

基础网络服务 产品介绍

产品版本: v6.0.2

发布日期: 2023-06-20

目录

1 产品介绍	1
1.1 什么是基础网络服务	1
1.2 使用场景	5
1.3 基本概念	8
1.4 产品获取	9
1.5 使用限制	10
1.6 与其他服务的关系	11

1 产品介绍

1.1 什么是基础网络服务

基础网络服务旨在为云主机、容器、安全容器和裸金属等计算资源构建安全隔离的、自主配置和自主管理的虚拟网络环境，提升云上资源的安全性，简化网络的部署。客户可以按需配置子网、虚拟网卡和安全组等功能，并允许灵活搭配路由器和公网IP，支撑其业务部署。

产品优势

- 安全可靠

构建的网络环境保证逻辑隔离，并提供完善的安全组策略，此外，还支持多网络可用区部署，提供高可靠的网络服务。

- 灵活配置

通过软件定义网络的方式，实现子网、IP地址范围、安全组、路由器和公网IP等网络对象的按需配置和灵活定义。

- 高性能网络

网络节点性能实现全面优化，即通过DPDK纵向提升性能，通过多活部署横向提升性能。

- IPv4/IPv6双栈

在同一套云平台中，通过统一架构，实现IPv4和IPv6双栈网络，降低使用复杂度和应用成本。

- 互联互通

在安全隔离基础上，支持灵活配置网络之间互联互通，包括内外部网络之间和不同私有网络之间。

- 全栈网络

支持云主机、容器、安全容器和裸金属共用网络规划，实现互联互通。

主要功能

网络

• 自定义虚拟网络

支持在物理网络基础上构建二层隔离的虚拟网络，虚拟网络类型可以选择Geneve或VLAN，不同虚拟网络之间二层逻辑隔离。支持在虚拟网络中，创建IPv4、IPv6或者双栈的一个或多个子网。支持自定义子网的网段、网关、IP地址范围、DHCP等配置，按需对网络进行规划和管理。

• 自定义外部网络

支持构建能通过任意路由器访问的外部网络，以满足虚拟网络访问公网、专线、办公网等的需求，外部网络类型可以选择VLAN或Flat。仅云管理员有创建外部网络的操作权限，但是，部门/项目管理员和普通用户可以直接云管理员创建的外部网络或使用系统默认创建的外部网络（public_net）。

• 自定义可用区

支持为网络选择多个可用区，通过将节点划分入不同可用区的方式，实现节点之间的物理隔离。然后，通过在构建虚拟网络和路由器时选择独立的可用区，以满足业务隔离的需求。

• 多生产网

支持构建多个物理网络，即在创建虚拟网络时，选择在指定的物理网络上构建，使在不同物理网络上构建的虚拟网络实现二层物理隔离。

• 实例互联互通

支持在同一个虚拟网络中，云主机、容器、安全容器和裸金属等资源之间能够互联互通。

虚拟网卡

• 自定义虚拟网卡

支持灵活配置虚拟网卡的IP地址、安全组等，并支持将虚拟网卡与云主机、容器、安全容器和裸金属等资源进行绑定与解绑。

• IPv4/IPv6双栈

支持灵活配置虚拟网卡的IP地址为IPv4、IPv6或IPv4/IPv6双栈类型，以满足客户多样化的组网需求。

• 绑定虚拟IP

支持为多个虚拟网卡分配相同的虚拟IP地址，以满足高可用架构对于虚拟IP的需求，提供虚拟IP管理。

- **自定义带宽限制**

支持灵活配置虚拟网卡的QoS带宽，方便自定义虚拟网卡的带宽能力。

安全组

- **自定义安全组**

支持自行创建安全组，并绑定到相应的资源网卡上，使绑定相同安全组的网卡属于同一安全域。

- **自定义安全组规则**

支持灵活配置安全组的访问规则，即访问规则支持配置多种协议类型和多种匹配方式，以满足用户各类安全隔离规范的要求，而且安全组规则的更新能够自动应用到关联的资源网卡。

路由器

- **自定义互联子网**

支持通过绑定不同子网到同一路由器的方式，实现子网间互联互通的能力。

- **自定义路由规则**

支持根据业务需求灵活配置路由器路由规则，即通过设置目标网段和下一跳的方式，精细化管理网络流量的转发路径。

- **共享带宽**

支持在设置路由器网关时，使子网通过配置的SNAT，获得访问外部网络的能力。

- **自定义共享带宽限制**

支持灵活配置路由器QoS带宽，方便自定义路由器的带宽能力。

- **连接多外部网络**

支持将路由器同时连接到不同的外部网络，使其除连接公网外还可同时连接到办公网、专线等，方便构建混合云业务。

- **路由器多活**

支持自定义路由器ECMP等价路由连接到多个网络节点，以及水平灵活扩展多活网络节点，以满足高可用与高带宽的需求。

公网IP

- **绑定公网IP**

支持将创建的公网IP资源，根据需求绑定到云主机和裸金属主机等资源或路由器上，使资源或路由器获取与公网互相访问的能力。

- **自定义带宽限制**

支持灵活配置公网IP的QoS带宽，方便自定义公网IP的带宽能力。

拓扑展示

- **支持网络拓扑图形化展示**

支持直观查看云平台中的网络拓扑。拓扑图中包含已创建好的路由器、网络及各个子网下关联的云主机等资源信息。

1.2 使用场景

网络

- **业务系统独立网络部署**

对于安全性要求高的企业，通常需要按IT业务类型对内部网络进行隔离，可以通过使用基础网络服务云产品，灵活按照内部业务类型，配置不同的网络，实现网络之间的逻辑隔离。

- **云主机与容器统一网络**

随着容器技术的日臻完善，部分企业应用已经逐步开始容器化。基础网络服务云产品支持云主机与容器共享网络规划，统一进行管理，实现容器与云主机之间的互联互通。

- **多生产网**

基础网络服务云产品支持多生产网部署，实现生产网与生产网之间物理隔离。多生产网承载不同的客户业务，彻底解决共享物理网络逻辑隔离时的带宽争抢问题。

虚拟网卡

- **IPv4/IPv6双栈虚拟网卡**

当IPv4地址紧张，需要利用IPv6缓解新业务上线压力，或政策导向IPv6时，可以通过使用基础网络服务云产品，配置IPv6资源池，为云主机、容器、安全容器和裸金属等资源分配IPv6地址。此外，虚拟网卡支持同时分配IPv4地址和IPv6地址，通过为各资源绑定此类网卡，实现IPv4/IPv6双栈访问。

- **虚拟网卡支持业务高可用**

当需要提高业务系统的高可用性，避免单点故障时，可以通过使用基础网络服务云产品，将云主机、容器、安全容器和裸金属等资源配置为“一主一备”或“一主多备”，使用一个虚拟IP对外提供服务。当主资源故障时，备资源可以转为主资源，继续对外提供服务。

安全组

- **不同安全组资源相互访问**

在同一个网络中，同一安全组内的云主机、容器、安全容器和裸金属等资源默认互通，不同安全组内的云主机默认无法通信。当在同一个网络中，不同安全组的资源需要相互访问时，可以通过将资源双方设置为内网互通后再进行通信。

- **仅允许特定IP地址远程连接资源**

为了防止云主机、容器、安全容器和裸金属等资源被网络攻击，可以通过使用基础网络服务云产品，修改远程登录端口号，并设置安全组规则为只允许特定的IP地址远程登录到资源。

- **云主机作Web服务器**

当在云主机上部署网站，将其作为Web服务器使用时，可以通过使用基础网络服务云产品，在云主机所在安全组中添加指定安全组规则，允许用户通过HTTP或HTTPS服务访问此网站。

路由器

- **不同网络的资源相互访问**

不同网络的云主机、容器、安全容器和裸金属等资源默认无法通信，通过配置路由器连接子网，实现不同网络对应子网内的资源可以相互访问。

- **通过静态路由实现资源跨子网访问**

通过在路由器上配置需要通信的子网的静态路由，实现子网内的资源互连互通。

- **通过SNAT实现资源外部网络访问**

为了使云主机、容器、安全容器和裸金属等资源进行外网访问，基础网络服务云产品除了提供绑定公网IP方式外，还支持通过为路由器设置网关，获得外部网络访问的能力，使各资源无需绑定公网IP也可以完成内部子网的数据流量SNAT到外部网络。

- **路由器连接多个外部网络**

当同一路由器下的云主机、容器、安全容器和裸金属等资源需要通过不同路径访问不同的网络资源时，可以通过使用基础网络服务云产品，将路由器连接到不同的外部网络后，为其配置对应的静态路由，使其连通不同的外部网络。

- **多活路由器提升带宽与高可用性**

通过使用基础网络服务云产品，在路由器上设置ECMP等价路由，将路由器连接到多活的路由器上，实现路由器的高可用和高带宽，并且还可以随时平滑地扩容或缩容多活路由器。

公网IP

- **资源绑定公网IP**

通过为云主机和裸金属主机等资源绑定公网IP，实现资源对公网的访问。

- **路由器绑定公网IP**

通过为路由器外部网关绑定公网IP，实现内部资源对公网的访问。

1.3 基本概念

- **网络**

与物理基础设施网络功能基本相同，云平台提供内部网络和外部网络两种网络类型。其中，内部网络主要用于为云主机和裸金属主机等资源提供二层隔离的私有网络环境。外部网络主要用于创建公网IP地址池。

- **虚拟网卡**

是绑定私有网络内资源的一种弹性网络接口，可在多个资源之间自由迁移。通过配置多个虚拟网卡，可以扩展资源原有的网络接入端口，使资源能够同时连接到多个网络链路。

- **安全组**

是一个逻辑分组，为具有相同安全保护需求并相互信任的资源提供相同的访问策略。

- **路由器**

通过提供三层路由功能，不仅可以使不同子网资源之间互联互通，还可以使内部资源与外部网络之间互相访问。

- **公网IP**

独立的IP地址资源。公网IP通过与资源绑定，可以使各资源独立对外提供服务，通过与路由器绑定，可以使不同子网之间或内部网络与外部网络之间相互访问。

- **网络可用区**

指在同一资源池内，独立提供DHCP服务以及三层网络服务的逻辑区域。

- **CIDR (Classless Inter-Domain Routing)**

即无类别域间路由，用于分配IP地址以及有效路由IP数据包并对IP地址进行归类。其是一种新的寻址方式，与传统的A类、B类和C类寻址模式相比，CIDR在IP地址分配方面更为高效。其采用斜线记法，表示为：IP地址/网络ID的位数。

1.4 产品获取

前提条件

在执行下述产品获取操作步骤前，请确保以下条件均已满足：

- 如需获取正式版云产品，请提前将已获取的许可文件准备就绪。

操作步骤

1. 获取并安装基础网络服务云产品。

在云平台的顶部导航栏中，依次选择[产品与服务]-[产品与服务管理]-[云产品]，进入“云产品”页面获取“基础网络服务”云产品。具体的操作说明，请参考“产品与服务管理”帮助中“云产品”的相关内容。

2. 访问基础网络服务。

在云平台的顶部导航栏中，依次选择[产品与服务]-[网络]后，选择各子菜单，即可访问该服务的各项功能。

1.5 使用限制

- 路由器、外部网络、负载均衡暂不支持IPv6功能。而且，目前IPv6功能为技术预览版，尚在持续研发中，敬请期待。
- 受物理节点上承载外部网络流量的物理网卡带宽所限，公网IP、路由器和虚拟网卡的最大带宽设置不能超过1000Mbps。

1.6 与其他服务的关系

服务	说明
云监控服务	监控网络状态与告警。
身份与访问管理	提供鉴权服务。
标签服务	使用标签标识网络、虚拟网卡、安全组和路由器等网络对象，便于分类和搜索。

咨询热线：400-100-3070

北京易捷思达科技发展有限公司：

北京市海淀区西北旺东路10号院东区1号楼1层107-2号

南京易捷思达软件科技有限公司：

江苏省南京市雨花台区软件大道168号润和创智中心4栋109-110

邮箱：

contact@easystack.cn (业务咨询)

partners@easystack.cn(合作伙伴咨询)

marketing@easystack.cn (市场合作)