情页。
4. 单击 **+新增路由策略** 。
5. 在弹框中输入目的端网段，下一跳类型选择**专线网关**，下一跳选择网关名。

配置路由策略：

配置参数	参数说明
目的端	目的端即为您要转发到的目标网段，配置要求如下： 目的网段描述仅支持网段格式，如果您希望目的端为单个 IP，可设置掩码为32（例如172.16.1.1/32）。 目的端不能为路由表所在私有网络内的 IP 段，原因是 Local 路由已表示此私有网络内默认内网互通。
下一跳类型	选择专线网关。
下一跳	指定具体跳转到的下一跳专线网关实例。
备注	可自行添加路由条目的描述信息，便于资源管理。
新增一行	如需配置多条路由策略，可单击**新增一行**，如需删除可单击操作列的删除图标，创建自定义路由表时，至少需要配置一条路由策略。

6. 单击**创建**即可。

完成上述步骤后，您即可将特定目的端流量指向专线网关，与您的本地数据中心关联。

绑定 NAT 网关

最近更新时间：2024-11-05 11:05:18

创建专线网关完成后如果您业务需要通过 NAT 网关方式进行公网访问，那么您需要为专线网关绑定 NAT 网关。本文将介绍如何为专线网关绑定 NAT 网关。

前提条件

已 创建 VPC 网络。
已 创建 VPC 型专线网关。
已 创建 NAT 网关。

绑定 NAT 网关

1. 登录 私有网络控制台。
2. 在左侧目录中，单击**专线网关**，进入管理页面。
3. 在专线网关列表中单击需要绑定 NAT 网关的专线网关名称，进入详情页面。
4. 在**基本信息**页面选择需要绑定的 NAT 网关。

解绑 NAT 网关

如果您不再需要专线网关上绑定的 NAT 网关，您可以进入专线网关详情页面的**基本信息**页签解绑。
1. 登录 私有网络控制台。
2. 在左侧目录中，单击**专线网关**，进入管理页面。
3. 在专线网关列表中单击需要解绑 NAT 网关的专线网关名称，进入详情页面。
4. 在**基本信息**页面**绑定 NAT 网关**所在行单击**解绑**，并在弹出的对话框中单击**确定**。

删除专线网关

最近更新时间：2024-11-05 11:05:18

您在不使用专线网关后，可以对专线网关进行删除。删除专线网关，将一同删除连接至此专线网关的专用通道，请确认专线网关删除不会影响到您的正常业务。

1. 登录 腾讯云控制台，选择**云产品 > 网络 > 私有网络**，进入私有网络控制台。
2. 单击左侧导航栏**专线网关**，进入管理页面。
3. 选择需要删除的专线网关，单击操作栏的**删除**。
4. 单击**确定**即可。

管理专线网关
网关流控

最近更新时间：2024-01-13 16:40:45

网关流控可以为您提供网关上 IP 粒度的 “监” 与 “控” 能力，可以对内网IP与网关之间的带宽进行监控和限制。
开启网关流控可使流量管理精细化、可视化，帮助网络运维人员掌握网关中流量的情况，IP 粒度的限速能力帮助您快速排查故障，屏蔽异常流量，保障关键业务。
目前支持开启网关流控的有：专线网关。
说明：
1. 网关流控的源端仅支持云服务器，其它服务到网关的流量不支持统计。
2. 目前网关流控处于灰度中，如有需要，请提交 工单申请。

主要功能

精确的网关故障排查能力，最小化网络故障时间；可以结合流量提供实时查询、展示 TOP N 排名的 IP 功能，分析来源 IP 及其关键指标，快速定位异常流量。
基于 IP - 网关粒度的 “监” 与 “控” 能力；结合分钟级的网络流量查询，可及时发现异常流量抢占带宽，设置 IP - 网关粒度带宽限制，保障核心业务稳定畅行。
全时全流的网关流量分析能力，降低云上网络成本。通过 QoS 控制成本，可在网络预算有限的情况下，限制非关键业务带宽，以降低成本。

应用场景

主要应用于公司网关流量在夜间突增场景，通过智能网关流控，运维人员可根据该突增时间点，追踪造成流量突增的 IP，从而快速定位根源。不仅如此，网关流控提供基于 IP - 网关粒度的带宽控制，可限制某 IP 到网关的带宽，屏蔽异常流量，保障关键业务。

计费相关

网关流控功能不收费。

操作指南

开启网关流控明细

1. 登录 私有网络控制台。
2. 根据您的需求，在左侧导航栏选择**专线网关**，进入对应管理页面，如下以 VPN 网关为例。
3. 单击需要开启的网关或连接 ID，进入详情页。
4. 单击**监控**选项卡，开启右上角**网关流控明细**。
5. 开启 VPN 网关流控明细需要5 - 6分钟采集和发布数据，之后，您即可在监控图表下方查看监控明细表格。

设置流控明细

1. 登录 私有网络控制台。
2. 根据您的需求，在左侧导航栏选择**专线网关**，进入对应管理页面，如下以 VPN 网关为例。
3. 单击需要设置的网关或连接 ID，进入详情页。
4. 单击**监控**选项卡。
5. 找到需要限制出带宽上限的 IP，单击**修改**。
6. 调整带宽后，单击**保存**。

查看流控明细

1. 登录 私有网络控制台。
2. 根据您的需求，在左侧导航栏选择**专线网关**，进入对应管理页面，如下以 VPN 网关为例。
3. 单击需要查看的网关或连接 ID，进入详情页。
4. 单击**监控**选项卡。
5. 在网关流控明细表右上方，单击**查看已限制 IP**。

网关流量分析

最近更新时间：2024-01-13 16:40:45

在腾讯云专线使用过程中，每条通道的业务不同其承载的流量负荷不同，如果通道被业务流量占满则会导致线路不可用。针对这一问题，腾讯云专线推出了网关粒度的流量分析功能，让您第一时间了解流量 Top N 的 IP 及流量详情，协助您进行业务调整。

前提条件

已创建专线网关，详情请参见 创建专线网关。
已有业务流量在网关中流通。

操作步骤

1. 登录 专线接入控制台，并在左侧导航栏单击**专线网关**。
2. 在“专线网关”页面上方选择地域和私有网络，然后在专线网关列表中单击目标实例 ID。
3. 在专线实例详情页单击**流量分析**，并开启流量采集任务。
开启后，系统会自动统计所有通过本网关的数据流量，约3 - 5分钟后将采集结果展示。
4. 查看流量分析结果。
时间周期和时间粒度设置。
时间周期包括**3分钟前**、**1小时前**、**7天前**。
时间粒度包括**1分钟**、**1小时**和**1天**，即按分钟/小时/天粒度来统计流量。
说明：
如果您预计流量分析时间约0 ~ 30分钟，时间粒度建议选择1分钟，超过30分钟时间粒度建议选择小时。
如果您想要3分钟内更加准确、细粒度的流量统计分析，建议时间周期选**三分钟前**，自定义时间段跨度为1分钟（如2021-08-06 14:18～2021-08-06 15:17），时间粒度选择**1分钟**。
TOP N 查看。在流量列表中展示了**TOP 5**、**TOP 20**、**TOP 50**和自定义等四种通道流量排行榜，如果您需要查看指定 IP 的流量信息可在右侧输入框键入相应的 IP 地址。

专用通道
专用通道概述

最近更新时间：2024-11-05 11:05:18

专用通道是物理专线的网络链路划分，您可以创建不同的专用通道与不同专线网关关联，实现本地数据中心与多个私有网络的互联。创建专用通道后，系统将自动为您配置专用通道事件告警，帮助您监控、运维专用通道。本文将介绍如何申请通道。

背景信息

腾讯云专线接入有自主独占物理专线和共享合作伙伴线路两种接入方式：
自主独占型专线接入：用户自主拉通本地数据中心到腾讯云接入点的物理专线，独享物理端口。
共享合作伙伴专线接入：使用合作伙伴在腾讯预连接的物理专线接入腾讯云。目前合作伙伴有中国电信、中国移动、中国联通、中信网络等具有 A14 和 A26 电信资质的合作伙伴。
物理专线接入方式不同，则在其上创建的通道不同。
使用自主独占型物理专线创建的通道为独占型专用通道，即独占专用通道，适用于大带宽接入、业务独享等场景，创建详情请参见 独享专用通道。
使用合作伙伴与腾讯预连接的物理专线创建的专用通道为共享型专用通道，即共享专用通道，适用于无大带宽入云需求、上云时间要求较短的场景，创建详情请参见 共享专用通道。

独享专用通道

最近更新时间：2024-11-05 11:05:18

前提条件

您已申请物理专线，具体操作请参见 申请物理专线。
您已创建专线网关，具体操作请参见 创建专线网关。

操作步骤

步骤一：申请专用通道

1. 登录 专线接入 - 专用通道 控制台。
2. 在左侧导航栏，单击**专用通道** > **独享专用通道**，在页面上方单击 **+新建**，并配置名称、专线类型、接入网络、地域、关联的专线网关等基本名称配置，完成后单击**下一步**。

字段	含义
名称	专用通道名称。
通道类型	通道类型随关联的物理专线变化，分为1.0和2.0。
物理专线	选择您已申请的物理专线。
接入网络	若通道类型为 1.0，则可选择云联网、私有网络。 若通道类型为 2.0，则可选择云联网、私有网络和 NAT 网络。
地域	若选择云联网，则地域默认为云联网专线网关所在地域。 若选择私有网络，专用通道 2.0 仅可选择物理专线所在地域，专用通道1.0可选择任何地域。
私有网络	选择目标私有网络实例。
专线网关	关联已创建的专线网关，专用通道2.0不支持 NAT 型专线网关。

3. 在**高级配置**页面配置以下参数。

字段	含义
VLAN ID	一个 VLAN 对应一个通道，取值范围[0，3000)： 若值为0，表示仅能创建一个专用通道，请使用三层物理口对接。

	若值为[1，2999]，代表可创建多个专用通道，请使用三层子接口对接。若特殊情况只能二层对接，建议在 IDC 侧关闭接口下 STP 协议。在多专用通道下，MSTP 专线透传多 VLAN 时，需运营商线路开启 Trunk 模式。
带宽	专用通道的最大带宽值，不可超过关联的物理专线的带宽值。月95后付费的计费模式下，“带宽”参数不代表计费带宽。
互联IP	若您的通道类型是2.0，默认为手动分配。 若您的通道类型是1.0，可选择手动指定或自动分配。若选择自动分配，则无需配置腾讯云边界主 IP 和用户边界 IP。
腾讯云边界 IP1	物理专线腾讯云侧的边界互联 IP。请勿使用以下网段或网络地址：169.254.0.0/16、127.0.0.0/8、255.255.255.255、224.0.0.0 - 239.255.255.255、240.0.0.0 - 255.255.255.254。
腾讯云边界 IP2	物理专线腾讯云侧的备用边界互联 IP，在主边界 IP 发生故障不可用时，自动启用备用 IP，来确保您的业务正常运行。若配置腾讯云边界 IP 掩码为30、31时，则不支持配置腾讯云边界备 IP。
用户边界 IP	物理专线用户侧（或运营商网络侧）互联 IP，需用户自行配置。
路由方式	支持 BGP 路由和静态路由： BGP 路由：适用于不同自治域间交换路由信息和网络可达信息。 静态路由：适用于较简单的网络环境。
健康检查	默认开启健康检查，支持 BFD 和 NQA 两种检测模式，详情请参见 专用通道健康检查。
检测模式	支持 BFD 和 NQA 两种检测模式。
健康检查间隔	两次健康检查间隔时间。
健康检查次数	如果连续执行设定次数的健康检查失败后，则执行路由切换。
BGP ASN	输入 CPE 侧的 BGP 邻居的 AS 号，腾讯云 ASN 为 45090。若不输入将由系统随机分配。
BGP 密钥	输入 BGP 邻居的 MD5 值。默认 "tencent"，留空表示不需要 BGP 密钥。BGP 密钥不支持 ? & 空格" \\ +六种特殊字符。

说明：

若选择路由方式为**静态路由**，配置 IDC 网段时，请勿直接发布 `9.0.0.0/8`，`10.0.0.0/8`，`11.0.0.0/8`，`30.0.0.0/8`，`100.64.0.0/10`，`131.87.0.0/16`、`172.16.0.0/12`、`192.168.0.0/16` 等大网段路由。若需发布，则需拆分网段。

`9.0.0.0/8` 拆分为：`9.0.0.0/9` + `9.128.0.0/9`。

`10.0.0.0/8` 拆分为：`10.0.0.0/9` + `10.128.0.0/9`。

`11.0.0.0/8` 拆分为：`11.0.0.0/9` + `11.128.0.0/9` 。
`30.0.0.0/8` 拆分为：`30.0.0.0/9` + `30.128.0.0/9` 。
`100.64.0.0/10` 拆分为：`100.64.0.0/11` + `100.96.0.0/11` 。
`131.87.0.0/16` 拆分为：`131.87.0.0/17` + `131.87.128.0/17` 。
`172.16.0.0/12` 拆分为：`172.16.0.0/13` + `172.24.0.0/13` 。
`192.168.0.0/16` 拆分为：`192.168.0.0/17` + `192.168.128.0/17` 。

4. 配置 IDC 设备。单击**下载配置指引**下载 CPE 配置指引文件，按照文件中提供的几款通用厂商的配置方法进行配置。

参数	描述	备注
用户 IDC 网段	静态路由输入用户侧 CPE 的网段，非 NAT 模式下注意不能和 VPC 网段冲突。	支持变更：后期可通过控制台“通道变更”更新网段。

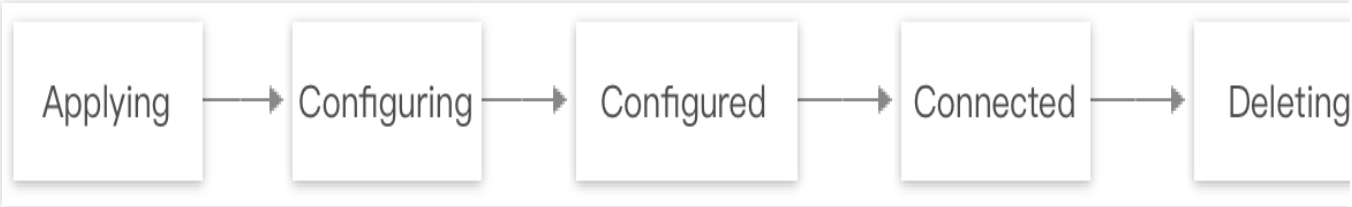
5. 单击**提交**。

步骤二：设置告警联系人

创建专用通道后，腾讯云将自动为该专用通道配置专用通道 Down、专用通道 BFD 检测 Down、专用通道 BGP 会话 Down 和 BGP通道路由条目数超限四类事件告警，帮助您监控、运维专用通道。告警事件说明请参见 告警事件说明。
自动创建的默认告警策略未配置接收人信息，仅支持控制台告警，您可以自行配置告警接收人，详情请参见 **配置告警**。

连接状态说明

创建成功后，专用通道将出现在专用通道列表中，且连接状态为“申请中”。
专用通道可能出现的连接状态流转如下：



申请中
系统已接收用户申请新通道指令，准备发起创建任务。
配置中
系统正在下发参数配置，若连接状态长时间在“配置中”，则表示系统下发配置遇到问题，请您联系架构师或 提交工单 咨询。

配置完成

系统已根据您所填参数完成配置，但尚未 ping 通您的 IDC 互联地址，该状态支持删除操作。

已连接

系统已 ping 通您的 IDC 设备互联地址，但不代表业务已顺利连接。请前往 VPC 或云联网 路由表 完成相关配置，实现连接。

删除中

若您在控制台删除专用通道，则连接状态流转为“删除中”。若连接状态长时间在“删除中”，表示系统删除配置遇到问题，请您联系架构师或 提交工单 咨询。

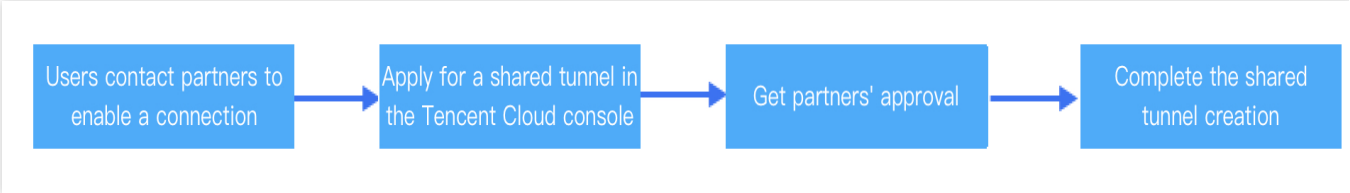
共享专用通道

最近更新时间：2024-11-05 11:05:18

专用通道是物理专线的网络链路划分，您可以创建不同的专用通道与不同专线网关关联，实现本地数据中心与多个私有网络的互联。本文介绍如何创建共享型专用通道。

背景说明

中国电信、中国移动、中国联通、中信网络等具有A14和A26电信资质的合作伙伴和腾讯专线接入点之间预先建立了物理专线连接，您可以依据实际需求通过共享合作伙伴的物理专线方式接入腾讯云。
共享型专用通道即使用合作伙伴的物理专线创建专用通道，也称共享专用通道，适用于无大带宽入云需求、上云时间要求较短的场景。
共享专用通道开通流程如下：



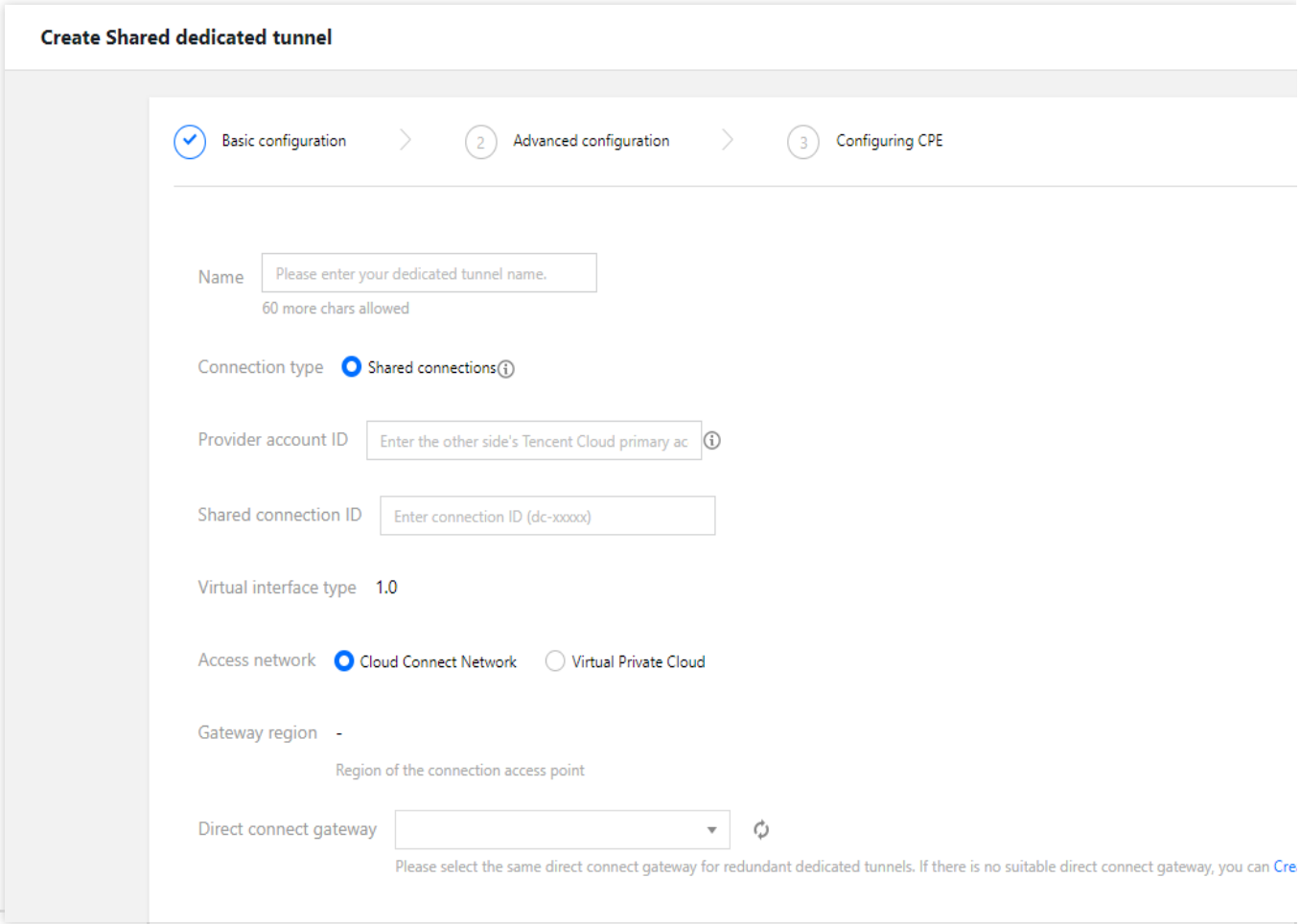
前提条件

您已从供应商获取用于共享通道物理专线实例 ID 和物理线提供方的腾讯云主体账户（UIN）。
您已创建专线网关，具体操作请参见 创建专线网关。

操作步骤

步骤一：申请专用通道

1. 登录 专用通道 控制台。
2. 在左侧导航栏，单击**专用通道** > **共享专用通道**，单击 **+新建**，并配置名称、专线类型、接入网络、地域、关联的专线网关等基本配置，完成后单击**下一步**。



字段	含义
名称	专用通道名称。
专线类型	共享专线。
专线提供方	与腾讯建立预连接的物理线路提供方： 目前仅支持具有A14和A26电信资质供应商（如电信、移动、联通、中信）线路创建共享通道。 如果您需要将自己的物理专线共享给子公司或者自己其他腾讯云账户请联系腾讯技术支持。 共享通道产生的费用由通道使用方支付。
共享专线 ID	用于创建共享通道的物理专线实例 ID。
接入网络	若通道类型为1.0，则可选择云联网或私有网络。 若通道类型为2.0，则可选择云联网、私有网络和 NAT 网络。
地域	若选择云联网，则地域默认为云联网专线网关所在地域。 若选择私有网络，专用通道2.0 仅可选择物理专线所在地域，专用通道1.0可选择任何地域。
私有网络	选择目标私有网络实例。
专线网关	关联已创建的专线网关，专用通道2.0不支持 NAT 型专线网关。

3. 在“高级配置”页面配置以下参数。

字段	含义
VLAN ID	一个 VLAN 对应一个通道，取值范围[0，3000)： 若值为0，表示仅能创建一个专用通道，请使用三层物理口对接。 若值为[1，2999]，代表可创建多个专用通道，请使用三层子接口对接。若特殊情况只能二层对接，建议在 IDC 侧关闭接口下 STP 协议。在多专用通道下，MSTP 专线透传多 VLAN 时，需运营商线路开启 Trunk 模式。
带宽	专用通道的最大带宽值，不可超过关联的物理专线的带宽值。月95后付费的计费模式下，“带宽”参数不代表计费带宽。
腾讯云边界主 IP1	物理专线腾讯云侧的边界互联 IP。请勿使用以下网段或网络地址：169.254.0.0/16、127.0.0.0/8、255.255.255.255、224.0.0.0 - 239.255.255.255、240.0.0.0 - 255.255.255.254。
腾讯云边界主 IP2	物理专线腾讯云侧的备用边界互联 IP，在主边界 IP 发生故障不可用时，自动启用备用 IP，来确保您的业务正常运行。若配置腾讯云边界 IP 掩码为 30、31 时，则不支持配置腾讯云边界备 IP。
用户边界 IP	物理专线用户侧（或运营商网络侧）互联 IP，需用户自行配置。
路由方式	支持 BGP 路由和静态路由： BGP 路由：适用于不同自治域间交换路由信息和网络可达信息。 静态路由：适用于较简单的网络环境。
健康检查	默认开启健康检查，支持 BFD 和 NQA 两种检测模式，详情请参见 专用通道健康检查。
检测模式	支持 BFD 和 NQA 两种检测模式。
健康检查间隔	两次健康检查间隔时间。
健康检查次数	如果连续执行设定次数的健康检查失败后，则执行路由切换。
BGP ASN	输入 CPE 侧的 BGP 邻居的 AS 号，腾讯云 ASN 为 45090。若不输入将由系统随机分配。
BGP 密钥	输入 BGP 邻居的 MD5 值。默认 "tencent"，留空表示不需要 BGP 密钥。BGP 密钥不支持 ? & 空格" \\ +六种特殊字符。

说明：

若选择路由方式为**静态路由**，配置 IDC 网段时，请勿直接发布 9.0.0.0/8，10.0.0.0/8， 11.0.0.0/8， 30.0.0.0/8， 100.64.0.0/10，131.87.0.0/16、172.16.0.0/12、192.168.0.0/16 等大网段路由。若需发布，则需拆分网段。

`9.0.0.0/8` 拆分为： `9.0.0.0/9` + `9.128.0.0/9` 。

`10.0.0.0/8` 拆分为： `10.0.0.0/9` + `10.128.0.0/9` 。

`11.0.0.0/8` 拆分为：`11.0.0.0/9` + `11.128.0.0/9` 。
`30.0.0.0/8` 拆分为：`30.0.0.0/9` + `30.128.0.0/9` 。
`100.64.0.0/10` 拆分为：`100.64.0.0/11` + `100.96.0.0/11` 。
`131.87.0.0/16` 拆分为：`131.87.0.0/17` + `131.87.128.0/17` 。
`172.16.0.0/12` 拆分为：`172.16.0.0/13` + `172.24.0.0/13` 。
`192.168.0.0/16` 拆分为：`192.168.0.0/17` + `192.168.128.0/17` 。

4. 配置 IDC 设备。单击下载配置指引下载 CPE 配置指引文件，按照文件中提供的几款通用厂商的配置方法进行配置。

参数	描述	备注
用户 IDC 网段	静态路由输入用户侧 CPE 的网段，非 NAT 模式下注意不能和 VPC 网段冲突。	支持变更：后期可通过控制台“通道变更”更新网段。

5. 单击**提交**。
共享专用通道创建后通道状态为“待接受”，需要线路提供方审批，审批通过后共享通道显示“已连接”。

步骤二：设置告警联系人

创建专用通道后，腾讯云将自动为该专用通道配置专用通道 Down、专用通道 BFD 检测 Down、专用通道 BGP 会话 Down 和 BGP 通道路由条目数超限四类事件告警，帮助您监控、运维专用通道。告警事件说明请参见 告警事件说明。
自动创建的默认告警策略未配置接收人信息，仅支持控制台告警，您可以自动配置告警接收人，详情请参见 配置告警。

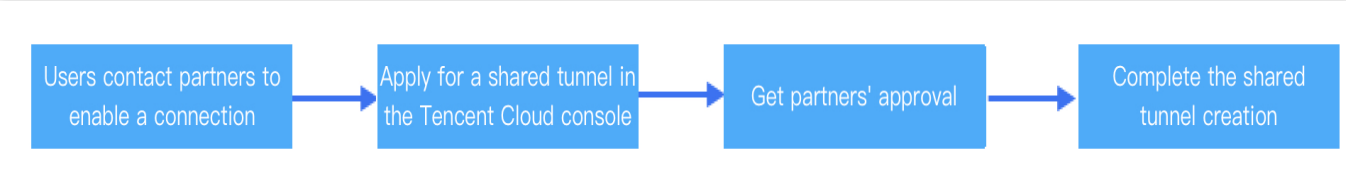
共享通道审批（合作伙伴）

最近更新时间：2024-11-05 11:05:18

您的物理专线共享给第三方客户后，在客户申请后您需要在控制台进行审批，审批后该共享通道才可用。

背景说明

中国电信、中国移动、中国联通、中信网络等具有A14和A26电信资质的合作伙伴和腾讯专线接入点之间预先建立了物理专线连接，您可以依据实际需求通过共享合作伙伴的物理专线方式接入腾讯云。
共享型专用通道即使用合作伙伴的物理专线创建专用通道，也称共享专用通道，适用于无大带宽入云需求、上云时间要求较短的场景。
共享专用通道开通流程如下。



前提条件

您的物理专线已预连接腾讯云。
客户已在控制台发起共享通道申请，详情可参见 共享专用通道。

操作步骤

1. 登录 共享专用通道 控制台。
2. 在**共享专用通道**列表页中**连接状态**为**待接受**所在行的操作列单击**更多** > **去审批**，并在弹出的页面进行审批。
3. 单击**确定**。审批后，共享通道连接状态将变更为“已连接”。

变更通道路由

最近更新时间：2024-11-05 11:05:18

当专用通道状态为“已连接”后，您还可以在专线接入控制台进行变更通道参数、修改通道带宽等操作。本文将分别介绍通道1.0和通道2.0如何在控制台修改通道配置信息和路由方式。

说明：

共享专线模式下，专用通道无法进行带宽变更，需由物理专线所有者发起带宽变更。

前提条件

在变更通道前，需已 申请通道。

大网段使用限制

在配置用户 IDC 网段时，若发布大网段路由，专线网关将直接拒收。为确保网络的精细化调度能力，请勿发布以下路由：

`9.0.0.0/8`，`10.0.0.0/8`，`11.0.0.0/8`，`30.0.0.0/8`，`100.64.0.0/10`，`131.87.0.0/16`、`172.16.0.0/12`、`192.168.0.0/16`。

若需发布以上大网段路由，请将其拆分为以下网段组合发布：

`9.0.0.0/8`

拆分为：`9.0.0.0/9` + `9.128.0.0/9`。

`10.0.0.0/8`

拆分为：`10.0.0.0/9` + `10.128.0.0/9`。

`11.0.0.0/8`

拆分为：`11.0.0.0/9` + `11.128.0.0/9`。

`30.0.0.0/8`

拆分为：`30.0.0.0/9` + `30.128.0.0/9`。

`100.64.0.0/10`

拆分为：`100.64.0.0/11` + `100.96.0.0/11`。

`131.87.0.0/16`

拆分为：`131.87.0.0/17` + `131.87.128.0/17`。

`172.16.0.0/12`

拆分为：`172.16.0.0/13` + `172.24.0.0/13`。

`192.168.0.0/16`

拆分为：`192.168.0.0/17` + `192.168.128.0/17`。

变更通道路由

说明：

本文以独享专用通道为例，共享专用通道同理。

1. 登录 专线接入控制台，在左侧导航栏单击**独享专用通道**。

2. 在“专用通道”页面，在需要变更参数的通道右侧“操作”列选择**通道变更**。

3. 按您的专用通道类型，选择对应的方式修改专用通道信息，专用通道类型请在该通道“基本信息”页面查看。

专用通道1.0

在“通道变更”对话框中编辑以下信息，并单击**确定**。

字段	说明
带宽上限	专用通道的最大带宽值，不可超过关联的物理专线的带宽值。月95后付费的计费模式下，“带宽”参数不代表计费带宽。修改带宽上线灰度中，若需体验，请提 工单申请。
腾讯云边界 IP	物理专线腾讯云侧的边界互联 IP。变更腾讯云边界 IP 会中断业务，请谨慎操作。
用户边界 IP	物理专线用户侧（或运营商网络侧）互联 IP。变更用户边界 IP 会中断业务，请谨慎操作。
BGP ASN	输入 CPE 侧的 BGP 邻居 AS 号，腾讯云 ASN 为 45090。若不输入将由系统随机分配。
BGP 密钥	输入 BGP 邻居的 MD5 值。默认 "tencent"，留空表示不需要 BGP 密钥。BGP 密钥不支持 ? & 空格" \\ +六种特殊字符。

专用通道 2.0

在“高级通道”页签中，按需修改以下信息：

修改通道配置

在“通道配置”右侧单击**编辑**，然后在展开的编辑页面修改腾讯云边界 IP、用户边界 IP 和 VLAN ID、Jumbo 帧等信息，并单击**保存**。

说明：

帧是数据链路层的协议数据单元，由很多个字节组成，以太网帧大小一般为1500字节，实际传输的帧的大小通常由设备的最大传输单元 MTU 来确定，即设备单次能够传输的最大字节数。Jumbo 帧是比标准以太网帧更大的帧，通常可称为巨型帧。

字段	说明
腾讯云边界 IP	物理专线腾讯云侧的边界互联 IP。变更腾讯云边界 IP 会中断业务，请谨慎操作。
用户边界 IP	物理专线用户侧（或运营商网络侧）互联 IP。变更用户边界 IP 会中断业务，请谨慎操作。
VLAN ID	一个 VLAN 对应一个通道，取值范围为[0,3000]，若取值为0，代表仅能创建一个专用通道。MSTP 专线透传多 VLAN 时，需运营商线路开启 Trunk 模式。
Jumbo 帧	巨型以太网帧，专用通道2.0支持 Jumbo 巨型帧。其最大传输单元（MTU）为9001 Byte，系

	统默认未开启（1464 Byte），如需开启该功能，请提交 工单申请。

编辑路由模式

3.1.1 在“路由模式”右侧单击**编辑**，并在展开区域内修改路由信息。

静态路由模式：修改用户 IDC 网段信息。为确保网络的精细化调度能力，IDC 网段信息请遵循 大网段使用限制。

BGP 路由模式：修改 BGP asn 和 BGP 密钥。

字段	说明
BGP asn	输入 CPE 侧的 BGP 邻居 AS 号，腾讯云 ASN 为 45090。若不输入将由系统随机分配。
BGP 密钥	输入 BGP 邻居的 MD5 值。默认 "tencent"，留空表示不需要 BGP 密钥。BGP 密钥不支持 ? & 空格" \\ +六种特殊字符。

3.1.2 变更健康检查。

详情请参见 专用通道健康检查。

3.1.3 单击**保存**。

通道变更需求提交后，系统将在几分钟内（具体时间依据网络情况而定）完成设备配置。

探测专用通道

最近更新时间：2024-11-05 11:05:18

专线接入控制台提供专用通道网络探测工具，可以从腾讯云侧向 IDC 侧的互联 IP 发送探测包来测试网络连通性。建议您在 申请专用通道 或 修改专用通道 后，使用通道工具来测试腾讯云到 IDC 侧的网络连通性。

前提条件

如果您在专用通道2.0中需要开通 Ping 功能，请提交 工单申请。
您的专用通道类型为2.0，专用通道类型请在该通道**基本信息**页面查看。

操作步骤

1. 登录 专线接入控制台，在左侧导航栏单击**独享专用通道**。
2. 在专用通道列表中，单击目标专用通道的 ID。
3. 在**独享专用通道**详情页面，单击**通道工具**页签。
4. 在**通道工具**页面，设置探测包量和探测包长，然后单击**开始探测**。根据探测 loss 延时情况判断网络是否连通。

删除专用通道

最近更新时间：2024-11-05 11:05:18

说明：

为了保护通道使用者的业务正常，已共享的通道仅能更改带宽，不允许删除。

1. 登录 专线接入控制台 。
2. 单击左侧导航栏中**独享专用通道**，进入管理页面。
3. 在列表中找到需要删除的专用通道，选择**删除** > **删除**。
4. 通道删除未完成时，无法创建相同 VLAN ID 的专用通道。

专用通道健康检查

最近更新时间：2024-11-05 11:05:18

当专用通道状态为“已连接”后，您还可以在专线接入控制台进行变更通道参数、修改通道带宽、通道健康检查等操作。本文将介绍通道2.0如何在控制台进行通道健康检查。

说明：

共享专线模式下，专用通道无法进行带宽变更，需由物理专线所有者发起带宽变更。

前提条件

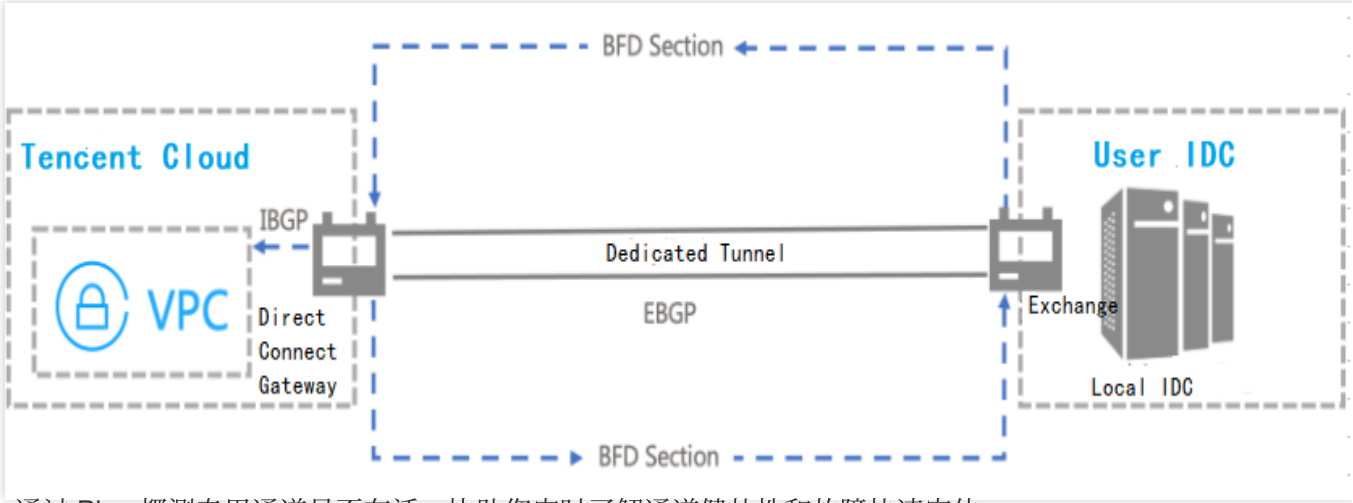
在变更通道前，需已 申请通道。

专用通道已做主备。

背景信息

腾讯云专线接入提供了 BFD 和 NQA 两种专用通道健康检查方法：

BFD：在网络设备间建立会话，用来检测网络设备间的双向转发路径。建立会话后周期性发送报文，如果检测时间内没有收到报文则认为该路径故障，将检测结果反馈给其所服务的应用。目前 BFD 支持 BGP 和静态两种路由模式联动。



NQA：通过 Ping 探测专用通道是否存活，协助您实时了解通道健壮性和故障快速定位。

创建通道后配置健康检查

1. 登录 专线接入控制台，在左侧导航栏单击**独享专用通道**。

2. 在“独享专用通道”页面，单击待健康检查的通道名称。
3. 在通道详情页的**高级配置**页签中，单击**路由模式**右侧**编辑**。
4. 在**健康检查**所在行开启该功能。
5. 配置健康检查参数。

健康检查配置参数	含义	取值范围
健康检查间隔	两次健康检查间隔时间。	BFD：1000ms - 3000ms，默认值1000ms。 NQA：1000ms - 5000ms，默认值2000ms。
健康检查次数	如果连续执行设定次数的健康检查失败后，则执行路由切换。	BFD：3 - 8，默认值3。 NQA：3 - 8，默认值5。

说明：
路由模式不同，专用通道所支持的健康检查方式不同。目前 BGP 路由模式的专用通道仅支持与 BFD 联动进行通道健康检查。静态路由模式的专用通道支持 BFD 和 NQA 两种健康检查方式。
静态路由模式的专用通道支持 NQA 和 BFD 两种模式相互切换，切换后，系统依据当前的模式进行健康检查。
6. 单击**保存**。

创建通道过程中配置健康检查

1. 登录 专线接入控制台，在左侧导航栏单击独享专用通道。
2. 在“专用通道”页面单击**新建**，然后在创建页面完成**基本配置**，并在**高级配置**中依据界面提示完成其他参数以及健康检查配置。
本节仅介绍健康检查如何配置，其他参数配置请参见 独享专用通道 或者 共享专用通道。

健康检查配置参数	含义	取值范围
健康检查间隔	两次健康检查间隔时间。	BFD：1000ms - 3000ms，默认值1000ms。 NQA：1000ms - 5000ms，默认值2000ms。
健康检查次数	如果连续执行设定次数的健康检查失败后，则执行路由切换。	BFD：3 - 8，默认值3。 NQA：3 - 8，默认值5。

说明：

路由模式不同，专用通道所支持的健康检查方式不同。目前 BGP 路由模式的专用通道仅支持与 BFD 联动进行通道健康检查。静态路由模式的专用通道支持 BFD 和 NQA 两种健康检查方式。

静态路由模式的专用通道支持 NQA 和 BFD 两种模式相互切换，切换后，系统依据当前的模式进行健康检查。

3. 单击**下一步**，然后继续通道配置直至创建完成。

修改专用通道带宽

最近更新时间：2024-11-05 11:05:18

当专用通道状态为**已连接**后，您还可以在专线接入控制台进行变更通道参数、修改通道带宽等操作。本文将介绍通道1.0和通道2.0如何在控制台修改带宽。

说明：

共享专线模式下，专用通道无法进行带宽变更，需由物理专线所有者发起带宽变更。

前提条件

在变更通道前，需已 申请通道。

专用通道 1.0

1. 登录 专线接入控制台，在左侧导航栏单击**独享专用通道**。
2. 在**独享专用通道**页面，在需要变更参数的通道右侧**操作**列选择**更多 > 通道变更**。
3. 在**通道变更**对话框中调整带宽上限，并单击**确定**。

说明：

大于1Gbps带宽的通道带宽升配，调整步长须为1Gbps整数倍调整，即1G升配时只能调整为2Gbps、3Gbps类似的整值。

专用通道 2.0

1. 登录 专线接入控制台，在左侧导航栏单击**独享专用通道**。
2. 在独享专用通道列表中目标通道右侧**带宽**列单击

。

说明：

仅连接状态为**已连接**的专用通道可以修改带宽。

3. 在展开的编辑框中修改通道带宽值，并单击**确定**。

说明：

专用通道最大带宽不可超过关联的物理专线带宽，若物理专线带宽仍不能满足您的业务需求，请提 工单申请 扩容。

监控与告警
查看监控信息

最近更新时间：2024-11-05 11:05:18

您可以在腾讯云控制台，查看物理专线或专用通道的网络监控数据，帮助您排查网络故障。您还可以通过 API 查看监控信息，详情请参见 专线接入-物理专线监控指标。

操作步骤

1. 登录 专线接入 控制台。
2. 查看物理专线网络监控数据。
3. 在左侧导航栏单击**物理专线**。
4. 在物理专线列表中，单击目标物理专线“监控”列的

。

说明：

状态为“运营中”的物理专线才支持查看监控数据。

5. 在监控详情页面，可查看网络出带宽、网络入带宽数据，并通过单击**近24小时**、**近7天**或自定义日期，调整监控数据的时间轴。

网络出带宽：物理专线的平均每秒出流量。

网络入带宽：物理专线的平均每秒入流量。

端口丢包：端口每分钟丢包的个数。

端口错包：端口每分钟错包的个数。

6. 查看专用通道网络监控数据。
7. 在左侧导航栏单击**独享专用通道**。
8. 在专用通道列表页面，单击目标专用“监控”列的

。

9. 在监控详情页面，可查看网络出带宽、网络入带宽、出包量、入包量数据，并通过单击**近24小时**、**近7天**或自定义日期，调整监控数据的时间轴。

网络出带宽：专用通道的平均每秒出流量。

网络入带宽：专用通道的平均每秒入流量。

出包量：专用通道出方向的流量累计值。

入包量：专用通道入方向的流量累计值。

10. 查看专线网关监控数据。
11. 在左侧导航栏单击**专线网关**。
12. 在专线网关页面，单击目标专线网关右侧”监控“列的

。
13. 在监控详情页面，可查看专线网关的网络出带宽、网络入带宽、出包量、入包量、出流量、入流量数据，并通过单击**近24小时**、**近7天**或自定义日期，调整监控数据的时间轴。

网络出带宽：专线网关的平均每秒出流量。
网络入带宽：专线网关的平均每秒入流量。
出包量：专用通道出方向的流量包累计值。
入包量：专用通道入方向的流量包累计值。
出流量：专用通道出方向的流量累计值。
入流量：专用通道入方向的流量累计值。
出方向丢包量：专用通道出方向的丢包累计值。
入方向丢包量：专用通道出入向的丢包累计值。

配置告警

最近更新时间：2024-11-05 11:05:18

通过云监控，您可以制定针对物理专线、专用通道、专线网关的告警规则。当规则被触发时，系统将以您指定的告警渠道发送告警信息，您可以根据告警信息判断是否采取问题解决措施。

操作步骤

1. 登录 云监控 控制台，并在左侧导航栏选择**告警配置 > 告警策略**。
2. 在“告警策略”页面单击**新建**。
3. 在“新建策略”页面进行以下配置：
4. 编辑“策略名称”和“备注”，并根据实际需求选择“策略类型”，策略类型包括 物理专线、专用通道、专线网关。

说明：

若需选择”专线网关“，则在 VPC 产品下选择。

5. 根据实际需求选择该报警策略所属项目，每个项目可以创建300条报警策略。
6. 设置告警对象。

若选择全部对象，则该告警策略绑定当前账号的全部实例。

若指定具体实例，则该告警策略绑定用户选中的实例。

若选择实例组，则该告警策略绑定用户选中的实例分组。若您没有实例组，可以单击**新建实例组**进行创建。

7. 选择以下任意一种方式设置告警触发条件。

使用现有模板

勾选“选择模板”，在下拉列表中选择配置好的模板。

说明：

若您没有告警规则模板，请单击**新增触发条件模板**进行配置，具体配置请参见 配置触发条件模板。若新建的模板没有显示，请单击右侧的**刷新**。

手动配置

选择“手动配置”后请按需设置触发条件，如果需要新建指标，请单击“添加指标”。指标详情请参见 告警指标说明。

例如，若指定指标为 “入带宽” 、“统计周期1分钟” 、比较关系为 “>” 、阈值为 “100个 Mbps” 、持续周期为 “持续2个周期” 、重复通知为 “每1天警告一次” 则表示：每1分钟收集一次入带宽数据，若某个物理专线/专用通道/专线网关的入带宽连续两次大于100 Mbps，则触发告警，且每天警告一次。

说明：

若需配置多条告警触发条件，则单击**添加**进行配置。当有多条触发条件时，请根据实际选择满足所有条件或任意条件时触发告警。

如果需要配置事件告警，请参见 快速配置云监控事件告警推送。

8. 配置告警通知。

告警通知接收人配置在通知模板中，如果使用现有模板，请单击“选择模板”，选中已有的模板；如果新建模板，请单

击“新建模板”，并依据界面提示完成创建。

9. （可选）接口回调配置。

9.1 单击“新建模板”，并在弹出的对话框中单击“更多配置请到通知模板页”。

9.2 在“新建通知模板”页面填写通知模板信息，和公网可访问到的 url 作为回调接口地址（域名或 IP[:端口][/path]）。

9.3 返回告警策略配置页面，选择刚所创建的通知模板。

云监控将及时把告警信息推送到该地址。

10. 完成配置后，单击**完成**。

管理告警策略

创建告警策略后，您可以在控制台进行启停、复制、删除等操作。

1. 在 云监控 控制台左侧导航栏选择**告警配置** > **告警策略**。

2. 按需在“告警策略”页面进行以下操作：

若需停用该策略，则在目标告警策略右侧“告警启停”列关闭开关，若需启用该告警策略，则打开开关。

若需复制该策略，则在目标告警策略右侧“操作”列单击**复制**，并在“新建策略”页面按需修改策略，然后单击**完成**。

若需查看历史告警，则在目标告警策略右侧“操作”列单击**告警历史**。

若需删除该策略，则在目标告警策略右侧“操作”列单击**删除**，并在确认框中单击**确认**。

告警说明

最近更新时间：2024-11-05 11:05:18

本文列出了物理专线、专用通道或专线网关的指标告警指标说明和事件信息说明，帮助您配置告警。

告警指标说明

若为物理专线创建告警策略，则可以配置指标为出带宽、入带宽、带宽使用率的触发条件；若为专用通道配置告警策略，则可以配置指标为出带宽、入带宽的触发条件；若为专线网关配置告警策略，可配置指标为出带宽、入带宽、出包量、入包量的触发条件。

指标	含义
出带宽	物理专线/专用通道/专线网关的平均每秒出流量。
入带宽	物理专线/专用通道/专线网关的平均每秒入流量。
带宽使用率	当前带宽值/物理专线带宽值*100%。
出包量	专线网关的平均每秒出包量。
入包量	专线网关的平均每秒入包量。

告警事件说明

若为物理专线创建告警事件，则可以配置物理专线 Down 为触发条件；若为专用通道配置告警事件，则可以配置专用通道 Down、专用通道 BGP 会话 Down、BGP 通道路由条目超限告警和专用通道 BFD 检测 Down 为触发条件。

事件中文名	事件英文名	事件类型	从属维度	有无恢复概念	事件描述	处理方法和建议
物理专线 Down	DirectConnect Down	异常事件	物理专线维度	有	专线物理链路传输中断或异常	1. 检查物理线路是否有异常中断情况（如光纤被挖断，线路被拔出设备等）。 2. 检查对接端口及光/电模块是否正常。

						3. 检查网络设备端口是否被关闭。
专用通道 Down	DirectConnectTunnelDown	异常事件	专用通道维度	有	专线物理链路传输中断或异常	1. 检查物理线路是否有异常中断情况（如光纤被挖断，线路被拔出设备等）。 2. 检查对接端口及光/电模块是否正常。 3. 检查网络设备端口是否被关闭。
专用通道 BGP 会话 Down	DirectConnectTunnelBGPSessionDown	异常事件	专用通道维度	有	专用通道 BGP 会话状态中断	1. 检查网络设备 BGP 进程是否正常。 2. 检查专用通道是否正常。 3. 检查物理线路是否正常。
BGP 通道路由条目超限告警	DirectConnectTunnelRouteTableOverload	异常事件	专用通道维度	无	专用通道 BGP 会话通道路由条目超过80%	检查专用通道 BGP 会话发布路由条目是否达到限制条目的80%（默认限制100条，详情请参见专线接入 使用限制）。
专用通道 BFD 检测 Down	DirectConnectTunnelBFDDown	异常事件	专用通道维度	有	专用通道 BFD 检测中断	1. 检查专用通道是否正常。 2. 检查物理线路是否正常。

查看告警信息

最近更新时间：2024-11-05 11:05:18

为物理专线、专用通道或专线网关配置指标告警/事件告警策略后，可以在云监控控制台查看告警历史和具体事件信息。

前提条件

您已配置告警策略，具体请参见 配置告警。

查看告警历史

1. 登录腾讯云可观测平台，并在左侧导航栏单击**告警历史**。
2. 在“告警历史”页面上方选择告警历史的时间段。
“告警历史”页面展示了告警对象、告警内容、持续时长、告警状态等内容。

查看产品事件

腾讯会自动检测物理专线和专用通道的异常状态，当端口/链路未正常连接时，会将该异常信息同步至云监控产品事件平台。您可以在产品事件平台查看近30天内的产品事件状态，其中包含已配置告警策略和未配置告警策略的产品事件，您可以根据实际需求为未配置告警策略的产品事件添加告警策略。
1. 登录 云监控控制台，并在左侧导航栏中选择**事件中心 > 产品事件**。
2. 在“产品事件”页面上方双击搜索栏中的“产品类型:全部”中的“全部”，并在下拉框中选择**物理专线**或**专用通道**，然后单击**完成**。
说明：
产品事件列表中默认展示了当前账号下自定义时间段内所有物理专线或专用通道的事件信息，包含事件类型、影响对象、对象详情、事件状态、开始时间等信息。
3. 若需为未配置告警策略的产品事件配置告警，则在该产品事件右侧“告警配置”列单击**新增配置**，并在“新建策略”页面按需修改策略，然后单击**完成**。

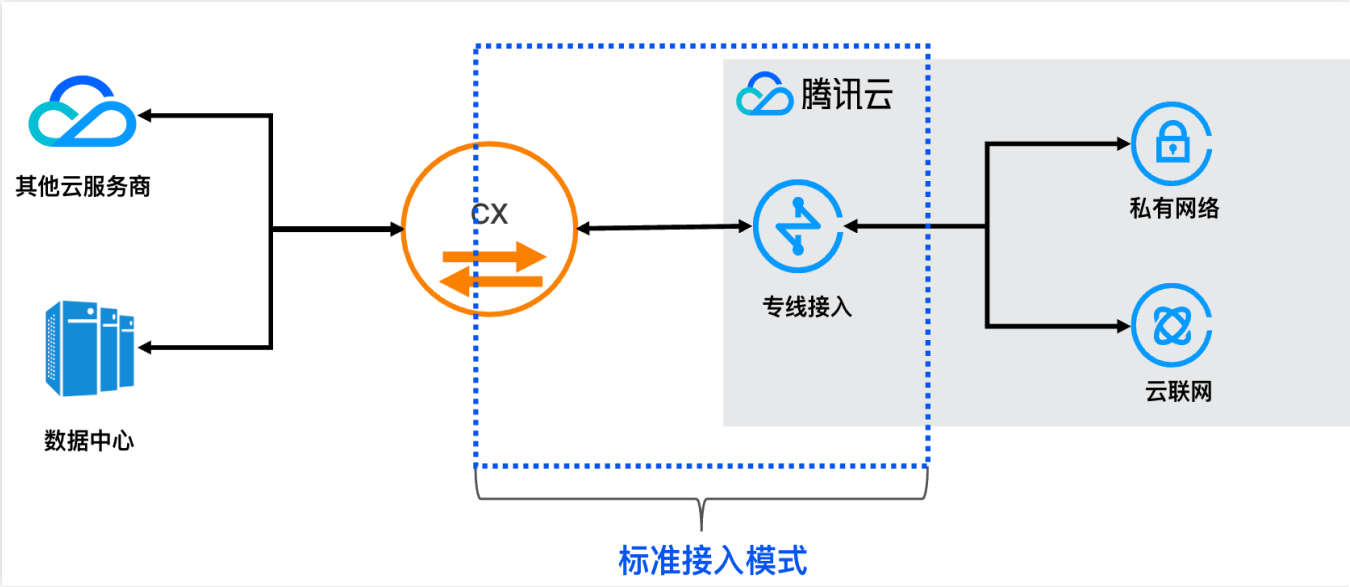
云交换
云交换简介

最近更新时间：2025-01-21 15:23:01

云交换服务（Cloud Exchange，简称 CX）是腾讯云专线与 CX 平台在国际/港澳台地区合作构建的生态共同体，为客户在海外提供互通服务。目前云交换服务提供两种模式：标准接入模式、一站式接入模式。

标准接入模式

标准接入模式下，腾讯云预先与 CX 平台建立预连接资源，帮助拥有 CX 平台账号的客户快速上云。腾讯云的服务边界为 CX 平台 - 腾讯云，即对端云 - CX 平台部分需由客户联系 CX 平台或对端云进行管理和运维。

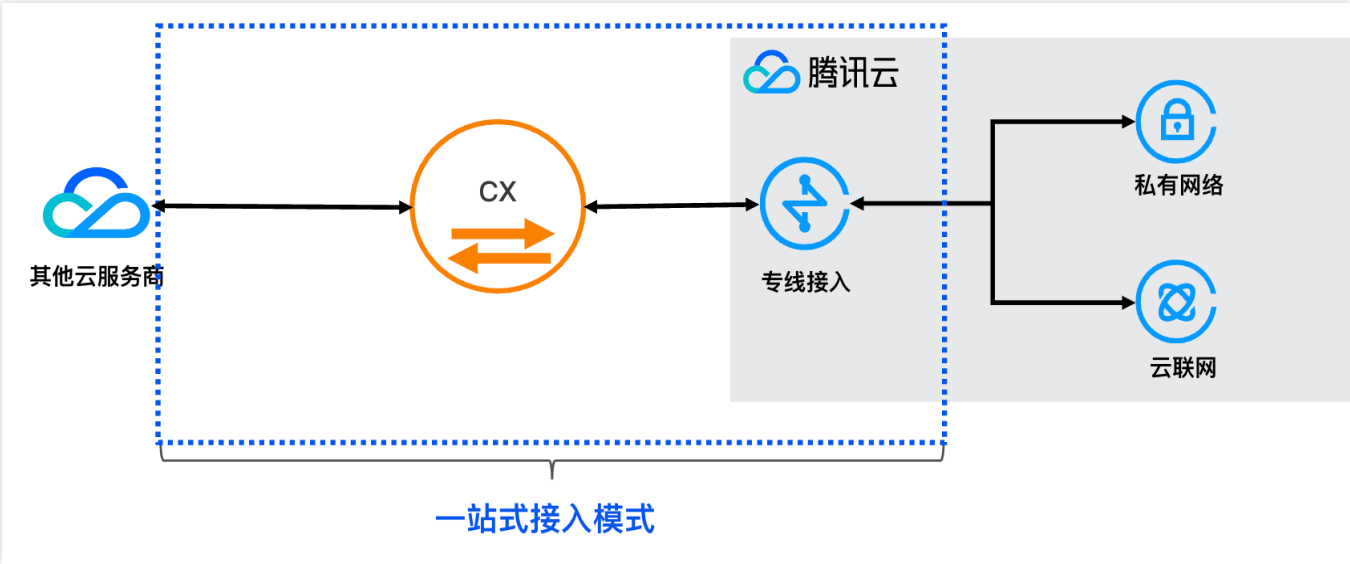


一站式接入模式

一站式接入模式，腾讯云预先与 CX 平台建立预连接资源，且借助 CX 平台与对端云互联的资源，帮助客户实现对端云 - 腾讯云的端到端互通，适用无 CX 平台账号的客户。客户无需感知 CX 平台，只需在腾讯云和对端云平台进行资源创建、接收、管理，即可实现端到端互通。

注意：

腾讯云为对端云 - 腾讯云的端到端运维提供支持，在出现故障后，腾讯云会尽力协查端到端和配合故障恢复，但是 CX 平台 - 对端云线路最终维护方为对端云或 CX 平台。



说明：

接入时请使用双线双点接入模式，其他模式腾讯云无法保证服务可用性。

一个 CX 实例仅能创建一个专用通道。

产品优势

多云部署

支持混合云、多云的部署架构，与境外云交换供应商合作，将腾讯云网络与境外的云服务商、境外数据中心的网络连接。

避免单一云服务故障时的服务宕机。

使用第二个云或数据中心进行灾难恢复。

可以与 AWS、微软等境外知名云厂商的云服务互通，避免受制于单一供应商。

快速上云

传统的接入模式下，打通用户的境外数据中心与腾讯云需要经过较为繁复的步骤，需要分别打通境外运营、布线、云上资源 VPC 等。云交换服务是腾讯云专线与境外云交换供应商合作，预先建立的物理交换链路，以云交换商为桥梁打通各大云厂商。

建设周期短，2~3工作日可以完成云间互通。

复杂性降低，可一键式腾讯云资源构建，为您省去繁琐的配置。

计费概述

最近更新时间：2025-01-21 15:26:16

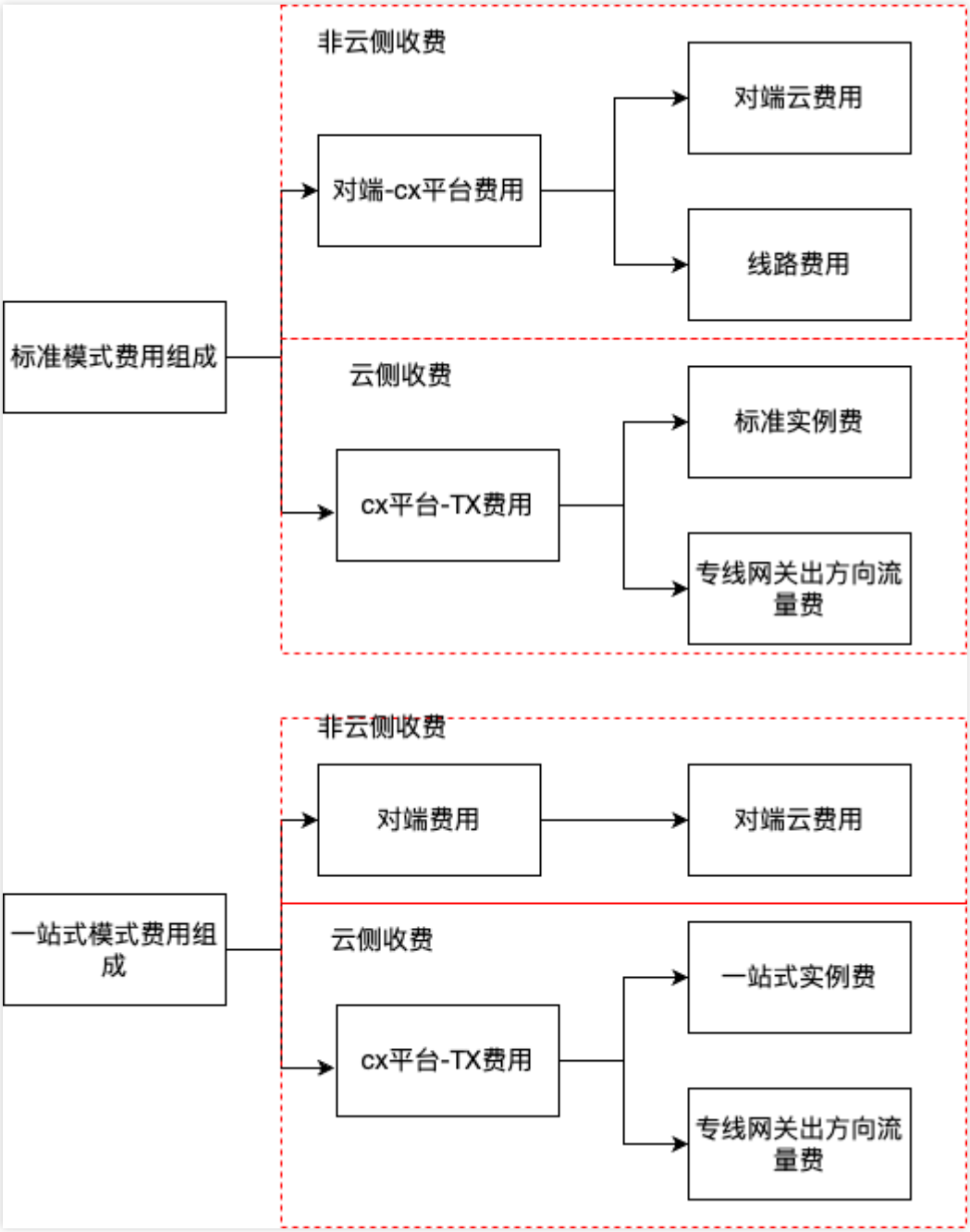
本文对专线云交换的计费和定价进行说明。

云交换支持的 CX 平台及地域

地域	接入点	EQUINIX	Megaport
日本东京	东京 - B - 有明	支持	-
新加坡	新加坡 - A - 亚逸拉惹	支持	支持
	新加坡 - B - 大成	支持	-
香港	中国香港 - A - 葵涌	支持	-
	中国香港 - B - 将军澳	支持	-
圣保罗	圣保罗 - A - 圣安娜	支持	-

计费说明

专线云交换接客模式不同，计费定价不同：
标准模式的费用由两部分组成：CX 云交换标准实例费、专线网关流量费。
一站式模式的费用由两部分组成：CX 云交换一站式实例费、专线网关流量费。
具体组成部分由下图所示：



注意：

专线网关流量费，详情可参见 专线接入计费概述。

标准模式

标准实例费：计费方式为日结后付费，每天产生的费用，将于次日进行扣费。

计费时间：当您在控制台单击 CX 实例接收且建设成功后，实例状态变更为“运营中”，开始收取费用。当您在云交换控制台申请裁撤实例且申请通过后，实例状态变更为“已裁撤”，停止收取费用。若计费时间不足一天，则按照实际有效小时收取。

计费公式：实例费用 =（当天有效小时/当天自然小时）* 实例单价。

带宽（Mbps）	国际站/中国站刊例价 (美金/天)
50	0.71
100	1.39
200	1.94
300	2.83
400	3.68
500	4.49
1000	7.96
2000	15.91
5000	39.85
10000	70.82
25000	149.83

一站式模式

标准实例费：计费方式为日结后付费，每天产生的费用，将于次日进行扣费。

计费时间：当您在控制台单击 CX 实例接收且建设成功后，实例状态变更为“运营中”，开始收取费用。当您在云交换控制台申请裁撤实例且申请通过后，实例状态变更为“已裁撤”，停止收取费用。若计费时间不足一天，则按照实际有效小时收取。

计费公式：实例费用 =（当天有效小时/当天自然小时）* 实例单价。

带宽规格（Mbps）	国际站/中国站刊例价（美金/天）
50	15
100	30
200	60
300	90
400	120
500	150

1000	233
2000	467
5000	1000
10000	2000
25000	5000

欠费说明

最近更新时间：2025-01-22 09:49:06

本文为您介绍专线云交换费用预警和欠费处理。

欠费停服说明：

资源	欠费保护期	停服隔离期	销毁时间
CX 云交换实例	1天	7天	账户欠费8天，且账户余额持续为负值

欠费保护期：当账户余额为负值时，资源继续提供服务并持续扣费。

停服隔离期：当账户余额为负值时，资源停止服务并停止扣费，资源暂时保留，后续账户余额充值为正后，可自动恢复服务并恢复计费。

销毁时间：账户余额为负值且时间到达销毁时间后，系统将对资源启动销毁，销毁动作执行后资源不可恢复，请知悉。

实践教程
标准模式

最近更新时间：2025-01-22 09:52:37

标准模式下，需要您优先创建 CX 平台的账号，并完成 CX 平台到对端的互联，对端类型可以为客户数据中心（IDC）或者其他云。
本文以在 Equinix 平台实现腾讯云和 AWS 云互通为例，进行实践教程介绍。不同的 CX 平台和不同的对端，其互联的详细操作略有不同，您可以根据需要进入相应的 CX 平台进行创建操作步骤。

前提条件

1. 您已拥有 equinix fabric 账号。
2. 您的 equinix fabric 账号在需要建立连接的地域有 Port 或者 Virtual device。

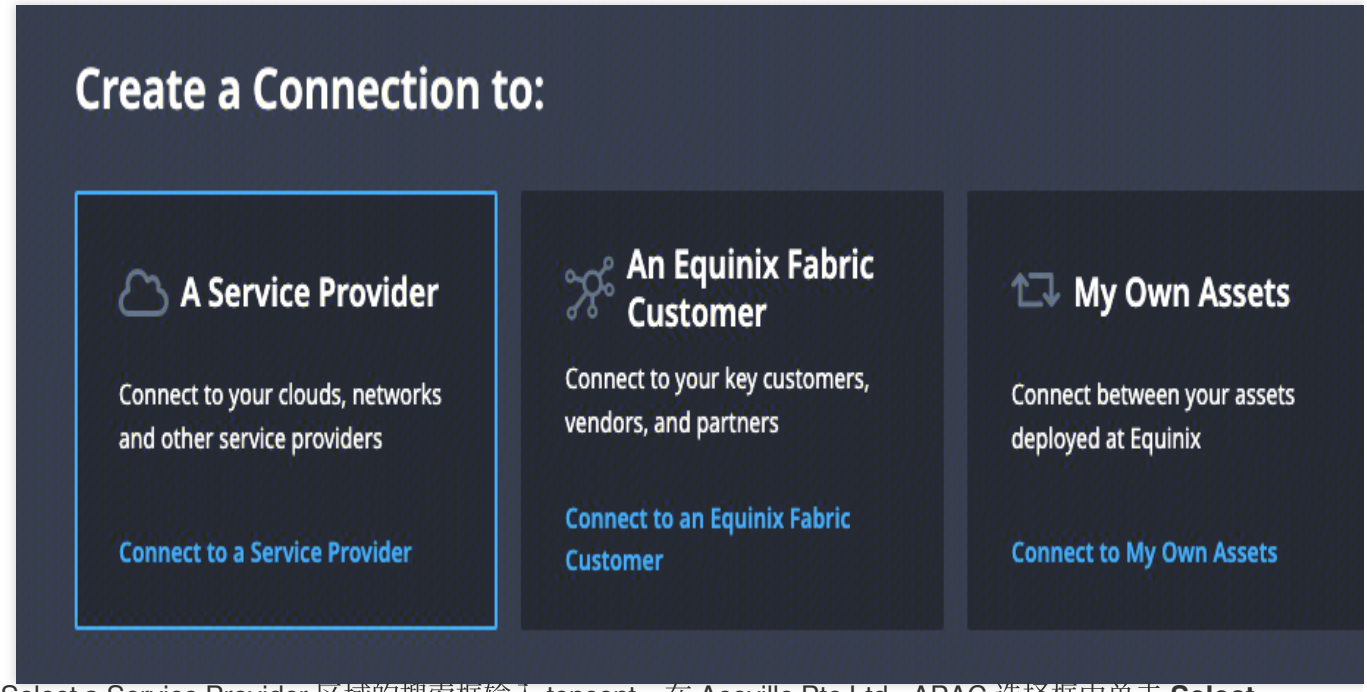
如果您暂无账号，您可以通过 equinix 页面联系销售或者自行创建。如果您对页面使用有疑问，可以联系 equinix 销售提供指导或者联系 equinix 在线服务获取支持。

操作步骤

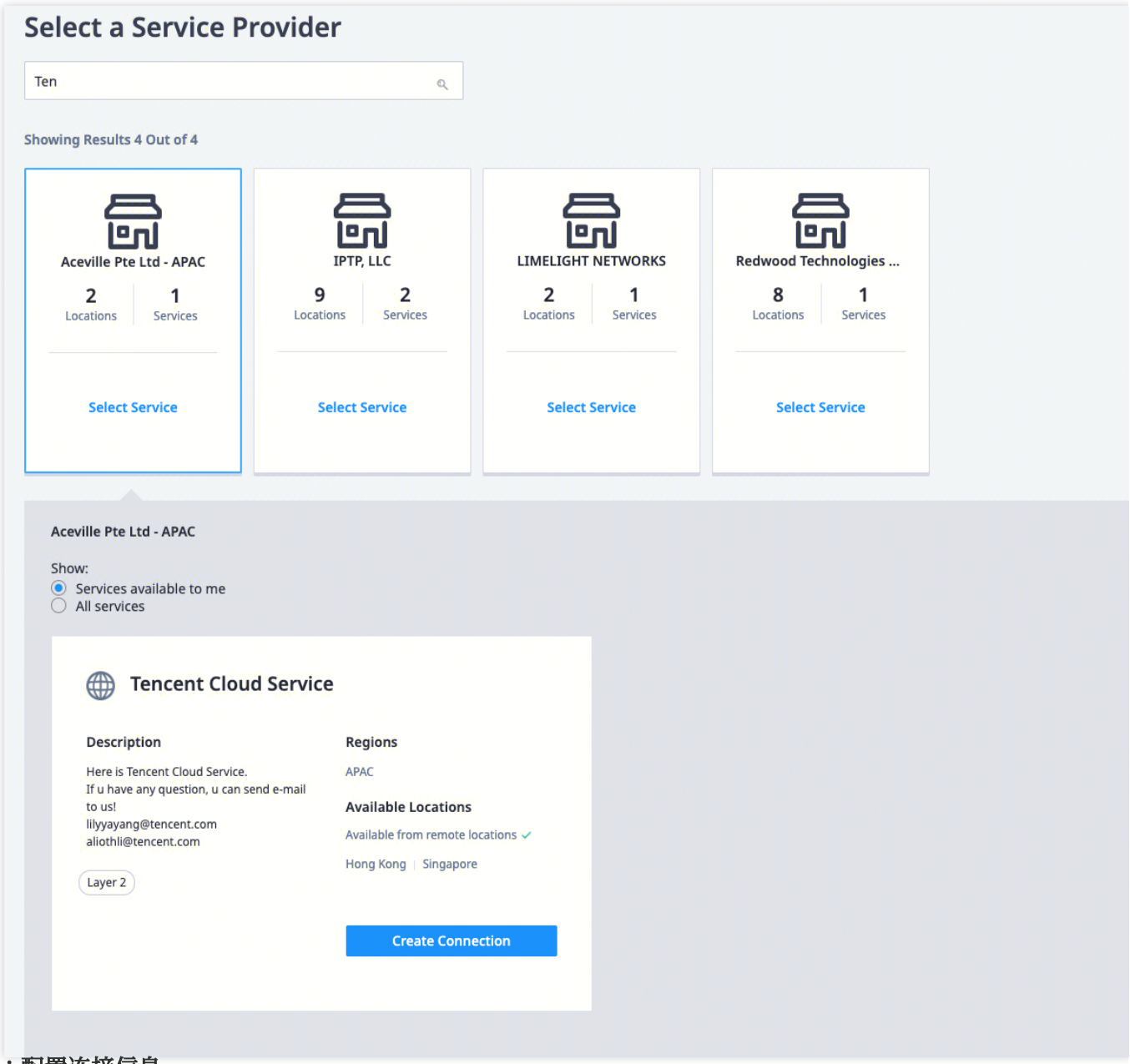
Equinix 侧下单

步骤1：选择服务提供者

1. 登录 Equinix Fabric。从 Connections 菜单中选择 Create Connection。
2. 单击 **A Service Provider**。

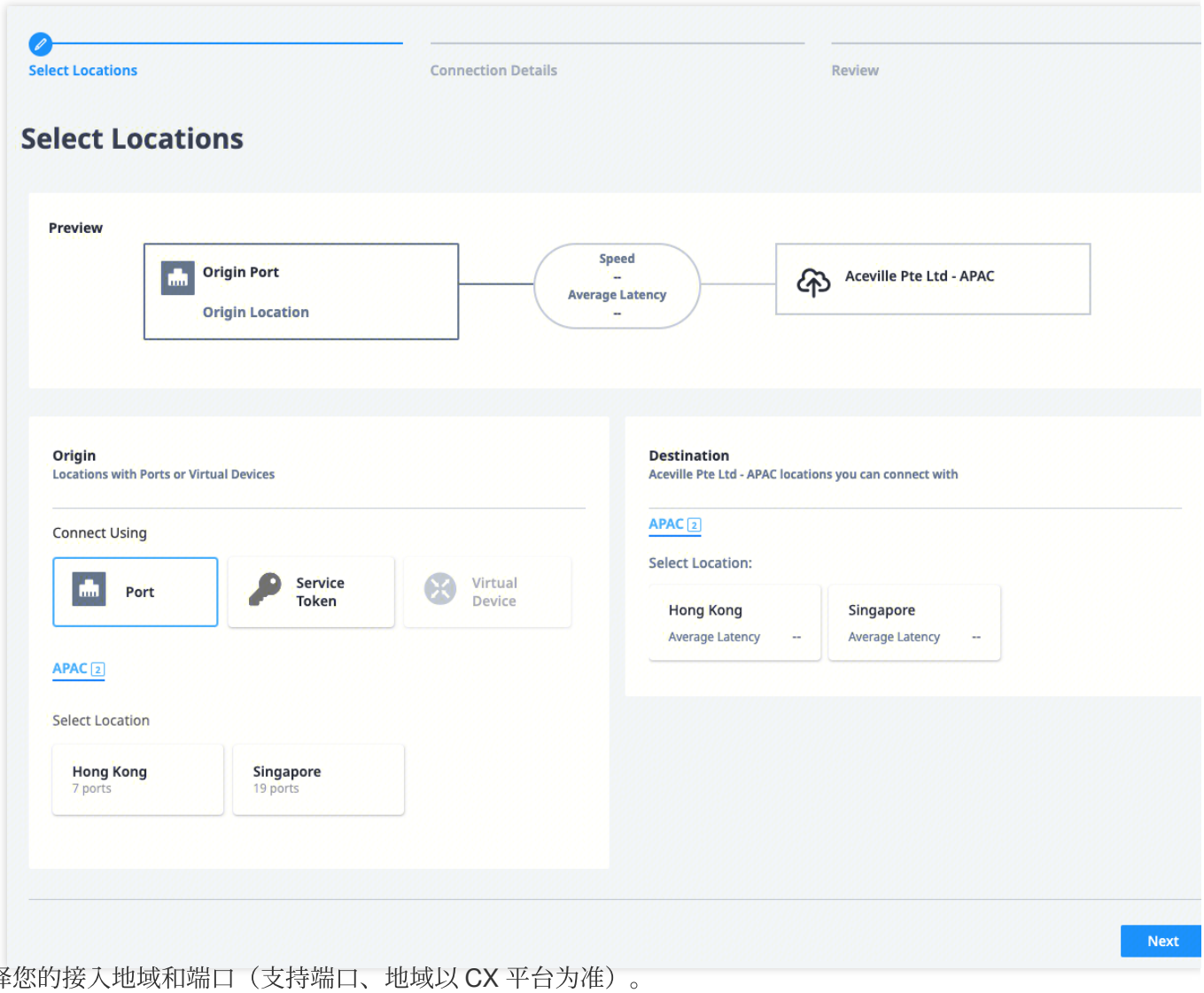


3. 在 Select a Service Provider 区域的搜索框输入 tencent，在 Aceville Pte Ltd - APAC 选择框中单击 **Select Service**，在弹出的浮窗中选择服务类型 **Services available to me**，并单击 **Create Connection**。

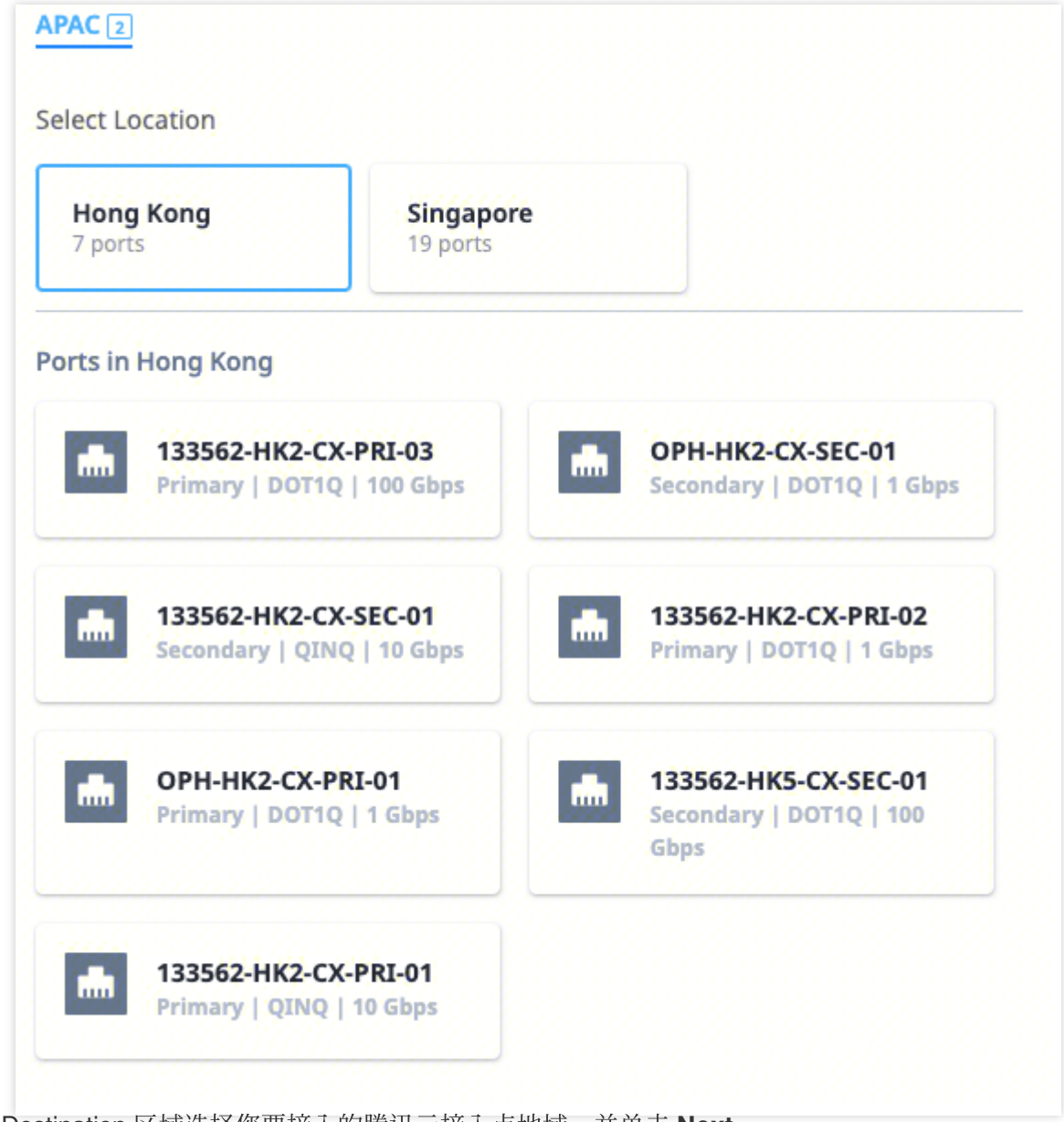


步骤2：配置连接信息

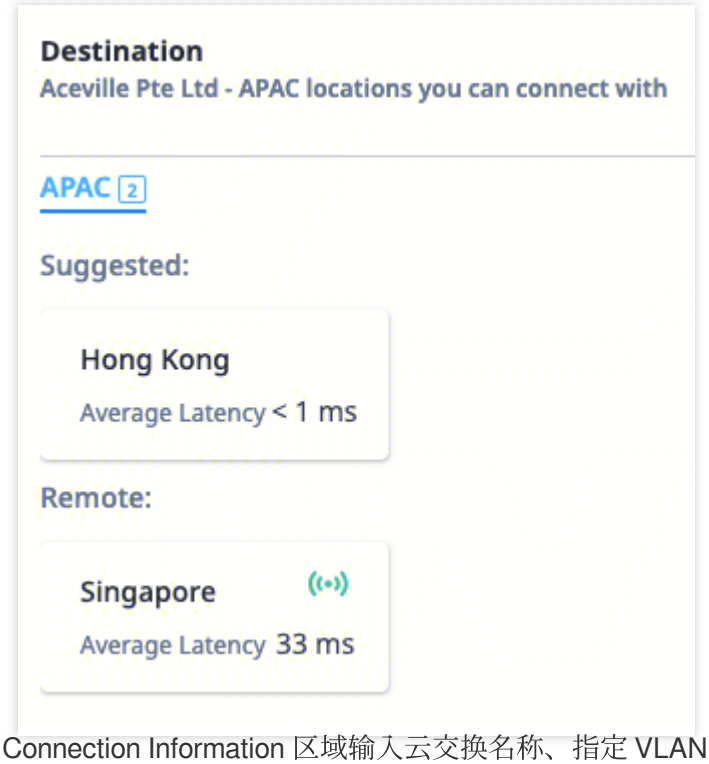
1. 在 Select Locations 的 Origin 配置区域单击 **Port** 或 **Virtual Device**。



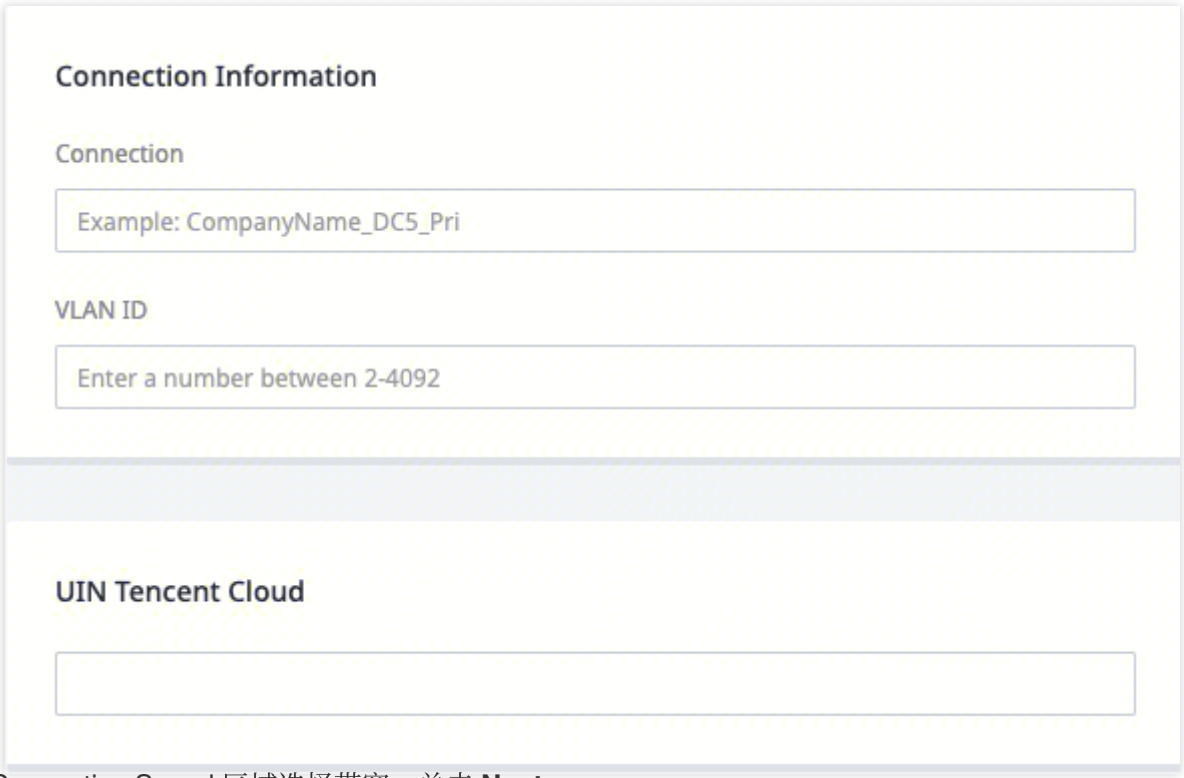
2. 选择您的接入地域和端口（支持端口、地域以 CX 平台为准）。



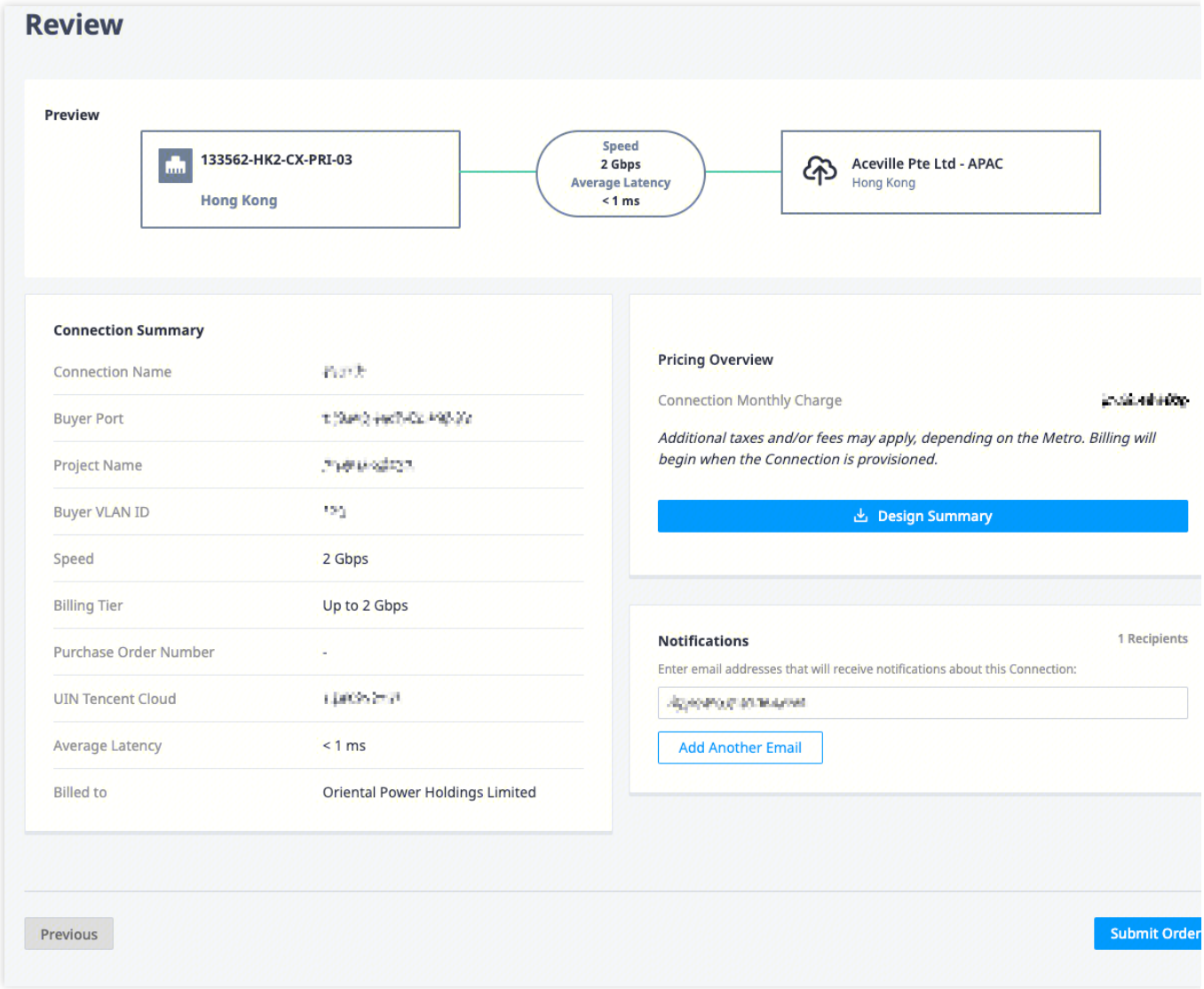
3. 在 Destination 区域选择您要接入的腾讯云接入点地域，并单击 **Next**。



4. 在 Connection Information 区域输入云交换名称、指定 VLAN ID 和 UIN（您用于互联的腾讯云账户 ID）。



5. 在 Connection Speed 区域选择带宽，单击 **Next**。
6. 在 Review 页面确认订单信息，单击 **Submit Order**。



腾讯云资源构建

1. 登录 专线接入控制台，在左侧导航单击**云交换**，进入云交换列表页。对云交换资源进行购买。

2. 当云交换实例状态为运营中，表示已和 Equinix 连通，可以创建腾讯云资源。您可以在具体实例所在行单击**一键构建云资源**，并在构建页面依据实际情况配置相应的参数，配置参数详情请参见 独享专用通道。

一站式部署

最近更新时间：2025-01-22 09:57:41

本场景适用于您没有 CX 平台账号，需要实现腾讯云与其他云互通的场景，此服务由腾讯云代替客户购买 CX 平台的连接服务，帮助客户实现一站式对接。
本文以在 Equinix 平台实现腾讯云和 AWS 云互通为例，进行实践教程介绍。
无论是不同的 CX 平台还是不同的对端云，客户仅需在腾讯云控制台和对端云控制台进行标准统一的操作。因此，本文适用于所有不同 CX 平台和不同对端云的一站式互联场景。

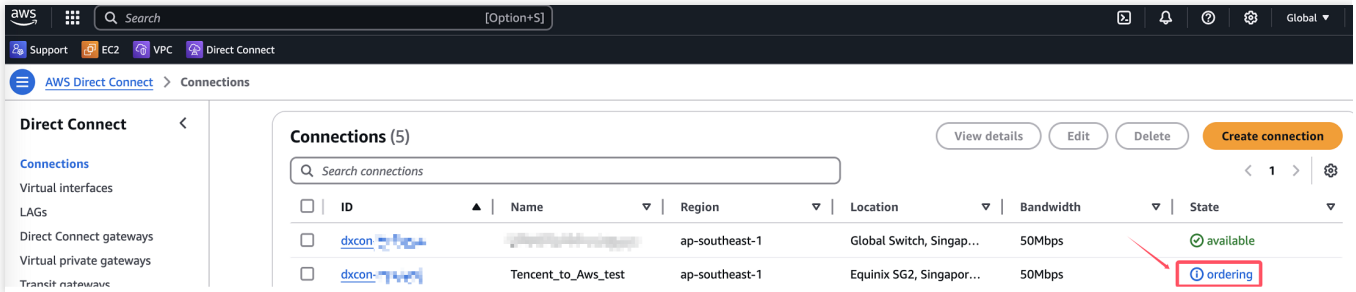
一、提供信息

若您有使用云交换的需求场景，请您先联系您的商务经理或者 提交工单 申请，我们将为您制定合适的组网方案。
同时，请您提前准备以下信息：
1. 对端云：例如 aws。
2. 对端地域：例如新加坡。
3. 对端云账号信息：例如 aws 账号 ID。
4. 带宽大小：例如10G*2。
5. 地域：例如新加坡。
6. 特殊需求：例如时延。
7. vlan 信息：例如2999。
在您提供上述信息后，我们将在第一时间进行资源核查，并在核查完成后及时通知您进行下一步操作。预计处理时间为1至7个工作日。

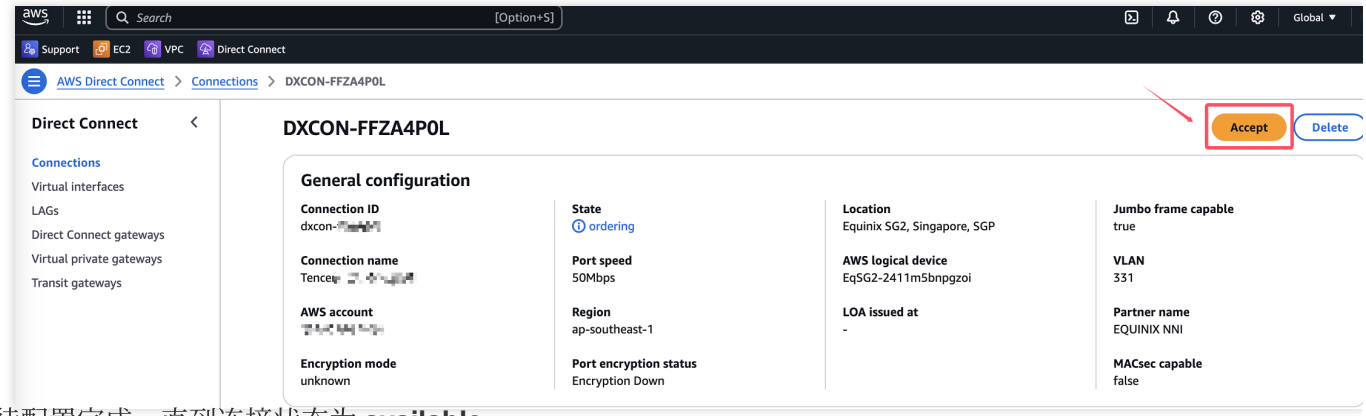
二、AWS 侧配置

步骤1：接受 CX 连接请求

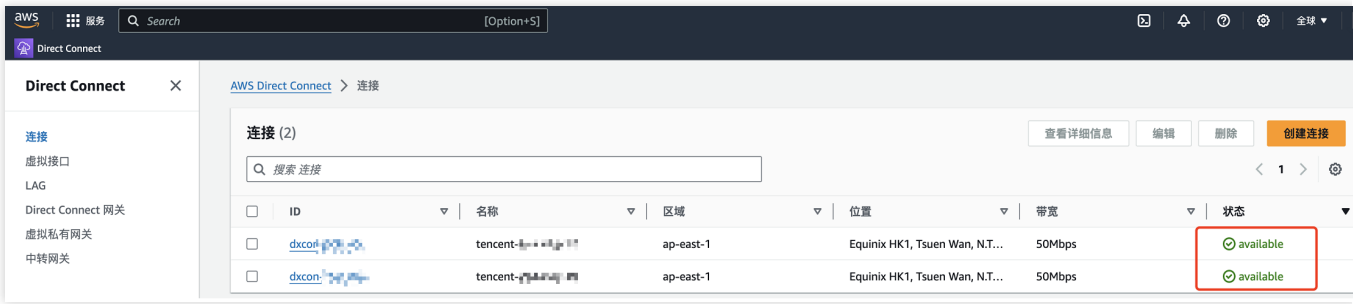
1. 登录 AWS 云的 Direct Connect 控制台，在左侧导航单击 **Connections**，进入连接列表页。单击 **ordering** 状态的连接 ID，查看连接详情。



2. 单击右侧 **Accept**，同意订购连接。



3. 等待配置完成，直到连接状态为 **available**。



说明：

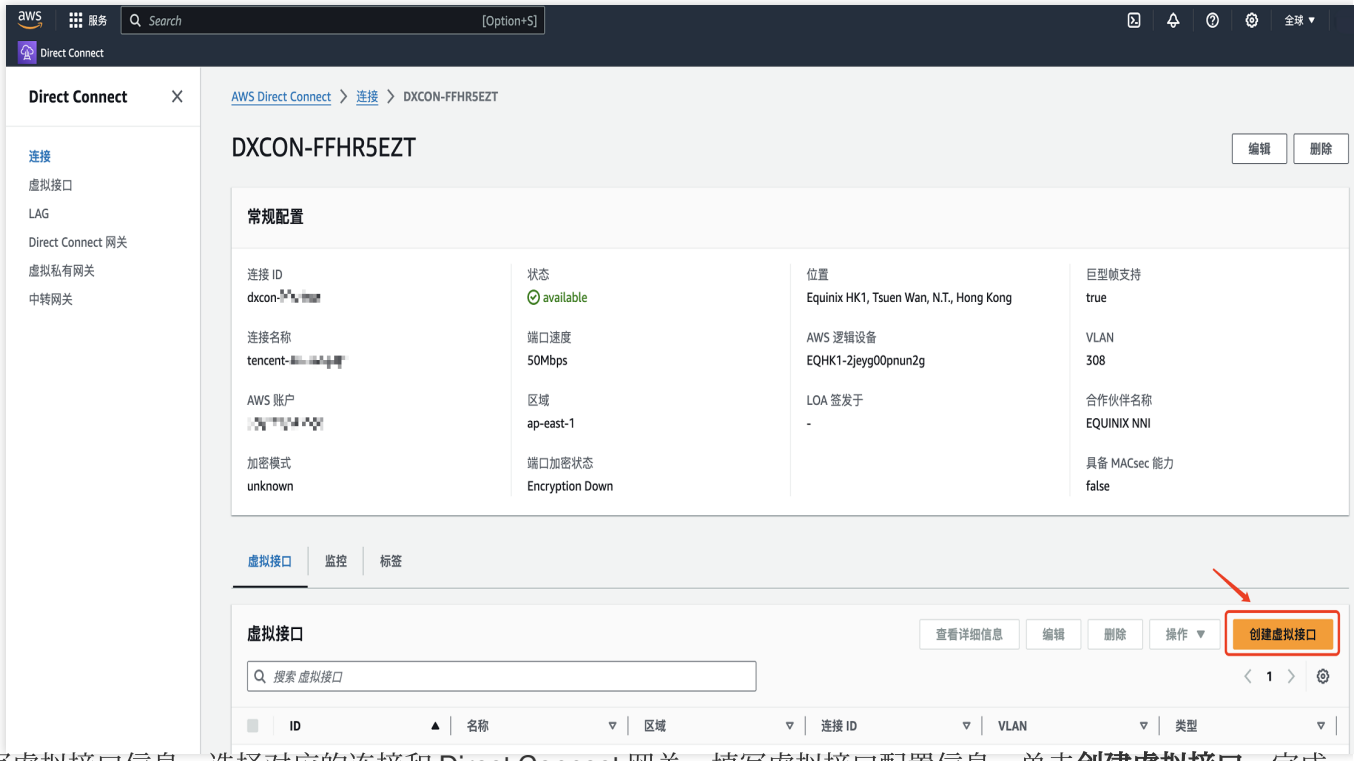
AWS 侧配置的后续步骤，客户可根据自身业务按需建设。其它云厂商类似。

步骤2：创建 EC2，并生成默认 vpc。

步骤3：创建虚拟专用网关，并关联默认 vpc。

步骤4：创建虚拟接口

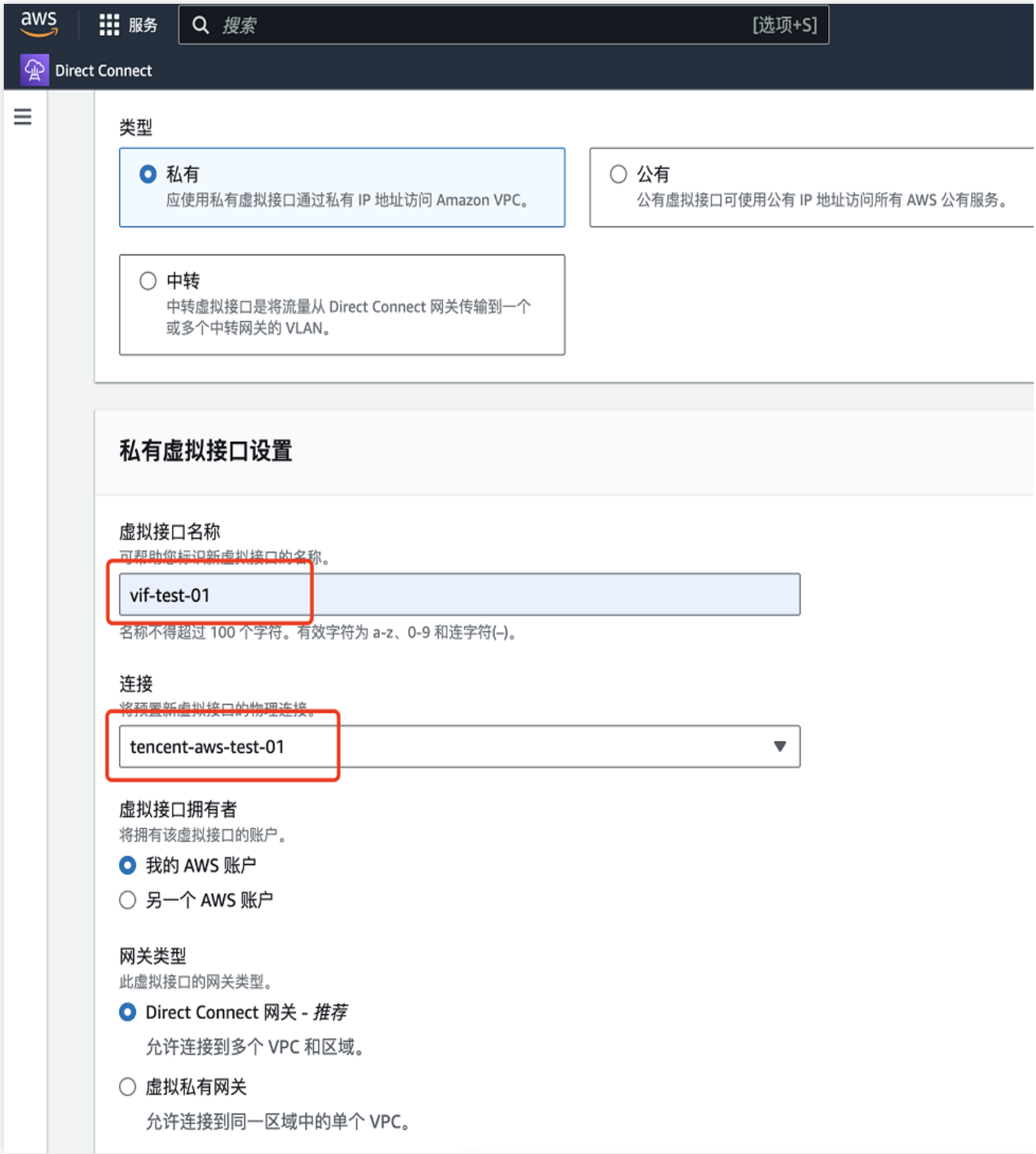
1. 在连接详情页，单击**创建虚拟接口**。



2. 填写虚拟接口信息，选择对应的连接和 Direct Connect 网关，填写虚拟接口配置信息，单击**创建虚拟接口**，完成虚拟接口配置。

注意：

此示例中 AWS 控制台填入的对等体 IP、BGP ASN、BGP 密钥均需与腾讯云控制台填入的配置匹配，否则虚拟接口无法连接。


aws
服务
搜索
[选项+S]
Direct Connect
类型
私有
应使用私有虚拟接口通过私有 IP 地址访问 Amazon VPC。
公有
公有虚拟接口可使用公有 IP 地址访问所有 AWS 公有服务。
中转
中转虚拟接口是将流量从 Direct Connect 网关传输到一个或多个中转网关的 VLAN。
私有虚拟接口设置
虚拟接口名称
可帮助您标识新虚拟接口的名称。
vif-test-01
名称不得超过 100 个字符。有效字符为 a-z、0-9 和连字符(-)。
连接
将预置新虚拟接口的物理连接。
tencent-aws-test-01
虚拟接口拥有者
将拥有该虚拟接口的账户。
我的 AWS 账户
另一个 AWS 账户
网关类型
此虚拟接口的网关类型。
Direct Connect 网关 - 推荐
允许连接到多个 VPC 和区域。
虚拟私有网关
允许连接到同一区域中的单个 VPC。


aws
服务
搜索
[选项+S]
Direct Connect
Direct Connect 网关
将附加新虚拟接口的 Direct Connect 网关。
test-dcg
虚拟局域网(VLAN)

新虚拟接口的虚拟局域网编号。

316

有效范围为 1 - 4094

BGP ASN

用于新虚拟接口的本地部署路由器的边界网关协议(BGP)自治系统编号(ASN)。

45090

有效范围为 1 - 2147483647。

▼ 其他设置

地址类型 - *可选*

确定是使用 IPv4 还是 IPv6 对等连接创建虚拟接口。

IPv4

IPv6

您的路由器对等体 IP - *可选*

在您的端点上配置的 BGP 对等体 IP。

10.0.0.1/30

Amazon 路由器对等体 IP - *可选*

AWS 终端节点上配置的 BGP 对等体 IP。

10.0.0.2/30

BGP 身份验证密钥 - *可选*

将用于 BGP 会话身份验证的密码。

tencent

巨型 MTU（MTU 大小 9001） - *可选*

虚拟接口上允许 9001 大小的 MTU。

已启用

启用 SiteLink - *可选*

启用 Direct Connect 节点之间的直接连接。需支付额外费用。单击此处了解详情。

已启用

标签

可帮助标识 AWS Direct Connect 资源的指定标签。

无与此资源关联的标签

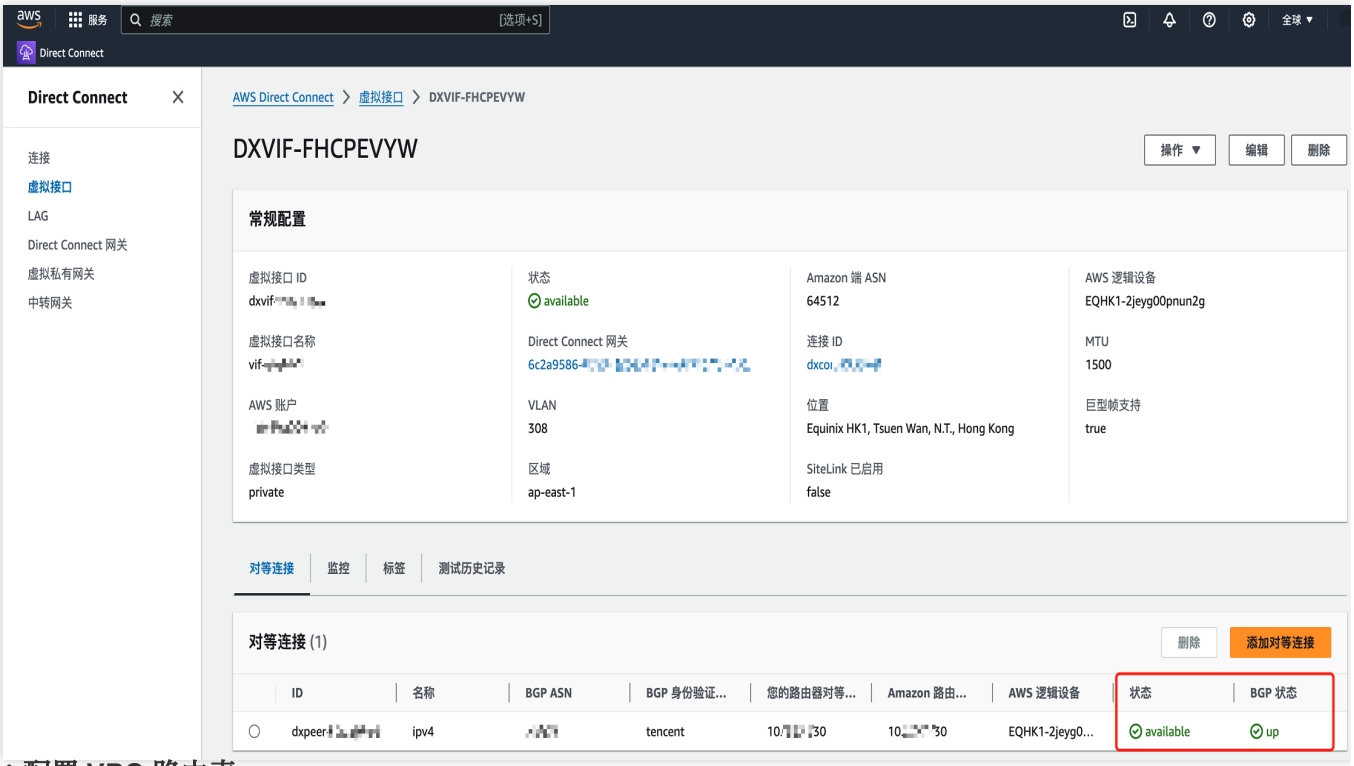
添加标签

取消

创建虚拟接口

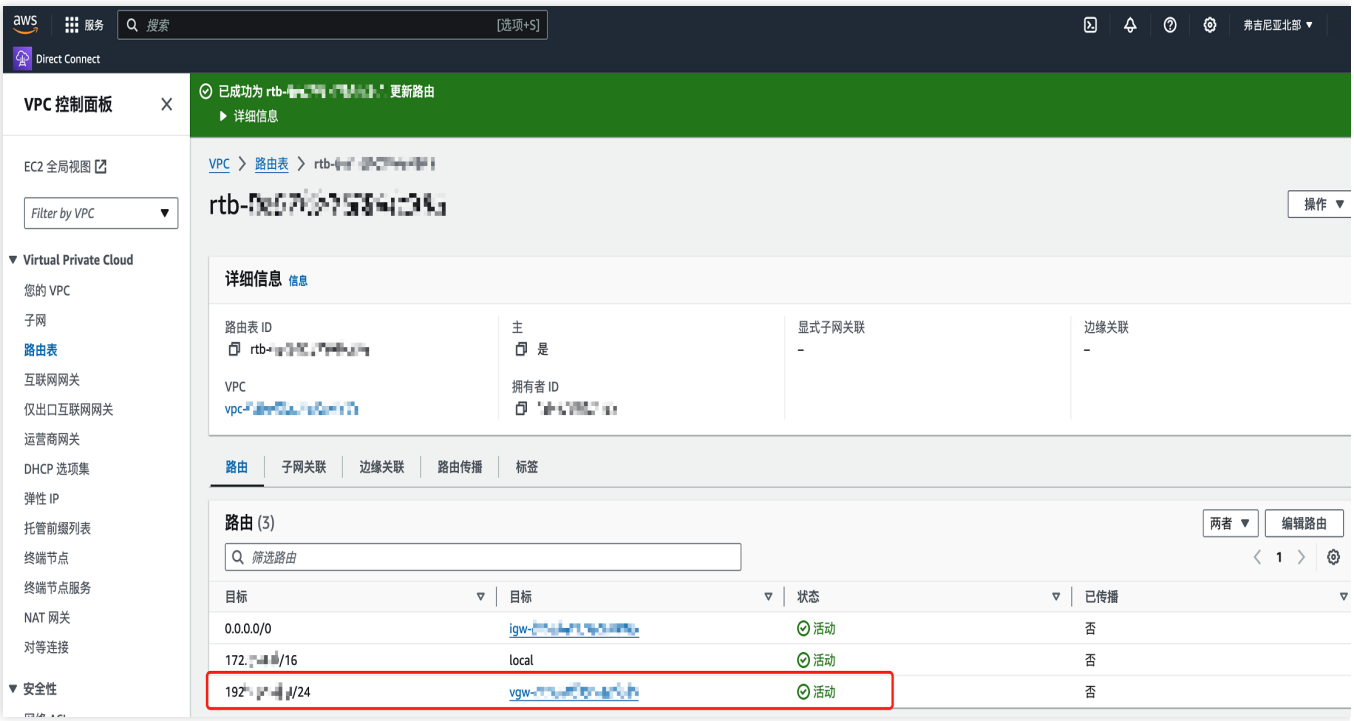
步骤5：确认虚拟接口状态

1. 等待腾讯云服务人员在腾讯侧完成配置。
2. 查看并确认虚拟接口 available，BGP 状态 up。



步骤6：配置 VPC 路由表

VPC 路由表配置出云路由。



三、腾讯侧配置

步骤1：控制台查看云交换信息

1. 登录 专线接入控制台，在左侧导航栏单击**云交换**。即可查看云交换实例信息，并完成接收，确认付费。

2. 等待您在 AWS 控制台完成连接接收，直到腾讯控制台查看云交换实例为运行中状态，开始计费。

步骤2：控制台一键构建云资源

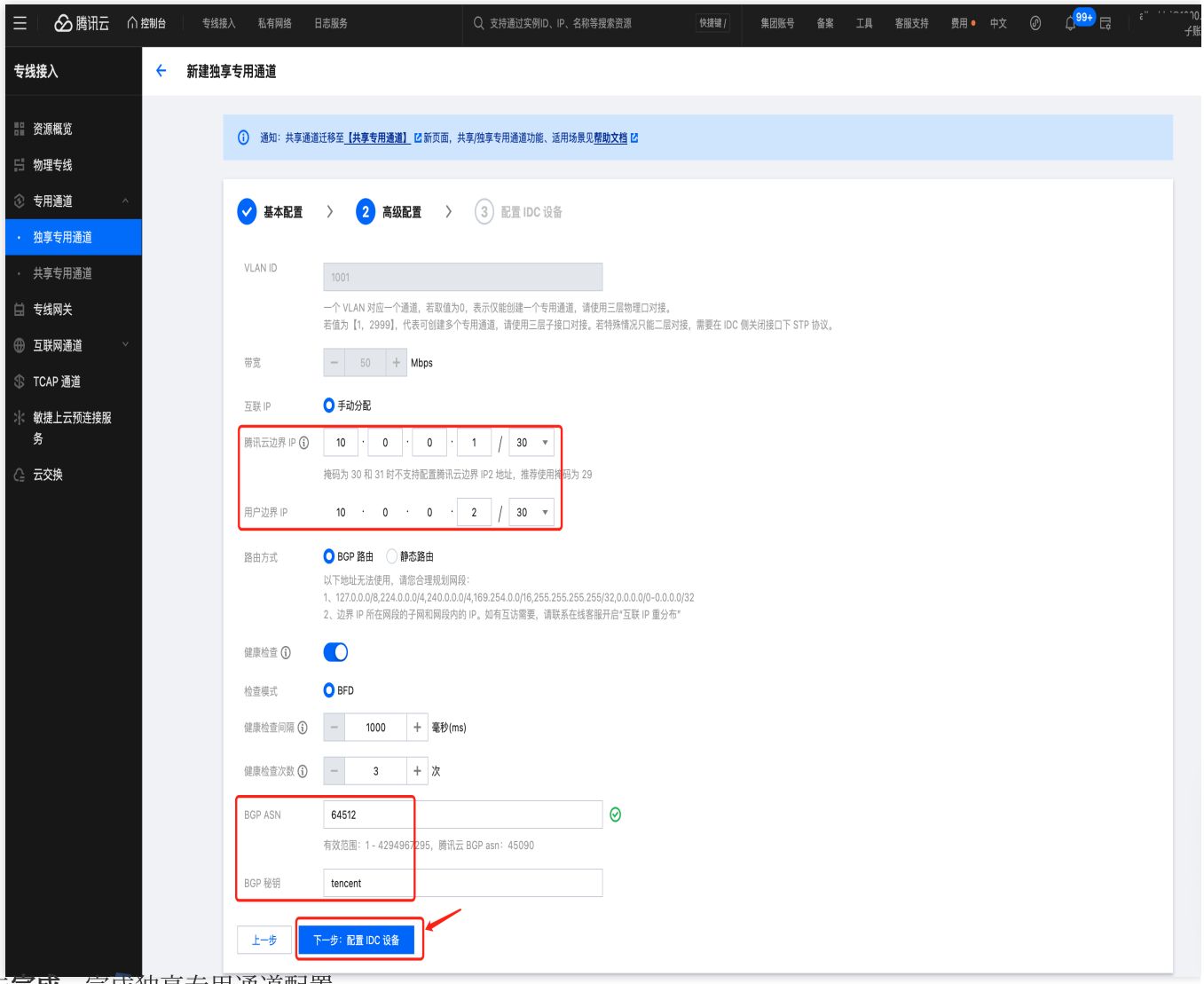
1. 在对应地域 创建云上 VPC、专线网关等资源。
2. 登录 专线接入控制台，在左侧导航栏单击**云交换**。
3. 在云交换列表页，单击**一键构建云资源**。

4. 填写独享专用通道的基本配置，单击**下一步：高级配置**。

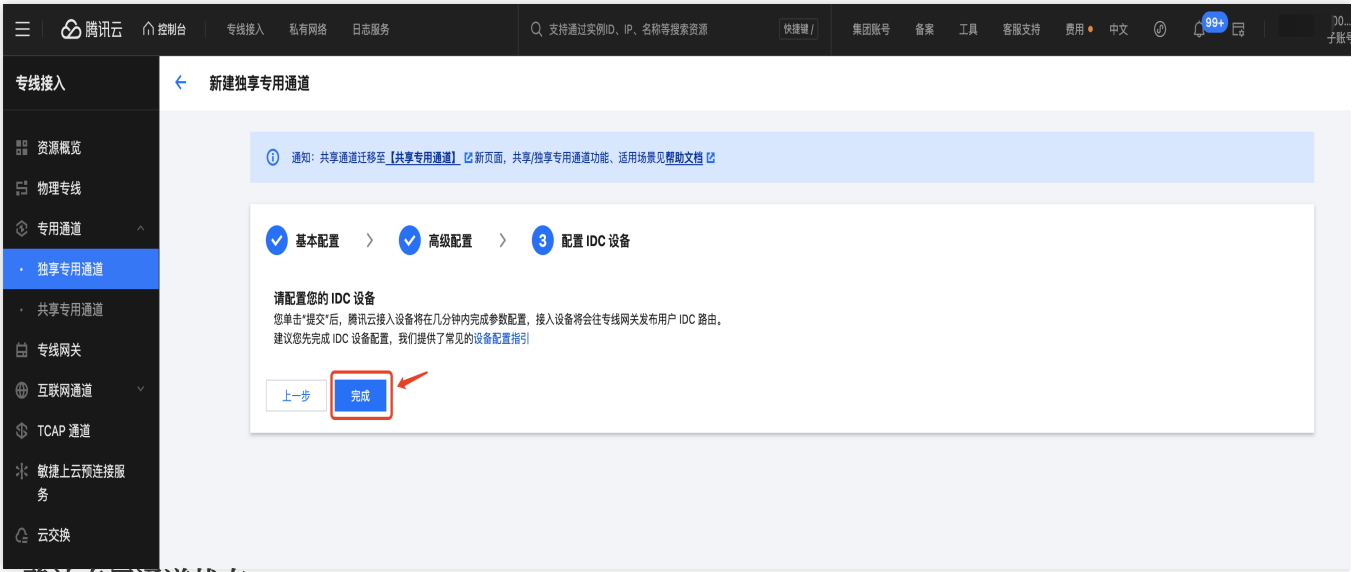
5. 填写专用通道关联的高级配置，单击**下一步：配置 IDC 设备**。

注意：

此示例中 Tencent 控制台填入的互联 IP、BGP ASN、BGP 密钥均需与 AWS 控制台填入的配置匹配，否则专用通道无法连接。



6. 单击**完成**，完成独享专用通道配置。

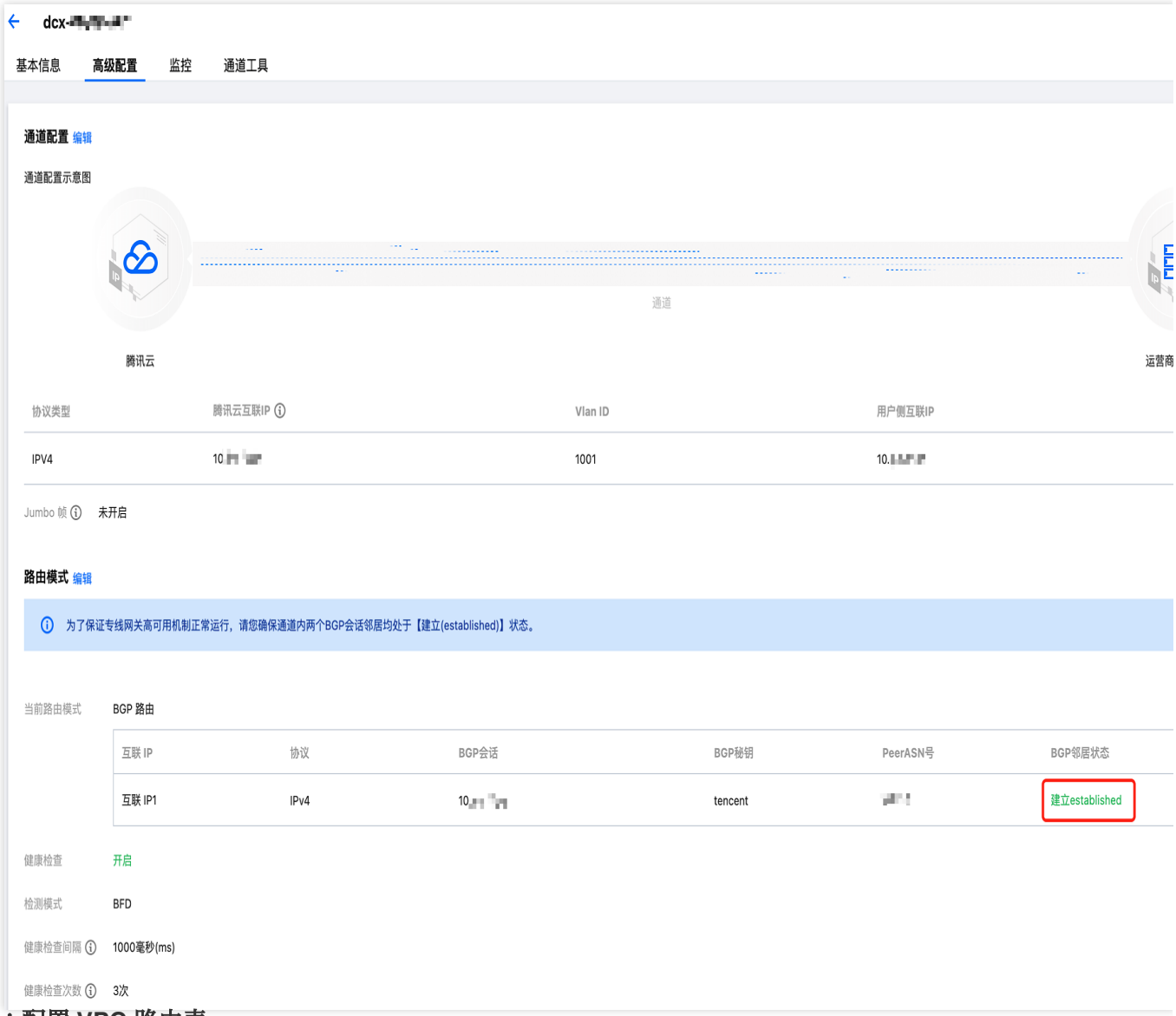


步骤3：确认专用通道状态

1. 等待您在 AWS 侧完成配置。

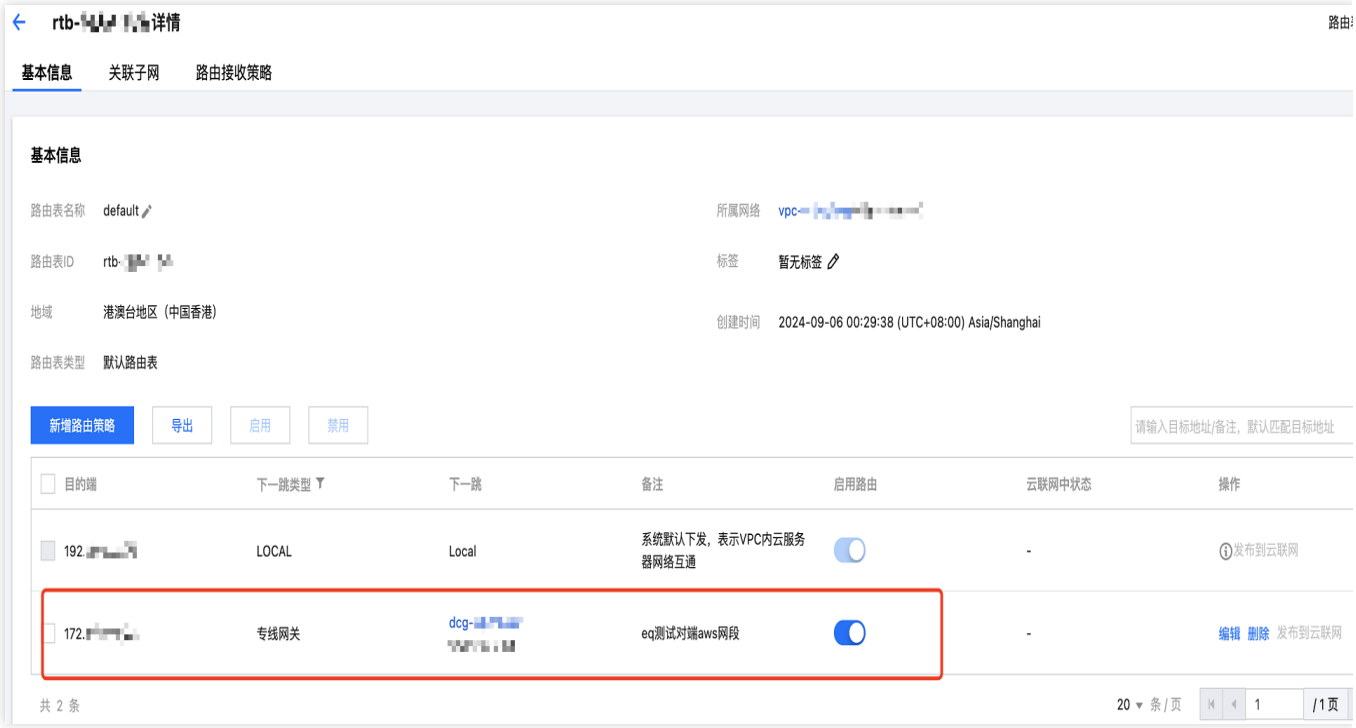
2. 登录 专线接入控制台，在左侧导航栏单击**云交换**。
3. 在云交换实例页面，单击**通道实例 ID**。

4. 在**通道实例** > **高级配置**页面，即可查看专用通道连接状态，BGP 邻居状态 **established** 表示已连接。



步骤4：配置 VPC 路由表

VPC 型专线网关，需要配置出云路由策略。详细操作可参见 创建自定义路由表 和 管理路由策略。



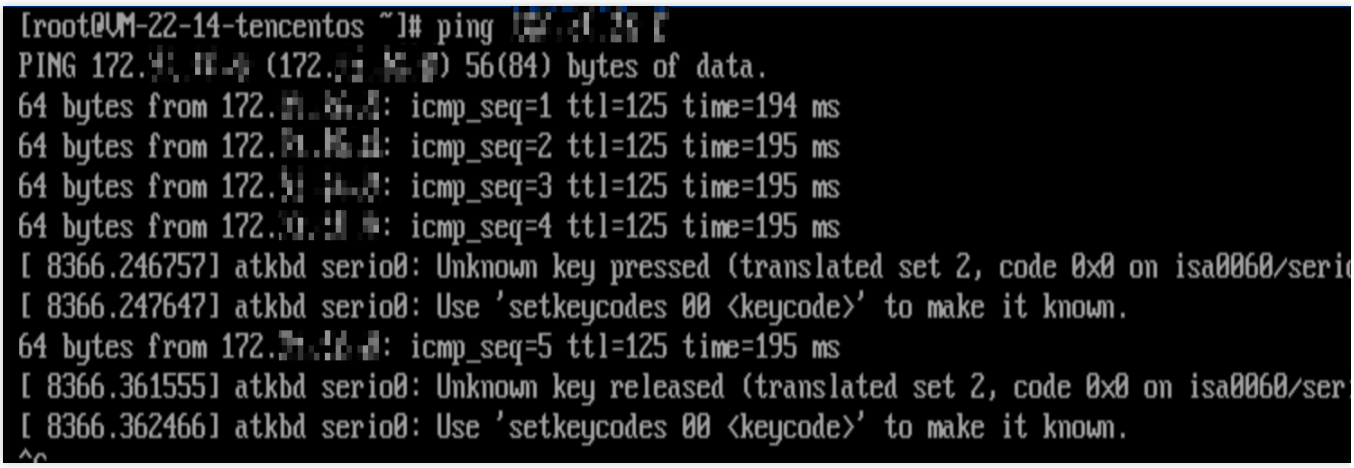
四、资源互通验证

注意：

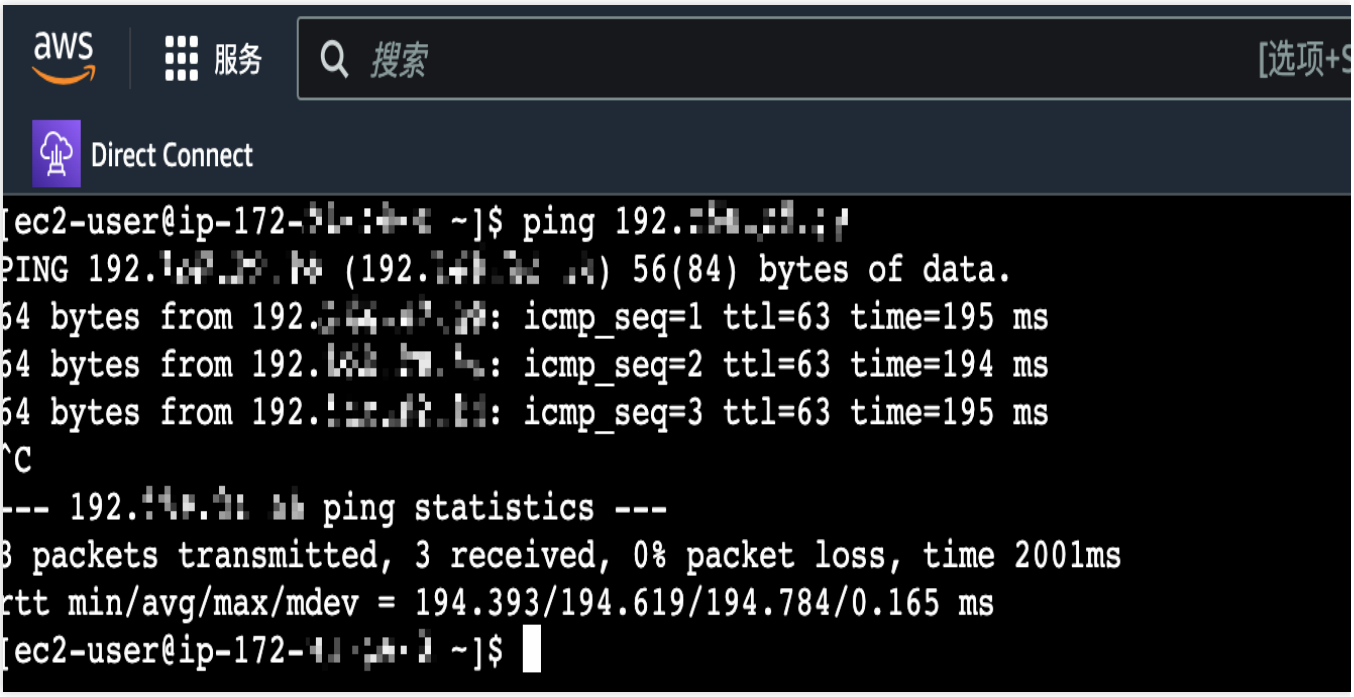
安全组规则需要放通流量。

测试 Tencent 侧与 AWS 侧之间的连通性。

步骤1：Tencent ping AWS



步骤2：AWS ping Tencent


aws
服务
搜索
[选项+
Direct Connect
ec2-user@ip-172- ~]$ ping 192.
PING 192. (192.) 56(84) bytes of data.
64 bytes from 192. : icmp_seq=1 ttl=63 time=195 ms
64 bytes from 192. : icmp_seq=2 ttl=63 time=194 ms
64 bytes from 192. : icmp_seq=3 ttl=63 time=195 ms
^C
--- 192. ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 194.393/194.619/194.784/0.165 ms
ec2-user@ip-172- ~]$