扁平网络 使用教程

产品版本：ZStack 2.5.1

文档版本：V2.5.1

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

扁平网络具备以下特性：

- 物理机和云主机均处于同一个二层广播域。
- 提供User Data、弹性IP、DHCP、安全组等服务。
- 分布式EIP、分布式DHCP可规避DHCP服务器的单点故障，高并发时，可有效提高系统整体并发性。

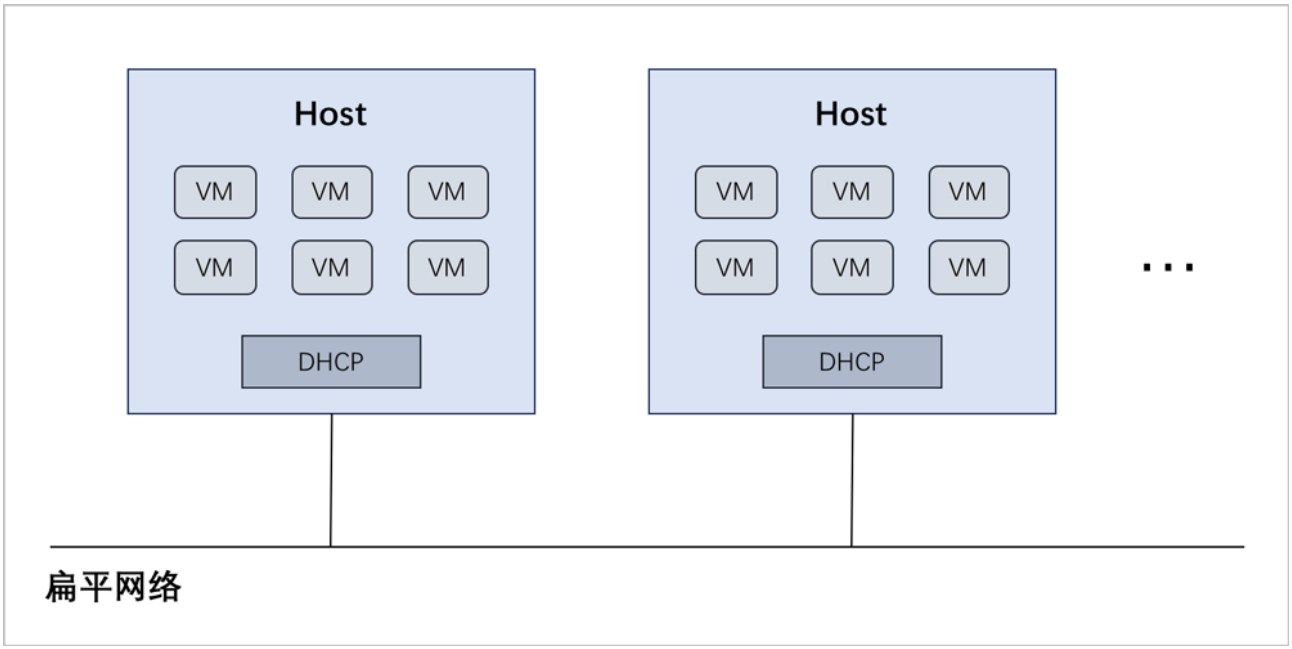
扁平网络提供以下网络服务：

- User Data：使用cloud-init进行云主机开机加载并执行特定的用户数据，例如ssh-key注入。
- 弹性IP：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。
- DHCP：分布式DHCP实现动态获取IP地址。

  注: DHCP服务包含了DNS的功能。
- 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。

扁平网络架构如图 *1:* 扁平网络架构图所示：

图 1: 扁平网络架构图



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。

本教程将详细介绍扁平网络的基本部署以及典型应用场景。

3 基本部署

背景信息

搭建扁平网络的基本流程如下：

1. 创建扁平网络对应的二层网络，并加载此二层网络到相应集群。
2. 创建扁平网络对应的三层网络，输入相应的IP范围、子网掩码、网关、DNS等信息。
3. 使用此扁平网络创建云主机。
4. 验证扁平网络连通性。

假定客户环境如下：

表 1: 扁平网络配置信息

扁平网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*172.20.108.40~172.20.108.50*
子网掩码	*255.255.0.0*
网关	*172.20.0.1*

以下介绍搭建扁平网络的实践步骤。

操作步骤

1. 创建扁平网络对应的二层网络，并加载此二层网络到相应集群。

   在ZStack私有云主菜单，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:* 扁平网络配置信息填写如下：

   - **名称**：设置L2-扁平网络名称
   - **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 *2: 创建L2-扁平网络*所示，点击**确定**，创建L2-扁平网络。

图 2: 创建L2-扁平网络

2. 创建扁平网络对应的三层网络，输入相应的IP范围、子网掩码、网关、DNS等信息。

   在ZStack私有云主菜单，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 1: 扁平网络配置信息*填写如下：

   - **名称**：设置L3-扁平网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-扁平网络
   - **DHCP服务**：选择是否需要DHCP服务
   - 网络类型选择**扁平网络**

- **添加网络段**：选择IP范围
- **起始IP**：*172.20.108.40*
- **结束IP**：*172.20.108.50*
- **子网掩码**：*255.255.0.0*
- **网关**：*172.20.0.1*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *3:* 创建*L3*-扁平网络所示，点击**确定**，创建L3-扁平网络。

图 3: 创建L3-扁平网络


确定
取消
创建私有网络
名称 *
L3-扁平网络
简介
二层网络 *
L2-扁平网络
关闭DHCP服务
扁平网络
云路由
添加网络段
方法
IP 范围
CIDR
起始IP *
172.20.108.40
结束IP *
172.20.108.50
子网掩码 *
255.255.0.0
网关 *
172.20.0.1
添加DNS
DNS
223.5.5.5

3. 使用此扁平网络创建私有云云主机。

在ZStack私有云主菜单，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**：从网络列表中选择已创建的L3-扁平网络

如图 *4: 创建云主机VM-1*所示，点击 **确定**，创建私有云云主机。

图 4: 创建云主机VM-1

4. 验证扁平网络连通性。

   - 内网连通性验证：

     1. 使用该扁平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 *5: VM-1 ping通 VM-2*所示：

        图 5: VM-1 ping通 VM-2

```
[root@172-20-108-48 ~]# ip r
default via 172.20.0.1 dev eth0
169.254.0.0/16 dev eth0  scope link  metric 1002
172.20.0.0/16 dev eth0  proto kernel  scope link  src 172.20.108.48
[root@172-20-108-48 ~]# ping 172.20.108.50
PING 172.20.108.50 (172.20.108.50) 56(84) bytes of data.
64 bytes from 172.20.108.50: icmp_seq=1 ttl=64 time=0.680 ms
64 bytes from 172.20.108.50: icmp_seq=2 ttl=64 time=0.428 ms
64 bytes from 172.20.108.50: icmp_seq=3 ttl=64 time=0.474 ms
64 bytes from 172.20.108.50: icmp_seq=4 ttl=64 time=0.608 ms
64 bytes from 172.20.108.50: icmp_seq=5 ttl=64 time=0.404 ms
64 bytes from 172.20.108.50: icmp_seq=6 ttl=64 time=0.398 ms
^C
--- 172.20.108.50 ping statistics ---
```

3. 登录VM-2，检查是否能够ping通VM-1，如图 *6: VM-2 ping通 VM-1*所示：

图 6: VM-2 ping通 VM-1

```
[root@172-20-108-50 ~]# ip r
default via 172.20.0.1 dev eth0
169.254.0.0/16 dev eth0  scope link  metric 1002
172.20.0.0/16 dev eth0  proto kernel  scope link  src 172.20.108.50
[root@172-20-108-50 ~]# ping 172.20.108.48
PING 172.20.108.48 (172.20.108.48) 56(84) bytes of data.
64 bytes from 172.20.108.48: icmp_seq=1 ttl=64 time=0.858 ms
64 bytes from 172.20.108.48: icmp_seq=2 ttl=64 time=0.620 ms
64 bytes from 172.20.108.48: icmp_seq=3 ttl=64 time=0.497 ms
64 bytes from 172.20.108.48: icmp_seq=4 ttl=64 time=0.530 ms
64 bytes from 172.20.108.48: icmp_seq=5 ttl=64 time=0.437 ms
64 bytes from 172.20.108.48: icmp_seq=6 ttl=64 time=0.316 ms
^C
--- 172.20.108.48 ping statistics ---
```

注: 如果有连接公网的需求，需要再创建一个与该扁平网络在同一网段的公有网络，然后该扁平网络即可连同公网。

至此，扁平网络的基本部署实践介绍完毕。

4 应用场景

扁平网络可用于以下典型应用场景：

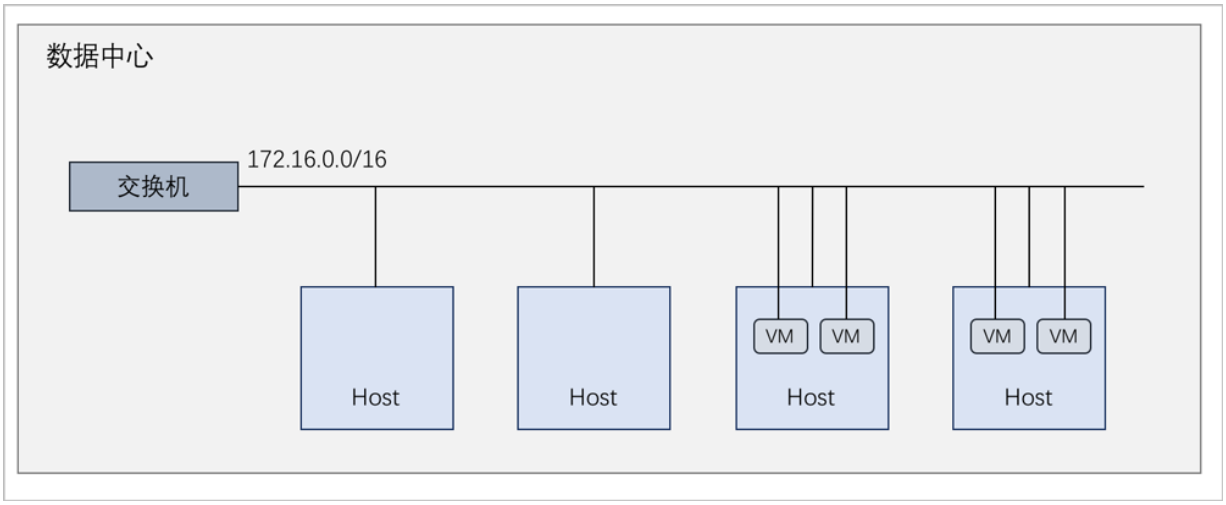
- 二层连通网络
- 安全组
- 弹性IP

4.1 二层连通网络

经典的二层扁平网络是一个二层连通网络，指在一个私有云数据中心里，所有的物理机和云主机都在一个二层网络之上，它们的IP地址也在相同的三层网络段。物理机和云主机之间互相访问不需要通过网关进行路由。

如图 7: 二层扁平网络所示，所有计算节点的IP地址均从*172.16.0.0/16*这一网络段中分配。

图 7: 二层扁平网络



对于中小型企业而言，二层扁平网络非常适合。网络拓扑架构简单，员工电脑之间可以直接相互访问；由于全员电脑都在一个二层网络之上，网络访问控制通常采用私有云的安全组（即分布式防火墙）来保证。

在实际部署中，三层网络的网关地址需设定为公司的网关地址。此外，分配给云主机的IP地址段需要避免和物理机相关的IP地址段进行人为的划分隔离。

4.2 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。

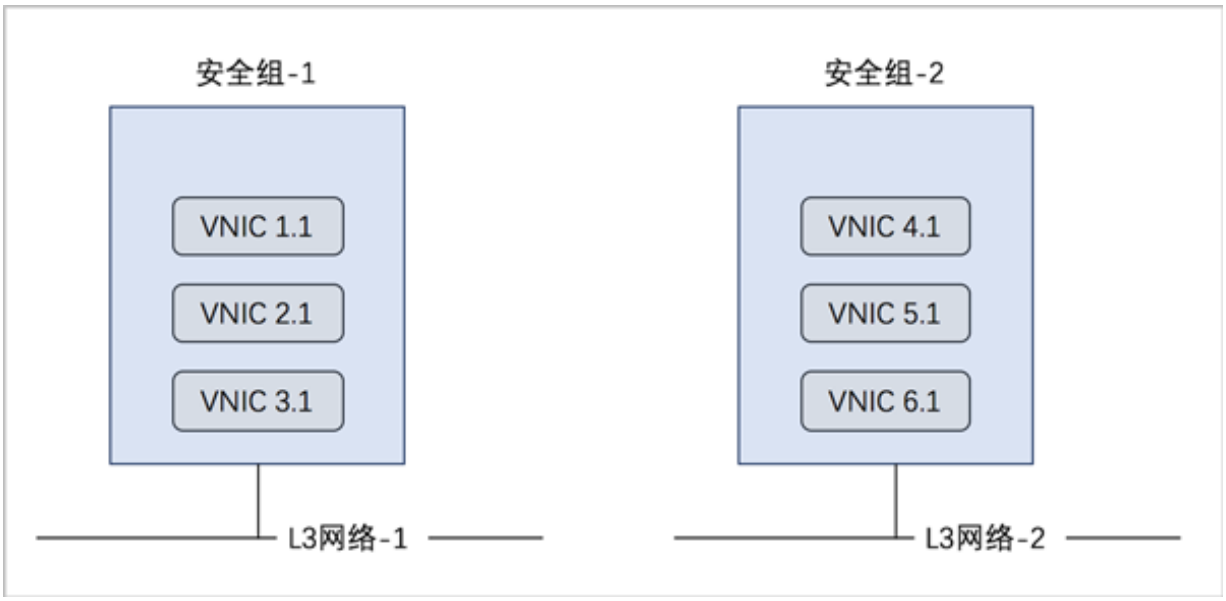
安全组规则：

- 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 *8:* 安全组所示：

图 8: 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。

以下介绍扁平网络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. 搭建扁平网络，并创建两台云主机VM-1和VM-2。详情可参考本教程基本部署章节。

   登录VM-1，通过SSH默认的22端口远程登录VM-2，如图 *9: SSH*远程登录成功所示：

   图 9: SSH远程登录成功

```
CentOS Linux 7 (Core)
Kernel 3.10.0-229.7.2.el7.x86_64 on an x86_64

zstack-test-image login: root
Password:
Last login: Mon Jan  8 13:51:37 on tty1
-bash-4.2# ip r
default via 192.168.0.1 dev eth0
192.168.0.0/16 dev eth0  proto kernel  scope link  src 192.168.0.223
-bash-4.2# ssh root@192.168.0.211
The authenticity of host '192.168.0.211 (192.168.0.211)' can't be established.
ECDSA key fingerprint is 82:cf:07:ff:68:f0:ab:4f:33:3b:da:a9:74:3b:b2:c9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.211' (ECDSA) to the list of known hosts.
root@192.168.0.211's password:
Last login: Mon Jan  8 13:51:49 2018
-bash-4.2# ip r
default via 192.168.0.1 dev eth0
192.168.0.0/16 dev eth0  proto kernel  scope link  src 192.168.0.211
-bash-4.2#
```

2. 对VM-1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**：选择已创建的扁平网络对应的三层网络
   - **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

     注:

     详见设置入方向规则以及设置出方向规则。
   - **网卡**：可选项，选择云主机网卡加入安全组，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

     注:

     详见添加云主机网卡到安全组。

   如图 *10:* 创建安全组所示，点击**确定**，创建安全组。

   图 10: 创建安全组

b) 设置入方向规则。

以创建安全组后再设置安全组规则为例。在**安全组**界面，选择已创建的安全组，展开其详情页，点击**规则**，进入**规则**子页面，点击**操作 > 添加规则**，在弹出的**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**：20
- **结束端口**：100
- **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

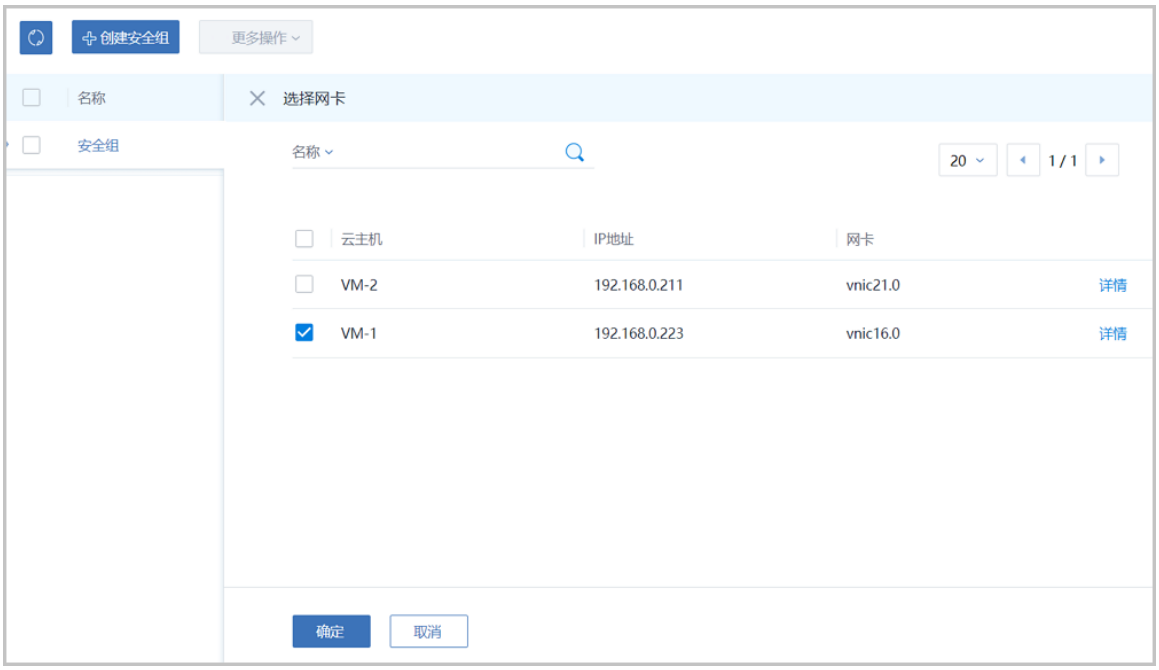
如图 *11:* 设置入方向规则所示，点击**确定**，设置入方向规则。

图 11: 设置入方向规则

c) 添加云主机网卡到安全组。

以创建安全组后再添加云主机网卡为例。在**安全组**界面，选择已创建的安全组，展开其详情页，点击**云主机网卡**，进入**云主机网卡**子页面，点击**操作** > **绑定云主机网卡**，在弹出的**选择网卡**界面，选择需要绑定的云主机网卡，例如VM-1，如图 *12:* 添加云主机网卡到安全组所示：

图 12: 添加云主机网卡到安全组



d) 入方向规则验证。

此时VM-1只允许外部通过端口20~100访问。

登录VM-2，尝试使用*nc*命令与VM-1建立通信连接。

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

1. 例如，使用规则范围外的端口10，VM-2与VM-1通信失败。

   如图 *13: VM-2在端口10尝试连接VM-1失败*所示：

   图 13: VM-2在端口10尝试连接VM-1失败

2. 例如，使用规则范围内的端口23，VM-2与VM-1通信成功。

   如图 *14: VM-2在端口23向VM-1发送信息*和图 *15: VM-1在端口23接收信息成功*所示：

   图 14: VM-2在端口23向VM-1发送信息

图 15: VM-1在端口23接收信息成功

3. 对VM-1设置出方向规则。

   a) 设置出方向规则。

   以创建安全组后再设置安全组规则为例。在**安全组**界面，选择已创建的安全组，展开其详情页，点击**规则**，进入**规则**子页面，点击**操作** > **添加规则**，在弹出的**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**：200
   - **结束端口**：1000
   - **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 *16:* 设置出方向规则所示，点击**确定**，设置出方向规则。

图 16: 设置出方向规则

b) 出方向规则验证。

此时云主机VM-1只允许通过端口200~1000访问外部地址。

登录VM-2，尝试使用*nc*命令与VM-1建立通信连接。

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

1. 例如，使用规则范围外的端口10，VM-2与VM-1通信失败。

   如图 *17: VM-1在端口10尝试连接VM-2失败*所示：

   图 17: VM-1在端口10尝试连接VM-2失败

```
-bash-4.2# nc 192.168.0.211 10
Ncat: Connection timed out.
-bash-4.2# _
```

2. 例如，使用规则范围内的端口200，VM-2与VM-1通信成功。

   如图 *18: VM-1在端口200向VM-2发送信息*和图 *19: VM-2在端口200接收信息成功*所示：

图 18: VM-1在端口200向VM-2发送信息

```
-bash-4.2# nc 192.168.0.211 200
HELLO
```

图 19: VM-2在端口200接收信息成功

```
-bash-4.2# iptables -F
-bash-4.2# nc -l 200
HELLO
```

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。

4.3 弹性IP

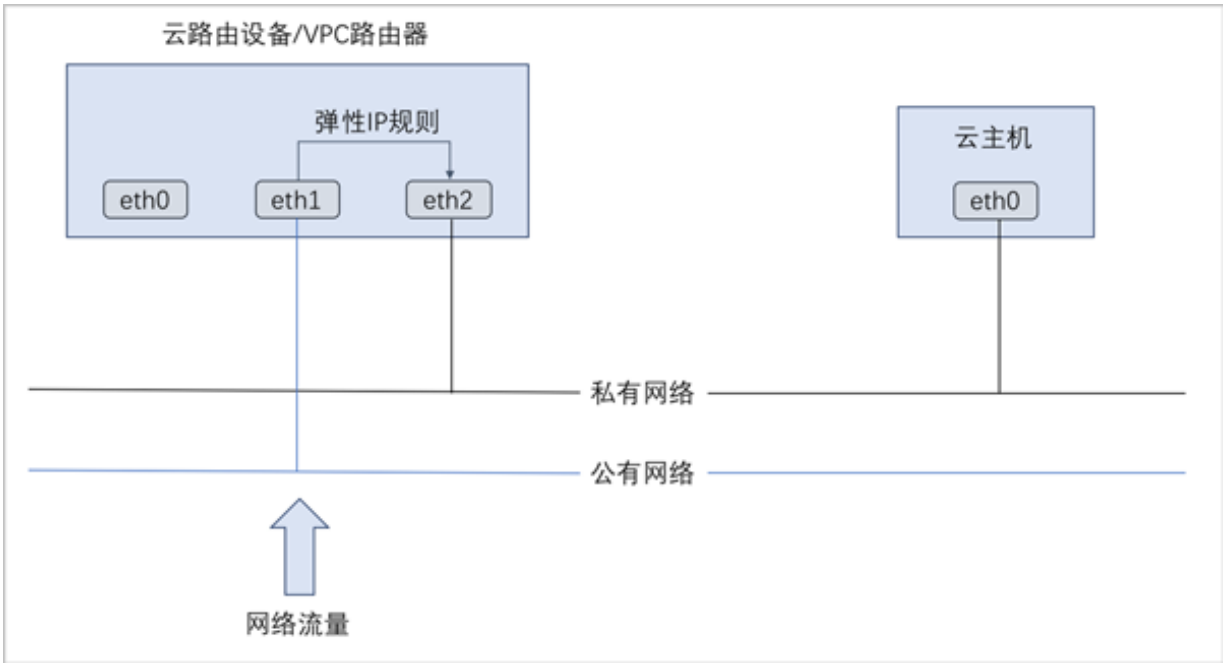
前提条件

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。

云路由网络/VPC下弹性IP的应用场景，如图 *20: 云路由网络/VPC下弹性IP的应用场景*所示：

图 20: 云路由网络/VPC下弹性IP的应用场景



背景信息

以下介绍扁平网络环境下弹性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. 搭建扁平网络，并使用扁平三层私网创建一台云主机VM-1。详情可参考本教程基本部署章节。
2. 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 *21: 新建虚拟IP*所示：

    图 21: 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 *22: 已有虚拟IP*所示：

    图 22: 已有虚拟IP

如图 *23: 创建弹性IP*所示：

图 23: 创建弹性IP

3. 将EIP-1绑定VM-1。

   云主机网卡可在创建弹性IP时直接添加，也可在创建弹性IP后再添加。

以创建弹性IP时直接绑定云主机网卡为例。在**创建弹性IP**界面点击**确定**后，会跳转到**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，选择需要绑定的云主机，如：VM-1，点击**确定**。

如图 *24: 选择VM-1*和图 *25: 将EIP-1绑定VM-1*所示：

图 24: 选择VM-1

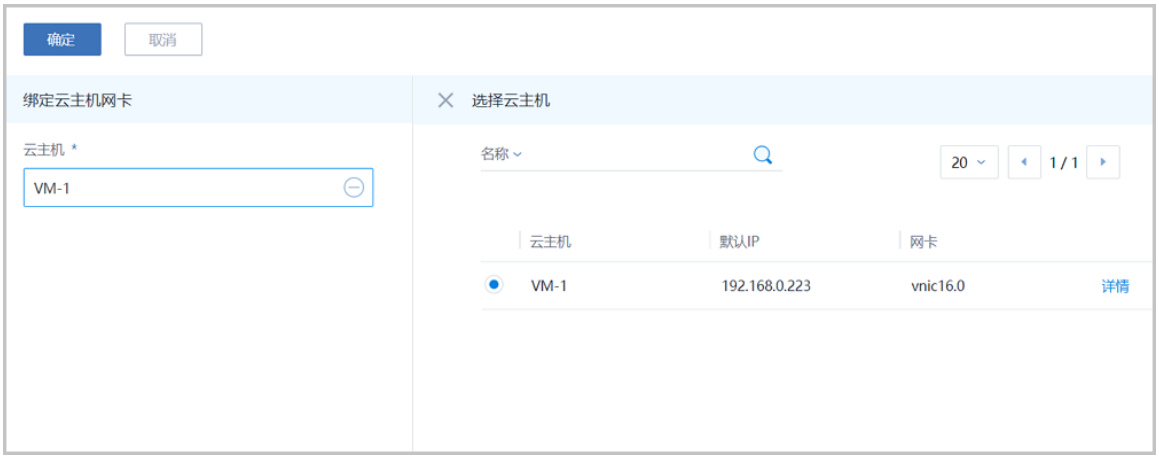
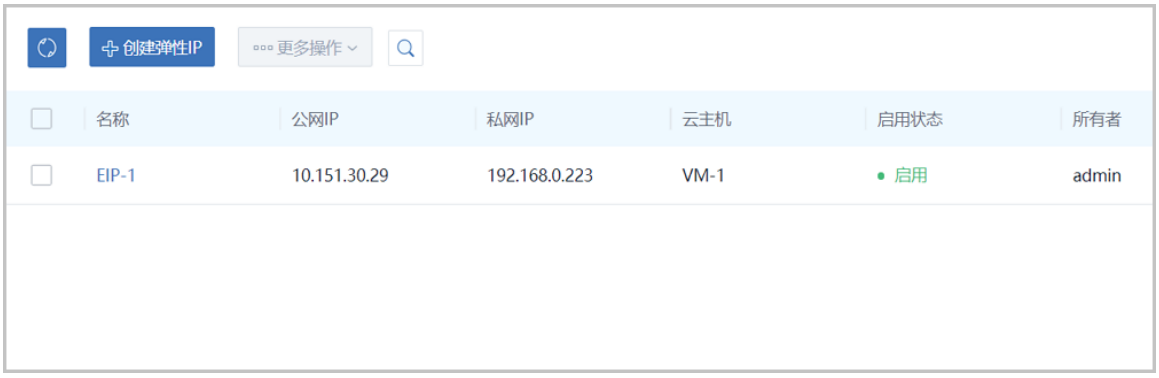


图 25: 将EIP-1绑定VM-1



4. 通过EIP-1登录VM-1。

使用某一可访问扁平网络公网网段（*10.151.30.0~10.151.30.30*）的主机SSH登录EIP-1：*10.151.30.29*，也就是登录到私网IP为*192.168.0.223*的VM-1。如图 *26: 通过EIP-1登录VM-1*所示：

图 26: 通过EIP-1登录VM-1

```
[root@10-0-93-37 ~]# ssh 10.151.30.29
The authenticity of host '10.151.30.29 (10.151.30.29)' can't be established.
ECDSA key fingerprint is 82:cf:07:ff:68:f0:ab:4f:33:3b:da:a9:74:3b:b2:c9.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.151.30.29' (ECDSA) to the list of known hosts.
root@10.151.30.29's password:
Last login: Wed Jan 10 06:37:59 2018
-bash-4.2# ip r
default via 192.168.0.1 dev eth0
192.168.0.0/16 dev eth0  proto kernel  scope link  src 192.168.0.223
-bash-4.2#
```

5. 将EIP-1绑定其它云主机。

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 *27: 将EIP-1从VM-1解绑*所示：

图 27: 将EIP-1从VM-1解绑

b) 将EIP-1绑定其它云主机。

弹性IP解绑后，可以点击**绑定**按钮重新绑定到其他云主机。

至此，扁平网络弹性IP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、FusionStor、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。