云专线

产品介绍

文档版本	01
发布日期	2024-04-30

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：
https://www.huawei.com/cn/psirt/vul-response-process
如企业客户须获取漏洞信息，请参见如下网址：
https://securitybulletin.huawei.com/enterprise/cn/security-advisory

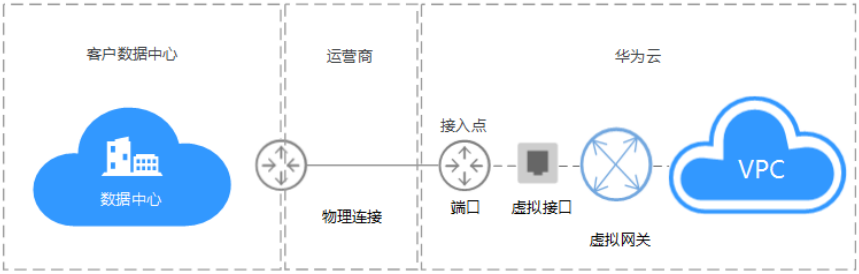
目 录

1 什么是云专线

云专线（Direct Connect）用于搭建用户本地数据中心与华为云VPC之间高速、低时延、稳定安全的专属连接通道，充分利用华为云服务优势的同时，继续使用现有的IT设施，实现灵活一体，可伸缩的混合云计算环境。

云专线组网图如图1-1所示。

图 1-1 云专线组网图



为什么选择云专线

- 网络质量：专用网络进行数据传输，网络性能高，延迟低，用户使用体验更佳。
- 安全性：用户使用云专线接入华为云上VPC，使用专享私密通道进行通信，网络隔离，满足各类用户对高网络安全性方面的需求。
- 传输带宽：华为云专线单线路最大支持100Gbps带宽连接，满足各类用户带宽需求。

组成部分

云专线服务主要包括物理连接、虚拟网关、虚拟接口三个组成部分。

- **物理连接**

  物理连接是用户本地数据中心与接入点的运营商物理网络的专线连接。物理连接提供两种专线接入方式：

  标准专线接入，是用户独占端口资源的物理连接，此种类型的物理连接由用户创建，并支持用户创建多个虚拟接口。

  托管专线接入，是多个用户共享端口资源的物理连接，此种类型的物理连接由合作伙伴创建，并且只允许用户创建一个虚拟接口。用户通过向合作伙伴申请来创建托管物理连接，需要合作伙伴为用户分配VLAN和带宽资源。

- **虚拟网关**

  虚拟网关是实现物理连接访问VPC的逻辑接入网关，虚拟网关会关联用户访问的VPC，一个虚拟网关只能关联一个VPC，多条物理连接可以通过同一个虚拟网关实现专线接入，访问同一个VPC。

- **虚拟接口**

  虚拟接口是用户本地数据中心通过专线访问VPC的入口，用户创建虚拟接口关联物理连接和虚拟网关，连通用户网关和虚拟网关，实现云下数据中心和云上VPC的互访。

访问方式

云专线服务提供了Web化的服务管理平台，即管理控制台。

用户可直接登录管理控制台访问云专线服务。

- 如果用户已注册账户，可直接登录管理控制台，在主页选择“网络 > 云专线”。
- 如果未注册，请参见**入门指引**中的“注册华为云”。

2 产品优势

云专线服务具有以下几大产品优势：

- **高安全**

  用户使用云专线接入华为云上VPC，使用专享私密通道进行通信，网络隔离，安全性极高。
- **低时延**

  专用网络进行数据传输，网络性能高，延迟低，用户使用体验更佳。
- **支持大带宽**

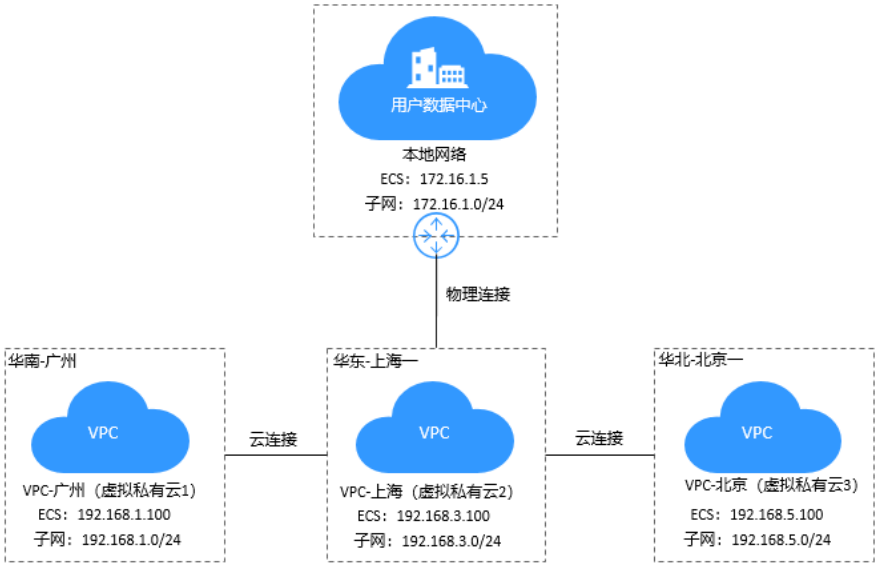
  华为云专线单线路最大支持100Gbps带宽连接，满足各类用户带宽需求。
- **资源无缝扩展**

  通过云专线将用户本地数据中心与云上资源互联，形成灵活可伸缩的混合云部署。

3 应用场景

本地数据中心跨区域访问多 VPC

通过云专线和云连接实现跨区域多VPC与用户IDC数据中心互通。



混合云部署

通过云专线将云下用户数据中心和云上VPC互联，利用云上的弹性，快速扩展能力，扩展应用层的计算能力。

图 3-1 混合云部署

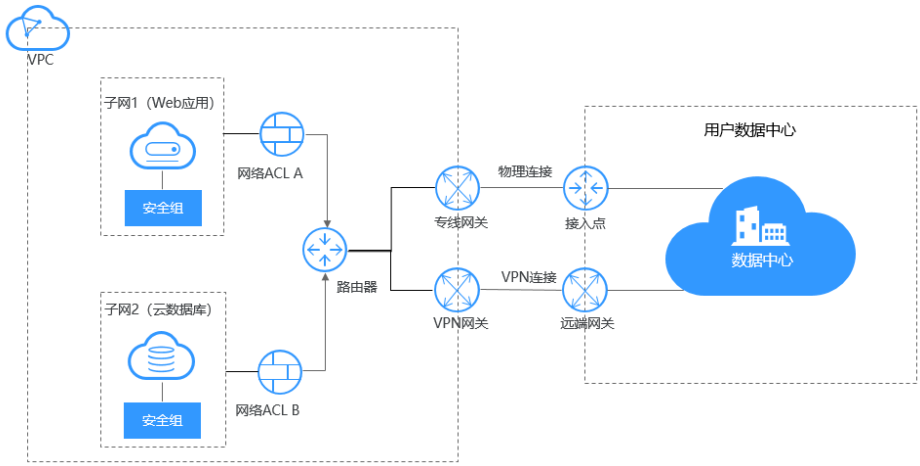


表 3-1 混合云部署

云产品	应用场景	描述	相关操作
虚拟专用网络	使用公网低成本连接VPC与本地IDC	基于Internet使用加密隧道将VPC与本地数据中心连接起来。具备成本低、配置简单、即开即用等优点。但它的网络质量依赖Internet。	**通过VPN连接VPC** **什么是企业交换机**
云专线	铺设物理专线高质量连接VPC与本地IDC	使用物理专线将VPC与本地数据中心连接起来。具备低时延、高安全、专用等优点。适用对网络传输质量和安全等级要求较高的场景 。	**通过用户专线访问多个VPC** **什么是企业交换机**

4 网络规划

方案概述

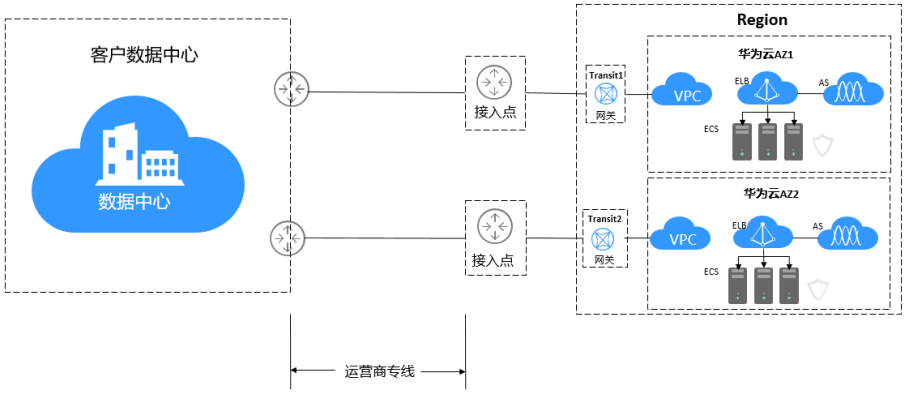
提供以下物理连接接入方式：

- 标准专线

  此方式独占华为云物理端口，您可以通过管理控制台自主申请物理连接。客户数据中心通过不同运营商专线，分别接入不同接入点，实现多链路多接入点互备，保障高可靠性。如果有特殊要求只能选择同一运营商，需确保不同物理路由。

  如图4-1所示。

  图 4-1 标准专线接入

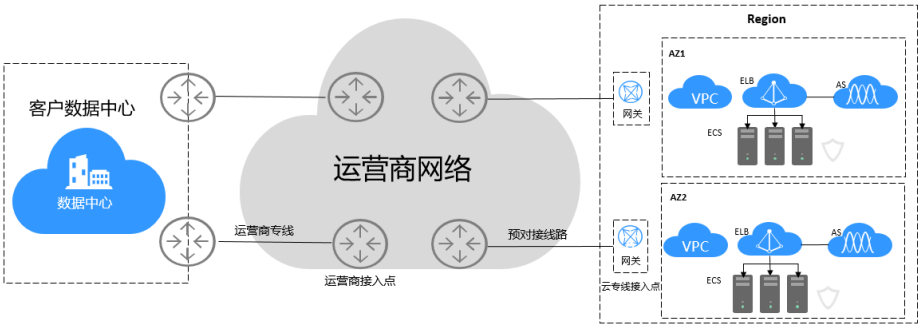
  

- 托管专线

  此方式运营商和华为云之间的连接端口是多租户共享的。

  用户本地数据中心通过合规运营商拉通专线，运营商和云专线接入点已做好专线预连接，运营商为用户分配上云连接。运营商和华为云连接端口是多租户共享的。图4-2所示。

图 4-2 托管专线接入



方案对比

对比项	标准专线	托管专线
端口性质	独占华为云物理端口	共享华为云物理端口
推荐接入带宽	1G - 100Gbps	<1Gbps
预计施工周期	本地线路2-3个月，长途线路3-4个月	1个月左右
实施主体	用户、专线运营商、机房运营商、华为云	用户、专线运营商、华为云
实施步骤	1. 用户在云控制台购买物理连接。 2. 用户自主联系专线运营商，并督促本地IDC到云接入点机房的专线部署。 3. 用户联系接入点机房主体完成进线和跳线。 4. 用户运营商与华为云完成接入侧设备调试。 5. 用户在云端相关网络配置。	1. 自主联系运营商伙伴完成本地IDC到接入点的专线部署。 2. 运营商完成接入侧设备调试。 3. 用户在云端相关网络配置。
计费	• 物理连接端口占用费用（按月或按年）向华为云支付 。 • 接入点机房的楼内线缆费向机房供应商支付。 • 本地IDC机房的楼内线缆费向本地机房供应商支付。 • 其他施工与带宽租用费用向运营商支付。详细请参考**计费说明**。	• 无需向云支付端口占用费。 • 本地IDC机房的楼内线缆费向本地机房供应商支付。 • 其他施工与带宽租用费用向运营商支付。

网络要求

- 您必须使用单模的1GE、10GE、40GE或100GE的光模块与华为云的接入设备对接。同时，需要提前对齐LC、波长、距离等关键参数。光模块参数举例：1GE、LC 单模、1310nm、10KM。

- 必须禁用端口的自动协商功能，同时必须手动配置端口速率和全双工模式。
- 必须跨整个连接 (包括中间设备) 支持 802.1Q VLAN 封装。
- 可以支持BGP或者静态路由对接，您的设备须支持边界网关协议（ BGP ）和BGP MD5认证或支持静态路由。
- (可选) 您可以在网络上配置双向转发检测 (BFD)。
- 在物理连接层上支持的最大传输单位 (MTU) 高达 1522 字节 (14 字节以太网标头 + 4 字节 VLAN 标记 + 1500 字节 IP 数据报 + 4 字节帧检测序列)。推荐参数值：1500。
- 云上云下建议使用私网IP地址，且互通的IP网段不能冲突。

5 约束与限制

资源	默认配额	如何提升配额
每个账户每个区域支持物理连接数	10	可以通过**提交工单**提高此限制。
每个账户每个区域支持虚拟网关数	5	可以通过**提交工单**提高此限制。
每个账户每个区域支持虚拟接口数	50	可以通过**提交工单**提高此限制。
虚拟接口上边界网关协议 (BGP) 会话的路由数量	100	可以通过**提交工单**提高此限制。
虚拟接口上远端子网的数量	50	可以通过**提交工单**提高此限制。

接入点限制

使用物理连接上云前，需要先选择接入点，接入点相关限制如下：

- 一个区域提供多个不同地址位置的接入点，每个同城接入点到同Region多可用区的网络延时均小于5毫秒。
- 您的业务对云下云上的网络延时要求比较高，可以**提交工单**咨询距离云服务器所在可用区距离最近的接入点。

产品使用约束

- 使用前应规划好云上VPC和本地IDC的网段，需保证云上VPC网段和本地IDC网段不会重叠。

  VPC内云服务地址网段100.64.0.0/10、127.0.0.0/8、169.254.0.0/16、224.0.0.0/3为VPC保留网段，请勿使用以上网段作为云专线的远端子网。
- 为您提供端口规格是1G和10G并且传输距离为10公里的光模块，超过10公里的光模块或者购买端口规格是40G和100G端口均需自行购买光模块。
- 如果您需要从专线访问ELB，请您使用ELB源IP负载均衡算法代替ELB会话保持功能。

- 云专线默认不支持对接企业交换机（ESW），如果您需要从专线访问ESW，请您**提交工单**开通ESW对接功能。
- 云专线只支持回应Ping探测的普通ICMP报文（type=8、code=0的echo报文且不携带ip option），不支持回应其余类型的ICMP报文。
- 云专线对物理连接端口接收到的本端网关IP的Ping探测限速为30次/秒。

施工规则

- 施工方进入机房施工时，请遵守机房运营商和工程师向您展示的施工规定，如果施工方不遵守机房规定，将无法完成施工。
- 机房不支持托管任何光电转换设备，施工方携带的任何光电设备无法安装到机房。
- 政策封网或华为云管理封网都将影响专线延时施工，如果遇到华为云封网，请向您的专线经理咨询。
- 接入点机房是电信运营商或第三方租赁的机房，如果存在专线入楼费和楼内线缆费，需接入方向机房运营商支付。
- 接入点机房是电信运营商或第三方数据中心运营，进入机房施工需提供机房专线接入授权书，请在施工前完成授权书申请。

6 专线接入点

接入点，指提供专线接入服务的地理位置。在使用专线接入华为云之前，您需要咨询接入点的详细地址。

您可以自主选择运营商的专线，连接云专线接入点，并**自助购买**对应的端口资源，完成物理连接接入。

如需更多信息或支持，可**提交工单**或联系销售经理。

表 6-1 专线接入点

大区	国家(城市)	区域	接入点	IDC
中国大陆	中国(北京)	华北-北京四	廊坊-广阳-华为	华为
			北京-通州-汇天	汇天
			北京-亦庄-中金	中金
			北京-亦庄-亚太	亚太
			北京-朝阳-酒仙桥	酒仙桥
			廊坊-万国	中立机房
			廊坊-润泽-电信	电信
中国大陆	中国(上海)	华东-上海二	上海-浦东-万国	万国
			上海-宝山-宝信	宝信
			上海-嘉定-光环	光环
	中国(苏州)	华东-上海一	苏州-昆山-万国	万国
			苏州-吴中-国科	联通
			苏州-吴江-汾湖-移动	移动
			杭州研究所	华为
			杭钢数据中心	中立机房

大区	国家(城市)	区域	接入点	IDC
			上海-万国	中立机房
			上海-宝信	移动
			苏州-昆山-坤汇	昆山坤汇
			苏州-吴中-华为基地	华为
			上海-光环	光环
	中国(广州)	华南-广州	广州-黄埔-华新园	大一互联
			广州-番禺-大学城	大一互联
			广州-明美-联通	联通
			广州-化龙-联通	联通
			广州-云浦-电信	电信
			深圳-宝德	中立机房
			深圳-南山	
			深圳-福田	
			深圳-奕峰	奕峰
			东莞-团泊洼	华为
	中国(贵阳)	西南-贵阳一	贵阳-贵安-移动	移动
			贵阳-贵安-七星湖	华为
			贵阳-贵安-高端园	华为
			贵阳-西安-西港	电信
			贵阳-西安-世纪互联	世纪互联
亚太	中国(香港)	中国-香港	香港-沙田-电信	电信
			香港-西贡-移动	移动
			香港-西贡-GlobalSwitch	GlobalSwitch
	泰国(曼谷)	亚太-曼谷	曼谷-NTT	NTT
			曼谷-TRUE	TRUE
	新加坡	亚太-新加坡	新加坡-DataPro	Equinix
			新加坡-Global Switch	Global Switch
	印尼（雅加达）	亚太-雅加达	雅加达-JK5	JK5
			雅加达-EDGE	EDGE

大区	国家(城市)	区域	接入点	IDC
非洲	南非(约翰内斯堡)	非洲-约翰内斯堡	肯尼亚-内罗毕SBP	内罗毕SBP
			尼日利亚-拉各斯Medallion	拉各斯Medallion
			约翰内斯堡-IS Parklands	IS Parklands
			约翰内斯堡-Teraco	Teraco
拉美	墨西哥	拉美-墨西哥城一	墨西哥城-COM Ixtlahuaca	COM Ixtlahuaca
			墨西哥-KIO MEX 5	KIO MEX 5
		拉美-墨西哥城二	墨西哥-Tultitlan	中立机房
			波哥大-equinix	equinix
	巴西（圣保罗）	拉美-圣保罗一	圣保罗-Equinix	Equinix
			圣保罗-ODATA	ODATA
	秘鲁（利马）	秘鲁-利马一	利马-Telefonica	Telefonica
	智利（圣地亚哥）	拉美-圣地亚哥	圣地亚哥-Paine	Paine
			圣地亚哥-Claro	Claro
欧洲	土耳其（伊斯坦布尔）	土耳其-伊斯坦布尔	土耳其-伊斯坦布尔-Turkcell	Turkcell
			土耳其-伊斯坦布尔-NGN	NGN
其他	沙特阿拉伯（利雅得）	中东-利雅得	利雅得 STC-KHURAIS	STC-KHURAIS
			利雅得 Remal	Remal

7 计费说明

通过云专线建立本地数据中心和云上VPC的专属连接通道，您可以选择标准专线方式接入（独享端口），也可以选择通过共享合作伙伴的托管专线接入（共享端口）。

计费项

- **标准专线计费**
  标准专线接入华为云的费用包括如下部分：

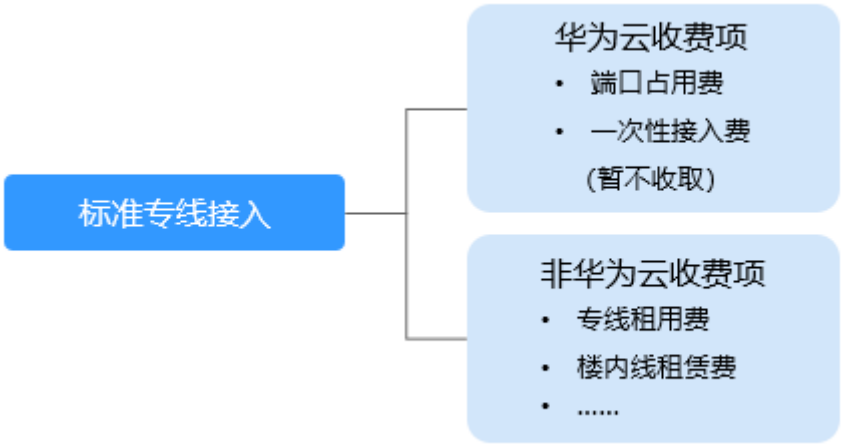


表 7-1 标准专线接入收费详情

收费方	计费项	说明	计费方式
华为云	端口占用费	按端口规格收取资源占用费。	预付费，包年包月。
	一次性接入费	暂不收取一次性接入费，如有收取计划，将提前一个月通知。	-

收费方	计费项	说明	计费方式
非华为云	专线租用费	用户数据中心与华为云专线接入点之间的运营商专线部署和租赁费用，由用户向运营商购买支付。	-
	楼内线租赁费	用户专线进入非华为云物业的专线接入点，一般是中立机房，可能会产生楼内线租赁费用。	-

- **托管专线计费**

  相比标准物理连接，托管连接是通过合作伙伴已有的共享端口接入，无需向华为云支付专线服务一次性接入费和端口占用费。

  托管专线接入华为云产生的费用包括如下部分：

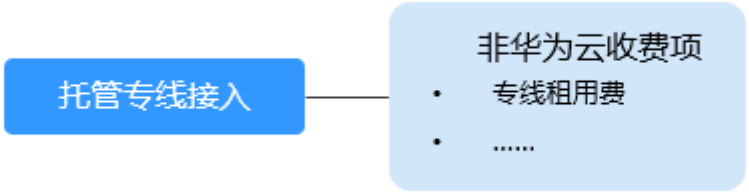


表 7-2 托管专线接入收费详情

收费方	计费项	说明	计费方式
非华为云	专线租用费	用户数据中心与华为云专线接入点之间的运营商专线部署和租赁费用，由用户向运营商购买支付。	-

云专线费用详情请参见**产品价格详情**。

计费模式

预付费，包年包月。

变更配置

云专线当前计费方式为包年包月的预付费方式，暂时不支持变更。

续费

详细请查看**续费管理**。

到期与欠费

详细请查看**资源停止服务或逾期释放说明**和**如何进行支付和还款**。

8 安全

8.1 责任共担

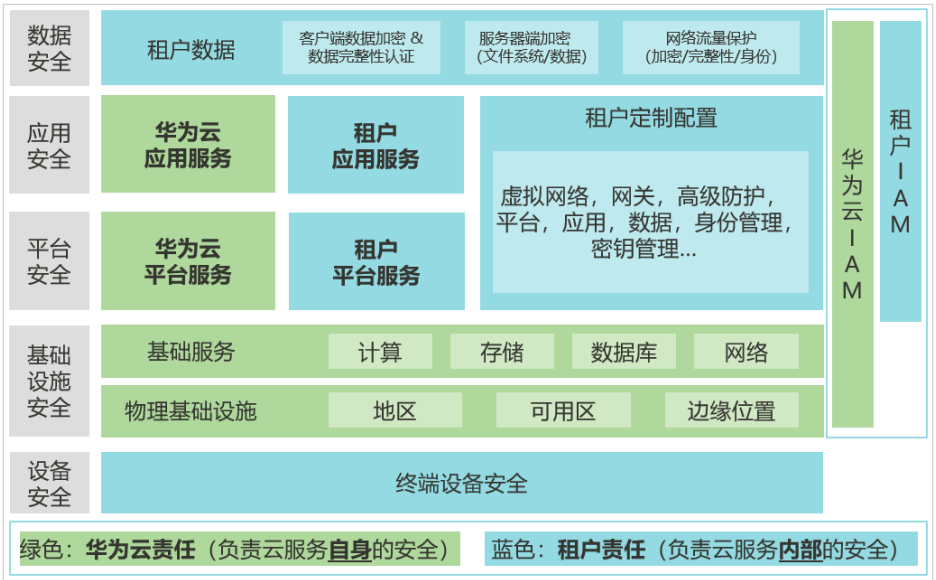
华为云秉承“将公司对网络和业务安全性保障的责任置于公司的商业利益之上”。针对层出不穷的云安全挑战和无孔不入的云安全威胁与攻击，华为云在遵从法律法规业界标准的基础上，以安全生态圈为护城河，依托华为独有的软硬件优势，构建面向不同区域和行业的完善云服务安全保障体系。

安全性是华为云与您的共同责任，如图8-1所示。

- **华为云**：负责云服务**自身**的安全，提供安全的云。华为云的安全责任在于保障其所提供的 IaaS、PaaS 和 SaaS 类云服务自身的安全，涵盖华为云数据中心的物理环境设施和运行其上的基础服务、平台服务、应用服务等。这不仅包括华为云基础设施和各项云服务技术的安全功能和性能本身，也包括运维运营安全，以及更广义的安全合规遵从。
- **租户**：负责云服务**内部**的安全，安全地使用云。华为云租户的安全责任在于对使用的 IaaS、PaaS 和 SaaS 类云服务内部的安全以及对租户定制配置进行安全有效的管理，包括但不限于虚拟网络、虚拟主机和访客虚拟机的操作系统，虚拟防火墙、API 网关和高级安全服务，各项云服务，租户数据，以及身份账号和密钥管理等方面的安全配置。

《华为云安全白皮书》详细介绍华为云安全性的构建思路与措施，包括云安全战略、责任共担模型、合规与隐私、安全组织与人员、基础设施安全、租户服务与租户安全、工程安全、运维运营安全、生态安全。

图 8-1 华为云安全责任共担模型



8.2 身份认证与访问控制

身份认证

云专线服务支持通过IAM权限策略进行访问控制。IAM权限是作用于云资源的，IAM权限定义了允许和拒绝的访问操作，以此实现云资源权限访问控制。管理员创建IAM用户后，需要将用户加入到一个用户组中，IAM可以对这个组授予DC所需的权限，组内用户自动继承用户组的所有权限。

详情请参见**权限管理**。

访问控制

安全组是一个逻辑上的分组，为同一个VPC内具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。

系统会为每个用户默认创建一个默认安全组，默认安全组的规则是在出方向上的数据报文全部放行，入方向访问受限，安全组内的实例无需添加规则即可互相访问。默认安全组您可以直接使用，详情请参见**默认安全组和规则**。

同时，华为云为用户提供了管理安全组和安全组规则的功能，包括创建、查看、删除、修改、克隆、添加安全组，以及添加、复制、修改、删除、导入/导出安全组规则、快速添加多条安全组规则、查看弹性云服务器的安全组、变更弹性云服务器的安全组、云资源加入/移出安全组等。

用户可以在安全组中定义各种访问规则，当弹性云服务器加入该安全组后，即受到这些访问规则的保护。详情请参见**安全组**。

8.3 审计与日志

云审计服务（Cloud Trace Service，CTS），是华为云安全解决方案中专业的日志审计服务，提供对各种云资源操作记录的收集、存储和查询功能，可用于支撑安全分析、合规审计、资源跟踪和问题定位等常见应用场景。

用户开通云审计服务后，CTS可记录DC的操作事件用于审计。

- CTS的详细介绍和开通配置方法，请参见**CTS快速入门**。
- DC支持审计的操作事件请参见**支持审计的关键操作列表**。
- 查看审计日志请参见**查看审计日志**。

8.4 监控安全风险

云监控（Cloud Eye）是面向华为云资源的监控平台，提供了实时监控、及时告警、资源分组、站点监控等能力，使您全面了解云上的资源使用情况、业务的运行状况，并及时收到异常告警做出反应，保证业务顺畅运行。

监控是保持云专线可靠性、可用性和性能的重要部分，通过监控，用户可以观察云专线资源。为使用户更好地掌握自己的云专线运行状态，公有云平台提供了云监控。您可以使用该服务监控您的云专线，执行自动实时监控、告警和通知操作，帮助您更好地了解云专线的各项性能指标。

关于云专线服务支持的监控指标，以及如何创建监控告警规则等内容，请参见**监控**。

8.5 认证证书

合规证书

华为云服务及平台通过了多项国内外权威机构（ISO/SOC/PCI等）的安全合规认证，用户可自行**申请下载**合规资质证书。

图 8-2 合规证书下载

资源中心

华为云还提供以下资源来帮助用户满足合规性要求，具体请查看**资源中心**。

图 8-3 资源中心

9 权限管理

如果您需要对华为云上购买的Direct Connect资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制华为云资源的访问。

通过IAM，您可以在华为账号中给员工创建IAM用户，并授权控制他们对华为云资源的访问范围。例如您的员工中有负责软件开发的人员，您希望他们拥有Direct Connect的使用权限，但是不希望他们拥有删除云专线等高危操作的权限，那么您可以使用IAM为开发人员创建用户，通过授予仅能使用云专线，但是不允许删除云专线的权限，控制他们对云专线资源的使用范围。

如果华为账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用云专线服务的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。关于IAM的详细介绍，请参见**IAM产品介绍**。

云专线权限

默认情况下，管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

云专线部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问云专线时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于华为云各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业对权限最小化的安全管控要求。例如：针对云专线服务，管理员能够控制IAM用户仅能对某一类云专线资源进行指定的管理操作。

如表9-1所示，包括了云专线的所有系统权限。

表 9-1 云专线系统权限

系统角色/策略名称	描述	类别	依赖关系
Direct Connect Administrator	云专线服务的管理员权限，拥有该权限的用户拥有云专线服务所有执行权限。 拥有该权限的用户必须同时拥有Tenant Guest、VPC Administrator权限。	系统角色	依赖Tenant Guest、VPC Administrator策略。 • VPC Administrator：项目级策略，在同项目中勾选。 • Tenant Guest：项目级策略，在同项目中勾选。
DCaaS Partner	云专线服务合作伙伴用户权限，拥有该权限的用户可以为其他用户创建托管和标准连接。 拥有该权限的用户必须同时拥有Tenant Guest、VPC Administrator权限。	系统角色	依赖Tenant Guest、VPC Administrator策略。 • VPC Administrator：项目级策略，在同项目中勾选。 • Tenant Guest：项目级策略，在同项目中勾选。
DCAAS FullAccess	操作权限：对云专线服务的所有执行权限。 作用范围：项目级服务。	系统策略	无
DCAAS ReadOnlyAccess	操作权限：对云专线服务的只读权限。 作用范围：项目级服务。	系统策略	无

表9-2列出了云专线常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 9-2 常用操作与系统权限的关系

操作	Direct Connect Administrator	DCaaS Partner	DCAAS FullAccess	DCAAS ReadOnlyAccess
创建物理连接	√	√	√	×
查询物理连接	√	√	√	√
修改物理连接	√	√	√	×
删除物理连接	√	√	√	×

操作	Direct Connect Administrator	DCaaS Partner	DCAAS FullAccess	DCAAS ReadOnlyAccess
创建虚拟网关	√	√	√	×
查询虚拟网关	√	√	√	√
修改虚拟网关	√	√	√	×
删除虚拟网关	√	√	√	×
创建虚拟接口	√	√	√	×
查询虚拟接口	√	√	√	√
修改虚拟接口	√	√	√	×
删除虚拟接口	√	√	√	×
创建运营物理连接	√	√	√	×
查询运营物理连接	√	√	√	√
修改运营物理连接	√	√	√	×
删除运营物理连接	√	√	√	×
创建租户物理连接	√	√	√	×
查询租户物理连接	√	√	√	√
修改租户物理连接	√	√	√	×
删除租户物理连接	√	√	√	×

相关链接

- IAM产品介绍
- 创建用户组、用户并授予云专线权限

10 与其他服务的关系

图 10-1 云专线服务与其他服务的关系示意图

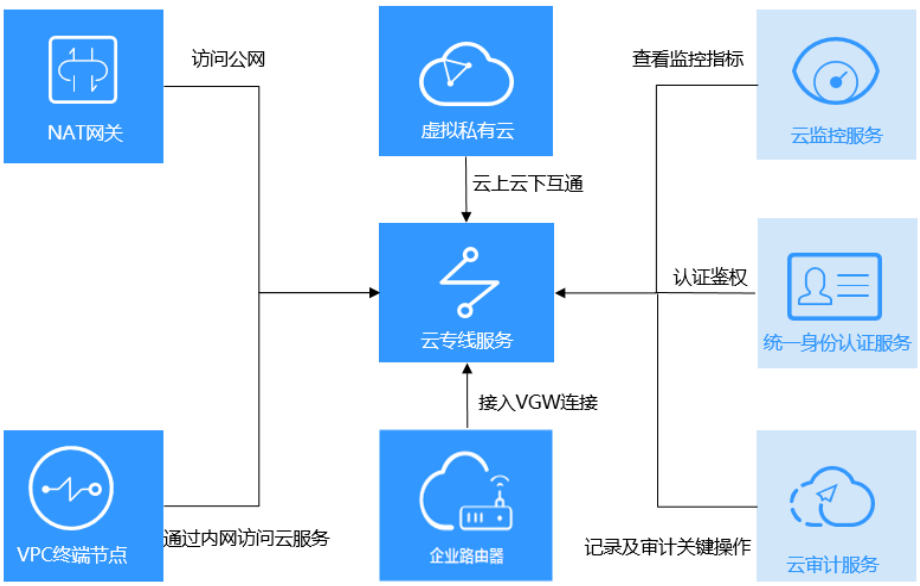


表 10-1 云专线服务与其他服务的关系

相关服务	交互功能	位置
虚拟私有云（Virtual Private Cloud，VPC）	通过VPC服务，创建VPC，本地数据中心才可以使用云专线上云。	创建虚拟私有云及默认子网
	通过云专线接入VPC后，用户可以使用VPC的对等连接访问多个VPC。	用户通过对等连接访问多个VPC
企业路由器（Enterprise Router，ER）	通过云专线接入企业路由器后，打通云下IDC和云上网络，实现多个VPC共享专线。	-

相关服务	交互功能	位置
NAT网关（NAT Gateway，NAT）	通过云专线接入VPC的本地服务器，可以通过NAT网关访问公网或为公网提供服务。	**NAT网关**
VPC终端节点（VPC Endpoint，VPCEP）	本地数据中心可以通过云专线，利用建立的终端节点通过内网访问云服务。	**配置访问OBS服务内网地址的终端节点**
云监控（Cloud Eye Service）	通过云监控服务，查看云专线资源的监控数据，还可以获取可视化监控图表。	**查看监控指标**
统一身份认证服务（Identity and Access Management，IAM）	通过IAM服务，针对您在华为云上创建的云专线资源，向不同用户设置不同的使用权限，可以帮助您安全地控制华为云云专线资源的访问权限。	**统一身份认证服务**
云审计服务（Cloud Trace Service，CTS）	记录与云专线服务相关的操作事件。	**支持审计的关键操作列表**

11 基本概念

11.1 物理连接

物理连接是对接入点和本地数据中心之间建立的网络线路的抽象，以方便对线路进行管理。

我们为您提供上云的物理线路端口，您创建物理连接后，还需要运营商为您进行线下施工，搭建物理线路。

物理连接是您本地数据中心上云的专属通道，与传统公网相比，更稳定可靠，安全隔离，并且提供最大100Gbps的高性能传输速率。

普通用户可以申请标准物理连接和托管物理连接。

- 标准物理连接，是用户独占端口资源的物理连接，此种类型的物理连接由用户创建，并支持用户创建多个虚拟接口。
- 托管物理连接，即租户物理连接，是多个用户共享端口资源的物理连接，此种类型的物理连接由合作伙伴创建，并且只允许用户创建一个虚拟接口。用户通过向合作伙伴申请来创建托管物理连接，需要合作伙伴为用户分配VLAN和带宽资源。

合作伙伴可以申请运营物理连接和租户物理连接。

- 运营物理连接是合作伙伴购买的物理连接，租户物理连接需要托管于运营物理连接。
- 租户物理连接是合作伙伴为普通用户创建的物理连接，普通用户通过合作伙伴购买方式购买的物理连接。

普通租户需要通过一条租用运营商的运营物理连接将本地数据中心连接到接入点，建立专线连接。

物理连接支持冗余专线配置，当两条专线接入同区域的不同接入点时，则两条物理连接互为冗余物理连接。冗余专线互为主备专线，当一条物理连接出现故障时，可自动切换到另外一条物理连接，保证业务正常平稳运行。

11.2 虚拟网关

虚拟网关是物理连接的接入路由器，是实现物理连接访问VPC的逻辑接入网关。虚拟网关与云专线需要直连的VPC绑定，如果用户需要访问多个VPC，则也可通过虚拟网关关联需要访问的VPC网段，通过对等连接或云连接实现访问多个VPC的功能。

一个虚拟网关只能关联一个VPC，多条物理连接可以通过同一个虚拟网关实现专线接入，访问同一个VPC。

11.3 虚拟接口

虚拟接口是用户本地数据中心通过专线访问VPC的入口，用户创建虚拟接口关联物理连接和虚拟网关，连通用户网关和虚拟网关，实现云下数据中心和云上VPC的互访。

虚拟接口支持静态路由和BGP动态路由协议。在物理专线接入的过程中，您可以使用BGP来实现本地数据中心与虚拟网关之间的内网互连。BGP可以帮您更高效、灵活且可靠地搭建混合云。

11.4 区域和可用区

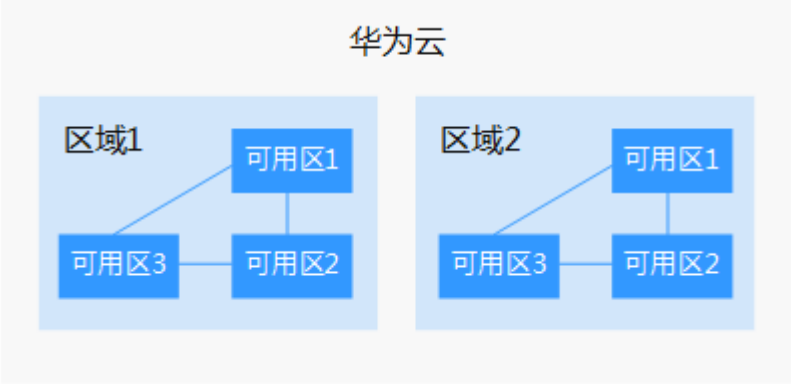
什么是区域、可用区?

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的Region；专属Region指只承载同一类业务或只面向特定租户提供业务服务的专用Region。
- 可用区（AZ，Availability Zone）：一个AZ是一个或多个物理数据中心的集合，有独立的风火水电，AZ内逻辑上再将计算、网络、存储等资源划分成多个集群。一个Region中的多个AZ间通过高速光纤相连，以满足用户跨AZ构建高可用性系统的需求。

图11-1阐明了区域和可用区之间的关系。

图 11-1 区域和可用区



目前，华为云已在全球多个地域开放云服务，您可以根据需求选择适合自己的区域和可用区。更多信息请参见**华为云全球站点**。

如何选择区域?

选择区域时，您需要考虑以下几个因素：

- 地理位置

  一般情况下，建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

  - 在除中国大陆以外的亚太地区有业务的用户，可以选择“中国-香港”、“亚太-曼谷”或“亚太-新加坡”区域。
  - 在非洲地区有业务的用户，可以选择“非洲-约翰内斯堡”区域。
  - 在拉丁美洲地区有业务的用户，可以选择“拉美-圣地亚哥”区域。

    说明

    “拉美-圣地亚哥”区域位于智利。

- 资源的价格

  不同区域的资源价格可能有差异，请参见**华为云服务价格详情**。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关华为云的区域和终端节点的更多信息，请参阅**地区和终端节点**。