虚拟私有云

快速入门

文档版本01发布日期2025-01-08





版权所有 © 华为云计算技术有限公司 2025。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

NUAWE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: <u>https://www.huaweicloud.com/</u>



1 通过 VPC 快速搭建 IPv4 网络	1
2 通过 VPC 快速搭建 IPv4/IPv6 双栈网络	<u>.</u>
3 入门实践	23

通过 VPC 快速搭建 IPv4 网络

您可以参考以下操作,通过虚拟私有云 (VPC)和弹性云服务器 (ECS)快速搭建一个具有 IPv4地址段的云上私有网络,同时,还可以通过弹性公网IP (EIP)实现云上网络和公网 通信的需求。

本示例的IPv4网络架构如<mark>图1-1</mark>所示,网络安全通过安全组Sg-A防护,放通特定流量, 拦截其他流量。网络通信需求和安全组配置说明如下:



1. 客户通过本地PC(IP地址为10.1.0.7)远程登录ECS-A01执行操作,入方向需要放通 以下流量:

- 规则A01: 使用ping命令验证ECS-A01网络连通性的流量
- 规则A02:假如ECS-A01为Linux操作系统,放通远程登录ECS-A01的流量
- 规则A03:假如ECS-A01为Windows操作系统,放通远程登录ECS-A01的流量
- 规则A04:安全组内ECS内网网络互通的流量
- 2. 安全组内的ECS-A01可以访问公网网络,出方向放通ECS-A01访问公网的流量。

使用须知

本示例网络规划仅供您参考,虚拟私有云和子网一旦创建完成,将无法修改网段,您 需要根据具体的业务需求提前规划VPC的数量、子网的数量和IP网段划分等。

具体请参见虚拟私有云和子网规划建议。

文档版本 01 (2025-01-08)

操作流程

操作步骤	说明
准备工作	使用云服务前,您需要注册华为账号并开通华为云、完 成实名认证、为账户充值。
步骤一:创建VPC和子网	创建一个IPv4网段的VPC,并从VPC中划分一个子网。 • VPC IPv4网段: 192.168.0.0/16 • 子网IPv4网段: 192.168.0.0/24
步骤二:购买ECS	基于已有的VPC和子网,购买一个ECS,并配置安全组 等参数。
步骤三:购买EIP并绑定至 ECS	为ECS绑定一个EIP,ECS可以通过EIP访问公网。
步骤四:验证网络通信情 况	验证ECS的通信情况: 1. 通过客户的本地PC可以登录ECS。 2. 通过ECS可以访问公网。

准备工作

在创建VPC和ECS等资源之前,请先注册华为账号并开通华为云、完成实名认证、为账 户充值。请保证账户有足够的资金,以免创建资源失败。

- 注册华为账号并开通华为云,完成实名认证。
 如果您已有一个华为账号,请跳到下一个任务。如果您还没有华为账号,请执行 以下操作。
 - a. 注册华为账号并开通华为云。
 - b. 参考<mark>实名认证</mark>,完成个人或企业账号实名认证。
- 为账户充值。
 您需要确保账户有足够金额,充值方式请参见账户充值。

步骤一: 创建 VPC 和子网

- 1. 进入创建虚拟私有云页面。
- 在"创建虚拟私有云"页面,根据界面提示配置虚拟私有云参数。
 本示例中需要创建一个VPC和一个子网。

图 1-2 虚拟私有云

< 创建虚拟私有云(0
基本信息	
区域	
名称	VPC-A
IPv4网段	
	 建议使用网段:10.0.0/8-24 透择 172.16.0.012-24 透择 192.168.0.016-24 透焊 当必要创建多个VPC,并且VPC与其他VPC,或者VPC与云下数编中心需要通信时,要适免网络网编的网段中央,否则无法正常通信,查看网络规划建议
企业项目	default ~ ③ Q 新建企业项目 C
✓ 高级配置 (可选) 标签: 描述:	

图 1-3子网设置

子网设置1	
子网名称	Subnet-A01
可用区	可用区3 可用区1 可用区2
子网IPv4网段	192 ・ 168 ・ 0 / 24 マ 可用P数: 251
	▲ 子网创建完成后,子网网段无法修改。因此创建之前,请您 查看子网规划建议,合理规划子网网段。
子网IPv6网段(可选)	□ 开启IPv6 ⑦
关联路由表	默认 ⑦
◇ 高级配置 (可选)	
网关: 192.168.0.1 DN	IS服务器地址: 100.125.3.250,100.125.3.251 域名: NTP服务器地址:

表 1-1 虚拟私有云参数说明

参数	示例	说明
区域	华东-上海一	请您选择靠近业务的区域,VPC需要和 ECS、EIP位于同一个区域内。 VPC创建完成后不支持修改该参数。
名称	VPC-A	请您按需设置VPC名称。 VPC创建完成后支持修改该参数。

参数	示例	说明
IPv4网段	192.168.0.0/16	VPC的IPv4地址范围,建议您从以下网段 中选择:
		● 10.0.0.~10.255.255.255(掩码范围可 选8~24)
		 172.16.0.0~172.31.255.255(掩码范围 可选12~24)
		 192.168.0.0~192.168.255.255(掩码范 围可选16~24)
		VPC创建完成后不支持修改该参数。
企业项目	default	请您将VPC加入已有的企业项目内,支持 按企业项目维度管理资源。
		VPC创建完成后不支持修改该参数。
高级配置 > 标签	无需配置	请您按需为VPC绑定标签,标签可用来分 类和标识资源。
		VPC创建完成后支持修改该参数。
高级配置 > 描述	无需配置	请您按需设置VPC的描述信息。
		VPC创建完成后支持修改该参数。

表 1-2 子网参数说明

参数	示例	说明
可用区	可用区4	一个区域内分为多个可用区,不同可用区 之间物理隔离,内网互通。请您任意选择 一个可用区,一个VPC的多个子网可以位 于不同可用区,不影响通信。
		当页面显示"边缘可用区"时,您需要根 据业务规划选择边缘可用区。不显示"边 缘可用区"时,您无需设置子网可用区, 不会影响实际使用。
		ECS可以和VPC子网位于不同可用区,比 如位于可用区1的云服务器,可以使用可 用区3的子网。 子网创建完成后不支持修改该参数。
子网名称	Subnet-A01	请您按需设置子网名称。 子网创建完成后支持修改该参数。
子网IPv4网段	192.168.0.0/2 4	子网的IPv4地址范围,子网网段需要从 VPC的IP网段中划分。 子网创建完成后不支持修改该参数。

参数	示例	说明
子网IPv6网段	不开启	是否自动为子网分配IPv6地址。 子网创建完成后支持修改该参数。
关联路由表	默认	创建VPC时会创建一个默认路由表,子网 自动关联至默认路由表。 默认路由表中已预置系统路由,确保同一 个VPC内不同子网之间的网络互通。 子网创建完成后支持修改该参数。
高级配置 > 网关	192.168.0.1	子网的网关,建议您保持系统默认。 子网创建完成后不支持修改该参数。
高级配置 DNS服务器地 址 域名 NTP服务器地 址 IPv4 DHCP租 约时间 	无需配置	此处的参数均是为VPC中的ECS实例配 置,本示例保持系统默认或者置空,无需 配置。 子网创建完成后支持修改该参数。
高级配置 > 标签	无需配置	请您按需为子网绑定标签,标签可用来分 类和标识资源。 子网创建完成后支持修改该参数。
高级配置 > 描述	无需配置	请您按需设置子网的描述信息。 子网创建完成后支持修改该参数。

参数设置完成后,单击"立即创建"。
 返回VPC列表页面,可以查看到已创建的VPC-A。

步骤二:购买 ECS

- 1. 进入购买弹性云服务器页面。
- 在"购买弹性云服务器"页面,根据界面提示配置弹性云服务器参数。
 本示例中,ECS的网络配置详情如下:
 - 网络:选择已创建的虚拟私有云和子网,VPC-A和Subnet-A01。

图 1-4 网络

网络				
虚拟私有云 ⑦				
VPC-A(192.168.0.0/16)	~	Q 新建虚拟私有云 [2]		
主网卡				
Subnet-A01(192.168.0.0/24)	~	自动分配IP地址	\sim	Q 可用私有IP数量250个
⊕ 新増扩展网卡				
您还可以增加 1 块网卡				
源/目的检查 ⑦				

 安全组:新建一个安全组Sg-A,并添加入方向和出方向规则。您在创建安全 组的时候,系统会自动添加部分规则,您需要根据实际情况进行检查修改, 确保表1-3中的规则均已正确添加。

图 1-5 安全组入方向

安全组								
选择安全组 ⑦								
Sg-A(70ee3d1e-27d3-4fd8	3-a0a4-8fd75448d2ad) $ imes$	~ Q #8	安全组					
请确保所远安全组已放通220	前口 (Linux SSH登录) , 3389鎖口	(Windows远程登录) 和 ICMP	协议 (Ping) . 🔂	置安全组规则 🕐				
降嚴安全組規則 へ								
已進安全组(1)		入方向规则 出方向规则						
安全组名称	排序	安全组名称	优先级	策略	协议端口 ⑦	类型	源地址 ③	描述
1 Sg-A	下修 上修		1	允许	TCP: 22	IPv4	10.1.0.7/32	允许外部访问安全组内实例的SS
		Sg-A	1	允许	ICMP: 全部	IPv4	0.0.0.0/0	允许外部使用ping命令验证安全
			1	允许	全部	IPv4	Sg-A	允许安全组内实例通过内网网络
			1	允许	TCP: 3389	IPv4	10.1.0.7/32	允许外部访问安全组内实例的R

图 1-6 安全组出方向

安全纲	fl								
选择支	全组 ⑦								
Sg-/	A(70ee3d1e-27d3-41d8-a	0a4-8fd75448d2ad) $ imes$	~ Q	新建安全组					
清晰保	师选安全组已放通22端[] (Linux SSH登录) , 3389第	□ (Windows远程登录) 和 I	CMP协议 (Ping) 。	配置安全组规则(3			
自豪多	全组规则 <								
已进步	全组(1)		入方向规则 出方向规	RDI					
	安全组名称	排序	安全组名称	优先级	策略	协议端口 ⑦	类型	目的地址 ⑦	描述
1	Sg-A	下移 上移	Sg-A	1	允许	全部	IPv4	0.0.0/0	允许所有流量从安全组内实例流

表 1-3 安全组 Sg-A 规则说明

方向	策 略	类型	协议端 口	源地址/目的 地址	描述
入方 向	允 许	IPv4	TCP: 22	源地址: 10.1.0.7/32	放通安全组内ECS的 SSH(22)端口,用于通过 本地PC (10.1.0.7/32)远 程登录Linux ECS。
入方 向	允 许	IPv4	TCP: 3389	源地址: 10.1.0.7/32	放通安全组内ECS的 RDP(3389)端口,用于通 过本地PC (10.1.0.7/32) 远程登录Windows ECS。

方向	策 略	类型	协议端 口	源地址/目的 地址	描述
入方 向	允 许	IPv4	ICMP: 全部	源地址: 0.0.0.0/0	放通安全组内ECS的 ICMP(全部)端口,用于 外部通过 ping 命令测试 ECS的网络连通性。
入方 向	允 许	IPv4	全部	源地址:当前 安全组Sg-A	用于安全组内ECS之间网 络互通。
出方 向	允 许	IPv4	全部	目的地址: 0.0.0.0/0	用于安全组内ECS访问外 部,允许流量从安全组内 ECS流出。

- 弹性公网IP:选择"暂不购买"。

图 1-7 弹性公网 IP

公网访问						
弹性公网IP 🕜						
现在购买	使用已有	暂不购买				

不使用弹性公网IP的云服务器不能与互联网互通,仅可作为私有网络中部署业务或者集群所需云服务器进行使用。

ECS的其他配置请您按需选择,具体可请参见自定义购买ECS。

参数设置完成后,单击"立即购买"。
 返回ECS列表页面,可以查看到已创建的ECS-A01。

步骤三: 购买 EIP 并绑定至 ECS

- 1. 进入购买弹性公网IP页面。
- 在"购买弹性公网IP"页面,根据界面提示配置弹性公网IP参数。 请您按需选择EIP的配置参数,具体可请参见购买弹性公网IP。
- 参数设置完成后,单击"立即购买"。
 返回EIP列表页面,可以查看到已创建的EIP-A。
- 在EIP列表中,单击EIP-A所在行的操作列下的"绑定"。
 弹出"绑定弹性公网IP"对话框。

图 1-8 绑定弹性公网 IP

绑定弹性公网IP							×
弹性公网IP	1.95.44. (eip-/)					
选择实例	云服务器	虚拟IP地址	裸金属服务器	辅助弹性网卡			
	Q 通过指定属性	生的关键字搜索					Q
	名称/ID	状态	弹性公网IP	私有IP地址	企业项目	虚拟私有云	
	ecs-A0 7a7cf6	1 43 → 运行中	-	192.168.0.230	default	vpc-A	
* 网卡	IP: 192.168.0.23	0, MAC: fa:16:3e:6e:c6:a	ıc (主网卡)	~			
	已选实例	ecs-A01					
	网卡 IP: 192.168.0.230, MAC: fa:16:3e:6e:c6:ac (主网卡)						
						取消	諚

5. 在对话框中,选择ECS-A01,并单击"确定",将EIP-A绑定至ECS-A01。 返回EIP列表中,在"已绑定实例"列下,可查看到已绑定的ECS-A01。

图 1-9 已绑定 ECS-A



步骤四:验证网络通信情况

- 验证远程登录,使用本地PC远程登录ECS-A01。
 弹性云服务器有多种登录方法,具体请参见登录弹性云服务器。
- 2. 执行以下命令,验证ECS-A01和公网的通信情况。

ping IPv4公网IP地址或者域名

命令示例:

ping support.huaweicloud.com

回显类似如下信息,表示ECS-A01可以访问公网。

[root@ecs-a01 ~]# ping support.huaweicloud.com PING hcdnw.cbg-notzj.c.cdnhwc2.com (203.193.226.103) 56(84) bytes of data. 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=1 ttl=51 time=2.17 ms 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=2 ttl=51 time=2.13 ms 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=3 ttl=51 time=2.10 ms 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=4 ttl=51 time=2.09 ms

--- hcdnw.cbg-notzj.c.cdnhwc2.com ping statistics ---

4 packets transmitted, 4 received, 0% packet loss, time 3004ms rtt min/avg/max/mdev = 2.092/2.119/2.165/0.063 ms

2 通过 VPC 快速搭建 IPv4/IPv6 双栈网络

您可以参考以下操作,通过虚拟私有云 (VPC)和弹性云服务器 (ECS)快速搭建一个同时 具有IPv4和IPv6地址段的云上私有网络。同时,还可以通过弹性公网IP (EIP)和共享带 宽,实现IPv4和IPv6公网通信需求。

本示例的IPv4/IPv6双栈网络架构如<mark>图2-1</mark>所示,网络安全通过安全组Sg-A来防护,放通特定流量,拦截其他流量。网络通信需求和安全组配置说明如下:



图 2-1 IPv4/IPv6 双栈网络架构图(VPC/EIP)

- 1. 客户通过本地PC(IPv4地址为10.1.0.7, IPv6地址为2002:20::44)远程登录ECS-A01 执行操作,入方向需要分别针对IPv4和IPv6地址,放通以下流量:
 - 规则A01和规则A02:使用ping命令验证ECS-A01网络连通性的流量
 - 规则A03和规则A04:假如ECS-A01为Linux操作系统,放通远程登录ECS-A01 的流量
 - 规则A05和规则A06:假如ECS-A01为Windows操作系统,放通远程登录ECS-A01的流量
 - 规则A07和规则A08:安全组内ECS内网网络互通的流量
- 2. 安全组内的ECS-A01可以访问公网网络,出方向需要分别针对IPv4和IPv6地址,放 通ECS-A01访问公网的流量。

使用须知

- 当前IPv4/IPv6双栈网络暂不收费,后续定价会根据运营商收费策略的变化进行调整。
- IPv6功能目前仅在部分区域公测,具体公测区域请参见功能总览中"IPv4/IPv6双 栈"功能的发布区域。申请公测权限后,才可以体验IPv6功能。
- 云耀云服务器L实例、旧版云耀云服务器不支持IPv6网络。
- 弹性云服务器ECS部分规格支持IPv6网络,只有选择支持IPv6的ECS,才可以使用 IPv4/IPv6双栈网络。

在ECS控制台,单击"购买弹性云服务器",进入购买页面查看ECS规格列表。当 ECS规格列表中包含"IPv6"参数,且取值为"是"时,表示该规格的ECS支持 IPv6网络。

图 2-2 ECS 规格列表



本示例网络规划仅供您参考,虚拟私有云和子网一旦创建完成,将无法修改网段,您需要根据具体的业务需求提前规划VPC的数量、子网的数量和IP网段划分等。

具体请参见虚拟私有云和子网规划建议。

操作流程

操作步骤	说明		
准备工作	使用云服务前,您需要注册华为账号并开通华为云、完 成实名认证、为账户充值。		
步骤一:创建VPC和子网	创建一个IPv4网段的VPC,并从VPC中划分一个子网。 ● VPC IPv4网段:192.168.0.0/16		
	• 子网IPv4网段: 192.168.0.0/24		
	 子网IPv6网段:系统自动分配IPv6地址,本示例为 2407:c080:1200:2075::/64 		
步骤二:购买ECS	基于已有的VPC和子网,购买一个ECS,并配置安全组 等参数。		
步骤三:购买EIP并绑定至 ECS(IPv4公网通信)	购买EIP,并将EIP绑定至ECS,则ECS可以通过IPv4类型的EIP地址实现公网通信。		
步骤四:购买共享带宽并 添加ECS的IPv6网卡 (IPv6公网通信)	购买共享带宽,并在共享带宽中添加ECS IPv6网卡,则 ECS可以通过IPv6类型的IP地址实现公网通信。		

操作步骤	说明		
步骤五:验证IPv4和IPv6 网络通信情况	验证ECS的IPv4和IPv6通信情况: 1. 验证通过客户的本地PC,使用ECS-A01的IPv4地址 (EIP)和IPv6地址可以登录ECS。 2. 验证ECS-A01的IPv4和IPv6公网通信情况。		

准备工作

在创建VPC和ECS等资源之前,请先注册华为账号并开通华为云、完成实名认证、为账 户充值。请保证账户有足够的资金,以免创建资源失败。

- 注册华为账号并开通华为云,完成实名认证。
 如果您已有一个华为账号,请跳到下一个任务。如果您还没有华为账号,请执行 以下操作。
 - a. 注册华为账号并开通华为云。
 - b. 参考<mark>实名认证</mark>,完成个人或企业账号实名认证。
- 为账户充值。
 您需要确保账户有足够金额,充值方式请参见账户充值。

步骤一: 创建 VPC 和子网

- 1. 进入创建虚拟私有云页面。
- 在"创建虚拟私有云"页面,根据界面提示配置虚拟私有云参数。
 本示例中需要创建一个VPC和一个子网,并为子网开启IPv6功能。

图 2-3 虚拟私有云

< 创建虚拟私有云	0
基本信息	
区域	
名称	VPC-A
IPv4网段	
	 ● 建议使用网段:10.0.0.06-24 透揮 172.16.0.0/12-24 透輝 192.168.0.0/16-24 透輝 - 当您要创建多个VPC,并且VPC与其他VPC,或者VPC与云下数据中心需要通信时,要避免网络两端的网段冲突,否则无法正常通信,重着网络规划建议
企业项目	default V ③ Q 新融企业项目 C
✓ 高级配置 (可选)	
标签: 描述:	

图 2-4 子网设置

子网设置1	
子网名称	Subnet-A01
可用区	可用区3 可用区1 可用区2
子网IPv4网段	192 ・ 168 ・ 0 / 24 マ 可用P数: 251
	▲ 子网创建完成后,子网网段无法修改。因此创建之前,请您 查看子网规划建议,合理规划子网网段。
子网IPv6网段(可选)	✓ 开启IPv6 ⑦
关联路由表	默认 ③
∨ 高级配置 (可选)	
网关: 192.168.0.1	DNS服务器地址: 100.125.3.250,100.125.3.251 域名: NTP服务器地址:

表 2-1 虚拟私有云参数说明

参数	示例	说明
区域	华东-上海一	请您选择靠近业务的区域,VPC需要和 ECS、EIP位于同一个区域内。
		VPC创建完成后不支持修改该参数。
名称	VPC-A	请您按需设置VPC名称。
		VPC创建完成后支持修改该参数。
IPv4网段	192.168.0.0/16	VPC的IPv4地址范围,建议您从以下网段 中选择:
		● 10.0.0.0~10.255.255.255(掩码范围可 选8~24)
		● 172.16.0.0~172.31.255.255(掩码范围 可选12~24)
		● 192.168.0.0~192.168.255.255(掩码范 围可选16~24)
		VPC创建完成后不支持修改该参数。
企业项目	default	请您将VPC加入已有的企业项目内,支持 按企业项目维度管理资源。
		VPC创建完成后不支持修改该参数。
高级配置 > 标签	无需配置	请您按需为VPC绑定标签,标签可用来分 类和标识资源。
		VPC创建完成后支持修改该参数。
高级配置 > 描述	无需配置	请您按需设置VPC的描述信息。
		VPC创建完成后支持修改该参数。

表 2-2 子网参数说明

参数	示例	说明
可用区	可用区4	一个区域内分为多个可用区,不同可用区 之间物理隔离,内网互通。请您任意选择 一个可用区,一个VPC的多个子网可以位 于不同可用区,不影响通信。
		当页面显示"边缘可用区"时,您需要根 据业务规划选择边缘可用区。不显示"边 缘可用区"时,您无需设置子网可用区, 不会影响实际使用。
		ECS可以和VPC子网位于不同可用区,比 如位于可用区1的云服务器,可以使用可 用区3的子网。
		子网创建完成后不支持修改该参数。
子网名称	Subnet-A01	请您按需设置子网名称。 子网创建完成后支持修改该参数。
子网IPv4网段	192.168.0.0/2 4	子网的IPv4地址范围,子网网段需要从 VPC的IP网段中划分。
		子网创建完成后不支持修改该参数。
子网IPv6网段	开启	是否自动为子网分配IPv6地址,开启IPv6 功能后,系统将会自动为子网分配IPv6地 址。
		子网创建完成后支持修改该参数。
关联路由表	默认	创建VPC时会创建一个默认路由表,子网 自动关联至默认路由表。
		默认路由表中已预置系统路由,确保同一 个VPC内不同子网之间的网络互通。 子网创建完成后支持修改该参数。
	102 169 0 1	
	192.100.0.1	子网创建完成后不支持修改该参数。
高级配置 ● DNS服务器地 址	无需配置	此处的参数均是为VPC中的ECS实例配置,本示例保持系统默认或者置空,无需配置。
● 域名		子网创建元成后文持修改该参数。
● NTP服务器地 址		
● IPv4 DHCP租 约时间		
高级配置 > 标签	无需配置	请您按需为子网绑定标签,标签可用来分 类和标识资源。
		子网创建完成后支持修改该参数。

参数	示例	说明
高级配置 > 描述	无需配置	请您按需设置子网的描述信息。 子网创建完成后支持修改该参数。

参数设置完成后,单击"立即创建"。
 返回VPC列表页面,可以查看到已创建的VPC-A。

步骤二:购买 ECS

- 1. 进入购买弹性云服务器页面。
- 在"购买弹性云服务器"页面,根据界面提示配置弹性云服务器参数。
 本示例中,ECS的网络配置详情如下:
 - 网络:选择已创建的虚拟私有云和子网、VPC-A和Subnet-A01。
 并选择"自动分配IPv6地址",则ECS会拥有IPv4和IPv6两个地址。

图 2-5 网络

网络				
虚拟私有云 ⑦				
VPC-A(192.168.0.0/16)	~	Q 新建虚拟私有云 [2]		
主网卡				
Subnet-A01(192.168.0.0/24 支持IPv6)	~	自动分配IP地址	~	○ 可用私有IP数量250个
自动分配IPv6地址	~	暂不绑定共享带宽	~	Q 新建共享带宽 [2]
⊕ 新増扩展网卡				
您还可以增加 1 块网卡				
源/目的检查 ⑦				

 安全组:新建一个安全组Sg-A,并添加入方向和出方向规则。您在创建安全 组的时候,系统会自动添加部分规则,您需要根据实际情况进行检查修改, 确保表2-3中的规则均已正确添加。

图 2-6 安全组入方向

安全组	安全相									
选择安全组	8巻史金組 ①									
Sg-A(70ee	Sg-A(70ee3d1e-27d3-4084-80d75448d2ad) × V Q 納證安全組									
请确保所选择	安全组已放通22端口((Linux SSH登录) , 3389端口	(Windows远程登录) 和 ICMP	协议 (Ping) . 配	安全组规则 🖸					
隐藏安全组织	現明へ									
已进安全组(1)		入方向规则 出方向规则							
安	全组名称	排序	安全组名称	优先级	策略	协议端口 ⑦	型类型	源地址 ⑦	描述	
1 S(g-A	下修 上修		1	允许	TCP: 22	IPv6	2002:20::44/128	允许外部访问安全组内实例的S	
				1	允许	TCP: 3389	IPv6	2002:20::44/128	允许外部访问安全组内实例的R	
				1	允许	ICMPV6: 全部	IPv6	::/0	允许外部使用ping命令验证安全	
			Sg-A	1	允许	TCP: 22	IPv4	10.1.0.7/32	允许外部访问安全组内实例的S	
				1	允许	TCP: 3389	IPv4	10.1.0.7/32	允许外部访问安全组内实例的R	

图 2-7 安全组出方向

安全组								
选择安全组 ⑦								
Sg-A(70ee3d1e-27d3-4fd8	-a0a4-8fd75448d2ad) $ imes$	~ Q 🗰	安全组					
请确保所选安全组已放通22岁	[[] (Linux SSH登录) , 3389號[]	(Windows远程登录) 和 ICMP	协议 (Ping) . 🔂	曹安全组规则 🕐				
隐蔽安全组规则 へ								
已选安全组(1)		入方向规则 出方向规则						
安全组名称	排序	安全组名称	优先级	論路	协议端口 ⑦	类型	目的地址 ②	描述
1 Sg-A	下移 上移	Sc. 4	1	允许	全部	IPv6	::/0	允许所有流量从安全组内实例流出
		vym		6.1M	625	IBv4	0.0.0.00	ム次和宇治島にある治水である山

表 2-3 安全组 Sg-A 规则说明

方向	策略	类 型	协议端 口	源地址/目的地 址	描述
入方 向	允许	IPv 4	TCP: 22	源地址: 10.1.0.7/32	针对IPv4,放通安全组内 ECS的SSH(22)端口,用 于通过本地PC (10.1.0.7/32)远程登录 Linux ECS。
入方 向	允许	IPv 6	TCP: 22	源地址: 2002:20::44/12 8	针对IPv6,放通安全组内 ECS的SSH(22)端口,用 于通过本地PC (2002:20::44/128)远程 登录Linux ECS。
入方 向	允许	IPv 4	TCP: 3389	源地址: 10.1.0.7/32	针对IPv4,针对IPv4,放 通安全组内ECS的 RDP(3389)端口,用于通 过本地PC (10.1.0.7/32) 远程登录Windows ECS。
入方 向	允许	IPv 6	TCP: 3389	源地址: 2002:20::44/12 8	针对IPv6,放通安全组内 ECS的RDP(3389)端口, 用于通过本地PC (2002:20::44/128)远程 登录Windows ECS。
入方 向	允许	IPv 4	ICMP: 全部	源地址: 0.0.0.0/0	针对IPv4,放通安全组内 ECS的ICMP(全部)端口, 用于外部通过 ping 命令 测试ECS的网络连通性。
入方 向	允许	IPv 6	ICMPV 6: 全部	源地址:::/0	针对IPv6,放通安全组内 ECS的ICMP(全部)端口, 用于外部通过 ping 命令 测试ECS的网络连通性。
入方 向	允许	IPv 4	全部	源地址:当前 安全组Sg-A	针对IPv4,用于安全组内 ECS之间网络互通。
入方 向	允许	IPv 6	全部	源地址:当前 安全组Sg-A	针对IPv6,用于安全组内 ECS之间网络互通。

文档版本 01 (2025-01-08)

方向	策略	类型	协议端 口	源地址/目的地 址	描述
出方 向	允许	IPv 4	全部	目的地址: 0.0.0.0/0	针对IPv4,用于安全组内 ECS访问外部,允许流量 从安全组内ECS流出。
出方 向	允许	IPv 6	全部	目的地址: ::/0	针对IPv6,用于安全组内 ECS访问外部,允许流量 从安全组内ECS流出。

– 弹性公网IP:选择"暂不购买"。

图 2-8 弹性公网 IP

公网访问		
弹性公网IP ⑦		
现在购买	使用已有	暂不购买

不使用弹性公网IP的云服务器不能与互联网互通,仅可作为私有网络中部署业务或者集群所需云服务器进行使用。

ECS的其他配置请您按需选择,具体可请参见自定义购买ECS。

- 参数设置完成后,单击"立即购买"。
 返回ECS列表页面,可以查看到已创建的ECS-A01。
- 4. 创建ECS完成后,需要您登录至ECS内,确认当前ECS是否已成功获取到IPv6地址。
 - Windows公共镜像默认已开启IPv6动态获取功能,无需额外配置。
 - Linux公共镜像开启动态获取IPv6功能时,需要先判断是否支持IPv6协议栈, 再判断是否已开启动态获取IPv6功能。

目前,所有Linux公共镜像均已支持IPv6协议栈。并且Ubuntu 16操作系统已 默认开启动态获取IPv6功能,即Ubuntu 16操作系统无需额外配置,其他 Linux公共镜像需要执行开启动态获取IPv6的操作。

如果您的镜像不支持自动分配IPv6地址,或者自动获取IPv6地址失败,您需要参考<mark>动态获取IPv6地址</mark>执行配置,否则ECS无法通过IPv6地址进行通信。

步骤三:购买 EIP 并绑定至 ECS(IPv4 公网通信)

购买EIP,并将EIP绑定至ECS,则ECS可以通过IPv4类型的EIP地址实现公网通信。

- 1. 进入购买弹性公网IP页面。
- 在"购买弹性公网IP"页面,根据界面提示配置弹性公网IP参数。 请您按需选择EIP的配置参数,具体可请参见购买弹性公网IP。
- 参数设置完成后,单击"立即购买"。
 返回EIP列表页面,可以查看到已创建的EIP-A。
- 在EIP列表中,单击EIP-A所在行的操作列下的"绑定"。
 弹出"绑定弹性公网IP"对话框。

图 2-9 绑定弹性公网 IP

绑定弹性公网IP						×
弹性公网IP	1.95.44. (eip-A)					
选择实例	云服务器 虚	翻IP地址 裸	全属服务器 辅助	防弹性网卡		
	Q 通过指定属性的关键字	搜索				Q
	名称/ID	状态	弹性公网IP	私有IP地址	企业项目	虚拟私有云
	ecs-A01 7a7cf643	⊖ 运行中	-	192.168.0.230	default	vpc-A
* 网卡	IP: 192.168.0.230, MAC: 1	fa:16:3e:6e:c6:ac (主网卡	E) ~			
	已选实例 ecs-A01					
	网卡 IP: 192.1	68.0.230, MAC: fa:16:36	e:6e:c6:ac (主网卡)			
						取消 確定

5. 在对话框中,选择ECS-A01,并单击"确定",将EIP-A绑定至ECS-A01。 返回EIP列表中,在"已绑定实例"列下,可查看到已绑定的ECS-A01。

图 2-10 已绑定 ECS-A

◎ 弹性公局IP 令	監控	状态 ⊖	安全	类型 ⇔	带宽 ⊖	带宽详情 ⇔	已绑定实例	计拨模式	企业项目 ↔	标签	操作
1.95.44.2 elp-A elp-A bfaa2689-916e-4500-b7t3-ddc44c52446f		1 御定	Θ	全动态BGP	bandwidth-7f86	按流量计费 5 Mbit/s	ecs-A01 云服务器	按嘴 2024/05/20 10:53:5	default	-	御定 解謝 更多 >

步骤四:购买共享带宽并添加 ECS 的 IPv6 网卡 (IPv6 公网通信)

购买共享带宽,并在共享带宽中添加ECS IPv6网卡,则ECS可以通过IPv6类型的IP地址 实现公网通信。

- 1. 进入**购买共享带宽**页面。
- 在"购买共享带宽"页面,根据界面提示配置共享带宽参数。 请您按需选择EIP的配置参数,具体可请参见购买共享带宽。
- 参数设置完成后,单击"立即购买"。
 返回共享带宽列表页面,可以查看到已创建的Bandwidth-A。
- 4. 在共享带宽列表中,单击Bandwidth-A所在行的操作列下的"添加公网IP"。 弹出"添加公网IP"对话框。

图 2-11 添加公网 IP

添加公网IP					X
 弹性公网IF 原本的计费 包年/包月3 当前共享带 	Y和IPv6网卡添加到共享带宽后,原本的带宽峰僵无效,并 約式无效,不感外计流量和带宽暴用。 単性公网IP暂时不支持添加到共享带宽。 预的线路类型为普通带宽,可添加的EIP线路类型为全动	和共享带宽相同:5Mbit/s。 态BGP、静态BGP。			
共享帝宽	bandwidth-A 当前共享带宽还可以添加公网IP数:20, 单个共享带宽最多可以添加公网IP的个数:20,如需由请	更多配额请点击 申请扩大配额。			
公网IP	弹性公网IP IPv6网卡				
所属VPC 子网	vpc-A V Q				
	Q 选择属性筛选, 或输入关键字搜索				0
	✓ IPv6网卡 ⇔	所属VPC	子网	所属实例	
	2407:c080:1880:6f8:f81d:5cab:79d1:e857	vpc-A	subnet-A01(192.168.0.0/24)	ecs-A01 云服务器	
	总条数:1 10 🗸 < 1 >				
	已选择: 1个对象				
	2407:c080:1880:6f8:f81d:5cab:79d1:e857 \times				

- 5. 根据以下说明设置参数,并单击"确定",将ECS-A01的IPv6网卡添加到共享带宽 Bandwidth-A中。
 - 公网IP:选择"IPv6网卡"。
 - 所属VPC:选择ECS所在的VPC,本示例为VPC-A。
 - 子网:选择ECS所在的子网,本示例为Subnet-A01。
 - IPv6网卡:选择ECS的IPv6网卡,本示例选择ECS-A01的网卡。

步骤五:验证 IPv4 和 IPv6 网络通信情况

- 分别验证使用ECS-A01的IPv4地址(EIP)和IPv6地址是否可以登录ECS-A01。
 弹性云服务器有多种登录方法,具体请参见登录弹性云服务器。
 以使用PuTTY工具远程登录ECS-A01为例:
 - 验证IPv4地址登录: Host Name (or IP address)中输入ECS-A01的EIP地址, 本示例为1.95.44.XX。
 - 验证IPv6地址登录: Host Name (or IP address)中输入ECS-A01的IPv6地址,本示例为2407:XXX:e857。

图 2-12 PuTTY 配置



- 2. 执行以下命令,分别验证ECS-A01的IPv4和IPv6公网通信情况。
 - 验证IPv4公网访问情况:

ping IPv4公网IP地址或者域名

命令示例:

ping support.huaweicloud.com

回显类似如下信息,表示ECS-A01的IPv4公网通信正常。

[root@ecs-a01 ~]# ping support.huaweicloud.com PING hcdnw.cbg-notzj.c.cdnhwc2.com (203.193.226.103) 56(84) bytes of data. 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=1 ttl=51 time=2.17 ms 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=2 ttl=51 time=2.13 ms 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=3 ttl=51 time=2.10 ms 64 bytes from 203.193.226.103 (203.193.226.103): icmp_seq=4 ttl=51 time=2.09 ms

--- hcdnw.cbg-notzj.c.cdnhwc2.com ping statistics ---4 packets transmitted, 4 received, 0% packet loss, time 3004ms rtt min/avg/max/mdev = 2.092/2.119/2.165/0.063 ms

- 验证IPv6公网通信情况:

ping6 IPv6公网地址

假设2002:20::45是一个公网IP地址,命令示例如下:

ping6 2002:20::45

回显类似如下信息,表示ECS-A01的IPv6公网通信正常。 [root@ecs-a01~]# ping6 2002:20::45 PING 2002:20::45(2002:20::45) from 2002:20::45 : 56 data bytes 64 bytes from 2002:20::45: icmp_seq=1 ttl=64 time=0.770 ms 64 bytes from 2002:20::45: icmp_seq=2 ttl=64 time=0.295 ms 64 bytes from 2002:20::45: icmp_seq=3 ttl=64 time=0.245 ms ^C --- 2002:20::45 ping statistics --- 3 packets transmitted, 3 received, 0% packet loss, time 2080ms rtt min/avg/max/mdev = 0.245/0.436/0.770/0.237 ms



当您创建了虚拟私有云后,可以根据业务需要搭建为不同的环境、网站或应用。 本文介绍虚拟私有云常见的搭建实践,帮助您更好的使用虚拟私有云。

组网规划说明

实践	描述
虚拟私有云和子 网规划建议	介绍如何根据实际业务需求规划VPC和子网的数量、网段划分, 并提供VPC常用组网的规划说明。
VPC网络连接方 案	华为云拥有丰富的网络服务,提供安全、可扩展的云上网络环境,同时提供了高速、可靠的云上云下连接服务,能够实现VPC 和其他VPC之间的网络互通、VPC内实例(比如ECS、RDS)访 问公网、以及云上VPC和云下数据中心(IDC)网络互通的需 求。
连通VPC和其他 VPC的网络(私 网网络)	华为云提供了针对不同业务规模和场景的VPC互连服务。您可以 通过对等连接、企业路由器(ER)、云连接、虚拟专用网络 (VPN)、云专线(DC)等灵活连通不同VPC之间的网络,包 括同一个区域的VPC,不同区域的VPC,或者不同账号下的VPC 等。
连通VPC和公网 的网络(公网网 络)	VPC中云资源默认无法访问公网。您可通过弹性公网IP(EIP)、 NAT网关、弹性负载均衡(ELB)等连通VPC和公网的网络,实 现VPC内的实例主动访问公网、或者面向公网提供服务。
连通VPC和云下 数据中心的网络 (混合云网络)	对于拥有云下数据中心的用户,由于利旧和平滑演进的原因,并 非所有的业务都可以迁移至云上,通过虚拟专用网络(VPN)、 云专线(DC)、云连接等可以连通VPC和云下数据中心网络, 构建混合云组网。

组网配置指导

п

实践	描述
基于华为云弹性 云服务器自建容 器并实现通信	介绍在不使用华为云容器产品的情况下,支持用户在华为云弹性 云服务器中部署容器,并实现同一个子网中不同弹性云服务器内 的容器相互通信。
使用虚拟IP和 Keepalived搭建 高可用Web集群	介绍如何通过虚拟IP搭建高可用WEB集群。虚拟IP主要用于弹性 云服务器的主备切换,达到高可用性HA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。
为多网卡ECS配 置策略路由	当云服务器拥有多张网卡时,主网卡默认可以和外部正常通信, 扩展网卡无法和外部正常通信,此时需要在云服务器内部为这些 网卡配置策略路由,才可以确保多张网卡均可以和外部正常通 信。
VPC间对等连接 组网配置示例	不同的VPC之间内网隔离,您可以使用对等连接将两个VPC连通起来,对等连接两端的VPC使用私有IP地址进行通信。 本文档为您提供了不同组网的VPC对等连接配置示例,包括IPv4 和IPv6组网。
基于VPCEP实现 跨VPC连接ELB	该解决方案基于VPC终端节点和终端节点服务,帮助用户快速实 现同一区域不经过公网、跨VPC的弹性负载均衡ELB后端服务访 问。
基于SNAT实现公 网访问解决方案	该解决方案能帮您快速实现不同虚拟网络之间的流量互通,支持 同账号/不同账号之间高质量高安全的VPC网络连接,同时不依 赖某个独立硬件,解决单点故障或带宽瓶颈的问题。适用于在云 上数据备份,办公数据同步、企业商务数据传递、ERP及支付、 游戏行业等典型场景。
云上跨VPC添加 实例到ELB最佳 实践	该解决方案基于独享型负载均衡的跨VPC后端功能,帮助用户快 速实现云上跨VPC添加实例至弹性负载均衡ELB。

网络安全控制

实践	描述
安全组配置示例	当您在VPC子网内创建实例(云服务器、云容器、云数据库等) 时,您可以使用系统提供的默认安全组default,您也可以创建 其他安全组。无论是默认安全组,还是您创建的安全组,您均可 以在安全组内设置出方向和入方向规则,以此控制出入实例的流 量。本文档您介绍一些常用的安全组的配置示例。
网络ACL配置示 例	网络ACL可以控制流入/流出子网的流量,当网络ACL和安全组同时存在时,流量先匹配网络ACL规则,然后匹配安全组规则。您可以灵活调整安全组的规则,并使用网络ACL作为子网的额外防护。本文档为您提供了典型的网络ACL应用示例。

实践	描述
使用IP地址组提 升安全组规则管 理效率	IP地址组是一个或者多个IP地址的集合,您可以在配置安全组规 则的时候使用IP地址组。如果您变更了IP地址组内的IP地址,则 相当于直接变更了这些IP地址对应的安全组规则,免去逐条修改 安全组规则的工作量。
通过对等连接和 第三方防火墙实 现多VPC互访流 量清洗	介绍通过防火墙软件实现VPC内流量安全管控的需求,首先基于 VPC对等连接实现多个VPC网络互通,然后VPC之间互访流量通 过防火墙软件过滤清洗。
混合云使用第三 方防火墙	本文以用户同区域的多VPC与本地IDC连通为例,介绍混合云使 用第三方防火墙的应用场景。用户IDC数据中心和华为云通过云 专线(DC)或虚拟专用网络(VPN)通信成功,在华为云的内 网上使用第三方虚拟化防火墙,使得云上云下的业务流量经过自 定义的第三方防火墙,对云上的业务进行灵活的安全控制。

网络成本管理

实践	描述
节约公网成本	在您购买带宽产品之前一定要分析您业务系统的流量模型,以便 选择适合的产品及计费模式。