

云连接

产品介绍

文档版本 01
发布日期 2026-02-27



版权所有 © 华为云计算技术有限公司 2026。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI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云计算技术有限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，华为云计算技术有限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。

目录

1 什么是云连接	1
2 产品优势	6
3 应用场景	7
4 产品功能	10
5 支持区域	13
5.1 云连接实例和中心网络支持的区域.....	13
5.2 大区 and 区域的对应关系.....	15
5.3 区域和可用区.....	15
6 安全	18
6.1 责任共担.....	18
6.2 身份认证与访问控制.....	19
6.3 审计与日志.....	20
6.4 服务韧性.....	20
6.5 监控安全风险.....	20
6.6 认证证书.....	20
7 权限管理	23
8 约束与限制	31
9 与其他服务的关系	34

1 什么是云连接

云连接（Cloud Connect）通过其提供的云连接实例和中心网络功能，为用户提供了两种能够快速构建跨区域VPC之间以及云上多VPC与云下多数数据中心之间的高速、优质、稳定的网络能力，帮助用户打造一张具有企业级规模和通信能力的全球云上互连网络。如表1-1所示，您可以根据实际业务需求选择适合的云连接功能。

表 1-1 云连接功能说明

云连接功能	适用场景	关联能力	功能特点	支持区域
云连接实例	<ul style="list-style-type: none">• 连通不同区域的VPC网络（私有网络）。• 连通不同区域的多个VPC和云下IDC的网络（混合云网络）。	通过购买带宽包，配置连通不同区域的域间带宽，可以实现跨区域网络实例互通。	<ul style="list-style-type: none">• 组网简单• 分钟级连通跨区域的VPC网络• 将不同区域的VPC接入云连接实例，实现私网网络和混合云网络互通	云连接实例支持区域
中心网络	<ul style="list-style-type: none">• 连通不同区域的企业路由器网络，通过企业路由器连通不同区域的VPC网络（私有网络）。• 连通不同区域的多个企业路由器和云下IDC的网络，通过多个企业路由器连通不同区域的VPC网络（混合云网络）。	通过购买全域互联带宽，配置连通不同区域的全域互联带宽值，可以实现跨区域网络实例互通。	<ul style="list-style-type: none">• 组网灵活• 支持动态路由能力• 支持多种连接，可构造多种网络场景• 将不同区域的企业路由器接入中心网络，实现私网网络和混合云网络互通	中心网络支持区域

云连接实例

云连接实例（Cloud Connection）可帮助用户在不同区域VPC之间、VPC与本地数据中心之间搭建通信通道，实现跨区域VPC之间以及云上多VPC与云下多数据中心之间的网络互通。

- 连通不同区域的VPC网络

如图1-1所示，在区域A内将VPC-A01、VPC-A02接入云连接实例，在区域B内将VPC-B01、VPC-B02接入云连接实例，在区域C内将VPC-C01、VPC-C02接入云连接实例，通过云连接实例连通区域A、区域B、区域C的VPC网络，实现了跨区域VPC网络互通。即可以实现VPC-A01、VPC-A02、VPC-B01、VPC-B02、VPC-C01、VPC-C02的网络互通。

- 连通不同区域的多个VPC和云下IDC的网络

如图1-1所示，首先，在区域A内将VPC-A01、VPC-A02接入云连接实例，在区域B内将VPC-B01、VPC-B02接入云连接实例，在区域C内将VPC-C01、VPC-C02接入云连接实例，通过云连接实例连通区域A、区域B、区域C的VPC网络，实现了跨区域VPC网络互通。即可以实现VPC-A01、VPC-A02、VPC-B01、VPC-B02、VPC-C01、VPC-C02的网络互通。

然后结合云专线的虚拟网关能力，将云下数据中心IDC-A、IDC-B接入云连接实例网络，实现不同区域的VPC网络和本地数据中心之间互通。即可以实现VPC-A01、VPC-A02、VPC-B01、VPC-B02、VPC-C01、VPC-C02、IDC-A、IDC-B的网络互通。

云连接实例相关概念，请参见表1-2。

图 1-1 云连接实例网络原理图

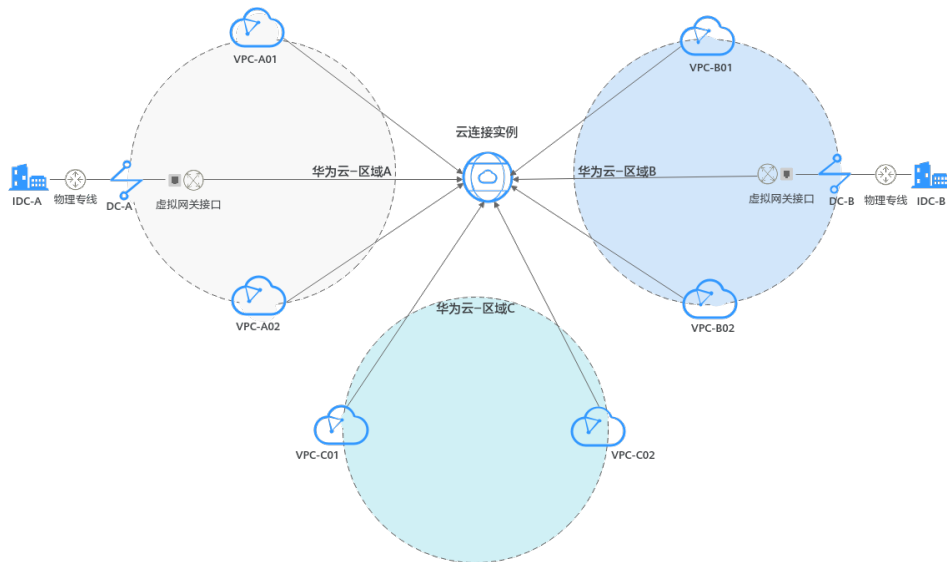


表 1-2 云连接实例相关概念

概念	说明
网络实例	<p>网络实例包括虚拟私有云（VPC）、虚拟网关（VGW）。</p> <ul style="list-style-type: none">将VPC加载到云连接实例，可以实现VPC之间的互通。将虚拟网关加载到云连接实例，可以实现云下IDC与云上多VPC互通，构建混合云。 <p>在云专线服务中，虚拟网关将虚拟接口和VPC关联，即可实现本地数据中心访问VPC。云专线的更多信息，请参见什么是云专线。</p>
带宽包	<ul style="list-style-type: none">跨区域网络实例互通需要购买带宽包，包括以下两种场景：<ul style="list-style-type: none">大区内互通的带宽，用于配置同一个大区内不同区域间，网络实例互通的域间带宽。大区之间互通的带宽，用于配置两个大区内不同区域间，网络实例互通的域间带宽。同区域网络实例互通不需要购买带宽包。 <p>说明 大区和区域的对应关系，请参见大区和区域的对应关系。</p>
域间带宽	域间带宽指所规划的场景中，一个区域到另一个区域的网络带宽，可以实现两个区域之间的互通。基于一个带宽包配置的多个域间带宽的总和不能超过带宽包的总带宽。

中心网络

中心网络（Central Network）基于华为云骨干网络面向客户提供全球网络管理能力。中心网络可帮助用户在不同区域企业路由器之间、企业路由器与本地数据中心间搭建通信通道，实现同区域或跨区域网络互通。同时，中心网络支持定义灵活的企业路由器互通策略，帮助您打造一张灵活、可靠、智能的企业级全球互连网络。

- 连通不同区域的VPC网络

如[图1-2](#)所示，首先，在区域A内将VPC-A01和VPC-A02接入ER-A，在区域B内将VPC-B01和VPC-B02接入ER-B，在区域C内将VPC-C01和VPC-C02接入ER-C，分别通过企业路由器连通同区域VPC网络，实现同区域VPC网络互通。即可以实现区域A的VPC-A01、VPC-A02的网络互通，区域B的VPC-B01、VPC-B02的网络互通，区域C的VPC-C01、VPC-C02的网络互通。

然后将ER-A、ER-B和ER-C接入中心网络中，连通不同区域的ER，从而实现跨区域VPC网络互通。即可以实现VPC-A01、VPC-A02、VPC-B01、VPC-B02、VPC-C01、VPC-C02的网络互通。

- 连通不同区域的多个VPC和云下IDC的网络

如[图1-2](#)所示，首先，在区域A内将VPC-A01和VPC-A02接入ER-A，在区域B内将VPC-B01和VPC-B02接入ER-B，在区域C内将VPC-C01和VPC-C02接入ER-C，并结合云专线的全域接入网关能力，快速实现同区域多个VPC和云下数据中心的网络互通。即可以实现区域A的VPC-A01、VPC-A02、IDC-A的网络互通，区域B的VPC-B01、VPC-B02、IDC-B的网络互通，区域C的VPC-C01、VPC-C02的网络互通。

然后将ER-A、ER-B和ER-C接入中心网络中，连通不同区域的云内网络，实现不同区域的VPC网络和本地数据中心之间互通。即可以实现VPC-A01、VPC-A02、VPC-B01、VPC-B02、VPC-C01、VPC-C02、IDC-A、IDC-B的网络互通。

中心网络相关概念，请参见表1-3。

图 1-2 中心网络原理图

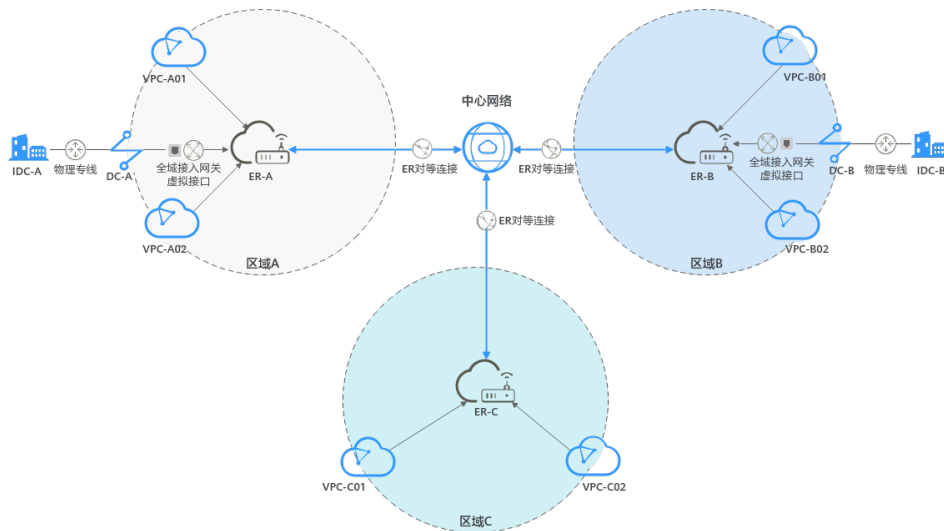


表 1-3 中心网络相关概念

概念	说明
企业路由器	通过企业路由器可以实现相同区域的VPC网络互通，并结合云专线的全域接入网关能力，实现相同区域的VPC和IDC网络互通，然后将两个及以上企业路由器接入云连接的中心网络中，构成ER对等连接，则可以实现云上跨区域多个VPC和云下IDC的网络互通。企业路由器的更多信息，请参见 什么是企业路由器 。
全域接入网关	通过企业路由器和云专线的全域接入网关可以构建线下IDC和云上VPC互通的混合云组网。全域接入网关与中心网络下的不同ER通过华为云骨干网络搭建连接，降低时延，简化网络拓扑，降低网络管理难度，提升网络运维效率。
全域互联带宽	全域互联带宽通过绑定中心网络，从而控制中心网络在云内骨干网络的通信速率，包括以下场景： <ul style="list-style-type: none"> 大区带宽：用于连通同一个大区内的云内骨干网络。 跨区带宽：用于连通不同大区内的云内骨干网络。 更多信息，请参见 大区/跨区带宽使用场景（中心网络） 。

如何访问云连接

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问云连接。

- 管理控制台方式

管理控制台是网页形式的，您可以使用直观的界面进行相应的操作。登录[管理控制台](#)，从主页选择“云连接”。

- API方式

如果用户需要将云平台上的云连接集成到第三方系统，用于二次开发，请使用API方式访问云连接，具体操作请参见《[云连接API参考](#)》。

2 产品优势

云连接服务具有以下几大产品优势：

- **全网互联**
云上网络任意两点互联，保证网络转发一跳可达，无须中转。
- **简单灵活**
只需三步，分钟级构建跨区域跨境多VPC互通网络，支持混合云架构。
- **性能优异**
华为全球网络基础设施能力，提供低时延、高质量体验。
- **全球合规**
提供全球一站式合规的网络能力，支持用户专注自身业务创新。

3 应用场景

云连接实例应用场景

云连接实例（Cloud Connection）可帮助用户在不同区域VPC之间、VPC与本地数据中心之间搭建通信通道，实现跨区域VPC之间以及云上多VPC与云下多数据中心之间的网络互通。

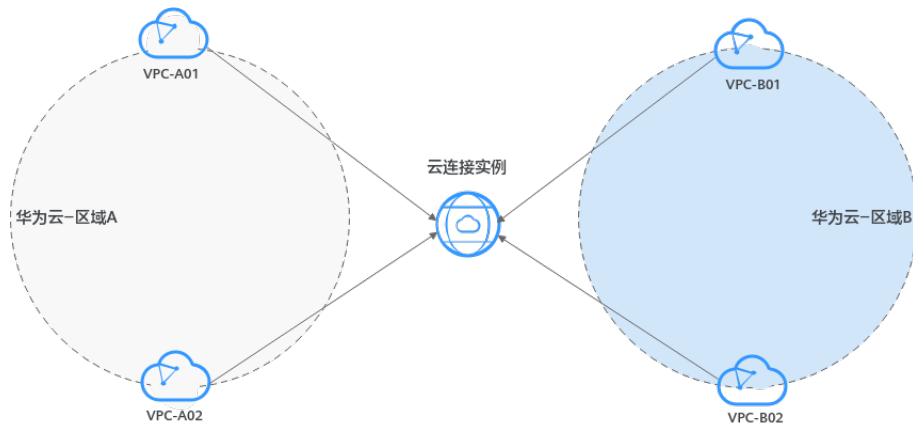
- 连通同区域的VPC网络（私有网络）
加载至云连接实例的同区域VPC之间默认互通。

图 3-1 同区域 VPC 互通场景图



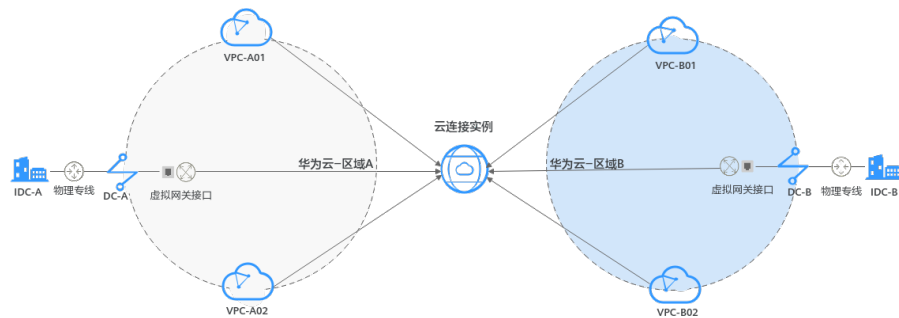
- 连通不同区域的VPC网络（私有网络）
当云上多个区域的VPC之间需要跨区域进行私网通信时，云连接实例可以根据您的网络规划，轻松实现多个跨区域VPC连通的场景，提高网络拓扑的灵活性，并为您提供安全可靠的私网通信。

图 3-2 跨区域 VPC 互通场景图



- 连通不同区域的多个VPC和云下IDC的网络（混合云网络）
当用户本地的多个数据中心需要与云上多个区域的VPC进行私网通信时，您可以通过云专线实现本地数据中心接入云上VPC，再通过云连接实例加载需要互通的VPC和数据中心接入的虚拟网关，实现本地数据中心与多区域的VPC的私网通信，实现多点全网通场景。

图 3-3 跨区域 VPC 与云下 IDC 互通场景图

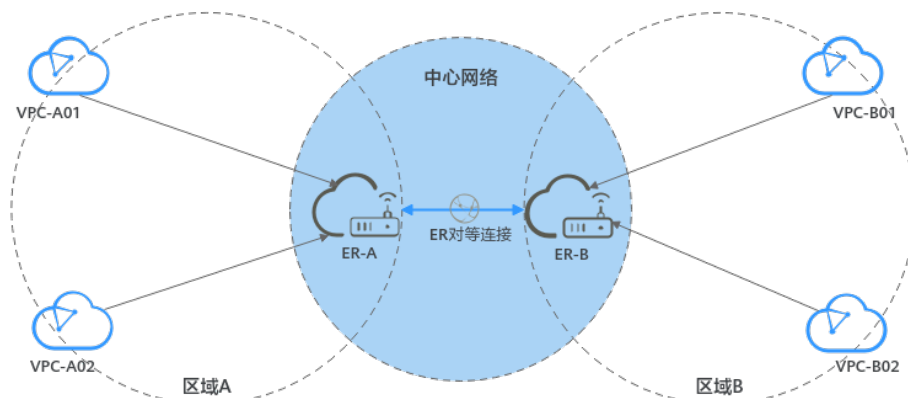


中心网络应用场景

当您的云服务实例需要通过接入企业路由器实现网络互通时，中心网络可帮助您在不同区域企业路由器之间、企业路由器与本地数据中心之间搭建通信通道，实现同区域或跨区域网络互通。

- 连通不同区域的企业路由器网络，通过企业路由器连通不同区域的VPC网络（私有网络）
云上不同区域的企业路由器通过接入中心网络实现跨区域互通。

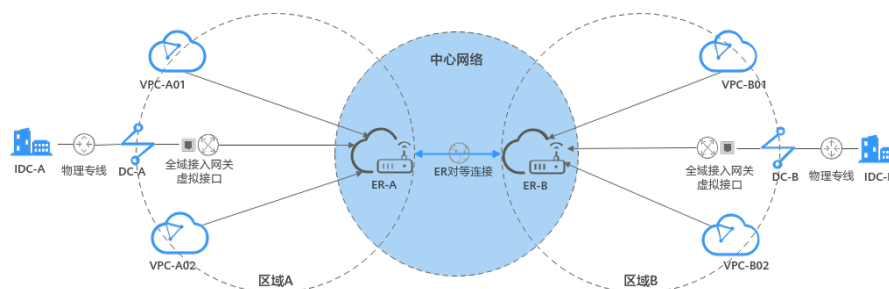
图 3-4 企业路由器跨区域 VPC 互通



- 连通不同区域的多个企业路由器和云下IDC的网络，通过多个企业路由器连通不同区域的VPC网络（混合云网络）

通过企业路由器结合云专线的全域接入网关能力，实现VPC与用户本地数据中心网络互通，然后将两个及以上企业路由器接入云连接的中心网络中，构成ER对等连接，则可以实现云上跨区域多个VPC和云下IDC的网络互通。

图 3-5 企业路由器与云下数据中心互通



- 通过灵活更换企业路由器的互通策略，更便捷地组建用户的全球网络。

4 产品功能

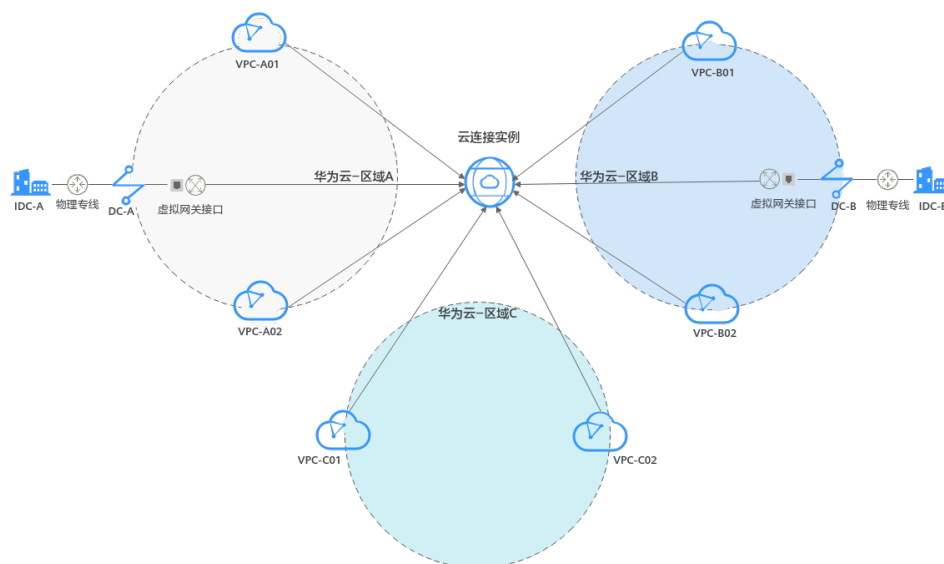
本页面介绍了CC服务支持的主要功能。关于各功能支持的地域（Region）信息，可通过控制台查询详情。

云连接实例

云连接实例（Cloud Connection）可帮助用户在不同区域VPC之间、VPC与本地数据中心之间搭建通信通道，实现跨区域VPC之间以及云上多VPC与云下多数据中心之间的网络互通。

通过创建云连接实例，将用户所需要实现互通的不同区域的网络实例加载到创建的云连接实例中，这里的网络实例可以是用户自己创建的VPC实例或用户创建的用于本地数据中心接入的虚拟网关实例，也可以是其他用户授予权限允许加载的VPC实例，最后通过配置需要互通的网络实例之间的域间带宽，就可以快速地为您提供全球网络互通服务。请参考[云连接实例概述](#)。

图 4-1 云连接实例网络原理图



网络实例

网络实例可以是用户自己创建的VPC实例或用户创建的用于本地数据中心接入的虚拟网关实例，也可以是其他用户授予权限允许加载的VPC实例，最后通过配置需要互通

的网络实例之间的域间带宽，就可以快速地为您提供全球网络互通服务。请参考[网络实例概述](#)。

带宽包

- 跨区域网络实例互通需要购买带宽包，包括以下两种场景：
 - 大区内互通的带宽，用于配置同一个大区内不同区域间，网络实例互通的域间带宽。
 - 大区之间互通的带宽，用于配置两个大区内不同区域间，网络实例互通的域间带宽。
- 同区域网络实例互通不需要购买带宽包。

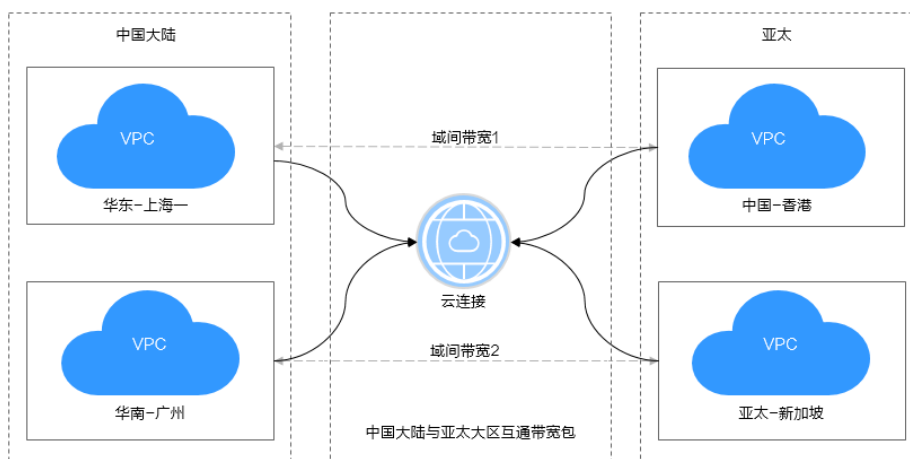
请参考[带宽包概述](#)。

域间带宽

域间带宽指所规划的场景中，一个区域到另一个区域的网络带宽，可以实现两个区域之间的互通。域间带宽是带宽包在跨区域互通场景下的实际带宽分配设置，基于一个带宽包配置的多个域间带宽的总和不能超过带宽包的总带宽。

以中国大陆与亚太大区互通为例，详细请参见[图4-2](#)。请参考[域间带宽概述](#)。

图 4-2 跨大区互通带宽包和域间带宽

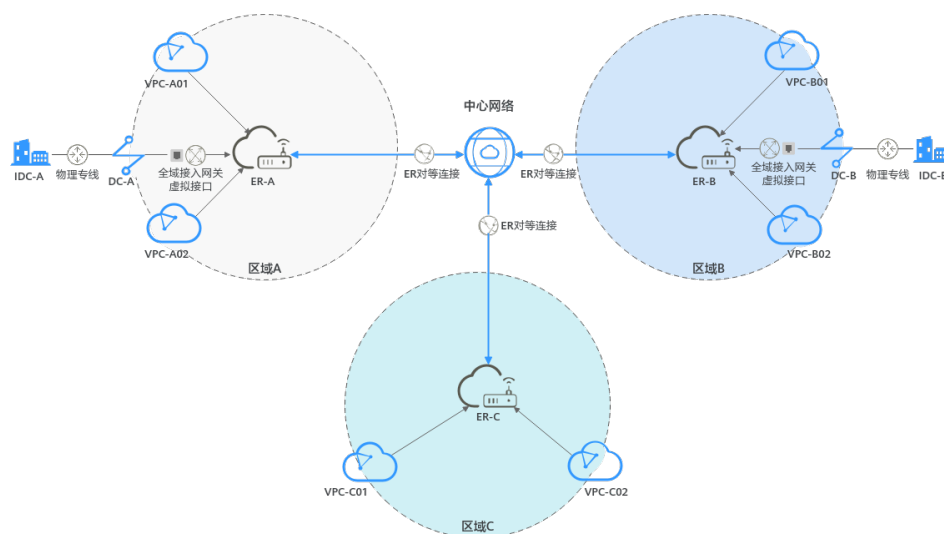


中心网络实例

中心网络（Central Network）基于华为云骨干网络面向客户提供全球网络管理能力。中心网络可帮助用户在不同区域企业路由器之间、企业路由器与本地数据中心间搭建通信通道，实现同区域或跨区域网络互通。同时，中心网络支持定义灵活的企业路由器互通策略，帮助您打造一张灵活、可靠、智能的企业级全球互连网络。

请参考[中心网络概述](#)。

图 4-3 中心网络原理图



全域互联带宽

全域互联带宽通过绑定云上的网络实例，从而控制网络实例在云内骨干网络的通信速率。

全域互联带宽根据连接范围大小，分为不同类型，连接范围由小到大依次为城域带宽、区域带宽、大区带宽、跨区带宽，云连接服务主要涉及大区带宽和跨区带宽。请参考[全域互联带宽概述](#)。

5 支持区域

5.1 云连接实例和中心网络支持的区域

本文介绍[云连接实例](#)和[中心网络](#)支持的区域。

云连接实例支持区域

云连接实例支持的区域，请参见[表5-1](#)。

表 5-1 云连接实例支持区域

大区	区域
中国大陆	华北-北京四
	华北-北京一
	华北-乌兰察布一
	华东-上海一
	华东-上海二
	华南-广州
	华南-广州-友好用户环境
	华南-深圳
	西南-贵阳一
	华东二（中国-华东-芜湖）
亚太	中国-香港
	亚太-新加坡
	亚太-曼谷
南非	非洲-约翰内斯堡

大区	区域
拉美西	拉美-圣地亚哥
拉美东	拉美-圣保罗一
拉美北	拉美-墨西哥城一
	拉美-墨西哥城二

中心网络支持区域

中心网络支持的区域，请参见表5-2。

表 5-2 中心网络支持区域

区域
华北-北京四
华北-乌兰察布一
华东-上海一
华南-广州
西南-贵阳一
华东-青岛
华东二（中国-华东-芜湖）
中国-香港
亚太-新加坡
亚太-曼谷
亚太-雅加达
亚太-马尼拉
非洲-约翰内斯堡
拉美-圣地亚哥
拉美-圣保罗一
拉美-墨西哥城二
土耳其-伊斯坦布尔
非洲-开罗
中东-利雅得

5.2 大区 and 区域的对应关系

表 5-3 大区 and 区域的对应关系

大区	区域
中国大陆	华北-北京一
	华北-北京四
	华北-乌兰察布一
	华东-上海一
	华东-上海二
	华南-广州
	华南-深圳
	西南-贵阳一
	华东二 您在控制台购买全域互联带宽，选择“指定互通区域”时，“华东二”对应的区域请选择“中国-华东-芜湖”。
亚太	中国-香港
	亚太-新加坡
	亚太-曼谷
	亚太-雅加达
南非	非洲-约翰内斯堡
拉美西	拉美-圣地亚哥
拉美东	拉美-圣保罗一
拉美北	拉美-墨西哥城一
	拉美-墨西哥城二

5.3 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。

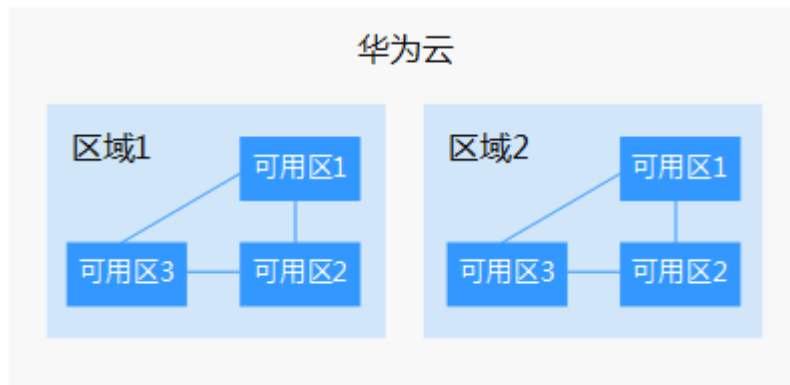
- 区域（Region）：从地理位置和网络时延维度划分，同一个Region内共享弹性计算、块存储、对象存储、VPC网络、弹性公网IP、镜像等公共服务。Region分为通用Region和专属Region，通用Region指面向公共租户提供通用云服务的

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5-1阐明了区域和可用区之间的关系。

图 5-1 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](#)。

6 安全

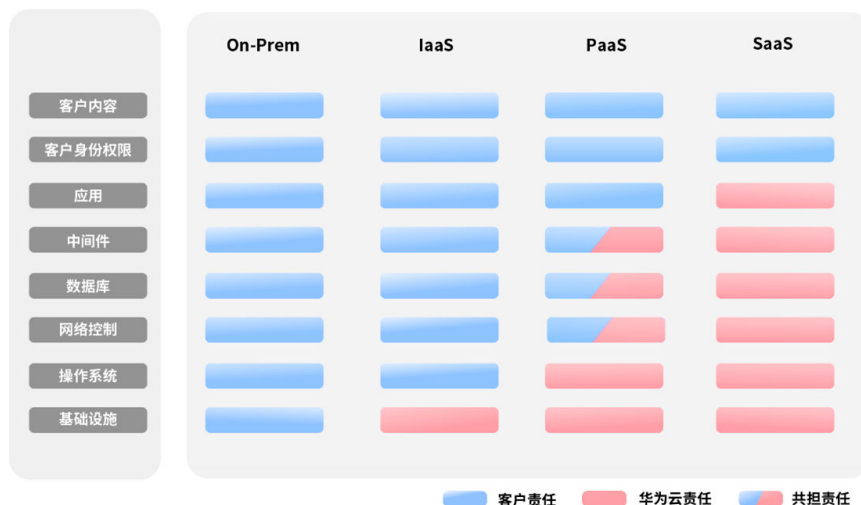
6.1 责任共担

华为云秉承“将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。

与传统的本地数据中心相比，云计算的运营方和使用方分离，提供了更好的灵活性和控制力，有效降低了客户的运营负担。正因如此，云的安全性无法由一方完全承担，云安全工作需要华为云与您共同努力，如图6-1所示。

- **华为云**：无论在任何云服务类别下，华为云都会承担基础设施的安全责任，包括安全性、合规性。该基础设施由华为云提供的物理数据中心（计算、存储、网络等）、虚拟化平台及云服务组成。在PaaS、SaaS场景下，华为云也会基于控制原则承担所提供服务或组件的安全配置、漏洞修复、安全防护和入侵检测等职责。
- **客户**：无论在任何云服务类别下，客户数据资产的所有权和控制权都不会转移。在未经授权的情况下，华为云承诺不触碰客户数据，客户的内容数据、身份和权限都需要客户自身看护，这包括确保云上内容的合法合规，使用安全的凭证（如强口令、多因子认证）并妥善管理，同时监控内容安全事件和账号异常行为并及时响应。

图 6-1 华为云安全责任共担模型



云安全责任基于控制权，以可见、可用作为前提。在客户上云的过程中，资产（例如设备、硬件、软件、介质、虚拟机、操作系统、数据等）由客户完全控制向客户与华为云共同控制转变，这也就意味着客户需要承担的责任取决于客户所选取的云服务。如图6-1所示，客户可以基于自身的业务需求选择不同的云服务类别（例如IaaS、PaaS、SaaS）。不同的云服务类别中，每个组件的控制权不同，这也导致了华为云与客户的责任关系不同。

- 在On-prem场景下，由于客户享有对硬件、软件和数据等资产的全部控制权，因此客户应当对所有组件的安全性负责。
- 在IaaS场景下，客户控制着除基础设施外的所有组件，因此客户需要做好除基础设施外的所有组件的安全工作，例如应用自身的合法合规性、开发设计安全，以及相关组件（如中间件、数据库和操作系统）的漏洞修复、配置安全、安全防护方案等。
- 在PaaS场景下，客户除了对自身部署的应用负责，也要做好PaaS服务中间件、数据库、网络控制的安全配置和策略工作。
- 在SaaS场景下，客户对客户内容、账号和权限具有控制权，客户需要做好自身内容的保护以及合法合规、账号和权限的配置和保护等。

传统本地部署(On-Prem)：由客户在自有数据中心内部署和管理软件及IT基础设施，而非依赖于远程的云服务提供商；

基础设施即服务(IaaS)：由云服务提供商提供计算、网络、存储等基础设施服务，如[弹性云服务器 ECS](#)、[虚拟专用网络 VPN](#)、[对象存储服务 OBS](#)；

平台即服务(PaaS)：由云服务提供商提供应用程序开发和部署所需要的平台，客户无需维护底层基础设施，如[AI开发平台 ModelArts](#)、[云数据库 GaussDB](#)；

软件即服务(SaaS)：由云服务提供商提供完整应用软件，客户直接应用软件而无需安装、维护应用软件及底层平台和基础设施，如[华为云会议 Meeting](#)。

6.2 身份认证与访问控制

云连接服务支持通过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CC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](#)。

6.3 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CC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](#)。
- CC支持审计的操作事件，请参见[支持审计的关键操作](#)。
- 查看审计日志，请参见[查看审计日志](#)。

6.4 服务韧性

基于华为在全球专属网络基础设施建设，提供安全的私网传输能力，华为云云连接服务累计在全球20+国家/地区部署，实现每个Region多AZ多集群容灾。

即使部分节点、部分线路发生故障也不会导致网络连接中断，极大提高服务可靠性。

6.5 监控安全风险

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

关于云连接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](#)。

6.6 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 6-2 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 6-3 资源中心

合规资质证书

华为云安全服务提供了网络安全专用产品安全检测证书、软件著作权等证书，供用户下载和参考。具体请查看[合规资质证书](#)。

图 6-4 网络安全专用产品安全检测证书&软件著作权证书

合规资质证书		
华为云安全服务提供了网络安全专用产品安全检测证书、软件著作权等证书，供用户下载和参考。		
软件著作权 <ul style="list-style-type: none">- 安全云脑- 主机安全服务- 容器安全服务- DDoS防护- Web应用防火墙- 数据布安全服务- 数据安全中心- 数据加密服务- 云防火墙- 网络检测与响应- 漏洞扫描服务- 云堡垒机	网络安全专用产品安全检测证书 <ul style="list-style-type: none">- 主机安全服务- 云堡垒机- 安全云脑- 漏洞扫描服务- Web应用防火墙- DDoS防护- 数据布安全服务- 网络检测与响应- 数据加密服务- 云防火墙	商用密码产品认证证书 <ul style="list-style-type: none">- 数据加密服务

7 权限管理

如果您需要对华为云上购买的Cloud 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。如果华为账号已经能满足您的要求，不需要通过IAM对用户进行权限管理，您可以跳过本章节，不影响您使用CC服务的其他功能。

IAM是华为云平台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。

通过IAM，您可以通过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Cloud Connect的使用权限，但是不希望他们拥有删除CC等高危操作的权限，那么您可以使用IAM进行权限分配，通过授予用户仅能使用CC，但是不允许删除CC的权限，控制他们对CC资源的使用范围。

目前IAM支持两类授权，一类是角色与策略授权，另一类为身份策略授权。

两者有如下的区别和关系：

表 7-1 两类授权的区别

名称	核心关系	涉及的权限	授权方式	适用场景
角色与策略授权	用户-权限-授权范围	<ul style="list-style-type: none">● 系统角色● 系统策略● 自定义策略	为主体授予角色或策略	核心关系为“用户-权限-授权范围”，每个用户根据所需权限和所需授权范围进行授权，无法直接给用户授权，需要维护更多的用户组，且支持的条件键较少，难以满足细粒度精确权限控制需求，更适用于对细粒度权限管控要求较低的中小企业用户。

名称	核心关系	涉及的权限	授权方式	适用场景
身份策略授权	用户-策略	<ul style="list-style-type: none">系统策略自定义身份策略	<ul style="list-style-type: none">为主体授予身份策略身份策略附加至主体	核心关系为“用户-策略”，管理员可根据业务需求定制不同的访问控制策略，能够做到更细粒度更灵活的权限控制，新增资源时，对比角色与策略授权，基于身份策略的授权模型可以更快地直接给用户授权，灵活性更强，更方便，但相对应的，整体权限管控模型构建更加复杂，对相关人员专业能力要求更高，因此更适用于中大型企业。

例如：如果需要对IAM用户授予可以创建华北-北京四区域的ECS和华南-广州区域的OBS的权限，基于角色与策略授权的场景中，管理员需要创建两个自定义策略，并且为IAM用户同时授予这两个自定义策略才可以实现权限控制。在基于身份策略授权的场景中，管理员仅需要创建一个自定义身份策略，在策略中通过条件键“g:RequestedRegion”的配置即可达到身份策略对于授权区域的控制。将身份策略附加主体或为主体授予该身份策略即可获得相应权限，权限配置方式更细粒度更灵活。

两种授权模型场景下的策略/身份策略、授权项等并不互通，推荐使用身份策略进行授权。[角色与策略权限管理](#)和[身份策略权限管理](#)分别介绍两种模型的系统权限。

关于IAM的详细介绍，请参见[IAM产品介绍](#)。

角色与策略权限管理

CC服务支持角色与策略授权。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。

CC部署时不区分物理区域，为全局级服务。授权时，在全局级服务中设置权限，访问CC时，不需要切换区域。

如[表7-2](#)所示，包括了CC的所有系统权限。角色与策略授权场景的系统策略和身份策略授权场景的并不互通。

表 7-2 CC 系统权限

系统角色/策略名称	说明	类别	依赖关系
Cross Connect Administrator	云连接服务的管理员权限，拥有该权限的用户拥有云连接服务所有执行权限。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。 <ul style="list-style-type: none"> • 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。
CC FullAccess	云连接服务的所有执行权限。	系统策略	依赖CC Network Depend QueryAccess策略。
CC ReadOnlyAccess	云连接服务的只读权限，拥有该权限的用户仅能查看云连接服务下的资源信息。	系统策略	-
CC Network Depend QueryAccess	云连接服务依赖的只读权限。拥有该权限的用户可以查看以下实例信息： <ul style="list-style-type: none"> • 虚拟私有云VPC • 云专线的虚拟网关VGW • 企业路由器ER 	系统策略	-

表7-3列出了Cloud Connect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 7-3 常用操作与系统权限的关系

操作	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
创建云连接实例	√	√	×
查看云连接实例	√	√	√
修改云连接实例	√	√	×

操作	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
删除云连接实例	√	√	×
绑定带宽包	√	√	×
解绑带宽包	√	√	×
加载网络实例	√	√	×
查看网络实例	√	√	√
更新网络实例	√	√	×
删除网络实例	√	√	×
购买带宽包	√	√	×
查看带宽包	√	√	√
修改带宽包	√	√	×
退订包年/包月带宽包	√	√	×
续费包年/包月带宽包	√	√	×
配置域间带宽	√	√	×
查看域间带宽	√	√	√
修改域间带宽	√	√	×
删除域间带宽	√	√	×
查看域间带宽监控数据	√	√	√
查看路由信息	√	√	√
跨账号授权网络实例	√	√	×
查看授权	√	√	√
查看被授权VPC	√	√	√
取消授权	√	√	×
创建中心网络	√	√	×
更新中心网络	√	√	×
删除中心网络	√	√	×
查询中心网络详情	√	√	√
查询中心网络列表	√	√	√
创建中心网络策略	√	√	×

操作	Cross Connect Administrator	CC FullAccess	CC ReadOnlyAccess
应用中心网络策略	√	√	×
删除中心网络策略	√	√	×
查询中心网络策略列表	√	√	√
查询策略变化集	√	√	√
查询中心网络连接列表	√	√	√
更新中心网络连接	√	√	×
创建中心网络DGW附件	√	√	×
更新中心网络DGW附件	√	√	×
查询中心网络附件详情	√	√	√
查询中心网络DGW附件列表	√	√	√
删除中心网络附件	√	√	×
查询中心网络附件列表	√	√	√
查询配额列表	√	√	√
查询能力列表	√	√	√
创建全域互联带宽	√	√	×
更新全域互联带宽	√	√	×
查询全域互联带宽	√	√	√
删除全域互联带宽	√	√	×

身份策略权限管理

CC服务支持身份策略授权。如表7-4所示，包括了CC身份策略中的所有系统身份策略。身份策略授权场景的系统身份策略与角色授权的系统策略并不互通。

表 7-4 CC 身份系统策略

系统策略名称	说明	策略类别
CCFullAccessPolicy	云连接服务所有权限。	系统身份策略

系统策略名称	说明	策略类别
CCReadOnlyPolicy	云连接服务只读权限。	系统身份策略

表7-5列出了Cloud Connect常用操作与系统身份策略的授权关系，您可以参照该表选择合适的系统身份策略。

表 7-5 常用操作与系统身份策略的关系

操作	CCFullAccessPolicy	CCReadOnlyPolicy
创建云连接实例	√	×
删除云连接实例	√	×
更新云连接实例	√	×
查询云连接实例详情	√	√
查询云连接实例列表	√	√
创建网络实例	√	×
删除网络实例	√	×
更新网络实例	√	×
查询网络实例详情	√	√
查询网络实例列表	√	√
创建带宽包	√	×
删除带宽包	√	×
更新带宽包	√	×
查询带宽包详情	√	√
查询带宽包列表	√	√
关联带宽包	√	×
解关联带宽包	√	×
创建域间带宽	√	×
删除域间带宽	√	×
更新域间带宽	√	×
查询域间带宽详情	√	√
查询域间带宽列表	√	√
查询云连接实例路由详情	√	√

操作	CCFullAccessPolicy	CCReadOnlyPolicy
查询云连接实例路由列表	√	√
查询配额列表权限	√	√
查询云连接实例和中心网络能力列表	√	√
创建中心网络	√	×
删除中心网络	√	×
更新中心网络	√	×
查询中心网络详情	√	√
查询中心网络列表	√	√
创建中心网络策略	√	×
应用中心网络策略	√	×
删除中心网络策略	√	×
查询中心网络策略列表	√	√
查询当前策略与被应用策略变化集	√	√
查询中心网络连接列表	√	√
更新中心网络连接	√	×
创建中心网络DGW附件	√	×
更新中心网络DGW附件	√	×
查询中心网络DGW附件详情	√	√
查询中心网络DGW附件列表	√	√
创建中心网络er-route-table附件	√	×
更新中心网络er-route-table附件	√	×
查询中心网络er-route-table附件详情	√	√
查询中心网络er-route-table附件列表	√	√
删除中心网络附件	√	×
查询中心网络附件列表	√	×

操作	CCFullAccessPolicy	CCReadOnlyPolicy
创建全域互联带宽	√	×
更新全域互联带宽	√	×
查询全域互联带宽	√	√
删除全域互联带宽	√	×

CC 控制台功能依赖的角色或策略

表 7-6 CC 控制台依赖服务的角色或策略

控制台功能	依赖服务	需配置角色/策略
为中心网络配置跨区域连接带宽	全域互联带宽	IAM用户设置了CCFullAccessPolicy权限，同时需要增加CC ReadOnlyAccess权限，之后为中心网络配置跨区域连接带宽时，才可以选择全域互联带宽资源。
为中心网络修改跨区域连接带宽	全域互联带宽	IAM用户设置了CCFullAccessPolicy权限，同时需要增加CC ReadOnlyAccess权限，之后才可以修改中心网络的跨区域连接带宽。
查看中心网络的跨区域连接带宽	全域互联带宽	IAM用户设置了CCFullAccessPolicy权限，同时需要增加CC ReadOnlyAccess权限，之后才可以查看到中心网络的跨区域连接带宽。

相关链接

- [IAM产品介绍](#)

8 约束与限制

使用限制

云连接在使用过程中存在以下限制，您可以单击以下链接，了解不同功能的限制说明。

[云连接实例限制](#)

[跨境申请限制](#)

[网络实例限制](#)

[带宽包限制](#)

[域间带宽限制](#)

[跨账号授权限制](#)

[路由限制](#)

[中心网络限制](#)

[全域互联带宽限制](#)

云连接实例使用限制

- 在同一个云连接实例里，所有网络实例Subnet子网CIDR不能冲突，否则可能会引起互通问题。
- 在云连接实例中，同账号加载VPC网络实例，并通过其他网段引入自定义CIDR时，不能引入回环地址，组播地址或广播地址。
- 在同一个云连接实例里加载的所有VPC网络实例里，如果某个VPC同时创建了NAT网关，则只能同时在该VPC网络实例里通过高级配置自定义子网的方式引入默认路由“0.0.0.0/0”。
- 云连接实例支持绑定多个不同计费模式的带宽包。
- 互通大区及计费模式相同的带宽包，一个云连接实例只能绑定一个带宽包。

中心网络使用限制

- 使用中心网络前需要先创建以下资源，否则将无法配置。
 - 企业路由器：用于创建中心网络。

- 全域接入网关：用于添加附件管理。
- 策略管理：
 - 同一中心网络仅支持应用一个策略，如需应用其他策略可直接选择要关联的策略，之前已应用的策略将自动取消关联。
 - 同一策略中一个区域仅支持添加一个企业路由器，创建的企业路由器之间默认互联。
 - 当策略实例处于应用中或取消中，不能执行删除操作。
- 跨区域连接带宽管理：
 - 当跨区域连接实例处于创建中、更新中、删除中、冻结中、解冻中或恢复中的过程状态时，不能执行修改连接带宽和删除连接带宽操作。
 - 配置的跨区域连接带宽大小不可超过购买的全域互联带宽的最大带宽。
 - 删除连接带宽后，未删除的全域互联带宽仍会继续收费。

CC 服务配额限制

配额是在某一区域或账号下最多可同时拥有的某种资源的数量。

例如：华为云A账户下，中心网络默认配额为6个，若在该账户下已创建2个中心网络，则在该账户的剩余配额为4个。

华为云为防止资源滥用，对云服务每个账户或每个区域的用户资源数量和容量做了配额限制。

如需查看每个配额项目支持的默认配额，请参考[怎样查看我的配额？](#)，登录控制台查询您的配额详情。如需扩大资源配额，请在华为云管理控制台[申请扩大配额](#)。

[表8-1](#)和[表8-2](#)介绍云连接实例和中心网络的默认配额限制。

云连接实例配额限制

表 8-1 云连接实例配额说明

配额类型	默认配额限制	是否支持调整
一个账号支持创建的云连接实例数	6	是 提交工单 申请提升配额
一个云连接实例支持加载的区域数	6	是 提交工单 申请提升配额
单个区域支持加载的网络实例数	6	是 跨区域互通时 提交工单 申请提升配额，最多可申请10个。
同一云连接实例内，支持购买的相同互通区域带宽包的数量	1	不支持修改
一个云连接实例内，支持创建的路由条目的数量	50	是 提交工单 申请提升配额

中心网络配额限制

表 8-2 中心网络配额说明

配额类型	默认配额限制	是否支持调整
一个账号的中心网络数	6	是 提交工单 申请提升配额
一个中心网络的策略版本数	500	是 提交工单 申请提升配额
中心网络策略文档大小 (KB)	10	不支持修改
一个中心网络单个区域的 ER 实例数	1	不支持修改
一个中心网络单个区域的全域接入网关 (DGW) 附件数	3	是 提交工单 申请提升配额

9 与其他服务的关系

云连接实例与其他服务的关系

图 9-1 云连接实例服务与其他服务的关系示意图

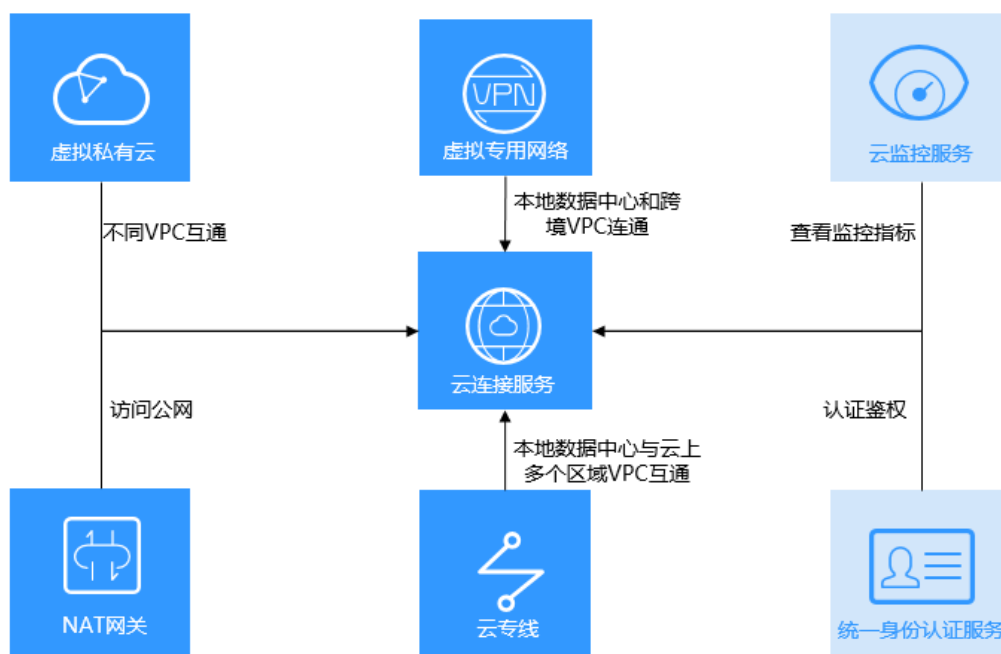


表 9-1 云连接实例与其他服务的关系

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, 不同VPC通过加载至云连接实例实现互通。	创建虚拟私有云及默认子网
云专线 (Direct Connect, DC)	通过云专线服务, 实现本地数据中心访问多个跨区域VPC。	多数据中心与多区域VPC互通

相关服务	交互功能	位置
虚拟专用网络（Virtual Private Network, VPN）	通过VPN服务，可以实现本地数据中心和跨境VPC之间的稳定网络连通。	构建稳定的跨境网络连接
NAT网关（NAT Gateway）	通过NAT网关服务，可以实现本地数据中心服务器访问公网或为公网提供服务。	基于云连接和SNAT实现跨区域内网访问公网服务器加速
云监控（Cloud Eye Service, CES）	通过云监控服务，查看云连接资源的监控数据，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连接资源，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连接资源的访问权限。	统一身份认证服务

中心网络与其他服务的关系

表 9-2 中心网络与其他服务的关系

相关服务	交互功能	位置
企业路由器（Enterprise Router, ER）	通过企业路由器可以实现相同区域的VPC网络互通，并结合云专线的全域接入网关能力，实现相同区域的VPC和IDC网络互通，然后将两个及以上企业路由器接入云连接的中心网络中，构成ER对等连接，则可以实现云上跨区域多个VPC和云下IDC的网络互通。	什么是企业路由器
全域接入网关（Global DC Gateways, DGW）	通过企业路由器和云专线的全域接入网关可以构建线下IDC和云上VPC互通的混合云组网。全域接入网关与中心网络下的不同ER通过华为云骨干网络搭建连接，降低时延，简化网络拓扑，降低网络管理难度，提升网络运维效率。	全域接入网关概述

相关服务	交互功能	位置
全域互联带宽 (Global Connection Bandwidths)	全域互联带宽通过绑定中心网络，从而控制中心网络在云内骨干网络的通信速率，包括以下场景： <ul style="list-style-type: none">大区带宽：用于连通同一个大区内的云内骨干网络。跨区带宽：用于连通不同大区内的云内骨干网络。	大区/跨区带宽使用场景 (中心网络)
云监控 (Cloud Eye Service, CES)	通过云监控服务，查看中心网络资源的监控数据，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，针对您创建的中心网络资源，向不同用户设置不同的使用权限，可以帮助您安全地控制中心网络资源的访问权限。	统一身份认证服务