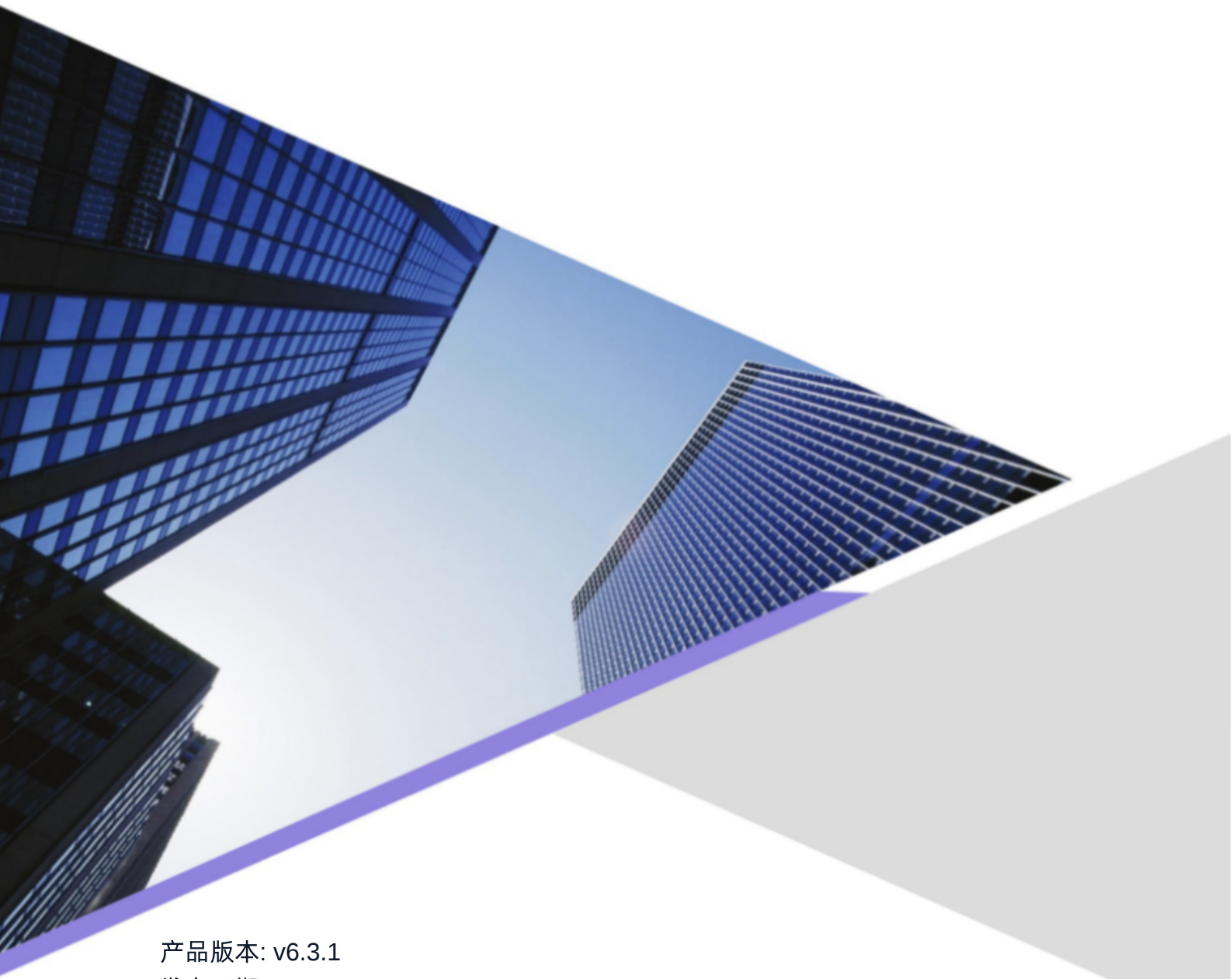
EasyStack
易捷行云

SDN网络服务

产品介绍



产品版本: v6.3.1

发布日期: 2024-06-05

目录

1 产品介绍 1
1.1 什么是SDN网络服务 1
1.2 使用场景 6
1.3 基本概念 7
1.4 产品获取 9
1.5 权限说明 10
1.6 使用限制 14
1.7 与其他服务的关系 15

1 产品介绍

1.1 什么是SDN网络服务

SDN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、网络ACL、网关防火墙，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。

- **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。

- **虚拟IP**

  支持创建虚拟IP，为虚拟IP地址绑定公网IP，多个虚拟网卡分配共同的虚拟IP，满足高可用架构对于虚拟IP的需求。

- **辅助私网IP**

  支持辅助私网IP，可以为云主机、裸金属分配多个辅助私网IP，满足云主机、裸金属使用多个IP提供业务的需求。

- **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，安全组支持有状态和无状态，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。

网络ACL

- **自定义网络ACL**

  支持自行创建网络ACL，网络ACL里配置出入向规则，绑定到子网网关实现子网级别的访问控制。

- **自定义网络ACL出入向规则**

  支持灵活配置网络ACL的出入向访问控制规则，规则可配置多种协议类型、多种匹配策略，支持调整优先级，满足用户子网间的访问控制要求，出入向规则的变化将自动应用到关联的子网网关。

网关防火墙

- **自定义网关防火墙**

支持自行创建网关防火墙，网关防火墙里配置出入向规则，绑定到路由器网关实现路由器北向的访问控制。

- **自定义网关防火墙出入向规则**

  支持灵活配置网关防火墙的出入向访问控制规则，规则可配置多种协议类型、多种匹配策略，支持调整优先级，满足用户路由器北向网络的访问控制要求，出入向规则的变化将自动应用到关联的路由器网关。

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。

网络节点

- **网络节点管理**

  支持查看网络节点状态，网络节点上承载的出口路由器，以及调整路由器的高可用优先级。

- **裸金属网关节点管理**

  支持查看裸金属网关节点状态，裸金属网关节点上承载的裸金属，以及调整裸金属网络端口的高可用优先级。

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SDN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、容器、裸金属统一网络**

  SDN网络服务云产品支持云主机、容器、裸金属主机共享网络规划，统一进行管理，实现容器、云主机、裸金属主机之间的互联互通。

- **多业务隔离区与多生产网**

  企业用户一朵云中根据监管或业务要求有业务网络物理隔离的需求，可以通过隔离区将业务网络物理隔离开，每个隔离区里有自己的网络、子网、路由器、公网IP等。

  企业用户的某些业务系统对网络性能要求严格，对网络质量非常敏感，可以划分出单独的物理生产网，彻底解决存在的带宽争抢、资源被占用的问题。

- **丰富的访问控制策略**

  网络安全对企业用户来说至关重要，易捷行云网络服务提供丰富的网络访问控制策略：包括云主机、裸金属、容器层级的安全组策略、子网层级的网络ACL策略以及路由器北向出口层级的网关防火墙策略，3种层级安全访问策略满足用户对不同安全级别的需求。

- **公网、办公网、专线等多外部网络访问**

  企业用户一般都有公网、办公网、专线网络等多种网络，对于云平台上的计算资源，会有多种网络访问需求，比如允许一些云主机只能访问公网、办公网、专线网络中的一种网络，或允许一些云主机同时可以访问三种网络的其中二种或三种网络。通过云平台提供的多外部网络搭配路由器功能可轻松实现按需的外部网络访问。

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，支持有状态和无状态。

  > 说明：
  > - 有状态：回复数据流会被自动允许，不受任何规则的影响。
  > - 无状态：回复数据流必须被规则明确允许。
  >
  > 一般使用安全组都是有状态的，以下场景需要使用无状态安全组：
  > - 无状态安全组性能比有状态性能好，在裸金属场景下，如果对网络性能有要求，考虑使用无状态安全组。
  > - 在LVS负载均衡的DR模式下，云主机的虚拟网卡需要使用无状态安全组。

- **网络ACL**

  网络ACL是一个子网层级的流量防护，通过将其与子网关联并配置相应的出/入方向的规则可以有效地控制出入子网的数据流。

  > 说明：
  > - 网络ACL的规则是无状态的规则。

- **网关防火墙**

  网关防火墙是一个路由器层级的流量防护，通过将其与外部网关关联，并配置相应的规则可以有效地控制内/外部网络的出入路由器的数据流。

> 说明：
> - 网关防火墙的规则是有状态的规则。

- **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。

- **网络节点**

  网络节点作为云平台业务网络南北向出口的节点，负责云平台内部的业务隧道网络与云外非隧道网络的转换，它承载了云平台的出口路由器，实现了公网IP、NAT、路由等功能。

- **裸金属网关节点**

  裸金属网关节点负责将裸金属的VLAN网络转换为业务隧道网络，让裸金属像云主机一样接入隧道网络，同时实现了裸金属的安全组、分布式路由器、分布式交换机等功能。

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：

- 请先获取SDN控制器服务平台云产品6.1.3版本并完成升级

操作步骤

1. 获取并升级SDN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“SDN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SDN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 权限说明

本章节主要用于说明SDN网络服务各功能的用户权限范围。其中，√ 代表该类用户可对云平台内所有项目的操作对象执行此功能，**XX项目** 代表该类用户仅支持对XX项目内的操作对象执行此功能，未标注代表该类用户无权限执行此功能。

功能		云管理员	部门管理员/项目管理员/普通用户
网络	信息展示	√	仅已加入项目
	创建网络		
	导出		
	编辑		
	创建/编辑/删除子网		
	编辑子网标签		
	编辑标签		
	删除网络		
虚拟网卡	信息展示	√	仅已加入项目
	创建虚拟网卡	√	
	导出	√	
	绑定到资源	仅Default/admin项目	
	从资源解绑	仅Default/admin项目	
	编辑	√	
	编辑安全组	仅Default/admin项目	

	功能	云管理员	部门管理员/项目管理员/普通用户
	绑定/解绑安全组	仅Default/admin项目	
	添加/删除安全组规则	仅Default/admin项目	
	管理虚拟IP	√	
	编辑标签	√	
	删除网卡	√	
安全组	信息展示	√	仅已加入项目
	创建安全组	√	
	添加/删除规则	仅Default/admin项目	
	编辑标签	√	
	删除安全组	√	
网络ACL	信息展示	√	仅已加入项目
	创建网络ACL	√	
	配置规则	√	
	导入/导出规则	√	
	关联/取消关联子网	√	
	编辑网络ACL	√	
	编辑标签	√	
	删除网络ACL	√	
网关防火墙	信息展示	√	仅已加入项目
	创建网关防火墙	√	

	功能	云管理员	部门管理员/项目管理员/普通用户
	配置规则	√	
	导入/导出规则	√	
	关联/取消关联路由器	√	
	编辑网关防火墙	√	
	编辑标签	√	
	删除网关防火墙	√	
路由器	信息展示	√	仅已加入项目
	创建路由器		
	导出		
	编辑		
	连接/断开子网		
	添加/删除静态路由		
	更新带宽		
	设置/清除网关		
	编辑标签		
	删除路由器		
公网IP	为项目申请IP	√	仅已加入项目
	导出		
	更新带宽		
	绑定到虚拟网卡		
	解除绑定		
	编辑标签		

	功能	云管理员	部门管理员/项目管理员/普通用户
	释放公网IP		
网络拓扑	查看网络拓扑	√	仅已加入项目
	开/关设备标签显示		
	开关资源折叠显示		
网络节点	查看网络节点	√	
	调整路由器高可用优先级		
	查看裸金属网关节点		
	调整裸金属端口高可用优先级		

1.6 使用限制

- 路由器、外部网络暂不支持IPv6功能。
- 网络ACL暂不支持容器路由器。
- 网关防火墙暂不支持多活路由器。

1.7 与其他服务的关系

服务	说明
SDN控制器服务	云平台底层SDN网络控制器，实现分布式的交换机、路由器等SDN网络资源。
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)