VPC 终端节点

产品介绍

文档版本 01

发布日期 2023-07-30

华为技术有限公司

版权所有 © 华为技术有限公司 2023。 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

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。

目 录

1 什么是 VPC 终端节点? 1
2 产品优势 4
3 应用场景 5
4 约束与限制 7
5 与其他服务的关系 8
6 计费说明 10
7 安全 12
7.1 责任共担 12
7.2 身份认证与访问控制 13
7.3 审计与日志 13
7.4 服务韧性 14
7.5 认证证书 14
8 权限管理 16
9 基本概念 18
9.1 终端节点服务 18
9.2 终端节点 19
9.3 用户权限 20
9.4 区域和可用区 20
9.5 项目和企业项目 21

 版权所有 © 华为技术有限公司

1 什么是 VPC 终端节点?

VPC终端节点（VPC Endpoint），能够将VPC私密地连接到终端节点服务（云服务、用户私有服务），使VPC中的云资源无需弹性公网IP就能够访问终端节点服务，提高了访问效率，为您提供更加灵活、安全的组网方式。

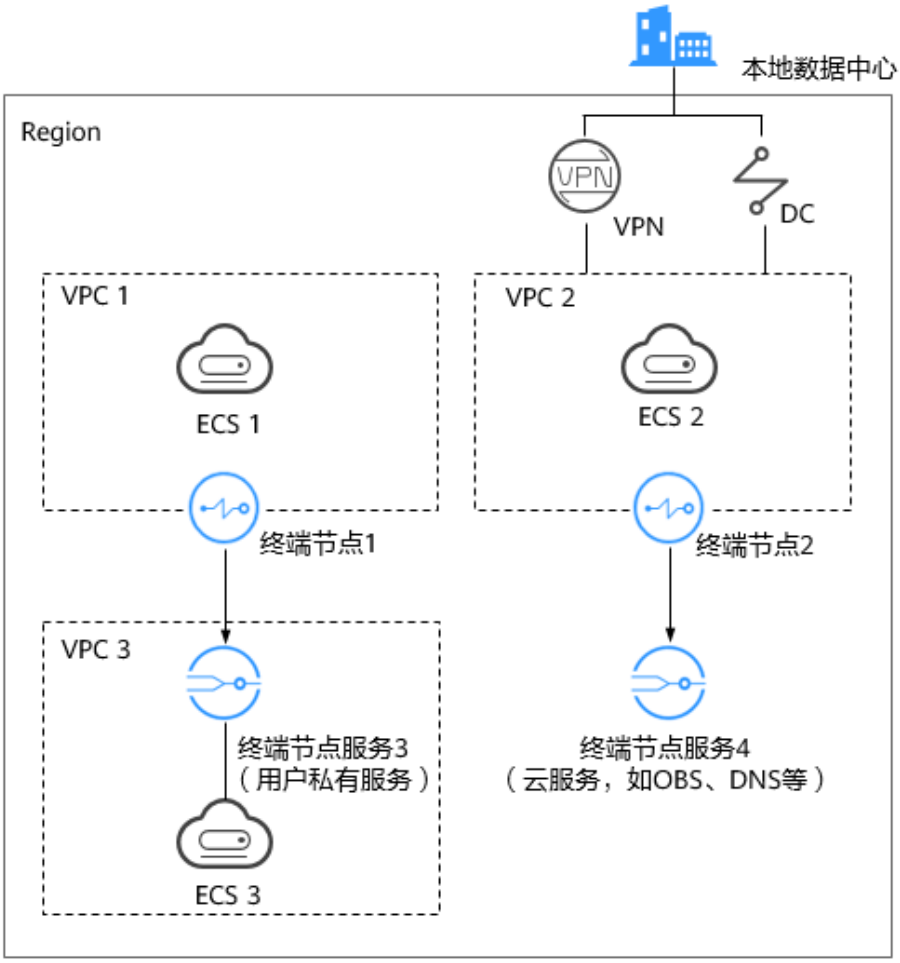
产品架构

VPC终端节点由“终端节点服务”和“终端节点”两种资源实例组成。

- 终端节点服务：指将云服务或用户私有服务配置为VPC终端节点支持的服务，可以被终端节点连接和访问。
  更多内容，请参考**终端节点服务**。
- 终端节点：用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。
  更多内容，请参考**终端节点**。

版权所有 © 华为技术有限公司

图 1-1 VPC 终端节点组网示意图



如图1-1所示，建立了“终端节点”到“终端节点服务”的访问通道，实现：

- VPC 1中的云资源（ECS 1）通过内网访问VPC 3中的云资源（ECS 3）。
- VPC 2中的云资源（ECS 2）通过内网访问云服务（如OBS、DNS）。
- 本地数据中心（IDC）通过VPN或者DC的方式与VPC 2连通，实现IDC通过内网访问云服务（如OBS、DNS）。

更多关于VPC终端节点的组网应用信息，请参见**应用场景**。

如何访问 VPC 终端节点

VPC终端节点提供了Web化的服务管理平台，即管理控制台和基于HTTPS请求的API（Application programming interface）管理方式。

- 控制台方式

  用户可直接登录管理控制台访问VPC终端节点。
  - 如果用户已注册帐户，可直接登录管理控制台，从主页选择“网络 > VPC终端节点”。
  - 如果未注册，请参见**准备工作**中的“注册华为云”。

  通过管理控制台上的简单配置，可以快速的使用VPC终端节点。

 版权所有 © 华为技术有限公司

- API方式

  如果用户需要将VPC终端节点集成到第三方系统，用于二次开发，请使用API方式访问VPC终端节点，具体操作请参见**《VPC终端节点API参考》**。

 版权所有 © 华为技术有限公司

2 产品优势

- **性能优异**：每个网关节点可提供百万级对话，满足多种应用场景需求。
- **即创即用**：秒级创建，快速生效，迅速响应，方便用户及时使用。
- **使用灵活**：无需弹性公网IP，直连内网，使用更加灵活。
- **安全性高：**用户能够通过终端节点私密地连接到终端节点服务，避免泄漏服务端相关信息所带来不可知的风险。

版权所有 © 华为技术有限公司

3 应用场景

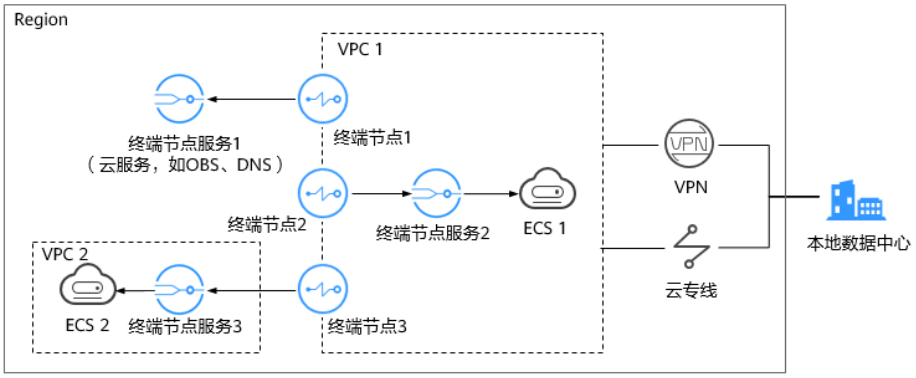
在同一区域中，VPC终端节点可以建立终端节点（VPC内云资源）到终端节点服务（用户私有服务、云服务）的便捷、安全、私密连接通道。

基于上述功能，VPC终端节点主要应用于以下场景。

高速上云

本地数据中心可以通过VPN或者云专线连通VPC，利用建立的终端节点通过内网访问终端节点服务（用户私有服务、云服务）。

图 3-1 高速上云场景示意图



如图3-1所示，本地数据中心通过VPN或者云专线与VPC 1连通，实现：

- 利用终端节点1，通过内网访问云服务（如OBS、DNS等）。
- 利用终端节点2，访问VPC 1的云资源（如ECS 1）。
- 利用终端节点3，跨VPC访问VPC 2的云资源（如ECS 2）。

这种场景具有以下优势：

- 简单快速
  本地数据中心直连终端节点服务，无需经过公网，访问时延小，效率高。
- 成本低廉
  本地数据中心访问云上资源不占用用户的公网资源，降低使用成本。

 版权所有 © 华为技术有限公司

具体示例请参考**配置访问OBS服务内网地址的终端节点**。

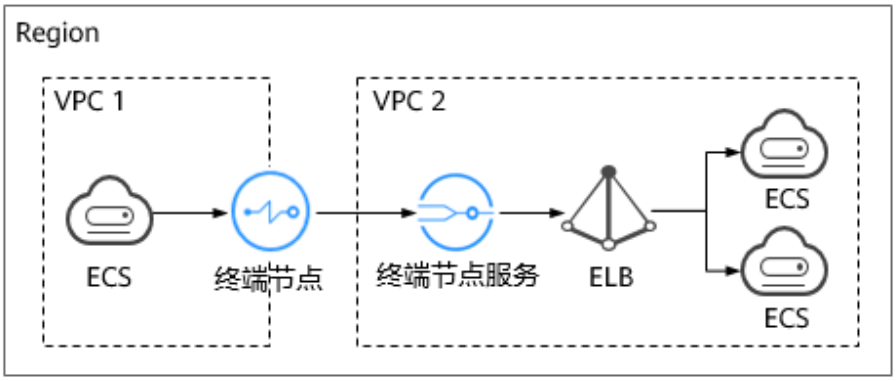
跨 VPC 连接

在同一区域中，由于VPC之间逻辑隔离，不同VPC内的云资源不能直接通信。利用在不同VPC间建立的终端节点到终端节点服务的连接通道，可以实现跨VPC的资源通信。

说明

VPC终端节点的跨VPC通信与VPC的对等连接在安全性、通信方向、路由配置等方面存在差异。详细内容，请参考**VPC终端节点和对等连接有什么区别?** 。

图 3-2 跨 VPC 连接场景示意图



如**图3-2**所示，利用终端节点与终端节点服务建立的跨VPC连接通道，实现VPC 1中的云资源（如ECS）通过内网访问VPC 2中的云资源（如ELB）。

这种场景具有以下优势：

- 性能高效
  每个网关节点可支持百万级会话。
- 简化操作
  资源秒级创建，快速生效，操作简单。

具体示例请参考：

- **配置跨VPC通信的终端节点（同一帐号）**
- **配置跨VPC通信的终端节点（不同帐号）**

版权所有 © 华为技术有限公司

4 约束与限制

资源配额

VPC终端节点资源的配额限制如表4-1所示。

表 4-1 VPCEP 资源配额

资源	默认限制	如何提升配额
一个用户在单个区域中创建终端节点服务的数量	20个	可以提交工单申请提升配额
一个用户在单个区域中购买终端节点的数量	50个	可以提交工单申请提升配额
支持的流量类型	IPv4流量	不可修改
终端节点服务支持的后端资源类型	弹性负载均衡、弹性云服务器、裸金属服务器	
终端节点服务支持的协议	TCP协议	

其他限制

- 购买终端节点时，需要确保连接的终端节点服务已经存在，并位于同一区域。
- 一个终端节点仅支持连接一个终端节点服务。
- 一个终端节点支持最大并发连接数为3000。
- 一个终端节点服务可被多个终端节点连接。
- 一个终端节点服务仅支持对应一个后端资源实例。

 版权所有 © 华为技术有限公司

5 与其他服务的关系

VPC终端节点与其他服务的关系如**表5-1**所示。

表 5-1 与其他服务的关系

交互功能	相关服务	相关内容
用户可以将自己VPC中的服务资源配置为终端节点服务。	虚拟私有云	• **配置跨VPC通信的终端节点（同一帐号）** • **配置跨VPC通信的终端节点（不同帐号）**
本地数据中心可以通过VPN，利用建立的终端节点以内网访问云服务。	虚拟专用网络	**配置访问OBS服务内网地址的终端节点**
本地数据中心可以通过云专线，利用建立的终端节点以内网访问云服务。	云专线	**配置访问OBS服务内网地址的终端节点**
当企业存在多用户访问VPC终端节点服务时，可以使用IAM新建用户，以及控制这些用户帐号对企业名下资源具有的操作权限。	统一身份认证服务	**权限管理**
由系统配置为“网关”型终端节点服务，可以购买终端节点访问该终端节点服务。	对象存储服务	**购买终端节点**
由系统配置为“接口”型终端节点服务，可以购买终端节点访问该终端节点服务。	云解析服务	**购买终端节点**

版权所有 © 华为技术有限公司

交互功能	相关服务	相关内容
由系统配置为“接口”型终端节点服务，可以购买终端节点访问该终端节点服务。	API网关	购买终端节点
支持将用户私有服务创建为终端节点服务，可以购买终端节点访问该终端节点服务。	弹性负载均衡	创建终端节点服务
支持将用户私有服务创建为终端节点服务，可以购买终端节点访问该终端节点服务。	云服务器	创建终端节点服务
支持将用户私有服务创建为终端节点服务，可以购买终端节点访问该终端节点服务。	裸金属服务器	创建终端节点服务

版权所有 © 华为技术有限公司

6 计费说明

计费项

VPC终端节点包含两种资源实例：终端节点服务、终端节点。其中，终端节点服务不收取费用，终端节点会按照购买时长计费。

终端节点支持的计费方式为：按需计费。

表 6-1 VPC 终端节点计费介绍

计费方式	计费项	计费公式
按需计费	终端节点（连接DNS/OBS类型的终端节点服务）	免费
	终端节点（连接除DNS/OBS类型之外的终端节点服务）	购买时长*配置费用 每小时$0.014 USD

VPCEP费用详情请参见**产品价格详情**。

计费模式

按需计费

VPCEP终端节点按照终端节点的购买时长（精确到秒）计费。

计费公式：购买时长*配置费用

例如，用户购买了1个连接API的终端节点，自购买成功到删除资源一共5小时，则会按照配置费用收取5个小时的费用。

说明

VPCEP的按需计费与终端节点是否产生业务交互无关，即使在5个小时中，用户实际没有使用终端节点，也会收取费用。

续费

详细请查看**续费管理**。

版权所有 © 华为技术有限公司

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**。

 版权所有 © 华为技术有限公司

7 安全

7.1 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。

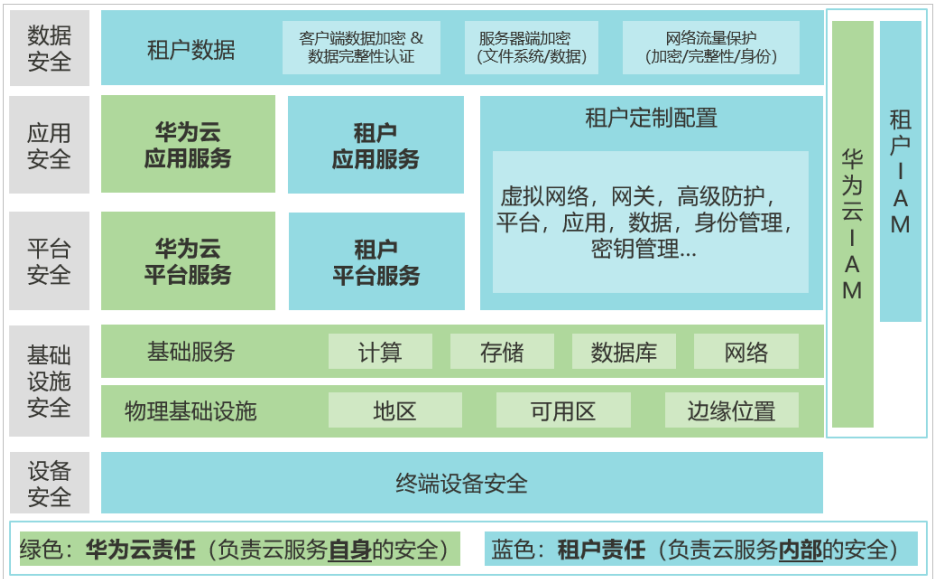
安全性是华为云与您的共同责任，如图7-1所示。

- **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，以及身份帐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。

 版权所有 © 华为技术有限公司

图 7-1 华为云安全责任共担模型



7.2 身份认证与访问控制

IAM 权限管理

VPC终端节点服务支持通过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VPCEP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**。

VPCEP 访问控制

- 终端节点服务的白名单：用于控制是否允许跨帐号的终端节点连接终端节点服务，通过设置终端节点服务的白名单实现，详情参见**管理终端节点服务的白名单**。
- 终端节点的访问控制：支持通过白名单设置允许访问终端节点的IP地址或网段。在购买终端节点时以及购买完成后，均可以开启或关闭终端节点的访问控制功能，也可以添加或删除白名单，详情参见**设置终端节点的访问控制**

7.3 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VPCEP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**。
- VPCEP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**。

版权所有 © 华为技术有限公司

7.4 服务韧性

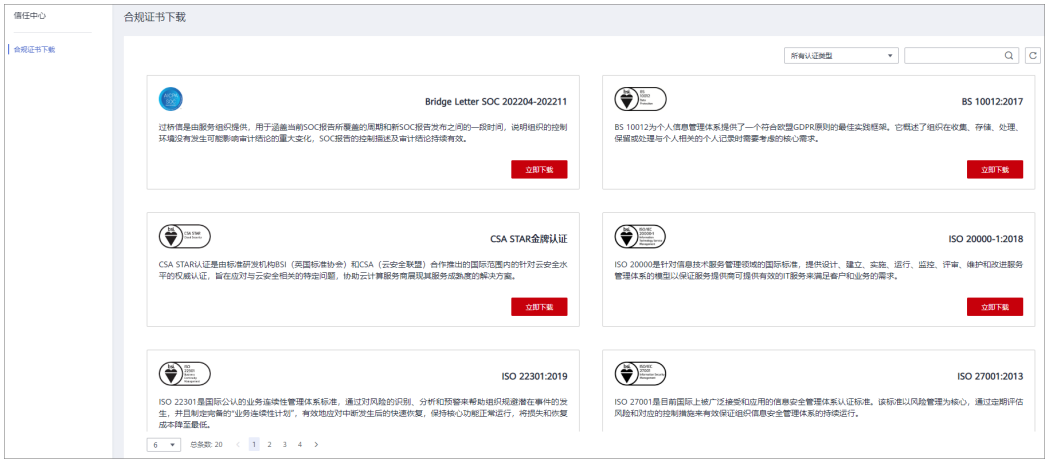
基于华为在全球ICT基础设施领域积累，华为云VPCEP服务累计在全球20+国家/地区部署上百个节点，实现每个Region多AZ多集群容灾，即使部分节点、集群、Region发生故障也不会导致服务中断，极大提高服务可靠性。

7.5 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 7-2 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**。

版权所有 © 华为技术有限公司

图 7-3 资源中心

 版权所有 © 华为技术有限公司

8 权限管理

如果您需要对华为云上购买的云资源，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的访问。

通过IAM，您可以在华为帐号中为员工创建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网站维护的人员，您希望他们拥有VPCEP的操作权限，但是不希望他们拥有删除其他云资源实例等高危操作的权限，那么您可以使用IAM为维护人员创建用户，通过授予仅能操作VPCEP，但是不允许操作其他云资源的权限策略，控制他们对云资源的使用范围。

如果华为帐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VPC终端节点的其它功能。

IAM是华为云提供权限管理的基础服务，无需付费即可使用，您只需要为您帐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**。

VPCEP 权限

默认情况下，帐号管理员创建的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。

VPCEP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（如亚太-曼谷）对应的项目（ap-southeast-2）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VPCEP时，需要先切换至授权区域。

如**表8-1**所示，包括了VPCEP的所有系统角色。

版权所有 © 华为技术有限公司

表 8-1 VPCEP 系统角色

系统角色	描述	类别	依赖关系
VPCEndpoint Administrator	VPC终端节点的所有执行权限。	系统角色	该角色有依赖，需要在同项目中勾选依赖的角色：**Server Administrator**、**VPC Administrator**和**DNS Administrator**。

表8-2列出了VPCEP服务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 8-2 常用操作与系统权限的关系

操作	VPCEndpoint Administrator
创建终端节点	√
删除终端节点	√
查询终端节点	√
修改终端节点	√
创建终端节点服务	√
删除终端节点服务	√
查询终端节点服务	√
修改终端节点服务	√

相关链接

- IAM产品介绍
- 创建用户组、用户并授予VPCEP权限请参考：创建用户并授权使用VPCEP

 版权所有 © 华为技术有限公司

9 基本概念

9.1 终端节点服务

VPC终端节点支持将云服务或者用户私有服务配置为可被终端节点访问的终端节点服务。

终端节点服务包括“网关”和“接口”两种类型。

- 网关：由系统配置的云服务类别的终端节点服务，用户无需创建，可直接使用。
- 接口：包括由系统配置的云服务类别的终端节点服务，以及由用户私有服务创建的终端节点服务。前者用户无需创建，可直接使用；后者需要用户自行创建。

“网关”型终端节点服务

“网关”型是由系统配置的云服务类别的终端节点服务，用户无需创建，可以直接使用，如表9-1所示。

说明

系统在不同区域支持的云服务不同，具体以管理控制台可配置的“服务列表”为准。

仅“拉美-墨西哥城一”、“拉美-圣保罗一”和“拉美-圣地亚哥”区域支持“网关”类型的OBS终端节点服务。

表 9-1 “网关”型终端节点服务

服务名称	服务类别	终端节点服务类型	终端节点服务示例	说明
对象存储服务	云服务	网关	以“拉美-墨西哥城一”为例： com.myhuaweicloud.na-mexico-1.obs	obs：实现通过终端节点访问OBS内网地址。

 版权所有 © 华为技术有限公司

“接口”型终端节点服务

“接口”型终端节点服务包括：

- 由系统配置的云服务类别的终端节点服务，用户无需创建，可以直接使用。
- 由用户私有服务创建的终端节点服务。

说明

系统在不同区域支持的云服务不同，具体以管理控制台可配置的“服务列表”为准。

表 9-2 “接口”型终端节点服务

服务名称	服务类别	终端节点服务类型	终端节点服务示例	说明
云解析服务	云服务	接口	以“中国-香港”为例：com.myhuaweicloud.ap-southeast-1.dns	dns：实现通过终端节点访问内网DNS。
API网关	云服务	接口	以“中国-香港”为例：com.myhuaweicloud.ap-southeast-1.api	api：实现通过终端节点访问API网关。
弹性负载均衡	用户私有服务	接口	无	弹性负载均衡：适用于高访问量业务和对可靠性和容灾性要求较高的业务。
云服务器	用户私有服务	接口	无	ECS：作为服务器使用。
裸金属服务器	用户私有服务	接口	无	BMS：作为服务器使用。

9.2 终端节点

终端节点用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。

在同一区域中，通过购买终端节点可以实现所属VPC内云资源跨VPC访问终端节点服务。

终端节点与终端节点服务一一对应，访问不同类型终端节点服务的终端节点存在差异：

- 访问“接口”型终端节点服务的终端节点：是具备私有IP地址的弹性网络接口，作为接口型终端节点服务的通信入口。
- 访问“网关”型终端节点服务的终端节点：是一个网关，在其上配置路由，用于将流量指向网关型终端节点服务。

版权所有 © 华为技术有限公司

说明

仅“拉美-墨西哥城一”、“拉美-圣保罗一”和“拉美-圣地亚哥”区域支持购买访问“网关”型终端节点服务的终端节点。

9.3 用户权限

系统默认提供两种权限：用户管理权限和资源管理权限。

- 用户管理权限可以管理用户、用户组及用户组的权限。
- 资源管理权限可以控制用户对云服务资源执行的操作。

VPC终端节点的资源包括终端节点服务和终端节点，均属于区域级别的资源，需要在资源所在项目为用户添加权限。

VPC终端节点服务的用户权限请参见**权限策略**。

9.4 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9-1阐明了区域和可用区之间的关系。

图 9-1 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**。

版权所有 © 华为技术有限公司

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**。

9.5 项目和企业项目

项目

IAM中的项目用于将资源（包括计算资源、存储资源和网络资源等）进行分组和隔离。用户拥有的资源必须挂载在项目下，项目可以是一个部门或者项目组。一个帐户中可以创建多个项目。

企业项目

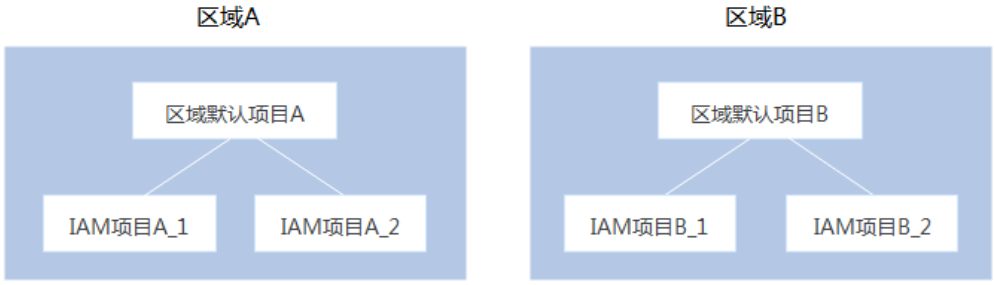
企业管理中的企业项目是对多个资源进行分组和管理，不同区域的资源可以划分到一个企业项目中。企业可以根据不同的部门或项目组，将相关的资源放置在相同的企业项目内进行管理，并支持资源在企业项目之间迁移。

项目和企业项目的区别

- IAM项目

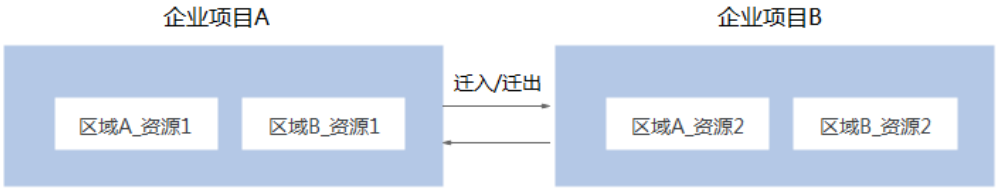
  IAM项目是针对同一个区域内的资源进行分组和隔离，是物理隔离。在IAM项目中的资源不能转移，只能删除后重建。

 版权所有 © 华为技术有限公司



- 企业项目

  企业项目是IAM项目的升级版，是针对企业不同项目间资源的分组和管理。企业项目中可以包含多个区域的资源，且项目中的资源可以迁入迁出。如果您开通了企业管理，将不能创建新的IAM项目（只能管理已有项目）。未来IAM项目将逐渐被企业项目所替代，推荐使用更为灵活的企业项目。



项目和企业项目都可以授权给一个或者多个用户组进行管理，管理企业项目的用户归属于用户组。通过给用户组授予策略，用户组中的用户就能在所属项目/企业项目中获得策略中定义的权限。

关于如何创建项目、企业项目，以及如何授权，请参阅**《企业项目管理用户指南》**。

 版权所有 © 华为技术有限公司