云原生应用网络

产品介绍

文档版本 01

发布日期 2025-09-02

华为云计算技术有限公司

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 什么是云原生应用网络.....1
2 产品优势.....5
3 应用场景.....6
4 原理介绍.....10
5 安全.....14
5.1 责任共担.....14
5.2 审计与日志.....15
5.3 监控安全风险.....16
5.4 认证证书.....16
6 约束与限制.....18
7 与其他服务的关系.....20
8 区域和可用区.....22

1 什么是云原生应用网络

什么是云原生应用网络

云原生应用网络（Application Native Cloud，ANC）是一种面向应用的全域互联服务，用于连接、保护和监控应用程序的服务。您可以将ANC与单个虚拟私有云（Virtual Private Cloud，VPC）关联，也可以与多个跨账号或跨区域的VPC关联。当您将ANC与VPC关联后，VPC中的任何客户端只要拥有所需的访问权限，即可连接到与ANC关联的服务端。

服务端是与ANC关联的一个或多个服务，服务是一种可独立部署并且可跨区域的软件单元，用于实现特定任务或功能，包含路由规则、成员组等组件。使用ANC会极大的简化网络复杂度，只需要创建一个ANC，创建好服务，并将服务和VPC关联到ANC，即可以实现VPC与服务的跨区域、跨账号通信。

须知

云原生应用网络功能目前处于邀测状态，如果您需要使用该功能，请提交工单申请开通。

产品架构

云原生应用网络

一个连通任意VPC和服务的逻辑网络，可以关联多个跨区域、跨账号的服务和VPC。当服务路由规则允许，VPC客户端可以直接访问该服务。客户端是部署在VPC中并与ANC关联的任何资源。如果获得授权，与同一ANC关联的客户端和服务可以相互通信。

虚拟私有云

与ANC关联的VPC，作为客户端可以访问关联ANC的服务。

服务

一种可独立部署的软件单元，包含路由规则、成员组等组件。用户可以通过ANC，根据定义的路由规则，访问服务中的资源（成员）。

成员组

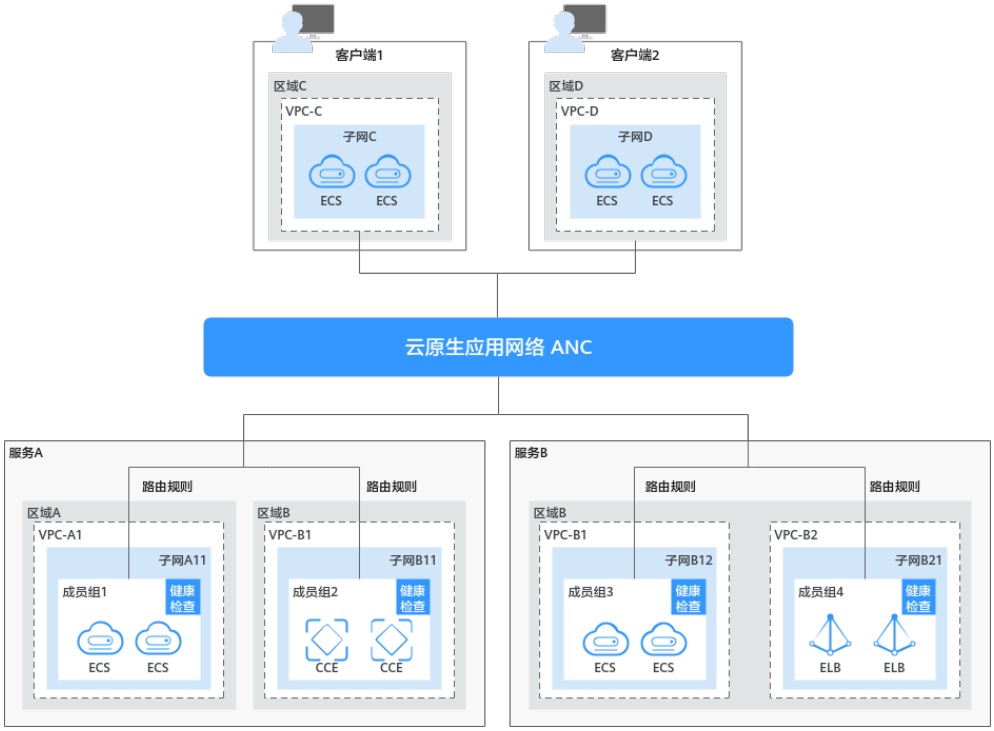
运行应用程序或服务的资源集合。运行应用程序或服务的资源也称为成员，成员可以是云服务器实例、辅助弹性网卡或弹性负载均衡实例等。

路由规则

服务默认组件，用于将请求转发至成员组中的一个成员。每条规则由优先级和权重组成。

在图1-1中，客户端可以与两个服务通信，因为客户端VPC和服务与同一个云原生应用网络关联。

图 1-1 ANC 产品架构图



使用 ANC 构建网络

图1-2和图1-3分别展示了不使用和使用ANC构建的网络拓扑，详细的对比说明如表1-1所示。

图 1-2 未使用 ANC 构建网络

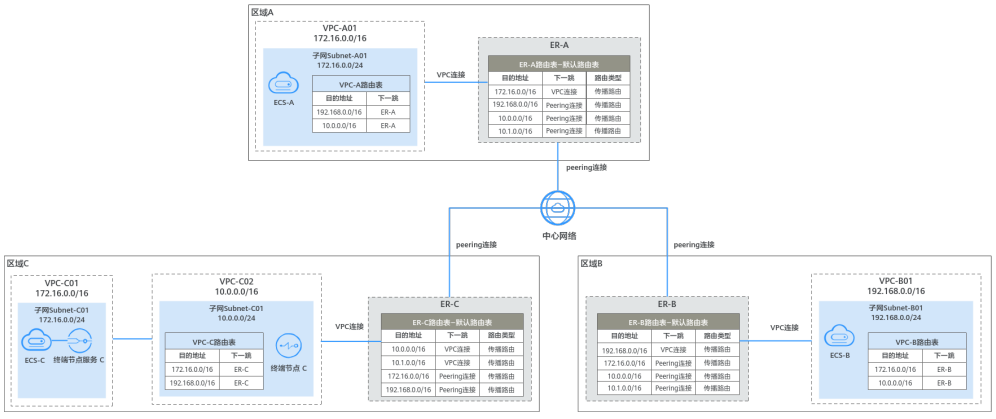


图 1-3 使用 ANC 构建网络

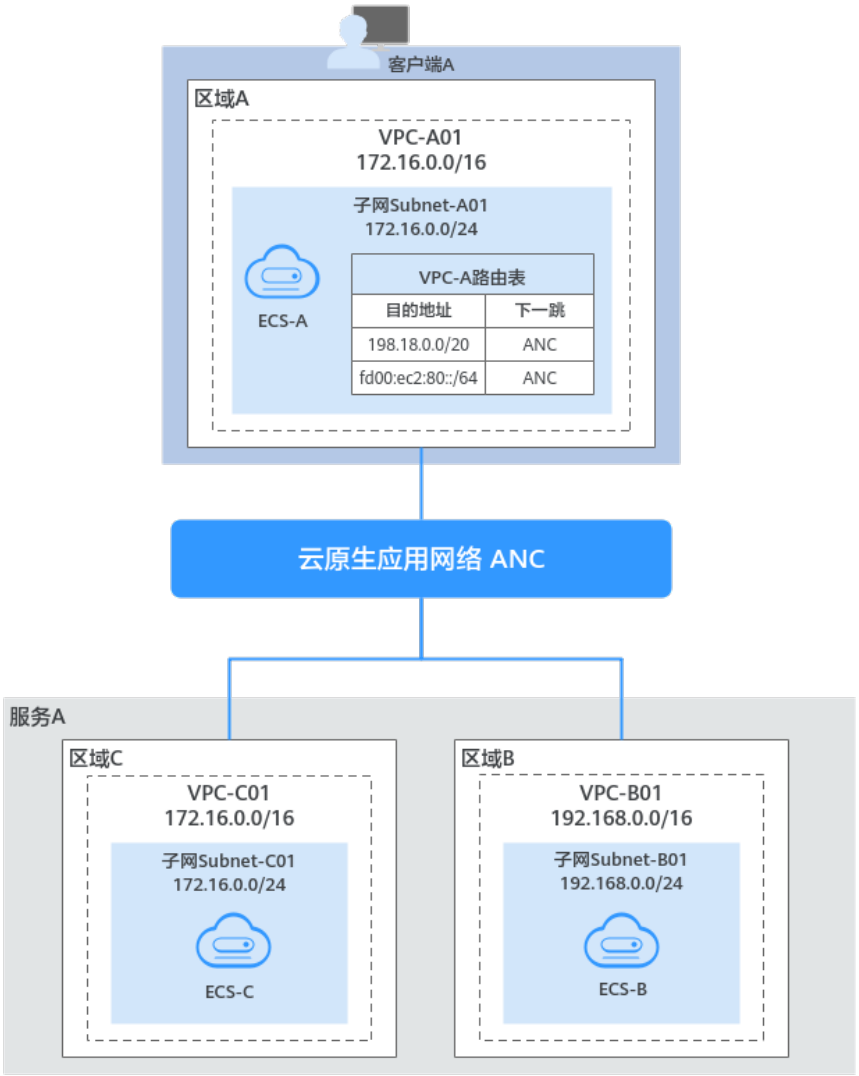


表 1-1 网络拓扑对比说明

对比项	不使用ANC	使用ANC	ANC价值
客户端VPC与目的端地址冲突	采用VPC终端节点，将VPC-C01中待访问的后端资源ECS-C创建为终端节点服务，并在VPC-C02中购买终端节点。 实现客户端VPC-A01通过访问VPC-C02终端节点，访问终端节点服务VPC-C01中ECS-C。	• 将VPC-A01客户端关联至ANC。 • 将目的端的资源ECS-C加入服务中，将服务关联至ANC。 即可实现VPC-A01客户端跨区域直接访问服务中的资源ECS-C。	无需规划地址和路由，地址冲突自动转换。

对比项	不使用ANC	使用ANC	ANC价值
访问多个跨区域的资源	所有区域需要互通的VPC均需配置企业路由器ER，并且接入云连接CC中。	• 将VPC-A01客户端关联至ANC。 • 将目的端的资源ECS-B和ECS-C加入服务中，将服务关联至ANC。 即可实现VPC-A01客户端跨区域访问服务中的资源ECS-B和ECS-C。	• 无需在云连接中接入所有网络实例，简化网络拓扑。 • 支持ANC跨账号、跨区域和跨VPC无感互联，免去繁复配置，降低维护难度。

通过对比，可以看出，使用ANC构建的网络拓扑更简洁，可扩展性高，同时网络维护工作也更简单。

2 产品优势

云原生应用网络是一种面向应用的全域互联服务，本章节为您介绍云原生应用网络的优势。

低时延

应用跨区域部署，自动优化体验，部署运行在成本最佳的区域，支持用户就近访问。

高可靠

云原生应用网络（ANC）支持多区域搭建服务，根据访问的目的地址所在区域，优先访问与客户端区域较近的目的端业务应用。打造区域双活或多活服务，故障快速切换，保障业务连续性。

- 区域生命周期终结(机房退租)，业务无感迁移到其他区域。
- 区域故障，流量自动切换到其他区域。

高弹性

业务突发，应用多区域算力弹性伸缩，承载较大业务量。

IPv4/IPv6 双栈

支持IPv4和IPv6应用跨协议互访，支持IPv4应用平滑演进IPv6。

极简网络配置

ANC可以连通任意VPC和服务之间网络，多账号、多区域无感互联，无需规划地址和路由，且无需关心源地址和目的地址是否冲突。

3 应用场景

本节介绍云原生应用网络（ANC）的主要应用场景。

- **场景一：跨区域极简网络配置访问**
- **场景二：VPC客户端和访问的目的地址冲突**
- **场景三：全域服务跨域容灾**

场景一：跨区域极简网络配置访问

跨区域网络配置访问，用于在多个全球跨区域互联的VPC内，您需要部署网络访问多个跨区域 VPC实例的场景。

传统VPC网络，业务部署之前需要综合整个云上业务，统一规划网络，设计VPC与业务的映射关系，统一规划IP地址，设计网络ACL和安全组，然后发放资源部署业务。网络配置复杂且易出错。

规划的云原生应用网络，应用使用统一的网络部署业务，基于ANC实现网络互通和隔离，无需再统一规划VPC。连接无需感知任何网络信息，应用跨账号、跨区域、跨VPC无感互联。应用灵活编排，网络配置简单，操作便捷。

图 3-1 传统 VPC 网络与 ANC 网络配置区别

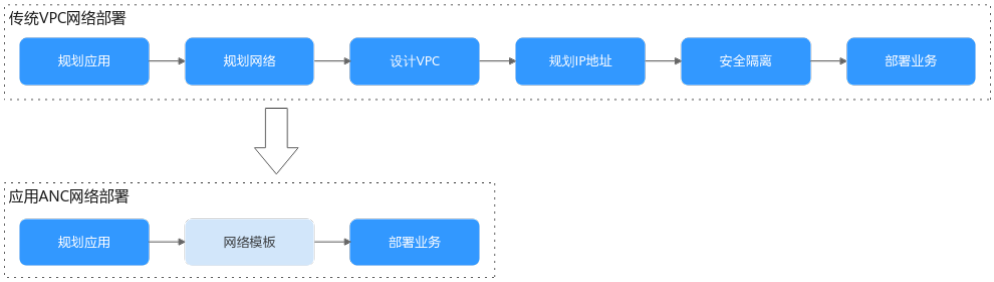
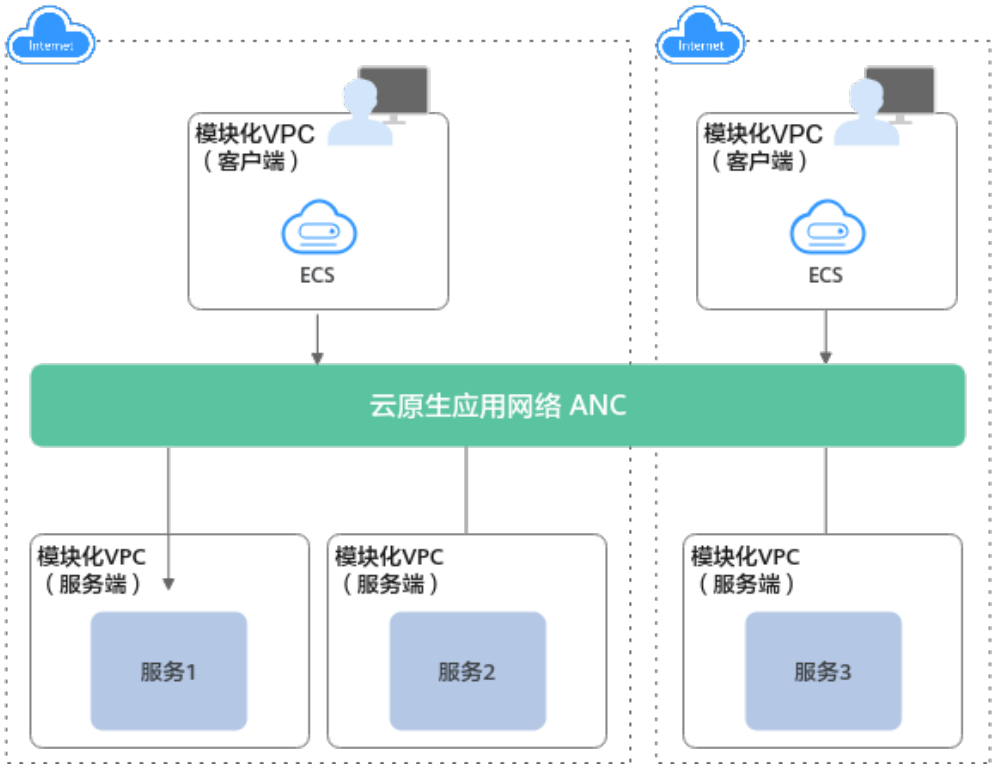


图 3-2 配置 ANC 网络



场景二：VPC 客户端和访问的目的地址冲突

如果VPC客户端和访问的服务端均采用IPv4地址，可能存在客户端网段和访问的服务端网段冲突，通过云原生应用网络可以解决地址冲突的问题。

如图3-3，客户端VPC ECS-1 IP地址为10.1.1.2，服务端ECS-2 IP地址为10.1.1.2，客户端与服务端地址冲突。

配置ANC网络后，客户端访问服务A的域名，即可以通过ANC访问服务端ECS-2。

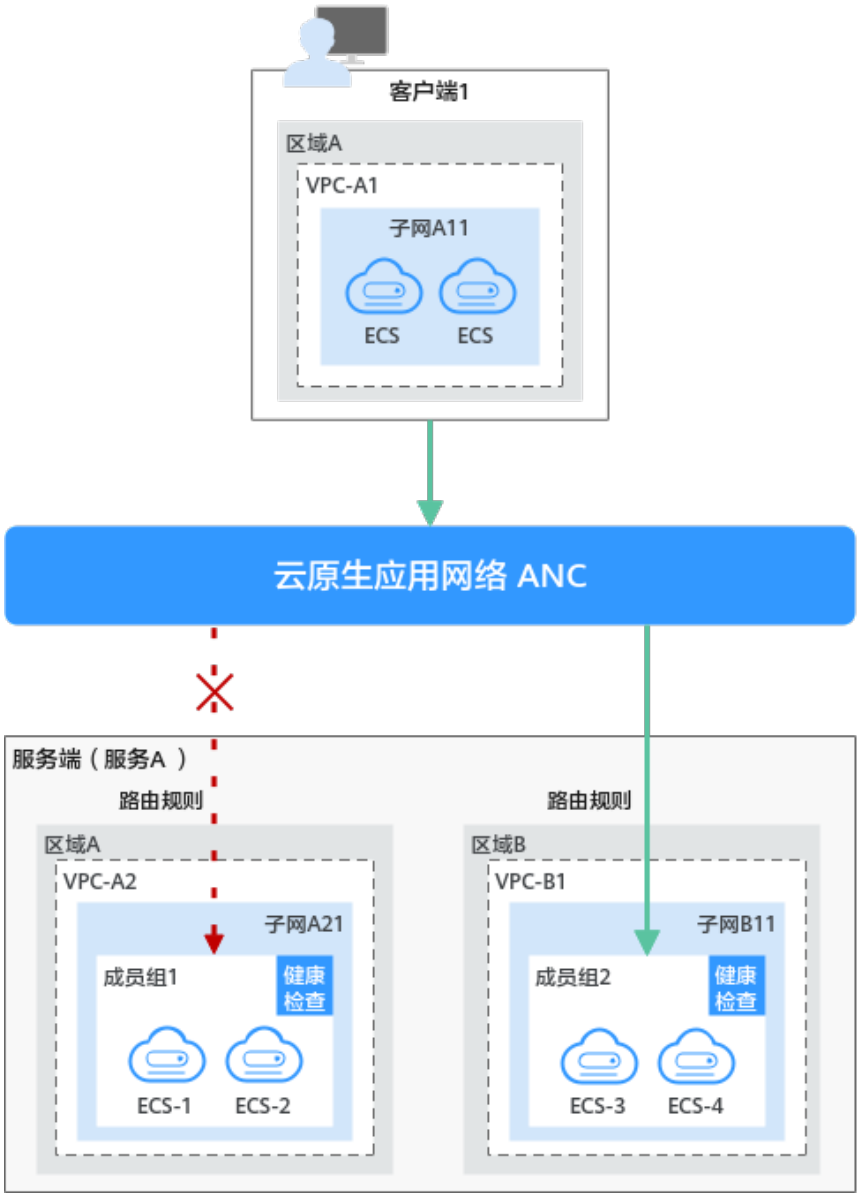
图 3-3 通过 ANC 访问

场景三：全域服务跨域容灾

对于需要高可用性的服务，对可靠性要求高，采用ANC网络跨多个区域搭建网络，保证可用性，避免业务中断。

如图3-4，配置ANC网络后，当服务端区域A健康检查探测到成员组1中成员全部故障，网络会自动切换到区域B的成员组2来保证业务连续性。

图 3-4 通过 ANC 全域服务跨域容灾



4 原理介绍

工作原理

云原生应用网络（ANC）旨在帮助您轻松有效地连接、保护和监控各个服务。

云原生应用网络的工作原理如图4-1所示，详细说明请参见表4-1。

图 4-1 云原生应用网络工作原理图

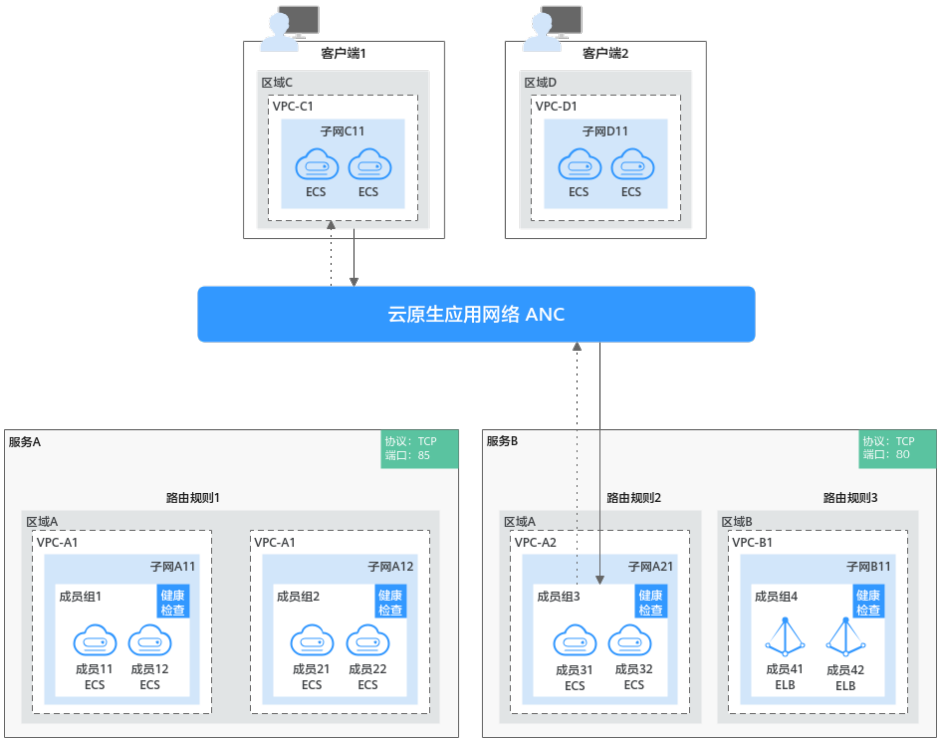


表 4-1 云原生应用网络工作原理说明

序号	原理	网络实例说明
1	ANC关联虚拟私有云VPC 不同区域的客户端VPC可以关联至同一个ANC。	将客户端所在的VPC关联至ANC中。 客户端1的VPC-C1和客户端2的VPC-D1关联ANC，访问服务端内部署的业务应用。
2	将成员组加入服务中 同一个成员组只能加入一个服务中。	将服务端的服务关联至ANC中，客户端即可通过ANC访问服务中的资源（成员）。 当客户端1通过ANC访问服务中的资源（成员）： • 服务A和服务B与ANC关联后，根据设置的协议和端口不同，服务B（协议TCP，端口80）匹配访问请求，成功接收访问流量。 • 服务B根据配置的路由规则2评估访问请求，匹配成功后，访问流量将被转发至成员组3。 • 成员组3健康检查正常后，将根据权重接收并处理访问请求，并通过云原生应用网络返回客户端。
3	ANC关联服务 不同区域的服务可以关联至同一个ANC。	

使用方法

原生应用网络使用方法参考图4-2，详细说明请参见表4-2。

图 4-2 云原生应用网络使用方法

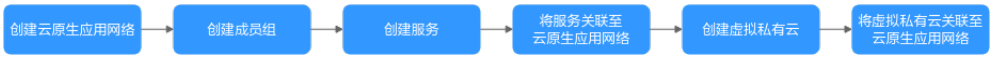


表 4-2 云原生应用网络典型任务工作流

序号	配置	网络实例说明
1	创建云原生应用网络	网络的所有者创建云原生应用网络。
2	创建成员组	通过指定需要运行服务的目标资源(例如实例)来进行创建成员组。选择目标资源所在的区域、虚拟私有云以及子网。创建好成员组后，为每个成员组添加成员。 • 成员组1 区域A • 成员组2 区域A • 成员组3 区域A • 成员组4 区域B

序号	配置	网络实例说明
3	创建服务	服务所有者创建相应的服务，可以根据需求创建跨区域的服务。 ● 同区域 – 服务A – 路由规则1，添加成员组1 区域A、成员组2 区域A ● 跨区域 – 服务B – 路由规则2，添加成员组3 区域A – 路由规则3，添加成员组4 区域B
4	将服务与云原生应用网络关联	将服务与云原生应用网络关联。 关联服务A、服务B。
5	将VPC与云原生应用网络关联	将客户端所在的VPC关联到云原生应用网络。 关联区域C的VPC和区域D的VPC。

成员组

成员组是运行应用程序或服务的资源集合，运行应用程序或服务的资源也称为成员。成员可以是云服务器实例、辅助弹性网卡、弹性负载均衡实例等。

- 每个成员组与其成员（目标资源）的区域、虚拟私有云和子网一致。
- 同区域可以创建一个或多个不同的成员组，例如您可以在区域A内创建成员组1和成员组2。

服务

服务是一种可独立部署的软件单元，接受客户端请求的服务载体。接受来自客户端的请求，根据定义的路由规则将请求转发到成员组的成员。

创建服务的步骤分为两部分：

1. 添加基本信息：选择服务的网络协议，设置协议端口号，指定服务访问的域名等。
2. 添加路由规则：为每个区域添加路由规则，配置健康检查，添加成员组，并为每个成员组设置权重。

表 4-3 服务说明

服务类型	说明
同区域	同一个服务可以添加相同区域的成员组。 在服务A中，添加区域A的路由规则，并添加区域A的多个成员组。 同一服务同一区域中，可添加1个路由规则。

服务类型	说明
跨区域	同一个服务可以添加不同区域的成员组。 在服务B中，添加区域A的路由规则和成员组。添加区域B的路由规则和成员组。

关联服务

关联服务指将服务与云原生应用网络关联。与云原生应用网络关联的服务可以从与云原生应用网络关联的VPC的客户端接收请求。

表 4-4 关联服务说明

关联服务类型	说明
关联同区域服务	服务中的各成员组属于同一个区域内。
关联跨区域服务	服务中的各成员组属于不同的区域内。

关联 VPC

关联VPC是将客户端所在的VPC关联到云原生应用网络。您可以将不同区域的VPC关联至云原生应用网络。例如，将区域C的VPC-C1和区域D的VPC-D1关联至云原生应用网络。

与云原生应用网络关联的VPC客户端可以发现与云原生应用网络关联的服务，可以向与云原生应用网络关联的服务发出请求。

表 4-5 关 VPC 客户端访问路径说明

客户端访问	说明
允许访问路径	● 客户端可以访问与客户端相同区域的服务。 ● 客户端可以访问与客户端不同区域的服务。 ● 客户端优先访问与客户端区域近的服务。
不允许访问路径	客户端无法向与云原生网络关联的其他VPC中的客户端发送请求。

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。

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5-1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，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 5-1 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5-1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服务）。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，也要做好自身控制的中间件、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。

5.2 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可记录云原生应用网络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**。
- ANC支持审计的操作事件，以及如何查看ANC的审计日志，请参见**查看审计日志**。

5.3 监控安全风险

云原生应用网络服务提供基于云监控服务的资源和操作监控能力，帮助用户监控账号下的云原生应用网络资源，执行自动实时监控、告警和通知操作，帮助您更好地了解云原生应用网络的各项性能指标。

- CES的详细介绍，请参见**CES功能介绍**。
- ANC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**使用CES服务监控ANC网络指标**。

5.4 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 5-2 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 5-3 资源中心

网络安全专用产品安全检测证书&软件著作权证书

另外，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 5-4 网络安全专用产品安全检测证书&软件著作权证书

6 约束与限制

ANC 服务使用限制

ANC在使用过程中存在一些限制，您可以单击以下链接，了解不同功能的限制说明。

- 云原生应用网络限制
- 服务限制
- 成员组和成员限制

ANC 服务配额限制

配额是在账号下或者某一区域下最多可同时拥有的某种资源的数量。

例如：单个账号下云原生应用网络ANC默认配额为5个，若在该账号下已创建2个ANC，则在该账号下，此ANC中的剩余配额为3个。

华为云为防止资源滥用，对云服务每个区域的用户资源数量和容量做了配额限制。

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6-1介绍ANC场景的默认配额限制，部分默认配额可以提升，您可以根据提示申请扩大配额。

表 6-1 云原生应用网络的配额说明

配额项目	默认配额限制	是否支持调整
一个用户可创建的云原生应用网络数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在配额限制查看您的个人配额详情。	是 提交工单申请提升配额。
一个云原生应用网络可关联的VPC数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在配额限制查看您的个人配额详情。	是 提交工单申请提升配额。
一个云原生应用网络可关联的服务数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在配额限制查看您的个人配额详情。	是 提交工单申请提升配额。

配额项目	默认配额限制	是否支持调整
一个用户可创建的成员组数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在**配额限制**查看您的个人配额详情。	是 **提交工单**申请提升配额。
一个用户在单个区域内，单个成员组可添加的成员数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在**配额限制**查看您的个人配额详情。	是 **提交工单**申请提升配额。
一个用户可创建的服务数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在**配额限制**查看您的个人配额详情。	是 **提交工单**申请提升配额。
一个用户在单个区域内，单个服务内一个路由规则可添加的成员组数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在**配额限制**查看您的个人配额详情。	是 **提交工单**申请提升配额。
一个服务可关联的ANC数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在**配额限制**查看您的个人配额详情。	是 **提交工单**申请提升配额。
一个健康检查可绑定的成员组数量	不同用户根据其账户类型和服务等级享有不同的默认资源配额。请在**配额限制**查看您的个人配额详情。	是 **提交工单**申请提升配额。

7 与其他服务的关系

原生应用网络与周边服务的依赖关系如图7-1所示。具体的交互功能请参考表7-1。

图 7-1 原生应用网络与其它服务的关系

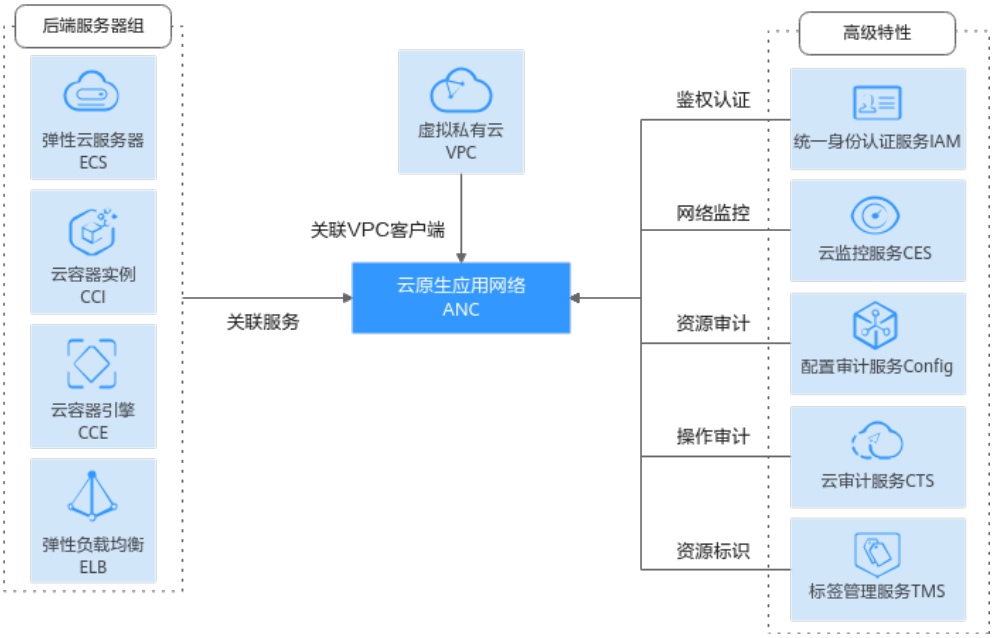


表 7-1 原生应用网络与其它服务的关系

服务名称	交互功能
弹性云服务器（Elastic Cloud Server，ECS）	您可以将ECS、CCI、CCE、ELB等实例作为成员加入成员组，将成员组添加至服务并关联云原生应用网络，客户端可以快速访问服务中的成员组。
云容器实例（Cloud Container Instance， CCI）	
云容器引擎（Cloud Container Engine，简称CCE）	

服务名称	交互功能
弹性负载均衡（Elastic Load Balance，ELB）	
虚拟私有云（Virtual Private Cloud，VPC）	您可以将客户端所在的VPC关联至云原生应用网络，快速打通云上网络，尤其对于客户端VPC跨区域访问场景，免去大量的网络配置。
统一身份认证服务（Identity and Access Management，IAM）	针对位于华为云上的云原生应用网络资源，您可以通过IAM进行精细的权限管理，即为不同的用户设置不同的使用权限，权限管理有助于实现资源的安全管控。
云监控服务（Cloud Eye Service，CES）	使用云监控服务可以监控云原生应用网络实例以及云原生应用网络连接的网络情况，并对异常进行报警，保证业务的顺畅运行。
配置审计Config	使用配置审计服务可以检索全局资源配置，追溯配置历史，持续的审计评估资源配置，确保云上资源配置变更符合预期。
云审计服务（Cloud Trace Service，CTS）	使用云审计服务可以记录与云原生应用网络相关的操作事件，便于日后的查询、审计和回溯。

8 区域和可用区

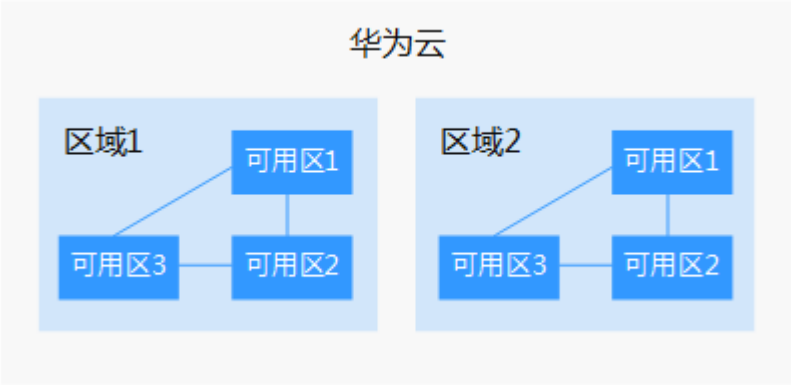
什么是区域、可用区?

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8-1阐明了区域和可用区之间的关系。

图 8-1 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**。