管理与配置教程

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。

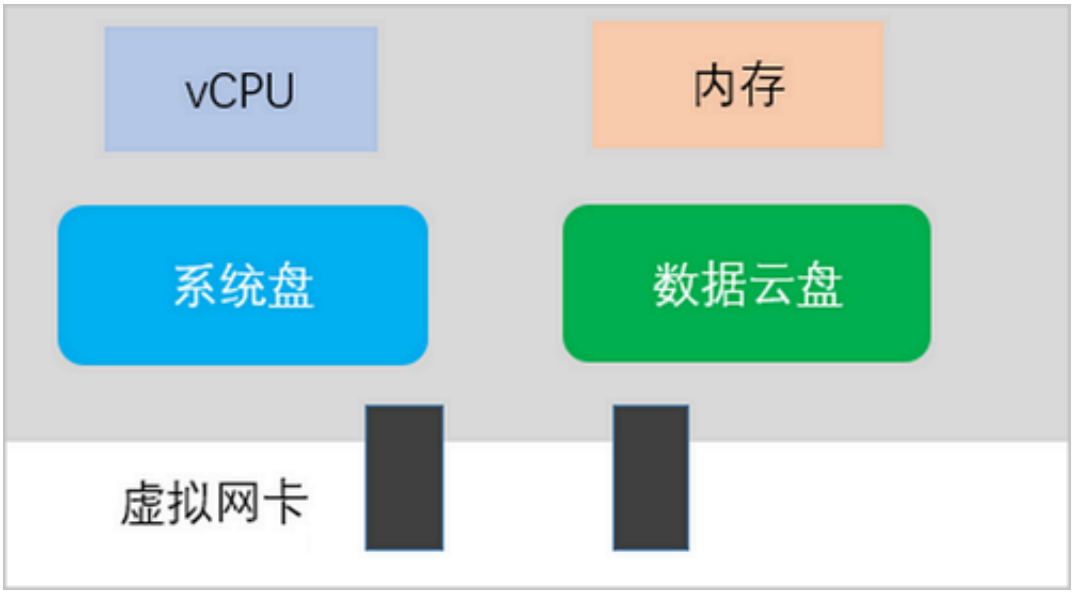
目录

1 云主机原理

云主机是用户安装与运行应用服务的基础环境，云主机可运行完整操作系统，不同云主机可运行不同的操作系统，例如：Windows、Linux和BSD等。用户获得云主机后，访问方式和使用习惯与传统物理主机租赁服务类似，可任意安装合适计算架构和操作系统环境的应用程序。

云主机由以下资源共同组成：vCPU、内存、系统云盘、数据云盘和虚拟网卡等。如图 1: 云主机组成所示：

图 1: 云主机组成



vCPU

vCPU（Virtual CPU，虚拟CPU），通过处理器分时技术实现计算资源时间片共享，在时间上分配CPU处理资源。

在CPU硬件虚拟化技术的辅助下，云主机内部执行的二进制指令可直接透传到硬件虚拟化接口，执行成功后返回。

硬件虚拟化技术相比传统纯软件模拟方式，其执行效率得到优化，vCPU与物理CPU执行效率相当。云主机的vCPU资源数量，可以通过更改计算规格进行调整。如图 2: 云主机计算规格所示：

图 2: 云主机计算规格

云主机内存

云主机内存，是直接在物理主机内存分配的逻辑区域。

在云主机内部，内存访问地址是连续的，而映射到物理主机的内存空间并非连续（根据虚拟化实现有所差异）。

虚拟化技术方案实现云主机内存到物理主机内存的映射，能让云主机运行的操作系统在不作变更或者翻译的情况下，就可以访问物理主机内存空间。云主机的内存资源数量可以通过更改计算规格进行调整。

云主机系统云盘与数据云盘

系统云盘（Root Volume）：承载云主机操作系统（Guest OS）。

注: 云主机操作系统安装在系统云盘内，云主机启动时候即读取系统云盘数据。系统云盘的生命周期与云主机紧密关切，当云主机被销毁时，系统云盘即销毁。

数据云盘（Data Volume）：用于存放应用运行的数据，应用程序可安装到数据云盘。

注: 数据云盘的生命周期独立于云主机，可动态加载到云主机上（云主机操作系统需格式化数据云盘后使用），当云主机被销毁时，数据云盘将被卸载。如图 3: 云主机云盘规格所示：

图 3: 云主机云盘规格

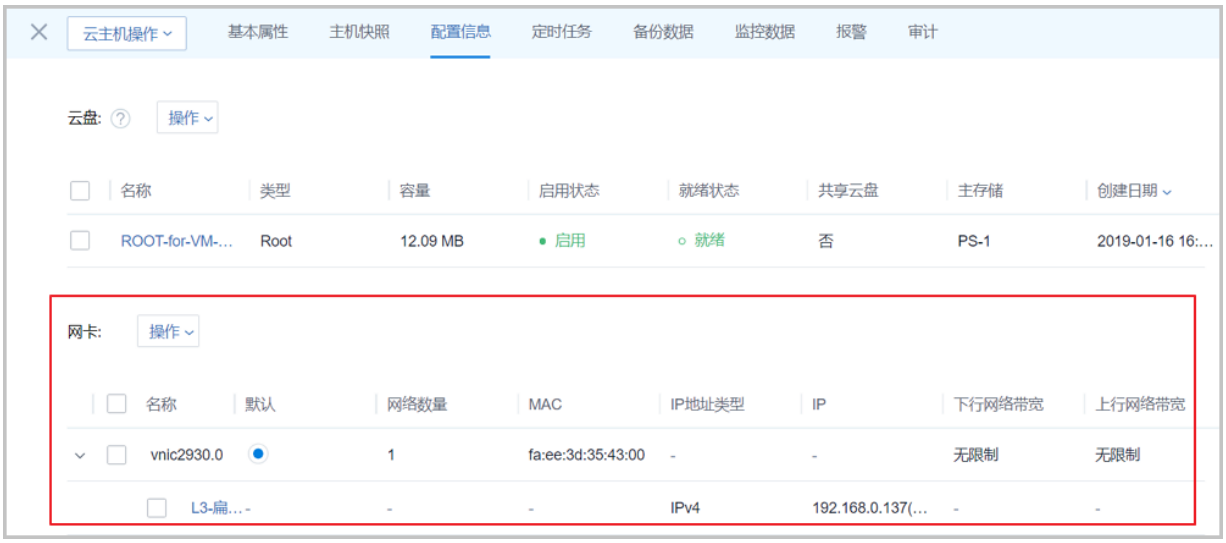
虚拟网卡

vNIC（Virtual NIC，虚拟网卡），是云主机与外部通信的网络设备。

创建云主机时，需要选择至少一个网络，从该网络中分配IP地址创建虚拟网卡。云主机启动前，vNIC附加到云主机；云主机启动后，云主机操作系统引导初始化，在默认配置下发起DHCP请求，收到DHCP请求后，云主机操作系统将在vNIC上配置网络信息。

此时，云主机即可获得网络访问，用户可通过操作系统远程访问协议进行交互操作。如图 *4:* 云主机虚拟网卡所示：

图 4: 云主机虚拟网卡



云主机操作

当需要删除云主机时，在**云主机**页面点击**更多操作** > **删除**按钮，云主机会变为**已删除**状态。如删除云主机所示：

图 5: 删除云主机

此时云主机并未完全删除，在**已删除**页面点击**恢复**或**彻底删除**按钮，可进行相应操作。

- 点击**恢复**按钮，表示将云主机由**已删除**状态转变为**可用**状态。
- 点击**彻底删除**按钮，表示将云主机各项资源回收。此时，云主机的数据云盘将被卸载（若挂载），系统云盘将会彻底删除。

如云主机操作所示：

图 6: 云主机操作

注: 用户务必注意彻底删除操作的作用对象，以免数据误删。

2 虚拟化技术

目前，ZStack仅支持**KVM**和**VMware vCenter**虚拟化技术。

2.1 KVM虚拟化

KVM，全称 Kernel-based Virtual Machine，即内核虚拟机。提供 KVM 虚拟化运行环境的物理主机，下文简称“KVM 主机”。

介绍

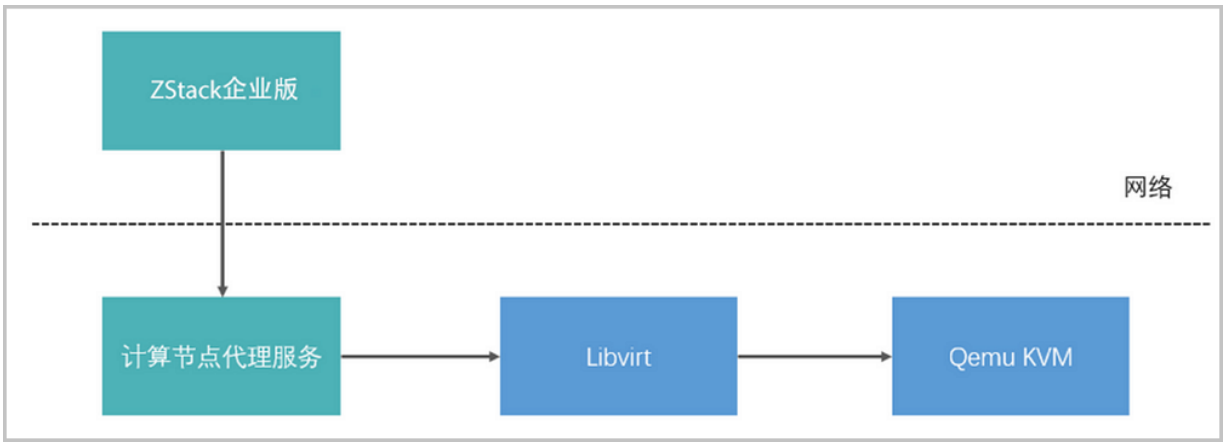
KVM 虚拟化技术包含两种实现方式：内核模块和用户空间应用程序。目前主流的 Linux 操作系统如 RHEL/CentOS 6.x/7.x，Debian 7/8 和 Ubuntu 14.04+已经完整支持 KVM 虚拟化。

虚拟机运行在 Qemu 进程内，并通过 Qemu-KVM 模块与 Linux 的 KVM 虚拟设备/dev/kvm 通信，即完成二进制指令透传。

ZStack-KVM

ZStack 对计算资源进行统一管理，在 KVM 主机上部署代理服务（zstack-kvmagent），代理服务将接收来自管理服务器的请求，完成各项指派任务。对于云主机的配置，代理服务器将与Libvirt 组件对接，下发云主机创建信息（XML）。如图 7: 通信结构所示：

图 7: 通信结构



具体操作

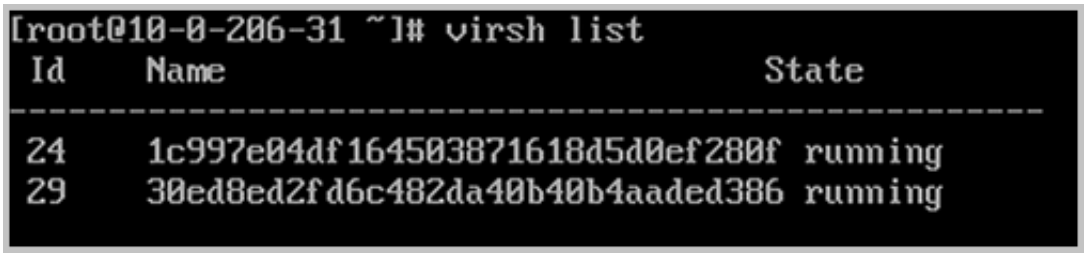
ZStack管理服务后端连接MariaDB数据库，云主机定义信息核心元素均存放在数据库。

创建云主机时，管理服务发送消息到代理服务，由此生成云主机XML配置。然后将XML配置发布到Libvirt，并触发启动信号，云主机创建成功。

执行以下命令可登录 KVM 主机并查看当前KVM主机所运行的云主机，如图 *8: KVM主机的云主机运行信息*所示：

```
[root@kvm-1 ~]# virsh list --all
```

图 8: KVM主机的云主机运行信息



执行以下命令可显示云主机的 XML 配置:

```
[root@kvm-1 ~]# virsh dumpxml 30ed8ed2fd6c482da40b40b4aaded386
```

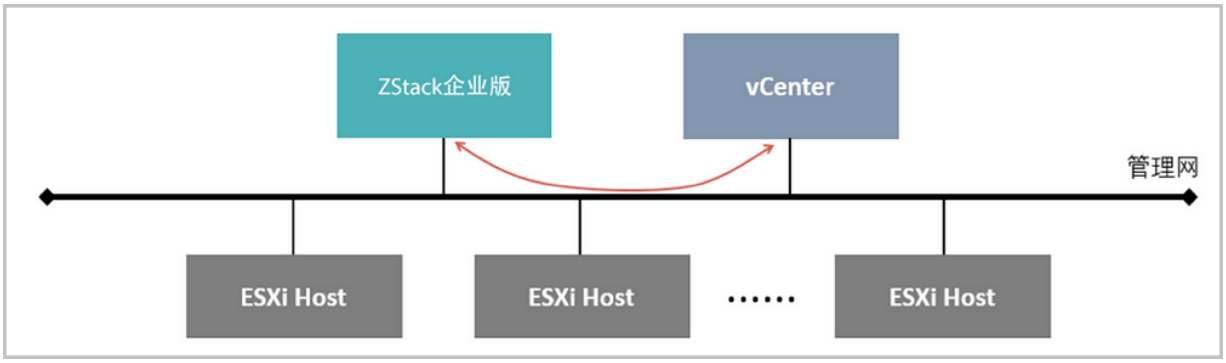
2.2 vCenter虚拟化

VMware vCenter（简称 vCenter）是企业中常见的服务器资源虚拟化技术。ZStack支持vCenter 5.5和vCenter 6.0版本。

管控逻辑模型

管理员可透过ZStack管理vCenter的虚拟化资源，并通过Web方式将资源的分配和使用情况呈现。ZStack与vCenter的管控逻辑模型如图 *9: ZStack与vCenter管理控制逻辑图*所示：

图 9: ZStack与vCenter管理控制逻辑图



添加vCenter资源

ZStack上可直接添加vCenter资源：在ZStack左侧菜单栏点击**vCenter** > **基础资源**按钮，在**基础资源**页面点击**添加vCenter**按钮，弹出**添加vCenter**页面，可参考以下示例输入相应内容：

- **名称**：设置需要添加的vCenter名称
- **域名**：设置访问域名地址
- **端口号**：设置开放端口号，默认443
- **用户名**：设置用户名称
- **密码**：设置用户名对应的密码
- **HTTPS/HTTP**：选择同步vCenter时的传输协议，支持HTTPS和HTTP，默认HTTPS

如图 *10: ZStack界面添加vCenter*所示，点击**确定**按钮，完成vCenter创建。

图 10: ZStack界面添加vCenter

成功登录后，ZStack将会拉取目前vCenter的运行信息，包括数据中心、集群、物理服务器、存储设备、分布式交换机、云主机和镜像模板等。

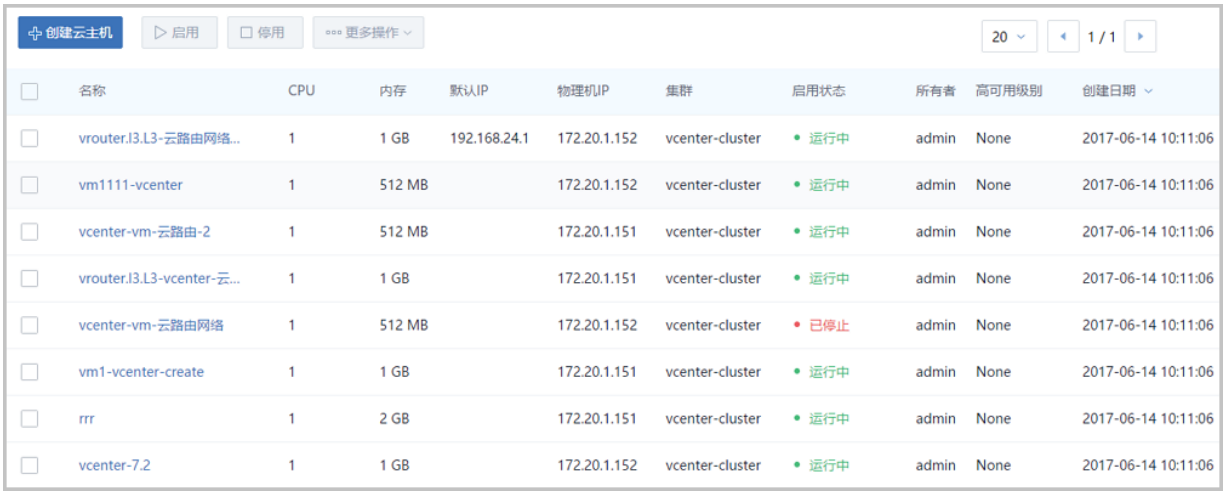
资源呈现特性

ZStack支持vCenter的资源呈现有以下特性：

- 支持显示集群、物理主机和虚拟主机信息以及其运行状态。
- 支持显示共享存储，包括FC、iSCSI和NFS存储。
- 支持分布式交换机的端口组信息，不支持标准交换机。
- 支持镜像模板显示，显示vCenter已经存在的模板。

如图 *11: ZStack显示vCenter存在的虚拟机*所示：

图 11: ZStack显示vCenter存在的虚拟机



3 存储池管理

3.1 云盘原理

云盘是在统一的存储资源池里分配的块设备资源。ZStack技术体系里，云盘分为系统云盘和数据云盘两类。

系统云盘

云主机系统云盘（Root Volume）用于承载云主机操作系统（Guest OS），云主机必须具备一块系统云盘。系统云盘的生命周期与云主机紧密相关，当云主机被销毁时，系统云盘同时被销毁。若云主机通过ISO光盘部署，系统云盘的容量为指定的云盘规格；若云主机通过模板镜像部署，其系统云盘的容量与模板容量一致。

数据云盘

数据云盘（Data Volume）用于存放应用运行的数据，用户可把应用程序安装到数据云盘。云主机支持加载多块数据云盘，加载后通过云主机操作系统的磁盘管理工具对该数据云盘进行格式化使用。数据云盘的生命周期是独立于云主机，可在关机或运行状态下加载到云主机上。当云主机被销毁时，数据云盘将被卸载。如图 *12:* 数据云盘显示面板所示：

图 12: 数据云盘显示面板

ZStack相关支持

- 支持云盘迁移。
- 支持创建云盘快照。
- 支持创建多个数据云盘。

3.2 本地存储

背景信息

ZStack支持利用计算节点的本地空间作为主存储。本地存储的操作通过KVM主机代理服务完成，包括创建、挂载、卸载、删除和快照等动作。

操作步骤

1. 选择本地存储类型

在主存储配置步骤，选择**本地存储**（LocalStorage）类型。如图 *13:* 选择本地存储所示：

图 13: 选择本地存储

选择本地存储后，需要填写本地存储URL路径，提示填写路径*/zstack_ps*作为主存储，也可以填写自定义路径。

注:

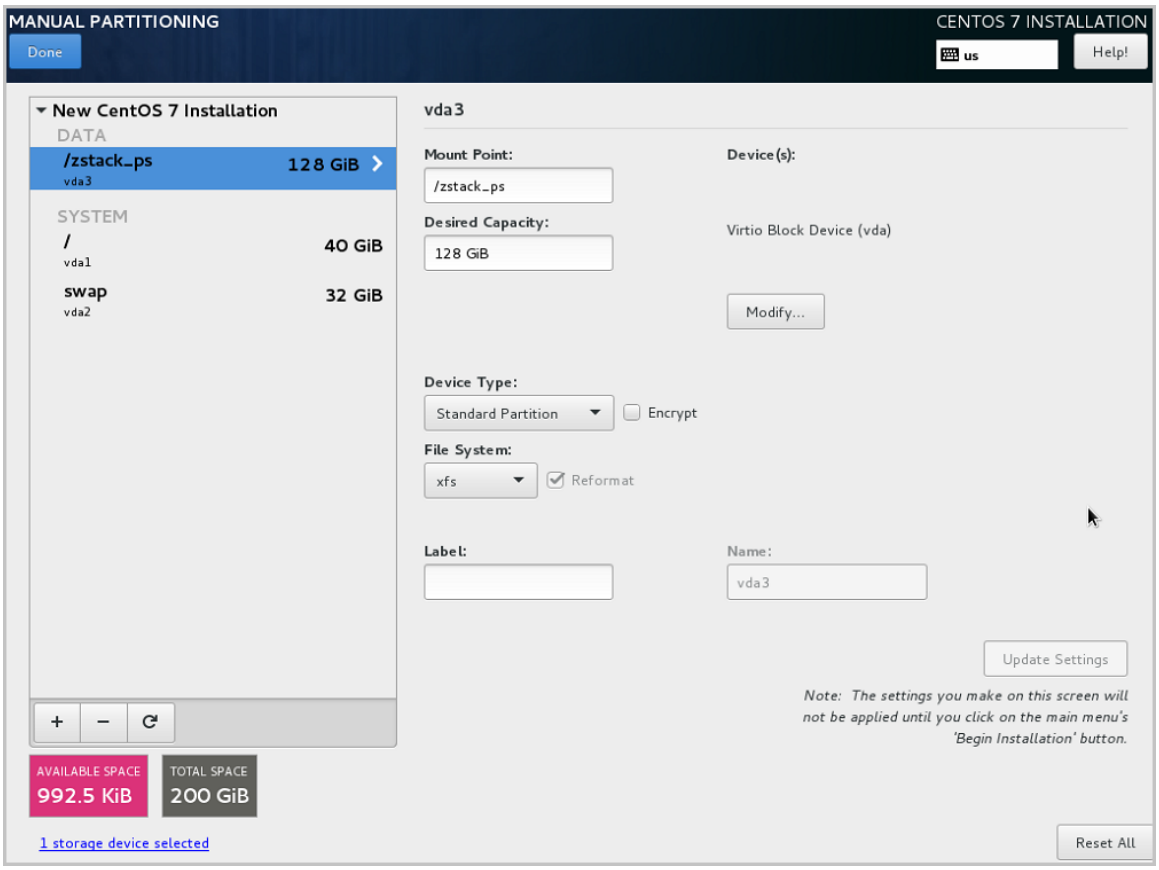
填写主存储路径时，建议路径由单独的硬盘设备分区提供存储空间，尽量避免直接使用根目录，防止消耗根目录大量空间。

由于Linux操作系统*/root*目录只允许root权限访问，所以管理员不能将*/root*以下的文件目录作为主存储空间。

2. 创建主存储分区

ZStack支持KVM主机使用本地空间作为主存储。安装操作系统过程中，为减少后续的存储目录创建操作，建议在安装Linux操作系统时，创建主存储分区并设定挂载点，如图 *14: CentOS 7创建本地存储空间*所示：

图 14: CentOS 7创建本地存储空间



3. 查询主存储信息

在ZStack左侧菜单栏点击**硬件设施** > **主存储**按钮，在**主存储**页面点击主存储名称可查看主存储信息。如图 *15:* 主存储-本地存储所示：

图 15: 主存储-本地存储

4. 本地存储文件目录信息

ZStack在本地存储路径创建以下文件目录：

- **Imagecache**：镜像缓存目录，存放模板和ISO镜像的缓存。
- **RootVolumes**：系统云盘目录，存放云主机系统云盘。
- **DataVolumes**：数据云盘目录，存放云主机数据云盘。

在**云主机**页面，点击云主机名称，再点击**配置信息**按钮，可看到云盘列表，点击云盘名称就可以看到云盘的详细信息如图 *16:* 云盘详情所示：

图 16: 云盘详情

点击**安装路径**后面的复制按钮，可登录到KVM主机查看云盘信息，如图 *17: KVM主机查看云盘信息*所示：

图 17: KVM主机查看云盘信息

```
[root@10-0-211-87 ~]# qemu-img info /zstack_ps/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e/vol-ae62268e5
ba7491face04a44103e3188/ae62268e5ba7491face04a44103e3188.qcow2
image: /zstack_ps/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e/vol-ae62268e5ba7491face04a44103e3188/ae622
68e5ba7491face04a44103e3188.qcow2
file format: qcow2
virtual size: 12M (12682240 bytes)
disk size: 16M
cluster_size: 2097152
backing file: /zstack_ps/imagecache/template/355148c3421d4c55872a01c5f1b7486f/355148c3421d4c55872a01c5f1b7486f
.qcow2
backing file format: qcow2
Format specific information:
    compat: 1.1
    lazy refcounts: false
    refcount bits: 16
    corrupt: false
```

5. 迁移特性

   本地存储场景，不支持云主机在线迁移；停止状态的云主机可进行冷迁移。

   注: 云主机迁移时，将对系统云盘和所加载的数据云盘进行迁移。如果云盘处于卸载状态，可进行单独迁移。云主机只允许加载相同KVM主机的云盘。

6. 高可用特性

   在本地存储场景，不支持云主机高可用特性。

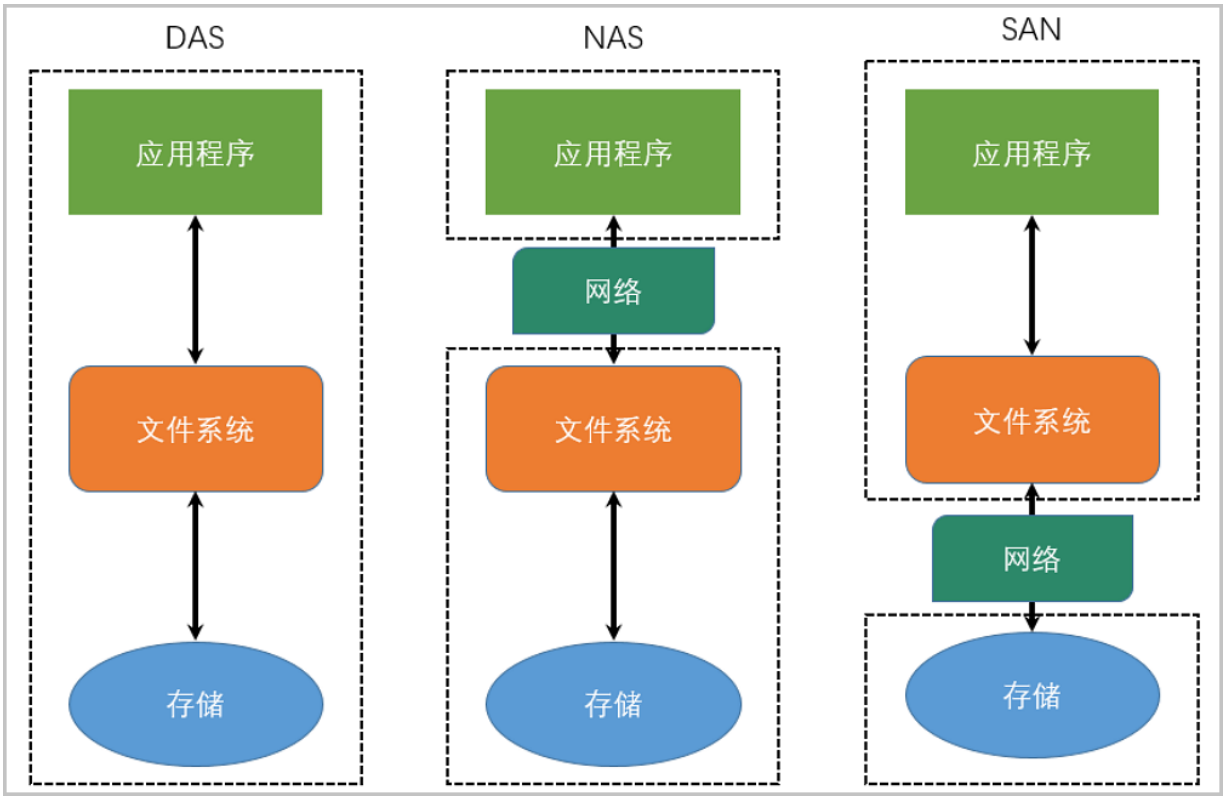
3.3 SAN存储

ZStack支持使用SAN作为主存储，支持SAS、iSCSI、FC和FCoE存储。

SAN存储与其他类型存储的区别

SAN存储是一种连接外接存储设备和服务器的架构，其特点是：它被操作系统识别为直接相连的存储块设备。DAS、NAS和SAN是经常被提及的存储类型，区别如图 *18: KVM主机查看云盘信息*所示：

图 18: KVM主机查看云盘信息



- NAS较为容易使用，不需要额外文件系统。
- DAS存储设备不存在共享访问点，可直接采用常用文件系统，例如：EXT3/4和XFS（DAS则使用本地存储类型）。
- 由于SAN通过网络共享访问块设备存储，需要使用共享文件系统，例如GFS2、OCFS2和VMware VMFS。

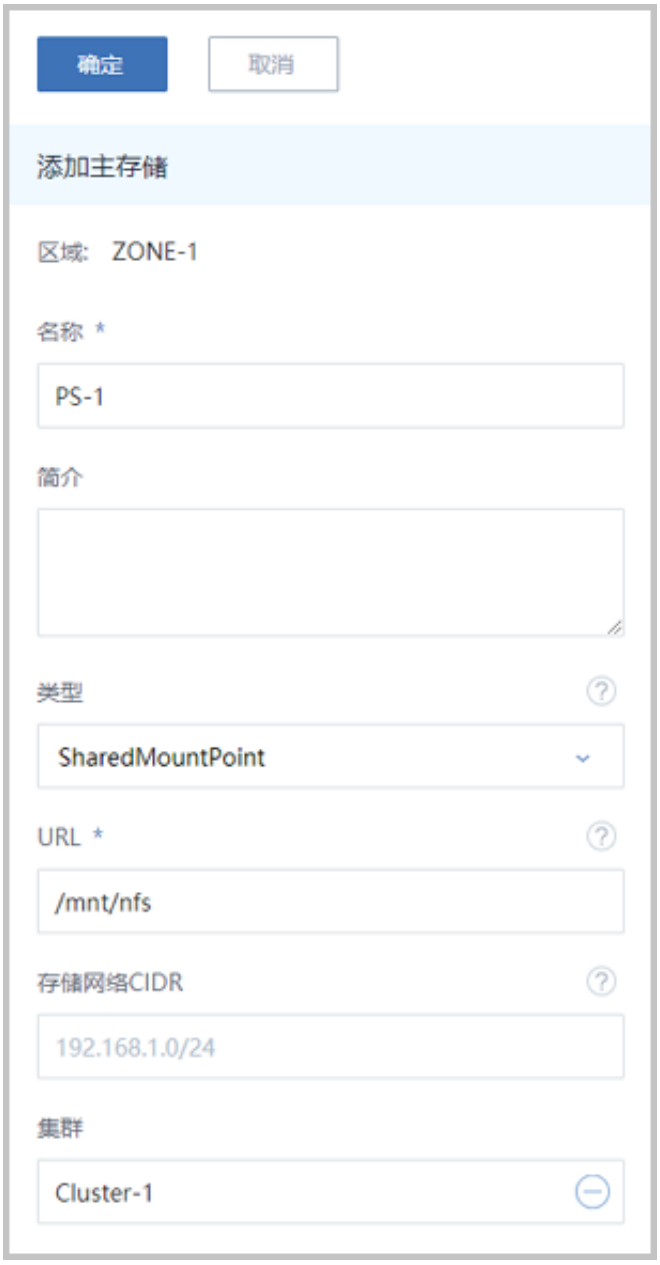
部署共享文件系统后，每个服务器节点即可访问相同的目录路径。

使用共享存储挂载访问SAN存储

KVM虚拟化场景使用共享存储挂载访问SAN存储时，管理员需要在KVM主机预先安装GFS2或OCFS2共享文件系统，完成后，KVM主机可共同访问挂载点，例如：*/opt/smp/*。

ZStack对共享存储的操作通过KVM主机代理服务完成，包括创建、挂载、卸载、删除和快照等动作。主存储配置步骤提供共享存储挂载点（Share Mount Point），如图 *19:* 选择共享存储所示：

图 19: 选择共享存储



查看共享存储信息

在ZStack左侧菜单栏点击**硬件设施** > **主存储**按钮，在**主存储**页面点击主存储名称可查看共享存储信息。如图 *20: ZStack*主存储-共享存储所示：

图 20: ZStack主存储-共享存储

共享存储文件目录信息

共享存储目录结构，与本地存储类似。ZStack在共享存储路径创建以下文件目录：

- **Imagecache**：镜像缓存目录，存放模板和ISO镜像的缓存。
- **RootVolumes**：系统云盘目录，存放云主机系统云盘。
- **DataVolumes**：数据云盘目录，存放云主机数据云盘。

在共享存储场景，系统云盘和数据云盘具体所在路径可通过云盘信息获得，与本地存储类似。

迁移特性

共享存储场景，支持云主机在线迁移。

高可用特性

共享存储场景，支持云主机高可用特性。若需要开启主机高可用特性，需要满足：

1. 在ZStack左侧系统菜单栏点击**设置** > **全局设置**按钮，在**全局设置**页面将配置**云主机高可用全局开关**状态调整为**ture**状态。如图 *21:* 设置云主机高可用开关所示：

图 21: 设置云主机高可用开关

2. 点击**云资源池** > **云主机**在**云主机**界面点击云主机名称，设定云主机高可用级别为**NeverStop**。如图 *22:* 修改高可用级别所示：

图 22: 修改高可用级别

开启高可用模式后， KVM代理对共享目录定期写入，并把检测信息通知给管理服务，以提供高可用切换机制判断依据。如图 *23: ZStack*高可用机制-共享存储心跳检测所示：

图 23: ZStack高可用机制-共享存储心跳检测

```
[root@       zstack-ps]# dir
dataVolumes                                          heartbeat-file-kvm-host-7a3ae71919b0457a9a7ed3f04f40b5b0.hb
heartbeat-file-kvm-host-242415d92592443eb38d65fcacca863f.hb  heartbeat-file-kvm-host-cfc711234c4642168e567a831b14817c.hb
heartbeat-file-kvm-host-2f7c1ff2ccc84854b7168f22f9759a96.hb  imagecache
heartbeat-file-kvm-host-70f5688839604ab0a4e28335e9757f62.hb  rootVolumes
```

3.4 NAS存储

NAS存储是基于标准网络协议实现数据传输，为网络中不同操作系统的计算机提供文件共享访问的方式。ZStack在KVM虚拟化场景中支持NFS存储。

选择NAS存储类型

ZStack通过KVM主机代理服务完成对NFS存储的操作，包括云盘创建、加载、卸载、删除和快照等动作。主存储配置步骤提供NFS存储类型。如图 *24:* 选择*NFS*存储所示：

图 24: 选择NFS存储

进行挂载操作

NFS存储添加后，将对所有KVM主机创建挂载点*/opt/zstack/nfsprimarystorage/UUID*，并进行mount -t nfs挂载操作。

注: 此过程通过代理服务完成，并在KVM主机重连时检测NFS挂载点状况，若无挂载则尝试挂载操作。

查看存储信息

在ZStack左侧菜单栏点击**硬件设施** > **主存储**按钮，在**主存储**页面点击主存储名称可查看查看NFS存储信息。如图 25: ZStack主存储-NFS存储所示：

图 25: ZStack主存储-NFS存储

NFS存储文件目录信息

NFS存储目录结构，与本地存储相似。ZStack在NFS路径创建以下文件目录：

- **Imagecache**：镜像缓存目录，存放模板和ISO镜像的缓存。
- **RootVolumes**：系统云盘目录，存放云主机系统云盘。
- **DataVolumes**：数据云盘目录，存放云主机数据云盘。

在NFS存储场景，系统云盘和数据云盘具体所在路径可通过云盘信息获得，与本地存储类似。

迁移特性

在NFS存储场景，支持云主机在线迁移。

高可用特性

在NFS存储场景，支持云主机高可用特性。若需要开启主机高可用特性，需要满足：

1. 在ZStack左侧系统菜单栏点击**设置** > **全局设置**按钮，在**全局设置**页面将配置**云主机高可用全局开关**状态调整为**ture**状态。如图 *26:* 设置云主机高可用开关所示：

图 26: 设置云主机高可用开关

2. 点击**云资源池** > **云主机**在**云主机**界面点击云主机名称，设定云主机高可用级别为**NeverStop**。如图 *27:* 修改高可用级别所示：

图 27: 修改高可用级别

与SAN共享存储相似，ZStack开启高可用模式后，KVM代理对NFS共享目录定期写入，并把检测信息通知给管理服务，以提供高可用切换机制判断依据。

3.5 分布式存储

分布式存储是将数据分散到不同的存储单元（Storage Unit）上。它满足在线横向扩容（Scale-Out）特性，可实现数据不断增长。目前分布式存储在云计算虚拟化场景中，主要用于存放云盘数据，主要以提供标准POSIX文件和块设备这两类访问方式。

为防止单点或多点失效后数据不可用或丢失，分布式存储实现数据冗余机制，例如：副本（Replication）和纠删码（Erasure Coding）：

- 副本即把一份原始数据复制若干份，再把相同的数据分散到不同的存储单元，与传统阵列技术RAID 10相似；
- 纠删码即把原始数据分割成片段，把冗余数据块扩展和编码后分散到不同的存储单元，与传统阵列技术RAID 5/6相似。

注: 纠删码相对副本而言，其空间有效利用率将提高，通常达到80%，而副本只能达到50%（两副本）或33%（三副本）;由于纠删码存在写惩罚，故副本的效能相对较高。

POSIX（Portable Operating System Interface）为可移植操作系统接口，是IEEE为各种UNIX操作系统上运行的软件定义一系列API标准总称。POSIX文件访问是目前支持最多的访问方式，应用程序能很方面地进行读写操作。不同的分布式存储实现独自的文件系统挂载方式（mount），允许多客户端读写相同目录，提供标准的POSIX文件访问。常见支持POSIX文件访问的开源分布式存储有MooseFS、GlusterFS和Lustre。

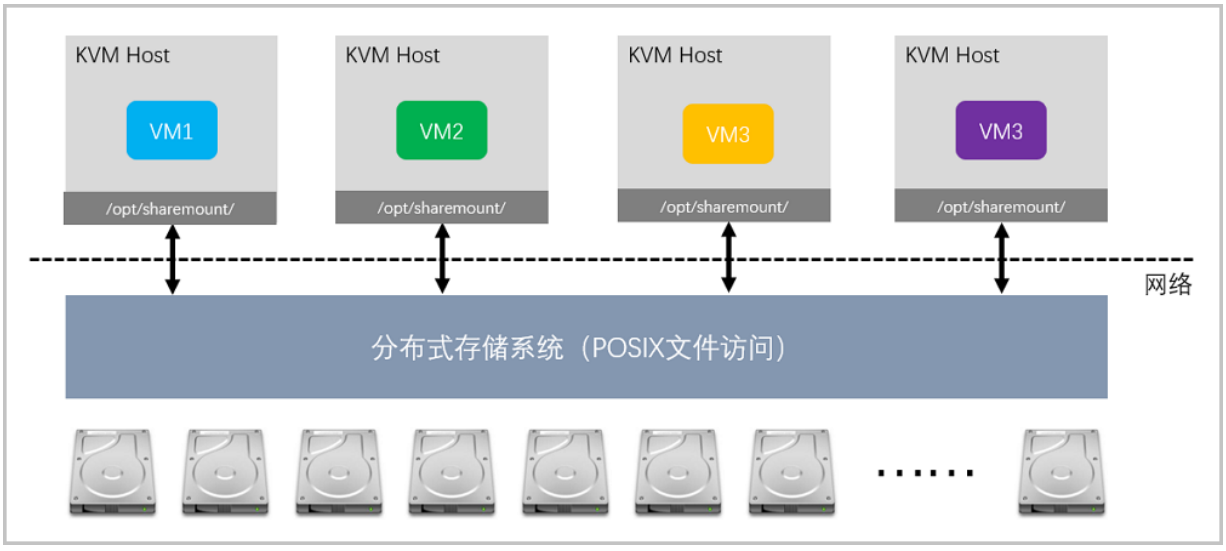
目前，ZStack在KVM虚拟化场景支持分布式存储POSIX文件访问和Ceph RBD块设备访问。

3.5.1 分布式存储-文件共享

逻辑架构

KVM虚拟化场景下，分布式存储POSIX文件访问的逻辑架构如图 *28: KVM虚拟化场景分布式存储POSIX文件访问*所示：

图 28: KVM虚拟化场景分布式存储POSIX文件访问

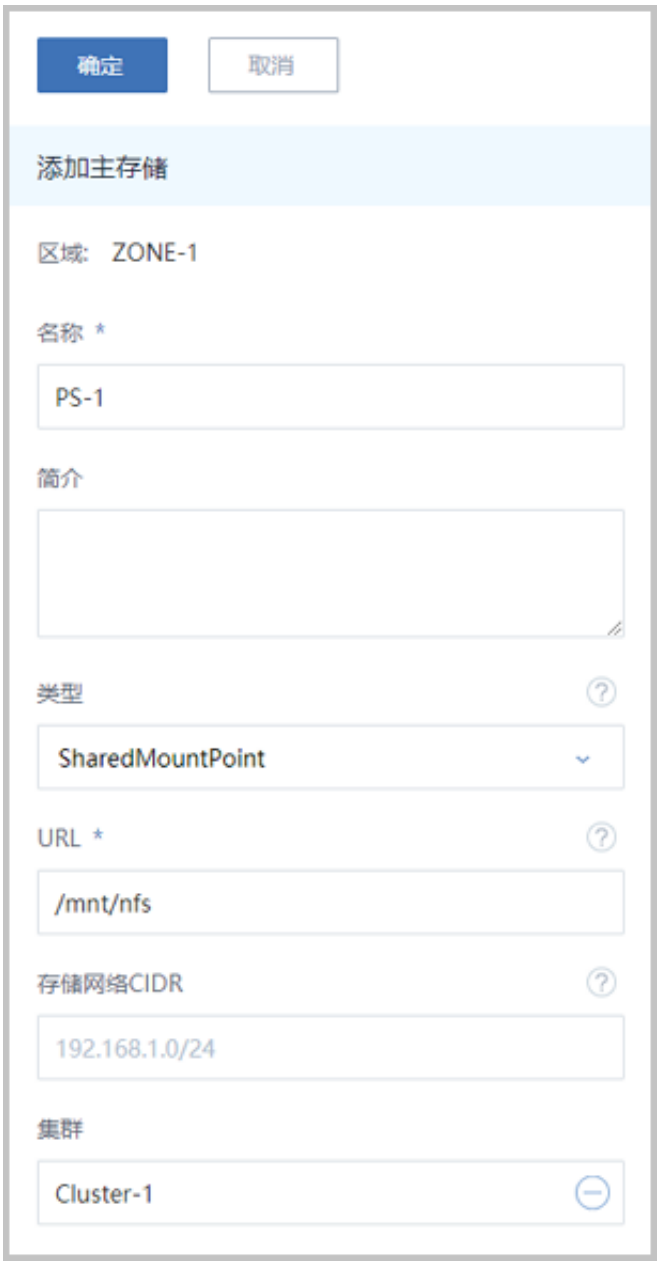


选择分布式存储-文件共享

对于分布式存储POSIX文件访问类型，需要预先在KVM主机节点手动进行挂载操作。若需要KVM主机开机后自动挂载文件系统，管理员可根据存储挂载的操作方式，填写自动挂载信息到*/etc/fstab* 。

ZStack与此类分布式存储对接时，无需在分布式存储节点里安装代理服务，存储空间使用情况，以及云盘创建、快照和删除等操作将在KVM主机发起。云盘格式以RAW和QCOW2类型存放。如图 *29: ZStack主存储-分布式存储共享访问*所示：

图 29: ZStack主存储-分布式存储共享访问



分布式存储目录信息

分布式存储POSIX文件访问的目录结构，与NAS存储相似。ZStack在共享存储路径创建以下文件目录：

- **Imagecache**：镜像缓存目录，存放模板和ISO镜像的缓存。
- **RootVolumes**：系统云盘目录，存放云主机系统云盘。
- **DataVolumes**：数据云盘目录，存储云主机数据云盘。

与NAS存储类似，管理员可通过云盘路径查找具体所在位置。

迁移特性

分布式存储文件共享访问场景，支持云主机在线迁移。

高可用特性

在分布式存储文件共享访问场景，支持云主机高可用特性。

1. 在ZStack左侧系统菜单栏点击**设置** > **全局设置**按钮，在**全局设置**页面将配置**云主机高可用全局开关**状态调整为**ture**状态。如图 *30:* 设置云主机高可用开关所示：

图 30: 设置云主机高可用开关

2. 点击**云资源池** > **云主机**在**云主机**界面点击云主机名称，设定云主机高可用级别为**NeverStop**。如图 *31:* 修改高可用级别所示：

图 31: 修改高可用级别

与NAS共享存储相似，ZStack开启高可用模式后，KVM主机对共享目录定期写入，并把检测信息通知给管理服务，以提供高可用切换机制判断依据。

3.5.2 分布式存储-块设备

块设备是将信息存储在有固定地址固定大小的块中。例如：常见类似**/dev/sda**和**/dev/sdb**是块设备，而经过分区**/dev/sdb1**和**/dev/sdb2**也属于块设备，LVM卷管理提供的逻辑卷也属于块设备。

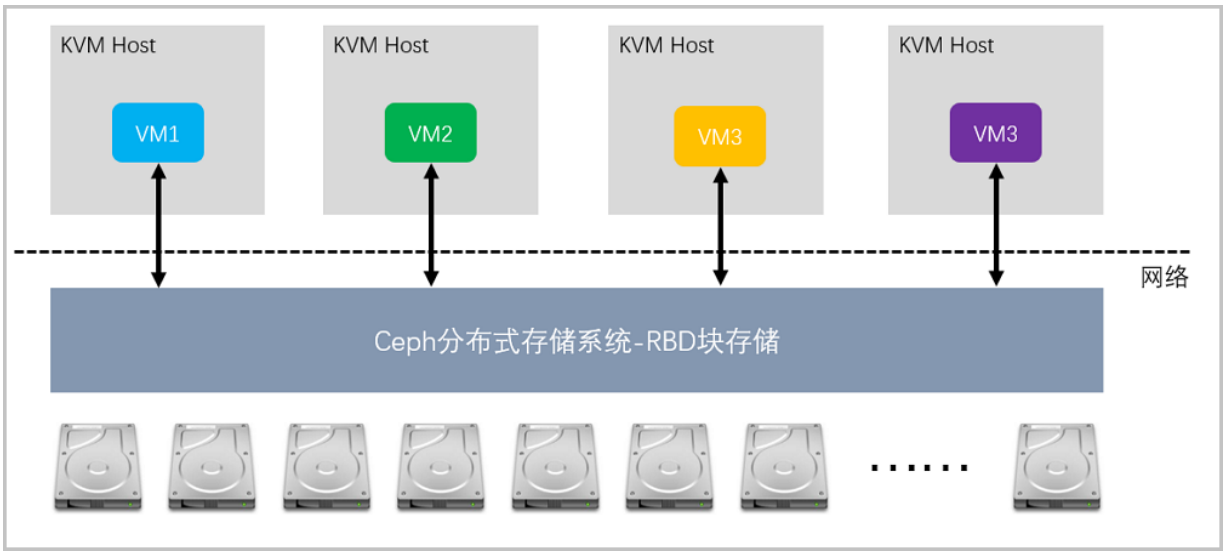
云盘在云主机内部表现形式为块设备，虚拟化管理程序（KVM）可将外部的块设备直接映射给云主机，当进行大量IO读写时，可减少中间文件系统的性能损耗，提高读写效能，获得更低的延迟性能。

3.5.2.1 Ceph分布式存储

Ceph分布式存储存储方案

ZStack支持Ceph分布式存储的RBD块存储方案，同时支持主存储和镜像服务器。如图 *32: KVM虚拟化场景Ceph RBD块存储访问*所示：

图 32: KVM虚拟化场景Ceph RBD块存储访问



添加Ceph RBD块存储

主存储和镜像服务器添加Ceph RBD块存储。如图 *33: ZStack添加Ceph RBD*所示：

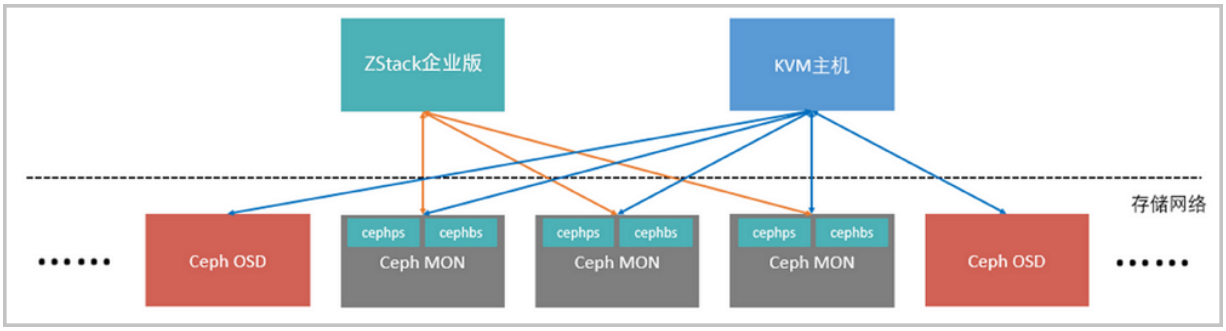
图 33: ZStack添加Ceph RBD


确定
取消
添加主存储
区域: ZONE-1
名称 *
PS-1
简介
类型
Ceph
关闭 CEPHX
Mon IP *
192.168.0.1
SSH端口 *
22
用户名 *
root
密码 *
••••••••
继续添加
镜像缓存池名
数据云盘池名
根云盘池名
存储网络CIDR
192.168.1.0/24
集群

存储对接

ZStack与Ceph分布式存储对接时，填写Ceph MON节点的IP地址和root密码，将安装主存储代理服务和镜像服务器代理服务，负责对Ceph的存储空间使用情况和其他状态的监控，以及发起RBD镜像的创建、快照和删除等操作。如图 *34: 主存储-分布式存储Ceph RBD访问原理*所示：

图 34: 主存储-分布式存储Ceph RBD访问原理



生成RBD块存储的云盘XML访问格式

添加MON过程中，ZStack将创建访问密钥，该密钥提供KVM主机用于访问RBD块镜像。ZStack根据提供的MON节点IP地址，在KVM主机上创建云主机时，将生成RBD块存储的云盘XML访问格式。如图 *35: ZStack云主机使用RBD作为云盘*所示：

图 35: ZStack云主机使用RBD作为云盘

```
<disk type='network' device='disk'>
  <driver name='qemu' type='raw'/>
  <auth username='zstack'>
    <secret type='ceph' uuid='acac5612-ae16-4f97-bcd2-f3a4348ebee5'/>
  </auth>
  <source protocol='rbd' name='pri-v-r-26ecf9c8c2314a9fa47b29253ea34858/4182e6ec78a3401cb37ad74582fcf5a3'>
    <host name='172.20.1.14' port='6789'/>
    <host name='172.20.1.13' port='6789'/>
    <host name='172.20.1.12' port='6789'/>
  </source>
  <backingStore/>
  <target dev='vda' bus='virtio'/>
  <alias name='virtio-disk0'/>
  <address type='pci' domain='0x0000' bus='0x00' slot='0x04' function='0x0'/>
</disk>
```

查看存储池

ZStack与Ceph对接过程中，默认创建若干存储池，查看方式：`ceph osd lspools`

- **pri-c-xxxxxx**： 镜像缓存目录，存放模板和ISO镜像的缓存。
- **pri-v-r-xxxxx**：系统云盘目录，存放云主机系统云盘。
- **pri-v-d-xxxxx**：数据云盘目录，存储云主机数据云盘。
- **bak-t-xxxx**： 镜像服务器目录，存放模板和ISO镜像。

默认情况下，ZStack添加Ceph作为主存储时，将会创建三个存储池（Pool）。若管理员已经在Ceph中创建存储池，可通过填写**镜像缓存池名**、**数据云盘池名**和**根云盘池名**的输入框，指定数据存放在对应的数据池。

查找云盘

基于Ceph存储池的云盘创建后，其位置在信息栏的**安装路径**。管理员需要通过*rbd*命令在Ceph存储池查找。例如，云盘路径为：*ceph://pri-v-d-5c37402e7f5c4cdd9a15d9212847bb59/db9d0dd57a7b46258a34a6f20ab86aff*

在Ceph MON节点查找的方式如图 *36: 在Ceph存储池查找云盘*所示：

图 36: 在Ceph存储池查找云盘

```
[root@hbm1 ~]# rbd info pri-v-d-5c37402e7f5c4cdd9a15d9212847bb59/db9d0dd57a7b46258a34a6f20ab86aff
rbd image 'db9d0dd57a7b46258a34a6f20ab86aff':
        size 500 GB in 128001 objects
        order 22 (4096 kB objects)
        block_name_prefix: rbd_data.6c865238e1f29
        format: 2
        features: layering
        flags:
[root@hbm1 ~]#
```

迁移特性

在Ceph分布式存储RBD块存储场景，支持云主机在线迁移。

高可用特性

在Ceph分布式存储RBD块存储场景，支持高可用特性。

3.6 镜像服务器

镜像服务器，在ZStack技术体系中负责模板和ISO镜像的管理。

添加备份存储应遵守以下规则：

- 若添加的主存储为Ceph，则对应的镜像服务器也是Ceph；
- 其他主存储对应的镜像服务器可选镜像仓库或Sftp存储。

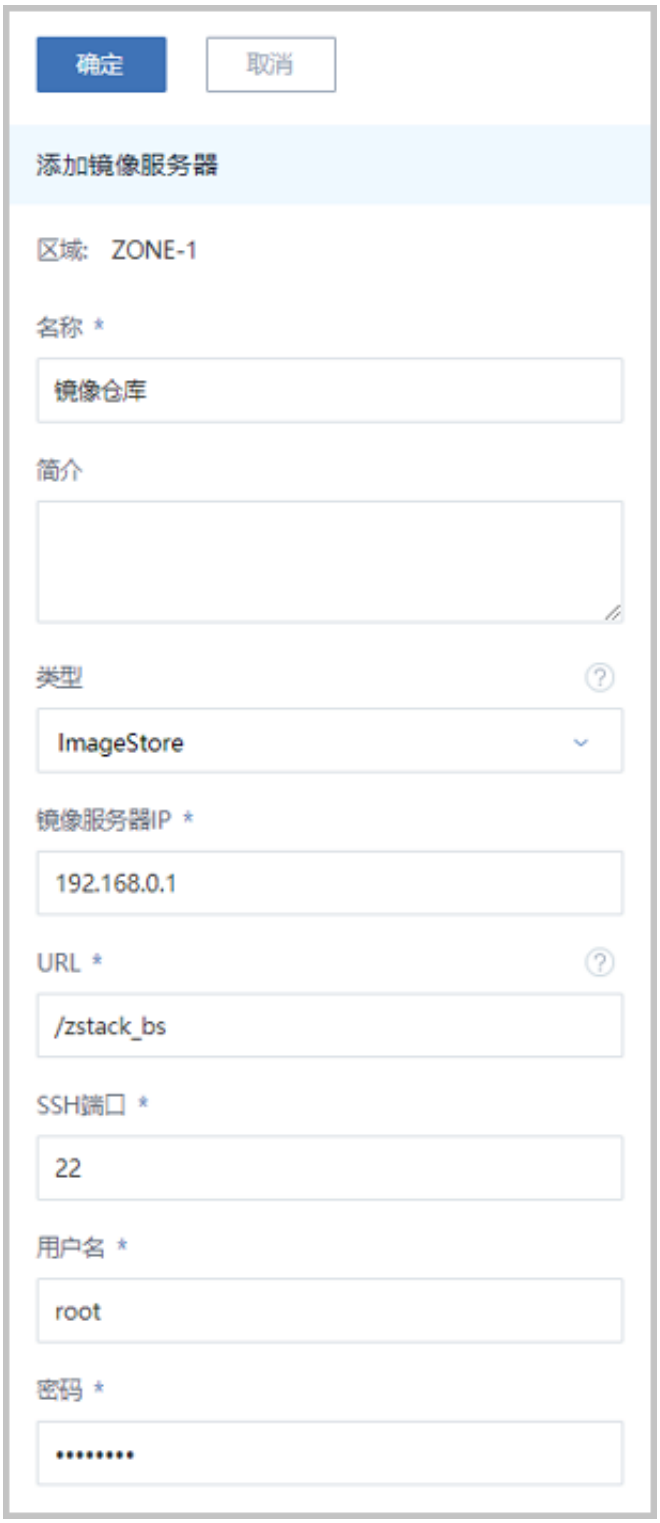
建议新部署的用户使用镜像仓库，使用其高级功能。

3.6.1 镜像仓库

镜像仓库（ImageStor）是ZStack率先在基础设施服务领域提供的模板和ISO管理集合。模板和ISO内容会以分块方式存放到镜像仓库，并提供类似GIT的版本控制管理策略，以实现对内增量修改与比对操作。ZStack将镜像仓库作为默认的镜像服务器类型。

添加镜像仓库时，填写主机IP和认证等信息，ZStack管理服务将主动访问登录到镜像服务器并在指定的路径上存放数据内容。数据内容将以分块的方式进行存放。如图 *37:* 添加镜像服务器-镜像仓库所示：

图 37: 添加镜像服务器-镜像仓库



注:

- 当管理员首次发起基于模板或镜像创建云主机时，如果在主存储缓存目录（Imagecache）没有发现与之对应的模板或镜像，则将会传输模板或镜像到主存储。
- 模板和镜像传输完毕，云主机状态继续流转。再次发起基于该模板或镜像创建云主机时，ZStack在主存储找到对应的模板或镜像，则无需从镜像服务器拉取内容。

ZStack在镜像仓库的路径里，创建两个文件目录：

- **export**：模板和ISO导出的目录，提供管理员和用户下载镜像。
- **registry**：模板和ISO的实际存放位置。

生产环境，镜像仓库路径建议使用单独的磁盘分区。

当操作系统损毁后，可在根分区重新安装操作系统，通过ZStack界面对镜像服务器执行重连，即可恢复服务。管理员可使用rsync或其他方式对路径内的数据执行增量备份，放置到远端数据中心。

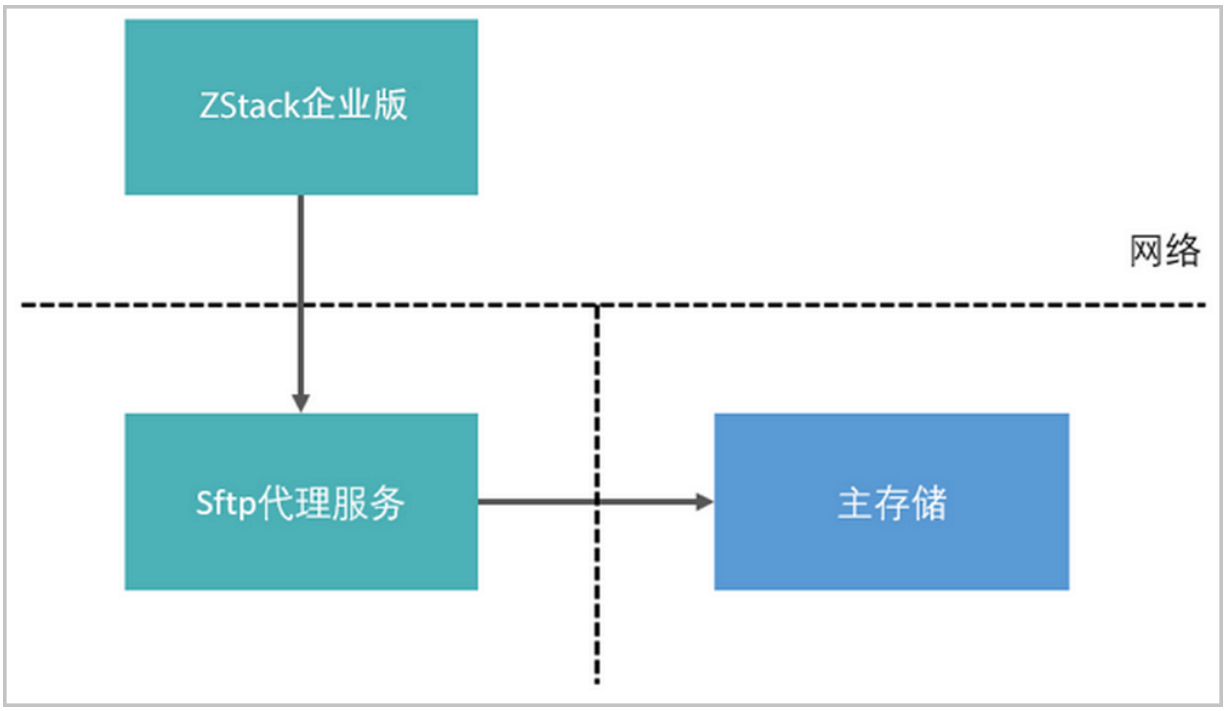
3.6.2 Sftp存储

Sftp（Secure **File Transfer Protocol**）是安全文件传输协议，提供加密传输的文件拷贝，是Linux常用的文件传输方式。

管理员添加Sftp镜像服务器后，ZStack将安装代理服务（zstack-sftpbackupstorage）。ZStack管理服务器与之通信，接收来自管理服务的API请求，执行下载和传输等操作。如图 *38:* 备份存储代理服务工作逻辑所示：

注: 目前仅企业版支持Sftp镜像服务器，社区版不支持。

图 38: 备份存储代理服务工作逻辑



首次发起基于模板或镜像创建云主机时，如果在主存储缓存目录（Imagecache）没有发现与之对应的模板或镜像，则将会传输模板或镜像到主存储。

模板和镜像传输完毕，云主机状态继续流转。管理员再次发起基于该模板或镜像创建云主机时，ZStack在主存储找到对应的模板或镜像，则无需从备份存储拉取内容，工作原理与镜像仓库一致。

ZStack在Sftp备份存储的路径里，创建两个文件目录：

- **rootVolumeTemplates**：添加镜像时选择**Image**类型，模板存放到此目录。
- **dataVolumeTemplates**：添加镜像时选择**ISO**类型，ISO文件存放在此目录。

管理员可通过查看镜像的信息，查找镜像所在的位置。

生产环境下，Sftp存储路径建议使用单独的磁盘分区。当操作系统损毁后，可在根分区重新安装操作系统，通过ZStack界面对备份存储执行重连，即可恢复服务。管理员可使用rsync或其他方式对备份存储数据执行增量备份，放置到远端数据中心。

4 基础网络服务

4.1 扁平网络

4.1.1 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：

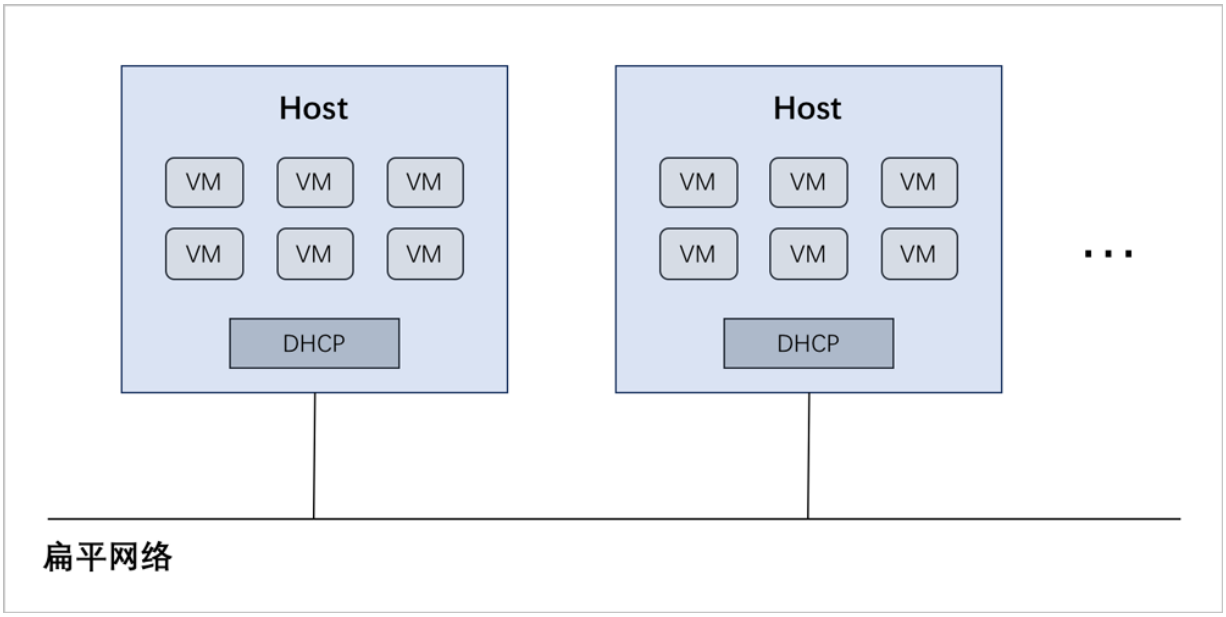
- User Data：使用cloud-init进行云主机开机加载并执行特定的用户数据，例如ssh-key注入。
- 弹性IP：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
- DHCP：分布式DHCP实现动态获取IP地址。

  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 *39:* 扁平网络架构图所示：

图 39: 扁平网络架构图



4.1.2 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*
DHCP IP	*172.20.180.41*

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 *40:* 创建*L2*-扁平网络所示，点击**确定**，创建L2-扁平网络。

   图 40: 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
   - **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；

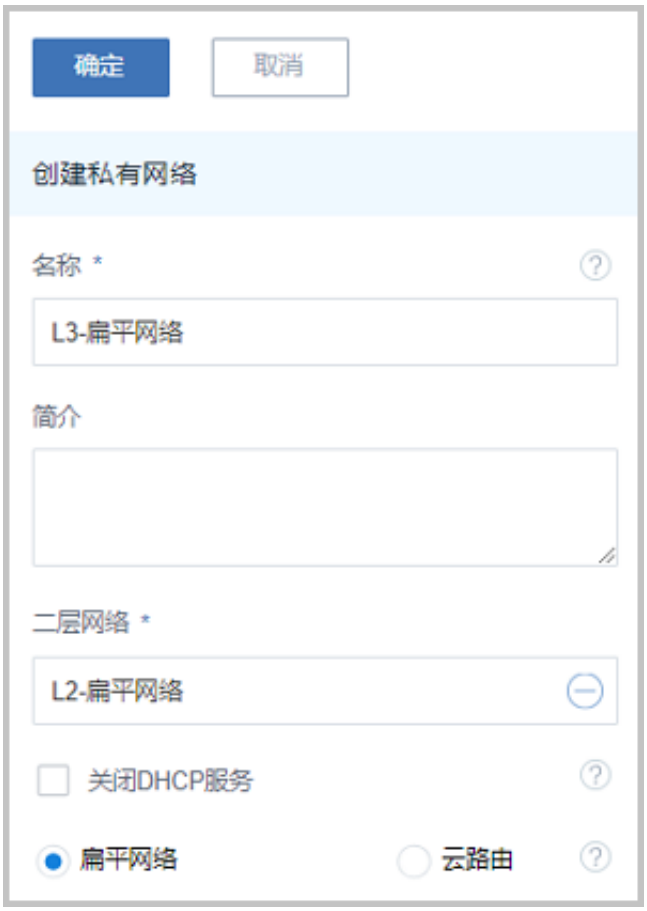
    - 勾选后，表示关闭DHCP服务，使用此网络的云主机将无法自动获取IP，需手动配置，此时DHCP IP不支持自定义设置，也不可由系统随机指定。
- 网络类型选择**扁平网络**
- **添加网络段**：选择IPv4类型网络地址、IP范围方式

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

图 41: 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

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**：选择IPv4或IPv6网络地址类型的扁平网络

本教程以IPv4类型网络地址为例，如图 *42: 创建云主机VM-1*所示，点击 **确定**，创建私有云云主机。

图 42: 创建云主机VM-1

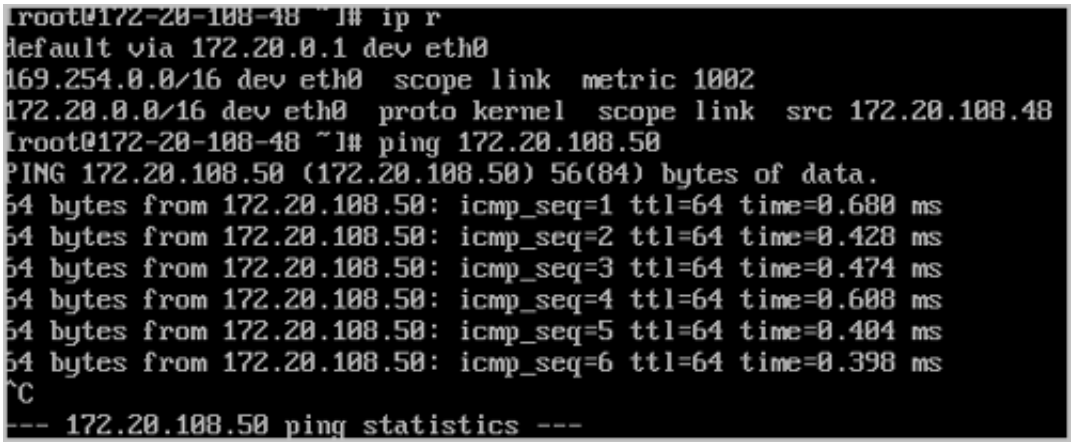

确定
取消
创建云主机
添加方式
单个
多个
名称 *
VM-1
简介
计算规格 *
InstanceOffering-1
镜像 *
Image-1
网络
网络地址类型 *
IPv4
IPv6
双栈
三层网络 *
L3-扁平网络
默认网络
设置网卡
高级

4. 验证扁平网络连通性。

- 内网连通性验证：

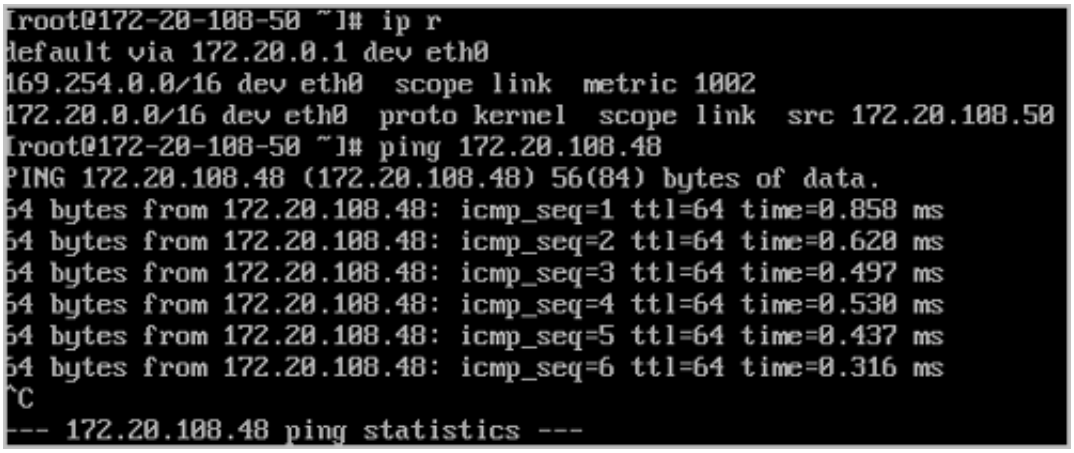
  1. 使用该扁平网络创建另一台私有云云主机，例如VM-2。
  2. 登录VM-1，检查是否能够ping通VM-2，如图 *43: VM-1 ping通 VM-2*所示：

     图 43: VM-1 ping通 VM-2



  3. 登录VM-2，检查是否能够ping通VM-1，如图 *44: VM-2 ping通 VM-1*所示：

     图 44: VM-2 ping通 VM-1



  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通公网。

至此，扁平网络的基本部署实践介绍完毕。

4.2 云路由网络

4.2.1 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：

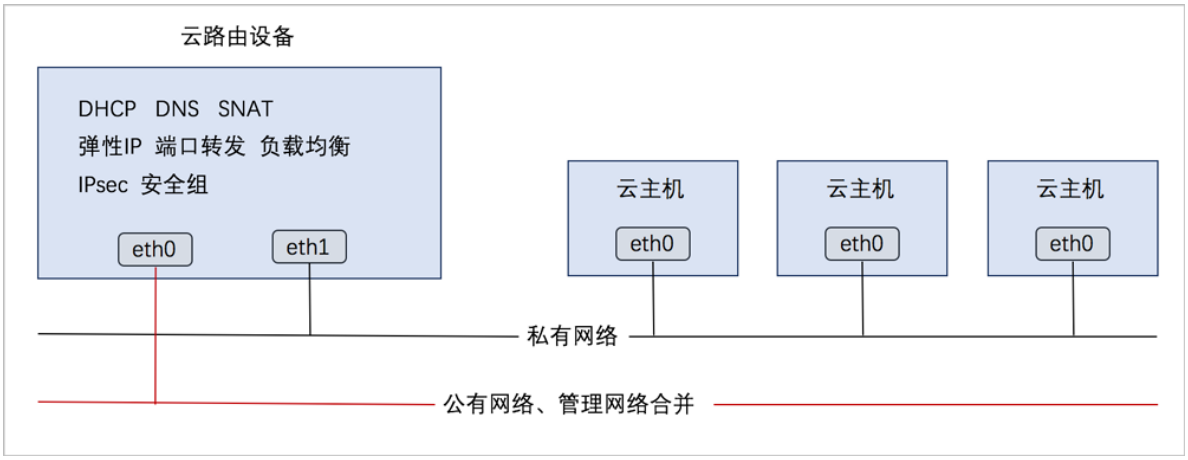
  也称之为业务网络或接入网络，是云主机使用的内部网络。

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 *45: 部署方式-1*所示：

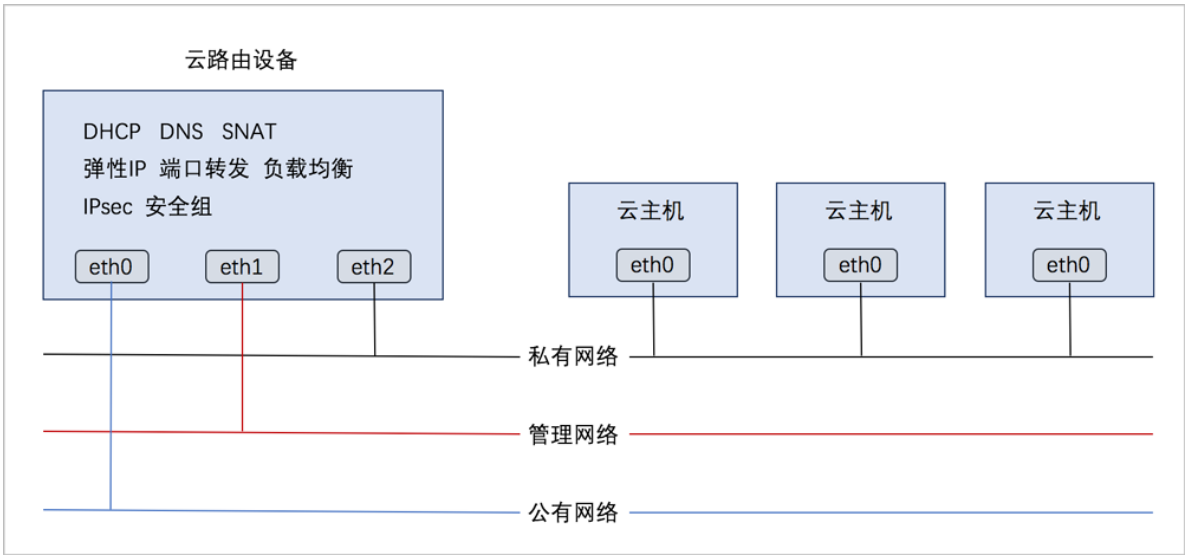
  图 45: 部署方式-1



- 公有网络、管理网络、私有网络均独立部署

如图 *46: 部署方式-2*所示：

图 46: 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。

4.2.2 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 2: 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 3: 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。

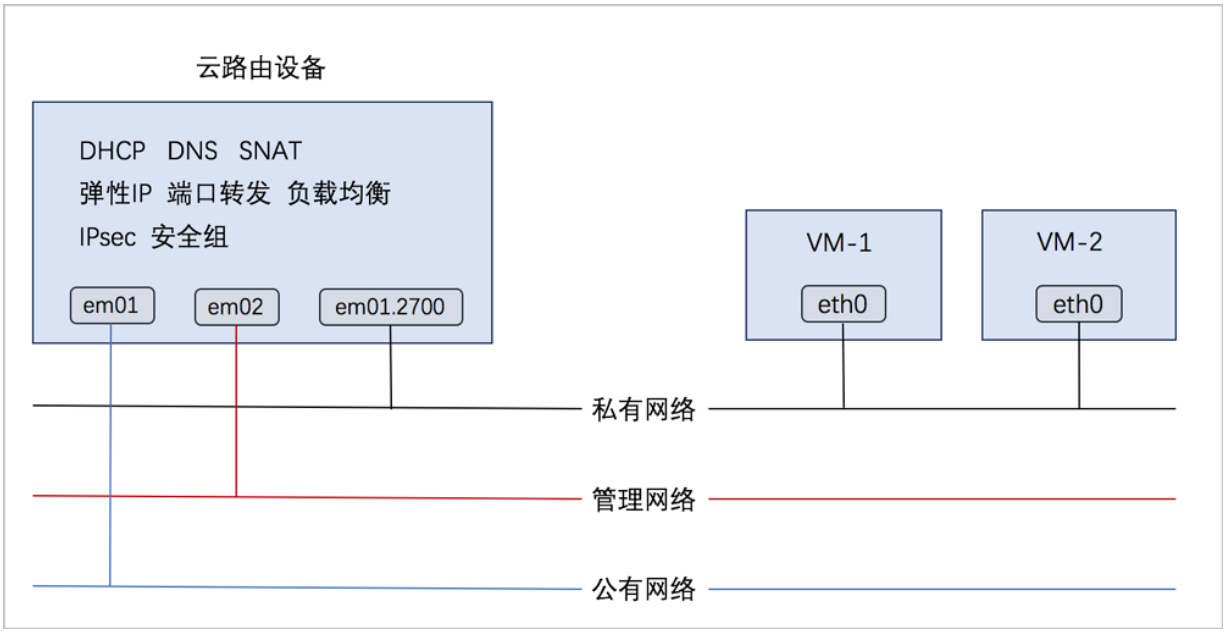
3. 私有网络

表 4: 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 *47:* 云路由网络架构图所示：

图 47: 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 *2:* 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 *48:* 创建*L2*-公有网络所示，点击**确定**，创建L2-公有网络。

   图 48: 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 *2: 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 *49: 创建L3-公有网络*所示，点击**确定**，创建L3-公有网络。

图 49: 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 *3:* 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 *50: 创建L2-管理网络*所示，点击**确定**，创建L2-管理网络。

图 50: 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 3: 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 *51:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 51: 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 *52:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 52: 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 *53:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 53: 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 4: 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 *54: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 54: 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 *4:* 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 *55:* 创建*L3*-私有网络所示，点击**确定**，创建L3-私有网络。

图 55: 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）：

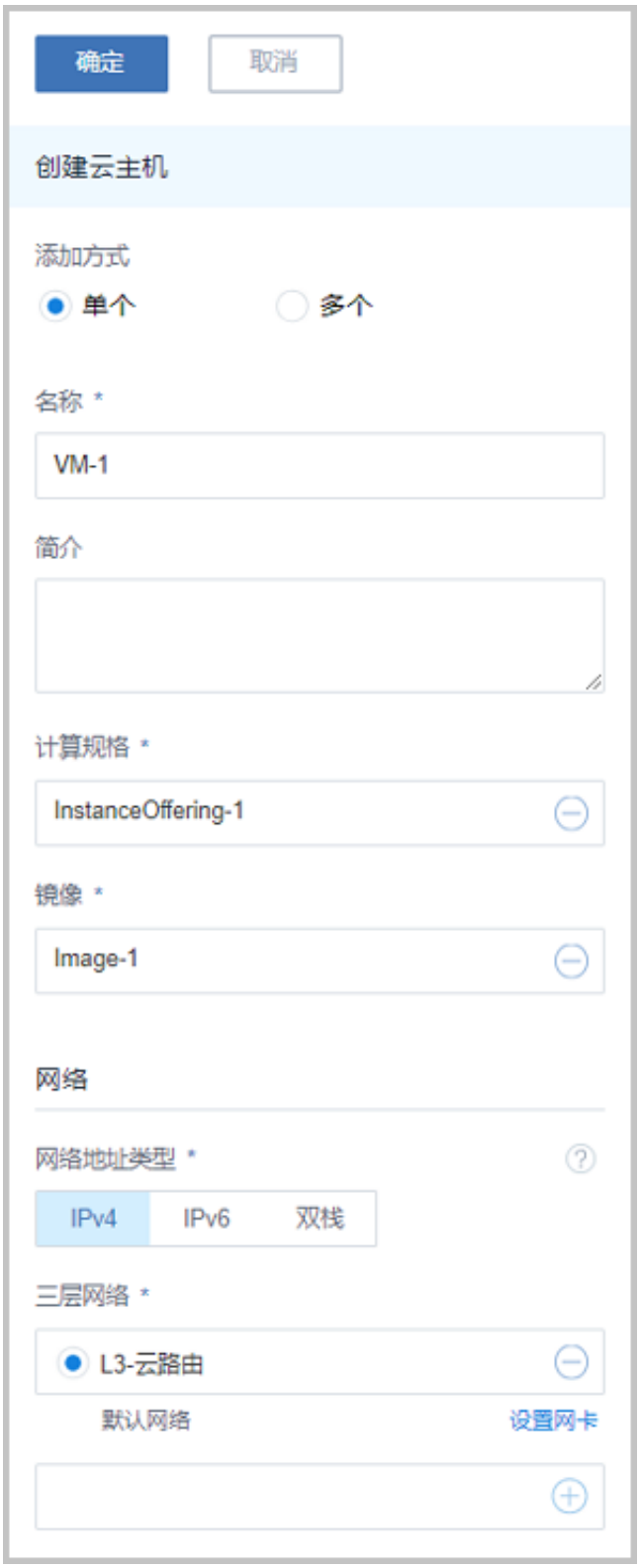
- **添加方式**：单个

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

图 56: 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：

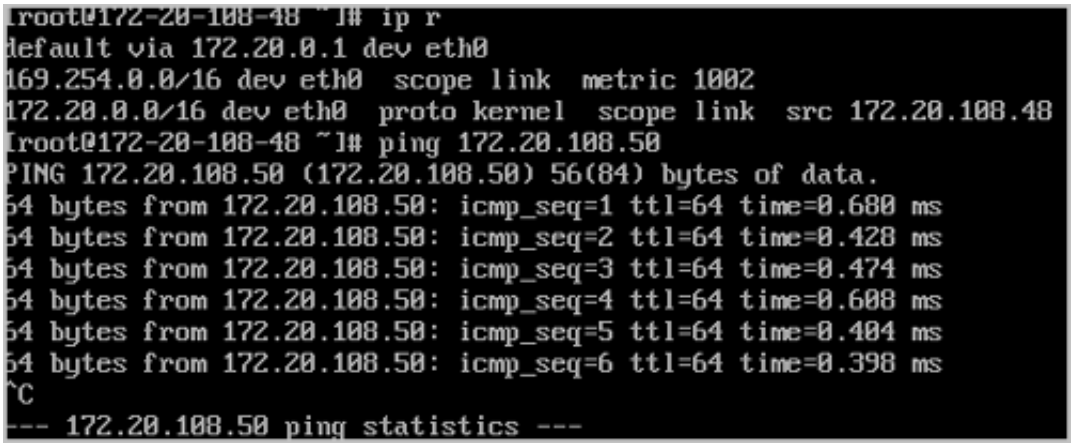
  登录VM-1，检查是否能够ping通公网，如图 *57: VM-1 ping通公网*所示：

  图 57: VM-1 ping通公网

- 内网连通性验证：

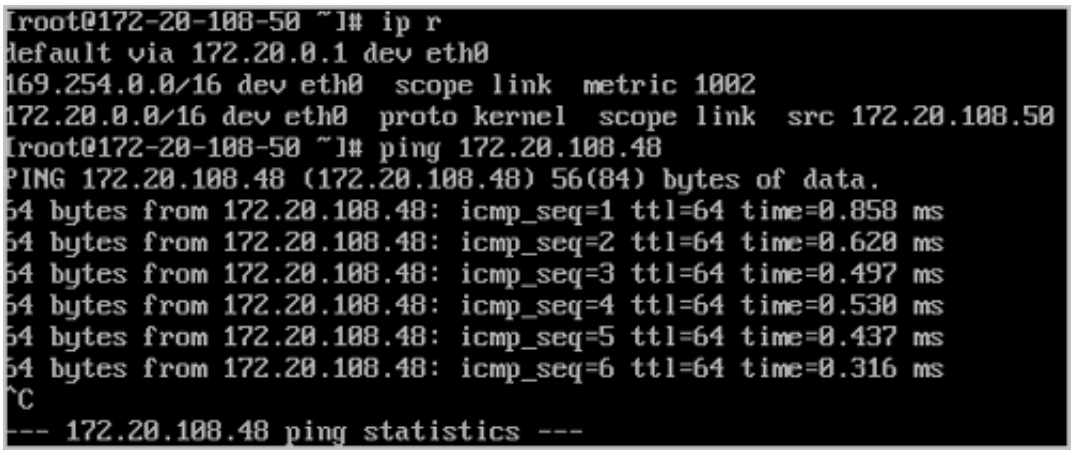
  1. 使用该云路由网络创建另一台私有云云主机，例如VM-2。
  2. 登录VM-1，检查是否能够ping通VM-2，如图 *58: VM-1 ping通 VM-2*所示：

     图 58: VM-1 ping通 VM-2



  3. 登录VM-2，检查是否能够ping通VM-1，如图 *59: VM-2 ping通 VM-1*所示：

     图 59: VM-2 ping通 VM-1



至此，云路由网络的基本部署实践介绍完毕。

4.3 VPC

4.3.1 介绍

专有网络VPC（Virtual Private Cloud，以下简称VPC），是基于VPC路由器和VPC网络共同组成的自定义私有云网络环境，帮助企业用户构建一个逻辑隔离的私有云。

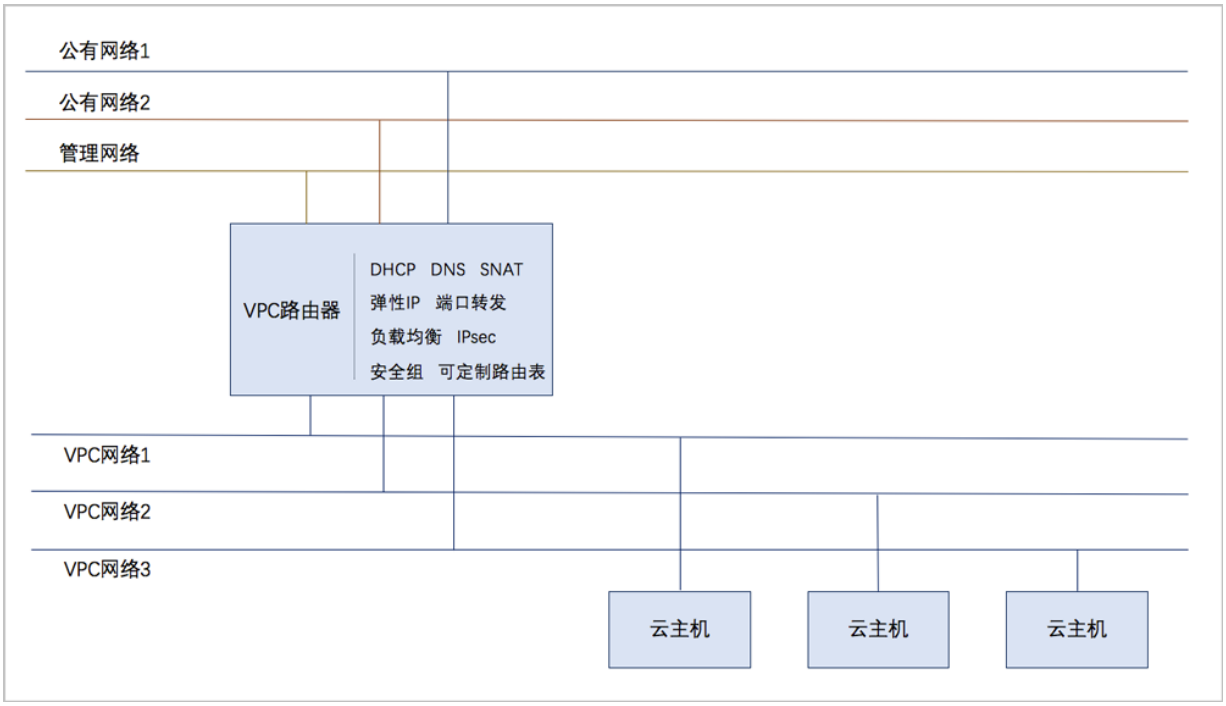
VPC路由器和VPC网络

VPC由VPC路由器和VPC网络组成。

1. VPC路由器：基于云路由规格直接创建的云路由器，拥有公有网络和管理网络。
   - VPC路由器是VPC的核心，可主动创建基于指定云路由规格的VPC路由器；
   - 须提前创建云路由规格所需的公有网络和管理网络、云路由镜像资源；
   - VPC路由器可灵活挂载或卸载VPC网络或其他公有网络；
   - 云路由规格定义的公有网络和管理网络，不可卸载；
   - 同一个云路由规格可以创建多个VPC路由器，这些VPC路由器共享使用同一个云路由规格里定义的公有网络段和管理网络段；
   - 公有网络作为默认网络，用于提供网络服务。
2. VPC网络：作为VPC的私有网络，可挂载至VPC路由器。
   - 须提前创建二层网络，用于创建三层的VPC网络；
   - 可在创建VPC网络时指定待挂载的路由器，也可创建VPC网络后再挂载路由器；
   - 如有云主机使用VPC网络，不支持从VPC路由器卸载；
   - 新建的网络段不可与VPC路由器内任一网络的网络段重叠。

VPC网络拓扑如图 *60: VPC网络拓扑示意图*所示：

图 60: VPC网络拓扑示意图



VPC特点

VPC具有以下特点：

- 灵活的网络配置，不同的VPC网络可灵活挂载到VPC路由器，每个VPC网络可自定义独立的网络段和独立的网关，VPC路由器支持加载/卸载网卡，并支持动态配置路由表和路由条目。
- 安全可靠的隔离，不同VPC下的VPC网络互相逻辑隔离，支持VLAN和VXLAN进行二层逻辑隔离，不同账户的VPC互不影响。
- 多子网互通：同一VPC下的多个VPC网络互联互通。
- 网络流量优化：支持分布式路由功能，优化东西向网络流量，并有效降低网络延迟。

VPC网络服务

VPC网络作为VPC的私有网络，使用VPC路由器提供各种网络服务。

- DHCP：默认采用扁平网络服务模块提供分布式DHCP服务。
- DNS：VPC路由器作为DNS服务器提供DNS服务。在云主机中看到的DNS地址默认为VPC路由器的IP地址，用户设置的DNS地址由VPC路由器负责转发配置。
- SNAT：VPC路由器向云主机提供原网络地址转换，云主机使用SNAT可直接访问外部互联网。
- 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。

- 弹性IP：可绑定弹性IP到VPC网络，实现公有网络到云主机私有网络的互联互通。
- 端口转发：提供公网IP到云主机私有网络IP的端口到端口的相关网络协议的互通。
- 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）的互联互通。

4.3.2 基本部署

背景信息

专有网络VPC的基本部署流程如下：

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. 基于云路由规格创建VPC路由器。
8. 创建二层私有网络（用于创建三层的VPC网络1），并加载此二层网络到相应集群。
9. 指定VPC路由器，创建三层的VPC网络1，注意网络段不可重叠。
10. 创建二层私有网络（用于创建三层的VPC网络2），并加载此二层网络到相应集群。
11. 指定VPC路由器，创建三层的VPC网络2，注意网络段不可重叠。
12. 使用VPC网络1创建云主机1，使用VPC网络2创建云主机2。
13. 验证VPC网络1与VPC网络2的互通性。

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	*10.108.10.100~10.108.10.200*

公有网络	配置信息
子网掩码	*255.0.0.0*
网关	*10.0.0.1*
DHCP IP	*10.108.10.101*

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	*192.168.29.10~192.168.29.20*
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. VPC网络1

表 7: VPC网络1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*
DHCP IP	*192.168.10.2*

4. VPC网络2

表 8: VPC网络2配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2900
IP CIDR	*192.168.11.0/24*
DHCP IP	*192.168.11.2*

以下介绍部署专有网络VPC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 *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 *61:* 创建*L2*-公有网络所示，点击**确定**，创建L2-公有网络。

   图 61: 创建L2-公有网络

2. 在ZStack私有云界面创建L3-公有网络。

   在ZStack私有云主菜单，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**：*10.108.10.100*
- **结束IP**：*10.108.10.200*
- **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 *62: 创建L3-公有网络*所示，点击**确定**，创建L3-公有网络。

图 62: 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 *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 *63: 创建L2-管理网络*所示，点击**确定**，创建L2-管理网络。

图 63: 创建L2-管理网络

4. 在ZStack私有云界面创建L3-管理网络。

   在ZStack私有云主菜单，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**：*192.168.29.10*
- **结束IP**：*192.168.29.20*
- **子网掩码**：*255.255.255.0*
- **网关**：*192.168.29.1*

如图 *64:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 64: 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 *65:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 65: 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 *66:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 66: 创建云路由规格

7. 基于云路由规格创建VPC路由器。

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

   - **名称**：设置VPC云路由规格名称
   - **简介**：可选项，可留空不填
   - **云路由规格**：选择已创建的云路由规格

- **DNS**：可选项，用于设置VPC路由器的DNS解析服务，默认指定223.5.5.5

如图 *67: 创建VPC路由器*所示，点击**确定**，创建VPC路由器。

图 67: 创建VPC路由器

8. 在ZStack私有云界面创建L2-私有网络（用于创建三层的VPC网络1）。

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 *7: VPC网络1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**：2800
- **网卡**：em01
- **集群**：选择集群，如Cluster-1

如图 *68: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 68: 创建L2-私有网络

9. 指定VPC路由器，在ZStack私有云界面创建三层的VPC网络1。

   在ZStack私有云主菜单，点击**网络资源** > **VPC** > **VPC网络**，进入**VPC网络**界面，点击**创建VPC网络**，在弹出的**创建VPC网络**界面，参考上述表 *7: VPC网络1配置信息*填写如下：

   - **名称**：设置VPC网络1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。

- **VPC路由器**：可选项，VPC路由器可在创建VPC网络时指定，也可在创建VPC网络后再挂载
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.10.0/24*

注: 网络段不可重叠。

- **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。

如图 *69: 创建VPC网络1*所示，点击**确定**，创建VPC网络1。

图 69: 创建VPC网络1

10.在ZStack私有云界面创建L2-私有网络（用于创建三层的VPC网络2）。

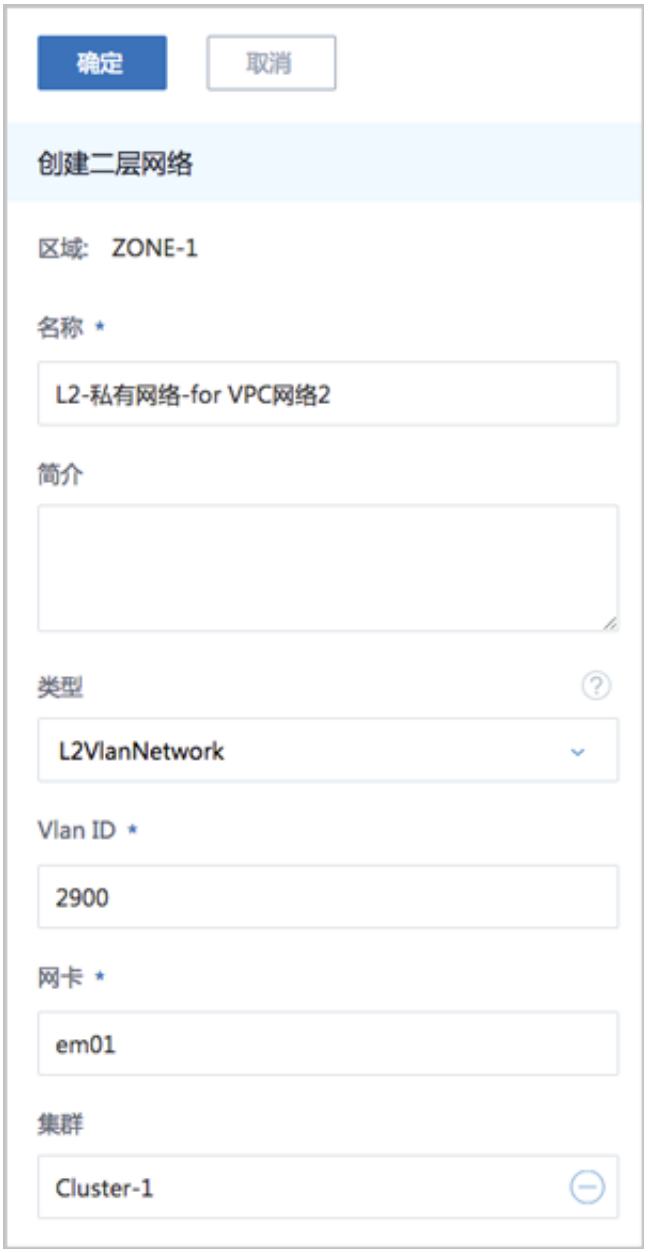
在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *8: VPC*网络*2*配置信息填写如下：

- **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**：2900
- **网卡**：em01
- **集群**：选择集群，如Cluster-1

如图 *70: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 70: 创建L2-私有网络



11.指定VPC路由器，在ZStack私有云界面创建三层的VPC网络2。

在ZStack私有云主菜单，点击**网络资源** > **VPC** > **VPC网络**，进入**VPC网络**界面，点击**创建VPC网络**，在弹出的**创建VPC网络**界面，参考上述表 *8: VPC网络2配置信息*填写如下：

- **名称**：设置VPC网络2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
- **VPC路由器**：可选项，VPC路由器可在创建VPC网络时指定，也可在创建VPC网络后再挂载
- **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CIDR
- **CIDR**：*192.168.11.0/24*

  注: 网络段不可重叠。
- **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。

如图 *71: 创建VPC网络2*所示，点击**确定**，创建VPC网络2。

图 71: 创建VPC网络2

12.使用VPC网络1创建私有云云主机1，使用VPC网络2创建私有云云主机2。

a) 使用VPC网络1创建私有云云主机1。

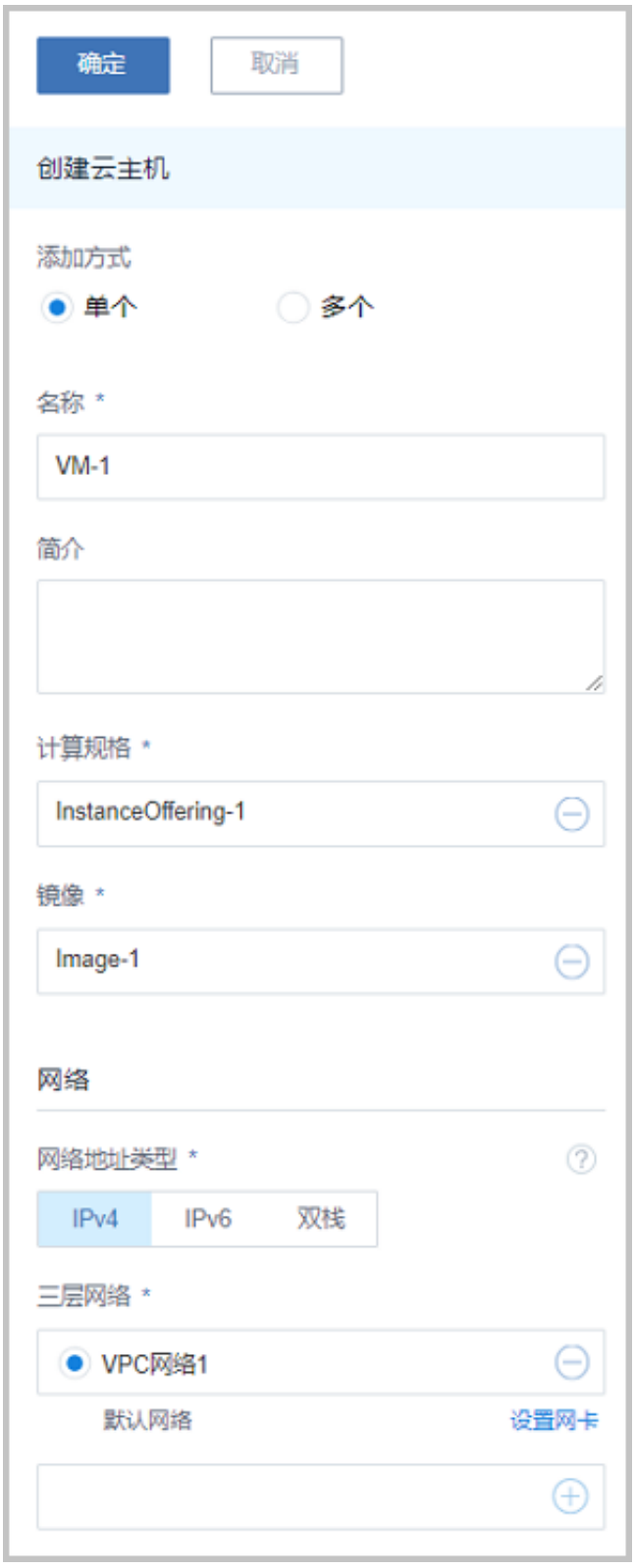
在ZStack私有云主菜单，点击 **云资源池** > **云主机**，进入**云主机**界面，点击**创建云主机**，在弹出的**创建云主机**界面，可参考以下示例输入相应内容：

- **添加方式**：单个

- **名称**：设置私有云云主机1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**：选择已添加的云主机镜像
- **网络**：选择IPv4网络地址类型中的VPC网络1

如图 *72: 创建私有云云主机1*所示，点击 **确定**，创建私有云云主机1。

图 72: 创建私有云云主机1

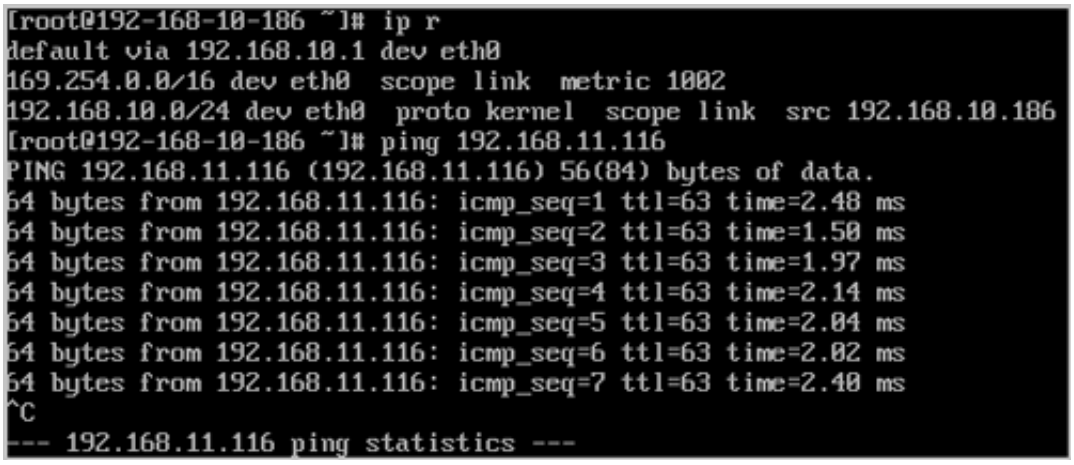


b) 同理，使用VPC网络2创建私有云云主机2。

13.验证VPC网络1与VPC网络2的互通性。

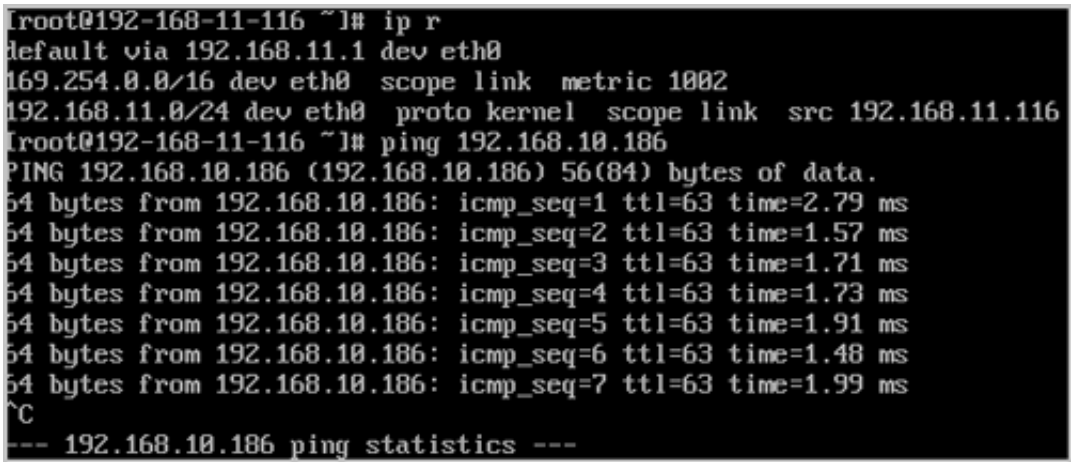
1. 登录VM-1，检查是否能够ping通VM-2，如图 *73: VM-1 ping通 VM-2*所示：

图 73: VM-1 ping通 VM-2



2. 登录VM-2，检查是否能够ping通VM-1，如图 *74: VM-2 ping通 VM-1*所示：

图 74: VM-2 ping通 VM-1



后续操作

至此，专有网络VPC的基本部署实践介绍完毕。

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。