虚拟私有云

产品介绍

文档版本	67
发布日期	2024-03-30

华为云计算技术有限公司

版权所有 © 华为云计算技术有限公司 2024。 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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

1 什么是虚拟私有云 1
2 产品优势 5
3 应用场景 8
4 功能总览 13
5 安全 18
5.1 责任共担 18
5.2 身份认证与访问控制 19
5.3 审计与日志 20
5.4 监控安全风险 20
6 约束与限制 21
7 与其他服务的关系 22
8 计费说明 24
9 权限管理 26
10 基本概念 30
10.1 子网 30
10.2 弹性公网 IP 31
10.3 路由表 31
10.4 安全组 34
10.5 对等连接 35
10.6 网络 ACL 36
10.7 虚拟 IP 36
10.8 弹性网卡 38
10.9 辅助弹性网卡 39
10.10 IP 地址组 40
10.11 区域和可用区 40

1 什么是虚拟私有云

虚拟私有云简介

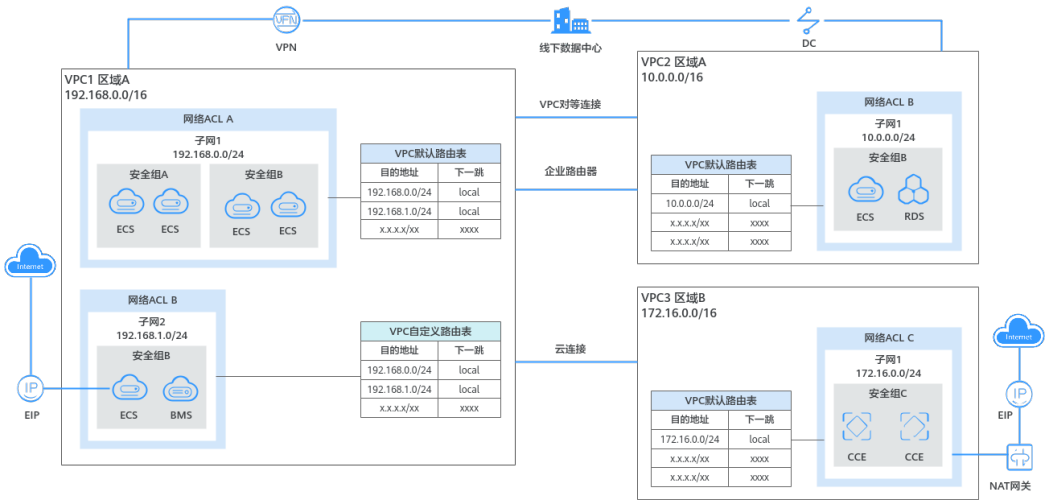
虚拟私有云（Virtual Private Cloud，VPC）是您在云上的私有网络，为云服务器、云容器、云数据库等云上资源构建隔离、私密的虚拟网络环境。VPC丰富的功能帮助您灵活管理云上网络，包括创建子网、设置安全组和网络ACL、管理路由表等。此外，您可以通过弹性公网IP连通云内VPC和公网网络，通过云专线、虚拟专用网络等连通云内VPC和线下数据中心，构建混合云网络，灵活整合资源。

VPC使用网络虚拟化技术，通过链路冗余，分布式网关集群，多AZ部署等多种技术，保障网络的安全、稳定、高可用。

虚拟私有云产品架构

接下来，本文档将从虚拟私有云VPC的基本元素、VPC的网络安全、VPC的网络连接以及VPC的网络运维方面进行介绍，带您详细了解VPC的产品架构。

图 1-1 VPC 产品架构



版权所有 © 华为云计算技术有限公司

表 1-1 VPC 的产品架构介绍

项目分类	简要说明	详细说明
VPC的基本元素	VPC是您在云上的私有网络，您可以指定VPC的IP地址范围，然后通过在VPC内划分子网来进一步细化IP地址范围。同时，您可以配置VPC内的路由表来控制网络流量走向。 不同VPC之间的网络不通，同一个VPC内的多个子网之间网络默认互通。	• IP地址范围：您在创建VPC时，需要指定VPC的IP网段，支持的网段为10.0.0.0/8~24、172.16.0.0/12~24和192.168.0.0/16~24。 • 子网：您可以根据业务需求在VPC内划分子网，VPC内至少需要包含一个子网。实例（云服务器、云容器、云数据库等）必须部署在子网内，实例的私有IP地址从子网网段中分配。 更多信息请参见**子网**。 • 路由表：在创建VPC时，系统会为您自动创建一个默认路由表，默认路由表确保同一个VPC内的子网网络互通。您可以在默认路由表中添加路由来管控网络，如果默认路由表无法满足需求时，您还可以创建自定义路由表。 更多信息请参见**路由表和路由**。
VPC的网络安全	安全组与网络ACL（Access Control List）用于保障VPC内部署实例的安全。	• 安全组：对实例进行防护，您可以在安全组中设置入方向和出方向规则，将实例加入安全组内后，该实例会受到安全组的保护。 更多信息请参见**安全组和安全组规则**。 • 网络ACL：对整个子网进行防护，您可以在网络ACL中设置入方向和出方向规则，将子网关联至网络ACL，则子网内的所有实例都会受到网络ACL保护。 更多信息请参见**网络ACL简介**。 相比安全组，网络ACL的防护范围更大。当安全组和网络ACL同时存在时，流量优先匹配网络ACL规则，然后匹配安全组规则。 更多信息请参见**VPC访问控制简介**。

版权所有 © 华为云计算技术有限公司

项目分类	简要说明	详细说明
VPC的网络连接	您可以使用VPC和云上的其他网络服务，基于您的业务诉求，构建不同功能的组网。 ● 连通同区域VPC：通过VPC对等连接或者企业路由器ER，连通同区域的不同VPC。 ● 连通跨区域VPC：通过云连接CC，连通不同区域的VPC。 ● 连通VPC和公网：通过弹性公网IP (EIP)或者NAT网关，连通云内VPC和公网。 ● 连通VPC和线下数据中心：通过云专线DC或者虚拟专用网络VPN，连通云内VPC和线下数据中心。	● 连通同区域VPC – VPC对等连接：对等连接用于连通同一个区域内的VPC，您可以在相同账户下或者不同账户下的VPC之间创建对等连接。 更多信息请参见**对等连接简介**。 – 企业路由器ER：企业路由器作为一个云上高性能集中路由器，可以同时接入多个VPC，实现同区域VPC互通。 更多信息请参见**什么是企业路由器**。 对等连接免费，企业路由器收费，相比使用VPC对等连接，企业路由器连接VPC构成中心辐射性组网，网络结构更加简洁，方便扩容和运维。 ● 连通跨区域VPC 云连接CC：云连接可以接入不同区域的VPC，快速实现跨区域网络构建。更多信息请参见**什么是云连接**。 ● 连通VPC和公网 – EIP：EIP是独立的公网IP地址，可以为实例绑定EIP，为实例提供访问公网的能力。 更多信息请参见**什么是弹性公网IP**。 – NAT网关：公网NAT网关能够为VPC内的实例（ECS、BMS等），提供最高20Gbit/s能力的网络地址转换服务，实现多个实例使用一个EIP访问公网。 更多信息请参见**什么是NAT网关**。 ● 连通VPC和线下数据中心 – DC：DC用于搭建线下数据中心和云上VPC之间高速、低时延、稳定安全的专属连接通道，通过DC可以构建大规模混合云组网。 更多信息请参见**什么是云专线**。 – VPN：VPN用于在线下数据中心和云上VPC之间建立一条安全加密的公网通信隧道。 更多信息请参见**什么是虚拟专用网络**。 相比通过DC构建混合云，使用VPN更加快速，成本更低。

版权所有 © 华为云计算技术有限公司

项目分类	简要说明	详细说明
VPC的网络运维	VPC流日志和流量镜像可以监控VPC内的流量，用于网络运维。	• 流日志：通过流日志功能可以实时记录VPC中的流量日志信息。通过这些日志信息，您可以优化安全组和网络ACL的控制规则，监控网络流量、进行网络攻击分析等。更多信息请参见**VPC流日志简介**。 • 流量镜像：通过流量镜像功能可以镜像弹性网卡符合筛选条件的报文到目的实例中，在目的实例中进行流量分析，不会影响运行业务的实例，适用于网络流量检查、审计分析以及问题定位等场景。更多信息请参见**流量镜像简介**。

如何访问虚拟私有云

通过管理控制台、基于HTTPS请求的API（Application Programming Interface）两种方式访问虚拟私有云。

- 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“虚拟私有云”。

- API方式

  如果用户需要将云平台上的虚拟私有云集成到第三方系统，用于二次开发，请使用API方式访问虚拟私有云，具体操作请参见**《虚拟私有云API参考》**。

版权所有 © 华为云计算技术有限公司

2 产品优势

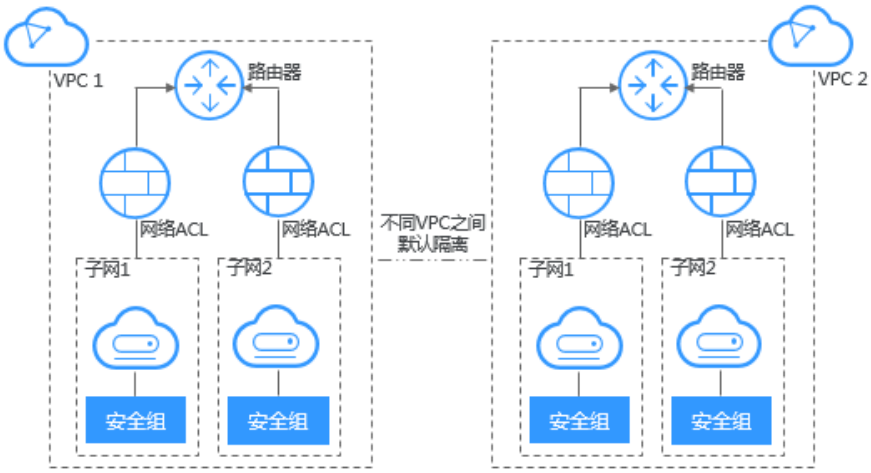
灵活配置

自定义虚拟私有网络，按需划分子网，配置IP地址段、DHCP、路由表等服务。支持跨可用区部署弹性云服务器。

安全可靠

VPC之间通过隧道技术进行100%逻辑隔离，不同VPC之间默认不能通信。网络ACL对子网进行防护，安全组对弹性云服务器进行防护，多重防护您的网络更安全。

图 2-1 安全可靠



互联互通

默认情况下，VPC与公网是不能通信访问的，可以使用弹性公网IP、弹性负载均衡、NAT网关、虚拟专用网络、云专线等多种方式连接公网。

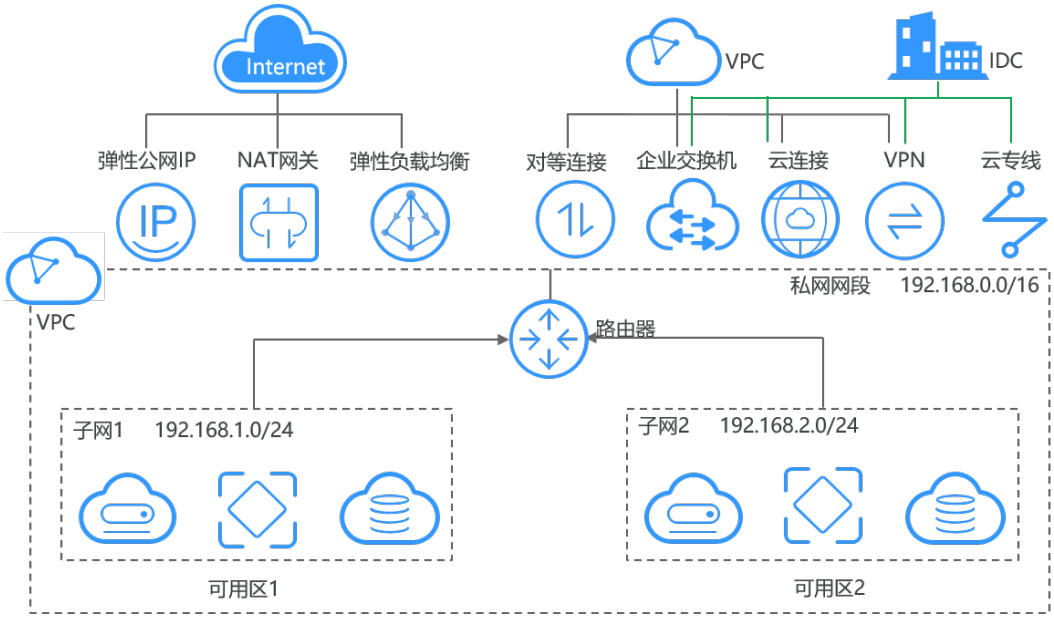
默认情况下，两个VPC之间也是不能通信访问的，可以使用对等连接的方式，使用私有IP地址在两个VPC之间进行通信。

对于云上和云下网络二层互通问题，企业交换机支持二层连接网关功能，允许您在不改变子网、IP规划的前提下将数据中心或私有云主机业务部分迁移上云。

版权所有 © 华为云计算技术有限公司

提供多种连接选择，满足企业云上多业务需求，让您轻松部署企业应用，降低企业IT运维成本。

图 2-2 互联互通



高速访问

使用全动态BGP协议接入多个运营商，可支持20多条线路。可以根据设定的寻路协议实时自动故障切换，保证网络稳定，网络时延低，云上业务访问更流畅。

优势对比

虚拟私有云相比传统IDC的优势如表2-1所示。

表 2-1 虚拟私有云与传统 IDC 对比

对比项	虚拟私有云	传统IDC
部署周期	• 用户无需工程规划，布线等复杂工程部署的工作。 • 用户基于业务需求在华为云上自主规划私有网络、子网和路由。	用户需要自行搭建网络并进行测试，整个周期很长，而且需要专业技术支持。
总成本	华为云网络服务提供了多种灵活的计费方式，加上客户无需前期投入和后期网络运维，整体上降低了TCO。	用户需要机房、供电、施工、硬件物料等固定重资产投入，也需要专业的运维团队来保障网络安全。随着业务变化，资产管理成本也会随之上升。

版权所有 © 华为云计算技术有限公司

对比项	虚拟私有云	传统IDC
灵活性	华为云提供多种网络服务，用户可以根据具体需求搭配服务。当业务发展需要更多的网络资源（如带宽资源）时，可以方便快捷的进行动态扩展。	业务部署需要严格遵守前期网络规划，当业务需求发生变化时，无法便捷的动态调整网络。
安全性	VPC逻辑隔离，结合网络控制网络ACL、安全组功能和DDoS等安全服务，保障了云上资源的安全使用。	网络很难得到专业维护，安全性较差，需要配置专业的网络安全人员来看护。

3 应用场景

云端专属网络

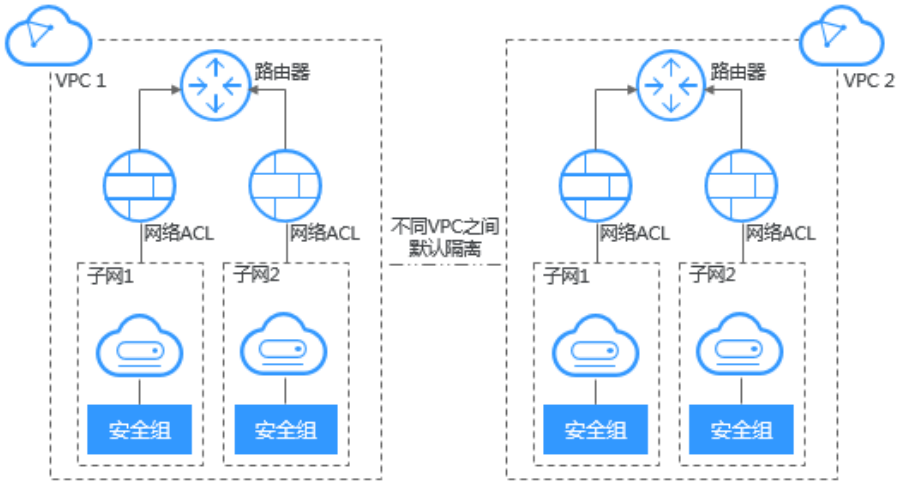
场景描述

每个虚拟私有云VPC代表一个私有网络，与其他VPC逻辑隔离，您可以将业务系统部署在华为云上，构建云上私有网络环境。如果您有多个业务系统例如生产环境和测试环境要严格进行隔离，那么可以使用多个VPC进行业务隔离。当有互相通信的需求时，可以在两个VPC之间建立对等连接。

搭配服务

弹性云服务器ECS

图 3-1 云端专属网络



Web 应用或网站托管

场景描述

在VPC中托管Web应用或网站，可以像使用普通网络一样使用VPC。通过弹性公网IP或NAT网关连接弹性云服务器与Internet，运行弹性云服务器上部署的Web应用程序。同时结合弹性负载均衡ELB服务，您可以将来自Internet的流量均衡分配到不同的弹性云服务器上。

版权所有 © 华为云计算技术有限公司

VPC内的云资源连接公网（Internet），可以通过如下云产品实现。

表 3-1 连接公网

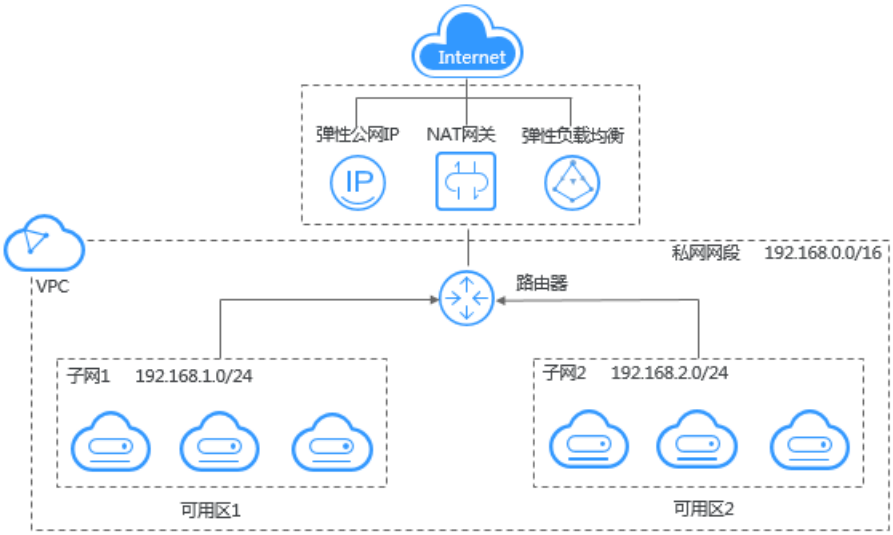
云产品	应用场景	描述	相关操作
弹性公网IP	单个ECS连接公网	申请一个弹性公网IP（EIP）并将其绑定到ECS上，ECS即可连接公网，实现主动访问公网或面向公网提供服务。 支持动态绑定和解绑ECS。 可以使用共享带宽和共享流量包，降低公网成本。	弹性公网IP介绍
NAT网关	多个ECS共享弹性公网IP连接公网	NAT网关提供SNAT和DNAT两种功能：SNAT可实现同一VPC内的多个ECS共享一个或多个EIP主动访问公网，有效降低管理成本，同时减少了ECS的EIP直接暴露的风险。DNAT功能还可以实现端口级别的转发，将EIP的端口映射到不同ECS的端口上，使VPC内多个ECS共享同一EIP和带宽面向公网提供服务，但没有均衡流量的功能。	使用SNAT连接公网 使用DNAT面向公网提供服务
弹性负载均衡	通过将访问流量均衡分发到多个ECS的方式对外提供服务，比如电商等高并发访问场景	弹性负载均衡（ELB）可以将访问流量均衡分发（支持4层和7层两种方式）到多个后端ECS上，通过绑定EIP支撑海量用户从公网访问ECS。 通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。	弹性负载均衡介绍

搭配服务

弹性云服务器ECS、弹性公网IP、NAT网关、弹性负载均衡

版权所有 © 华为云计算技术有限公司

图 3-2 Web 应用或网站托管



Web 应用访问控制

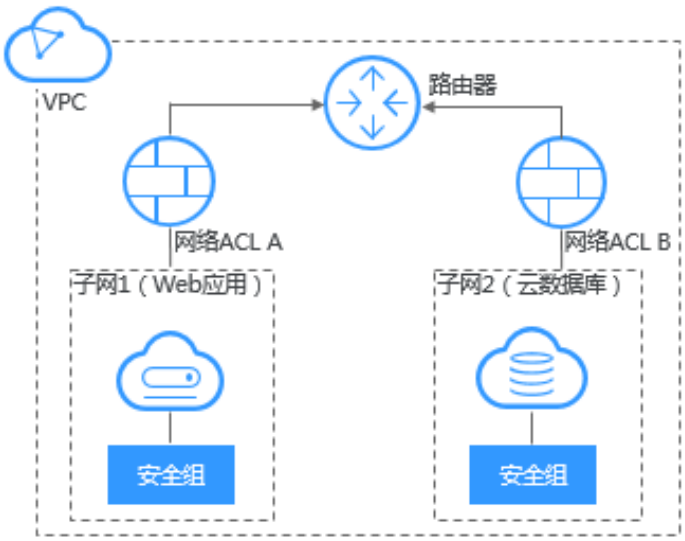
场景描述

将多层Web应用划分到不同的安全域中，按需在各个安全域中设置访问控制策略，可以通过创建一个VPC，将Web服务器和数据库服务器划分到不同的安全组中。Web服务器所在的子网实现互联网访问，而数据库服务器只能通过内网访问，保护数据库服务器的安全，满足高安全场景。

搭配服务

弹性云服务器ECS

图 3-3 Web 应用访问控制



云上 VPC 连接

场景描述

版权所有 © 华为云计算技术有限公司

对于相同或者不同区域下的VPC需要互通连接时，可通过如下云产品实现。

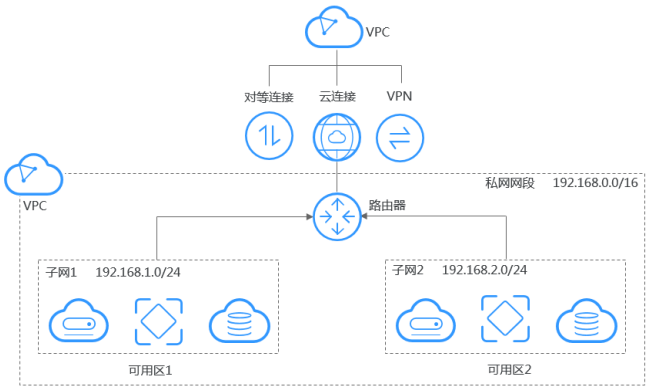
表 3-2 连接 VPC

云产品	应用场景	描述	相关操作
对等连接	同区域的VPC互连	对于同一区域的VPC，可以通过对等连接进行互连，同一账号与不同账号的连接方式略有差异。对等连接免费。	创建同一账户下的对等连接 创建不同账户下的对等连接
云连接	跨区域的VPC互连	对于不同区域的VPC，不区分是否同一账号，都可以互连，跨区域连接实现全球云上网络。	跨区域VPC互连
虚拟专用网络VPN	使用公网低成本连接跨区域VPC	基于Internet使用加密隧道将不同区域的VPC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

搭配服务

弹性云服务器ECS、云连接CC、虚拟专用网络VPN

图 3-4 云上 VPC 连接



混合云部署

场景描述

对于自建本地数据中心（IDC）的用户，由于利旧和平滑演进的原因，并非所有的业务都能放置在云上，这个时候就可以通过如下产品构建混合云，实现云上VPC与云下IDC之间的互连。

版权所有 © 华为云计算技术有限公司

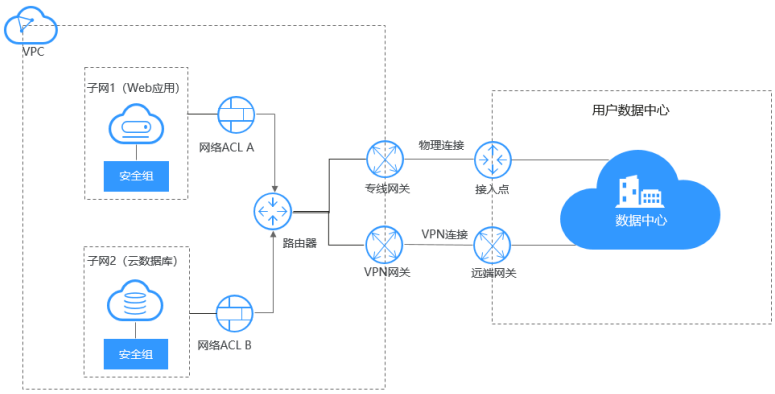
表 3-3 连接 IDC

云产品	应用场景	描述	相关操作
虚拟专用网络VPN	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** **通过企业交换机建立IDC和VPC之间的二层网络**
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** **通过企业交换机建立IDC和VPC之间的二层网络**
云连接	跨区域的VPC、IDC互连	将要互通的本地IDC关联的云专线加载到已创建的云连接实例中，实现跨区域的VPC、IDC互连。	**跨区域VPC互连** **多数据中心与多区域VPC互通**

搭配服务

弹性云服务器ECS、云专线DC、云连接CC、虚拟专用网络VPN

图 3-5 混合云部署



版权所有 © 华为云计算技术有限公司

4 功能总览

表4-1列出了虚拟私有云VPC的常用功能。

在使用虚拟私有云VPC之前，建议您先通过基本概念介绍了解子网、路由表、安全组、弹性公网IP等基本概念，以便更好地理解虚拟私有云VPC提供的功能。

表 4-1 虚拟私有云 VPC 常用功能

功能分类	功能名称	功能描述
虚拟私有云和子网	虚拟私有云	虚拟私有云可以为您的云资源构建隔离的、用户自主配置和管理的虚拟网络环境。 华为云提供了管理虚拟私有云的功能：创建虚拟私有云和默认子网、修改虚拟私有云基本信息、为虚拟私有云添加扩展网段、删除虚拟私有云扩展网段、删除虚拟私有云和导出虚拟私有云列表等。 详细内容，请参见创建虚拟私有云和子网。
	子网	子网是虚拟私有云内的IP地址块。虚拟私有云中的所有云资源都必须部署在子网内。 华为云提供了管理子网的功能：为虚拟私有云创建新的子网、修改子网网络信息和删除子网等。 详细内容，请参见为虚拟私有云创建新的子网。
	路由表	路由表中定义了路由规则，路由规则用于将目标网段的流量路由至指定的目的地。 当您创建虚拟私有云时，系统会自动为您创建一张默认路由表，其路由规则保证了虚拟私有云内的所有子网互通。您也可以添加自定义路由规则，将指定目标网段的流量路由至指定目的地。 华为云提供了管理路由表的功能：添加自定义路由、查询路由、修改路由和删除路由等。 详细内容，请参见路由表简介。

版权所有 © 华为云计算技术有限公司

功能分类	功能名称	功能描述
	虚拟IP	虚拟IP是一个未分配给真实弹性云服务器网卡的IP地址。弹性云服务器除了拥有私有IP地址外，还可以拥有虚拟IP地址，用户可以通过其中任意一个IP（私有IP/虚拟IP）访问此弹性云服务器。同时，虚拟IP地址拥有私有IP地址同样的网络接入能力。虚拟IP主要用在弹性云服务器的主备切换，达到高可用性HA的目的。 华为云提供的虚拟IP相关功能包括：申请虚拟IP地址、删除虚拟IP地址、为虚拟IP地址绑定弹性公网IP或弹性云服务器、通过弹性公网IP访问虚拟IP、通过VPN访问虚拟IP、通过云专线访问虚拟IP和通过对等连接访问虚拟IP等。 详细内容，请参见**虚拟IP简介**。
	IPv4/IPv6双栈网络	IPv4/IPv6双栈可为您的实例提供两个不同版本的IP地址：IPv4地址和IPv6地址，这两个IP地址都可以进行内网/公网访问。 华为云提供IPv4/IPv6双栈功能，支持新建IPv4/IPv6双栈网络，或在已有虚拟私有云下添加IPv6子网形成双栈网络。 详细内容，请参见**IPv4/IPv6双栈网络**。
	VPC流日志	VPC流日志功能可以记录虚拟私有云中的流量信息，帮助您检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。 华为云提供的VPC流日志功能包括：创建VPC流日志、查看VPC流日志、开启/关闭VPC流日志、删除VPC流日志等。 详细内容请参见**VPC流日志简介**。
	弹性网卡	弹性网卡即虚拟网卡，您可以通过创建并配置弹性网卡，并将其附加到您的ECS实例上，实现灵活、高可用的网络方案配置。 华为云提供的弹性网卡功能包括：创建弹性网卡、绑定弹性网卡到云服务器实例、绑定弹性网卡到弹性公网IP、绑定弹性网卡到虚拟IP、解绑定弹性云服务器或弹性公网IP、更改弹性网卡所属安全组、删除弹性网卡等。 详细内容请参见**弹性网卡简介**。

版权所有 © 华为云计算技术有限公司

功能分类	功能名称	功能描述
	辅助弹性网卡	辅助弹性网卡是基于弹性网卡的衍生资源，通过VLAN接口挂载在弹性网卡上，您可以通过创建辅助弹性网卡，使单个云服务器实例挂载更多网卡，实现灵活、高可用的网络方案配置。 华为云提供的辅助弹性网卡功能包括：创建辅助弹性网卡、绑定辅助弹性网卡到弹性公网IP、更改辅助弹性网卡所属安全组、删除辅助弹性网卡等。 详细内容请参见**辅助弹性网卡简介**。
访问控制	安全组	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弹性云服务器提供访问策略。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。 华为云提供了管理安全组和安全组规则的功能：创建安全组、删除安全组、添加安全组规则、快速添加多条安全组规则、复制安全组规则、修改区安全组规则、删除安全组规则、导入/导出安全组规则、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。 详细内容，请参见**安全组简介**。
	网络ACL	网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。 华为云提供了管理网络ACL和网络ACL规则的功能：创建网络ACL、查看网络ACL、修改网络ACL、删除网络ACL、开启/关闭网络ACL、关联/解除子网和网络ACL、添加网络ACL规则、修改网络ACL规则、修改网络ACL规则生效顺序、开启/关闭网络ACL规则、删除网络ACL规则等。 详细内容，请参见**网络ACL简介**。
	IP地址组	IP地址组是多个IP地址的集合，可被安全组规则引用，可统一管理具有相同安全要求或需要频繁修改的IP地址。通过使用IP地址组，可有效应对需要重复多次编辑安全组规则的场景，方便管理。 华为云提供了管理IP地址组的功能：创建IP地址组、关联IP地址组与安全组规则、修改、删除IP地址组等。 详细内容，请参见**IP地址组简介**。

版权所有 © 华为云计算技术有限公司

功能分类	功能名称	功能描述
弹性公网IP和带宽	弹性公网IP	弹性公网IP提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务，可以与云资源灵活绑定及解绑。 华为云提供的弹性公网IP相关功能包括：为云资源申请和绑定弹性公网IP、解绑和释放云资源的弹性公网IP、修改弹性公网IP带宽、静态BGP转换为动态BGP等。 详细内容，请参见**弹性公网IP简介**。
	共享带宽	共享带宽可以实现多个弹性公网IP共同使用一条带宽。提供区域级别的带宽共享及复用能力，同一区域下的所有已绑定弹性公网IP的弹性云服务器、裸金属服务器、弹性负载均衡等实例共用一条带宽资源。 华为云提供的共享带宽相关功能包括：申请共享带宽、修改共享带宽、删除共享带宽、添加弹性公网IP到共享带宽、从共享带宽中移出弹性公网IP等。 详细内容，请参见**共享带宽简介**。
	共享流量包	共享流量包是一款带宽流量套餐产品，使用方便，价格实惠。购买共享流量包后立即生效，并自动抵扣按需计费（按流量计费）的EIP带宽产生的流量资费，直到流量包用完或到期。 详细内容，请参见**共享流量包简介**。
	带宽加油包	带宽加油包用来临时调大带宽上限，适用于在有效期内的包年包月独享带宽和共享带宽。 华为云提供的带宽加油包相关功能包括：购买带宽加油包、修改带宽加油包和退订带宽加油包等。 详细内容，请参见**带宽加油包简介**。
资源互通	VPC对等连接	对等连接是指两个VPC之间的网络连接。您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。同一区域内，您可以在自己的VPC之间创建对等连接，也可以在自己的VPC与其他账户的VPC之间创建对等连接。不同区域间的VPC之间不能创建对等连接。 华为云提供的VPC对等连接相关功能包括：创建同一账户下的对等连接、创建不同账户下的对等连接、查看对等连接、修改对等连接和删除对等连接等。 详细内容，请参见**对等连接简介**。

版权所有 © 华为云计算技术有限公司

功能分类	功能名称	功能描述
监控	查看监控指标	当用户开通了虚拟私有云服务后，无需额外安装其他插件，即可在云监控查看带宽、弹性公网IP的使用情况，也可以创建和设置告警规则，自定义监控目标与通知策略，及时了解虚拟私有云的状况，从而起到预警作用。 详细内容，请参见支持的监控指标。
审计	查看审计日志	华为云审计，您可以记录与虚拟私有云相关的操作事件，便于日后的查询、审计和回溯。 华为云提供查看审计日志功能，支持在云审计服务管理控制台查看或导出最近7天的操作记录。 详细内容，请参见支持审计的关键操作。
标签	标签管理	标签功能方便您识别和管理云资源。华为云支持管理虚拟私有云标签、管理子网标签和管理弹性公网IP标签。
权限	权限管理	您可以使用统一身份认证服务IAM对您所拥有的虚拟私有云进行精细的权限管理，以满足企业基于组织划分、职能划分设置不同的访问权限。 华为云提供的虚拟私有云权限管理功能包括：创建用户并授权使用VPC、创建VPC自定义策略等。 详细内容，请参见权限管理。

版权所有 © 华为云计算技术有限公司

5 安全

5.1 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。

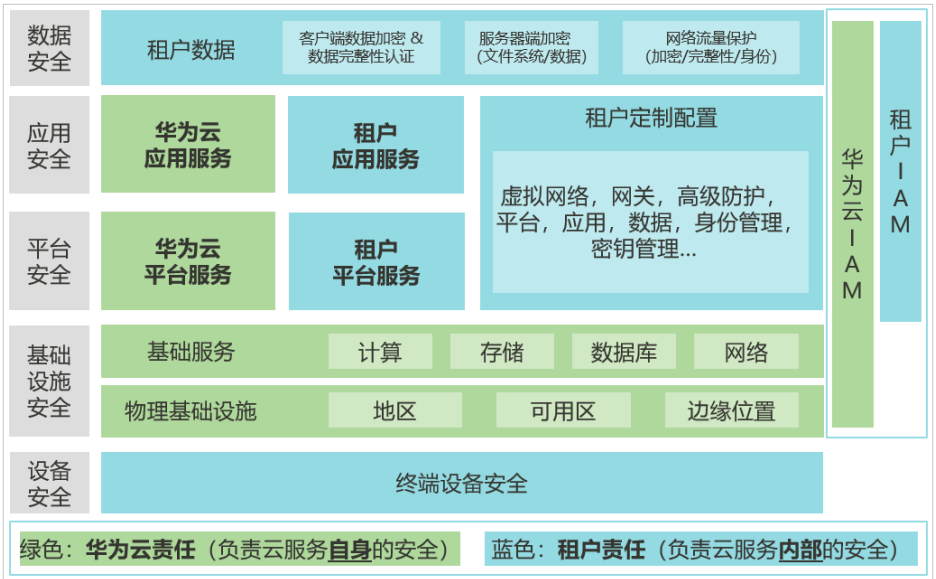
安全性是华为云与您的共同责任，如图5-1所示。

- **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。

版权所有 © 华为云计算技术有限公司

图 5-1 华为云安全责任共担模型



5.2 身份认证与访问控制

身份认证

统一身份认证（Identity and Access Management，简称IAM）是华为云提供权限管理的基础服务，可以帮助用户安全地控制云服务和资源的访问权限。

虚拟私有云支持通过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VPC所需的权限，组内用户自动继承用户组的所有权限。

- IAM的详细介绍，请参见**IAM功能介绍**。
- VPC所需的权限，请参见**权限管理**。

访问控制

- **安全组**

  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。

  华为云提供了管理安全组和安全组规则的功能：创建安全组、删除安全组、添加安全组规则、快速添加多条安全组规则、复制安全组规则、修改区安全组规则、删除安全组规则、导入/导出安全组规则、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**。

- **网络ACL**

版权所有 © 华为云计算技术有限公司

网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的数据流。

华为云提供了管理网络ACL和网络ACL规则的功能：创建网络ACL、查看网络ACL、修改网络ACL、删除网络ACL、开启/关闭网络ACL、关联/解除子网和网络ACL、添加网络ACL规则、修改网络ACL规则、修改网络ACL规则生效顺序、开启/关闭网络ACL规则、删除网络ACL规则等。

用户可以通过与子网关联的出方向/入方向规则控制出入子网的数据流。

详情请参见**网络ACL**。

5.3 审计与日志

审计

云审计服务，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VPC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**。
- VPC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**。

日志

VPC流日志功能可以记录虚拟私有云中的流量信息，帮助用户检查和优化安全组和网络ACL控制规则、监控网络流量、进行网络攻击分析等。

- 流日志的详细介绍，请参见**VPC流日志**。
- 创建VPC流日志，请参见**创建流日志**。

5.4 监控安全风险

云监控服务，为用户提供一个针对弹性云服务器、带宽等资源的立体化监控平台。使用户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。

用户开通云监控后，CES可以查看带宽、弹性公网IP的使用情况，也可以创建和设置告警规则，自定义监控目标与通知策略，及时了解虚拟私有云的状况，从而起到预警作用。

- CES的详细介绍，请参见**CES功能介绍**。
- VPC支持的监控指标，请参见**支持的监控指标**。
- 查看监控指标步骤，请参见**查看监控指标**。

6 约束与限制

虚拟私有云的配额详情如表6-1所示，部分默认配额可以提升，您可以根据提示申请扩大配额。

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。

表 6-1 虚拟私有云的配额说明

资源	如何提升配额
一个用户在单个区域可创建的虚拟私有云数量	如果您需要提升配额，请参见如何申请扩大配额？。
一个用户在单个区域可创建的子网数量	如果您需要提升配额，请参见如何申请扩大配额？。
一个用户在单个区域可创建的安全组数量	如果您需要提升配额，请参见如何申请扩大配额？。
一个用户在单个区域可添加的安全组规则数量	如果您需要提升配额，请参见如何申请扩大配额？。
一个用户在单个区域可创建的网络ACL数量	如果您需要提升配额，请参见如何申请扩大配额？。
一个用户在单个区域可创建的IP地址组数量	如果您需要提升配额，请参见如何申请扩大配额？。
一个用户在单个区域内，单个VPC可关联的路由表数量	如果您需要提升配额，请参见如何申请扩大配额？。
一个用户在单个区域内，单个路由表可添加的路由数量	该项不支持提升配额。
一个用户在单个区域可创建的对等连接数量	该项不支持提升配额。
一个用户在单个区域可创建的VPC流日志数量	该项不支持提升配额。

版权所有 © 华为云计算技术有限公司

7 与其他服务的关系

虚拟私有云VPC服务与其他服务的关系，如图7-1所示。

图 7-1 与其他服务的关系

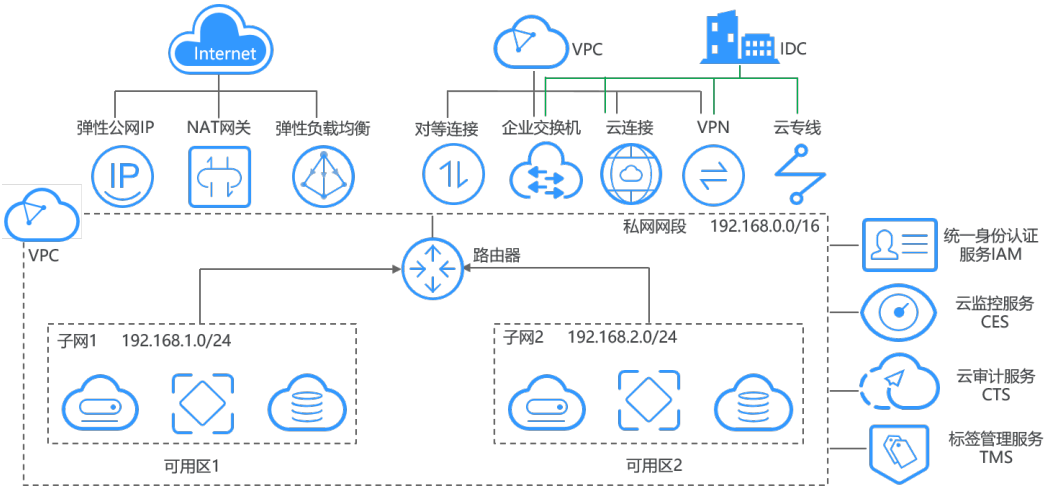


表 7-1 与其他服务的关系

交互功能	相关服务	位置
弹性云服务器的安全防护	弹性云服务器（Elastic Cloud Server，ECS）	添加安全组规则
虚拟私有云内的弹性云服务器与Internet互连	弹性公网IP（Elastic IP，EIP）	使用EIP连接Internet
	NAT网关（NAT Gateway，NAT）	使用SNAT连接Internet
虚拟私有云与本地数据中心互连	虚拟专用网络（Virtual Private Network，VPN）	虚拟专用网络
	云专线（Direct Connect，DC）	云专线
跨区域的虚拟私有云互连	云连接（Cloud Connect，CC）	跨区域VPC互通

版权所有 © 华为云计算技术有限公司

交互功能	相关服务	位置
访问流量分发到VPC内的多台弹性云服务器	弹性负载均衡（Elastic Load Balance，ELB）	弹性负载均衡
如果您需要对华为云上创建的VPC资源，给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。	统一身份认证服务（Identity and Access Management，IAM）	统一身份认证服务
查看带宽和流量使用情况	云监控服务（Cloud Eye Service，CES）	查看监控指标
记录虚拟私有云相关的操作事件，便于日后的查询、审计和回溯	云审计服务（Cloud Trace Service，CTS）	查看审计日志
使用标签标识云资源，实现对虚拟私有云、子网等的分类和搜索。	标签管理服务（Tag Management Service，TMS）	管理虚拟私有云标签

版权所有 © 华为云计算技术有限公司

8 计费说明

虚拟私有云VPC服务下包含了多种产品资源，部分资源可以免费使用，部分资源需要支付费用，表8-1中为您详细介绍了虚拟私有云VPC各项资源的收费情况。

表 8-1 VPC 资源收费一览表

产品资源	收费情况说明
虚拟私有云	免费
子网	免费
路由表	免费
对等连接	免费
弹性网卡	免费
辅助弹性网卡	免费
IP地址组	免费
安全组	免费
网络ACL	免费
VPC流日志	免费
流量镜像	免费

版权所有 © 华为云计算技术有限公司

产品资源	收费情况说明
弹性公网IP和带宽	如果您使用了弹性公网IP和带宽的相关资源，则需要支付费用，费用账单中计费的“产品”项目说明如下： ● 弹性公网IP：收取弹性公网IP保有费。 您购买的按需计费弹性公网IP未绑定至任何实例（如ECS、ELB）时，会收取弹性公网IP保有费。 ● 固定带宽：收取的可能是以下资源的费用。 – 弹性公网IP的带宽费用：包年/包月弹性公网IP的带宽费用、按需计费(按带宽计费)弹性公网IP的带宽费用、按需计费(按流量计费)弹性公网IP的流量费用。 – 共享带宽的费用 – 共享流量包的费用 ● 带宽加油包：收取带宽加油包的费用。 以上计费项目的详细说明，请参见**弹性公网IP计费说明**。
VPC终端节点	如果您使用了VPC终端节点资源，则需要支付费用。 详细计费说明请参见**VPC终端节点计费说明**。

说明

针对免费资源，当前暂不收费。待后续启动收费时，将会提前通知您。

版权所有 © 华为云计算技术有限公司

9 权限管理

如果您需要对华为云上创建的VPC资源，给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，并授权来控制员工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，您希望员工拥有VPC的使用权限，但是不希望员工拥有删除VPC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VPC，但是不允许删除VPC的权限，控制员工对VPC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VPC服务的其他功能。

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**。

VPC 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。

VPC部署时通过物理区域划分。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域（如华东-上海一）对应的项目（cn-east-3）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VPC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VPC服务，管理员能够控制IAM用户仅能对某一类网络资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，虚拟私有云（VPC）支持的API授权项请参见**策略及授权项说明**。

版权所有 © 华为云计算技术有限公司

如表9-1所示，包括了VPC的所有系统权限。

表 9-1 VPC 系统权限

策略名称	描述	策略类别	依赖关系
VPC FullAccess	虚拟私有云的所有执行权限。	系统策略	如果您需要使用VPC流日志功能，则依赖云日志服务的只读权限LTS ReadOnlyAccess。
VPC ReadOnlyAccess	虚拟私有云的只读权限。	系统策略	无
VPC Administrator	虚拟私有云的大部分操作权限，不包括创建、修改、删除、查看安全组以及安全组规则。 拥有该权限的用户必须同时拥有Tenant Guest权限。	系统角色	依赖Tenant Guest策略，在同项目中勾选依赖的策略。

表9-2列出了VPC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	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
创建VPC	x	√	√
修改VPC	x	√	√
删除VPC	x	√	√
查看VPC	√	√	√
创建子网	x	√	√
查看子网	√	√	√
修改子网	x	√	√
删除子网	x	√	√
创建安全组	x	x	√
查看安全组	√	x	√
修改安全组	x	x	√
删除安全组	x	x	√

版权所有 © 华为云计算技术有限公司

操作	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
添加安全组规则	x	x	√
查看安全组规则	√	x	√
修改安全组规则	x	x	√
删除安全组规则	x	x	√
创建网络ACL	x	√	√
查看网络ACL	√	√	√
修改网络ACL	x	√	√
删除网络ACL	x	√	√
添加网络ACL规则	x	√	√
修改网络ACL规则	x	√	√
删除网络ACL规则	x	√	√
创建对等连接	x	√	√
修改对等连接	x	√	√
删除对等连接	x	√	√
查询对等连接	√	√	√
接受对等连接	x	√	√
拒绝对等连接	x	√	√
创建路由表	x	√	√
删除路由表	x	√	√
修改路由表	x	√	√
将路由表关联至子网	x	√	√
添加路由	x	√	√
修改路由	x	√	√
删除路由	x	√	√

版权所有 © 华为云计算技术有限公司

操作	VPCReadOnlyAccess	VPC Administrator	VPC FullAccess
创建VPC流日志	x	√	√
查看VPC流日志	√	√	√
开启/关闭VPC流日志	x	√	√
删除VPC流日志	x	√	√

说明

对于企业项目用户，您可以对属于该企业项目的资源进行权限范围内的操作。

VPC 控制台功能依赖的角色或策略

表 9-3 VPC 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
VPC流日志功能	云日志服务 LTS	IAM用户设置了VPCFullAccess权限后，需要增加LTS ReadOnlyAccess权限，才可以使用流日志功能。

相关链接

- IAM产品介绍
- 创建用户并授权使用VPC
- 策略及授权项说明

版权所有 © 华为云计算技术有限公司

10 基本概念

10.1 子网

子网是虚拟私有云内的IP地址集，可以将虚拟私有云的网段分成若干块，子网划分可以帮助您合理规划IP地址资源。虚拟私有云中的所有云资源都必须部署在子网内。同一个虚拟私有云下，子网网段不可重复。

- 默认情况下，同一个VPC中，不同子网内的所有实例网络互通。同一个VPC内的子网可以位于不同可用区，不影响通信。比如VPC-A内有子网A01（可用区A）和子网A02（可用区B），子网A01和子网A02的网络默认互通。
- 子网创建成功后，不支持修改网段，请提前合理规划好子网网段。同一个虚拟私有云内的子网网段不可重复。

  创建VPC的时候会创建默认子网，VPC创建完成后，如果您需要创建新的子网，请参见为虚拟私有云创建新的子网。

  子网的网段必须在VPC网段范围内，子网网段的掩码长度范围是：所在VPC掩码~29，比如VPC网段为10.0.0.0/16，VPC的掩码为16，则子网的掩码可在16~29范围内选择。

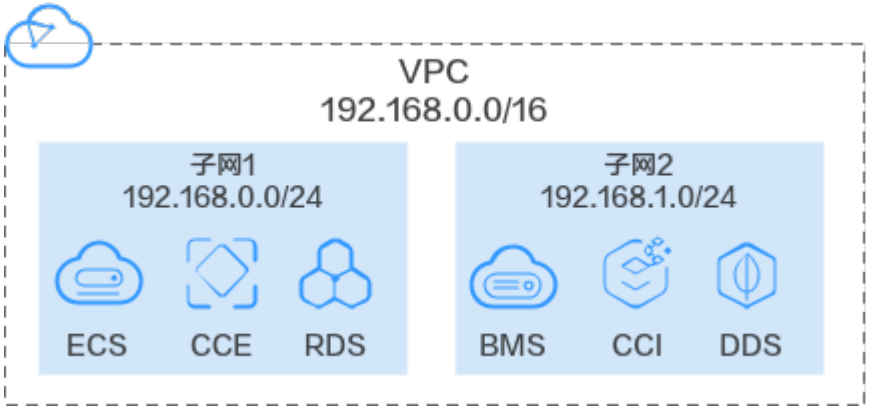
  比如VPC-A的网段为10.0.0.0/16，则您可以规划子网A01的网段为10.0.0.0/24，子网A02的网段为10.0.1.0/24，子网A03的网段为10.0.2.0/24。

  说明

  一个用户在单个区域可创建的虚拟私有云子网数量默认为100个，如果您需要提升配额，请参见如何申请扩大配额?

版权所有 © 华为云计算技术有限公司

图 10-1 子网

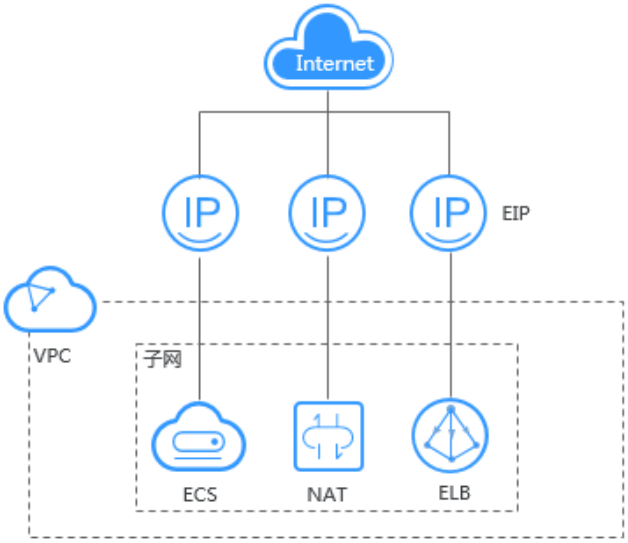


10.2 弹性公网 IP

弹性公网IP（Elastic IP，简称EIP）提供独立的公网IP资源，包括公网IP地址与公网出口带宽服务。可以与弹性云服务器、裸金属服务器、虚拟IP、弹性负载均衡、NAT网关等资源灵活地绑定及解绑。拥有多种灵活的计费方式，可以满足各种业务场景的需要。

一个弹性公网IP只能绑定一个云资源使用。

图 10-2 通过 EIP 访问公网



10.3 路由表

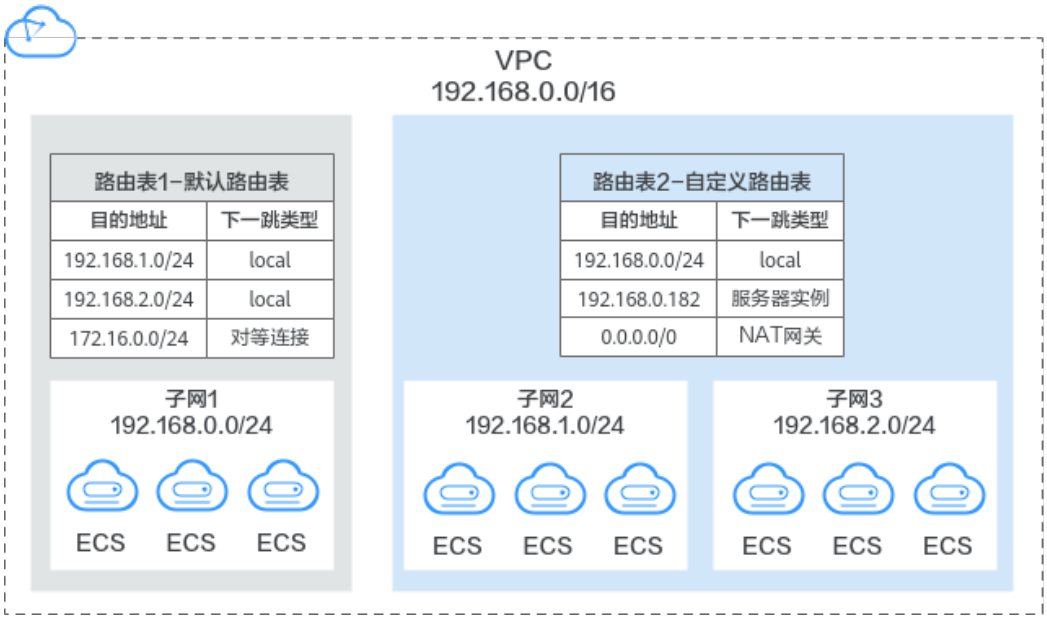
路由表

路由表由一系列路由规则组成，用于控制VPC内子网的出流量走向。VPC中的每个子网都必须关联一个路由表，一个子网只能关联一个路由表，但一个路由表可以同时关联至多个子网。

版权所有 © 华为云计算技术有限公司

路由表支持添加IPv4和IPv6路由。

图 10-3 路由表



- 默认路由表：用户创建VPC时，系统会自动为其生成一个默认路由表，创建子网后，子网会自动关联默认路由表。默认路由表可以确保VPC内子网之间网络互通。
  - 您可以在默认路由表中添加、删除和修改路由规则，但不能删除默认路由表。
  - 创建VPN、云专线、云连接服务时，默认路由表会自动下发路由，该路由不能删除和修改。
- 自定义路由表：您可以直接使用默认路由表，也可以为具有相同路由规则的子网创建一个自定义路由表，并将自定义路由表与子网关联。自定义路由表可以删除。

  子网关联自定义路由表仅影响子网的出流量走向，入流量仍然匹配子网所在VPC的默认路由表。

说明

当前自定义路由表需提交工单申请，如需使用自定义路由表，请在创建路由表页面单击“申请扩大配额”或在页面右上角单击“更多 > 工单 > 新建工单”申请扩大路由表配额。更多提交工单信息请参考提交工单。

路由

您可以在默认路由表和自定义路由表中添加路由，路由包括目的地址、下一跳类型、下一跳地址等信息，来决定网络流量的走向。路由分为系统路由和自定义路由。

- 系统路由：系统自动添加且无法修改或删除的路由。

  创建路由表后，系统会自动在路由表中添加如下的系统路由，表示VPC内实例互通。
  - 目的地址是100.64.0.0/10、198.19.128.0/20的路由。

版权所有 © 华为云计算技术有限公司

– 目的地址是子网网段的路由。

  您在创建子网时，开启IPv6功能，系统将自动为当前子网分配IPv6网段，就可以在路由表中看到IPv6路由。子网网段目的地址示例如下：

  - IPv4地址：192.168.2.0/24。
  - IPv6地址：2407:c080:802:be7::/64。

  说明

  除以上系统路由外，系统还会自动添加目的地址是127.0.0.0/8的路由，表示本地回环地址。

- 自定义路由：可以修改和删除的路由。自定义路由的目的地址不能与系统路由的目的地址重叠。

  您可以通过添加自定义路由来自定义网络流量的走向，您需要指定目的地址、下一跳类型、下一跳地址。支持的下一跳类型如表10-1所示。

  您无法在VPC路由表中添加目的地址相同的两条路由，即使路由的下一跳类型不同也不行。因此不论路由的下一跳是何种类型，路由的优先级均取决于目的地址，遵循最长匹配原则，即优先选择匹配度更高的目的地址进行路由转发。

表 10-1 下一跳类型

下一跳类型	说明	支持添加该类型路由的路由表
服务器实例	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例。	• 默认路由表 • 自定义路由表
扩展网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的扩展网卡。	• 默认路由表 • 自定义路由表
裸金属服务器自定义网络	将指向目的地址的流量转发到一个裸金属服务器自定义网络。	• 自定义路由表
VPN网关	将指向目的地址的流量转发到一个VPN网关。	自定义路由表
云专线网关	将指向目的地址的流量转发到一个云专线网关。	自定义路由表
云连接	将指向目的地址的流量转发到云连接。	自定义路由表
辅助弹性网卡	将指向目的地址的流量转发到虚拟私有云内的一台ECS实例的辅助弹性网卡。	• 默认路由表 • 自定义路由表
NAT网关	将指向目的地址的流量转发到一个NAT网关。	• 默认路由表 • 自定义路由表
对等连接	将指向目的地址的流量转发到一个对等连接。	• 默认路由表 • 自定义路由表

下一跳类型	说明	支持添加该类型路由的路由表
虚拟IP	将指向目的地址的流量转发到一个虚拟IP地址，可以通过该虚拟IP地址将流量转发到主备ECS。	• 默认路由表 • 自定义路由表
VPC终端节点	将指向目的地址的流量转发到一个VPC终端节点。	• 默认路由表 • 自定义路由表
云容器引擎	将指向目的地址的流量转发到一个云容器引擎的节点。	• 默认路由表 • 自定义路由表
企业路由器	将指向目的地址的流量转发到一个企业路由器。	• 默认路由表 • 自定义路由表
云防火墙	将指向目的地址的流量转发到一个云防火墙。	• 默认路由表 • 自定义路由表
互联网网关	将指向目的地址的流量转发到一个互联网网关。	• 默认路由表 • 自定义路由表

说明

个别由系统下发的路由可供用户修改和删除，这取决于创建对端服务时是否已设置目的地址。

例如，创建NAT网关时，系统会自动下发一条自定义类型的路由，没有明确指定目的地址（默认为0.0.0.0/0）,此时用户可修改该目的地址。而创建VPN网关时，可以指定远端子网，也就是路由表的目的地址，系统将下发系统类型的路由。如果在路由表页面更改路由将会导致与对端数据不一致，您可以前往对端服务页面修改远端子网来调整路由表中的路由规则。

10.4 安全组

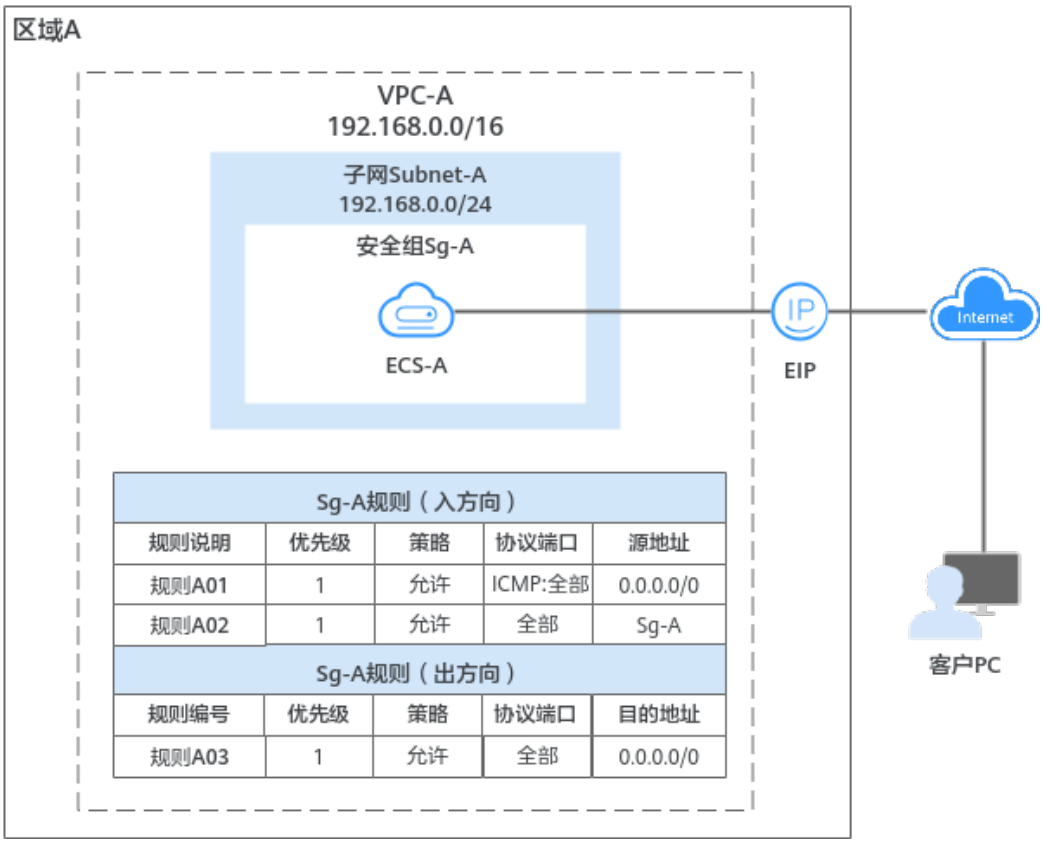
安全组是一个逻辑上的分组，为具有相同安全保护需求并相互信任的云服务器、云容器、云数据库等实例提供访问策略。安全组创建后，用户可以在安全组中定义各种访问规则，当实例加入该安全组后，即受到这些访问规则的保护。

安全组中包括入方向规则和出方向规则，您可以针对每条入方向规则指定来源、端口和协议，针对出方向规则指定目的地、端口和协议，用来控制安全组内实例入方向和出方向的网络流量。以**图10-4**为例，在区域A内，某客户有一个虚拟私有云VPC-A和子网Subnet-A，在子网Subnet-A中创建一个云服务器ECS-A，并为ECS-A关联一个安全组Sg-A来保护ECS-A的网络安全。

- 安全组Sg-A的入方向存在一条放通ICMP端口的自定义规则，因此可以通过个人PC(计算机)**ping**通ECS-A。但是安全组内未包含允许SSH流量进入实例的规则，因此您无法通过个人PC远程登录ECS-A。
- 当ECS-A需要通过EIP访问公网时，由于安全组Sg-A的出方向规则允许所有流量从实例流出，因此ECS-A可以访问公网。

版权所有 © 华为云计算技术有限公司

图 10-4 安全组架构图



10.5 对等连接

对等连接是建立在两个VPC之间的网络连接，不同VPC之间网络不通，通过对等连接可以实现不同VPC之间的云上内网通信。对等连接用于连通同一个区域内的VPC，您可以在相同账户下或者不同账户下的VPC之间创建对等连接。

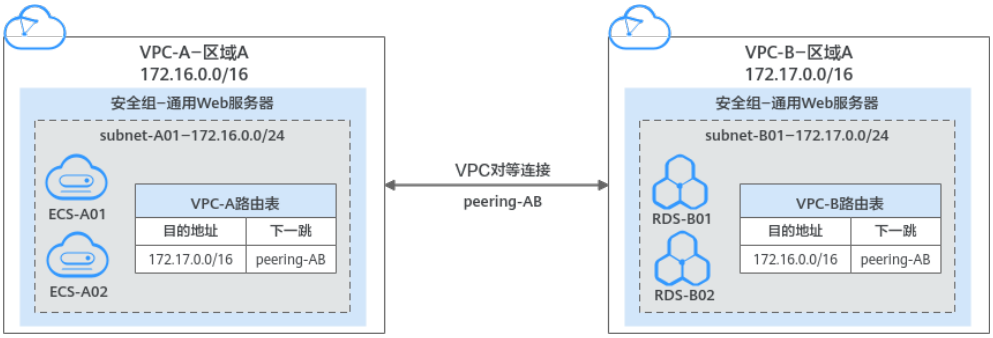
- 对等连接用于连通同一个区域的VPC，如果您要连通不同区域的VPC，请使用云连接。
- 您可以通过对等连接构建不同的组网，常见的使用示例请参见对等连接使用示例。

接下来，通过图10-5中简单的组网示例，为您介绍对等连接的使用场景。

- 在区域A内，您的两个VPC分别为VPC-A和VPC-B，VPC-A和VPC-B之间网络不通。
- 您的业务服务器ECS-A01和ECS-A02位于VPC-A内，数据库服务器RDS-B01和RDS-B02位于VPC-B内，此时业务服务器和数据库服务器网络不通。
- 您需要在VPC-A和VPC-B之间建立对等连接Peering-AB，连通VPC-A和VPC-B之间的网络，业务服务器就可以访问数据库服务器。

版权所有 © 华为云计算技术有限公司

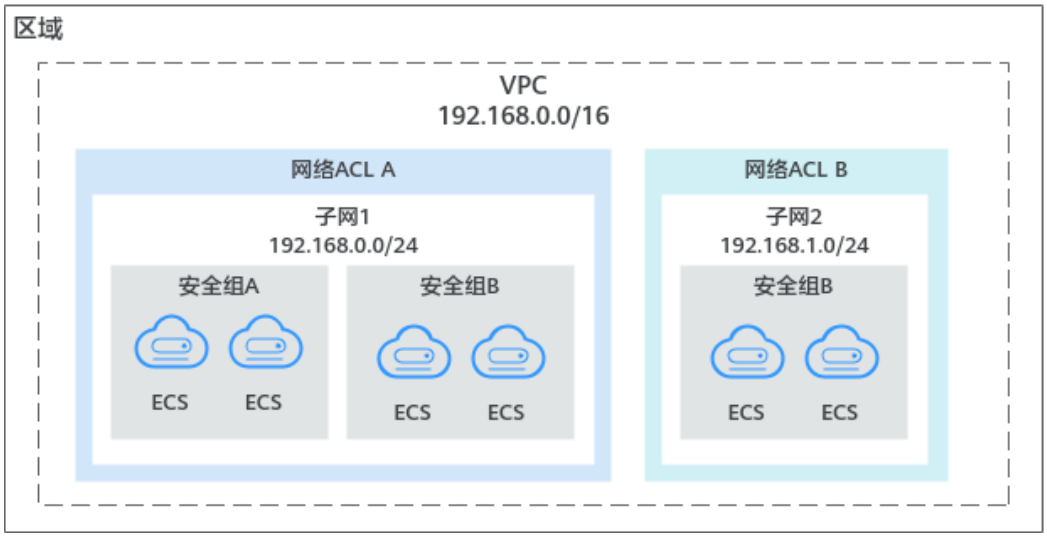
图 10-5 对等连接组网示意图



10.6 网络 ACL

网络ACL是一个子网级别的可选安全层，通过与子网关联的出方向/入方向规则控制出入子网的网络流量。

图 10-6 安全组与网络 ACL



网络ACL与安全组类似，都是安全防护策略，当您想增加额外的安全防护层时，就可以启用网络ACL。安全组对云服务器、云容器、云数据库等实例进行防护，网络ACL对子网进行防护，两者结合起来，可以实现更精细、更复杂的安全访问控制。

10.7 虚拟 IP

虚拟IP（Virtual IP Address，简称VIP）是一个未分配给真实弹性云服务器网卡的IP地址。弹性云服务器除了拥有私有IP地址外，还可以拥有虚拟IP地址，用户可以通过其中任意一个IP（私有IP/虚拟IP）访问此弹性云服务器。

同时，虚拟IP地址拥有私有IP地址同样的网络接入能力，包括VPC内二三层通信、VPC之间对等连接访问，以及弹性公网IP、VPN、云专线等网络接入。

您可以为多个主备部署的弹性云服务器绑定同一个虚拟IP地址，然后为虚拟IP绑定一个弹性公网IP，搭配Keepalived，实现主服务器故障后，自动切换至备服务器，打造高可用容灾组网。

版权所有 © 华为云计算技术有限公司

须知

通过虚拟IP和弹性云服务器构建高可用容灾组网，必须要搭配Keepalived相关配置才可以实现，具体可参考**搭建Keepalived Nginx高可用Web集群**。

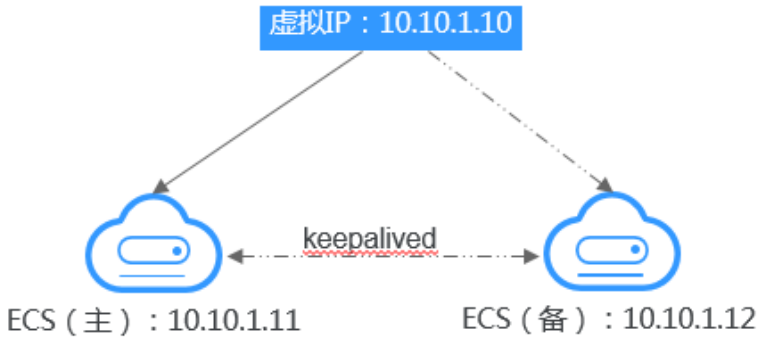
典型组网

虚拟IP主要用在弹性云服务器的主备切换，搭配Keepalived，达到高可用性HA（High Availability）的目的。当主服务器发生故障无法对外提供服务时，动态将虚拟IP切换到备服务器，继续对外提供服务。本节介绍两种典型的组网模式。

- **典型组网1：**HA高可用性模式

  场景举例：如果您想要提高服务的高可用性，避免单点故障，可以用“一主一备”或“一主多备”的方法组合使用弹性云服务器，这些弹性云服务器对外表现为一个虚拟IP。当主服务器故障时，备服务器可以转为主服务器，继续对外提供服务。

  图 10-7 HA 高可用性模式组网图

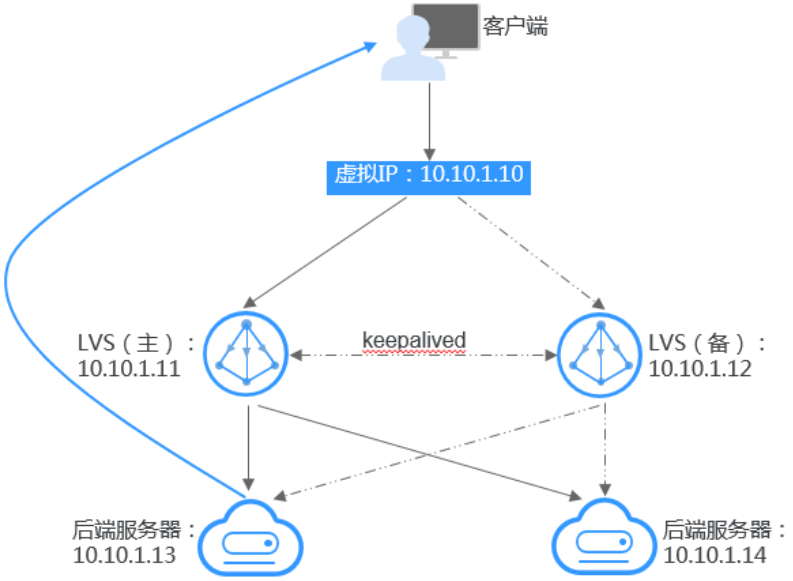
  - 将2台同子网的弹性云服务器绑定同一个虚拟IP。
  - 将这2台弹性云服务器配置Keepalived，实现一台为主服务器，一台为备份服务器。Keepalived可参考业内通用的配置方法，此处不做详细介绍。

- **典型组网2：**高可用负载均衡集群

  场景举例：如果您想搭建高可用负载均衡集群服务，您可以采用Keepalived + LVS(DR)来实现。

版权所有 © 华为云计算技术有限公司

图 10-8 高可用负载均衡集群



- 将2台弹性云服务器绑定同一个虚拟IP。
- 将绑定了虚拟IP的这2台弹性云服务器配置Keepalived+LVS（DR模式），组成LVS主备服务器。这2台服务器作为分发器将请求均衡地转发到不同的后端服务器上执行。
- 配置另外2台弹性云服务器作为后端RealServer服务器。
- 关闭2台后端RealServer弹性云服务器的源/目的检查。

Keepalived + LVS调度服务端安装配置以及后端RealServer服务器配置可以参考业内通用的配置方法，此处不做详细介绍。

应用场景

- 场景一：通过弹性公网IP访问虚拟IP。

  您的应用需要具备高可用性并通过Internet对外提供服务，推荐使用弹性公网IP绑定虚拟IP功能。

- 场景二：通过VPN/云专线/对等连接访问虚拟IP。

  您的应用需要具备高可用性并且需要通过Internet访问，同时需要具备安全性（VPN），保证稳定的网络性能（云专线），或者需要通过其他VPC访问（对等连接）。

10.8 弹性网卡

弹性网卡（Elastic Network Interfaces，以下简称ENI）即虚拟网卡，您可以通过创建并配置弹性网卡，并将其附加到您的云服务器实例（包括弹性云服务器和裸金属服务器）上，实现灵活、高可用的网络方案配置。

弹性网卡类型

- 主弹性网卡：在创建实例时，随实例默认创建的弹性网卡称作主弹性网卡。无法解除主弹性网卡和实例的绑定关系。

版权所有 © 华为云计算技术有限公司

- 扩展弹性网卡：您在弹性网卡控制台创建的是扩展弹性网卡，可以将网卡绑定到实例上，也可以解除网卡和实例的绑定关系。

应用场景

- 灵活迁移

  通过将弹性网卡从云服务器实例解绑后再绑定到另外一台服务器实例，保留已绑定私网IP、弹性公网IP和安全组策略，无需重新配置关联关系，将故障实例上的业务流量快速迁移到备用实例，实现服务快速恢复。

- 业务分离管理

  可以为服务器实例配置多个分属于同一VPC内不同子网的弹性网卡，特定网卡分别承载云服务器实例的内网、外网、管理网流量。针对子网可独立设置访问安全控制策略与路由策略，弹性网卡也可配置独立安全组策略，从而实现网络隔离与业务流量分离。

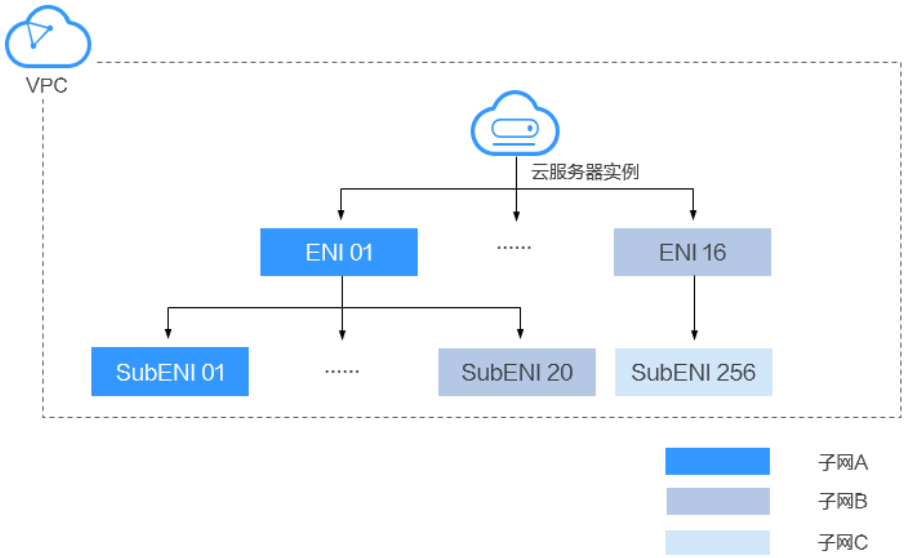
10.9 辅助弹性网卡

辅助弹性网卡是一种基于弹性网卡的衍生资源，用于解决单个云服务器实例挂载的弹性网卡超出上限，不满足用户使用需要的问题。辅助弹性网卡通过VLAN子接口挂载在弹性网卡上，您可以通过创建辅助弹性网卡，使单个云服务器实例挂载更多网卡，实现灵活、高可用的网络方案配置。

应用场景

辅助弹性网卡通过VLAN子接口挂载在弹性网卡上，其组网示意图如图10-9所示。

图 10-9 辅助弹性网卡示意图



单个云服务器实例支持绑定的弹性网卡数量有限，当因业务需要绑定超过弹性网卡上限的网卡时，可以通过为弹性网卡挂载辅助弹性网卡实现。

- 为云服务器实例配置多个分属于同一VPC内不同子网的辅助弹性网卡，每个辅助弹性网卡拥有不同的私网IP、弹性公网IP，可以分别承载云服务器实例的内网、外网和管理网流量。

版权所有 © 华为云计算技术有限公司

- 辅助弹性网卡可配置独立安全组策略，从而实现网络隔离与业务流量分离。

10.10 IP 地址组

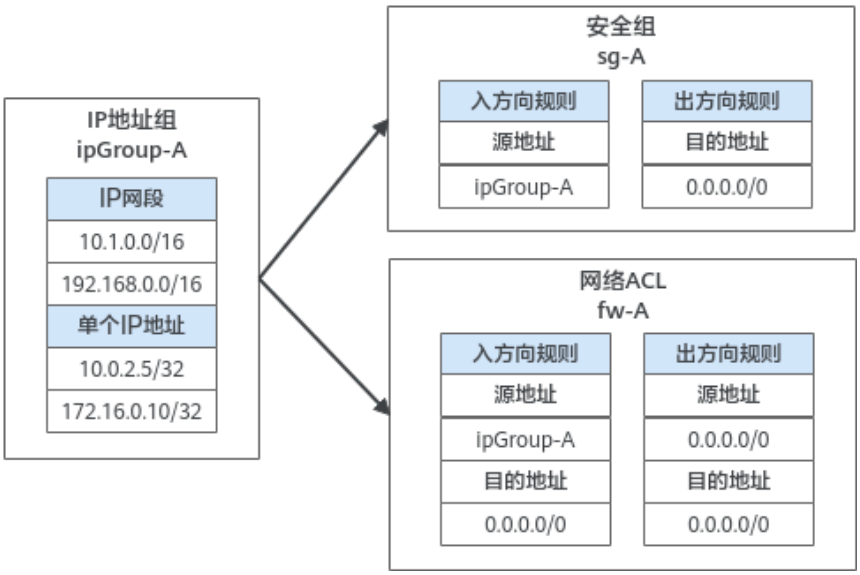
IP地址组是一个或者多个IP地址的集合，可关联至安全组、网络ACL，用于简化网络架构中IP地址的配置和管理。

对于需要统一管理的IP网段、单个IP地址，您可以将其添加到一个IP地址组内。IP地址组无法独立使用，需要将IP地址组关联至对应的资源，可关联IP地址组的资源说明如表10-2所示。

表 10-2 IP 地址组关联资源说明

资源	说明	示例
安全组	添加安全组规则的时候，源地址和目的地址可以选择IP地址组。	如图10-10所示，安全组sg-A的的入方向规则的源地址使用IP地址组ipGroup-A。
网络ACL	添加网络ACL规则的时候，源地址和目的地址可以选择IP地址组。	如图10-10所示，网络ACLfw-A的的入方向规则的源地址使用IP地址组ipGroup-A。

图 10-10 IP 地址组使用场景



10.11 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

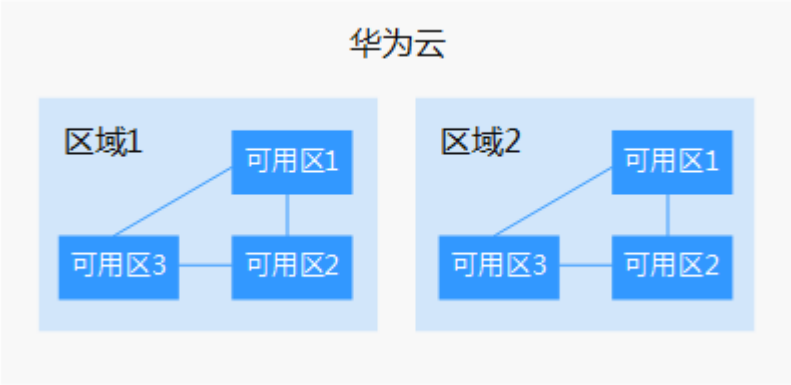
版权所有 © 华为云计算技术有限公司

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10-11阐明了区域和可用区之间的关系。

图 10-11 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**。

版权所有 © 华为云计算技术有限公司