云路由网络 使用教程

产品版本：ZStack 3.3.0

文档版本：V3.3.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴商标均为上海云轴信息科技有限公司的商标。

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、服务或特性等应受上海云轴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，上海云轴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。

目录

1 介绍

云路由网络：主要使用定制的Linux云主机作为路由设备，提供DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等网络服务。

云路由网络拓扑

云路由主要涉及以下3个基本网络：

- 公有网络：

  用于提供弹性IP、端口转发、负载均衡、IPsec隧道等网络服务需要提供虚拟IP的网络，公有网络一般要求可直接接入互联网。

- 管理网络：

  用于管理控制对应的物理资源，例如物理机、镜像服务器、主存储等需提供IP进行访问的资源时使用的网络。

- 私有网络：

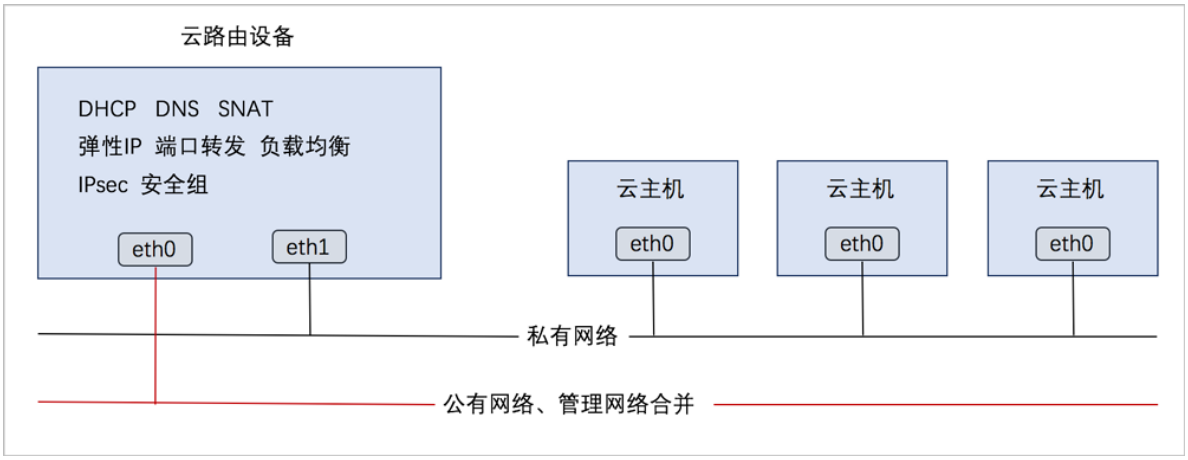
  也称之为业务网络或接入网络，是云主机使用的内部网络。

云路由网络部署方式：

- 公有网络和管理网络合并，私有网络独立部署

  如图 *1: 部署方式-1*所示：

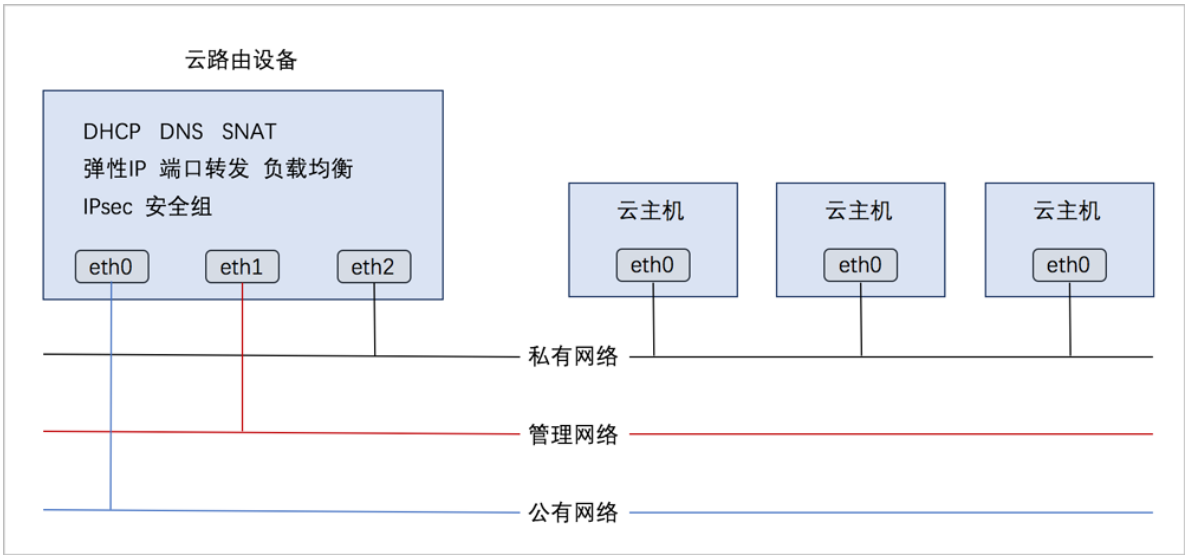
  图 1: 部署方式-1



- 公有网络、管理网络、私有网络均独立部署

如图 2: 部署方式-2所示：

图 2: 部署方式-2



云路由网络服务

云路由提供了DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等网络服务。

- DHCP：
  - 在云路由器中，默认由扁平网络服务模块提供分布式DHCP服务；
- DNS：
  - 云路由器可作为DNS服务器提供DNS服务；
  - 在云主机中看到的DNS地址默认为云路由器的IP地址，由用户设置的DNS地址由云路由器负责转发配置。
- SNAT：
  - 云路由器可作为路由器向云主机提供源网络地址转换；
  - 云主机使用SNAT可直接访问外部互联网。
- 弹性IP：使用云路由器可通过公有网络访问云主机的私有网络。
- 端口转发：提供将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。
- 负载均衡：将公网地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。

- 安全组：
  - 由安全组网络服务模块提供安全组服务；
  - 使用iptables进行云主机防火墙的安全控制。

2 前提

在此教程中，假定已安装最新版本ZStack，并完成基本的初始化，包括区域、集群、物理机、镜像服务器、主存储等基本资源的添加。具体方式请参考《用户手册》安装部署章节和Wizard引导设置章节。

本教程将详细介绍云路由网络的基本部署以及典型应用场景。

3 基本部署

背景信息

搭建云路由网络的基本流程如下：

1. 创建二层公有网络，并加载此二层网络到相应集群。
2. 创建三层公有网络。
3. 创建二层管理网络，并加载此二层网络到相应集群。
4. 创建三层管理网络，用于与物理资源通信，例如，物理机、主存储、镜像服务器等。
5. 添加云路由镜像。
6. 创建云路由规格。
7. 创建二层私有网络，并加载此二层网络到相应集群。
8. 创建云路由类型的三层私有网络。
9. 使用此私有网络创建云主机，创建云主机过程中会自动创建云路由器，云路由器会提供云路由网络的各种网络服务。
10. 验证云路由网络连通性。

假定客户环境如下：

1. 公有网络

表 1: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.108.10.0~10.108.11.255*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*
DHCP IP	*10.108.10.1*

2. 管理网络

表 2: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.30~192.168.29.40*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

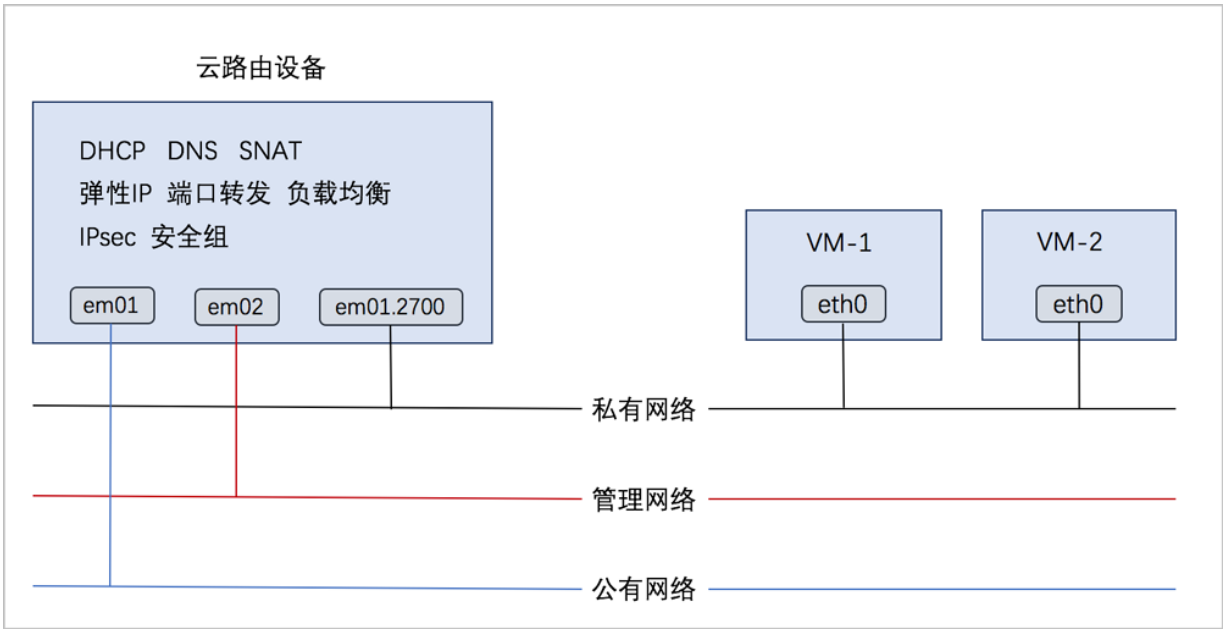
3. 私有网络

表 3: 私有网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2700
IP CIDR	*192.168.10.0/24*
DHCP IP	*192.168.10.10*

云路由网络架构如图 *3:* 云路由网络架构图所示：

图 3: 云路由网络架构图



以下介绍搭建云路由网络的实践步骤。

操作步骤

1. 在ZStack私有云界面创建L2-公有网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *1:* 公有网络配置信息填写如下：

   - **名称**：设置L2-公有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork
   - **网卡**：em01
   - **集群**：选择集群，如Cluster-1

   如图 *4:* 创建*L2*-公有网络所示，点击**确定**，创建L2-公有网络。

   图 4: 创建L2-公有网络

2. 在ZStack私有云界面创建L3-公有网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述表 *1:* 公有网络配置信息填写如下：

   - **名称**：设置L3-公有网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-公有网络
   - **关闭DHCP服务**：选择是否需要DHCP服务

     注:

     - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；

  - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。

- **添加网络段**：选择IPv4类型网络地址、IP范围方式

  注: ZStack支持IPv4、IPv6类型网络地址；可通过IP范围或CIDR方式添加网络段。本教程以IPv4类型网络地址、IP范围方式为例。

- **起始IP**：*10.108.10.0*
- **结束IP**：*10.108.11.255*
- **子网掩码**：*255.0.0.0*
- **网关**：*10.0.0.1*
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:

  - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
  - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
  - DHCP IP可以在添加的IP范围之内或之外，但必须在添加的IP范围所属的CIDR内，且未被占用；
  - 若留空不填，将由系统在添加的IP范围内随机指定。

- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *5:* 创建*L3*-公有网络所示，点击**确定**，创建L3-公有网络。

图 5: 创建L3-公有网络


确定
取消
创建公有网络
名称 *
L3-公有网络
简介
二层网络 *
L2-公有网络
关闭DHCP服务

3. 在ZStack私有云界面创建L2-管理网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *2:* 管理网络配置信息填写如下：

   - **名称**：设置L2-管理网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork

- **网卡**：em02
- **集群**：选择集群，如Cluster-1

如图 *6: 创建L2-管理网络*所示，点击**确定**，创建L2-管理网络。

图 6: 创建L2-管理网络

4. 在ZStack私有云界面创建L3-管理网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **系统网络**，进入**系统网络**界面，点击**创建系统网络**，在弹出的**创建系统网络**界面，参考上述*表 2: 管理网络配置信息*填写如下：

   - **名称**：设置L3-管理网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-管理网络

- **添加网络段**：选择IP范围
- **起始IP**：*192.168.29.30*
- **结束IP**：*192.168.29.40*
- **子网掩码**：*255.255.255.0*
- **网关**：*192.168.29.1*

如图 *7:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 7: 创建L3-管理网络

5. 添加云路由镜像。

   在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由镜像**，进入**云路由镜像**界面，点击**添加云路由镜像**，在弹出的**添加云路由镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置云路由镜像名称
   - **简介**：可选项，可留空不填

- **镜像服务器**：选择待存放云路由镜像的镜像服务器，如BS-1
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

1. **URL**：输入云路由镜像的可下载路径

   注:

   ZStack提供专用的云路由镜像供用户使用，可在*ZStack*官网下载最新的云路由镜像。

   - 文件名称：zstack-vrouter-3.3.0.qcow2
   - 下载地址：点击*ZStack*官网查看

2. **本地文件**：选择当前浏览器可访问的云路由镜像直接上传

   注:

   - 支持上传到镜像仓库和Ceph镜像服务器；
   - 采用本地浏览器作为中转上传镜像，请勿刷新或关闭当前浏览器，也不可停止管理节点服务，否则会添加失败。

如图 *8:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 8: 添加云路由镜像

6. 创建云路由规格。

在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由规格**，进入**云路由规格**界面，点击**创建云路由规格**，在弹出的**创建云路由规格**界面，可参考以下示例输入相应内容：

- **名称**：设置云路由规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置CPU个数，生产环境中建议个数设置为8以上
- **内存**：设置内存大小，单位包括：M、G、T，生产环境中建议设置为8G以上
- **镜像**：选择已添加的云路由镜像
- **管理网络**：从网络列表中选择已创建的L3-管理网络
- **公有网络**：从网络列表中选择已创建的L3-公有网络

如图 *9:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 9: 创建云路由规格

7. 在ZStack私有云界面创建L2-私有网络（云路由网络）。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *3:* 私有网络配置信息填写如下：

   - **名称**：设置L2-私有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2VlanNetwork

- **Vlan ID**：2700
- **网卡**：em01
- **集群**：选择集群，如Cluster-1

如图 *10: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 10: 创建L2-私有网络

8. 在ZStack私有云界面创建L3-私有网络（云路由网络）。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **私有网络**，进入**私有网络**界面，点击**创建私有网络**，在弹出的**创建私有网络**界面，参考上述*表 3: 私有网络配置信息*填写如下：

- **名称**：设置L3-私有网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-私有网络
- **关闭DHCP服务**：选择是否需要DHCP服务

  注:

  - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；
  - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- 网络类型选择**云路由**网络
- **云路由规格**：选择已创建的云路由规格
- **添加网络段**：选择CIDR方式
- **CIDR**：*192.168.10.0/24*
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:

  - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
  - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
  - DHCP IP必须在添加的CIDR内，且未被占用；
  - 若留空不填，将由系统在添加的CIDR内随机指定；
  - CIDR内首个IP地址已被默认为网关，不可作为DHCP IP。
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *11:* 创建*L3*-私有网络所示，点击**确定**，创建L3-私有网络。

图 11: 创建L3-私有网络


确定
取消
创建私有网络
名称 *
L3-云路由
简介
二层网络 *
L2-云路由
关闭DHCP服务
扁平网络
云路由
云路由规格 *
云路由规格

9. 使用云路由网络创建私有云云主机。

   在ZStack私有云界面，点击**云资源池** > **云主机**，进入**云主机**界面，点击**创建云主机**，在弹出的**创建云主机**界面，可参考以下示例输入相应内容（以创建单个云主机为例）：

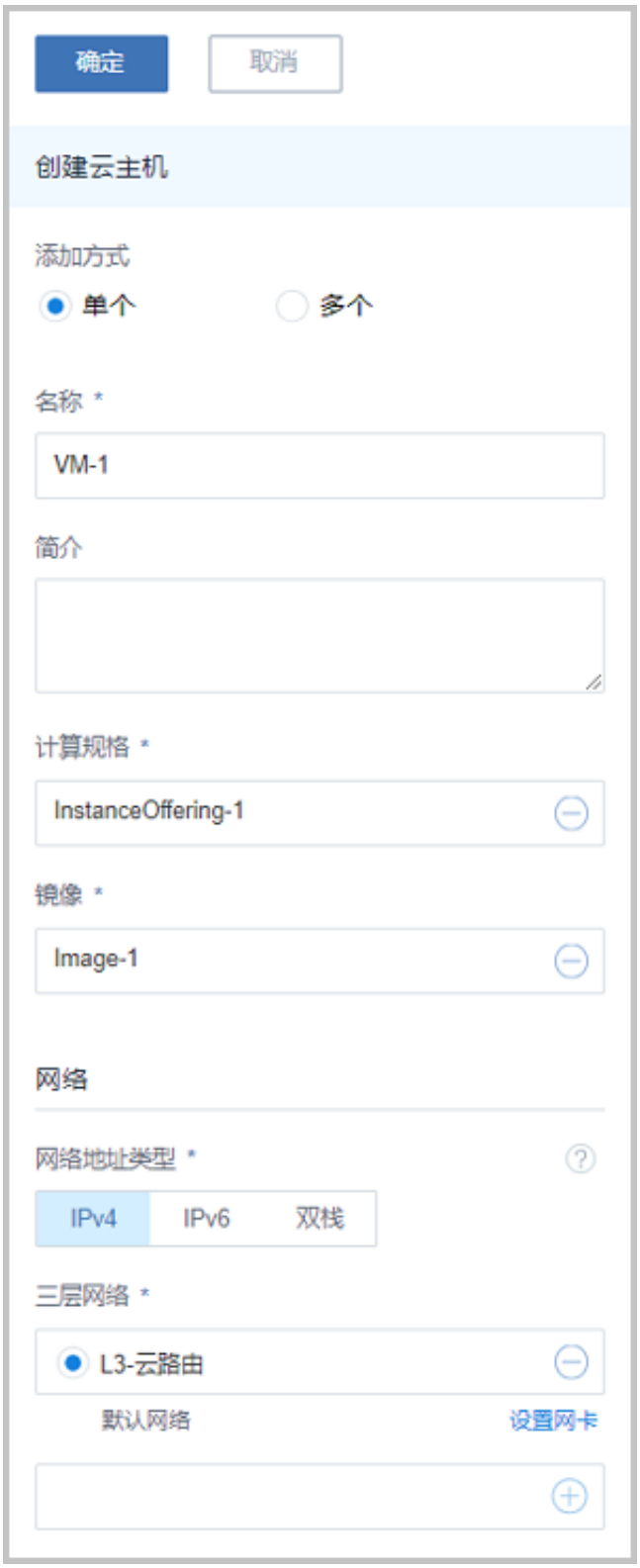
   - **添加方式**：单个

     注: 如需批量创建云主机，请选择**多个**，并输入需批量创建云主机的数量。

   - **名称**：设置私有云云主机名称，例如VM-1
   - **简介**：可选项，可留空不填
   - **计算规格**：选择已创建的计算规格
   - **镜像**：选择已添加的镜像
   - **网络**：选择IPv4网络地址类型的云路由网络

   如图 *12:* 创建私有云云主机所示，点击 **确定**，创建私有云云主机。

   图 12: 创建私有云云主机



10.使用云路由网络创建私有云云主机过程中，系统会自动创建云路由器。云路由器会提供云路由网络的各种网络服务。

11.验证云路由网络连通性。

- 公网连通性验证：

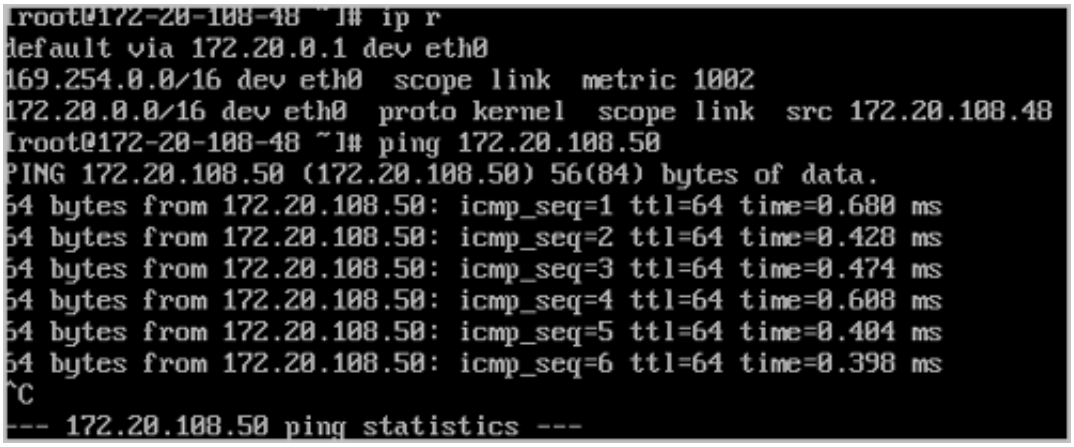
  登录VM-1，检查是否能够ping通公网，如图 *13: VM-1 ping通公网*所示：

  图 13: VM-1 ping通公网

- 内网连通性验证：

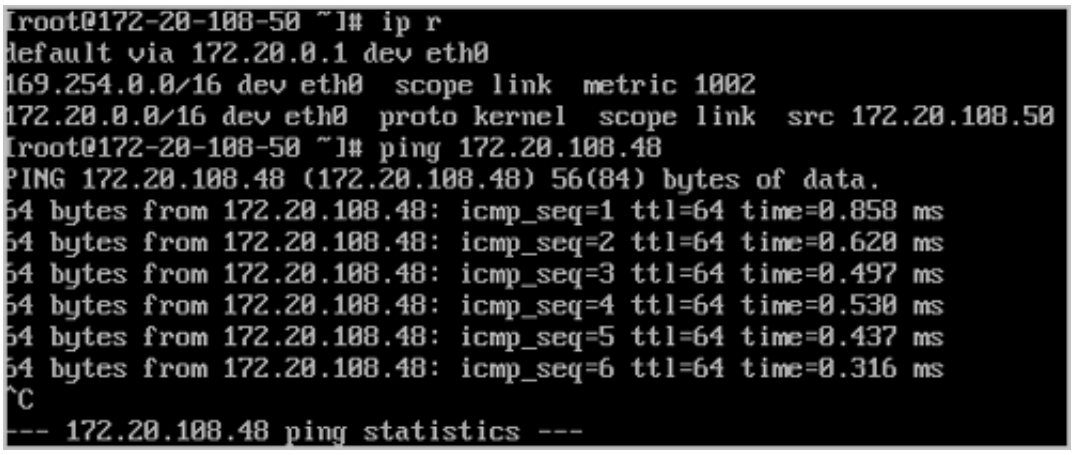
  1. 使用该云路由网络创建另一台私有云云主机，例如VM-2。
  2. 登录VM-1，检查是否能够ping通VM-2，如图 *14: VM-1 ping通 VM-2*所示：

     图 14: VM-1 ping通 VM-2



  3. 登录VM-2，检查是否能够ping通VM-1，如图 *15: VM-2 ping通 VM-1*所示：

     图 15: VM-2 ping通 VM-1



至此，云路由网络的基本部署实践介绍完毕。

4 应用场景

云路由网络可用于以下典型应用场景：

- 多租户隔离
- 多层Web服务器
- 多公网
- 安全组
- 弹性IP
- 端口转发
- 负载均衡
- IPsec隧道

4.1 多租户隔离

前提条件

使用VLAN或VXLAN技术，可提供多租户在二层网络上的隔离。

表 4: VLAN与VXLAN的比较

VLAN	VXLAN
• VLAN最多支持4096个VLAN ID，即一套环境中最多提供4096个隔离的租户网络，难以满足大规模云计算数据中心的需求 • 各厂商交换机配置VLAN方式各不相同	• VXLAN基于客户机房现有的网络拓扑，提供16M个逻辑网络用于多租户隔离 • VXLAN是基于现有三层网络之上Overlay虚拟出的二层网络，该Overlay虚拟过程可由软件方式实现，也可由支持VXLAN的交换机实现，客户可按需选择 • 相较于VLAN，VXLAN性能损耗较大，网络延迟也较高

背景信息

本场景主要介绍VXLAN-云路由网络提供多租户隔离的实践。

搭建VXLAN-云路由网络的基本流程：

1. 创建二层公有网络，并加载此二层网络到相应集群。
2. 创建三层公有网络。
3. 创建二层管理网络，并加载此二层网络到相应集群。
4. 创建三层管理网络，用于与物理资源通信，例如，物理机、主存储、镜像服务器等。
5. 添加云路由镜像。

6. 创建云路由规格。
7. 创建VXLAN网络池，并加载到相应集群。
8. 基于VXLAN网络池创建VXLAN网络1（虚拟的二层私有网络）。
9. 使用VXLAN网络1创建云路由类型的三层私有网络1。
10. 基于VXLAN网络池创建VXLAN网络2（虚拟的二层私有网络）。
11. 使用VXLAN网络2创建云路由类型的三层私有网络2。
12. 使用私有网络1创建云主机1，使用私有网络2创建云主机2。
13. 验证两台云主机的网络连通性。

注:

- VXLAN网络池和VXLAN网络共同提供了VXLAN网络类型的配置；
- 使用VXLAN网络需先创建VXLAN网络池，VXLAN网络对应了VXLAN网络池里的一个虚拟网络；
- VXLAN网络池不能用于创建三层网络，只表示VXLAN网络的集合，VXLAN网络可用于创建三层网络。

假定客户环境如下：

1. 公有网络

表 5: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.108.12.0~10.108.13.255*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*
DHCP IP	*10.108.12.1*

2. 管理网络

表 6: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.30~192.168.29.40*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. VXLAN网络池

表 7: VXLAN网络池配置信息

VXLAN网络池	配置信息
Vni范围	20-1200
VTEP CIDR	192.168.29.1/24

4. 私有网络1

表 8: 私有网络1配置信息

私有网络	配置信息
Vni	100
IP CIDR	*192.168.10.0/24*
DHCP IP	*192.168.10.2*

5. 私有网络2

表 9: 私有网络2配置信息

私有网络	配置信息
Vni	200
IP CIDR	*192.168.11.0/24*
DHCP IP	*192.168.11.2*

以下介绍搭建VXLAN-云路由网络的实践步骤。

操作步骤

1. 在ZStack私有云界面创建L2-公有网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *5:* 公有网络配置信息填写如下：

   - **名称**：设置L2-公有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork
   - **网卡**：em01
   - **集群**：选择集群，如Cluster-1

   如图 *16:* 创建*L2-*公有网络所示，点击**确定**，创建L2-公有网络。

   图 16: 创建L2-公有网络

2. 在ZStack私有云界面创建L3-公有网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述表 *5:* 公有网络配置信息填写如下：

   - **名称**：设置L3-公有网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-公有网络
   - **关闭DHCP服务**：选择是否需要DHCP服务

     注:

     - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；

  - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- **添加网络段**：选择IPv4类型网络地址、IP范围方式

  注: ZStack支持IPv4、IPv6类型网络地址；可通过IP范围或CIDR方式添加网络段。本教程以IPv4类型网络地址、IP范围方式为例。
- **起始IP**：*10.108.12.0*
- **结束IP**：*10.108.13.255*
- **子网掩码**：*255.0.0.0*
- **网关**：*10.0.0.1*
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:
  - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
  - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
  - DHCP IP可以在添加的IP范围之内或之外，但必须在添加的IP范围所属的CIDR内，且未被占用；
  - 若留空不填，将由系统在添加的IP范围内随机指定。
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *17: 创建L3-公有网络*所示，点击**确定**，创建L3-公有网络。

图 17: 创建L3-公有网络


确定
取消
创建公有网络
名称 *
L3-公有网络
简介
二层网络 *
L2-公有网络
关闭DHCP服务

3. 在ZStack私有云界面创建L2-管理网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *6: 管理网络配置信息*填写如下：

   - **名称**：设置L2-管理网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork

- **网卡**：em02
- **集群**：选择集群，如Cluster-1

如图 *18: 创建L2-管理网络*所示，点击**确定**，创建L2-管理网络。

图 18: 创建L2-管理网络

4. 在ZStack私有云界面创建L3-管理网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **系统网络**，进入**系统网络**界面，点击**创建系统网络**，在弹出的**创建系统网络**界面，参考上述*表 6: 管理网络配置信息*填写如下：

   - **名称**：设置L3-管理网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-管理网络

- **添加网络段**：选择IP范围
- **起始IP**：*192.168.29.30*
- **结束IP**：*192.168.29.40*
- **子网掩码**：*255.255.255.0*
- **网关**：*192.168.29.1*

如图 *19:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 19: 创建L3-管理网络

5. 添加云路由镜像。

   在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由镜像**，进入**云路由镜像**界面，点击**添加云路由镜像**，在弹出的**添加云路由镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置云路由镜像名称
   - **简介**：可选项，可留空不填

- **镜像服务器**：选择待存放云路由镜像的镜像服务器，如BS-1
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

1. **URL**：输入云路由镜像的可下载路径

   注:

   ZStack提供专用的云路由镜像供用户使用，可在*ZStack*官网下载最新的云路由镜像。

   - 文件名称：zstack-vrouter-3.3.0.qcow2
   - 下载地址：点击*ZStack*官网查看

2. **本地文件**：选择当前浏览器可访问的云路由镜像直接上传

   注:

   - 支持上传到镜像仓库和Ceph镜像服务器；
   - 采用本地浏览器作为中转上传镜像，请勿刷新或关闭当前浏览器，也不可停止管理节点服务，否则会添加失败。

如图 *20:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 20: 添加云路由镜像

6. 创建云路由规格。

在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由规格**，进入**云路由规格**界面，点击**创建云路由规格**，在弹出的**创建云路由规格**界面，可参考以下示例输入相应内容：

- **名称**：设置云路由规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置CPU个数，生产环境中建议个数设置为8以上
- **内存**：设置内存大小，单位包括：M、G、T，生产环境中建议设置为8G以上
- **镜像**：选择已添加的云路由镜像
- **管理网络**：从网络列表中选择已创建的L3-管理网络
- **公有网络**：从网络列表中选择已创建的L3-公有网络

如图 *21:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 21: 创建云路由规格

7. 在ZStack私有云界面创建VXLAN网络池。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **VXLAN Pool**，进入**VXLAN Pool**界面，点击**创建VXLAN Pool**，在弹出的**创建VXLAN Pool**界面，参考上述表 *7: VXLAN*网络池配置信息填写如下：

   - **名称**：设置VXLAN网络池名称
   - **简介**：可选项，可留空不填

- **起始Vni**：可从1-16777214之间选择一个数字作为起始Vni
- **结束Vni**：可从1-16777214之间选择一个数字作为结束Vni，需大于或等于起始Vni

  注:

  - VXLAN网络池最大可支持16M（16777216）个虚拟网络，Vni范围支持1-16777216。
  - 最后两个Vni（即：16777215、16777216）为系统保留。
- **集群**：可选项，可在创建VXLAN网络池时直接加载相应集群，也可在创建VXLAN网络池后再加载集群。

  注: 加载的集群内物理机需存在VTEP IP。
- **VTEP CIDR**：设置VTEP相应的CIDR，例如192.168.29.1/24

  注:

  - 创建VXLAN网络池，加载集群，需设置相应的VTEP（VXLAN隧道端点），VTEP一般对应于集群内物理机的某一网卡IP地址，设置VTEP是基于相应的CIDR来配置；
  - VXLAN网络池加载到集群时，检查的是VTEP IP，与物理的二层设备无关。

如图 *22: 创建VXLAN网络池*所示，点击**确定**，创建VXLAN网络池。

图 22: 创建VXLAN网络池

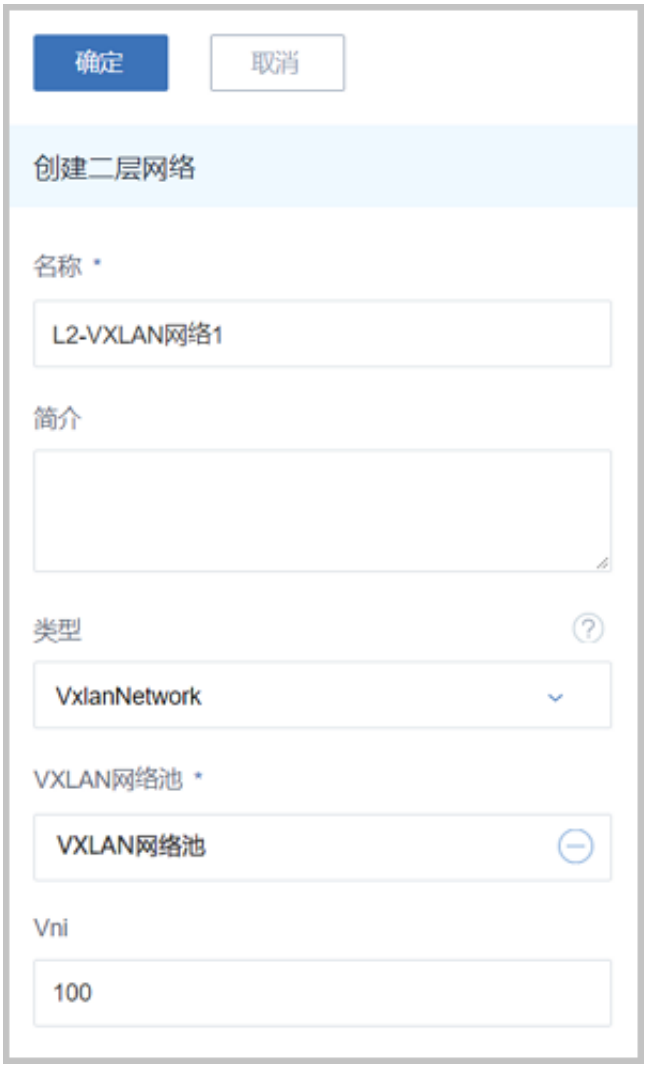
8. 基于VXLAN网络池创建VXLAN网络1（虚拟的L2-私有网络）。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网络**，在弹出的**创建二层网络**界面，参考上述表 *8: 私有网络1配置信息*填写如下：

   - **名称**：设置VXLAN网络1名称，例如L2-VXLAN网络1
   - **简介**：可选项，可留空不填
   - **类型**：选择VxlanNetwork
   - **VXLAN网络池**：选择已创建的VXLAN网络池
   - **Vni**：可选项，从VXLAN网络池指定Vni，可在创建VXLAN网络1时直接指定，例如100，也可留空不填，由系统随机指定

如图 *23: 创建L2-VXLAN网络1*所示，点击**确定**，创建L2-VXLAN网络1。

图 23: 创建L2-VXLAN网络1



9. 使用L2-VXLAN网络1创建云路由类型的L3-私有网络1。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **私有网络**，进入**私有网络**界面，点击**创建私有网络**，在弹出的**创建私有网络**界面，参考上述表 *8: 私有网络1*配置信息填写如下：

   - **名称**：设置L3-私有网络1名称，例如L3-VXLAN-云路由网络1
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-VXLAN网络1
   - **关闭DHCP服务**：选择是否需要DHCP服务

   注:

    - 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；
    - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- 网络类型选择**云路由**网络
- **云路由规格**：选择已创建的云路由规格
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.10.0/24*
- **DHCP IP**：可选项，可按需设置DHCP IP

    注:

    - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
    - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
    - DHCP IP必须在添加的CIDR内，且未被占用；
    - 若留空不填，将由系统在添加的CIDR内随机指定；
    - CIDR内首个IP地址已被默认为网关，不可作为DHCP IP。
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *24: 创建L3-VXLAN-云路由网络1*所示，点击**确定**，创建L3-VXLAN-云路由网络1。

图 24: 创建L3-VXLAN-云路由网络1


确定
取消
创建私有网络
名称 *
L3-VXLAN-云路由网络1
简介
二层网络 *
L2-VXLAN网络1
关闭DHCP服务
扁平网络
云路由
云路由规格 *
云路由规格

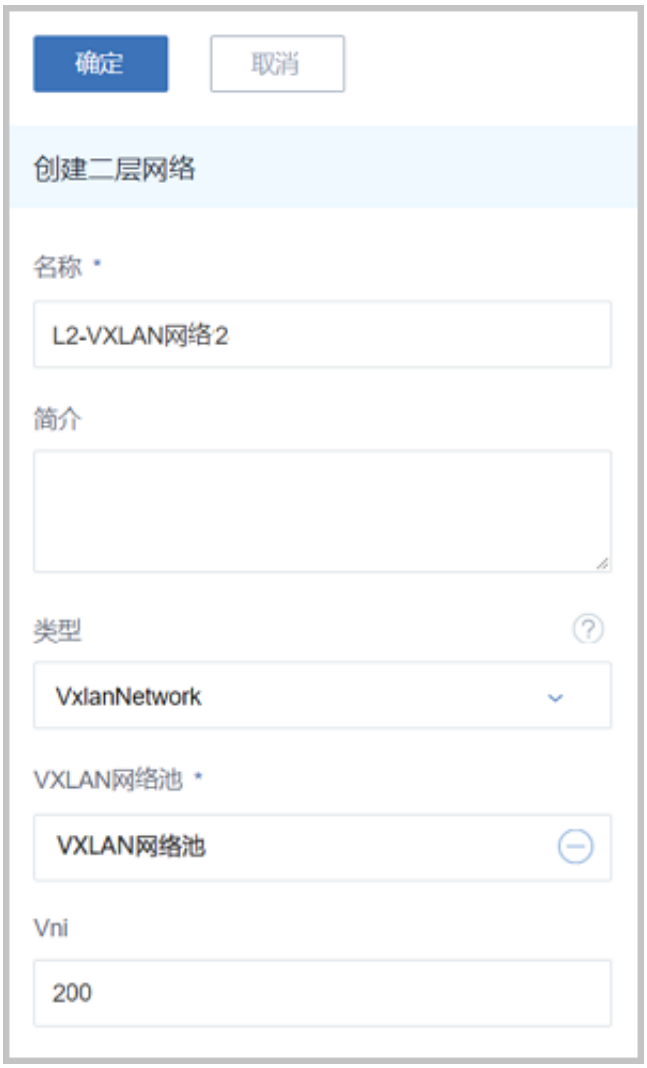
10.基于VXLAN网络池创建VXLAN网络2（虚拟的L2-私有网络）。

在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *9:* 私有网络*2*配置信息填写如下：

- **名称**：设置VXLAN网络2名称，例如L2-VXLAN网络2
- **简介**：可选项，可留空不填
- **类型**：选择VxlanNetwork
- **VXLAN网络池**：选择已创建的VXLAN网络池
- **Vni**：可选项，从VXLAN网络池指定Vni，可在创建VXLAN网络2时直接指定Vni，例如200，也可留空不填，由系统随机指定Vni

如图 *25:* 创建*L2-VXLAN*网络*2*所示，点击**确定**，创建L2-VXLAN网络2。

图 25: 创建L2-VXLAN网络2



11.使用L2-VXLAN网络2创建云路由类型的L3-私有网络2。

在ZStack私有云界面，点击**网络资源** > **三层网络** > **私有网络**，进入**私有网络**界面，点击**创建私有网络**，在弹出的**创建私有网络**界面，参考上述表 *9:* 私有网络2配置信息填写如下：

- **名称**：设置L3-私有网络2名称，例如L3-VXLAN-云路由网络2
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-VXLAN网络2
- **关闭DHCP服务**：选择是否需要DHCP服务

注:

- 默认不勾选，表示启用DHCP服务，为云主机提供自动分配IP，此时DHCP IP支持自定义设置，也可由系统随机指定；

    - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- 网络类型选择**云路由**网络
- **云路由规格**：选择已创建的云路由规格
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.11.0/24*
- **DHCP IP**：可选项，可按需设置DHCP IP

  注:

    - 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP IP；
    - 若三层网络已存在DHCP IP，添加网络段不允许自定义设置DHCP IP；
    - DHCP IP必须在添加的CIDR内，且未被占用；
    - 若留空不填，将由系统在添加的CIDR内随机指定；
    - CIDR内首个IP地址已被默认为网关，不可作为DHCP IP。
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *26: 创建L3-VXLAN-云路由网络2*所示，点击**确定**，创建L3-VXLAN-云路由网络2。

图 26: 创建L3-VXLAN-云路由网络2


确定
取消
创建私有网络
名称 *
L3-VXLAN-云路由网络2
简介
二层网络 *
L2-VXLAN网络2
关闭DHCP服务
扁平网络
云路由
云路由规格 *
云路由规格

12.使用L3-VXLAN-云路由网络1创建云主机VM-1，使用L3-VXLAN-云路由网络2创建云主机VM-2。

基于云路由网络创建云主机，详情可参考本教程基本部署章节。

创建的云主机如图 *27: VM-1、VM-2*所示：

图 27: VM-1、VM-2

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-2	1	1 GB	192.168.11.212	192.168.29.252	Cluster-1	运行中	admin	None
VM-1	1	1 GB	192.168.10.164	192.168.29.252	Cluster-1	运行中	admin	None

13.验证两台云主机的网络连通性。

1. 登录VM-1，用*ping*命令验证网络连通性：

   预期结果：

   - ping baidu.com：可以成功
   - ping VM-2：会失败（两套VXLAN-云路由环境二层隔离）

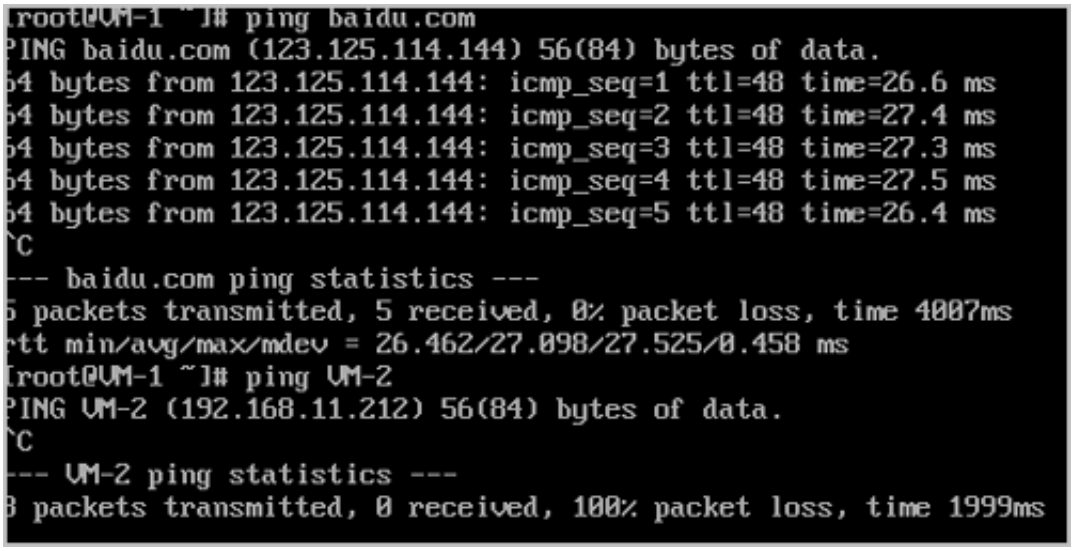
   注:

在VM-1系统中，手动添加VM-2的IP地址到*/etc/hosts*文件路径下。

```
[root@VM-web ~]# vim /etc/hosts
...
192.168.11.212 VM-2
...
```

实际结果如图 *28:* 验证*VM-1*网络连通性所示：

图 28: 验证VM-1网络连通性



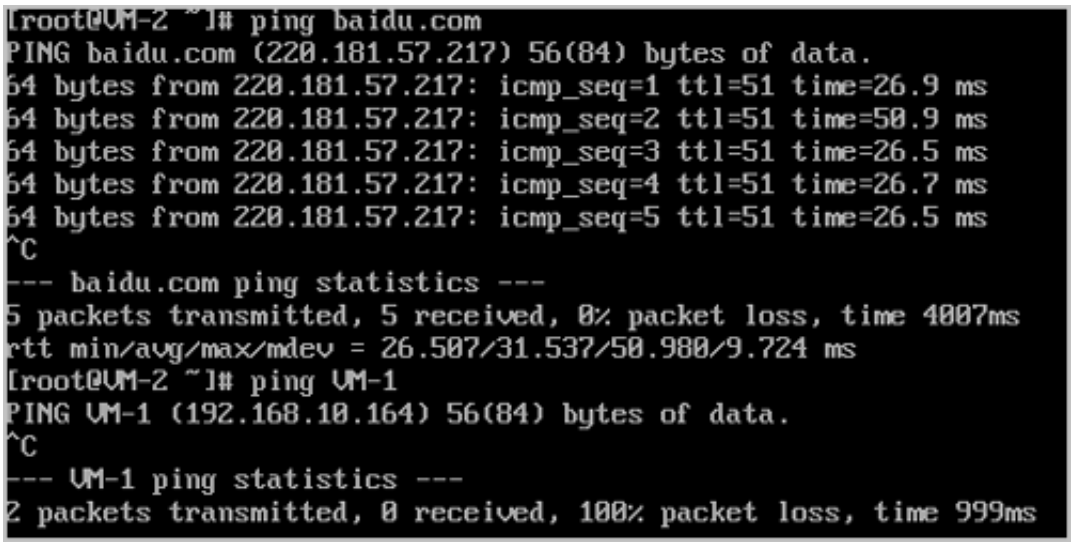
2. 登录VM-2，用*ping*命令验证网络连通性：

   预期结果：

   - ping baidu.com：可以成功
   - ping VM-1：会失败（两套VXLAN-云路由环境二层隔离）

   实际结果如图 *29:* 验证*VM-2*网络连通性所示：

   图 29: 验证VM-2网络连通性



14.通过配置路由表，可让二层隔离的云主机VM-1与VM-2互相访问。

a) 创建路由表。

在ZStack私有云界面，点击**网络资源** > **路由资源** > **路由表**，进入**路由表**界面，点击**创建路由表**，在弹出的**创建路由表**界面，可参考以下示例输入相应内容：

- **名称**：设置路由表名称
- **简介**：可选项，可留空不填
- **路由器**：选择VM-1、VM-2相应的云路由器

如图 *30:* 创建路由表所示：

图 30: 创建路由表

b) 添加两条自定义路由条目。

	目标网段	**下一跳**
自定义路由条目1	VM-2相应的云路由器挂载的私有网络CIDR	VM-2相应的云路由器的公网IP
自定义路由条目2	VM-1相应的云路由器挂载的私有网络CIDR	VM-1相应的云路由器的公网IP

在**路由表**界面，点击已创建的路由表，进入路由表详情页，点击**路由条目**，进入**路由条目**界面，点击**操作** > **添加路由条目**，弹出**添加路由条目**界面，可依次添加上述两条自定义路由条目。

如图 *31:* 添加两条自定义路由条目所示：

图 31: 添加两条自定义路由条目

c) 验证两台云主机的网络连通性。

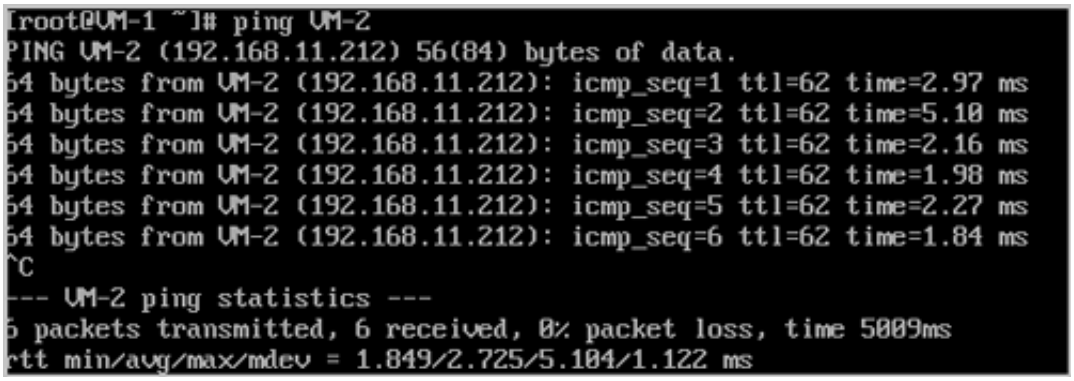
1. 登录VM-1，验证是否*ping*通VM-2：

   预期结果：

   - ping VM-2：成功（通过配置的路由表进行转发）

   实际结果如图 *32: VM-1 ping通 VM-2*所示：

   图 32: VM-1 ping通 VM-2



2. 登录VM-2，验证是否*ping*通VM-1：

   预期结果：

   - ping VM-1：成功（通过配置的路由表进行转发）

   实际结果如图 *33: VM-2 ping通 VM-1*所示：

   图 33: VM-2 ping通 VM-1

```
[root@VM-2 ~]# ping VM-1
PING VM-1 (192.168.10.164) 56(84) bytes of data.
64 bytes from VM-1 (192.168.10.164): icmp_seq=1 ttl=62 time=4.73 ms
64 bytes from VM-1 (192.168.10.164): icmp_seq=2 ttl=62 time=1.86 ms
64 bytes from VM-1 (192.168.10.164): icmp_seq=3 ttl=62 time=1.59 ms
64 bytes from VM-1 (192.168.10.164): icmp_seq=4 ttl=62 time=2.11 ms
64 bytes from VM-1 (192.168.10.164): icmp_seq=5 ttl=62 time=2.23 ms
^C
--- VM-1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4007ms
rtt min/avg/max/mdev = 1.596/2.507/4.730/1.134 ms
```

至此，基于VXLAN-云路由网络提供多租户隔离的部署实践介绍完毕。

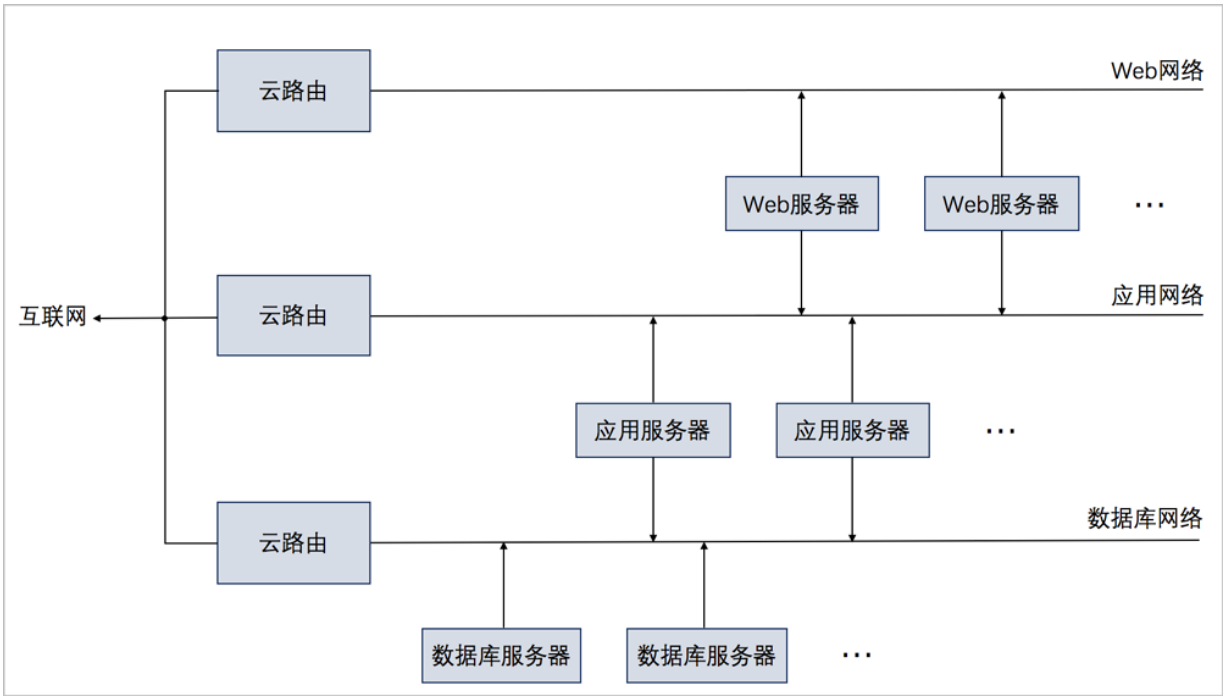
4.2 多层Web服务器

前提条件

基于云路由类型的三层网络架构，可提供多层Web服务器的三层隔离部署。例如，可将网页服务器、应用服务器、数据库服务器分别部署在不同的网络层面，即：展示层、应用层、数据库层，从而保证网络隔离和安全。

多层Web服务器网络架构如图 *34: 多层Web服务器网络架构图*所示：

图 34: 多层Web服务器网络架构图



背景信息

云路由环境下部署多层Web服务器的基本流程：

1. 分别搭建三个云路由类型的三层网络：Web网络、应用网络、数据库网络。

   注: 三个云路由网络的私有网络段不可重叠。

2. 基于三个云路由网络分别创建三台云主机：VM-web、VM-app、VM-database。

   - VM-web：加载两张网卡，一张接入Web网络，一张接入应用网络
   - VM-app：加载两张网卡，一张接入应用网络，一张接入数据库网络
   - VM-database：加载一张网卡，仅接入数据库网络

3. 验证三台云主机的网络连通性。

假定客户环境如下：

1. 公有网络

表 10: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.108.12.0~10.108.13.255*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

表 11: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.10~192.168.29.20*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. Web网络（云路由网络1）

表 12: Web网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2850
IP CIDR	*192.168.10.0/24*

4. 应用网络（云路由网络2）

表 13: 应用网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2860
IP CIDR	*192.168.11.0/24*

5. 数据库网络（云路由网络3）

表 14: 数据库网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2870
IP CIDR	*192.168.12.0/24*

以下介绍云路由环境下部署多层Web服务器的实践步骤。

操作步骤

1. 分别搭建三个云路由类型的三层网络：Web网络、应用网络、数据库网络，详情可参考本教程基本部署章节。

注: 三个云路由网络的私有网络段不可重叠。

搭建的三个云路由网络如图 *35:* 三个云路由网络所示：

图 35: 三个云路由网络

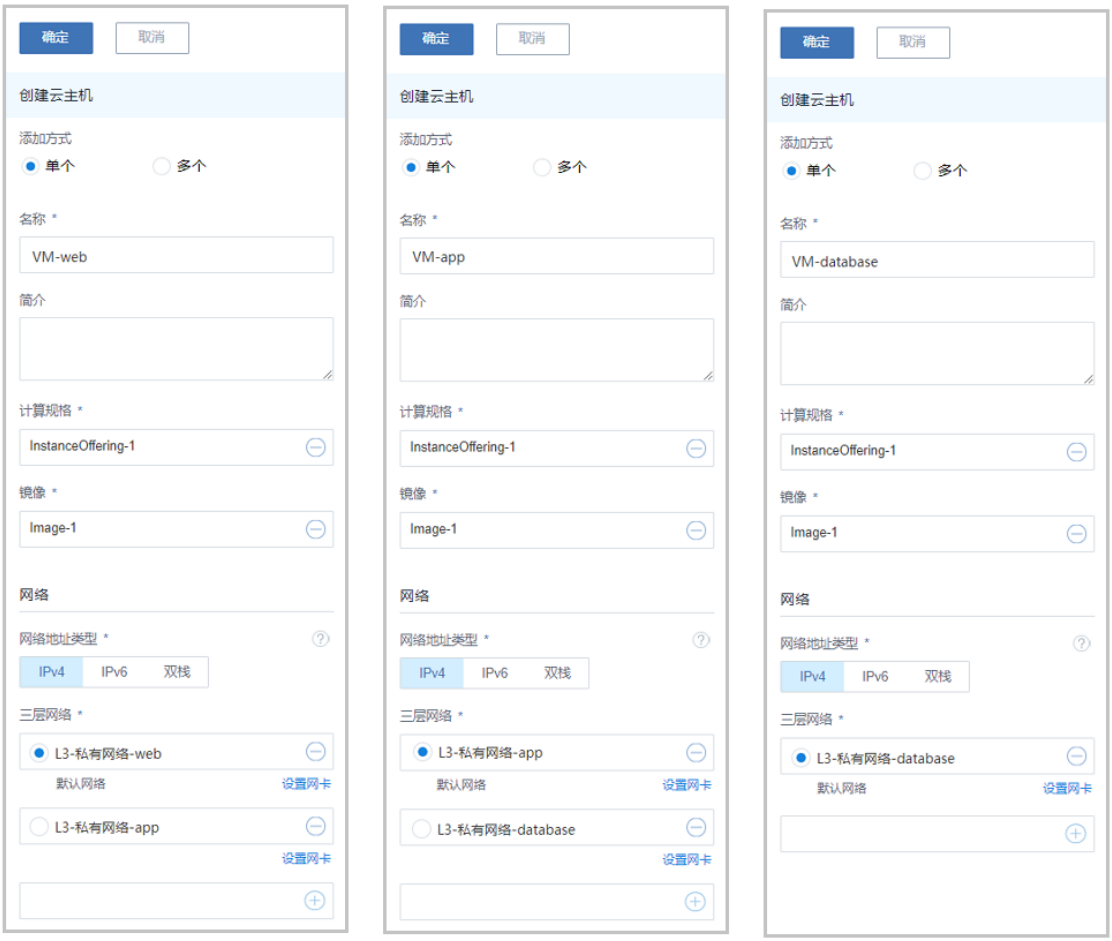
名称	网络类型	IP可用量/总额	CIDR	DHCP IP
L3-私有网络-database	云路由	250 / 253	192.168.12.0/24	192.168.12.196
L3-私有网络-app	云路由	250 / 253	192.168.11.0/24	192.168.11.187
L3-私有网络-web	云路由	251 / 253	192.168.10.0/24	192.168.10.93

2. 基于三个云路由网络分别创建三台云主机：VM-web、VM-app、VM-database。

   如图 *36:* 创建三台云主机所示：

   - VM-web：加载两张网卡，一张接入Web网络（默认），一张接入应用网络
   - VM-app：加载两张网卡，一张接入应用网络（默认），一张接入数据库网络
   - VM-database：加载一张网卡，仅接入数据库网络（默认）

   图 36: 创建三台云主机



基于云路由网络创建云主机，详情可参考本教程基本部署章节。

创建的云主机如图 *37: VM-web、VM-app、VM-database*所示：

图 37: VM-web、VM-app、VM-database

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-database	1	1 GB	192.168.12.222	192.168.29.68	Cluster-1	运行中	admin	None
VM-app	1	1 GB	192.168.11.208	192.168.29.68	Cluster-1	运行中	admin	None
VM-web	1	1 GB	192.168.10.153	192.168.29.68	Cluster-1	运行中	admin	None

注:

- 云主机加载多网卡，可在创建云主机时直接加载多网卡，也可在创建云主机后再加载其它网卡。
- 本例中使用了CentOS 7.2镜像，云主机加载多网卡后，需自行配置网卡信息。

以VM-web为例：

```
[root@VM-web ~]# ip r
default via 192.168.10.1 dev eth0
192.168.10.0/24 dev eth0 proto kernel scope link src 192.168.10.153
# 配置eth1网卡信息
[root@VM-web ~]# cd /etc/sysconfig/network-scripts/
[root@VM-web network-scripts]# vim ifcfg-eth1
...
TYPE=Ethernet
BOOTPROTO=dhcp
NAME=eth1
DEVICE=eth1
ONBOOT=yes
...
# 重启网络服务生效
[root@VM-web network-scripts]# systemctl restart network
[root@VM-web network-scripts]# ip r
default via 192.168.10.1 dev eth0
169.254.0.0/16 dev eth0 scope link metric 1002
169.254.0.0/16 dev eth1 scope link metric 1003
192.168.10.0/24 dev eth0 proto kernel scope link src 192.168.10.153
192.168.11.0/24 dev eth1 proto kernel scope link src 192.168.11.153
```

3. 验证三台云主机的网络连通性。

    1. 登录VM-web，用*ping*命令验证网络连通性：

        预期结果：

        - ping baidu.com：可以成功
        - ping VM-app：可以成功
        - ping VM-database：会失败（不可访问数据库网络）

        注:

        在VM-web系统中，手动添加VM-app、VM-database的IP地址到*/etc/hosts*文件路径下。

        ```
        [root@VM-web ~]# vim /etc/hosts
        ...
        192.168.11.208 VM-app
        192.168.12.222 VM-database
        ...
        ```

        实际结果如图 *38:* 验证*VM-web*网络连通性所示：

        图 38: 验证VM-web网络连通性

```
[root@VM-web ~]# ip r
default via 192.168.10.1 dev eth0
169.254.0.0/16 dev eth0  scope link  metric 1002
169.254.0.0/16 dev eth1  scope link  metric 1003
192.168.10.0/24 dev eth0  proto kernel  scope link  src 192.168.10.153
192.168.11.0/24 dev eth1  proto kernel  scope link  src 192.168.11.153
[root@VM-web ~]# ping baidu.com
PING baidu.com (220.181.57.217) 56(84) bytes of data.
64 bytes from 220.181.57.217: icmp_seq=1 ttl=50 time=26.9 ms
64 bytes from 220.181.57.217: icmp_seq=2 ttl=50 time=26.8 ms
64 bytes from 220.181.57.217: icmp_seq=3 ttl=50 time=26.4 ms
64 bytes from 220.181.57.217: icmp_seq=4 ttl=50 time=26.6 ms
^C
--- baidu.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 26.480/26.737/26.981/0.219 ms
[root@VM-web ~]# ping VM-app
PING VM-app (192.168.11.208) 56(84) bytes of data.
64 bytes from VM-app (192.168.11.208): icmp_seq=1 ttl=64 time=2.68 ms
64 bytes from VM-app (192.168.11.208): icmp_seq=2 ttl=64 time=0.744 ms
64 bytes from VM-app (192.168.11.208): icmp_seq=3 ttl=64 time=0.865 ms
64 bytes from VM-app (192.168.11.208): icmp_seq=4 ttl=64 time=0.624 ms
^C
--- VM-app ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 0.624/1.229/2.685/0.845 ms
[root@VM-web ~]# ping VM-database
PING VM-database (192.168.12.222) 56(84) bytes of data.
^C
--- VM-database ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 4999ms
```

2. 同理，登录VM-app，用*ping*命令验证网络连通性：

   预期结果：

   - ping baidu.com：可以成功
   - ping VM-web：可以成功
   - ping VM-database：可以成功

   实际结果如图 *39: 验证VM-app网络连通性*所示：

图 39: 验证VM-app网络连通性

```
[root@VM-app ~]# ip r
default via 192.168.11.1 dev eth1
169.254.0.0/16 dev eth0  scope link  metric 1002
169.254.0.0/16 dev eth1  scope link  metric 1003
192.168.11.0/24 dev eth1  proto kernel  scope link  src 192.168.11.208
192.168.12.0/24 dev eth0  proto kernel  scope link  src 192.168.12.208
[root@VM-app ~]# ping baidu.com
PING baidu.com (111.13.101.208) 56(84) bytes of data.
64 bytes from 111.13.101.208: icmp_seq=1 ttl=48 time=37.2 ms
64 bytes from 111.13.101.208: icmp_seq=2 ttl=48 time=33.6 ms
64 bytes from 111.13.101.208: icmp_seq=3 ttl=48 time=33.4 ms
64 bytes from 111.13.101.208: icmp_seq=4 ttl=48 time=33.6 ms
^C
--- baidu.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 33.464/34.490/37.227/1.592 ms
[root@VM-app ~]# ping VM-web
PING VM-web (192.168.11.153) 56(84) bytes of data.
64 bytes from VM-web (192.168.11.153): icmp_seq=1 ttl=64 time=2.41 ms
64 bytes from VM-web (192.168.11.153): icmp_seq=2 ttl=64 time=0.672 ms
64 bytes from VM-web (192.168.11.153): icmp_seq=3 ttl=64 time=1.27 ms
64 bytes from VM-web (192.168.11.153): icmp_seq=4 ttl=64 time=1.53 ms
^C
--- VM-web ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3006ms
rtt min/avg/max/mdev = 0.672/1.475/2.418/0.628 ms
[root@VM-app ~]# ping VM-database
PING VM-database (192.168.12.222) 56(84) bytes of data.
64 bytes from VM-database (192.168.12.222): icmp_seq=1 ttl=64 time=2.10 ms
64 bytes from VM-database (192.168.12.222): icmp_seq=2 ttl=64 time=0.654 ms
64 bytes from VM-database (192.168.12.222): icmp_seq=3 ttl=64 time=0.920 ms
64 bytes from VM-database (192.168.12.222): icmp_seq=4 ttl=64 time=0.752 ms
^C
--- VM-database ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 0.654/1.107/2.102/0.582 ms
```

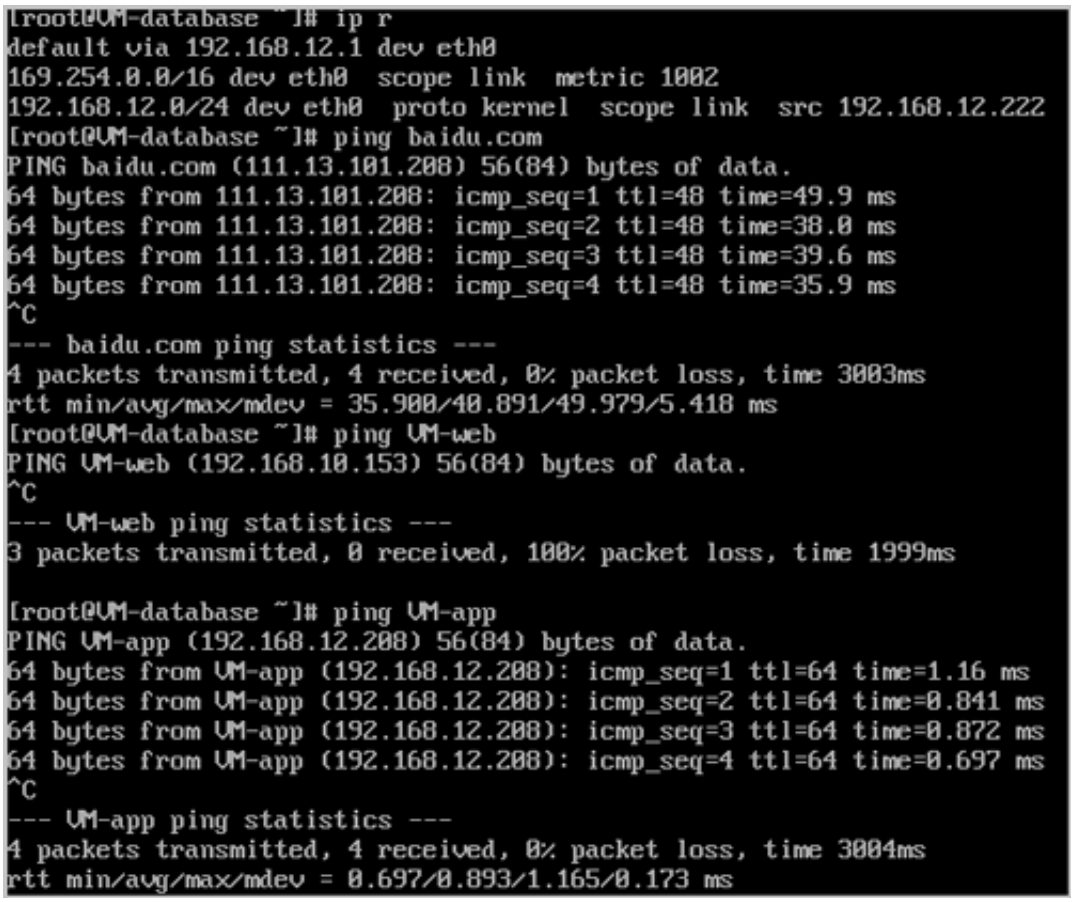
3. 登录VM-database，用*ping*命令验证网络连通性：

   预期结果：

   - ping baidu.com：可以成功
   - ping VM-web：会失败（不可访问Web网络）
   - ping VM-app：可以成功

   实际结果如图 *40: 验证VM-database网络连通性*所示：

图 40: 验证VM-database网络连通性



至此，多层Web服务器的部署实践介绍完毕。

4.3 多公网

前提条件

通过给云路由器添加多公网，并配置相关路由表和路由条目，可实现多公网场景。例如，本地机房的业务云主机与阿里云上的业务云主机互通，且与异地机房的业务云主机互通。

背景信息

本场景中，本地机房部署一套ZStack私有云环境，通过IPsec VPN方式实现本地云路由网络与阿里云VPN网络互通；同时异地机房部署另一套ZStack私有云环境，通过给本地云路由器添加多公网，并配置双向路由，实现本地云路由网络与异地机房云路由网络的互通。

基于云路由网络部署多公网场景的基本流程：

1. 本地机房部署一套ZStack私有云环境，并依次搭建公有网络（用于与阿里云互通）、管理网络、私有网络（云路由类型）。

2. 使用本地云路由网络创建一台业务云主机：VM-业务-本地机房，创建云主机过程中会自动创建云路由器。
3. 在阿里云上创建一台ECS业务云主机：ECS-业务-阿里云。
4. 搭建IPsec VPN隧道，实现本地云路由网络与阿里云VPN网络的互通。
5. 验证本地业务云主机与阿里云上的ECS业务云主机是否互通。
6. 在本地ZStack环境里，搭建另一套公有网络（用于与异地机房互通），并将该公有网络加载到本地业务云主机对应的云路由器上。
7. 异地机房部署另一套ZStack私有云环境，并依次搭建公有网络（用于与本地机房互通）、管理网络、私有网络（云路由类型）。
8. 使用异地机房云路由网络创建一台业务云主机：VM-业务-异地机房。
9. 在本地机房与异地机房之间配置双向路由。
10. 验证本地业务云主机与异地机房的业务云主机是否互通。

假定客户环境如下：

- 本地机房：

  1. 公有网络（用于与阿里云互通）

     表 15: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	3
IP地址段	*180.169.211.117~180.169.211.118*
子网掩码	*255.255.255.240*
网关	*180.169.211.113*

  2. 管理网络

     表 16: 管理网络配置信息

管理网络	配置信息
网卡	em03
VLAN ID	非VLAN
IP地址段	*192.168.210.10~192.168.210.20*

管理网络	配置信息
子网掩码	*255.255.240.0*
网关	*192.168.208.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. 私有网络

表 17: 私有网络配置信息

私有网络	值
网卡	em01
VLAN ID	1982
IP CIDR	*172.31.0.0/18*

4. 公有网络（用于与异地机房互通）

表 18: 公有网络配置信息

公有网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*10.0.108.10~10.0.108.20*
子网掩码	*255.255.0.0*
网关	*10.0.0.1*

- 阿里云端：

1. 已购买的阿里云VPN网关IP地址为*106.14.13.45*
2. 阿里云VPN网关所在的VPC的CIDR为*192.168.0.0/16*

- 异地机房：

1. 公有网络（用于与本地机房互通）

表 19: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.0.108.100~10.0.108.110*
子网掩码	*255.255.0.0*
网关	*10.0.0.1*

2. 管理网络

表 20: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.30~192.168.29.40*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

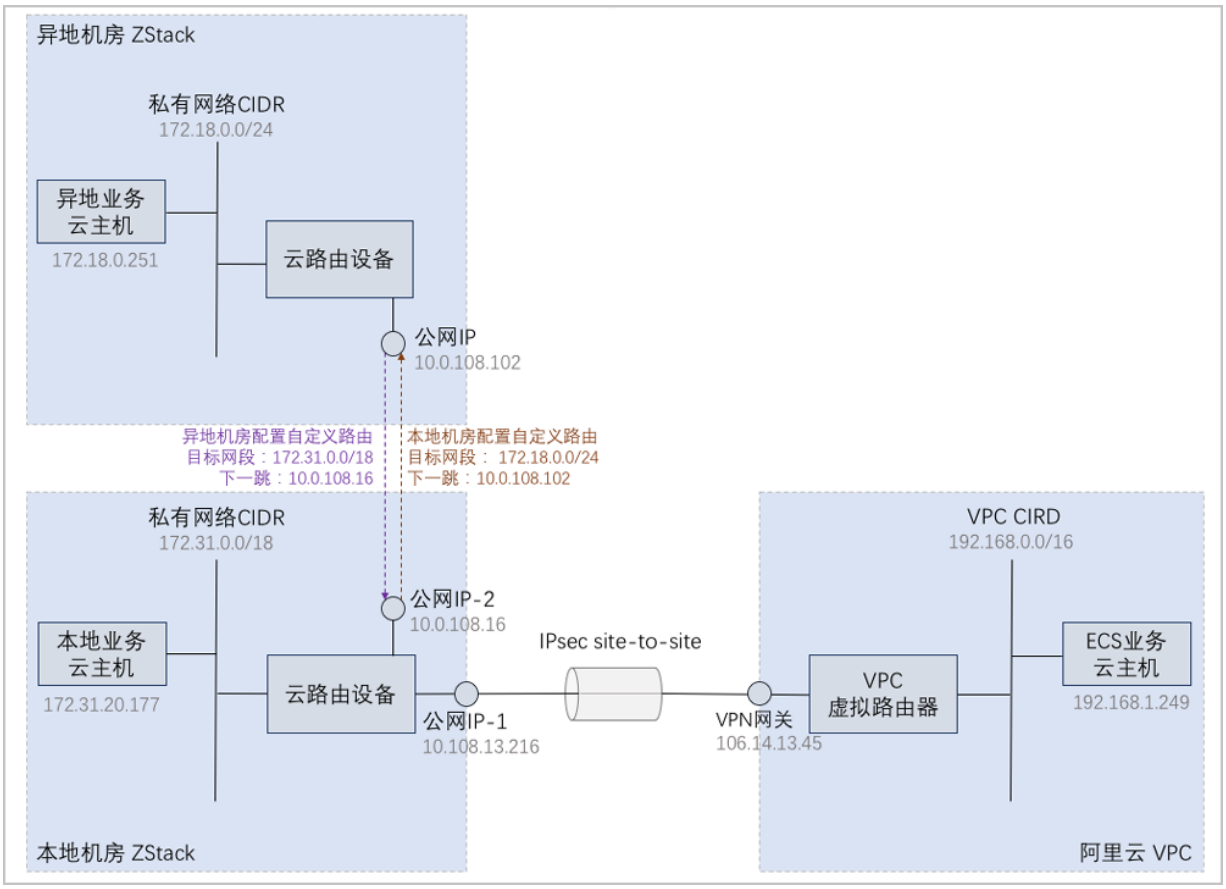
3. 私有网络

表 21: 私有网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2200
IP CIDR	172.18.0.10/24

多公网场景网络架构如图 *41: 多公网场景网络架构图*所示：

图 41: 多公网场景网络架构图



以下介绍基于云路由网络部署多公网场景的实践步骤。

操作步骤

1. 本地机房部署一套ZStack私有云环境，并依次搭建公有网络（用于与阿里云互通）、管理网络、私有网络（云路由类型）。

   详情可参考本教程基本部署章节。

   搭建的公有网络（用于与阿里云互通）、管理网络、云路由网络如图 *42:* 公有网络-用于与阿里云互通、图 *43:* 管理网络和图 *44:* 云路由网络所示：

   图 42: 公有网络-用于与阿里云互通

名称	网络类型	IP可用量/总额	CIDR	DHCP IP
L3-公有网络-混合云VPN	公有网络	1 / 2	180.169.211.113/28	

   图 43: 管理网络

名称	网络类型	IP可用量/总额	CIDR
L3-管理网络	系统网络	10 / 11	192.168.208.1/20

图 44: 云路由网络

名称	网络类型	IP可用量/总额	CIDR	DHCP IP
L3-私有网络-云路由-本地机房	云路由	16379 / 16381	172.31.0.0/18	172.31.4.254

2. 使用本地云路由网络创建一台业务云主机：VM-业务-本地机房，创建云主机过程中会自动创建云路由器。

   基于云路由网络创建云主机，详情可参考本教程基本部署章节。

   创建的本地业务云主机如图 *45: 本地业务云主机*所示：

   图 45: 本地业务云主机

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-业务-本地机房	1	1 GB	172.31.20.177	192.168.210.42	Cluster-1	运行中	admin	None

3. 在阿里云上创建一台ECS业务云主机：ECS-业务-阿里云。

   创建ECS云主机，详情请参考《混合云使用教程》的**创建ECS云主机**章节。

   创建的ECS业务云主机如图 *46: ECS业务云主机*所示：

   图 46: ECS业务云主机

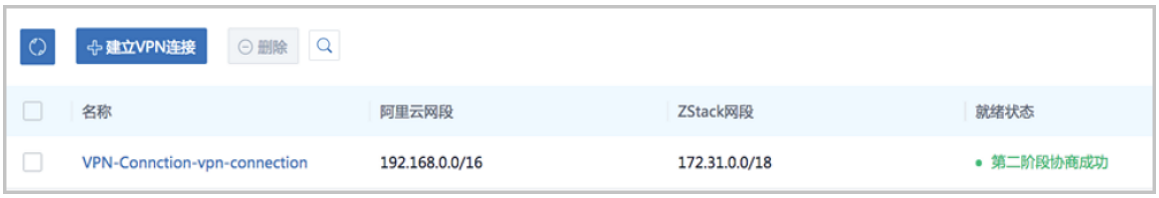
名称	ECS云主机ID	处理器	内存	私网IP	公网IP	付费信息	VPC	可用区	安全组	启用状态
ECS-业务-阿里云	i-uf6a0elu320ruf8...	1	1G	192.168.1.249		后付费	test-for-ipsec	华东 2 可用区 D	安全组-允许所有	运行中

4. 搭建IPsec VPN隧道，实现本地云路由网络与阿里云VPN网络的互通。

   可利用操作向导快速创建阿里云VPN连接，详情请参考《混合云使用教程》的**IPsec VPN实践**章节。

   搭建的IPsec VPN隧道如图 *47: IPsec VPN隧道搭建完成*所示：

   图 47: IPsec VPN隧道搭建完成



注:

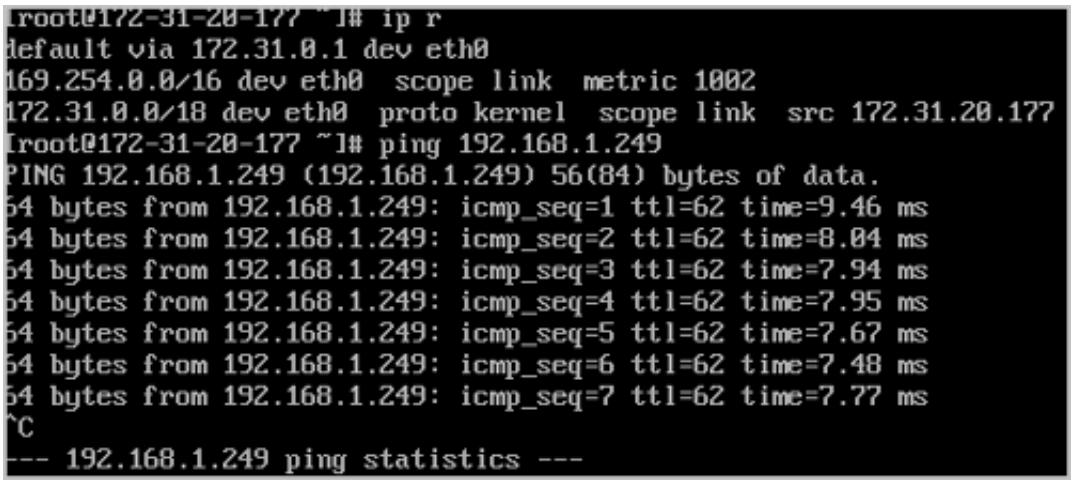
VPN连接的**就绪状态**显示为**第二阶段协商成功**，表示IPsec VPN隧道搭建完成，只有互通验证通过，IPsec VPN隧道才创建成功。

5. 验证本地业务云主机与阿里云上的ECS业务云主机是否互通。

a) 登录本地业务云主机，检查是否能够ping通ECS业务云主机。

如图 *48:* 本地业务云主机 *ping*通 *ECS*业务云主机所示：

图 48: 本地业务云主机 ping通 ECS业务云主机



b) 登录ECS业务云主机，检查是否能够ping通本地业务云主机。

如图 *49: ECS*业务云主机 *ping*通 本地业务云主机所示：

图 49: ECS业务云主机 ping通 本地业务云主机

```
[root@zstack]# ip r
default via 192.168.1.253 dev eth0  metric 10
192.168.1.0/24 dev eth0  src 192.168.1.249
[root@zstack]# ping 172.31.20.177
PING 172.31.20.177 (172.31.20.177): 56 data bytes
64 bytes from 172.31.20.177: seq=0 ttl=62 time=7.689 ms
64 bytes from 172.31.20.177: seq=1 ttl=62 time=8.361 ms
64 bytes from 172.31.20.177: seq=2 ttl=62 time=7.835 ms
64 bytes from 172.31.20.177: seq=3 ttl=62 time=7.628 ms
64 bytes from 172.31.20.177: seq=4 ttl=62 time=7.607 ms
64 bytes from 172.31.20.177: seq=5 ttl=62 time=8.495 ms
64 bytes from 172.31.20.177: seq=6 ttl=62 time=8.963 ms
^C
--- 172.31.20.177 ping statistics ---
```

6. 在本地ZStack环境里，搭建另一套公有网络（用于与异地机房互通），并将该公有网络加载到本地业务云主机对应的云路由器上。

   a) 在本地ZStack环境里，搭建另一套公有网络（用于与异地机房互通）。

   详情可参考本教程基本部署章节。

   搭建的公有网络（用于与异地机房互通）如图 *50:* 公有网络-用于与异地机房互通所示：

   图 50: 公有网络-用于与异地机房互通

   b) 将公有网络（用于与异地机房互通）加载到本地业务云主机对应的云路由器上。

   在ZStack私有云主菜单，点击**网络资源** > **路由资源** > **云路由器**，进入**云路由器**界面，选择本地业务云主机对应的云路由器，展开其详情页，点击**配置信息**，进入**配置信息**子页面，点击**操作** > **加载**，将公有网络（用于与异地机房互通）加载到该云路由器上。

   如图 *51:* 云路由器加载多公网所示：

   图 51: 云路由器加载多公网

7. 异地机房部署另一套ZStack私有云环境，并依次搭建公有网络（用于与本地机房互通）、管理网络、私有网络（云路由类型）。

   详情可参考本教程基本部署章节。

   搭建的公有网络（用于与本地机房互通）、管理网络、云路由网络如图 *52:* 公有网络-用于与本地机房互通、图 *53:* 管理网络和图 *54:* 云路由网络所示：

图 52: 公有网络-用于与本地机房互通

图 53: 管理网络

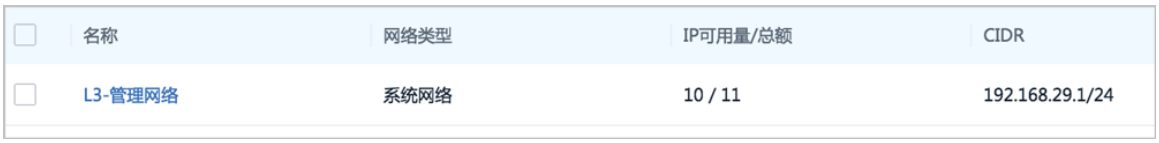


图 54: 云路由网络

8. 使用异地机房云路由网络创建一台业务云主机：VM-业务-异地机房。

   基于云路由网络创建云主机，详情可参考本教程基本部署章节。

   创建的异地业务云主机如图 *45:* 本地业务云主机所示：

图 55: 异地业务云主机

9. 在本地机房与异地机房之间配置双向路由。

在本地机房配置路由表和路由条目。

a) 创建路由表。

在ZStack私有云主菜单，点击**网络资源** > **路由资源** > **路由表**，进入**路由表**界面，点击**创建路由表**，在弹出的**创建路由表**界面，可参考以下示例输入相应内容：

- **名称**：设置路由表名称
- **简介**：可选项，可留空不填
- **路由器**：选择本地业务云主机对应的云路由器

b) 添加自定义路由条目。

	目标网段	下一跳
自定义路由条目	异地业务云主机对应的云路由器挂载的私有网络CIDR	异地业务云主机对应的云路由器的公网IP

在**路由表**界面，点击已创建的路由表，进入路由表详情页，点击**路由条目**，进入**路由条目**界面，点击**操作** > **添加路由条目**，弹出**添加路由条目**界面，可添加上述自定义路由条目。

如图 *56:* 本地机房配置路由所示：

图 56: 本地机房配置路由

同理，在异地机房配置路由表和路由条目，如图 *57:* 异地机房配置路由所示：

图 57: 异地机房配置路由

10.验证本地业务云主机与异地机房的业务云主机是否互通。

a) 登录本地业务云主机，检查是否能够ping通异地业务云主机。

如图 *58:* 本地业务云主机 *ping*通 异地业务云主机所示：

图 58: 本地业务云主机 ping通 异地业务云主机

```
[root@172-31-20-177 ~]# ip r
default via 172.31.0.1 dev eth0
169.254.0.0/16 dev eth0  scope link  metric 1002
172.31.0.0/18 dev eth0  proto kernel  scope link  src 172.31.20.177
[root@172-31-20-177 ~]# ping 172.18.0.251
PING 172.18.0.251 (172.18.0.251) 56(84) bytes of data.
64 bytes from 172.18.0.251: icmp_seq=1 ttl=62 time=3.72 ms
64 bytes from 172.18.0.251: icmp_seq=2 ttl=62 time=2.54 ms
64 bytes from 172.18.0.251: icmp_seq=3 ttl=62 time=3.44 ms
64 bytes from 172.18.0.251: icmp_seq=4 ttl=62 time=4.48 ms
64 bytes from 172.18.0.251: icmp_seq=5 ttl=62 time=3.65 ms
64 bytes from 172.18.0.251: icmp_seq=6 ttl=62 time=1.62 ms
^C
--- 172.18.0.251 ping statistics ---
```

b) 登录异地业务云主机，检查是否能够ping通本地业务云主机。

如图 *59:* 异地业务云主机 *ping*通 本地业务云主机所示：

图 59: 异地业务云主机 ping通 本地业务云主机

```
[root@172-18-0-251 ~]# ip r
default via 172.18.0.1 dev eth0
169.254.0.0/16 dev eth0  scope link  metric 1002
172.18.0.0/24 dev eth0  proto kernel  scope link  src 172.18.0.251
[root@172-18-0-251 ~]# ping 172.31.20.177
PING 172.31.20.177 (172.31.20.177) 56(84) bytes of data.
64 bytes from 172.31.20.177: icmp_seq=1 ttl=62 time=4.87 ms
64 bytes from 172.31.20.177: icmp_seq=2 ttl=62 time=2.27 ms
64 bytes from 172.31.20.177: icmp_seq=3 ttl=62 time=3.61 ms
64 bytes from 172.31.20.177: icmp_seq=4 ttl=62 time=3.17 ms
64 bytes from 172.31.20.177: icmp_seq=5 ttl=62 time=2.70 ms
64 bytes from 172.31.20.177: icmp_seq=6 ttl=62 time=2.35 ms
^C
--- 172.31.20.177 ping statistics ---
```

至此，基于云路由网络的多公网场景部署实践介绍完毕。

4.4 安全组

前提条件

安全组：给云主机提供三层网络防火墙控制，控制TCP/UDP/ICMP等数据包进行有效过滤，对指定网络的指定云主机按照指定的安全规则进行有效控制。

- 扁平网络、云路由网络和VPC均支持安全组服务，安全组服务均由安全组网络服务模块提供，使用方法均相同：使用iptables进行云主机防火墙的安全控制。
- 安全组实际上是一个分布式防火墙；每次规则变化、加入/删除网卡都会导致多个云主机上的防火墙规则被更新。

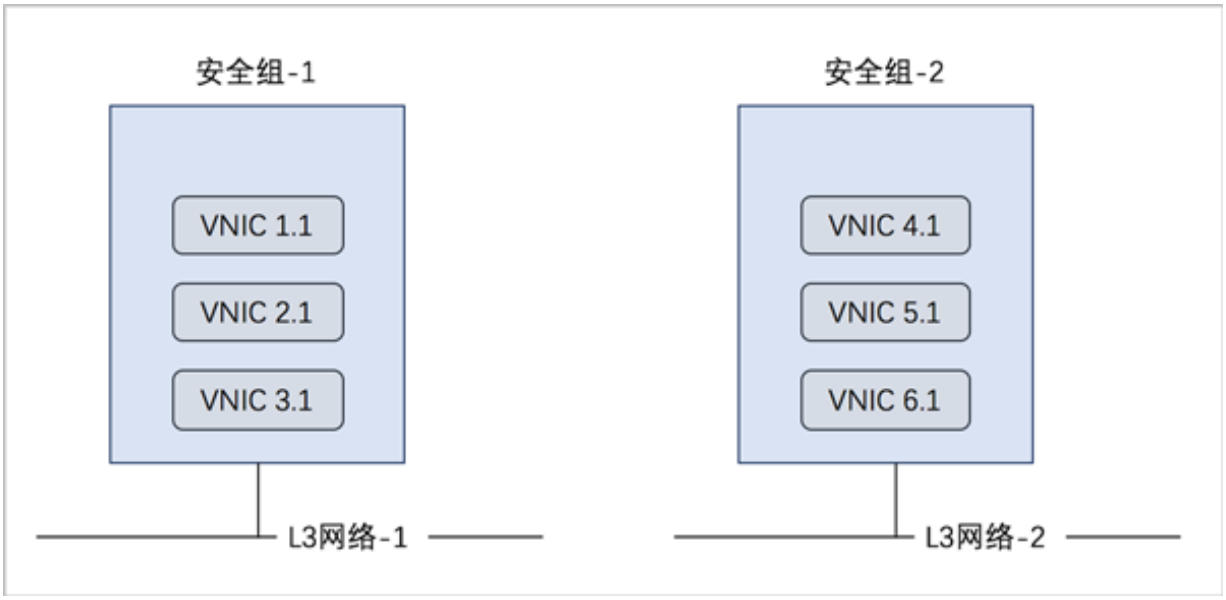
安全组规则：

- 安全组规则按数据包的流向分为两种类型：
  - 入方向（Ingress）：代表数据包从外部进入云主机。
  - 出方向（Egress）：代表数据包从云主机往外部发出。
- 安全组规则对通信协议支持以下类型：
  - ALL：表示涵盖所有协议类型，此时不能指定端口。
  - TCP：支持1-65535端口。
  - UDP：支持1-65535端口。
  - ICMP：默认起始结束端口均为-1，表示支持全部的ICMP协议。
- 安全组规则支持对数据来源的限制，目前源可以设置为CIDR和安全组。
  - CIDR作为源：仅允许指定的CIDR才可通过
  - 安全组作为源：仅允许指定的安全组内的云主机才可通过

注: 如果两者都设置，只取两者交集。

如图 *60:* 安全组所示：

图 60: 安全组



背景信息

使用安全组的基本流程为：选择三层网络，设置相应的防火墙规则，选择指定的云主机加入规则中。

以下介绍云路由环境下安全组的使用方法，包括两个场景：

- 对云主机设置入方向规则；
- 对云主机设置出方向规则。

操作步骤

1. 搭建云路由网络，详情可参考本教程基本部署章节。
2. 使用云路由网络创建三台私有云云主机，例如VM-1、VM-2、VM-3，详情可参考本教程基本部署章节。

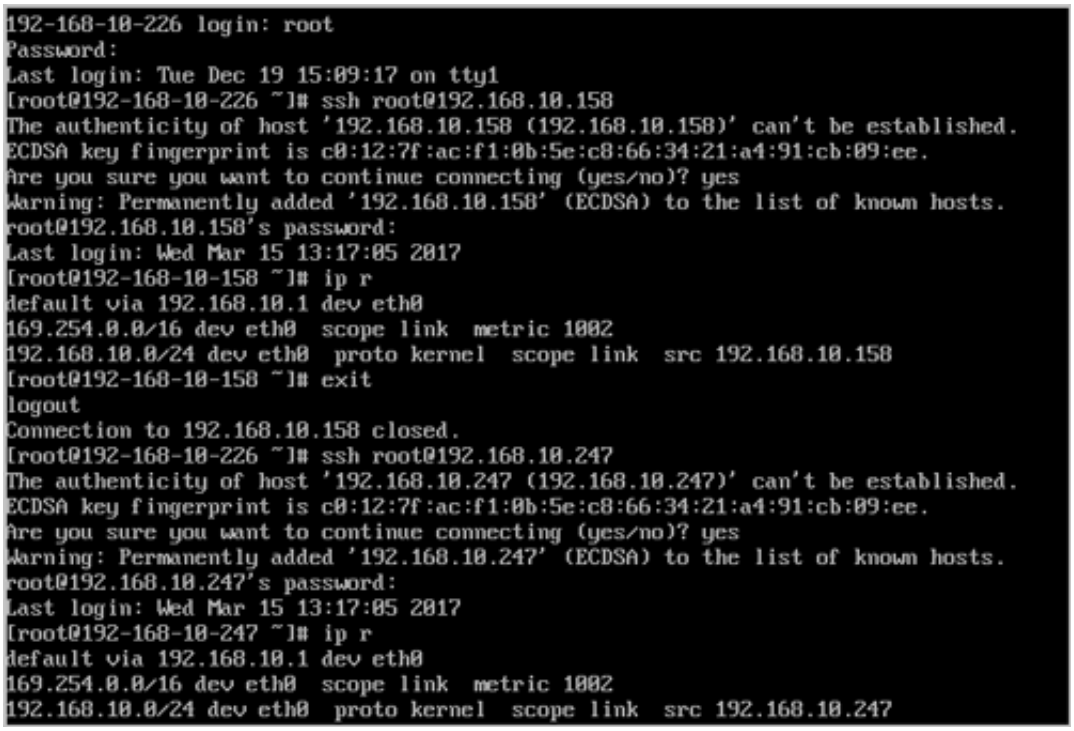
   创建的云主机如图 *61: VM-1、VM-2、VM-3*所示：

   图 61: VM-1、VM-2、VM-3

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-3	1	1 GB	192.168.10.247	10.0.182.41	Cluster-1	运行中	admin	None
VM-2	1	1 GB	192.168.10.158	10.0.182.41	Cluster-1	运行中	admin	None
VM-1	1	1 GB	192.168.10.226	10.0.182.41	Cluster-1	运行中	admin	None

登录VM-1，可通过SSH默认的22端口远程登录VM-2、VM-3，如图 *62: SSH远程登录成功*所示：

图 62: SSH远程登录成功



3. 对VM-2、VM-3设置入方向规则。

   a) 创建安全组。

   在ZStack私有云主菜单，点击 **网络服务** > **安全组**，进入**安全组**界面，点击**创建安全组**，在弹出的**创建安全组**界面，可参考以下示例输入相应内容：

   - **名称**：设置安全组名称
   - **简介**：可选项，可留空不填
   - **网络**：选择已创建的云路由网络
   - **规则**：可选项，防火墙规则可在创建安全组时直接设置，也可在创建安全组后再设置

     本场景以前者为例，详见设置入方向规则。
   - **网卡**：可选项，选择云主机加入安全组，云主机网卡可在创建安全组时直接添加，也可在创建安全组后再添加

     本场景以前者为例，详见选择*VM-2*、*VM-3*加入安全组。

如图 *63:* 创建安全组所示：

图 63: 创建安全组


确定
取消
创建安全组
名称 *
安全组
简介
网络地址类型
IPv4
IPv6
网络 *
L3-云路由
规则
类型: 入方向
协议: TCP
起始端口: 23
结束端口: 1024
CIDR:
源安全组:
网卡
vnic15.0

b) 设置入方向规则。

在**创建安全组**界面，点击**规则**栏里的加号按钮，弹出**设置规则**界面，可参考以下示例输入相应内容：

- **类型**：入方向
- **协议**：TCP
- **开始端口**：23
- **结束端口**：1024
- **CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填
- **源安全组**：可选项，仅允许指定的安全组内的云主机才可通过，可留空不填

如图 *64:* 设置规则所示，点击**确定**，设置入方向规则。

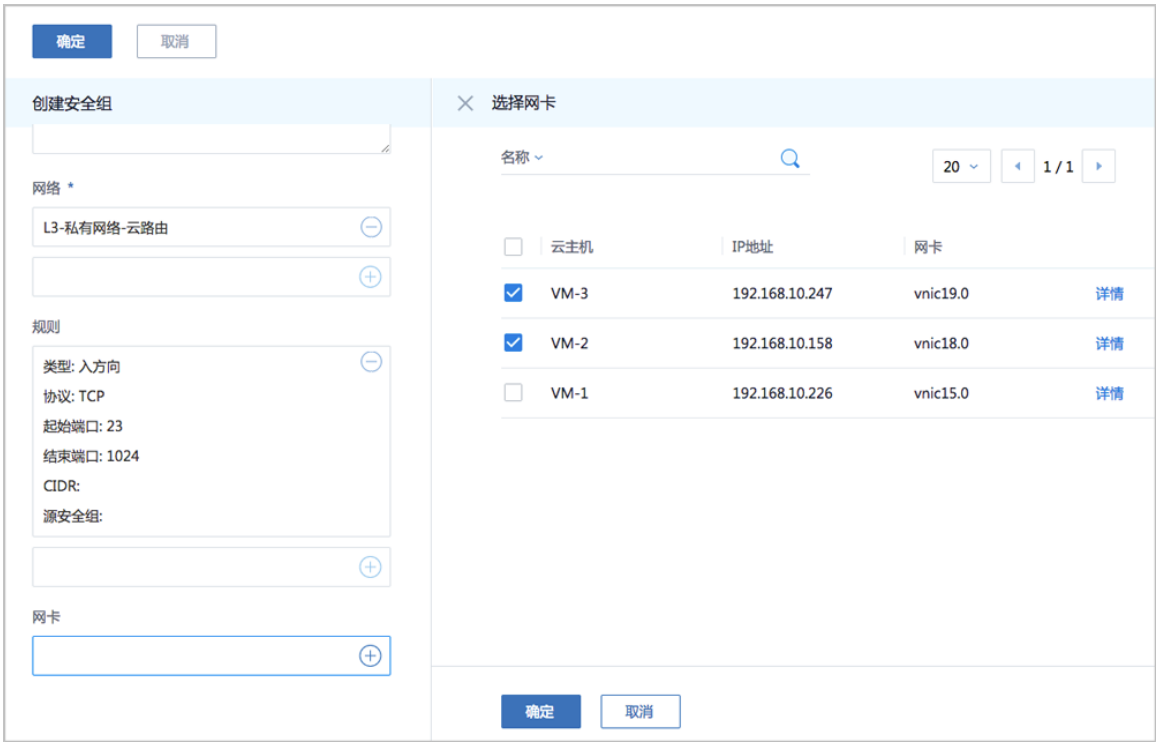
图 64: 设置规则

c) 选择VM-2、VM-3加入安全组。

在**创建安全组**界面，点击**网卡**栏里的加号按钮，弹出**选择网卡**界面，选择VM-2、VM-3。

如图 *65: VM-2、VM-3加入安全组*所示，依次点击**确定**，VM-2、VM-3加入安全组。

图 65: VM-2、VM-3加入安全组



d) 入方向规则验证。

此时VM-2、VM-3只允许外部通过端口23~1024访问。

1. 登录VM-1，尝试SSH默认的22端口远程登录VM-2、VM-3失败。
2. 登录VM-1，尝试使用*nc*命令与VM-2、VM-3建立通信连接。

   例如，使用规则范围内的端口23，VM-1可与VM-2成功通信。

   注: 需将VM-2中原先的iptables规则清除，可使用命令`iptables -F`

   如图 *66: VM-1在端口23向VM-2发送信息*和图 *67: VM-2在端口23接收信息成功*所示：

   图 66: VM-1在端口23向VM-2发送信息

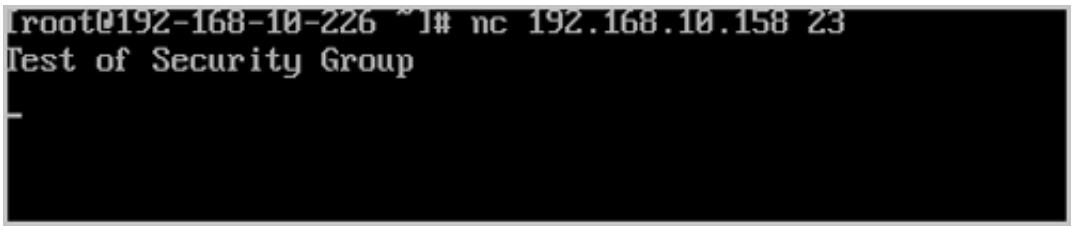
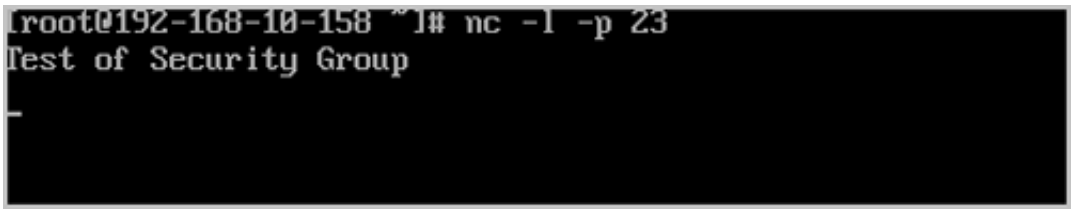


图 67: VM-2在端口23接收信息成功



4. 对VM-2、VM-3设置出方向规则。

a) 添加出方向规则到安全组。

在**安全组**界面，选择已创建的安全组，展开详情页，点击**规则**，进入**规则**子页面，点击**操作** > **添加规则**，添加出方向规则到安全组。

如图 *68:* 添加出方向规则所示：

图 68: 添加出方向规则

b) 设置出方向规则。

弹出**设置规则**界面，可参考以下示例输入相应内容：

- **类型**：出方向
- **协议**：TCP
- **开始端口**：23
- **结束端口**：1024
- **CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填

- **源安全组**：可选项，仅允许指定的安全组内的云主机才可通过，可留空不填

如图 *69:* 设置规则所示，点击**确定**，设置出方向规则。

图 69: 设置规则

c) 出方向规则验证。

此时云主机VM-2、VM-3只允许通过端口23~1024访问外部地址。

1. 登录VM-2或VM-3，尝试使用*nc*命令与VM-1建立通信连接。

   例如，使用规则范围外的端口21，VM-2与VM-1通信失败。

   如图 *70: VM-2*在端口*21*尝试连接*VM-1*失败和图 *71: VM-1*在端口*21*接收信息失败所示：

   图 70: VM-2在端口21尝试连接VM-1失败

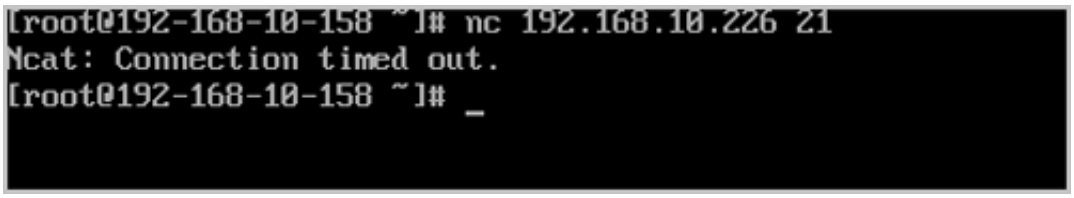


图 71: VM-1在端口21接收信息失败

2. 登录VM-2或VM-3，尝试使用*nc*命令与VM-1建立通信连接。

   例如，使用规则范围内的端口23，VM-2与VM-1通信成功。

   如图 *72: VM-2在端口23向VM-1发送信息*和图 *73: VM-1在端口23接收信息成功*所示：

   图 72: VM-2在端口23向VM-1发送信息

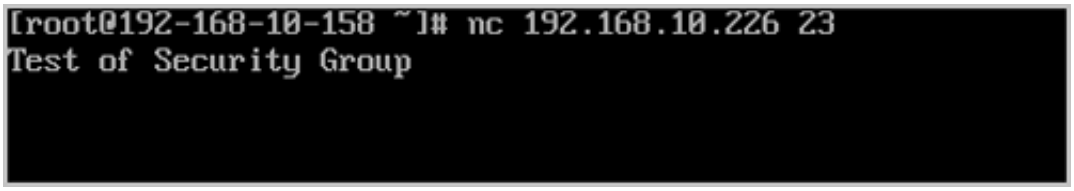


   图 73: VM-1在端口23接收信息成功

后续操作

安全组有以下约束条件：

- 安全组可以挂载到多个云主机，它们会共享相同的安全组规则。
- 安全组可以挂载到多个三层网络，它们会共享相同的安全组规则。
- 安全组支持白名单机制，即设置的所有规则均为允许机制，一旦对指定端口设置了允许机制，那么没有被允许的端口就无法通过。

- 新建安全组时，默认配置了两条规则（即：协议类型为ALL的进口规则和出口规则），用于设置组内互通。用户可以删除这两条默认规则，取消组内互通。
- 新建安全组时，如果没有设置任何规则，则默认所有的外部访问均禁止进入安全组内的云主机，安全组内云主机访问外部不受限制。

至此，安全组的使用方法介绍完毕。

4.5 弹性IP

前提条件

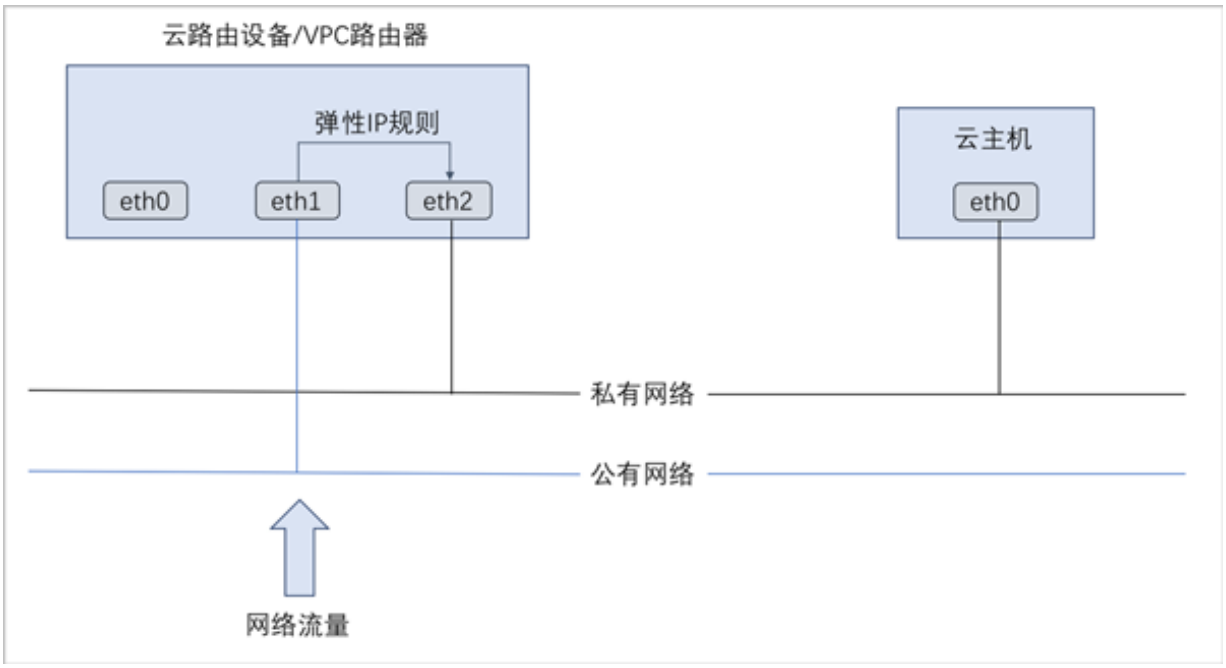
弹性IP（EIP）：定义了通过公有网络访问内部私有网络的方法。

- 内部私有网络是隔离的网络空间，不能直接被外部网络访问。
- 弹性IP基于网络地址转换（NAT），将一个网络（通常是公有网络）的IP地址转换成另一个网络（通常是私有网络）的IP地址；通过弹性IP，可对公网的访问直接关联到内部私网的云主机IP。
- 弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
- 云主机使用的扁平网络、云路由网络、VPC均可使用弹性IP服务：
  - 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
  - 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。

- 内部私有网络是隔离的网络空间，不能直接被外部网络访问。
- 弹性IP基于网络地址转换（NAT），将一个网络（通常是公有网络）的IP地址转换成另一个网络（通常是私有网络）的IP地址；通过弹性IP，可对公网的访问直接关联到内部私网的云主机IP。
- 弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
- 云主机使用的扁平网络、云路由网络、VPC均可使用弹性IP服务：
  - 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
  - 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。
- 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
- 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。

云路由网络/VPC下弹性IP的应用场景，如图 *74: 云路由网络/VPC下弹性IP的应用场景*所示：

图 74: 云路由网络/VPC下弹性IP的应用场景



背景信息

以下介绍云路由环境下弹性IP的使用方法，包括两个场景：

- 创建弹性IP并绑定一个云主机；
- 将弹性IP绑定其它云主机。

操作步骤

1. 搭建云路由网络，详情可参考本教程基本部署章节。
2. 使用云路由网络创建两台私有云云主机，例如VM-1、VM-2，详情可参考本教程基本部署章节。

   创建的云主机如图 *75: VM-1、VM-2*所示：

   图 75: VM-1、VM-2

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-2	1	1 GB	192.168.10.167	10.0.182.41	Cluster-1	运行中	admin	None
VM-1	1	1 GB	192.168.10.226	10.0.182.41	Cluster-1	运行中	admin	None

3. 创建弹性IP并绑定VM-1。

   a) 创建弹性IP。

   在ZStack私有云主菜单，点击**网络服务** > **弹性IP**，进入**弹性IP**界面，点击**创建弹性IP**，在弹出的**创建弹性IP**界面，可参考以下示例输入相应内容：

- **名称**：设置弹性IP名称，例如EIP-1
- **简介**：可选项，可留空不填
- **选择虚拟IP**：通过虚拟IP提供弹性IP服务

  使用虚拟IP的方法有以下两种：

  - **新建虚拟IP**：

    如选择新建虚拟IP，需设置以下内容：

    - **网络**：选择提供虚拟IP的公有网络
    - **指定IP**：可选项，可指定虚拟IP；若留空不填，系统会自动分配虚拟IP

    如图 *76: 新建虚拟IP*所示：

    图 76: 新建虚拟IP

  - **已有虚拟IP**：

    如选择已有虚拟IP，需设置以下内容：

    - **虚拟IP**：选择已有的虚拟IP地址

    如图 *77: 已有虚拟IP*所示：

    图 77: 已有虚拟IP

注: 云路由器提供的系统虚拟IP不支持用于弹性IP服务。

如图 *78: 创建弹性IP*所示：

图 78: 创建弹性IP

b) 点击**下一步**，跳转到**绑定云主机网卡**界面。

c) 将EIP-1绑定VM-1。

在弹出的**绑定云主机网卡**界面，点击**云主机**栏里的加号按钮，弹出**选择云主机**界面，选择VM-1，点击**确定**。

如图 *79: 选择VM-1*和图 *80: 将EIP-1绑定VM-1*所示：

图 79: 选择VM-1

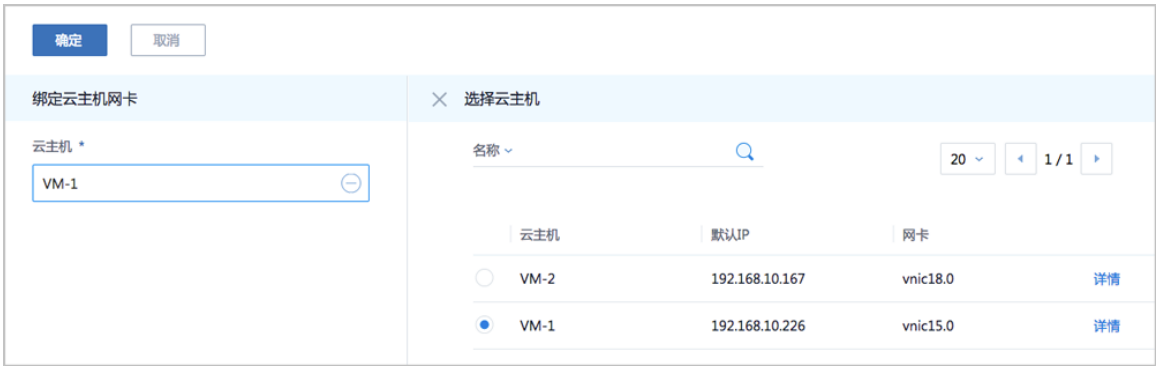
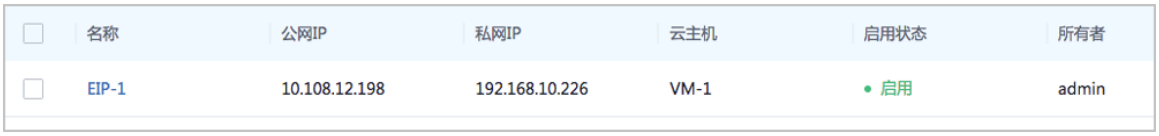


图 80: 将EIP-1绑定VM-1



d) 通过EIP-1登录VM-1。

使用某一可访问云路由网络公网网段（*10.108.12.0~10.108.13.255*）的主机SSH登录EIP-1：*10.108.12.198*，也就是登录到私网IP为*192.168.10.226*的VM-1。

如图 *81: 通过EIP-1登录VM-1*所示：

图 81: 通过EIP-1登录VM-1

4. 将EIP-1绑定VM-2。

a) 将EIP-1从VM-1解绑。

在**弹性IP**界面，选择EIP-1，点击**更多操作 > 解绑**，弹出**解绑云主机**确认窗口，点击**确定。**

如图 *82: 将EIP-1从VM-1解绑*所示：

图 82: 将EIP-1从VM-1解绑

b) 将EIP-1绑定VM-2。

在**弹性IP**界面，选择EIP-1，点击**更多操作 > 绑定**，弹出**选择云主机**窗口，选择VM-2，点击**确定。**

如图 *83: 选择VM-2*和图 *84: 将EIP-1绑定VM-2*所示：

图 83: 选择VM-2

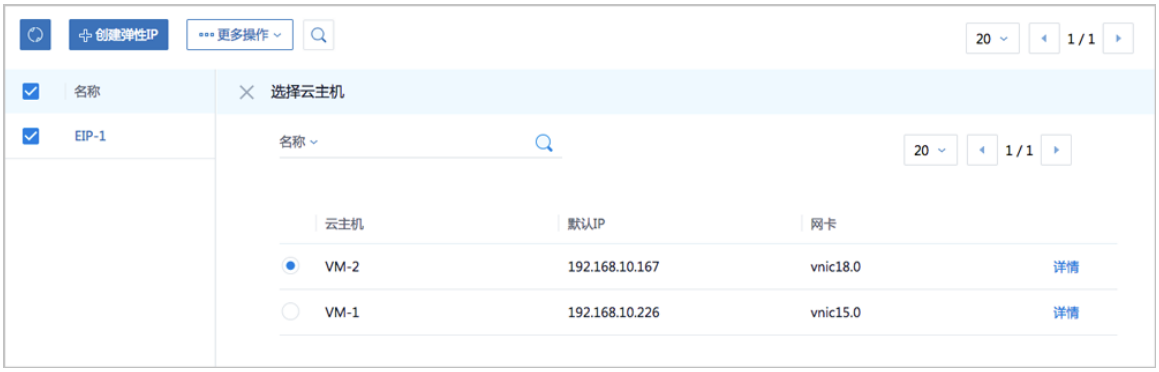
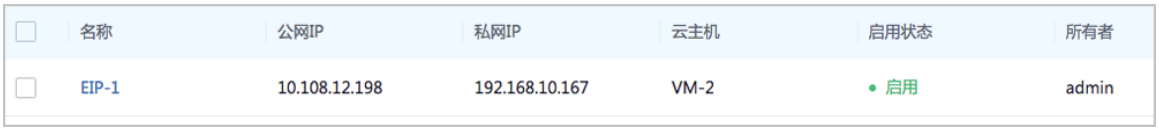


图 84: 将EIP-1绑定VM-2

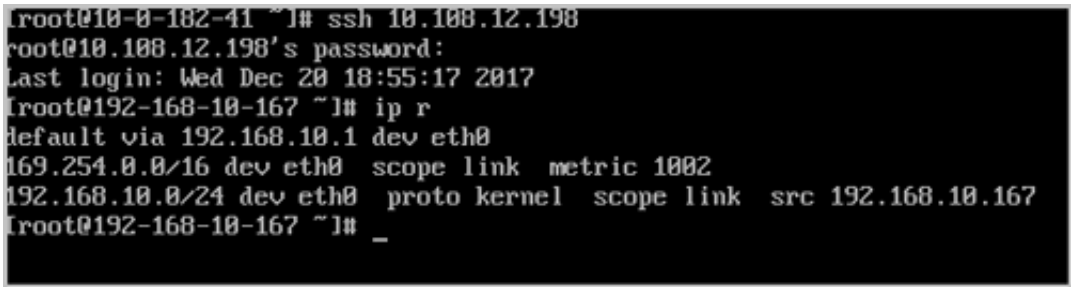


c) 通过EIP-1登录VM-2。

再次SSH登录EIP-1：*10.108.12.198*，可发现此时登录到私网IP为*192.168.10.167*的VM-2。

如图 *81: 通过EIP-1登录VM-1*所示：

图 85: 通过EIP-1登录VM-2



至此，弹性IP的使用方法介绍完毕。

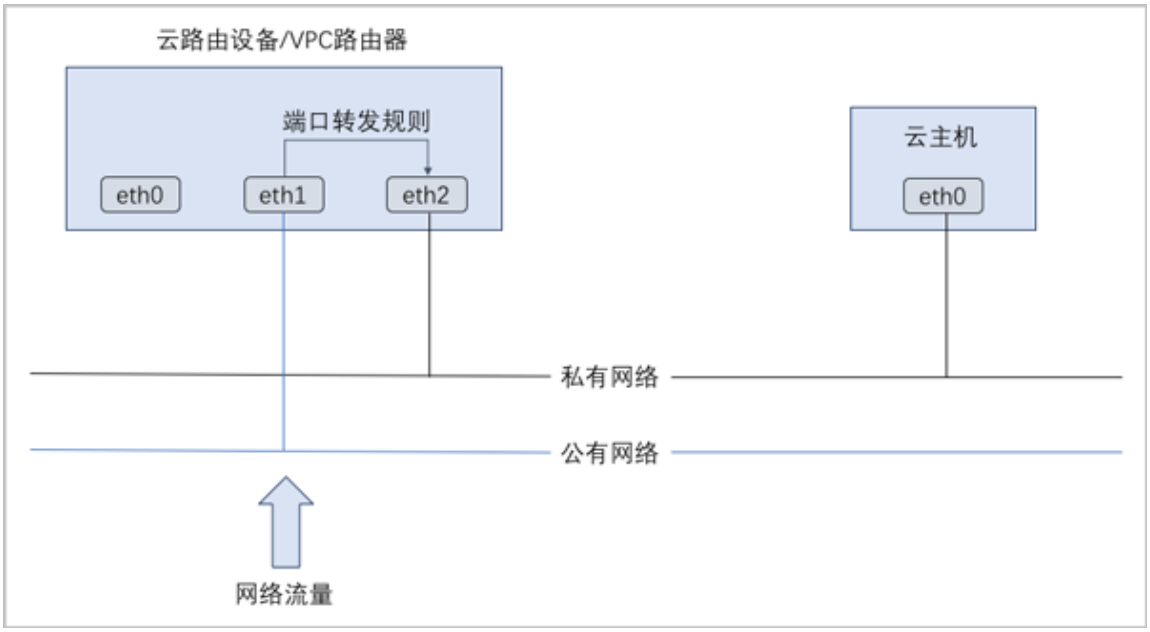
4.6 端口转发

前提条件

端口转发（PF）：基于云路由器/VPC路由器提供的三层转发服务，可将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。在公网IP地址紧缺的情况下，通过端口转发可提供多个云主机对外服务，节省公网IP地址资源。

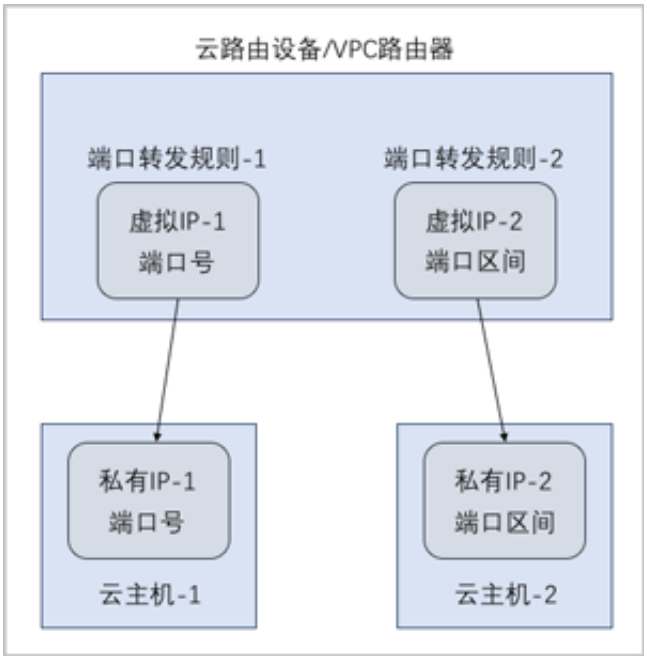
- 启用SNAT服务的私有网络中，云主机可访问外部网络但不能被外部网络所访问；使用端口转发规则，允许外部网络访问SNAT后面云主机的某些指定端口。
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *86: 端口转发*所示：

图 86: 端口转发



- 通过虚拟IP提供端口转发服务。
  - 虚拟IP对应于公网IP地址资源池中的一个可用IP。
  - 端口转发使用虚拟IP有两种方法：新建虚拟IP、使用已有虚拟IP。
  - 端口转发指定端口映射有两种方法：单个端口到单个端口的映射、端口区间的映射。
  - 如图 *87: 虚拟IP-端口转发*所示：

图 87: 虚拟IP-端口转发



背景信息

以下介绍云路由环境下端口转发的使用方法，包括三个场景：

- 创建端口转发规则并绑定一个云主机；
- 将端口转发规则绑定其它云主机；
- 绑定同一虚拟IP的不同端口到不同云主机。

操作步骤

1. 搭建云路由网络，详情可参考本教程基本部署章节。
2. 使用云路由网络创建两台私有云云主机，例如VM-1、VM-2，详情可参考本教程基本部署章节。

   创建的云主机如图 *88: VM-1、VM-2*所示：

   图 88: VM-1、VM-2

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-2	1	1 GB	192.168.10.167	10.0.182.41	Cluster-1	运行中	admin	None
VM-1	1	1 GB	192.168.10.226	10.0.182.41	Cluster-1	运行中	admin	None

3. 创建端口转发规则并绑定VM-1。

   a) 创建端口转发规则。

   在ZStack私有云主菜单，点击**网络服务** > **端口转发**，进入**端口转发**界面，点击**创建端口转发**，在弹出的**创建端口转发**界面，可参考以下示例输入相应内容：

   - **名称**：设置端口转发规则名称，例如PF-1
   - **简介**：可选项，可留空不填
   - **选择虚拟IP**：通过虚拟IP提供端口转发服务

     使用虚拟IP的方法有以下两种：

     - **新建虚拟IP**：

       如选择新建虚拟IP，需设置以下内容：

       - **网络**：选择提供虚拟IP的公有网络
       - **指定IP**：可选项，可指定虚拟IP；若留空不填，系统会自动分配虚拟IP

       如图 *89: 新建虚拟IP*所示：

       图 89: 新建虚拟IP

- **已有虚拟IP**：

  如选择已有虚拟IP，需设置以下内容：

  - **虚拟IP**：选择已有的虚拟IP地址

  如图 *90: 已有虚拟IP*所示：

  图 90: 已有虚拟IP

注: 云路由器提供的系统虚拟IP支持用于端口转发服务。

- **协议**：选择协议类型，包括：TCP、UDP
  - TCP：支持1-65535端口
  - UDP：支持1-65535端口
- **端口**：支持两种端口映射方法，包括：单个端口到单个端口的映射、端口区间的映射
  - **指定端口**：

如选择指定端口，需设置以下内容：

- **源起始端口**：可从1-65535端口之间选择一个端口作为源端口
- **源结束端口**：系统自动填写，默认与源起始端口一致
- **云主机起始端口**：可从1-65535端口之间选择一个端口作为云主机端口
- **云主机结束端口**：系统自动填写，默认与云主机起始端口一致
- **允许CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填

例如：源端口选择24，云主机端口选择22，表示对公网IP的24端口访问会转发到云主机的22端口。

如图 *91:* 创建端口转发规则-指定端口所示：

图 91: 创建端口转发规则-指定端口

- **端口区间**：

如选择端口区间，需设置以下内容：

- **源起始端口**：可从1-65535端口之间选择一个端口作为源起始端口

- **源结束端口**：可从1-65535端口之间选择一个端口作为源结束端口
- **云主机起始端口**：系统自动填写，默认与源起始端口一致
- **云主机结束端口**：系统自动填写，默认与源结束端口一致
- **允许CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填

例如：源端口区间选择22-80，云主机端口区间也默认为22-80，表示对公网IP的22-80端口访问会转发到云主机的22-80端口。

如图 *92:* 创建端口转发规则-端口区间所示：

图 92: 创建端口转发规则-端口区间

本场景下，创建的端口转发规则PF-1如图 *93:* 创建端口转发规则*PF-1*所示：

图 93: 创建端口转发规则PF-1


确定
取消
创建端口转发
名称 *
PF-1
简介
选择虚拟IP
虚拟IP方法
新建虚拟IP
已有虚拟IP
虚拟IP *
vip-for-vrouter.l3.L3-私有网络-云...
协议
TCP
端口
指定端口
端口区间
源起始端口 *
24
源结束端口 *
24
云主机起始端口 *
22
云主机结束端口 *
22
允许CIDR:
192.168.1.0/24

b) 点击**确定**，跳转到**绑定云主机网卡**界面。

c) 将PF-1绑定VM-1。

在弹出的**绑定云主机网卡**界面，点击**云主机**栏里的加号按钮，弹出**选择云主机**界面，选择VM-1，点击**确定**。

如图 *94: 选择VM-1*和图 *95: 将PF-1绑定VM-1*所示：

图 94: 选择VM-1

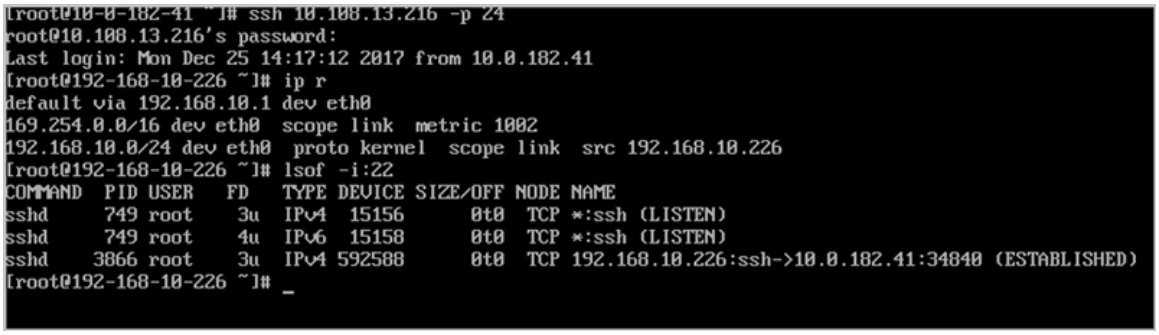
图 95: 将PF-1绑定VM-1

d) 通过PF-1登录VM-1。

使用某一可访问云路由网络公网网段（*10.108.12.0~10.108.13.255*）的主机SSH登录公网IP：*10.108.13.216*的24端口，也就是登录到私网IP为*192.168.10.226*的VM-1的22端口。

如图 *96: 通过PF-1登录VM-1*所示：

图 96: 通过PF-1登录VM-1



4. 将PF-1绑定VM-2。

a) 将PF-1从VM-1解绑。

在**端口转发**界面，选择PF-1，点击**更多操作** > **解绑**，弹出**解绑云主机**确认窗口，点击**确定**。

如图 *97: 将PF-1从VM-1解绑*所示：

图 97: 将PF-1从VM-1解绑

b) 将PF-1绑定VM-2。

在**端口转发**界面，选择PF-1，点击**更多操作** > **绑定**，弹出**选择云主机**窗口，选择VM-2，点击**确定**。

如图 *98: 选择VM-2*和图 *99: 将PF-1绑定VM-2*所示：

图 98: 选择VM-2

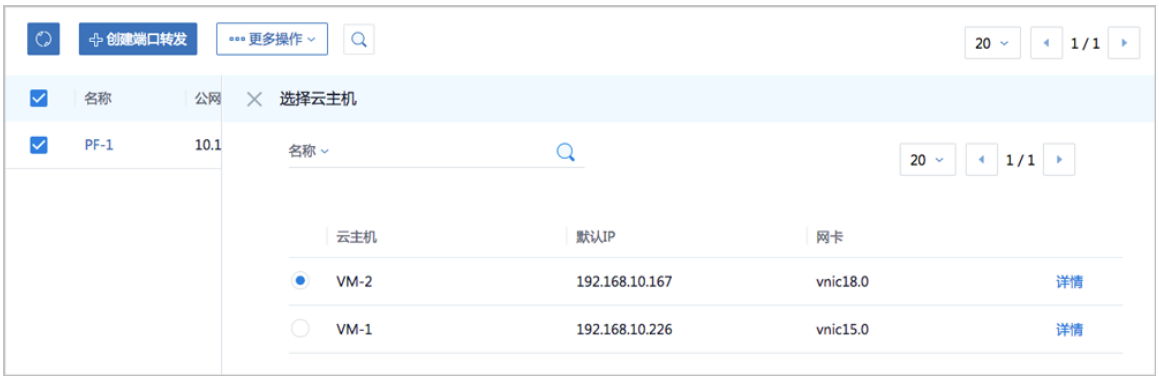


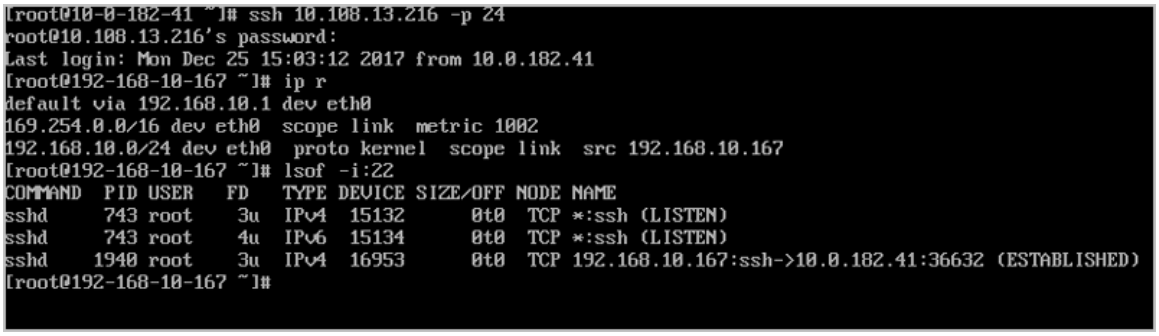
图 99: 将PF-1绑定VM-2

c) 通过PF-1登录VM-2。

再次SSH登录公网IP：*10.108.13.216*的24端口，可发现此时登录到私网IP为*192.168.10.167*的VM-2的22端口。

如图 *100: 通过PF-1登录VM-2*所示：

图 100: 通过PF-1登录VM-2



5. 绑定同一虚拟IP的不同端口到不同云主机。

a) 使用同一虚拟IP创建端口转发规则PF-2。

在**端口转发**界面，点击**创建端口转发**，在弹出的**创建端口转发**界面，可参考以下示例输入相应内容：

- **名称**：设置端口转发规则名称，例如PF-2
- **简介**：可选项，可留空不填
- **选择虚拟IP**：已有虚拟IP
  - **虚拟IP**：与端口转发规则PF-1同一虚拟IP
  - **协议**：选择协议类型，例如TCP
- **端口**：选择端口映射方法，例如端口区间
  - **源起始端口**：可从1-65535端口之间选择一个端口作为源起始端口，例如5900
  - **源结束端口**：可从1-65535端口之间选择一个端口作为源结束端口，例如5910
  - **云主机起始端口**：系统自动填写，默认与源起始端口一致
  - **云主机结束端口**：系统自动填写，默认与源结束端口一致
  - **允许CIDR**：可选项，仅允许指定的CIDR才可通过，可留空不填

如图 *93: 创建端口转发规则PF-1*所示：

图 101: 创建端口转发规则PF-2

b) 点击**确定**，跳转到**绑定云主机网卡**界面。

c) 将PF-2绑定VM-1。

在弹出的**绑定云主机网卡**界面，点击**云主机**栏里的加号按钮，弹出**选择云主机**界面，选择VM-1，点击**确定**。

如图 *102: 选择VM-1*和图 *103: 将PF-2绑定VM-1*所示：

图 102: 选择VM-1

图 103: 将PF-2绑定VM-1

d) 可见，同一虚拟IP（*10.108.13.216*），通过不同的端口转发规则，绑定到不同云主机。

e) 通过PF-2向VM-1发送信息。

使用某一可访问云路由网络公网网段（*10.108.12.0~10.108.13.255*）的主机，通过*nc*命令向公网IP：*10.108.13.216*的5900~5910某端口发送信息，可在私网IP为*192.168.10.226*的VM-1相应端口接收信息。

例如，使用规则范围内的源端口5900发送信息，在VM-1的端口5900接收信息。

注： 需将VM-1中原先的iptables规则清除，可使用命令iptables -F

如图 *104: 在源端口5900发送信息*和图 *105: 在VM-1的端口5900接收信息*所示：

图 104: 在源端口5900发送信息

图 105: 在VM-1的端口5900接收信息

后续操作

端口转发有以下约束条件：

- 端口转发要求云主机内部的防火墙策略对指定的转发端口开放。
- 同一个虚拟IP，在提供端口转发服务时， 该虚拟IP所用的端口之间不可重复。
- 同一个虚拟IP，可对同一个三层网络上的多个云主机网卡的不同端口提供端口转发服务。
- 同一个云主机，只能使用一个虚拟IP来提供端口转发服务。
- 虚拟IP从云主机解绑后，再次绑定云主机时，只能选择解除绑定关系前的同一个三层网络上的云主机网卡。
- 端口转发区间需一一对应，例如，设置了源端口22-80端口的端口区间，在云主机私网，默认也选择22-80端口。

至此，端口转发的使用方法介绍完毕。

4.7 负载均衡

前提条件

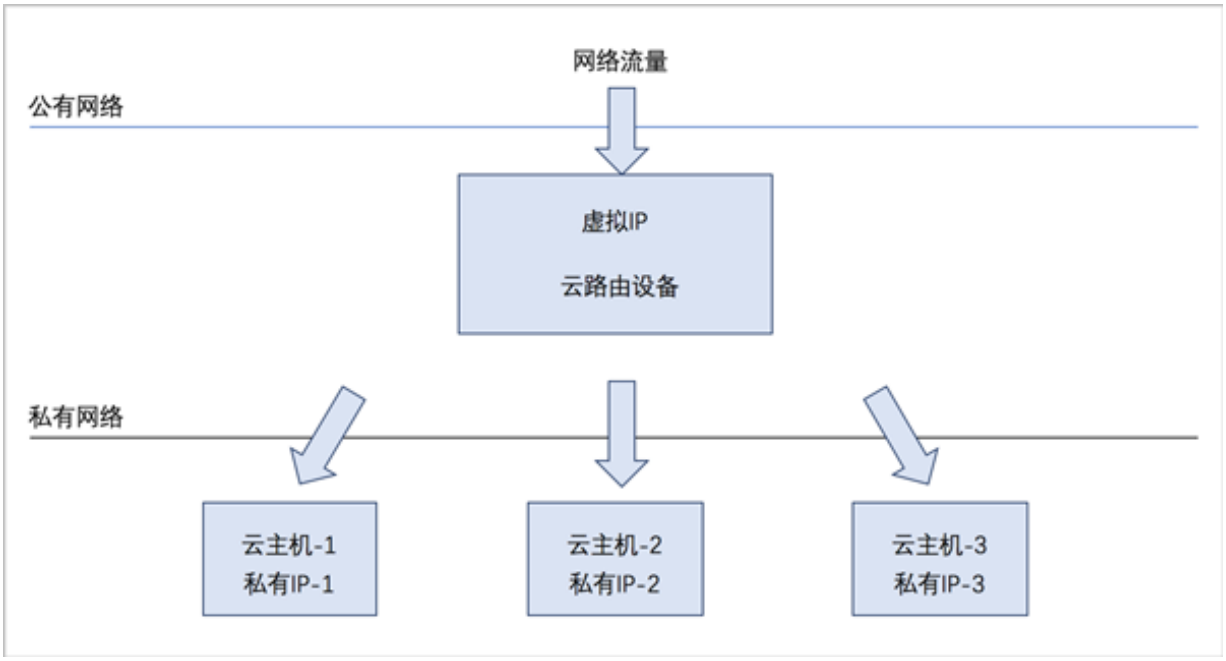
负载均衡（LB）：将公网地址的访问流量分发到一组后端的云主机， 并支持自动检测并隔离不可用的云主机，从而提高业务的服务能力和可用性。

- 负载均衡自动把访问用户应用的流量分发到预先设置的多个后端云主机，以提供高并发高可靠的访问服务。
- 根据实际情况，动态调整负载均衡监听器中的云主机来调整服务能力，且不会影响业务的正常访问。
- 负载均衡监听器支持TCP/HTTP/HTTPS/UDP四种协议。

- 当监听协议为HTTPS，需绑定证书使用，支持上传证书和证书链。
- 负载均衡器支持灵活配置多种转发策略，实现高级转发控制功能。

如图 *106: 虚拟IP-负载均衡*所示，云路由网络/VPC下虚拟IP提供负载均衡服务。

图 106: 虚拟IP-负载均衡



背景信息

负载均衡的基本使用流程：

1. 创建负载均衡器。
2. 创建并添加监听器，指定公网端口到云主机端口的对应关系，设置规则及算法等。
3. 选择指定三层网络的云主机网卡绑定到监听器，使负载均衡器生效。

以下介绍云路由环境下负载均衡的使用方法，场景如下：

- 创建负载均衡器，添加一个监听器并绑定三台云主机，基于默认的轮询算法向三台云主机提供负载均衡服务。

操作步骤

1. 搭建云路由网络，详情可参考本教程基本部署章节。
2. 使用云路由网络创建三台私有云云主机，例如VM-1、VM-2、VM-3，详情可参考本教程基本部署章节。

创建的云主机如图 *107: VM-1、VM-2、VM-3*所示：

图 107: VM-1、VM-2、VM-3

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-3	1	1 GB	192.168.10.99	10.0.182.41	Cluster-1	运行中	admin	None
VM-2	1	1 GB	192.168.10.167	10.0.182.41	Cluster-1	运行中	admin	None
VM-1	1	1 GB	192.168.10.226	10.0.182.41	Cluster-1	运行中	admin	None

3. 创建负载均衡器。

在ZStack私有云主菜单，点击**网络服务 > 负载均衡 > 负载均衡器**，进入**负载均衡器**界面，点击**创建负载均衡器**，在弹出的**创建负载均衡器**界面，可参考以下示例输入相应内容：

- **名称**：设置负载均衡器名称
- **简介**：可选项，可留空不填
- **选择虚拟IP**：通过虚拟IP提供负载均衡服务

  使用虚拟IP的方法有以下两种：

  - **新建虚拟IP**：

    如选择新建虚拟IP，需设置以下内容：

    - **网络**：选择提供虚拟IP的公有网络
    - **指定IP**：可选项，可指定虚拟IP；若留空不填，系统会自动分配虚拟IP

    如图 *108: 新建虚拟IP*所示：

    图 108: 新建虚拟IP

- **已有虚拟IP**：

  如选择已有虚拟IP，需设置以下内容：

  - **虚拟IP**：选择已有的虚拟IP地址

  如图 *109: 已有虚拟IP*所示：

  图 109: 已有虚拟IP

注: 云路由器提供的系统虚拟IP支持用于负载均衡服务。

- **监听器**：可选项，监听器可在创建负载均衡器时点击**创建监听器**按钮直接添加，也可在创建负载均衡器后再添加

  本场景以前者为例，详见添加监听器。

如图 *110: 创建负载均衡器*所示：

图 110: 创建负载均衡器

4. 添加监听器。

   在**创建负载均衡器**界面，点击**创建监听器**按钮，弹出**添加监听器**界面，可参考以下示例输入相应内容：

- **名称**：设置监听器名称
- **简介**：可选项，可留空不填
- **协议**：选择协议类型，包括：TCP、HTTP、HTTPS、UDP
  - TCP：支持1-65535端口
  - HTTP：支持1-65535端口
  - HTTPS：支持1-65535端口
  - UDP：支持1-65535端口
- **负载均衡端口**：可从1-65535端口之间选择一个端口作为负载均衡器公网端口
- **云主机端口**：可从1-65535端口之间选择一个端口作为云主机端口

  例如：公网端口选择80，云主机端口选择5000，表示对负载均衡器公网IP的80端口访问会转发到云主机的5000端口。

  如图 *111:* 添加监听器所示：

  图 111: 添加监听器

- **高级**：可对高级选项进行设置
  - **空闲连接超时**：没有数据传输时，触发负载均衡器终止服务器和客户端连接的超时时间，默认设置为60秒
  - **健康检查阈值**：对不健康的云主机，如果连续检查成功次数超过阈值，则认定其健康，默认设置为2次
  - **健康检查协议**：当监听协议为TCP/HTTP/HTTPS时，健康检查协议显示为TCP协议，当监听协议为UDP时，健康检查协议显示为UDP协议
  - **健康检查端口**：默认为default，表示与所选云主机端口一致，也可指定其它端口
  - **非健康检查阈值**：对云主机健康检查失败次数超过阈值，则认定其不健康，默认设置为2次
  - **健康检查间隔**：对云主机进行检查的时间间隔，默认设置为5秒
  - **最大连接数量**：设置监听器最大的连接数量，默认设置为5000条，取值范围：1-100,000

- **负载均衡算法**：对网络包设定不同的路由规则，默认设置为**roundrobin**（轮询）

  支持的负载均衡算法包括：

  - **roundrobin**（轮询）

    通过轮询调度算法，将外部请求按顺序轮流分配到负载均衡规则指定的云主机中，它均等地对待每一台云主机，而不管其上实际的连接数和系统负载。

  - **leastconn**（最少连接）

    通过最少连接调度算法，将网络请求动态地调度到已建立的连接数最少的云主机上。如果集群中的服务器（云主机）具有相近的系统性能，采用最少连接调度算法可以较好地均衡负载。

  - **source**（源地址哈希）

    源地址哈希算法，根据请求的源IP地址，作为散列键（Hash Key）从静态分配的散列表找出对应的服务器，若该服务器可用且未超载，将请求发送到该服务器，否则返回空。

如图 *112:* 创建监听器-高级选项所示：

图 112: 创建监听器-高级选项

5. 绑定VM-1、VM-2、VM-3的云主机网卡到监听器。

   a) 进入绑定云主机网卡界面

   在ZStack私有云主菜单，点击**网络服务** > **负载均衡** > **监听器**按钮，进入**监听器**页面，选择一个监听器，点击**更多操作** > **绑定云主机网卡**，进入**绑定云主机网卡**界面。如图 *113:* 进入监听器详情页所示：

   图 113: 进入监听器详情页

b) 在弹出的**绑定云主机网卡**界面，可参考以下示例输入相应内容：

- **网络**：选择云路由器挂载的三层私有网络
- **云主机网卡**：选择VM-1、VM-2、VM-3的云主机网卡

如图 *114: 绑定云主机网卡到监听器*所示，点击**确定**，绑定VM-1、VM-2、VM-3的云主机网卡到监听器。

图 114: 绑定云主机网卡到监听器

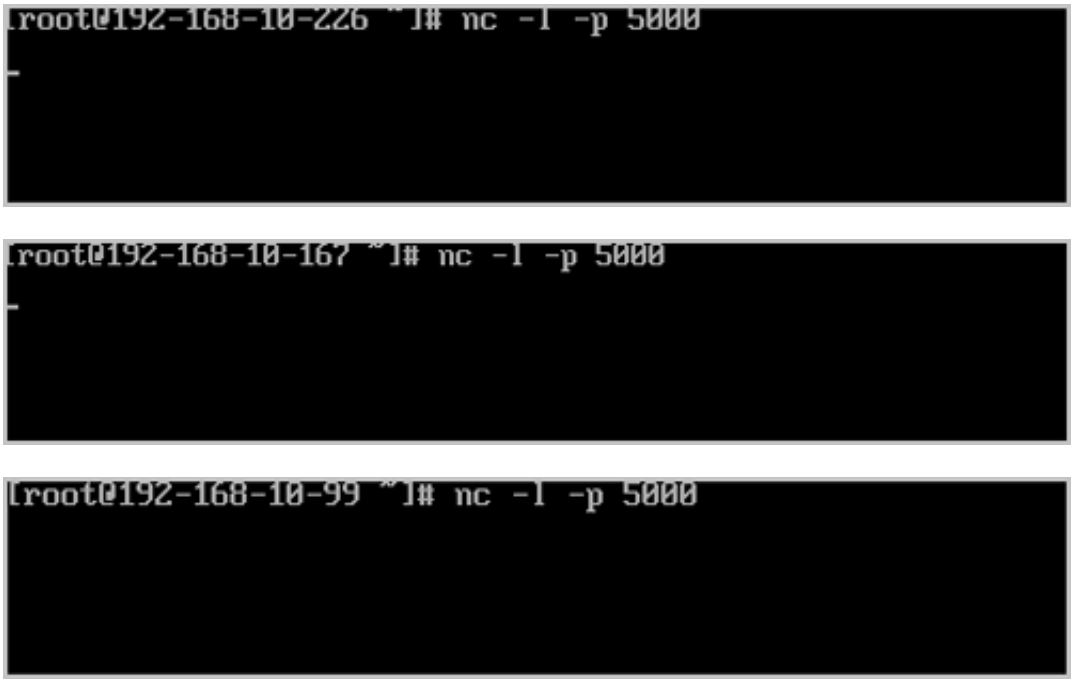
6. 负载均衡器以默认的轮询方式向三台云主机发送信息。

使用某一可访问云路由网络公网网段（*10.108.12.0~10.108.13.255*）的主机，通过*nc*命令向负载均衡器公网IP：*10.108.13.216*的80端口发送信息，可在VM-1（私网IP：*192.168.10.226*）、VM-2（私网IP：*192.168.10.167*）、VM-3（私网IP：*192.168.10.99*）的5000端口以默认的轮询方式接收信息。

注： 需将VM-1、VM-2、VM-3中原先的iptables规则清除，可使用命令iptables -F

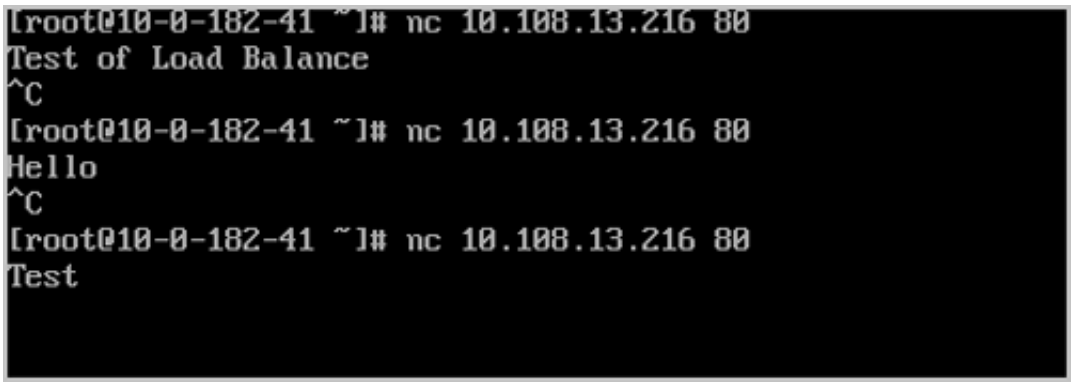
1. 开启VM-1、VM-2、VM-3的5000端口侦听，如图 *115: 开启三台云主机的5000端口侦听*所示：

图 115: 开启三台云主机的5000端口侦听



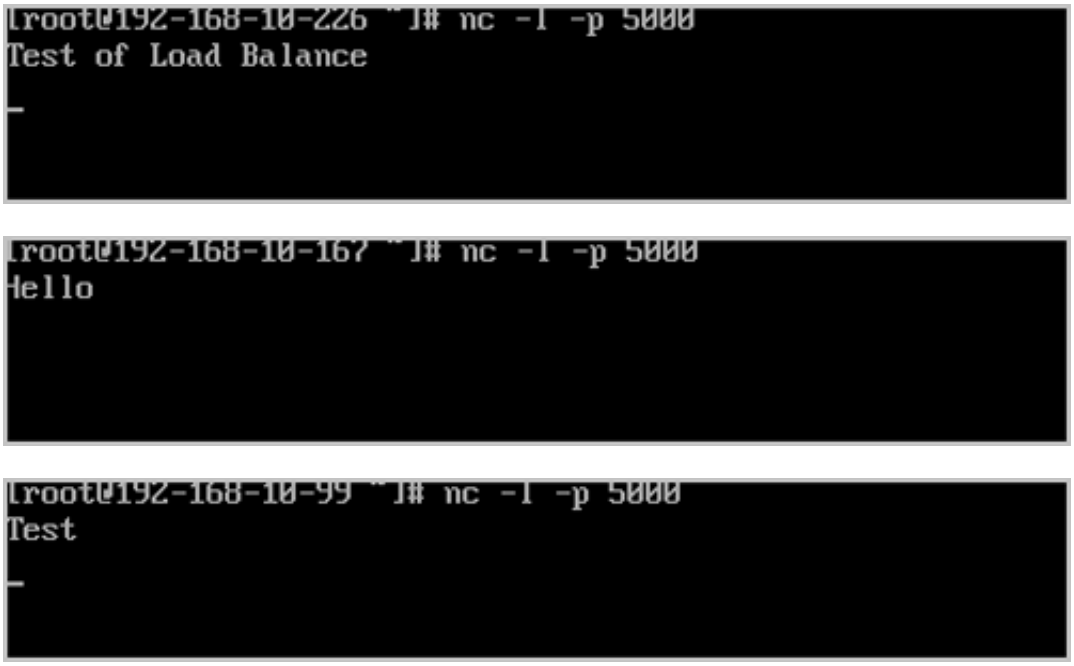
2. 向负载均衡器公网IP的80端口发送三条信息，如图 *116: 向负载均衡器公网IP的80端口发送三条信息*所示：

图 116: 向负载均衡器公网IP的80端口发送三条信息



3. VM-1、VM-2、VM-3的5000端口分别接收到一条信息，如图 *117:* 三台云主机的*5000*端口分别接收到一条信息所示：

图 117: 三台云主机的5000端口分别接收到一条信息



后续操作

负载均衡有以下约束条件：

- 一个负载均衡器可以支持多个监听器。
- 一个负载均衡器支持的监听器指定的云主机网卡必须在同一个三层网络。
- 当监听协议为HTTPS，一个监听器同一时间只能绑定一个证书，如需更换证书，需先解绑当前证书。
- ZStack支持内部访问业务流量的负载均衡。如果内部用户希望通过虚拟IP访问负载均衡，需进行如下设置：

进入**设置** > **全局设置** > **高级设置**，将**三层网络安全默认规则**设置为**accept**，且重连云路由器生效。

至此，负载均衡的使用方法介绍完毕。

4.8 IPsec隧道

前提条件

IPsec隧道：透过对IP协议的分组加密和认证来保护IP协议的网络传输数据，实现站点到站点（site-to-site）的虚拟私有网络（VPN）连接。

云路由网络下IPsec隧道的典型场景：

- 在两套隔离的ZStack私有云环境中，使用云路由网络；两套环境中云主机的私有网络无法直接通信，使用IPsec隧道可实现两套云主机的私有网络互相通信。

背景信息

云路由网络下IPsec隧道的基本使用流程：

1. 在第一套环境中，创建IPsec隧道，指定第一套网络的本地公网IP、并指定本地可用的私有网络，输入第二套网络指定的公网IP作为远端IP，并输入第二套网络指定的私有网络作为远端网路；
2. 在第二套环境中，创建IPsec隧道，指定第二套网络的本地公网IP，并指定本地可用的私有网络，输入第一套网络指定的公网IP作为远端IP，并输入第一套网络指定的私有网络作为远端网络。

注: 两套云路由网络环境中的私有网络段不可重叠。

假定客户环境如下：

- 第一套ZStack：

  1. 公有网络

     表 22: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN

公有网络	配置信息
IP地址段	*10.108.12.0~10.108.13.255*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

表 23: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.10~192.168.29.20*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

注:

- 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
- 此管理网络与ZStack私有云中的管理网络为相同概念（即：管理物理机、主存储、镜像服务器的网络），如果已创建可直接复用。

3. 私有网络

表 24: 私有网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2800
IP CIDR	*192.168.10.0/24*

- 第二套ZStack：

1. 公有网络

表 25: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*10.108.14.0~10.108.15.255*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

表 26: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*192.168.29.110~192.168.29.120*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

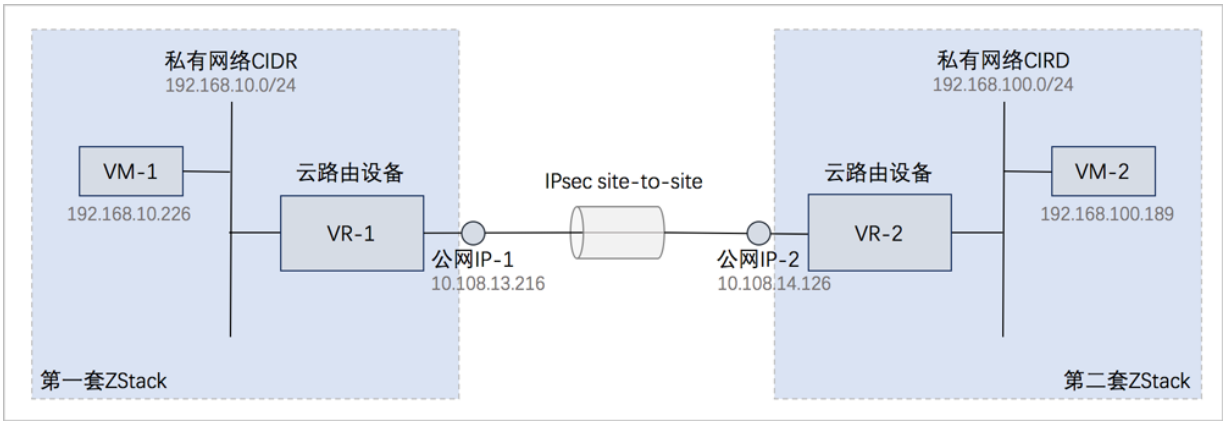
3. 私有网络

表 27: 私有网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2900
IP CIDR	*192.168.100.0/24*

IPsec隧道网络架构如图 *118: IPsec隧道网络架构图*所示：

图 118: IPsec隧道网络架构图



以下介绍云路由环境下搭建IPsec隧道的实践步骤。

操作步骤

1. 搭建第一套ZStack的云路由网络，并使用该云路由网络创建一台私有云云主机，例如VM-1，详情可参考本教程基本部署章节。

   创建的云主机如图 *119: VM-1*所示：

   图 119: VM-1

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-1	1	1 GB	192.168.10.226	10.0.182.41	Cluster-1	运行中	admin	None

2. 同理，搭建第二套ZStack的云路由网络，并使用该云路由网络创建一台私有云云主机，例如VM-2。

   创建的云主机如图 *120: VM-2*所示：

   图 120: VM-2

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者	高可用级别
VM-2	1	1 GB	192.168.100.189	10.0.138.149	Cluster-1	运行中	admin	None

3. 检测VM-1与VM-2的连通性。

   - 登录VM-1，尝试SSH默认的22端口远程登录VM-2失败，也不能ping通VM-2。

     如图 *121: VM-1尝试连通VM-2失败*所示：

     图 121: VM-1尝试连通VM-2失败

```
[root@192-168-10-226 ~]# ssh root@192.168.100.189
^C
[root@192-168-10-226 ~]# ping 192.168.100.189
PING 192.168.100.189 (192.168.100.189) 56(84) bytes of data.
From 61.213.146.217 icmp_seq=1 Destination Net Unreachable
^C
--- 192.168.100.189 ping statistics ---
4 packets transmitted, 0 received, +1 errors, 100% packet loss, time 3001ms
```

- 登录VM-2，尝试连通VM-1亦失败。

4. 在第一套ZStack中创建IPsec隧道。

a) 创建IPsec隧道-1。

ZStack**网络服务** > **IPsec隧道**，进入**IPsec隧道**界面，点击**创建IPsec隧道**，在弹出的**创建IPsec隧道**界面，可参考以下示例输入相应内容：

- **名称**：设置IPsec隧道名称，例如IPsec隧道-1
- **简介**：可选项，可留空不填
- **选择虚拟IP**：通过虚拟IP提供IPsec服务

  使用虚拟IP的方法有以下两种：

  - **新建虚拟IP**：

    如选择新建虚拟IP，需设置以下内容：

    - **网络**：选择提供虚拟IP的公有网络
    - **指定IP**：可选项，可指定虚拟IP；若留空不填，系统会自动分配虚拟IP

    如图 *122: 新建虚拟IP*所示：

    图 122: 新建虚拟IP

- **已有虚拟IP**：

  如选择已有虚拟IP，需设置以下内容：

  - **虚拟IP**：选择已有的虚拟IP地址

  如图 *123: 已有虚拟IP*所示：

  图 123: 已有虚拟IP

注: 云路由器提供的系统虚拟IP支持用于IPsec服务。

- **本地子网**：选择本地云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网
- **远端网络IP**：填写远端网络用于IPsec服务的公网IP
- **远端网络CIDR**：填写远端网络指定的私有网络CIDR
- **认证密钥**：设置密钥，建议设置强度较高的密钥
- **高级选项**：可对高级选项进行设置，以下默认选项为可连通双边私网的选项

- **认证模式**：psk（默认）
- **工作模式**：tunnel（默认）
- **IKE 验证算法**：sha1（默认）
- **IKE 加密算法**：3des（默认）
- **IKE 完整前向保密**：2（默认）
- **传输安全协议**：esp（默认）
- **ESP 认证算法**：sha1（默认）
- **ESP 加密算法**：3des（默认）
- **完全正向保密(PFS)**：dh-group2（默认）

注:

- 如果客户场景设计ZStack私有云的云路由与支持IPsec隧道的第三方设备对接，则需两端协商具体的高级配置信息。
- 创建IPsec隧道时，需根据远端网络设备IPsec配置内容，调整本地高级设置内容。

如图 *124: 创建IPsec隧道-1*所示：

图 124: 创建IPsec隧道-1

b) IPsec隧道-1创建完成。

如图 *125: IPsec隧道-1*所示：

图 125: IPsec隧道-1

5. 同理，在第二套ZStack中创建IPsec隧道。

   a) 创建IPsec隧道-2。

   如图 *126: 创建IPsec隧道-2*所示：

   图 126: 创建IPsec隧道-2

b）IPsec隧道-2创建完成。

如图 *127: IPsec隧道-2*所示：

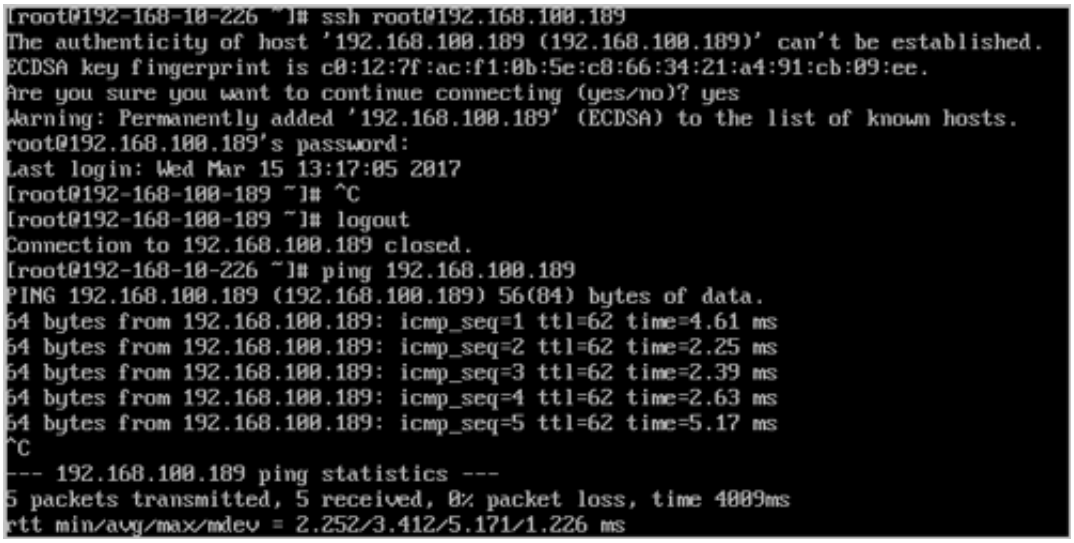
图 127: IPsec隧道-2

6. 检测VM-1与VM-2的连通性。

   - 登录VM-1，可通过SSH默认的22端口远程登录VM-2，以及ping通VM-2。

     如图 *128: VM-1成功连通VM-2*所示：

     图 128: VM-1成功连通VM-2



   - 登录VM-2，亦可通过SSH默认的22端口远程登录VM-1，以及ping通VM-1。

   至此，IPsec隧道的使用方法介绍完毕。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

一个集群是类似物理主机（Host）组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统（虚拟机管理程序，Hypervisor），拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架（Rack）。

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

也称之为物理主机（或物理机），为云主机实例提供计算、网络、存储等资源的物理主机。

主存储（Primary Storage）

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、 Ceph、、Shared Mount Point等类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。

镜像仓库（Image Store）

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机（VM Instance）

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

二层网络对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池（VXLAN Network Pool）

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络（即 VXLAN 网络），这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络（VXLAN）

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一个时间点上某一个磁盘的数据备份。包括自动快照和手动快照两种类型。