用户手册

产品版本：ZStack 2.5.1

文档版本：V2.5.1

ZStack

版权声明

版权所有©上海云轴信息科技有限公司 2018。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标说明

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

版权声明 I
1 引言 1
2 概述 11
3 配置需求 26
3.1 网络环境 26
3.2 硬件要求 27
4 安装部署 28
4.1 环境准备 28
4.1.1 网卡归一化(可选) 41
4.2 安装ZStack 52
4.2.1 ZStack管理节点模式(企业版/社区版) 54
4.2.2 ZStack计算节点模式 90
4.2.3 ZStack专家模式 91
4.3 管理ZStack 92
4.4 升级ZStack 93
4.4.1 c72版 升级 93
4.4.2 c74版 升级 97
5 系统登录 102
6 Wizard引导设置 103
6.1 创建区域 103
6.2 创建集群 103
6.3 添加物理机 104
6.4 添加镜像服务器 106
6.4.1 ImageStore（镜像仓库） 106
6.4.2 Ceph镜像服务器 108
6.4.3 FusionStor镜像服务器 109
6.5 添加主存储 110
6.5.1 LocalStorage（本地存储） 110
6.5.2 NFS 111
6.5.3 Shared Mount Point 113
6.5.4 Ceph 114
6.5.5 FusionStor 116
6.5.6 Shared Block 117
6.6 创建计算规格 118
6.7 添加镜像 120
6.8 创建二层网络 122
6.9 创建三层网络 124
7 云平台操作指南 126
7.1 首页 126
7.1.1 产品与服务快速入口 128
7.1.2 大屏监控 129
7.1.3 关于 134
7.2 云资源池 139
7.2.1 云主机 139

7.2.1.1 云主机管理..... 139
7.2.1.2 创建云主机..... 140
7.2.1.2.1 创建单个云主机..... 140
7.2.1.2.2 批量创建云主机..... 149
7.2.1.3 云主机操作..... 151
7.2.1.3.1 单个云主机操作..... 151
7.2.1.3.2 批量云主机操作..... 172
7.2.1.3.3 SSH公钥管理..... 173
7.2.1.3.4 系统扩容教程..... 174
7.2.1.4 云主机详情..... 184
7.2.1.4.1 云主机定时任务..... 184
7.2.1.4.2 云主机监控数据..... 186
7.2.1.4.3 云主机报警..... 189
7.2.2 云盘..... 192
7.2.2.1 云盘操作..... 193
7.2.2.2 创建云盘..... 195
7.2.2.3 云盘详情..... 199
7.2.2.3.1 云盘定时任务..... 200
7.2.3 镜像..... 201
7.2.3.1 镜像操作..... 203
7.2.3.2 添加镜像..... 205
7.2.3.3 镜像详情..... 211
7.2.4 亲和组..... 211
7.2.4.1 介绍..... 211
7.2.4.2 前提..... 213
7.2.4.3 使用入口..... 213
7.2.4.3.1 亲和组..... 213
7.2.4.3.2 云主机..... 216
7.2.4.4 场景实践..... 220
7.2.4.4.1 云主机 | 物理机 反亲和组(非强制)..... 220
7.2.4.4.2 云主机 | 物理机 反亲和组(强制)..... 223
7.2.5 计算规格..... 226
7.2.5.1 计算规格操作..... 226
7.2.5.2 创建计算规格..... 227
7.2.5.3 计算规格详情..... 230
7.2.6 云盘规格..... 230
7.2.6.1 云盘规格操作..... 231
7.2.6.2 创建云盘规格..... 231
7.2.6.3 云盘规格详情..... 232
7.3 硬件设施..... 233
7.3.1 区域..... 233
7.3.1.1 区域操作..... 235
7.3.1.2 区域详情..... 236
7.3.2 集群..... 239
7.3.2.1 集群操作..... 243
7.3.2.2 集群详情..... 246
7.3.3 计算服务器..... 250
7.3.3.1 物理机..... 250
7.3.3.1.1 物理机操作..... 251
7.3.3.1.2 物理机详情..... 256

7.3.3.1.3 物理机监控数据 261
7.3.3.1.4 GPU及USB设备透传 使用教程 264
7.3.3.1.4.1 GPU透传 264
7.3.3.1.4.2 USB透传 282
7.3.3.2 裸机部署教程 293
7.3.3.2.1 介绍 293
7.3.3.2.2 准备工作 294
7.3.3.2.2.1 手动安装管理节点 294
7.3.3.2.2.2 进入物理机BIOS启用PXE 294
7.3.3.2.2.3 规划裸机安装网络 295
7.3.3.2.2.4 配置物理机IPMI 295
7.3.3.2.3 自动化批量部署 296
7.3.3.2.3.1 安装服务 296
7.3.3.2.3.2 裸机管理 299
7.3.4 主存储 311
7.3.4.1 主存储操作 313
7.3.4.2 主存储类型--本地存储 314
7.3.4.3 主存储类型--NFS 316
7.3.4.4 主存储类型--Shared Mount Point 318
7.3.4.5 主存储类型--Ceph 321
7.3.4.6 主存储类型--Shared Block 324
7.3.4.7 主存储类型--FusionStor 327
7.3.4.8 主存储详情 329
7.3.4.9 主存储详情--本地存储 329
7.3.4.10 主存储详情--NFS 333
7.3.4.11 主存储详情--Shared Mount Point 335
7.3.4.12 主存储详情--Ceph 337
7.3.4.13 主存储详情--Shared Block 339
7.3.4.14 主存储详情--FusionStor 341
7.3.5 镜像服务器 342
7.3.5.1 镜像服务器操作 345
7.3.5.2 镜像服务器详情 349
7.4 网络资源 353
7.4.1 网络拓扑 355
7.4.1.1 全局拓扑 356
7.4.1.2 自定义拓扑 357
7.4.2 二层网络资源 359
7.4.2.1 VXLAN Pool 359
7.4.2.2 二层网络 361
7.4.2.2.1 L2NoVlanNetwork 363
7.4.2.2.2 L2VlanNetwork 364
7.4.2.2.3 VxlanNetwork 366
7.4.2.3 二层网络操作 368
7.4.3 三层网络 368
7.4.3.1 公有网络 370
7.4.3.2 系统网络 373
7.4.3.3 私有网络 376
7.4.3.4 三层网络操作 379
7.4.4 路由资源 380
7.4.4.1 云路由器 382
7.4.4.2 云路由镜像 385

7.4.4.3 云路由规格 388
7.4.4.4 路由表 390
7.4.5 VPC 392
7.4.5.1 VPC路由器 394
7.4.5.2 VPC网络 403
7.5 网络服务 405
7.5.1 安全组 408
7.5.2 虚拟IP 413
7.5.3 弹性IP 419
7.5.4 端口转发 423
7.5.5 负载均衡 431
7.5.6 IPsec隧道 439
7.6 网络教程 446
7.6.1 扁平网络使用教程 446
7.6.1.1 介绍 446
7.6.1.2 前提 447
7.6.1.3 基本部署 447
7.6.1.4 应用场景 454
7.6.1.4.1 二层连通网络 455
7.6.1.4.2 安全组 455
7.6.1.4.3 弹性IP 464
7.6.2 云路由网络使用教程 469
7.6.2.1 介绍 469
7.6.2.2 前提 472
7.6.2.3 基本部署 472
7.6.2.4 应用场景 490
7.6.2.4.1 多租户隔离 490
7.6.2.4.2 多层Web服务器 515
7.6.2.4.3 多公网 523
7.6.2.4.4 安全组 534
7.6.2.4.5 弹性IP 543
7.6.2.4.6 端口转发 549
7.6.2.4.7 负载均衡 561
7.6.2.4.8 IPsec隧道 571
7.6.3 专有网络VPC使用教程 581
7.6.3.1 介绍 581
7.6.3.2 前提 583
7.6.3.3 基本部署 583
7.6.3.4 应用场景 603
7.6.3.4.1 多租户隔离 604
7.6.3.4.2 多层Web服务器 629
7.6.3.4.3 安全组 635
7.6.3.4.4 弹性IP 643
7.6.3.4.5 端口转发 649
7.6.3.4.6 负载均衡 660
7.6.3.4.7 IPsec隧道 670
7.7 vCenter 681
7.7.1 介绍 681
7.7.2 环境准备 682
7.7.3 基础资源 686
7.7.4 云主机 690

7.7.5 网络 696
7.7.5.1 云路由网络 696
7.7.5.2 扁平网络 703
7.7.5.3 网络服务 705
7.7.5.3.1 虚拟IP(ESX类型) 705
7.7.5.3.2 弹性IP 708
7.7.5.3.3 端口转发 710
7.7.5.3.4 负载均衡 713
7.7.5.3.5 IPsec隧道 716
7.7.6 云盘 720
7.7.7 镜像 724
7.7.8 事件消息 727
7.8 企业管理(Plus) 728
7.8.1 平台管理员 733
7.8.2 组织架构 735
7.8.2.1 用户 736
7.8.2.2 组织 739
7.8.3 项目管理 742
7.8.3.1 项目 744
7.8.3.2 项目模板 750
7.8.4 工单管理 752
7.8.4.1 我的审批 752
7.9 平台运维 755
7.9.1 性能TOP5 755
7.9.2 性能分析 758
7.9.3 ZWatch 760
7.9.3.1 报警器 761
7.9.3.1.1 资源报警器 761
7.9.3.1.2 事件报警器 764
7.9.3.2 报警消息模板 765
7.9.4 通知服务 768
7.9.4.1 接收端 768
7.9.5 消息中心 773
7.9.6 操作日志 773
7.9.7 资源编排 776
7.9.7.1 概述 776
7.9.7.2 准备工作 777
7.9.7.3 典型使用流程 778
7.9.7.4 资源栈 778
7.9.7.5 资源栈模板 784
7.9.7.6 资源栈示例模板 790
7.9.7.7 快速实践 792
7.9.7.8 附录 802
7.9.7.8.1 资源栈模板语法 802
7.9.7.8.1.1 参数(Parameters) 804
7.9.7.8.1.2 资源(Resources) 806
7.9.7.8.1.3 输出(Outputs) 810
7.9.7.8.1.4 函数(Functions) 812
7.9.7.8.1.5 映射(Mappings) 817
7.9.7.8.2 资源索引 819
7.9.7.8.2.1 Resource类型 819

7.9.7.8.2.2 Action类型 820
7.10 平台管理 821
7.10.1 用户管理 821
7.10.1.1 账户 824
7.10.1.2 用户组 829
7.10.1.3 用户 832
7.10.2 计费管理 835
7.10.2.1 账单 835
7.10.2.2 计费设置 836
7.10.3 定时 839
7.10.3.1 定时器 839
7.10.3.2 定时任务 842
7.10.4 应用中心 844
7.10.5 邮箱服务器 847
7.10.6 AD/LDAP 850
7.10.6.1 介绍 850
7.10.6.2 前提 851
7.10.6.3 添加AD/LDAP 851
7.10.6.4 绑定AD/LDAP成员 856
7.10.6.5 AD/LDAP登录 859
7.10.7 控制台代理 861
7.10.8 证书 861
7.11 设置 863
7.11.1 全局设置 864
7.11.2 自定义UI 868
术语表 872

1 引言

产品版本

目前与本文档相对应的产品版本为：ZStack企业版 2.5.1

读者对象

本文档详述了ZStack企业版 2.5.1的安装部署和使用方法。本文档主要适用于以下读者：

- 技术支持工程师
- 部署运维工程师
- 产品咨询工程师
- 有兴趣研究ZStack的相关人员

版本更新

2.5.1

2018/07/10主要更新：

1. Shared Block主存储功能增强
   - 一个集群支持挂载多个Shared Block主存储
   - 跨Shared Block主存储的整机迁移
2. 资源编排支持普通账户/企业管理账号体系使用
3. 修复已知问题，提升系统稳定性

2.5.0

2018/07/05主要更新：

1. 资源编排
2. 整机克隆
3. vCenter接管功能增强
   - vCenter监控报警
   - 多vCenter区分
   - 独立CPU授权
4. 操作日志/审计信息优化展示
5. 性能Top5页面展示优化

6. 其它相关功能和优化

- 新增多个操作场景进度条
- 操作助手和帮助文档
- 优化界面交互
- 优化部分业务逻辑

2.4.0

2018/06/11主要更新：

1. 企业管理模块：项目管理、工单审批、独立区域管理
2. 支持ARM服务器
3. 应用中心
4. 资源监控增强

- 详情页资源监控
- 资源实时监控

5. 新增主存储类型：Shared Block共享块存储
6. GPU功能增强
7. 模块许可证
8. 云主机导出增强
9. 计算规格的物理机分配策略新增非强制/强制模式
10. VPC路由器配置DNS
11. 其它相关功能和优化

- 新增多个操作场景进度条
- 操作助手和帮助文档
- 优化界面交互
- 优化部分业务逻辑

2.3.2

2018/05/11主要更新：

1. 云资源池：

- 云主机根云盘/数据云盘容量在线扩展

- 通过FTP和SFTP方式在线添加镜像模板

2. 硬件设施：
   - 分布式存储Ceph以存储池（Pool）粒度显示容量使用情况
   - 识别物理机CPU架构，识别主流Intel和AMD处理器
   - 集群按照物理机CPU架构定义属性，为云主机提供丰富的CPU多媒体指令集，以及提升热迁移兼容性
   - 指定集群云主机热/冷迁移网络
3. 网络服务：
   - 负载均衡监听协议支持HTTPS，需绑定证书使用
   - 强化监听器功能
4. VMware vCenter接管：
   - vCenter云主机迁移、克隆
   - vCenter物理机维护模式
5. 平台运维：TOP5性能分析，支持对应项搜索排序
6. 平台管理：
   - 强化定时任务功能
   - 在管理界面上修改控制台代理地址
7. 大屏监控：解决登录会话超时失效
8. 混合云：对接大河云联SD-WAN服务，提供混合云高速链路
9. 超融合解决方案：
   - 管理节点云主机管理员密码重置
   - 管理节点云主机跨网段创建/启动，跨网络异地部署
   - 管理节点云主机部署/迁移至非超融合节点，适应更广泛场景
10. 其它相关功能和优化：
    - 新增多个操作场景进度条
    - 操作助手和帮助文档
    - 优化界面交互
    - 优化部分业务逻辑

2.3.1

2018/04/03主要更新：

1. 网络拓扑
2. 新版菜单导航、新版首页
3. ZWatch：全新监控报警系统
4. ZStack定制版ISO新增：基于CentOS 7.4深度定制版本
5. 亲和组
6. 增强vCenter接管功能：接管vCenter云盘、基于vCenter云路由网络提供网络服务
7. 一个云主机加载多个ISO
8. 多种策略创建云主机
9. 一个二层网络可用于创建多个三层网络
10. 操作日志/审计全新改版
11. HTTPS安全访问UI管理界面
12. 内部访问业务流量的负载均衡
13. 优化自定义UI
14. 多个场景新增进度条、操作助手和帮助文档，优化UI交互
15. 优化部分业务逻辑

2.3.0

2018/02/08主要更新：

1. 专有网络VPC
2. 混合云灾备（混合云版支持）
3. 大屏监控
4. 用户自定义UI
5. ImageStore类型镜像服务器支持Ceph类型主存储
6. 支持vSwitch
7. 支持vCenter资源同步
8. ESXi云主机支持扁平网络
9. 云主机更换操作系统
10. 跨NFS存储数据迁移
11. 虚拟IP支持QoS
12. 支持AD认证

13.云主机自定义MAC地址

14.强化浏览器上传镜像功能

15.新增云盘镜像资源

16.数据云盘扩容

17.数据云盘规格支持QoS

18.停止NeverStop状态的云主机

19.开放云路由公网IP，并支持同一虚拟IP多网络服务复用

20.支持USB设备透传，强化外接设备透传功能

21.增加VDI SPICE流量优化选项

22.支持修改已设置的存储网络

23.支持设置VXLAN对普通账户的配额

24.支持ImageStore类型镜像服务器间的数据同步

25.管理节点数据库自动备份到远程服务器

26.多个场景新增进度条、操作助手和帮助文档，优化UI交互

27.优化部分业务逻辑

2.2

2017/10/16主要更新：

1. 公有网络创建云主机

2. 自定义DHCP模式

3. 新增系统网络

4. 云主机根云盘扩容

5. 浏览器添加镜像（目前支持ImageStore类型镜像服务器）

6. 管理节点高可用：多网络配置

7. 跨Ceph存储数据迁移

8. 增强Ceph存储功能

9. 增强VDI功能

10.LDAP自定义过滤规则

11.增强裸机管理

12.单集群支持多类型主存储（目前支持本地存储+NFS/SMP类型）

13.更换License支持本地上传

14.共享存储指定存储网络，增强云主机高可用

15.多个场景新增进度条、操作助手和帮助文档，优化UI交互

16.优化部分业务逻辑

2.1

2017/08/14主要更新：

1. VDI

2. 裸机管理

3. GPU透传

4. 智能报警

5. 集群挂载多个主存储

6. 新版定时器

7. 静态路由

8. User Data导入

9. 云路由加载多个公有网络

10.增量升级

11.优化部分业务逻辑

2.0

2017/06/09主要更新：

1. 全新UI 2.0界面

2. 支持管理多个区域

3. 支持VXLAN网络

4. 本地存储在线迁移云主机

5. 支持在线修改CPU、内存

6. 资源审计功能

7. 支持导出csv文件

8. UI开放全部全局配置选项

9. 优化部分业务逻辑

1.10

2017/03/20主要更新：

1. 超融合管控节点高可用方案
2. 支持指定不同性能的磁盘卷创建云盘
3. 优化TUI界面
4. 完善接管vCenter功能（技术预览版）
5. 支持选择云主机显卡类型
6. 优化部分UI界面

1.9

2017/02/13主要更新：

1. ZStack企业版ISO支持全新TUI及使用模式
2. vCenter支持ZStack云路由（技术预览）
3. 完善接管vCenter部分功能（技术预览）
4. 支持共享云盘
5. 部分操作支持进度条显示
6. 云路由新增负载均衡服务
7. 一个云主机支持使用多个EIP
8. 实时更新云主机的网络和数据云盘的QoS
9. 支持云主机修改CPU和Memory
10. 支持创建云主机时添加virtio-scsi选项
11. 新增云主机、镜像QGA开关
12. 优化部分界面内容
13. 优化部分业务逻辑

1.8

2016/12/05主要更新：

1. 接管vCenter（技术预览）
2. 云路由（IPsec、端口转发、弹性IP、DNS、DHCP）
3. 在线修改云主机密码
4. 指定主存储创建云主机
5. 主存储维护模式
6. 重置云主机

7. 限制普通账户快照、云主机、定时任务数量
8. 数据云盘的virtioscsci 选项
9. 云主机暂停/恢复
10. 管理节点提供ntp时间同步服务
11. 自动更新定时任务状态
12. 显示集群资源信息
13. 设置云主机boot选项
14. 优化部分页面显示内容

1.7

2016/10/09主要更新：

1. 新增LDAP组件
2. 支持删除已导出的镜像
3. 新增关闭电源
4. 支持创建云主机时设置console密码
5. 指定IP时提示可用IP资源
6. 支持多管理节点一键安装
7. 支持启用/停用定时任务
8. 关闭显示日志功能
9. 优化资源监控性能
10. 优化部分页面显示内容

1.6

2016/08/31主要更新：

1. 新增集群功能
2. 新增操作助手
3. 新增定时任务功能
4. 新增云主机克隆功能
5. 新增设置云主机控制台密码功能
6. 新增镜像仓库镜像导出功能
7. 已创建云主机支持添加V删除SSH

8. 支持为账户分配EIP的配额
9. Ceph存储支持指定池名
10. 支持UI界面查看DHCP Server IP
11. 优化Wizard用户体验
12. 优化部分操作顺序

1.5

2016/07/30主要更新：

1. 新增镜像仓库
2. 新增删除计费规则功能
3. 支持在线创建镜像
4. 优化性能监控信息
5. 新增日志语言切换

1.4

2016/06/29主要更新：

1. Java版本从1.7升级到1.8版本
2. 新增性能监控与日志信息
3. 新增FusionStor存储支持
4. 删除本地yum源配置
5. 新增数据库恢复
6. 新增Cassandra数据库备份与恢复
7. 新增ZStack定制版ISO升级yum源
8. 新增在线快照

1.3

2016/05/27主要更新：

1. 初始化界面新增普通用户和SSH指定端口的支持
2. 新增计算规格上行下行网络带宽限制
3. 新增CPU、内存、云盘等计费功能
4. 新增CPU超分
5. 新增云主机操作:更改所有者、指定物理机启动

6. 新增镜像、云盘资源实际占用空间和虚拟占用空间
7. 新增日志收集工具
8. 修改云主机可用与已删除显示列表

1.2

2016/04/27主要更新：

1. 初始化界面新增主存储
2. 新增NFS、Ceph、Shared Mount Point等存储类型支持
3. 新增弹性IP
4. 新增云主机缓存模式
5. 新增云主机高可用
6. 修改SSH key注入方式为Amazon AWS方式
7. 新增控制台代理菜单

1.1

2016/04/01主要更新：

1. 新增用户管理
2. 新增多网络管理
3. 更新Windows Virtio驱动安装
4. 修改章节显示方式

1.0

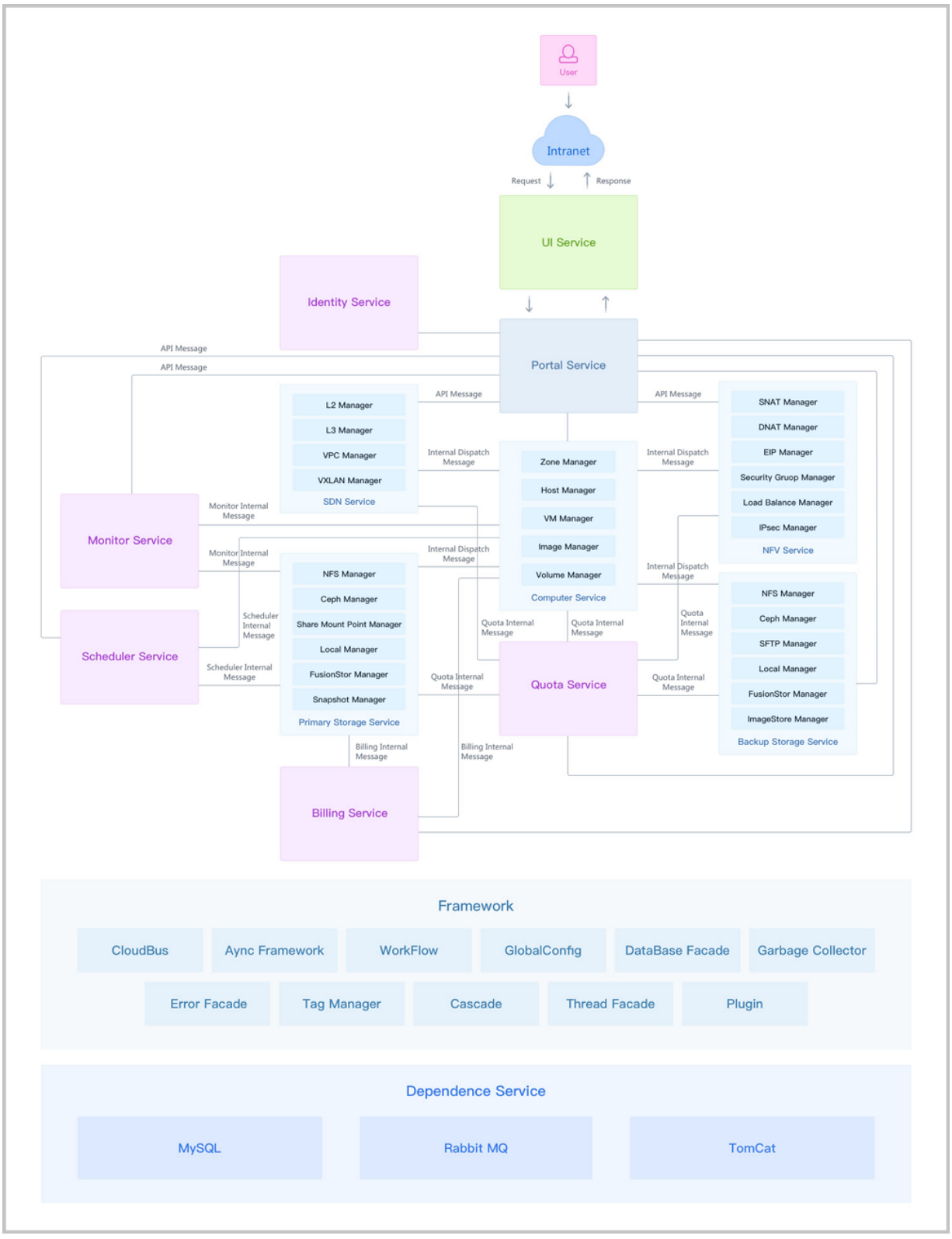
2016/03/01第一次正式发布。

2 概述

产品概述

ZStack是下一代开源的云计算IaaS（基础架构即服务）软件。它主要面向未来的智能数据中心，通过提供灵活完善的APIs来管理包括计算、存储和网络在内的数据中心资源。用户可以利用ZStack快速构建自己的智能云数据中心，也可以在稳定的ZStack之上搭建灵活的云应用场景，例如VDI（虚拟桌面基础架构）、PaaS（平台即服务）、SaaS（软件及服务）等。

图 1: 系统架构示意图



产品功能

ZStack作为产品级私有云平台，提供了对用户数据中心的计算、存储、网络等资源的管理和调度。用户使用ZStack可以快速配置私有云环境，并快速创建云主机、分配云盘和自动配置云主机网络。

ZStack企业版功能列表：

类别	特性	ZStack企业版
区域	管理多个区域	用户可以根据实际情况创建并管理多个区域，一般情况下可将一个物理数据中心归为一个Zone来管理；用户根据不同的业务需求，每个Zone内建立自己独立的集群、主存储、网络等资源
vCenter	管理vCenter	• 支持对现有数据中心中的VMware虚拟化环境进行管理，VMware vCenter Server所管理的vSphere服务器资源和虚拟机资源，能够在虚拟数据中心中使用VMware vSphere资源，并在VMware vCenter集群中完成对云主机的常用操作 • 支持按vCenter区分查看云主机、云盘、镜像等资源
		支持以vCenter为单元对其下资源进行数据同步，保证信息一致
	ESXi云主机	支持云主机的创建、启动、停止、迁移、克隆、重启、暂停、恢复、关闭电源、修改计算规格、设置高可用、打开控制台、设置控制台密码、删除等全生命周期管理及常用功能
	网络	支持创建云路由网络和扁平网络，云路由网络支持所有ZStack网络服务
		支持vSwitch/dvSwitch
	存储	支持按datastore区分主存储和镜像服务器
	镜像	支持添加、启用、停用、删除镜像
	物理机	支持维护模式
	云盘	支持云盘的创建、删除、加载、卸载
	实时性能监控	采集ESXi云主机的CPU、内存、存储和网络运行数据，提供图形可视化
集群	存储架构	集群内使用同构存储服务，存储服务挂载到集群，提供云主机高可用
	物理机	集群内管理物理机，支持实时查看物理机全部CPU使用率、物理机全部内存使用百分比、物理机全部网卡出入速度和物理机全部磁盘读/写IOPS

类别	特性	ZStack企业版
	云主机	集群内管理云主机，支持实时查看云主机全部CPU使用率、云主机全部内存已用百分比、云主机全部网卡出入速度和云主机全部磁盘读/写IOPS
	集群功能	提供高可用特性，支持按照物理机CPU架构定义集群属性
	网络服务	支持VLAN、VXLAN网络加载到集群并统一管理、提供网络自助服务（IP池管理和弹性网络）、支持集群指定迁移网络、支持定义集群的CPU模式
物理机	虚拟化	支持KVM虚拟化技术，支持VMware虚拟化
	c74 ISO	• 支持使用最新英特尔® 至强® 可扩展处理器，例如支持部署在DELL EMC R740 14代服务器上，进一步提升平台稳定性 • 初装用户推荐安装c74 ISO
	资源设定超分	支持CPU、内存和存储空间设定超分比例，适应云环境资源使用
	嵌套虚拟化	支持KVM/ESXi嵌套虚拟化，云主机内部开启CPU硬件虚拟化功能
	实时监控	采集物理机的CPU、内存、存储和网络运行数据，提供图形可视化
	停用与启用	对物理机设定可用属性，以便停止在该物理机上创建云主机
	维护模式	对物理机设定维护状态，设定维护模式后，物理机上的云主机将会迁移（共享存储）
	裸机管理	• 通过PXE技术，使管理员自动化完成对新上线物理裸机的批量部署 • 支持对裸机进行远程电源管理 • 支持VNC无人值守模式
	GPU透传	支持物理机GPU设备透传，让云主机拥有高性能计算和图形处理能力
	USB透传	支持USB透传，满足多种USB应用场景
	操作日志	展示物理机执行任务的事件审计
	导出CSV文件	支持物理机列表导出为CSV表格，方便统计分析处理
云主机	批量操作	批量管理云主机

类别	特性	ZStack企业版
	创建云主机	提供多种策略创建云主机，高效利用资源
	云主机生命周期	支持创建、停止、启动、重启、关闭电源、删除、暂停、恢复等基本生命周期控制
	根云盘在线扩容	支持云主机根云盘在线扩大容量，方便修改云主机配置
	数据云盘在线扩容	支持云主机数据云盘在线扩大容量，即时生效
	云主机控制台	用户可通过终端方式访问云主机，而不依赖云主机远程工具，支持控制台设置密码
	云主机快照	• 在云主机运行过程中进行快照 • 在线快照（支持ImageStore/Ceph/FusionStor类型的镜像服务器） • 关机快照（支持ImageStore/Sftp/Ceph/FusionStor类型的镜像服务器）
	云盘在线快照	在使用云盘的过程中进行快照
	云主机在线修改密码	支持Windows/Linux的云主机在线修改密码
	云主机在线创建镜像	运行中的云主机在线创建镜像
	云主机QGA开关	灵活控制qemu guest agent的状态
	云主机RDP模式开关	针对VDI用户界面，启用后默认以RDP模式打开控制台
	云主机显卡切换	支持选择云主机显卡类型：qxl、cirrus、vga
	云主机显卡透传	支持英伟达和AMD GPU设备透传给云主机
	User Data导入	支持创建云主机时导入User Data
	云主机克隆（不带数据云盘）	• 基于云主机快速克隆若干个云主机 • 在线克隆（支持ImageStore/Ceph类型的镜像服务器） • 关机克隆（支持ImageStore/Ceph类型的镜像服务器）
	整机克隆（带数据云盘）	• 同时克隆云主机的根云盘和数据云盘内容 • 仅支持ImageStore类型的镜像服务器 • LocalStorage/NFS/SMP类型的主存储，支持在线/暂停/关机克隆 • Ceph类型的主存储，支持在线/暂停/关机克隆 • Shared Block类型的主存储，支持暂停/关机克隆 • 挂载共享云盘的云主机不支持整机克隆

类别	特性	ZStack企业版
	更换系统盘	支持云主机关机状态下修改操作系统
	重置云主机	支持恢复云主机状态为模板初始状态
	根云盘扩容	支持在线/关机状态下的云主机根云盘扩容，方便修改云主机配置
	基于ISO部署	• 基于ISO系统光盘部署云主机，引导安装系统 • 允许一个云主机加载多个ISO，提升业务部署效率
	基于模板部署	基于系统模板创建云主机
	制作镜像模板	基于当前某个云主机制作模板
	创建镜像	• 云主机运行中在线创建镜像 • 在线创建镜像（支持ImageStore/Ceph类型的镜像服务器） • 关机创建镜像（支持ImageStore/Sftp/Ceph/FusionStor类型的镜像服务器）
	自定义MAC地址	• 支持创建云主机时指定MAC地址 • 支持云主机修改MAC地址
	云主机启动顺序	调整云主机的启动顺序，用于切换ISO引导
	动态加载、卸载云盘	云主机可动态加载和卸载云盘，支持优化驱动模型，支持SCSI WWN号唯一识别
	动态加载、卸载网卡	云主机可动态加载和卸载网卡，支持设置默认网卡
	加载GPU卡	支持创建云主机时加载GPU设备
	共享云盘	支持Ceph存储或Shared Block主存储下多云主机共享使用同一数据云盘
	实时性能监控	采集云主机的CPU、内存、存储和网络运行数据，提供图形可视化
	高可用特性	物理机故障，云主机自动重启
	在线修改云主机CPU/内存	支持在线修改云主机配置，不用重启VM
	实时更新云盘和网络QoS	提供云盘和网络的限速能力，避免单个云主机占用过量资源

类别	特性	ZStack企业版
	SSH密钥注入	支持Linux和BSD操作系统SSH密钥注入，支持创建和删除秘钥
	自定义计算规格	支持自定义计算规格，满足各种应用资源消耗特性
	自定义标签	支持自定义标签，满足查询和编写定时任务
	资源删除保护	云资源删除后，将移入回收站，提供恢复和确认销毁
	冷迁移	支持本地主存储类型上的云主机进行关机状态迁移
	在线迁移	支持所有主存储类型上的云主机进行在线迁移
	存储迁移	• 多NFS主存储之间的云主机支持跨存储设备冷迁移 • 多Ceph主存储之间的云主机支持跨存储设备冷迁移 • 多Shared Block主存储之间的云主机支持跨存储设备冷迁移，且支持同时迁移加载的云盘
	操作日志	展示云主机操作过程的事件审计
	Windows系统性能优化	提供Windows云主机性能优化加速
	USB重定向	支持将VDI客户端USB设备重定向至云主机
	导出CSV文件	支持云主机列表导出为CSV表格，方便统计分析处理
云盘	云盘管理	支持云盘的创建、启用、停用、加载、卸载、迁移、创建快照、创建镜像、扩容、更改所有者、存储迁移、删除
云盘规格	云盘规格管理	支持云盘规格的创建、启用、停用、全局共享、全局召回、云盘规格QoS、删除
计算规格	计算规格管理	• 支持计算规格的创建、启用、停用、磁盘QoS、网络QoS、全局共享、全局召回、删除 • 支持选择物理机分配策略 • 当物理机分配策略为CPU使用率最低/内存使用率最低，支持选择强制、非强制策略模式
镜像管理	系统模板	支持系统模板，支持QCOW2和RAW格式，自动匹配镜像类型
	ISO镜像	支持ISO镜像，支持从ISO镜像引导云主机
	系统镜像上传	支持URL上传和本地浏览器上传
	云盘镜像上传	支持URL上传和本地浏览器上传

类别	特性	ZStack企业版
	镜像迁移	支持Ceph主存储上的镜像跨存储设备迁移、支持NFS主存储上的镜像跨存储设备迁移
镜像仓库	镜像存放	存放镜像数据，包括ISO和系统模板
	镜像导出	支持镜像导出下载链接
	镜像同步	支持镜像仓库间的镜像互传，可以跨区域使用
	标准系统镜像	支持标准的系统，支持Windows、红帽、Ubuntu和其他开源Linux系统
	预设运行镜像	支持众多的软件运行环境，支持Windows IIS和Dot Net Framework运行环境，支持Linux Tomcat、JAVA、Apache Web、Jboss、PHP、Node JS、Golang、Python等语言和运行环境，支持数据库Oracle、MySQL、Postgres、Mongodb、Influxdb、Cassandra和Redis等数据库服务；支持广泛的应用中间件
	预设应用镜像	支持众多的应用系统，论坛BBS、社交SNS、博客Blog、微博的常用应用系统；支持phpmyadmin等运维管理应用；支持厂商提供的应用镜像
	自定义镜像	支持管理员根据标准系统镜像和预设运行镜像，定义满足自身业务系统运行环境的镜像，以增量方式保存镜像内容，并实现智能去重功能
	存储支持	与本地存储、NFS、SMP、Ceph、Shared Block类型的主存储无缝支持
存储管理	本地存储	• 支持云盘存放到物理机本地 • 支持实时查看主存储已用容量百分比趋势图
	NFS存储	• 支持云盘存放到NFS协议存储，物理机共享访问 • 共享文件系统管理节点高可用方案 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持实时查看主存储已用容量百分比趋势图
	共享挂载存储	• 支持云盘存放到POSIX兼容的共享存储，支持iSCSI/FC存储 • 共享文件系统管理节点高可用方案 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用

类别	特性	ZStack企业版
		• 支持实时查看主存储已用容量百分比趋势图
	Shared Block存储	• 支持添加iSCSI/FC协议存储，物理机共享访问 • 支持添加多个LUN • 支持实时查看主存储已用容量百分比趋势图
	Ceph存储	• 支持共享云盘 • 超融合管理节点高可用方案 • 支持指定不同性能的磁盘卷创建云盘 • 支持云盘存放到Ceph分布式存储 • 支持数据冷迁移 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持创建Ceph pool，以pool计算容量并设置显示名，并设置显示名 • 支持实时查看主存储已用容量百分比趋势图
	FusionStor存储	• 支持云盘存放到FusionStor分布式存储 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用
	多主存储支持	支持同一集群挂载多个主存储，包括：多个本地存储、多个NFS存储、多个Shared Block存储、一个本地存储和一个NFS/SMP/Shared Block存储
网络管理	VLAN二层隔离	支持VLAN 802.1q作为网络隔离手段
	VXLAN网络	支持VXLAN网络，有效解决云数据中心逻辑网段不足、上层交换机MAC地址溢出等问题、支持云主机的跨地域迁移
	分布式扁平网络	支持云主机直接使用真实网络IP资源
	分布式弹性网络	支持云主机使用虚拟网络地址，与真实网络映射
	分布式DHCP服务	支持云主机自动获取分配的IP地址
	网络地址空间预留	支持预留网络地址空间，以便与物理网络混合使用
	动态和静态分配IP	支持动态分配IP地址，支持指定使用某个IP地址
	多级网络管理	支持云主机接入多个网络，构建复杂场景的业务
	虚拟IP的QoS设置	支持对虚拟IP做QoS限制，对网络服务的高效分配管理
	MTU	自定义限制网络传输数据包的大小

类别	特性	ZStack企业版
	VPC路由器	支持创建VPC路由器的全生命周期管理，包括：创建、删除、修改、VPC网络的加载/卸载，东西向流量的设置、云路由网络的所有网络服务，集中在VPC路由器中配置DNS
	VPC网络	支持创建VPC网络、添加网络段、添加DNS、加载/卸载VPC路由器、删除
	公有网络	• 支持创建云主机 • 支持为网络服务提供虚拟IP
	系统网络	可作为管理网络、存储网络、迁移网络等使用
	云路由网络	• 支持基于云路由的弹性IP • 支持基于云路由的端口转发 • 支持基于云路由的外部负载均衡以及内部访问业务流量的负载均衡 • 支持基于云路由的IPsec隧道服务 • 支持多个弹性IP绑定同一个云主机网卡 • 支持一个云路由器接多个公有网络 • 支持配置静态路由表 • 支持分布式DHCP提升服务性能
	网络拓扑	• 全局网络拓扑查看，支持高亮显示 • 自定义选择资源展示拓扑图
定时任务	定时对象	支持云主机、云盘的定时操作
	定时操作	可对云主机关闭/重启，云盘快照等设置定时操作
资源编排	资源栈	• 支持在线编辑方式和使用模板方式创建资源栈 • 支持预览/校验模板内容，支持云主机插入userdata • 支持删除资源栈和级联删除资源栈中所有资源
	自定义模板	支持通过文本编辑器方式和本地上传方式创建资源栈模板，并支持创建、查看、修改、删除、预览操作
	示例模板	云平台默认提供的资源栈模板示例，作为参考模板
安全管理	三层安全策略	支持基于TCP/UDP端口的安全策略
	安全组统一管理	支持安全组统一管理云主机安全策略，实现组内互通，组间策略

类别	特性	ZStack企业版
性能TOP5和性能分析	性能TOP5	支持物理机、云主机、路由器、虚拟IP、三层网络等多种资源排序，并可自定义不同时间段查看
	云主机性能统计	支持自定义时间段查看，指定资源范围，对云主机CPU使用率、内存使用率、磁盘读速度、磁盘写速度、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	路由器性能分析	支持自定义时间段查看，指定资源范围，对路由器CPU使用率、内存使用率、磁盘读速度、磁盘写速度、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	物理机性能统计	支持自定义时间段查看，指定资源范围，对物理机CPU使用率、内存使用率、磁盘读速度、磁盘写速度、磁盘读IOPS、磁盘写IOPS、磁盘已用量百分比、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	三层网络性能分析	支持自定义时间段查看，指定资源范围，对三层网络已用IP数、已用IP百分比、可用IP数、可用IP百分比行过滤分析排序
	虚拟IP性能分析	支持自定义时间段查看，指定资源范围，对虚拟IP的下行网络流量、下行网络入包速率、上行网络流量、上行网络入包速率进行过滤分析排序
	镜像服务器性能分析	支持自定义时间段查看，指定资源范围，对镜像服务器的可用容量百分比进行过滤分析排序
ZWatch	物理机监控	对物理机运行实时监控，显示CPU、内存、磁盘和网络时序监控图
	云主机监控	对云主机运行实时监控，显示CPU、内存、磁盘和网络时序监控图
	监控	• 支持对系统时序数据进行监控，例如云主机内存使用率、物理机CPU使用率等 • 支持对系统事件进行监控，例如云主机状态变化事件、物理机失联事件等
	报警	对时序性数据和事件设置报警器，并通过SNS通知系统接收报警信息，支持邮件/钉钉/HTTP 应用方式接收报警信息
	多接收端	支持邮件/钉钉/HTTP应用等多种接收端

类别	特性	ZStack企业版
审计	资源审计	• 支持ZStack所有资源的审计查询，用户能对该资源的所有操作行为审计，有效保障用户在云环境下核心数据的安全 • 支持查看调用API名称、消耗时间、任务结果、操作员，任务创建/完成时间，以及API行为的消息详情，且支持CSV格式导出
操作日志	操作日志	支持查看操作描述、任务结果、操作员、登录IP、任务创建/完成时间，以及操作返回的消息详情，实现更细粒度管理，且支持CSV格式导出
账户管理	账户和用户管理	账户管理功能，分为账户和用户，其中账户是资源计量团体，用户可定义操作权限
	AD/LDAP账户	• 支持添加AD/LDAP账户，并绑定普通账户 • 支持自定义清除规则
	账户云资源配额	支持自定义分配账户最大可用资源，包括云主机运行数量、CPU、内存、云盘数量、云盘总容量、镜像数量、镜像总容量、弹性IP数量等
	用户组权限分配	支持用户组权限分配，统一编排用户权限
	用户操作权限分配	支持对用户进行权限分配
	云主机更改所有者	支持变更云主机所有者，指定云主机所属账户
	云盘更改所有者	支持变更云盘所有者，指定云盘所属账户
	计算规格指定分配	支持计算规格共享特性，可指定账户是否可使用
	镜像资源指定分配	支持镜像资源共享特性，可指定账户是否可使用
	云盘规格指定分配	支持云盘规格共享特性，可指定账户是否可使用
	网络资源指定分配	支持网络资源共享特性，可指定账户是否可使用
	全局配置	管理员可以直接在UI上对很多特性进行全局配置 • 所有的全局配置都有一个默认值 • 更新全局配置并不需要重启管理节点
	修改admin账户密码	忘记admin账户的登录密码，可以使用`zstack-ctl reset_password`还原默认值
计费	自定义计费单价	支持自定义CPU、GPU、内存、系统云盘和数据云盘的计费单价，其计费单价支持秒、分、小时和天；支持删除某时段的计费设置

类别	特性	ZStack企业版
	基于账户计费	基于账户进行计费，统计账户各项目消费情况
	灵活计费单价	动态可调的计费单价，满足周期性促销需求
访问	TUI	支持常用运维操作，定制化OS界面
	图形界面	支持以HTTP/HTTPS方式访问图形界面的云管理平台，账户（用户名密码方式或AD/LDAP方式）和用户支持图形界面登录访问
	命令行	支持通过命令行方式访问云管理平台，命令行支持全功能访问，账户和用户支持命令行登录访问
	API接口	支持全功能的API交付，API支持消息总线访问和HTTP接口访问
操作助手	智能提示	对ZStack的核心操作给出智能的环境检查和操作指导
亲和组	反亲和组	目前提供针对云主机与物理机的两种亲和组策略：反亲和组(非强制)、反亲和组(强制)，从而合理调度平台资源
UI强化	自定义产品信息	对UI上的产品Logo和产品名称等进行自定义
	首页大屏	华丽大屏展示平台整体情况
	加密访问	支持HTTPS安全访问登录平台
	过程展示	增加多个场景进度条
VDI	解决方案	• 通过定制客户端，支持SPICE，RDP，VNC等协议，并进行了优化 • 支持指定VDI网络 • 支持USB重定向，兼容多种USB设备 • 支持设置独立VDI网络 • 支持多屏显示 • 支持麦克风 • 支持SPICE流量优化
UI导航	快速入口	增加快速进入产品与服务的入口，并支持高亮标注
UI信息导出	列表信息CSV导出	导出云主机和物理机主列表的信息，离线管理便于图表编辑
应用中心	应用中心	支持添加包括存储、数据库、安全、IaaS、PaaS、SaaS类型在内的应用插件
License	云平台许可证	• 云平台许可证 (Basic License) 包括企业版和混合云版

类别	特性	ZStack企业版
		• 支持本地浏览器上传License • License到期提醒
	模块许可证	• 模块许可证 (Plus License) 为用户提供附加功能 • 依赖于平台许可证使用 • 已包括：企业管理模块、VMware管理模块 • 支持本地浏览器上传License • License到期提醒
管理节点	管理节点高可用（基于超融合方案）	• 支持基于Ceph的超融合场景 • 支持基于NFS、SMP的共享文件系统场景 • 支持多网络灵活配置
安装	一键安装	一条命令，30分钟完成从裸机到云平台的安装部署
升级	无缝升级	ZStack支持低版本至高版本的无缝升级
	增量升级	支持增量升级，大幅提高升级速度
	环境升级	可以指定只升级部署环境，通过专家模式自定义安装升级

ZStack企业管理模块功能列表：

类别	特性	企业管理模块
组织架构	用户	• 用户是企业管理中的最基本单位 • admin/平台管理员可创建用户，并基于用户建立相应的组织架构 • 支持添加用户、删除用户、修改用户名、修改密码、修改个人信息、加入部门、从部门移除、加入项目、从项目移除 • 用户的个人信息包括姓名、手机号码、邮箱地址和编号
	组织	• 组织是企业管理中组织架构的基本单位 • 组织以组织架构树的方式呈现，分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门，支持创建多个顶级部门 • 支持添加组织、删除组织、更改上级部门、更改部门负责人、创建子部门、删除子部门、添加用户、移除用户
项目管理	项目	• 用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务

类别	特性	企业管理模块
		• 企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池 • 支持创建项目、删除项目、启用项目、停用项目、更换项目负责人、生成项目模板、添加成员、移除成员、停用项目资源、恢复过期项目
	项目模板	• 用于标识各个资源配额的模板 • 在创建项目时，可直接使用模板定义的配额来快速创建项目 • 支持创建项目模板、删除项目模板
	成员	• 成员作为项目的基本组成人员，一般由admin/平台管理员/项目负责人/项目管理员添加进入项目 • 项目成员的权限可由admin/平台管理员/项目负责人/项目管理员进行相应控制
	成员组	• 项目负责人/项目管理员可在项目中创建成员组，对成员进行分组管理 • 可以成员组为单位进行权限控制
工单管理	工单申请	• 项目成员可对云平台资源提出工单申请 • 支持项目成员创建、撤回、重新打开以及删除工单
	工单审批	• admin可进行一键审批，资源可自动部署成功并分发到项目中 • 支持admin通过、驳回工单，审批通过后会自动部署，该项目下的资源会立即生效
独立区域管理	平台管理员	• 平台管理员主要是带有区域属性的管理员 • admin可划分不同区域给不同平台管理员来管控不同区域的数据中心 • 支持创建/删除平台管理员、修改密码、添加区域和移除区域
	资源隔离	• 在对区域进行资源隔离的基础上，可对每个区域指定相应的区域管理员，实现各地机房的独立管理 • 同时admin可对所有区域进行巡查和管理

3 配置需求

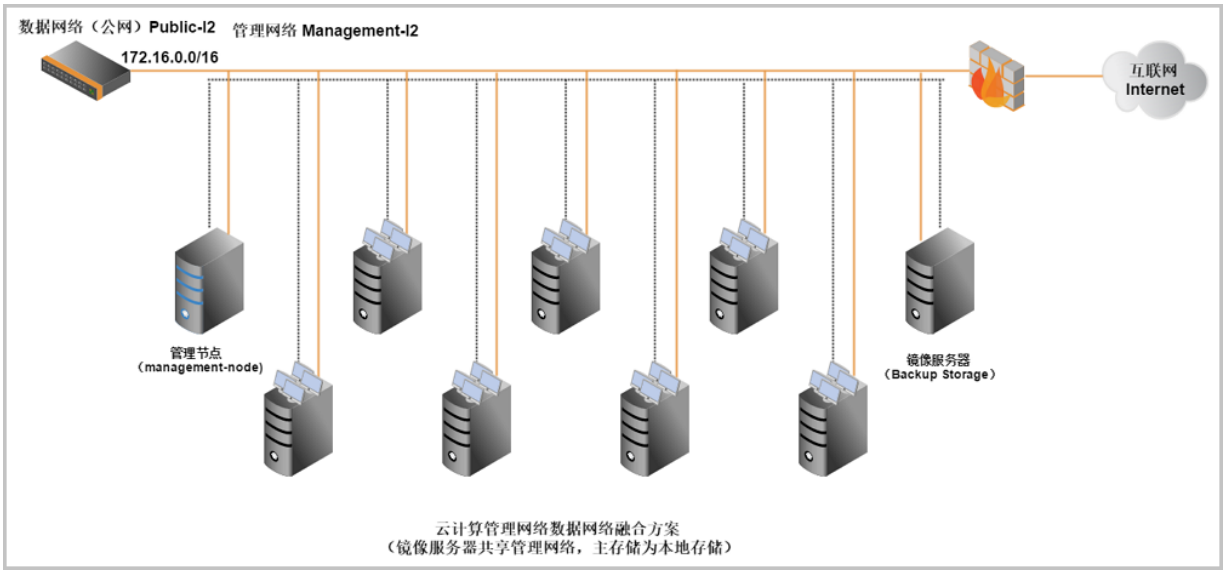
本章主要针对ZStack私有云平台运行所必须的基本环境配置进行简要说明。

3.1 网络环境

云计算环境是公司内非常重要的IT基础架构。安装ZStack前，请仔细阅读并依照配置需求完成基础环境的软硬件环境准备。不当的环境配置，可能导致无法完成随后的私有云环境部署，或者在使用中遇到异常。

如图 2: 网络环境示意图所示，是搭建在一个小型数据中心上典型的私有云环境。该环境由若干台功能不同的服务器，两个独立的网络环境构成。

图 2: 网络环境示意图



其中有两台服务器用于ZStack管理节点和存放云主机的镜像（在小型数据中心中，管理节点和镜像服务器可以共用一台服务器，在大规模的物理环境中可以配置多台管理节点提供高可用性和多台镜像服务器扩展镜像存储容量和吞吐率），其余服务器作为云主机的物理宿主机。

每台服务器均连接到管理网络和数据网络，其中数据网络可以通过防火墙访问互联网。管理网络是管理节点管理物理机、云主机、云盘等云端资源的网络。数据网络是云主机提供数据服务的网络，图中的IP地址仅作为示例给用户参考。

注:

- 连接管理网络的服务器需指定静态的IP地址，并在之后添加物理服务器时使用。

- 连接数据网络服务器上的网卡可以不用指定IP地址，但是每台服务器连接数据网络的网卡设备名称需相同（例如都是eth0）。

3.2 硬件要求

建议的最低系统配置：

1. 主机：物理机的CPU不低于4核心，需支持x86架构的硬件虚拟化特性（例如Intel的VMX，或者AMD的SVM），并需在BIOS打开CPU虚拟化支持。用户可采用服务器或PC机做演示和一般的开发环境。物理机需要配置统一的CPU型号，以防止CPU指令集支持的不同。
2. 内存：8G以上。内存总量的大小直接决定了服务器运行云主机的数量。
3. 网络：物理机需配置千兆网卡，物理机之间搭建千兆网络。所有物理机网卡命名一致，并且使用相同网卡承载相同的通信流量，例如管理流量都使用eth0网卡。用户需提前对网络交换机完成必要的配置。

   注: 如需采用VLAN网络环境，请提前在交换机上配置对应的VLAN网络通讯。ZStack会主动给云主机分配IP地址，需预留一段和系统不冲突的IP地址，同时要避免和原有网络环境中的DHCP服务冲突。
4. 存储：主存储或镜像存储均建议2T以上容量。

   - 如果采用了本地硬盘做主存储，考虑到镜像服务器和主存储的可靠性，建议采用存储冗余备份方案。例如4块硬盘做RAID10。如果云主机的IO读写性能均要求很高，建议采用全SSD硬盘的RAID配置。
   - 如果云主机的IO访问更多偏向读性能，也可以采用SSD和机械硬盘混合的配置（如有需求请咨询ZStack公司技术支持获取帮助）。镜像存储服务器可以根据实际云主机环境中使用的情况，随时扩容。
   - 如果采用NFS、Ceph、FusionStor或者支持Shared Mount Point的分布式文件系统的网络存储，则需提前配置好相应的存储或文件系统。如果镜像服务器采用了Ceph，那么主存储也需使用Ceph来配置。如果镜像服务器采用了FusionStor，那么主存储也需使用FusionStor来配置。

4 安装部署

本章主要介绍ZStack企业版 2.5.1的安装/升级过程。

4.1 环境准备

前提条件

安装/升级ZStack都必须使用ZStack定制版ISO，特性如下：

1. ZStack定制版ISO提供以下两个版本：
   - c72版（基于CentOS 7.2深度定制）：ZStack-x86_64-DVD-2.5.1-c72.iso
   - c74版（基于CentOS 7.4深度定制）：ZStack-x86_64-DVD-2.5.1-c74.iso

   注:
   - c72 ISO不支持英特尔新一代铂金/金/银/铜系列处理器（Intel® Xeon® Scalable Processors）。如已部署ZStack（基于c72 ISO），可升级至最新版本，详情请参考*c72版 升级*章节。
   - c74 ISO支持英特尔新一代铂金/金/银/铜系列处理器（Intel® Xeon® Scalable Processors），例如支持部署在DELL EMC R740 14代服务器上。如初次安装ZStack，推荐安装c74 ISO。如已部署ZStack（基于c74 ISO），可升级至最新版本，详情请参考*c74版 升级*章节。
2. 友好的TUI管理界面，支持多种系统配置；
3. 安装ZStack无需连接外网，也无须配置yum源，就可以实现完全离线安装；
4. 提供以下几种安装模式：企业版管理节点模式、社区版管理节点模式、计算节点模式、专家模式，用户按需选择即可；
5. 取消了eth设置，采用系统默认的网卡命名规则；
6. 默认选项：**DATE&TIME**为亚洲东八区，**LANGUAGE**为English(United States)，**KEYBOARD**为English(US)。

由于c72 ISO与c74 ISO的初始安装步骤基本相同，因此以初装c72 ISO为例进行介绍。

操作步骤

1. 安装ZStack之前，请管理员准备好以下必要的软件包，以便安装部署过程顺利执行。
   - ZStack定制版ISO
     - 文件名称：ZStack-x86_64-DVD-2.5.1-c72.iso

- 下载地址：点击这里

- ZStack安装包
  - 文件名称：ZStack-installer-2.5.1.bin
  - 下载地址：点击这里

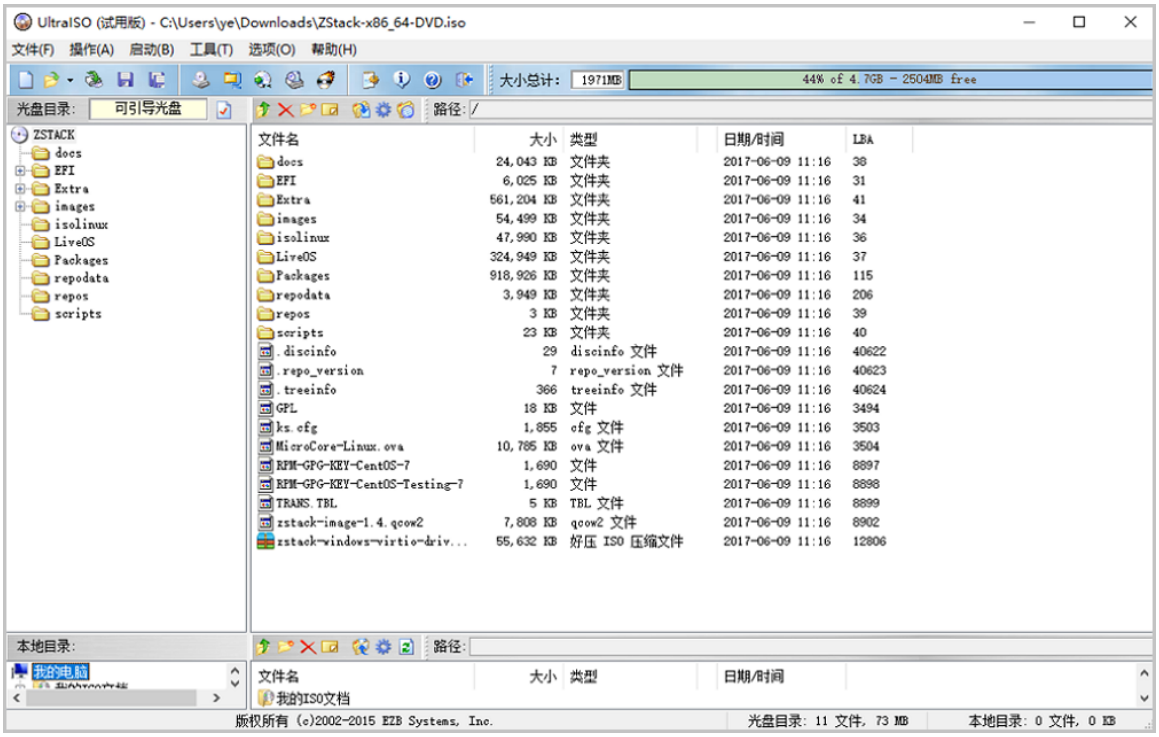
注: 软件下载后，需通过MD5校验工具核对校验码，以确保软件完整无损。

2. 使用UltraISO，将此ISO镜像刻录到U盘。

a) 在UltraISO打开ISO镜像。

打开UltraISO，点击**文件**按钮，选择打开已下载好的ISO镜像文件，如图 3: 在UltraISO打开ISO镜像所示：

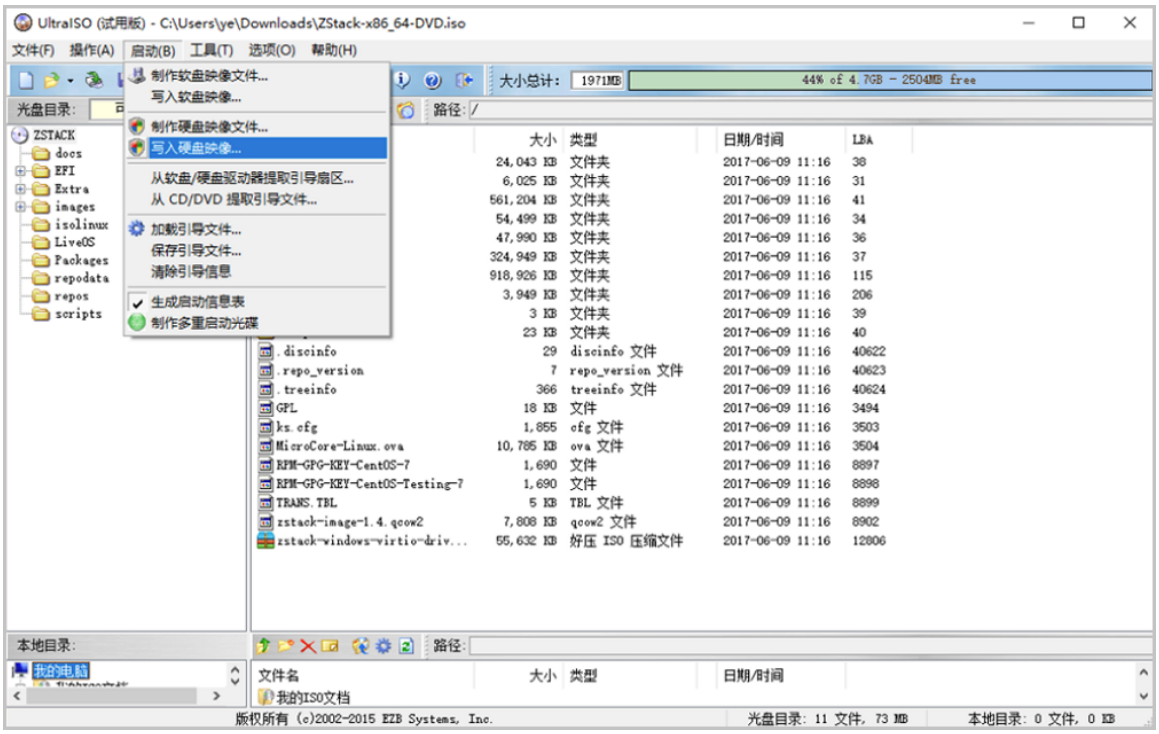
图 3: 在UltraISO打开ISO镜像



b) 写入硬盘镜像。

在UltraISO，点击**启动** > **写入硬盘映像**，如图 4: 在UltraISO写入硬盘映像所示：

图 4: 在UltraISO写入硬盘映像



c) 在**硬盘驱动器**列表选择相应的U盘进行刻录。

注:

- 如果系统只插了一个U盘，则默认以此U盘进行刻录和写入，在刻录前，**注意备份U盘之前的内容。**
- 其他选项，按照默认设置，无须额外配置，点击**写入。**

如图 *5: 在UltraISO确认写入ISO镜像*所示：

图 5: 在UltraISO确认写入ISO镜像

d) 在新界面中点击**是**进行确认，UltraISO将会把ISO镜像刻录到U盘。

e) 此时U盘可用来作为启动盘，支持Legacy模式和UEFI模式引导。

3. 安装操作系统。

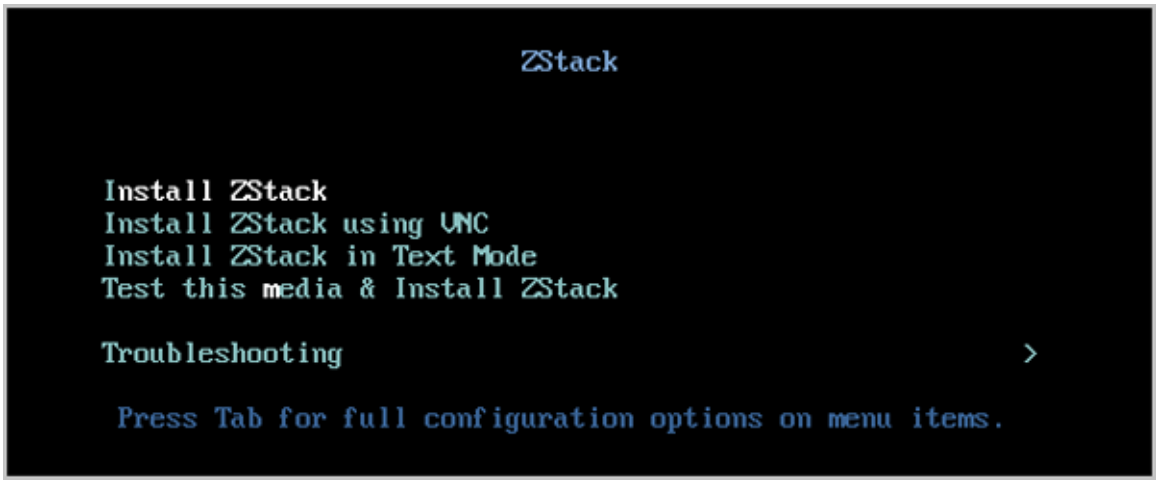
a) 管理员需要预先在服务器进行以下配置：

- 确认服务器内硬盘的数据已作备份，安装过程会覆盖写入；
- 进入BIOS，开启CPU VT选项；开启超线程HT选项；
- 进入阵列卡配置合适的RAID级别，以提供一定的数据冗余特性；
- 设置U盘为第一启动顺序。

b) 以上设置完毕后，服务器重启或上电后，进入安装导航。

如图 *6: U盘引导界面*所示，进入ISO引导安装界面，默认选择**Install ZStack**开始安装操作系统。

图 6: U盘引导界面



注:

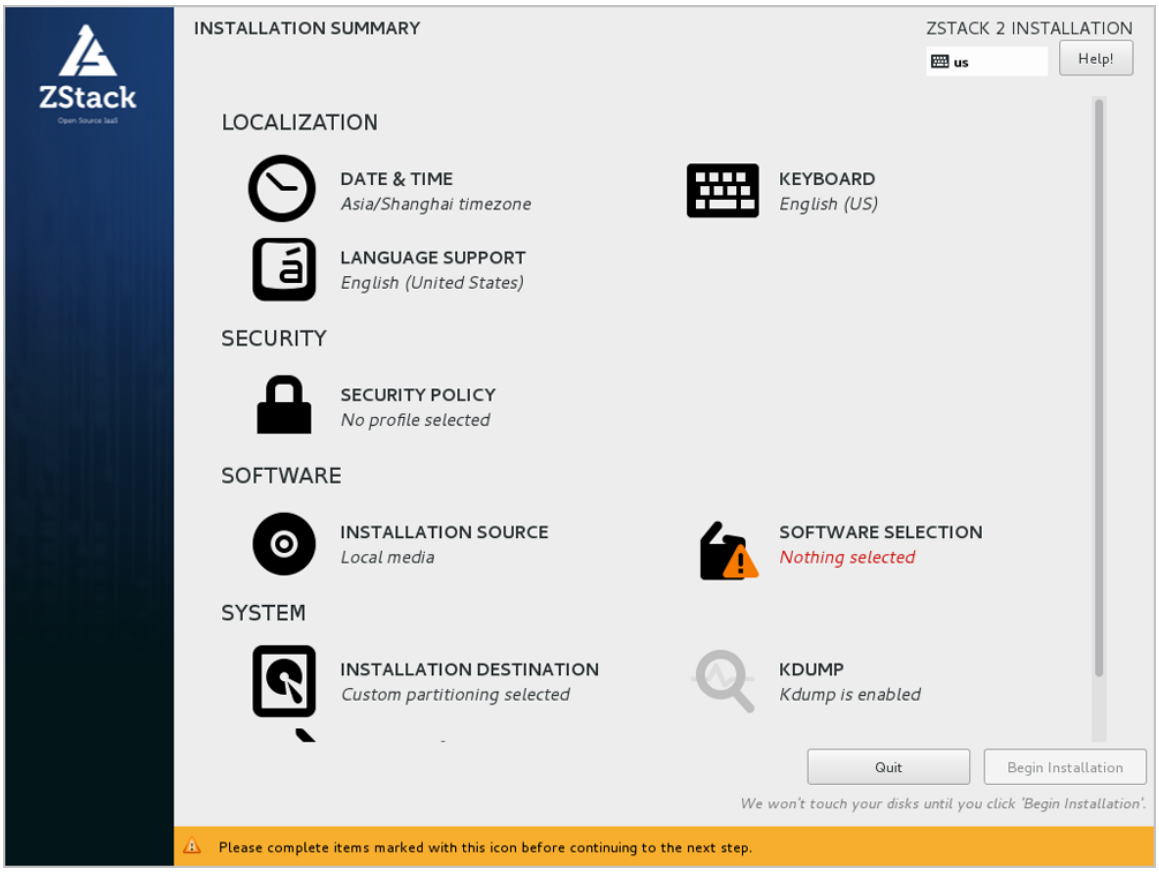
- ZStack提供了三种安装方式：图形界面安装、通过VNC安装和字符界面安装，用户可根据实际情况选择。
- ZStack建议图形界面安装是最好的选择。
- 考虑到某些服务器是不带VGA接口的，只能通过串口连接，这时用户可以选择VNC或者Text Mode。

c) 进入系统安装界面后，已经预先配置如下默认选项，一般情况下管理员无需更改配置。

- **DATE&TIME**：为亚洲东八区
- **LANGUAGE**：English(United States)
- **KEYBOARD**：English(US)

如图 *7: 系统安装界面*所示：

图 7: 系统安装界面



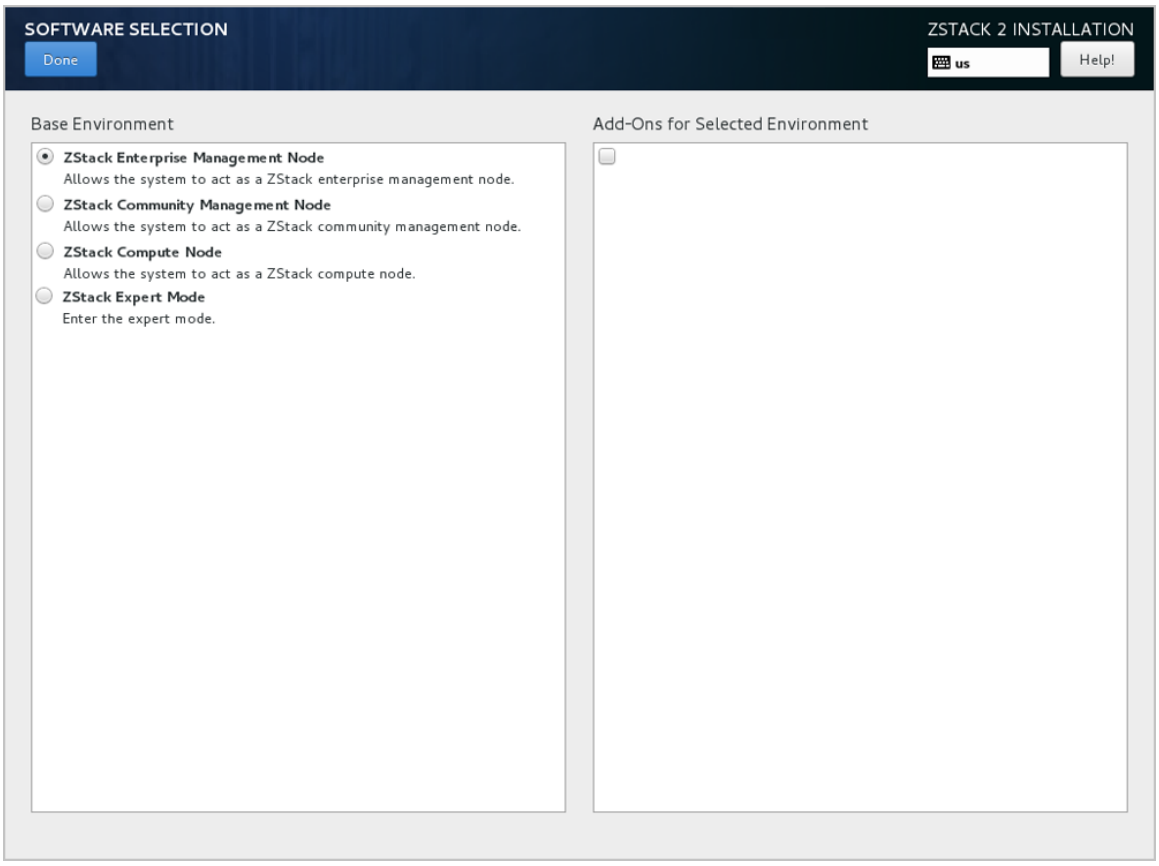
d) 选择安装模式。

在系统安装界面，点击**SOFTWARE SELECTION**进入服务器安装模式候选，如图 *8:* 选择安装模式所示：

注:

- 有以下几种安装模式可供选择：
  1. ZStack Enterprise Management Node：ZStack企业版管理节点模式
  2. ZStack Community Management Node：ZStack社区版管理节点模式
  3. ZStack Compute Node：ZStack计算节点模式
  4. ZStack Expert Node：ZStack专家模式
- 首次安装建议选择**ZStack Enterprise Management Node**。

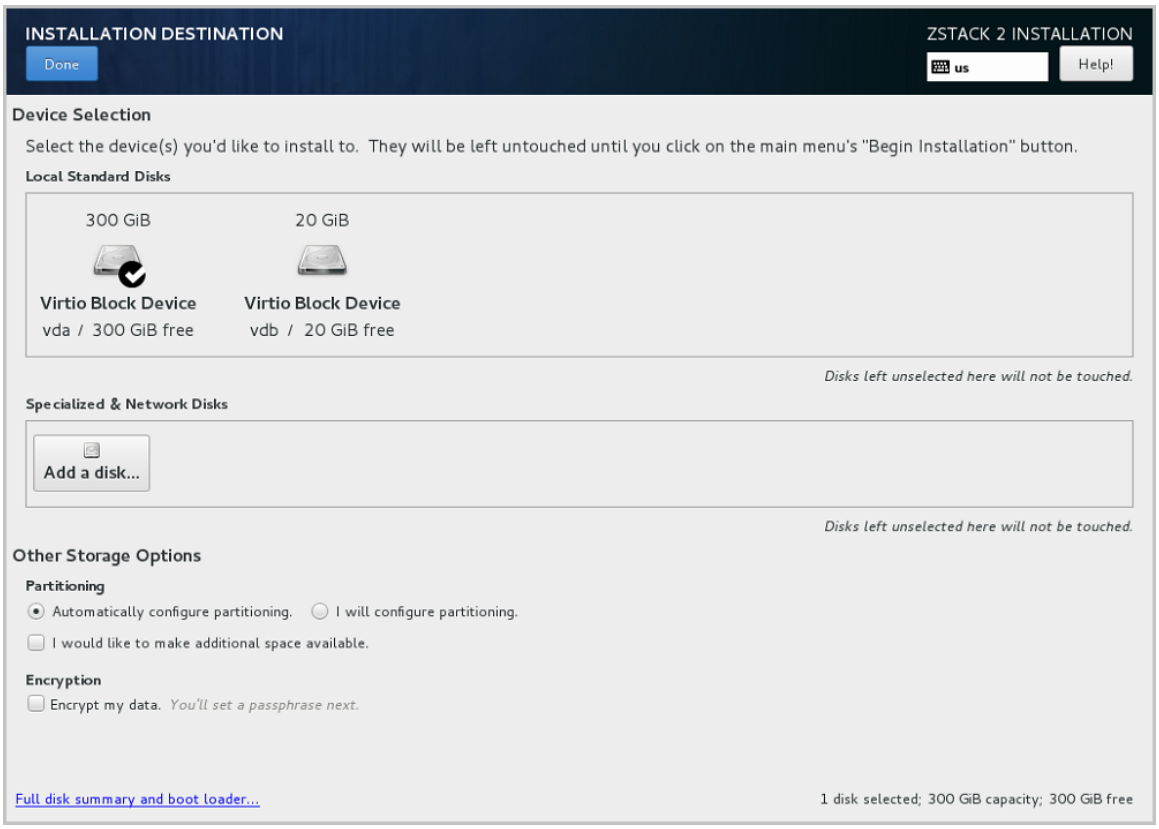
图 8: 选择安装模式



e) 配置硬盘分区。

在系统安装界面，点击**INSTALLATION DESTINATION**进入硬盘分区配置界面，如图 *9:* 系统预先默认设置 - 自动硬盘分区所示：

图 9: 系统预先默认设置 - 自动硬盘分区



注: 安装系统时，建议只勾选系统盘需要使用的硬盘，其他硬盘如果有特殊用途，建议不做勾选。

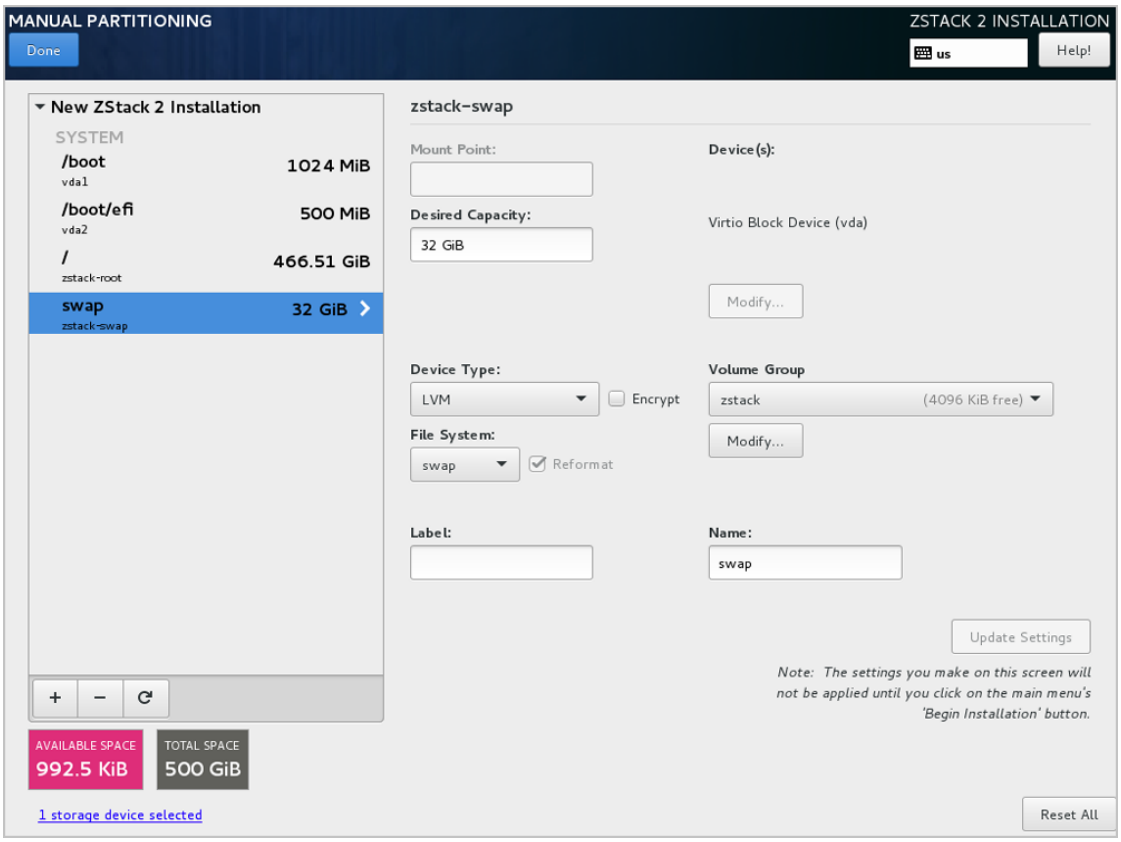
系统预先默认设置：**Automatically configure partitioning**，ZStack建议遵循默认设置，执行自动硬盘分区。

如果选择自定义手动分区，建议如下：

- 分区模式有UEFI 模式和Legacy模式两种，应与BIOS设置的引导模式一致。
  - UEFI 模式
    - */boot*：创建分区 1GB
    - */boot/efi*：创建分区 500MB
    - *swap*（交换分区）：创建分区 32GB
    - /（根分区）：配置剩下容量
  - Legacy模式
    - */boot*：创建分区 1GB
    - *swap*（交换分区）：创建分区 32GB
    - /（根分区）：配置剩下容量

- 以上数值为ZStack建议分区容量（硬盘总容量在300G以上）
- Legacy模式不支持单盘容量大于2T，而UEFI模式没有此限制，且还支持GPT分区，因此ZStack推荐手动分区用户采用UEFI模式来分区，如图 *10: 手动分区推荐UEFI模式*所示：

图 10: 手动分区推荐UEFI模式



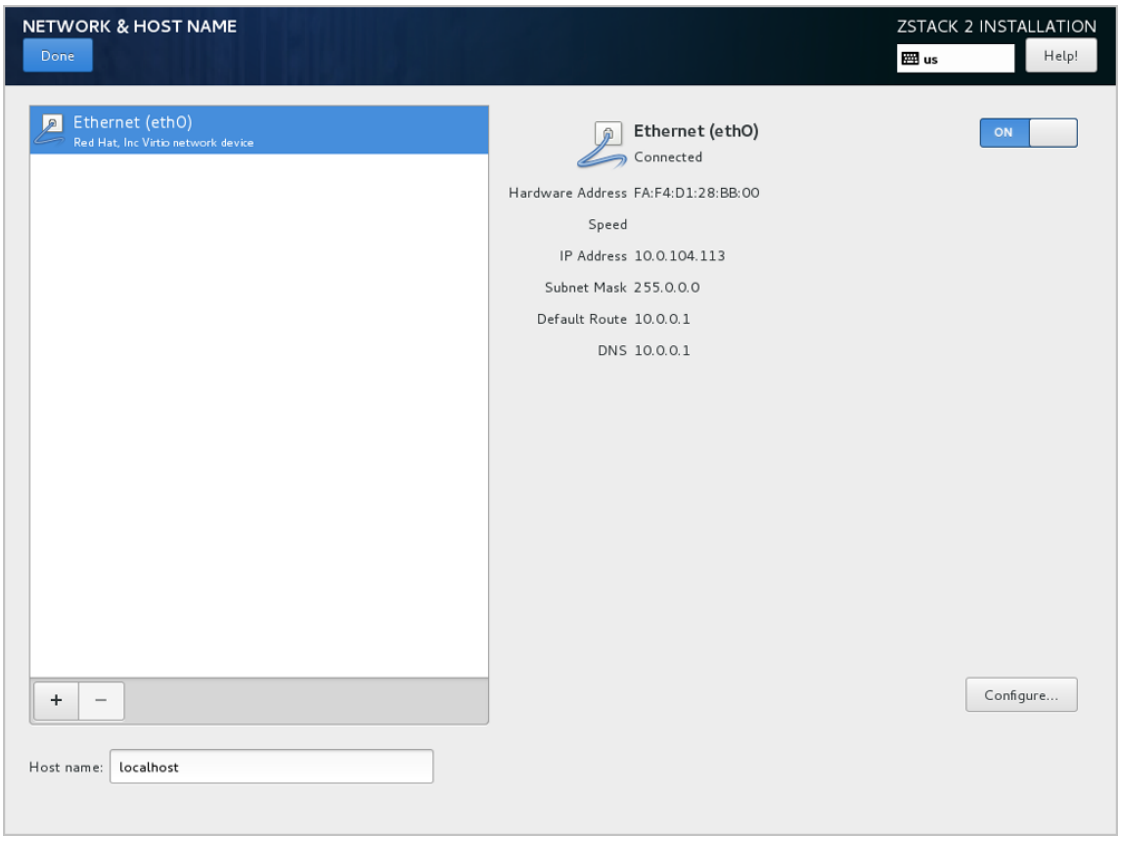
f) 配置网络。

1. 配置网卡。

   在系统安装界面，点击**NETWORK & HOST NAME**进入网卡配置主界面，如图 *11: 网卡配置主界面*所示。

   1. 选中待配置网卡：如**eth0**
   2. 开启网卡：选择**On**
   3. 查看获取的DHCP地址

图 11: 网卡配置主界面



2. 网卡归一化(可选)。

   如果在实际生产环境中安装部署ZStack，建议进行网卡归一化配置，网卡归一化可进一步提高网络带宽以及网络可靠性。详细配置步骤请参考网卡归一化(可选)章节。

   如果仅POC测试可选择跳过网卡归一化配置，直接进行以下步骤即可。

3. 如果**eth0**无法获取DHCP地址，需手动配置**eth0**的静态地址。

   a. 在图 *11:* 网卡配置主界面，选中**Ethernet**（eth0），点击**Configure...**，打开**eth0**配置界面，如图 *12:* 配置*eth0*静态*IP*所示。

   b. 进入**eth0**的**IPv4 Settings**选项页。

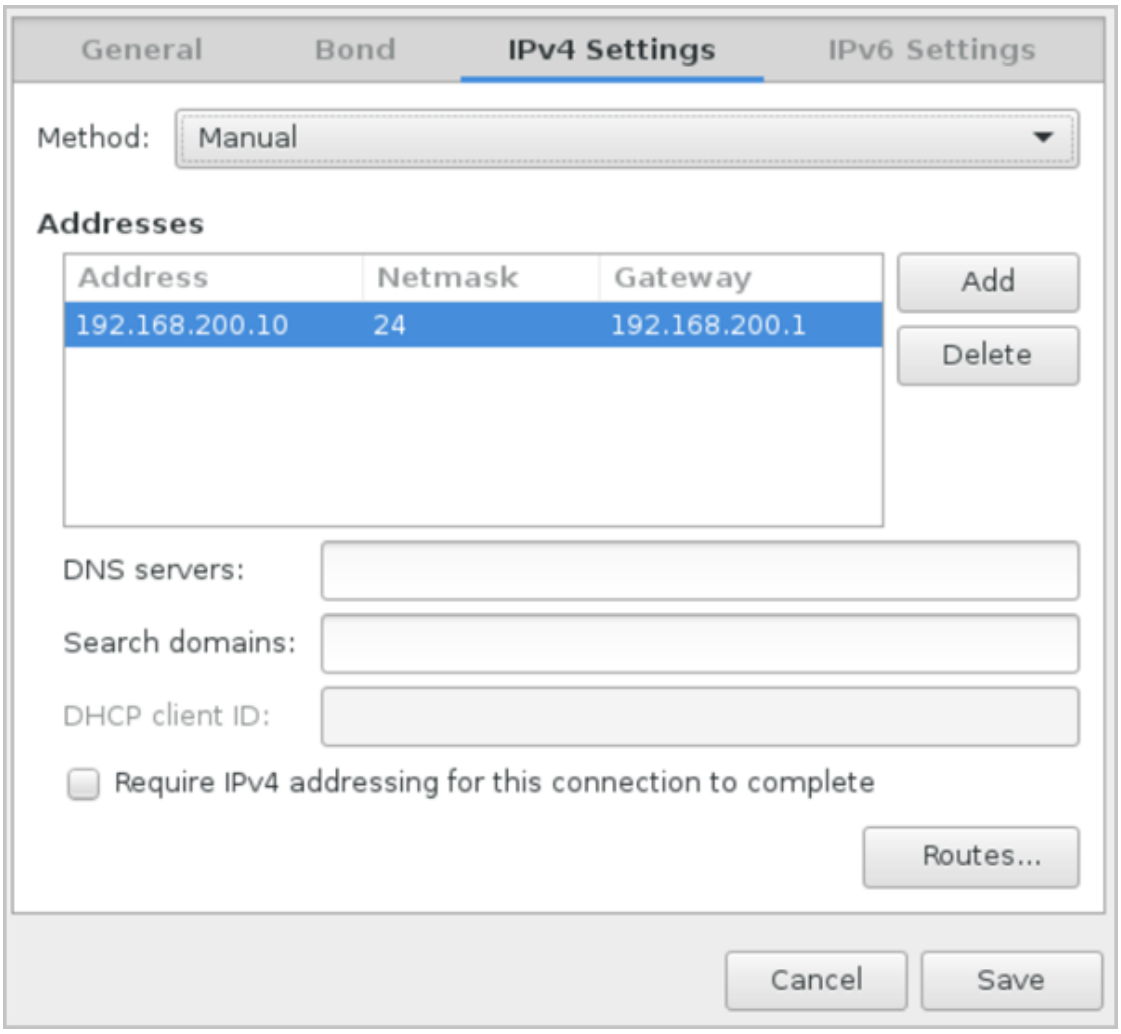
   c. 在**Method**列表选择**Manual**以进行手动配置。

   d. 点击**Add**增加新的配置条目。

   e. 根据实际情况配置网卡地址信息。

   f. 点击**Save**保存。

图 12: 配置eth0静态IP



4. 设置eth0自动连接。

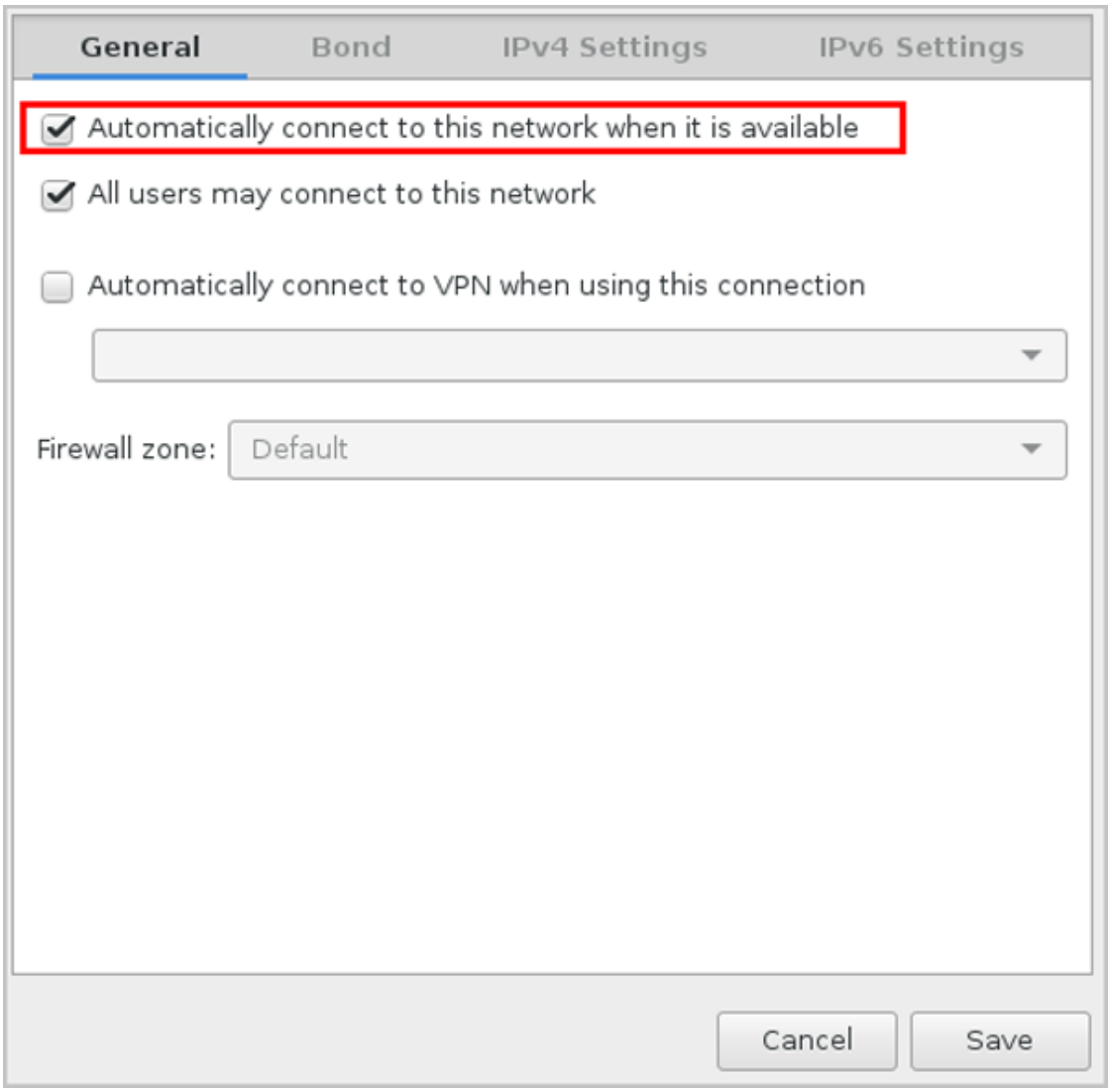
   a. 在图 *11:* 网卡配置主界面，选中**Ethernet**（eth0），点击**Configure...**，打开**eth0**配置界面，如图 *13:* 设置*eth0*自动连接所示。

   b. 进入**General**选项页。

   c. 确认已勾选**Automatically connect to this network when it is available**

   d. 点击**Save**保存。

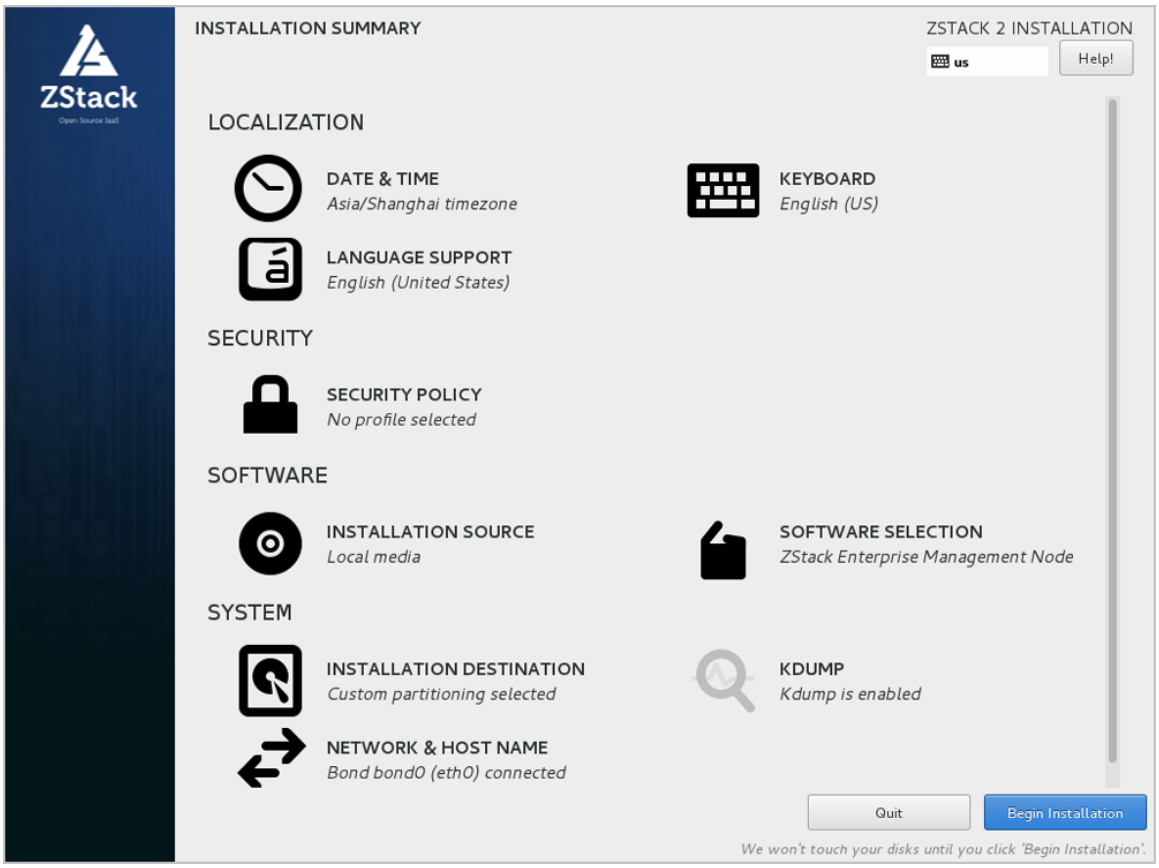
图 13: 设置eth0自动连接



g) 网络配置完后，回到系统安装主界面，点击**Begin Installation**开始安装。

如图 *14: 点击Begin Installation*所示：

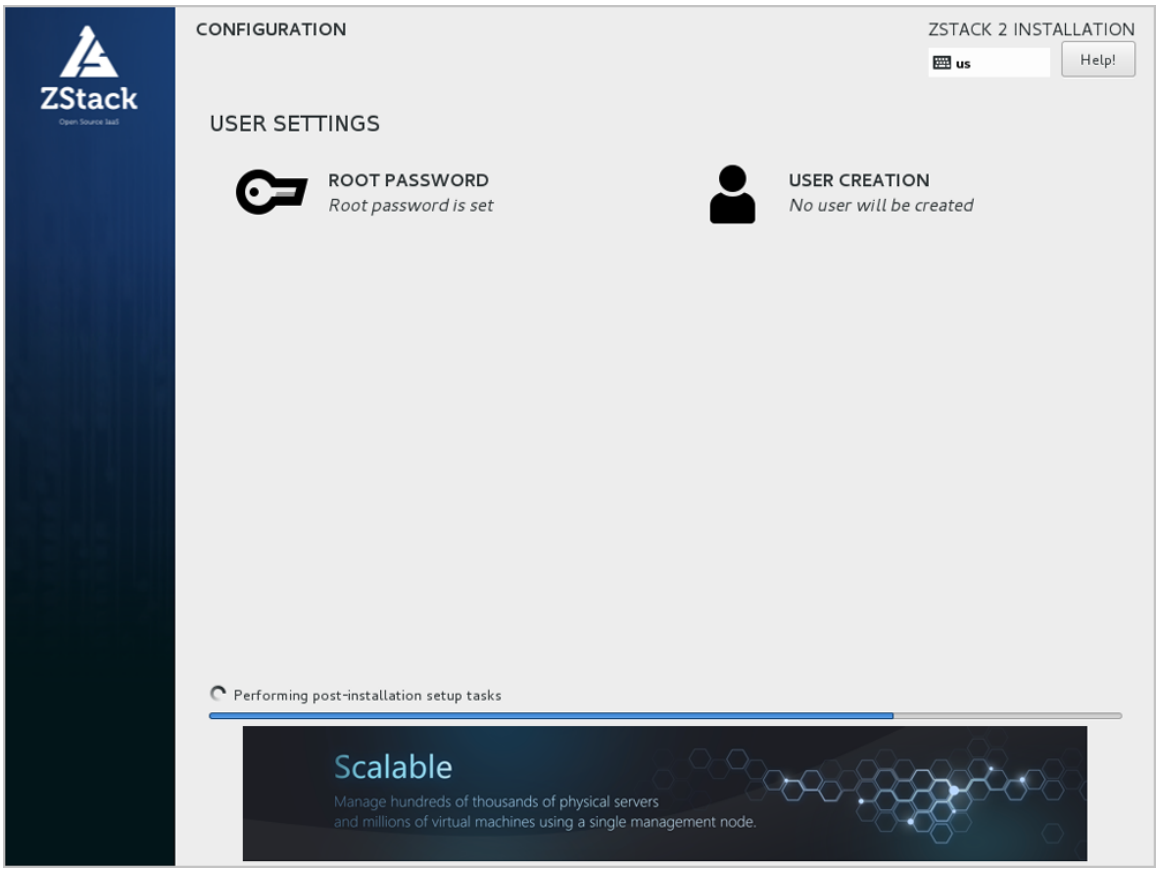
图 14: 点击Begin Installation



h) 安装过程自动进行，安装过程中请设置**ROOT PASSWORD**。

如图 *15:* 系统安装过程界面所示：

图 15: 系统安装过程界面



i) 安装完毕后，点击**重启**，即可启动进入ZStack定制版CentOS 7.x系统。

后续操作

- 选择企业版管理节点模式/社区版管理节点模式/计算节点模式，系统重启后会自动安装对应的ZStack安装包。
- 选择专家模式，系统重启后进入shell界面，由高级用户自定义安装。

4.1.1 网卡归一化(可选)

本章节主要介绍网卡归一化配置方法。如果在实际生产环境中安装部署ZStack，建议采用网卡归一化方式配置网络；如果仅POC测试可选择跳过本章节。

以下介绍网卡归一化的两种配置方式：命令行方式和图形界面方式。

命令行方式

管理员可在ZStack安装完成后，按照具体部署场景需求，参考以下命令快速实现网卡归一化：

```
# 修改网卡名
zs-change-nic -c [old-nic-name] [new-nic-name]
zs-change-nic -c eth0 em1
```

```
# 创建链路聚合虚拟接口，基于LACP模式
zs-bond-lacp -c [bond-name]
zs-bond-lacp -c bond0

# 创建链路聚合虚拟接口，基于主备模式
zs-bond-ab -c [bond-name]
zs-bond-ab -c bond0

# 加载物理接口到聚合接口
zs-nic-to-bond -a [bond-name] [nic-name]
zs-nic-to-bond -a bond0 em1

# 创建VLAN接口
zs-vlan -c [nic-name] [vlan]
zs-vlan -c bond0 10

# 创建网桥并配置网络地址
zs-network-setting -b [interface] [ipaddress] [netmask] [gateway]
zs-network-setting -b bond0.10 192.168.1.10 255.255.255.0 192.168.1.1
```

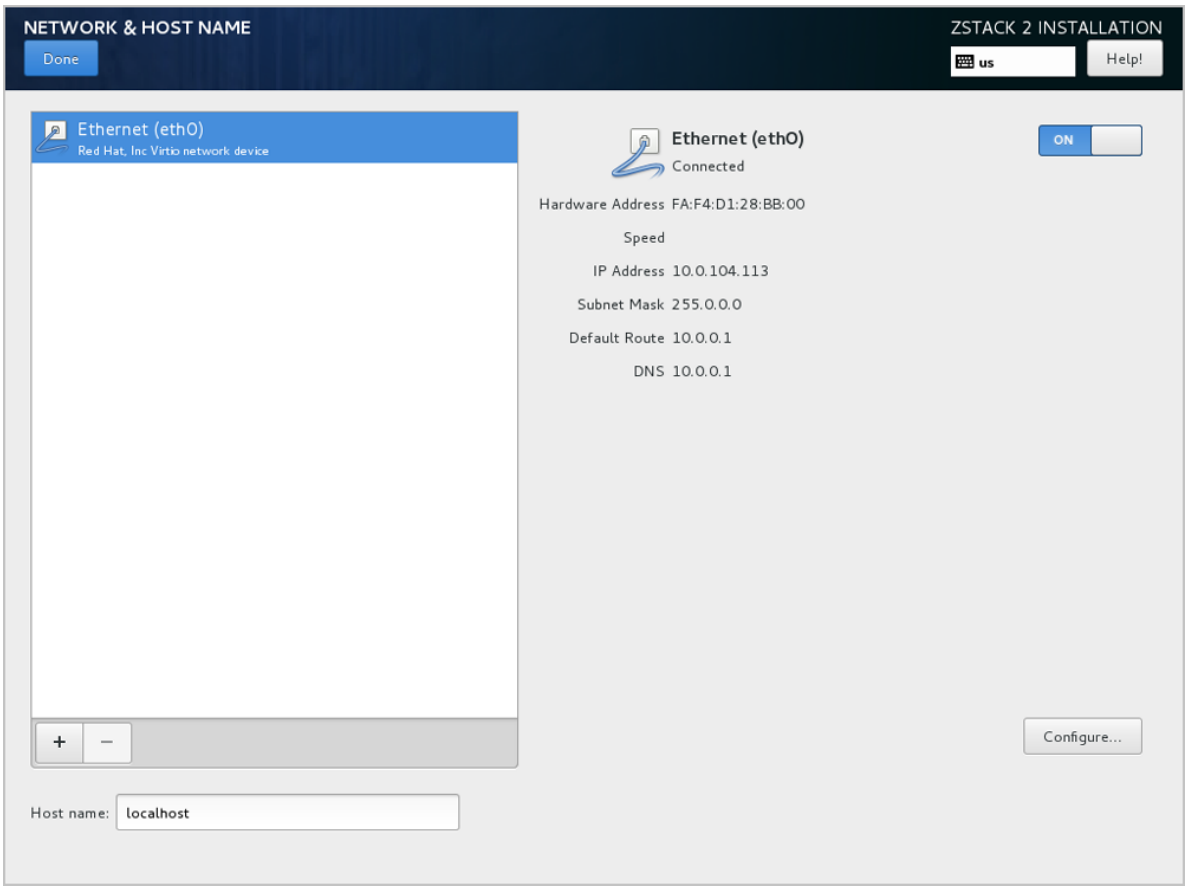
图形界面方式

1. 配置网卡。

   在系统安装界面，点击**NETWORK & HOST NAME**进入网卡配置主界面，如图 *16:* 网卡配置主界面所示。

   1. 选中待配置网卡：如**eth0**
   2. 开启网卡：选择**On**
   3. 查看获取的DHCP地址

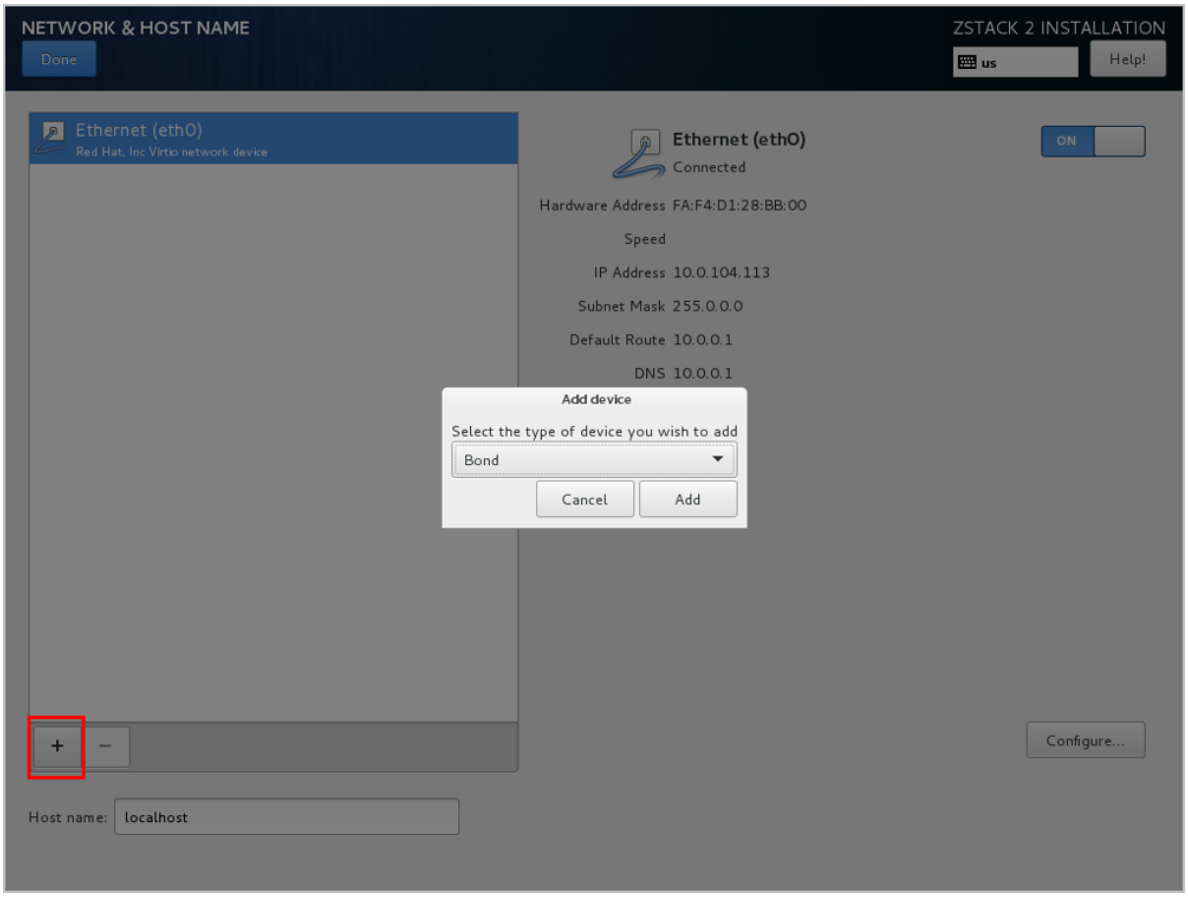
   图 16: 网卡配置主界面



2. 添加一个Bond设备。

   点击左下角的**"+"**号，弹出**Add device**界面，在下拉菜单中选择**Bond**，点击**Add**，如图 *17: 添加一个Bond设备*所示：

   图 17: 添加一个Bond设备



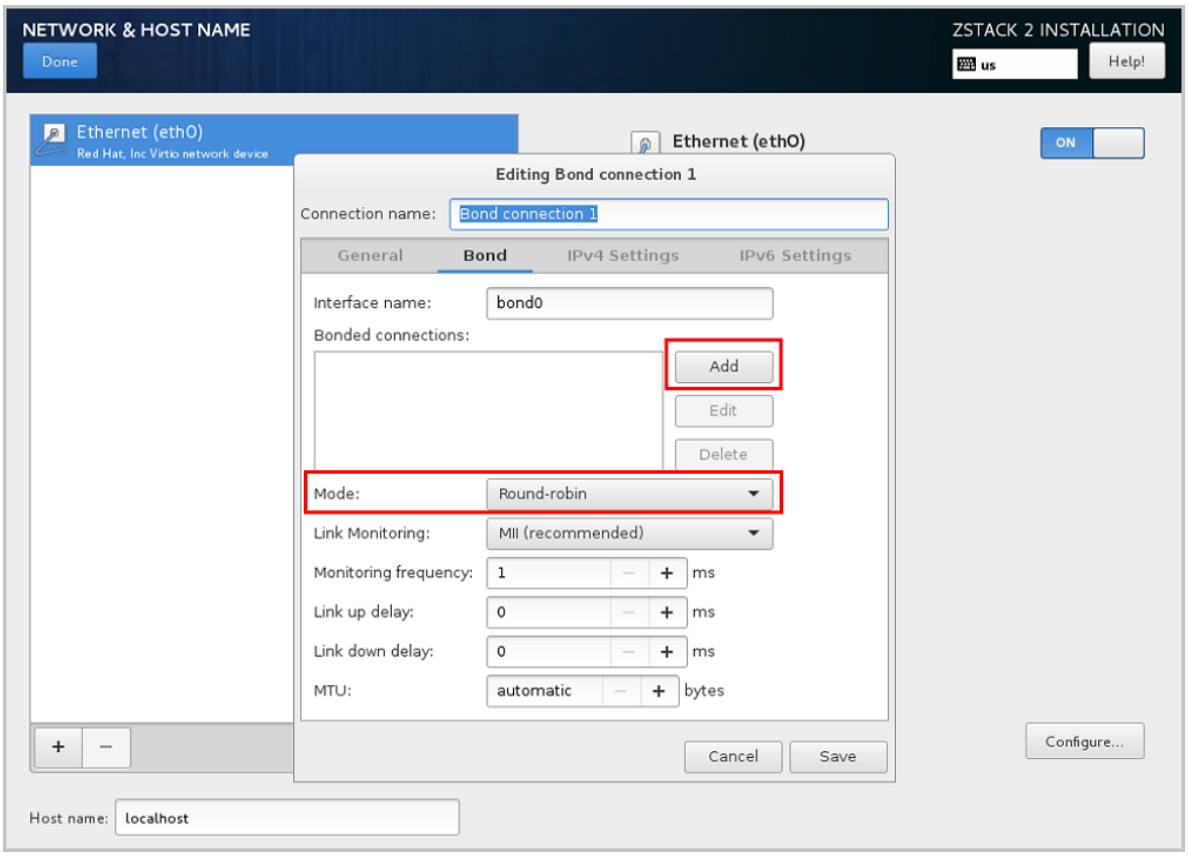
3. 配置Bond。

   弹出**Editing Bond connection 1**界面的**Bond**子页面，如图 *18:* 配置*Bond*所示，用户需手动配置的主要有两项：

   - **Add**：添加Bond Slave，详见添加*Bond Slave*。
   - **Mode**：选择Bond模式，详见选择*Bond*模式。

   其它可选择默认或按需自定义设置。

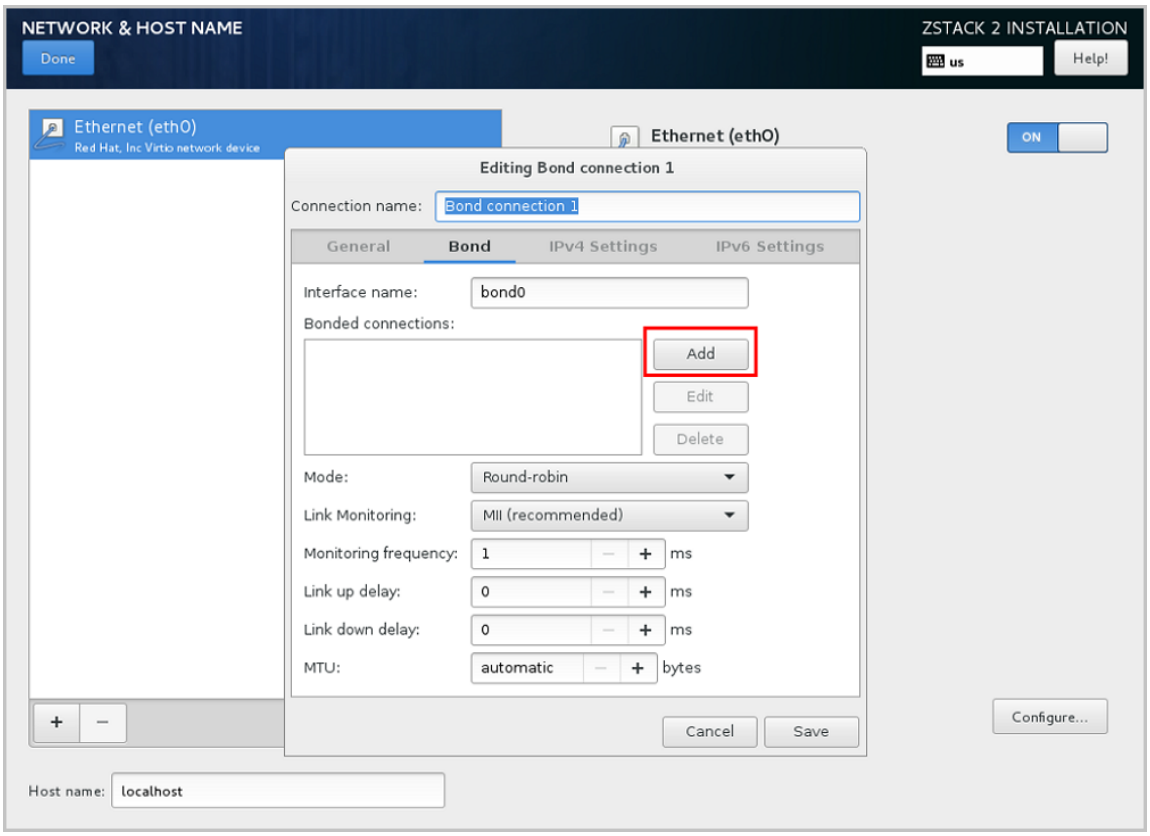
   图 18: 配置Bond



4. 添加Bond Slave。

   - 在Bond配置界面，点击**Add**，添加Bond Slave，如图 *19: 添加Bond Slave*所示：

   图 19: 添加Bond Slave

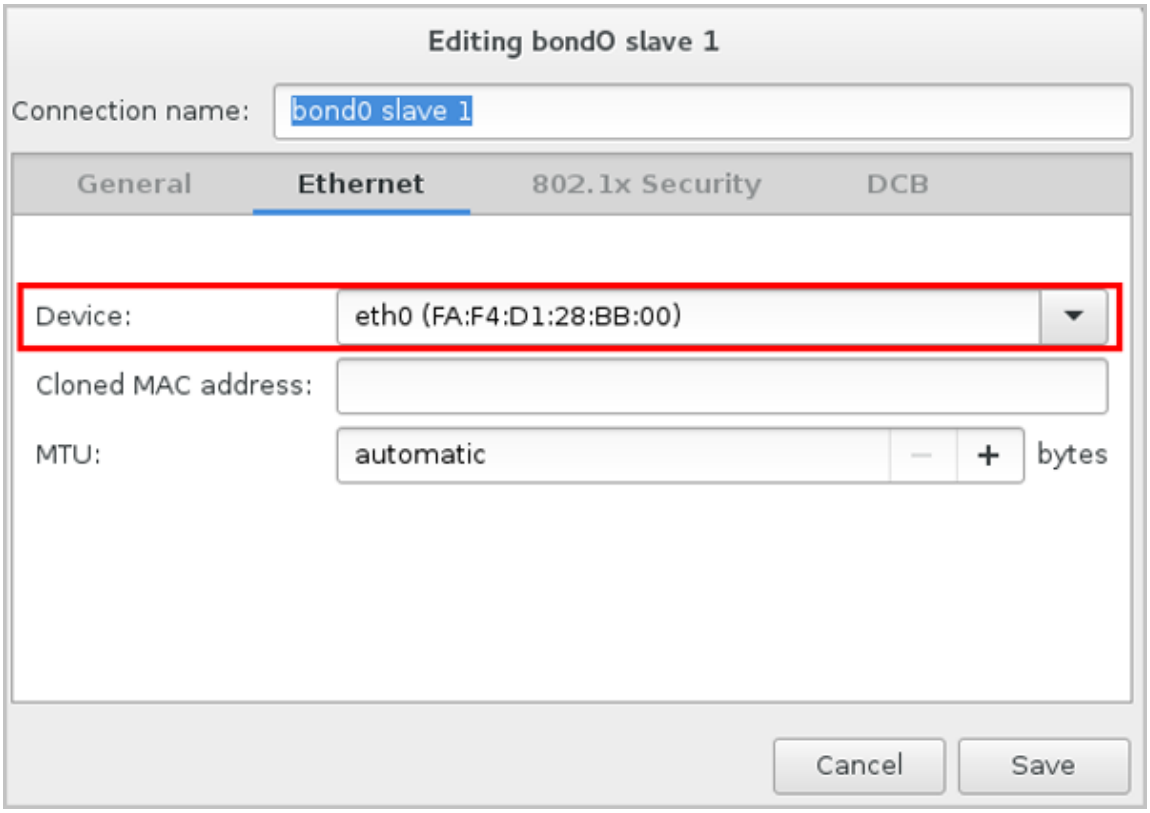


- 弹出**Chooes a Connection Type**界面，在下拉菜单中选择Bond Slave连接类型，如**Ethernet**，点击**Create...**，如图 *20: 选择Bond Slave连接类型*所示：

图 20: 选择Bond Slave连接类型

- 弹出**Editing bond0 slave1**界面的**Ethernet**子页面，在**Device**下拉菜单中选择需要Bond的Slave设备，如eth0（**相应MAC地址**），其它选择默认或按需自定义设置，点击**Save**，如图 *21: 选择Bond Slave设备*所示：

图 21: 选择Bond Slave设备

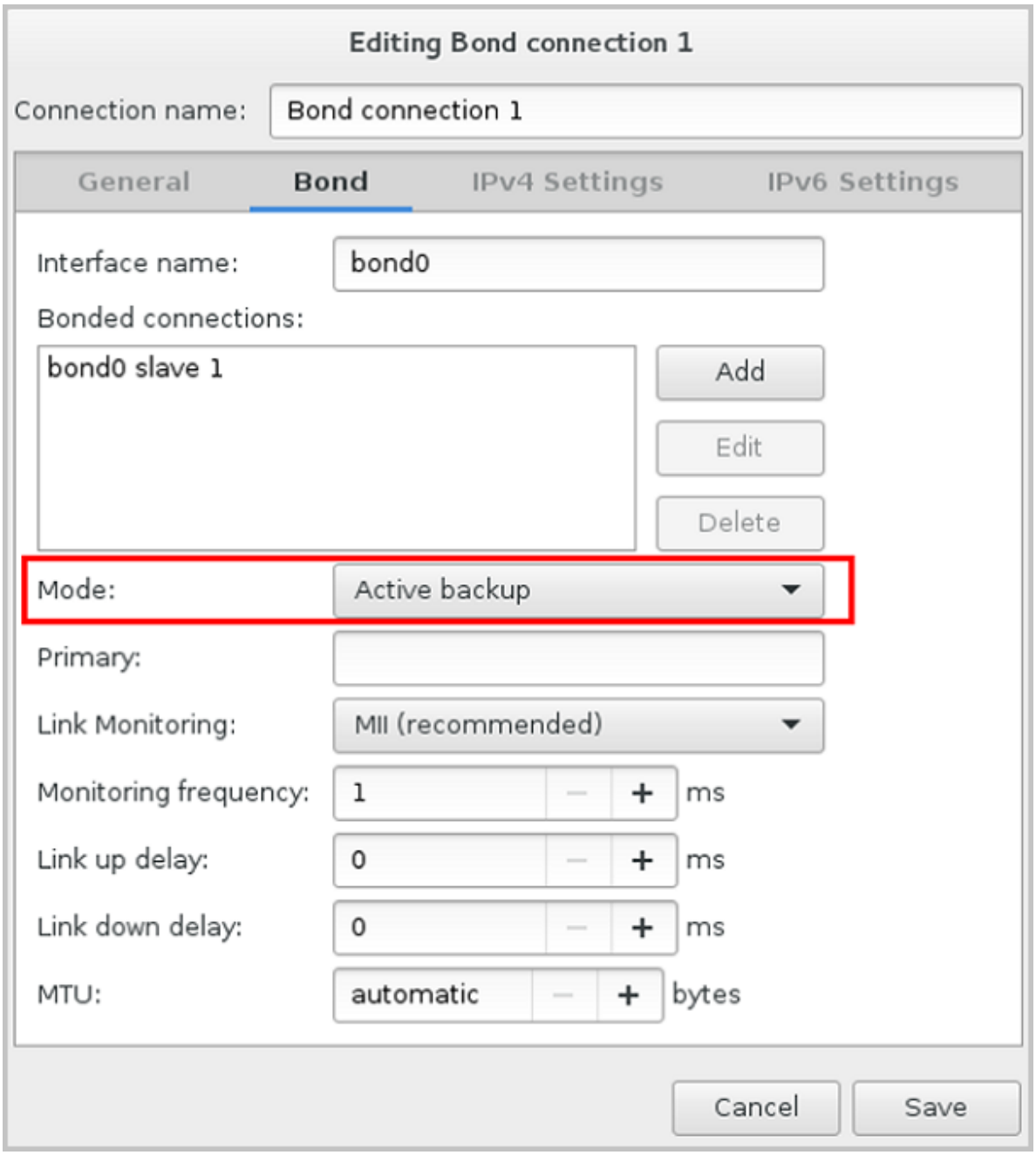


- 至此，Bond Slave已成功添加。

5. 选择Bond模式。

在Bond配置界面，**Mode**下拉菜单中，按需选择Bond模式，如**Active backup**（主备模式），其它选择默认或按需自定义设置，点击**Save**，如图 *22: 选择Bond模式*所示：

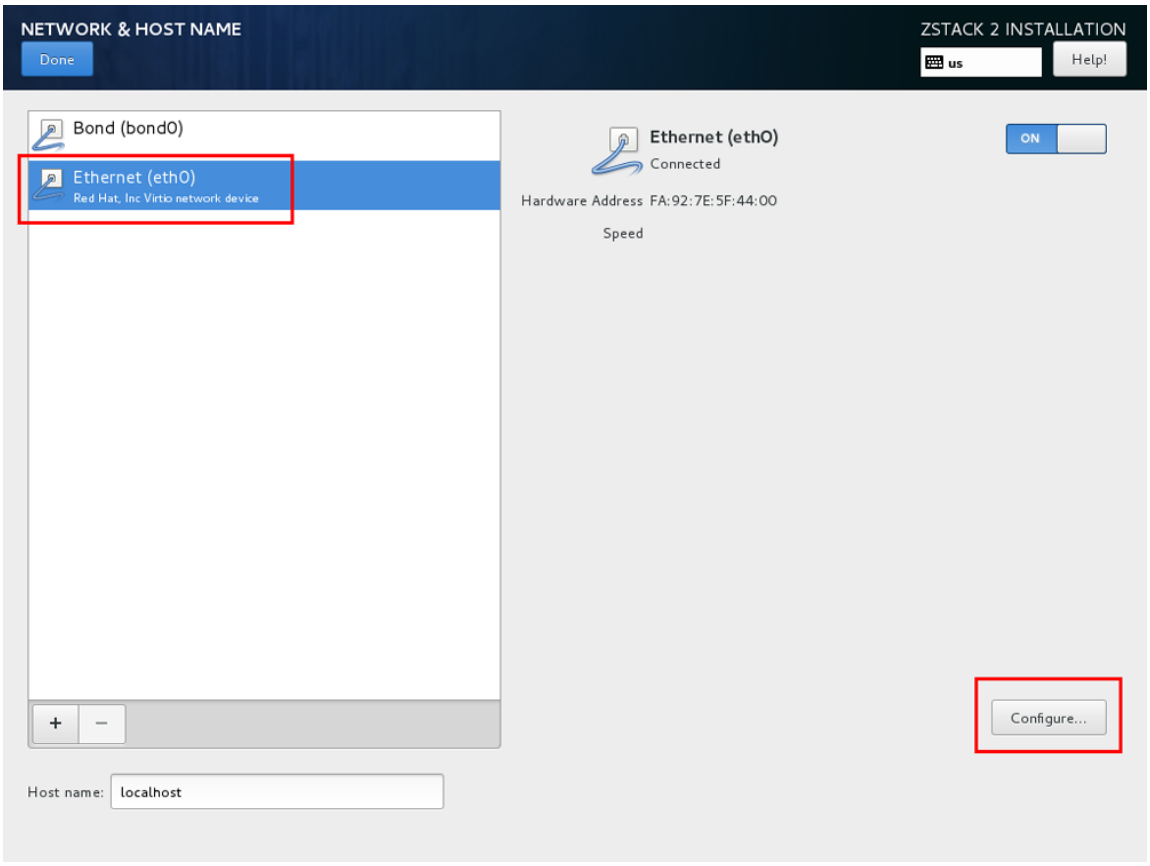
图 22: 选择Bond模式



6. Bond Slave的IPv4设置为禁用。

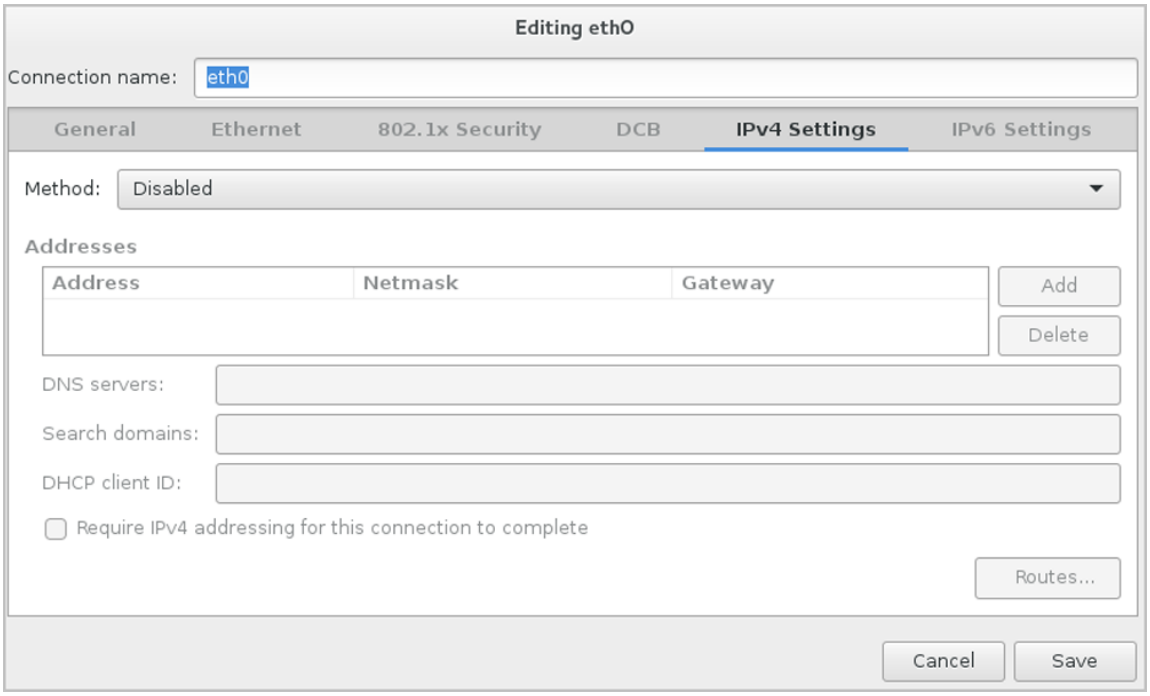
   - 回到网卡配置主界面，选中Bond Slave（如eth0），点击**Configure...**，如图 *23: 打开Bond Slave配置界面*所示：

     图 23: 打开Bond Slave配置界面



- 进入**Editing eth0**界面的**IPv4 Settings**子页面，**Method**下拉菜单中，选择**Disabled**，点击**Save**，如图 *24: Bond Slave的IPv4设置为禁用*所示：

图 24: Bond Slave的IPv4设置为禁用



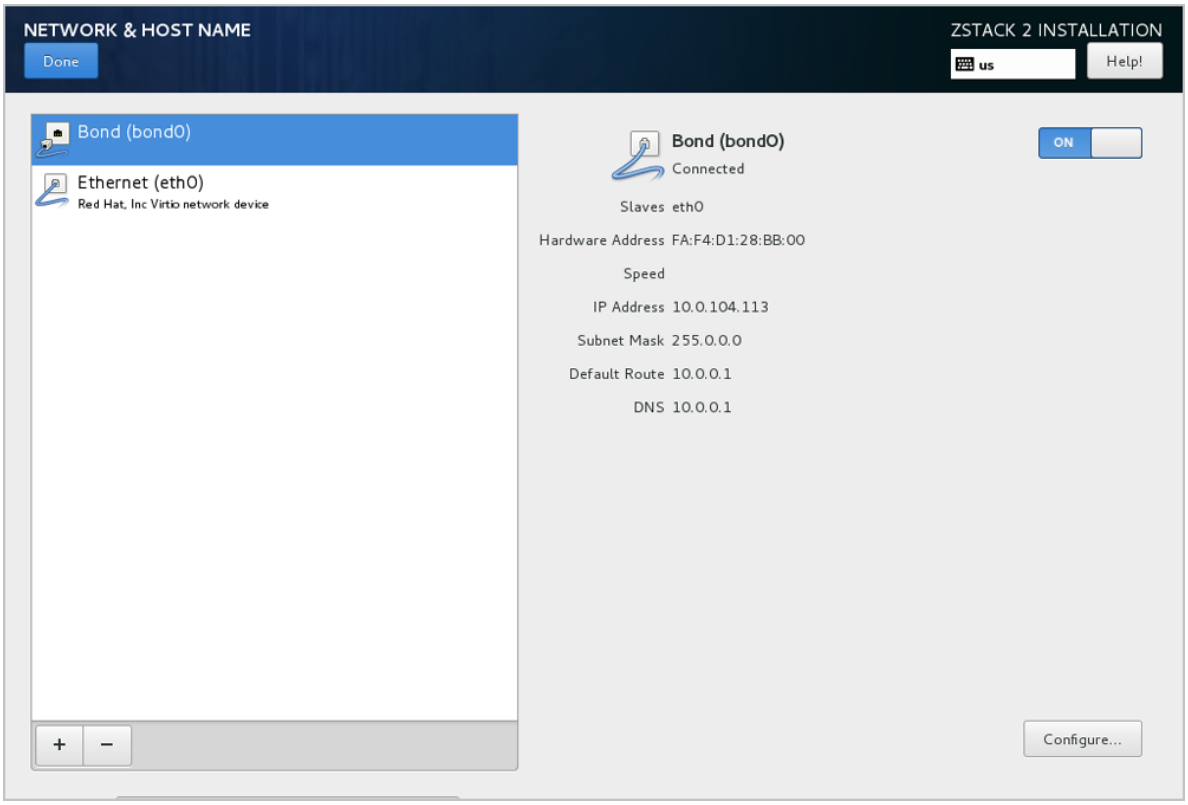
7. 网卡归一化完成。

   如图 *25: 网卡归一化完成*所示：

   注:

   请检查Bond配置项，必须保证**On**开启且配置了地址，同时Bond Slave（如eth0）也**On**开启，否则ZStack无法正常安装。

   图 25: 网卡归一化完成



8. 如果Bond无法获取DHCP地址，需手动配置Bond的静态地址。

   a. 在图 *16: 网卡配置主界面*，选中**Bond**（bond0），点击**Configure...**，打开Bond配置界面，如图 *26: 配置Bond静态IP*所示。

   b. 进入Bond的**IPv4 Settings**选项页。

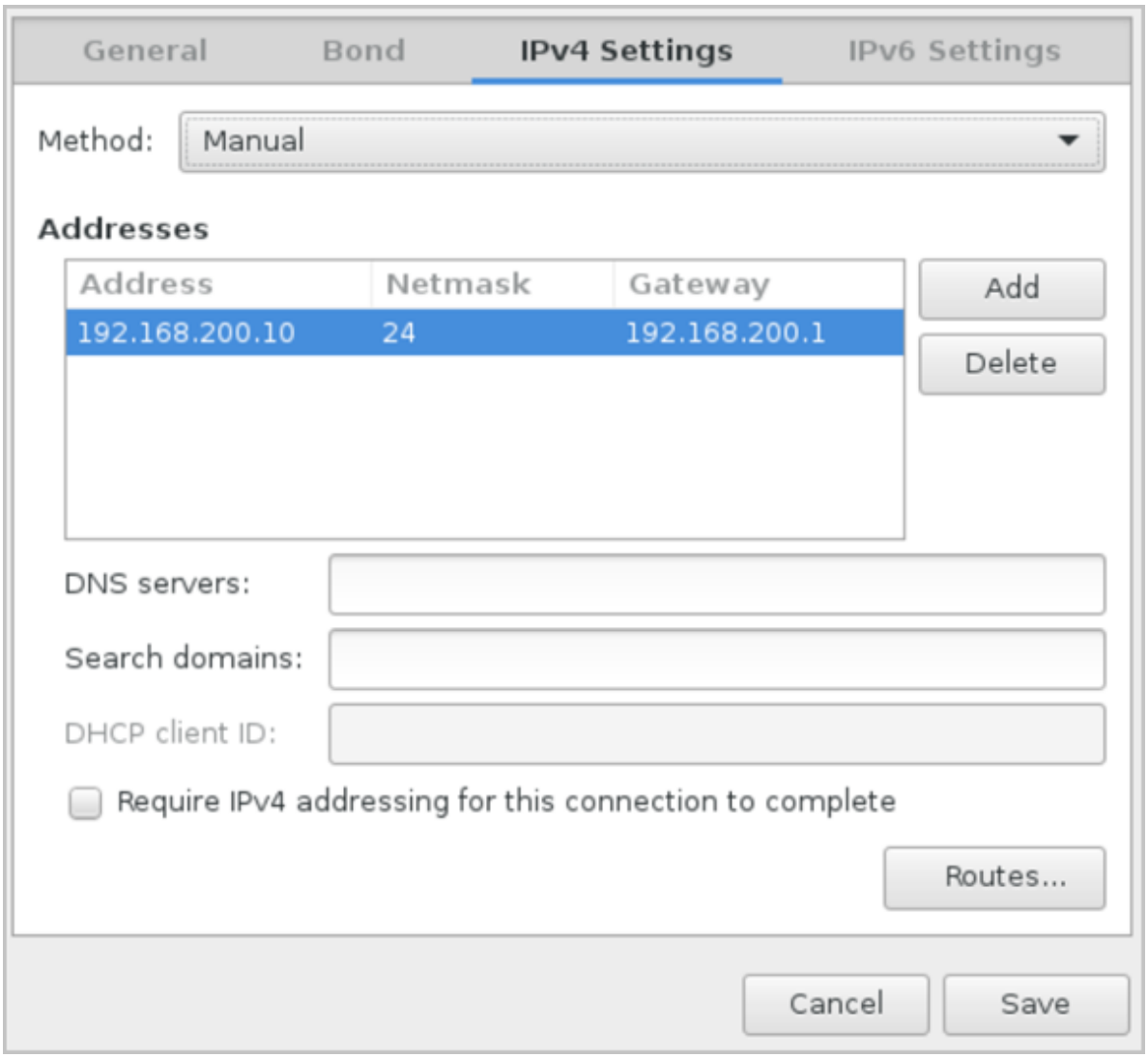
   c. 在**Method**列表选择**Manual**以进行手动配置。

   d. 点击**Add**增加新的配置条目。

   e. 根据实际情况配置网卡地址信息。

   f. 点击**Save**保存。

   图 26: 配置Bond静态IP



9. 设置Bond自动连接。

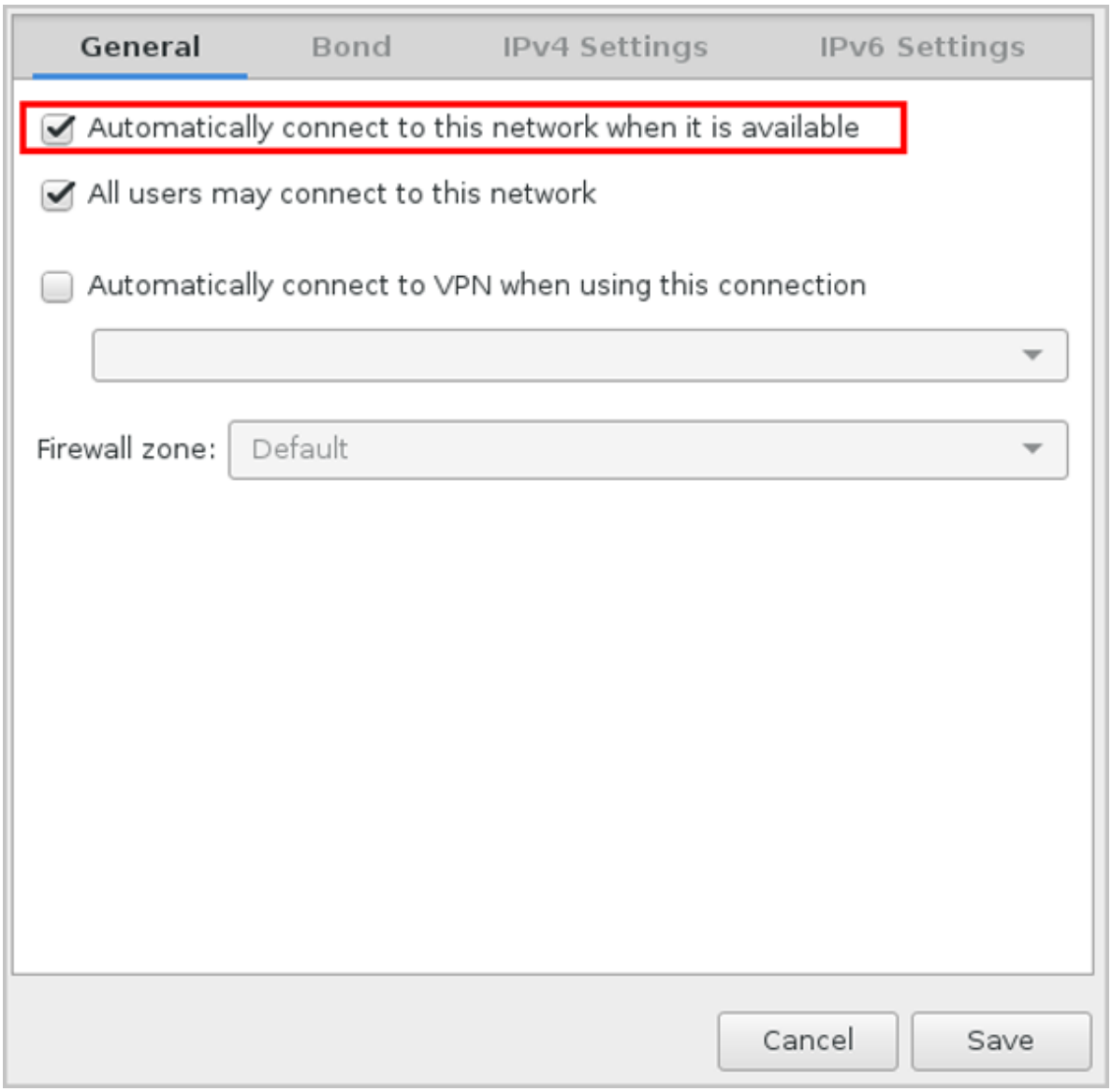
   a. 在图 *16:* 网卡配置主界面，选中**Bond**（bond0），点击**Configure...**，打开Bond配置界面，如图 *27:* 设置*Bond*自动连接所示。

   b. 进入**General**选项页。

   c. 确认已勾选**Automatically connect to this network when it is available**

   d. 点击**Save**保存。

图 27: 设置Bond自动连接



10.至此，基于网卡归一化配置网络的方法介绍完毕。

4.2 安装ZStack

本节主要介绍ZStack企业版 2.5.1的四种安装模式以及TUI的功能介绍。

ZStack TUI简介

ZStack TUI是专为ZStack 集群中物理服务器准备的一套用户界面，其意义包含两方面：

- **分流UI的部分功能**

  将针对服务器的配置密码、配置网络、重启机器等操作从UI中剥离出来，集中显示在TUI中。

- **降低管理员登录服务器的频率**

  这是为了在降低物理机维护难度的同时，保护物理机内部的配置不被损坏。

用户可以使用**Ctrl + Alt + F2**进入命令行模式；使用**Ctrl + Alt + F1**退出命令行模式。按下**Ctrl + Alt + F11**可以进入保留终端，用户可以在里面执行常规命令 ，但是请谨慎使用，以免对系统造成破坏，影响ZStack 服务运行。

ZStack定制版ISO四种安装模式

ZStack定制版ISO提供了以下四种安装模式：

- 企业版管理节点模式
- 社区版管理节点模式
- 计算节点模式
- 专家模式

四种安装模式的步骤介绍：

1. **企业版管理节点模式**
   - 安装基础系统
   - 安装MariaDB、RabbitMQ等ZStack依赖包
   - 安装企业版管理节点TUI
   - 自动安装并启动ZStack及其UI
2. **社区版管理节点模式**
   - 安装基础系统
   - 安装MariaDB、RabbitMQ等ZStack依赖包
   - 安装社区版管理节点TUI
   - 自动安装并启动ZStack及其UI

   注:
   - 企业版管理节点模式与社区版管理节点模式的区别在于**License的不同导致相关功能的不同。**
   - 企业版管理节点模式与社区版管理节点模式在安装步骤上完全相同。
3. **计算节点模式**
   - 安装基础系统
   - 安装Libvirt、Qemu等虚拟化组件
   - 安装计算节点TUI
4. **专家模式**

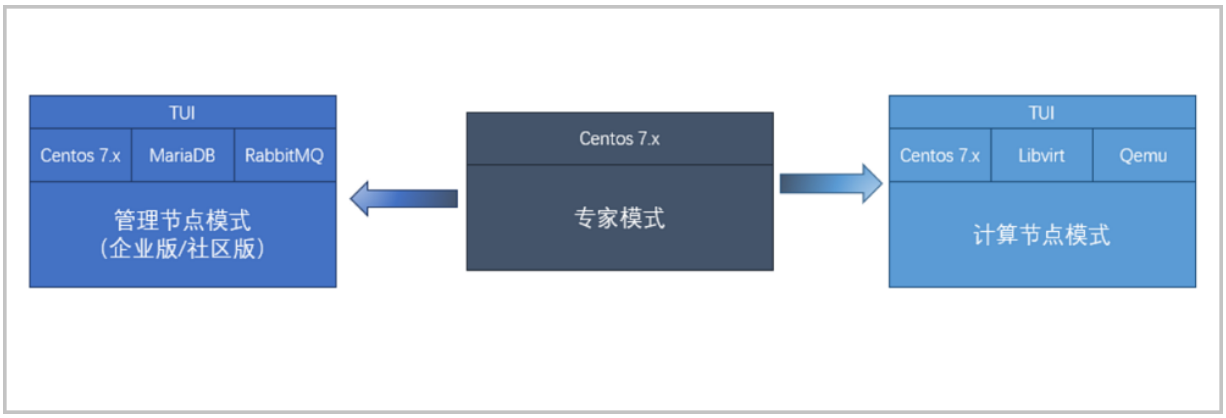
- 安装基础系统

注:

- 专家模式基本等同于CentOS 7.x最小安装模式。
- 当管理员需要做更深度的定制时，可以选择进入专家模式，手动转化为其它三种模式中的任何一种。

四种安装模式如图 *28:* 四种安装模式示意图所示：

图 28: 四种安装模式示意图



4.2.1 ZStack管理节点模式(企业版/社区版)

如前所述：

- 企业版管理节点模式与社区版管理节点模式的区别在于**License的不同导致相关功能的不同。**
- 企业版管理节点模式与社区版管理节点模式在安装步骤上完全相同。

下面将企业版/社区版管理节点模式合为一篇，以管理节点TUI为主介绍其功能和使用方法。

自动安装ZStack管理节点

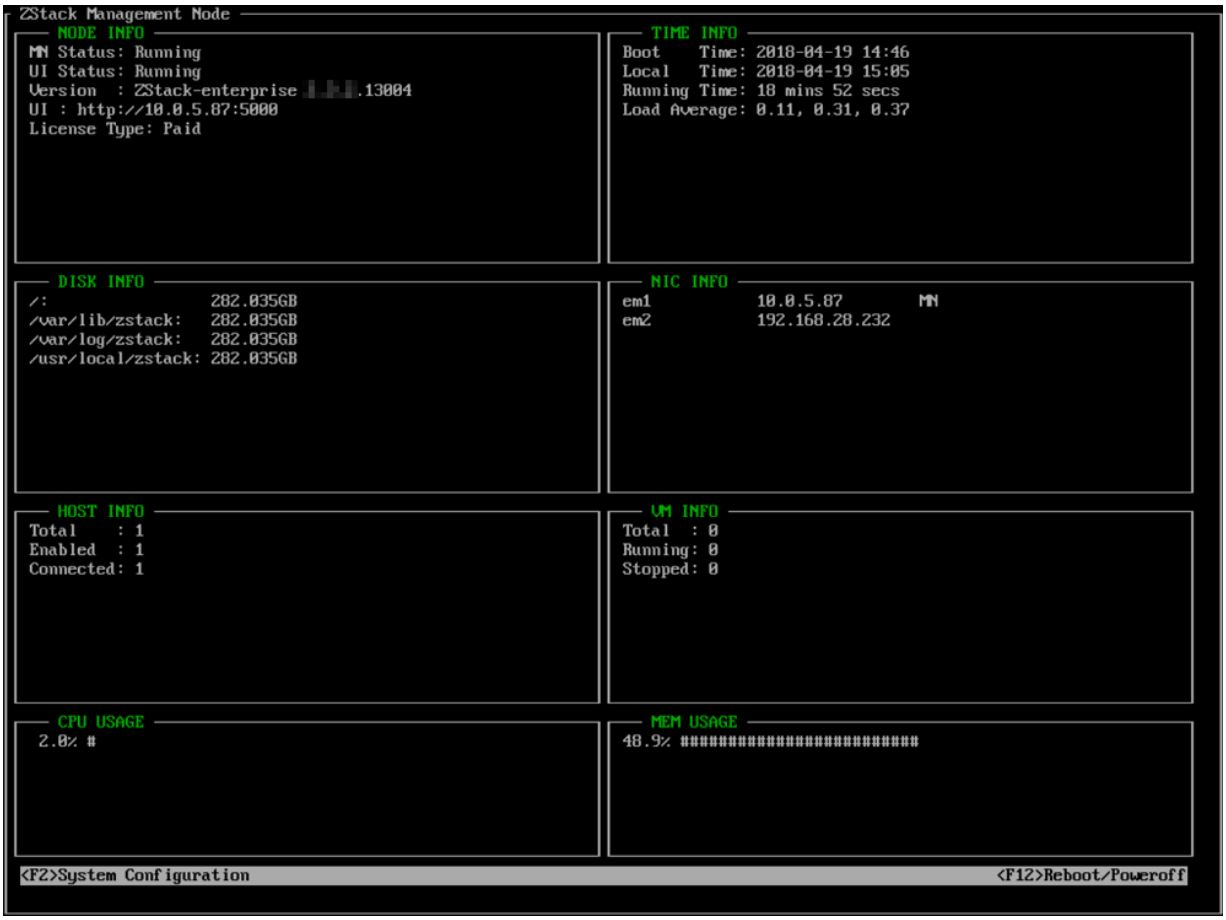
如果选择企业版/社区版管理节点模式，重启后会自动安装ZStack管理节点，安装完成后将自动进入TUI，如图 *29:* 自动安装管理节点所示：

图 29: 自动安装管理节点

管理节点TUI主界面

管理节点TUI主界面实时显示物理机的主要信息，如图 *30:* 管理节点*TUI*主界面所示:

图 30: 管理节点TUI主界面



- **NODE INFO**：

  显示管理节点当前状态，包括服务是否运行、UI是否运行、ZStack版本、UI地址以及License类型等

- **TIME INFO**：

  显示服务器启动时间、当前时间、服务器运行时长、服务器平均负载等

- **DISK INFO**：

  显示默认安装目录以及日志目录等的剩余磁盘空间

- **NIC INFO**：

  显示管理节点所有网卡的信息，包括物理网卡和逻辑网卡，其中DOWN表示网卡关闭、UP表示网卡启动、MN表示该网卡为管理网卡

- **HOST INFO**：

  显示当前集群共有多少台计算节点，其中**Enabled**和**Connected**的各有多少；

- **VM INFO**：

  显示当前集群共有多少台云主机，其中**Running**和**Stopped**的各有多少；

- **CPU USAGE和MEM USAGE**：

  分别显示该管理节点的实时资源利用率。

注:

主界面底部还提供了进入**系统配置**和**重启/关机**两个入口，根据提示按下**F2**或者**F12**即可进入相应窗口。

系统密码

在主界面按下**F2**或者**F12**时，需要首先输入系统密码，因为无论**系统配置**还是**重启/关机**都属于特权操作。

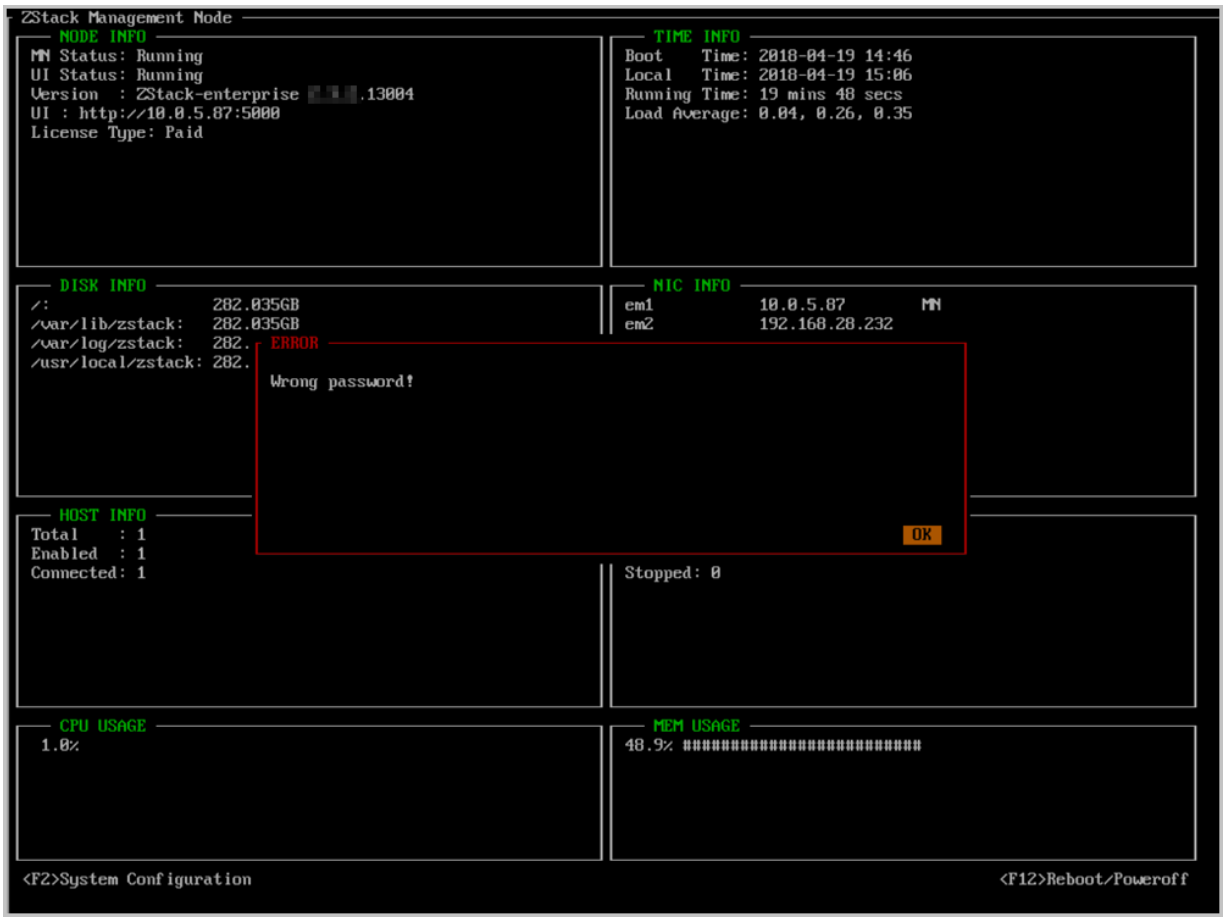
下图中显示了输入系统密码的窗口，**根据提示输入ROOT密码**，**回车即可**。

图 31: 输入密码

若密码不正确，操作会被阻止，TUI返回主界面。

注: 任何时候，只要按下ESC键，就可以退出当前窗口，返回系统配置界面。

图 32: 输入密码错误



系统配置

系统配置的功能包括：

- 修改密码
- 重命名网卡
- 测试网络
- 配置网络
- 配置管理网络
- 配置控制台代理
- 收集日志
- 备份数据库
- 启动/关闭/重启ZStack服务

- 重装ZStack服务
- 重装ZStack服务并删除数据库
- 终端信息

注:

- 系统配置界面提供若干系统配置入口。**使用上下键移动光标**，**选择需要的配置按钮**，**按下回车即可进入相应配置界面**。对于熟悉Vim的用户，也可以使用**j**和**k**实现光标上下移动。
- 根据提示，按下**F2**可以退出至主界面。再次回到系统配置界面时需要重新输入ROOT密码。

如图 *33:* 系统配置所示：

图 33: 系统配置

以下将逐一介绍系统配置各功能条目。

1. 修改密码

将光标移动至**Change Passwords**处，按下回车，即可进入密码配置窗口。

该配置项集中了管理节点需要的四种密码修改动作：

1. 修改系统root密码
2. 修改root账号的MySQL密码
3. 修改ZStack账号的MySQL密码
4. 修改ZStack账号的RabbitMQ密码

如图 *34:* 四种密码修改动作所示：

图 34: 四种密码修改动作

四种密码修改动作具体介绍：

1. 修改系统root密码

   根据提示输入旧系统密码、新系统密码以及新密码确认，回车即可，如图 *35:* 修改系统*root*密码所示：

   图 35: 修改系统root密码

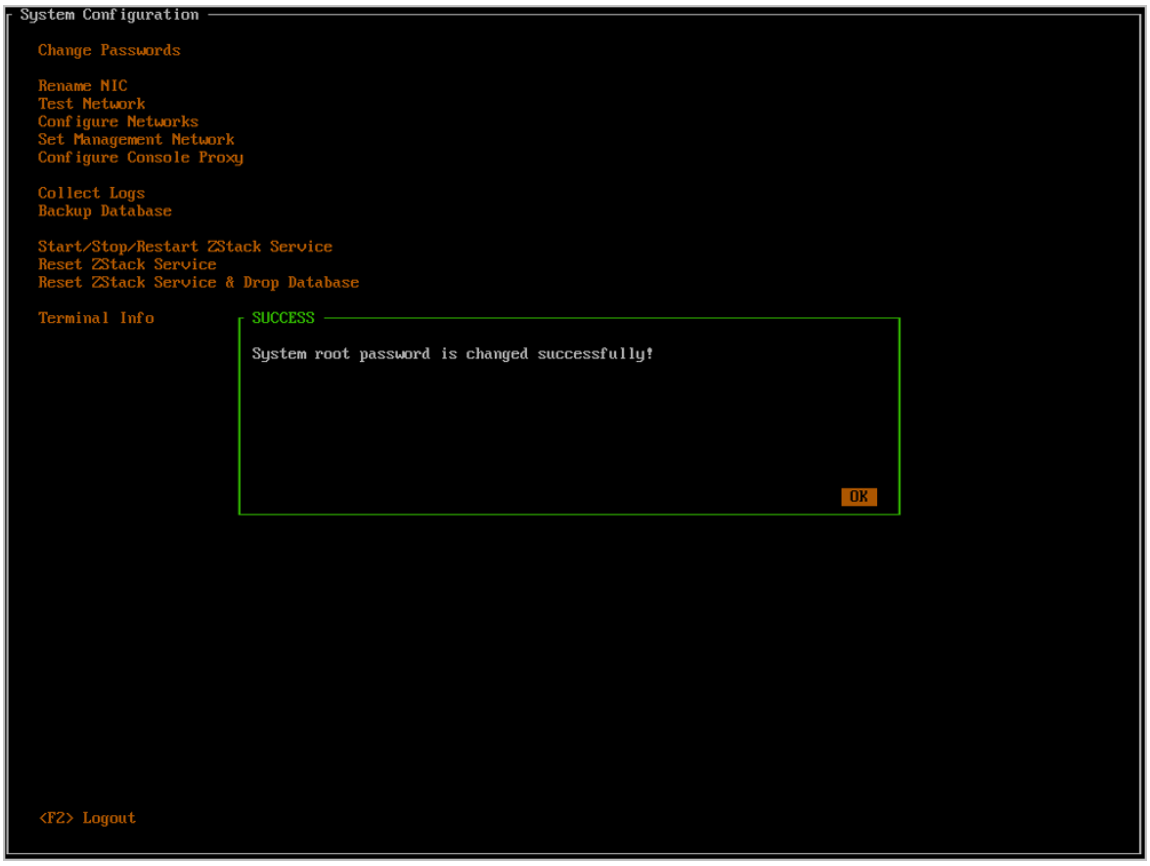
如果旧系统密码不正确、或者密码确认不一致，都会弹出错误窗口，如图 *36: 错误窗口*所示：

图 36: 错误窗口

需要根据提示，按**Y**键以确认，如图 *37: 修改系统root密码的确认界面*所示；修改系统root密码成功，如图 *38: 修改系统root密码成功*所示。

图 37: 修改系统root密码的确认界面

图 38: 修改系统root密码成功



2. 修改root账号/ZStack账号的MySQL密码

   - 修改root账号/ZStack账号的MySQL密码，需要MySQL的root权限，因此**首先需要输入MySQL root密码**，然后根据提示输入新密码和密码确认，回车即可。
   - 如果MySQL root密码不正确、或者密码确认不一致，都会弹出错误窗口。
   - 此操作需要重启ZStack服务，耗时较长，需要用户按**Y**键确认。

   如图 *39: 修改root账号/ZStack账号的MySQL密码*所示：

图 39: 修改root账号/ZStack账号的MySQL密码

3. 修改ZStack账号的RabbitMQ密码

   - 修改ZStack账号的RabbitMQ密码需要管理员权限，因此**首先需要输入系统root密码**，然后根据提示再输入新密码和密码确认，回车即可。
   - 如果系统密码不正确、或者密码确认不一致，都会弹出错误窗口。
   - 此操作需要重启ZStack服务，耗时较长，需要用户按**Y**键确认。

   如图 *40: 修改ZStack账号的RabbitMQ密码*所示：

图 40: 修改ZStack账号的RabbitMQ密码

2. 重命名网卡

   将光标移动至**Rename NIC**处，按下回车，即可进入重命名网卡窗口。

   - 用户可以在此修改网卡名。
   - 修改完成后，按下回车，此操作需要按**Y**键确认。

   如图 *41:* 重命名网卡所示：

   图 41: 重命名网卡

3. 测试网络

   将光标移动至**Test Network**处，按下回车，即可进入网络测试窗口。

   这里默认填写了*114.114.114.114*，用户测试外网连接；若要测试内网连接，请自行填写内网IP。

   如图 *42: 测试网络*所示：

   图 42: 测试网络

4. 配置网络

将光标移动至**Configure Networks**处，按下回车，即可进入网络配置窗口。

如图 *43:* 配置网络所示：

图 43: 配置网络

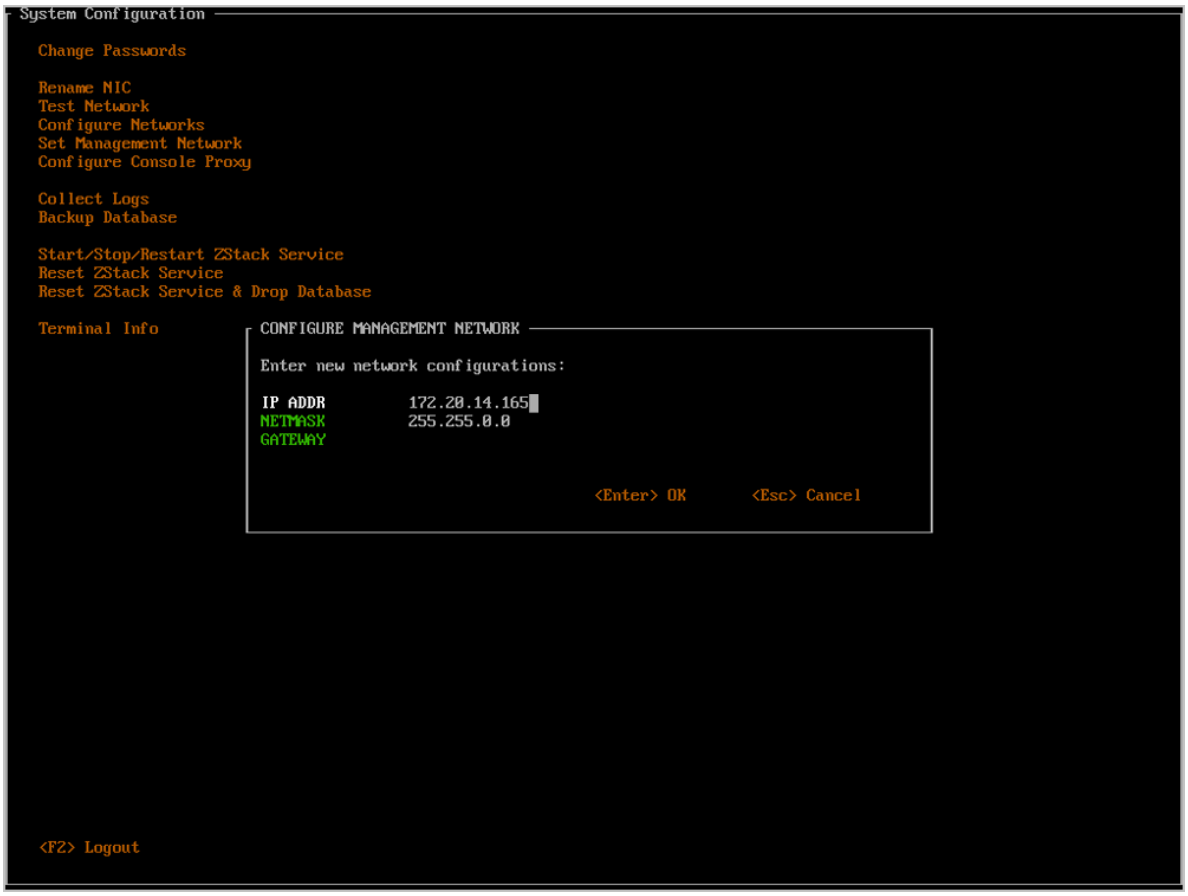
这里罗列了管理节点中所有处于启动状态的网卡，包括物理网卡和逻辑网卡。由于前文已做网卡归一化，这里仅需关心Bond的配置即可。

将光标移动至目标Bond，如bond0，再次回车，即可进入该设备的配置界面。

注: 如果目标Bond后带有（MN）的标记，则意味着修改管理网络配置，需要较长的等待时间，请谨慎操作。

如图 *44:* 填写信息所示：

图 44: 填写信息



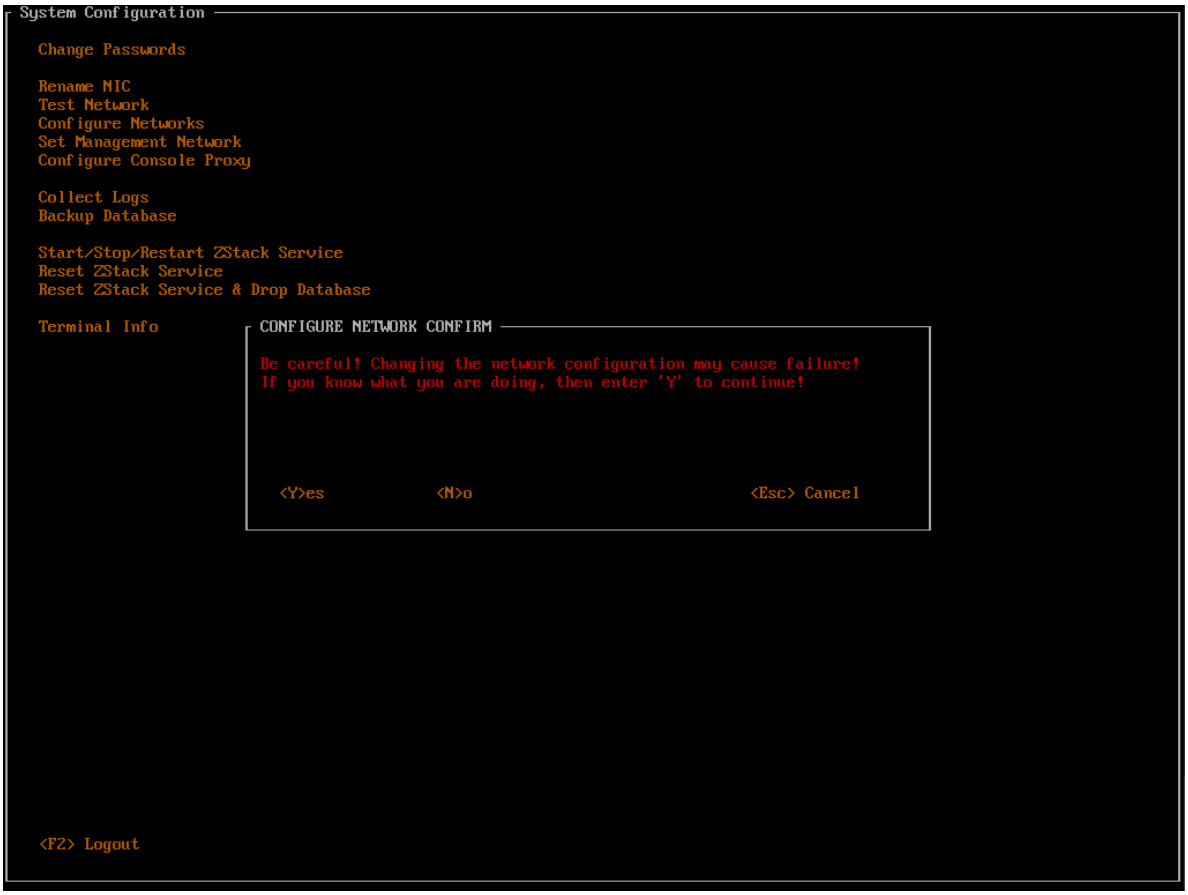
所选Bond设备的已有配置会默认显示在输入框中（网关除外），用户可根据实际情况修改。

如果出现以下任何一种情况，均认为输入有误：

- 有某个或某些输入项为空
- 有某个或某些输入项不是合法的IP地址
- IP地址和网关不在掩码所确定的同一个子网内

确认界面如图 *45:* 确认界面所示：

图 45: 确认界面



5. 配置管理网络

将光标移动至**Set Management Network**处，按下回车，即可进入管理网络配置窗口。

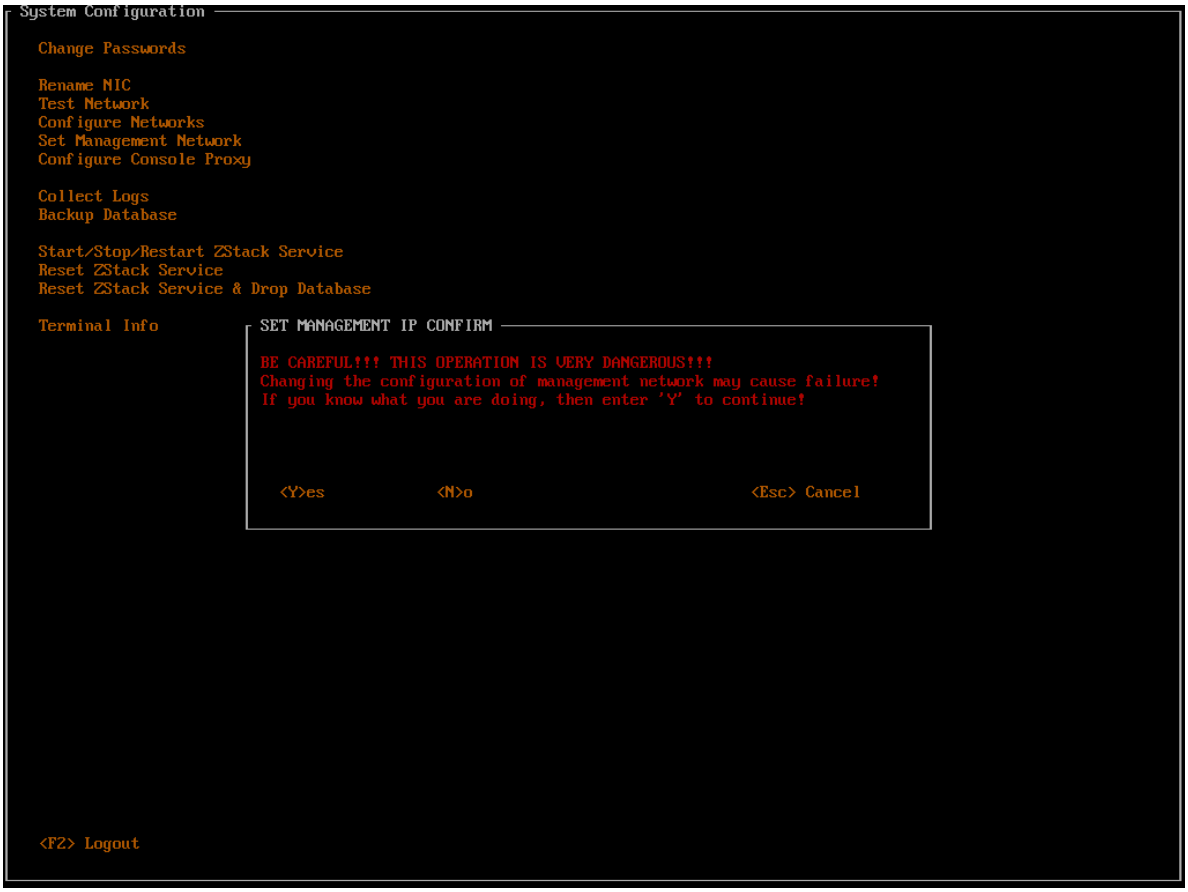
注: 配置管理网络耗时较长，请谨慎操作。

如图 *46:* 配置管理网络所示：

图 46: 配置管理网络

确认界面如图 *47: 确认界面*所示：

图 47: 确认界面



6. 配置控制台代理

将光标移动至**Configure Console Proxy**处，按下回车，即可进入终端代理配置窗口。

输入代理IP和代理端口，回车即可。

控制台代理的原值将被读出并填充在输入项内，用户可按实际需要进行修改。

如果出现以下任何一种情况，均认为输入有误：

- 代理地址和端口均为空
- 代理地址不是合法的IP地址
- 端口号不是1024至65535之间的数字

注:

- 此操作只需要在管理节点执行
- 此操作需要重置RabbitMQ服务，耗时较长。
- 需要用户按**Y**键确认。

如图 *48:* 配置控制台代理所示：

图 48: 配置控制台代理

7. 收集日志

将光标移动至**Collect Logs**处，按下回车，即可进入日志收集窗口。

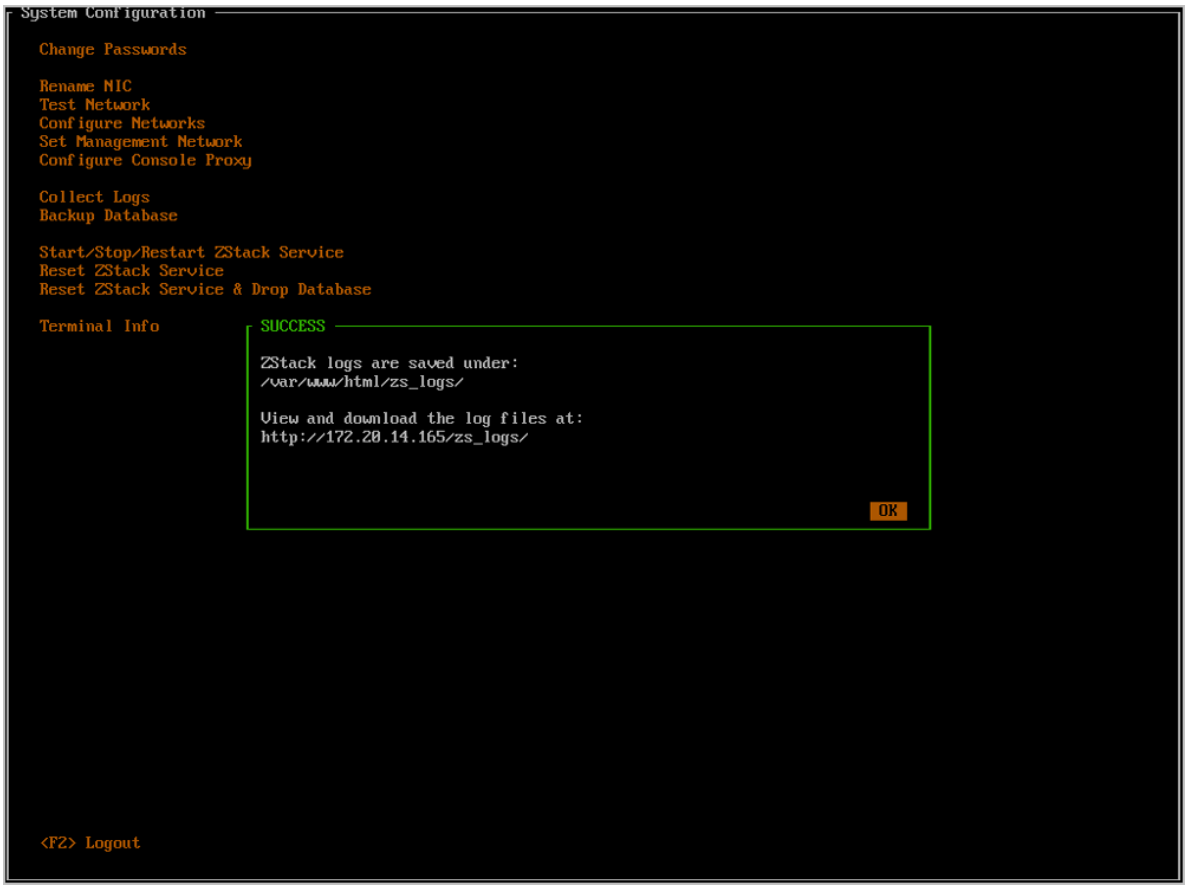
如图 *49:* 收集日志所示：

图 49: 收集日志

点击回车，即可将整个集群的日志收集，并导出至HTTP服务器中，以供下载/在线浏览。

如图 *50:* 日志导出成功所示：

图 50: 日志导出成功

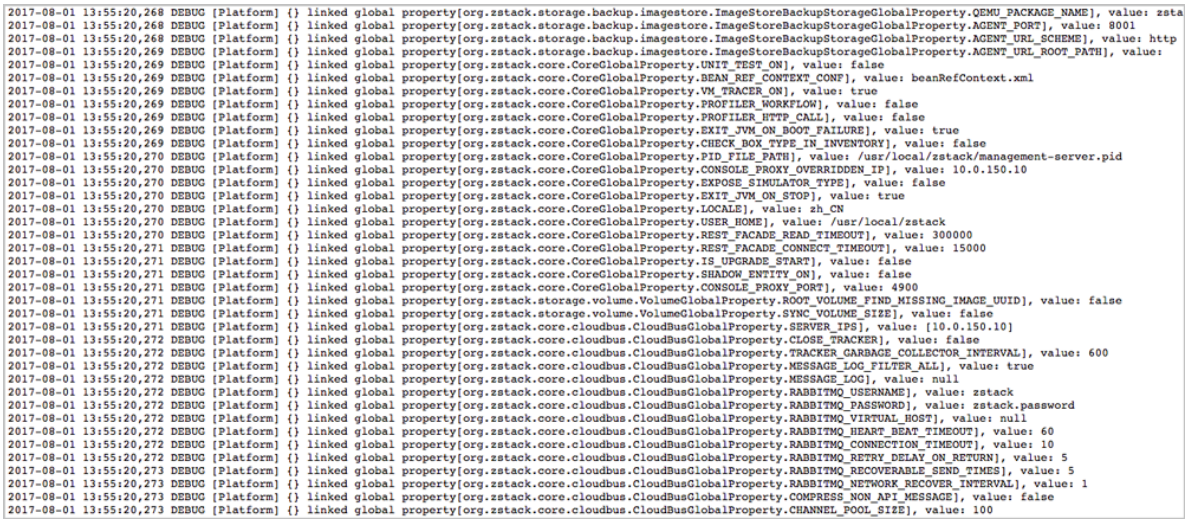


根据提示，用户可以通过浏览器直接访问所有日志内容，支持下载/在线浏览日志。

如图 *51:* 导出日志至*HTTP*服务器中所示，

图 51: 导出日志至HTTP服务器中

图 52: 在线浏览日志



8. 备份数据库

   将光标移动至**Backup Database**处，按下回车，即可进入数据库备份窗口。

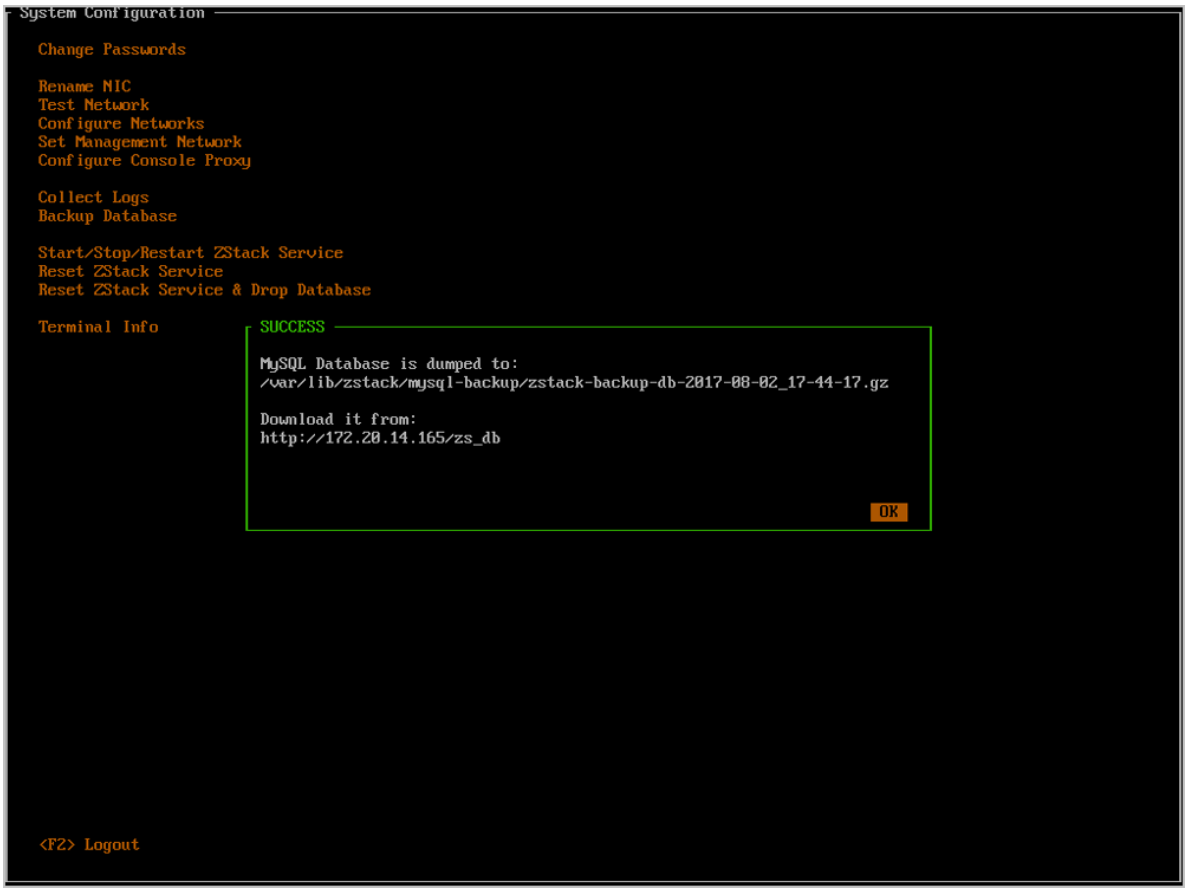
   回车即可导出数据库至HTTP服务器中，以供下载。

   如图 *53:* 备份数据库和图 *54:* 备份数据库成功所示：

图 53: 备份数据库

System Configuration
Change Passwords
Rename NIC
Test Network
Configure Networks
Set Management Network
Configure Console Proxy
Collect Logs
Backup Database
Start/Stop/Restart ZStack Service
Reset ZStack Service
Reset ZStack Service & Drop Database
Terminal Info
BACKUP DATABASE
Press <Enter> to dump database.
This may take a few seconds.
<Enter> OK
<Esc> Cancel
<F2> Logout

图 54: 备份数据库成功



注:

目前，ZStack支持以cli方式将管理节点数据库备份到远程服务器。

执行以下操作，可实现管理节点数据库自动备份到远程服务器，并定时执行自动远程备份。

1. 手动执行以下命令将管理节点数据库进行远程备份

```
#10.0.50.0为远程服务器IP地址
zstack-ctl dump_mysql --host root@10.0.50.0 --d --keep-amount 24
```

2. 执行crontab -e命令将管理节点数据库自动备份脚本修改为以下格式：

```
30 */2 * * * zstack-ctl dump_mysql --host root@10.0.50.0 --d --keep-amount 24
```

该操作表示每两小时将管理节点数据库备份到远程服务器（IP地址：*10.0.50.0*）的*/var/lib/zstack/from-zstack-remote-backup/*目录下。

注:

- **-d**表示只保留最新的指定份数的备份。

- 需提前配置管理节点到远程服务器的SSH免密登录。
- 如需更多技术支持，请联系ZStack官方技术支持团队。

9. 启动/关闭/重启ZStack服务

将光标移动至**Start/Stop/Restart ZStack Servicec**处，按下回车，即可进入启动/关闭/重启ZStack服务窗口。

回车后，再次移动光标，选择具体操作并回车。

如图 *55: 启动/关闭/重启ZStack服务*所示：

图 55: 启动/关闭/重启ZStack服务

根据提示，输入**start zstack**以确认启动ZStack、输入**stop zstack**以确认停止ZStack、输入**restart zstack**以重启ZStack：

如图 *56: 启动ZStack服务*所示：

图 56: 启动ZStack服务

如图 *57: 关闭ZStack服务*所示：

图 57: 关闭ZStack服务

如图 *58:* 重启*ZStack*服务所示：

图 58: 重启ZStack服务

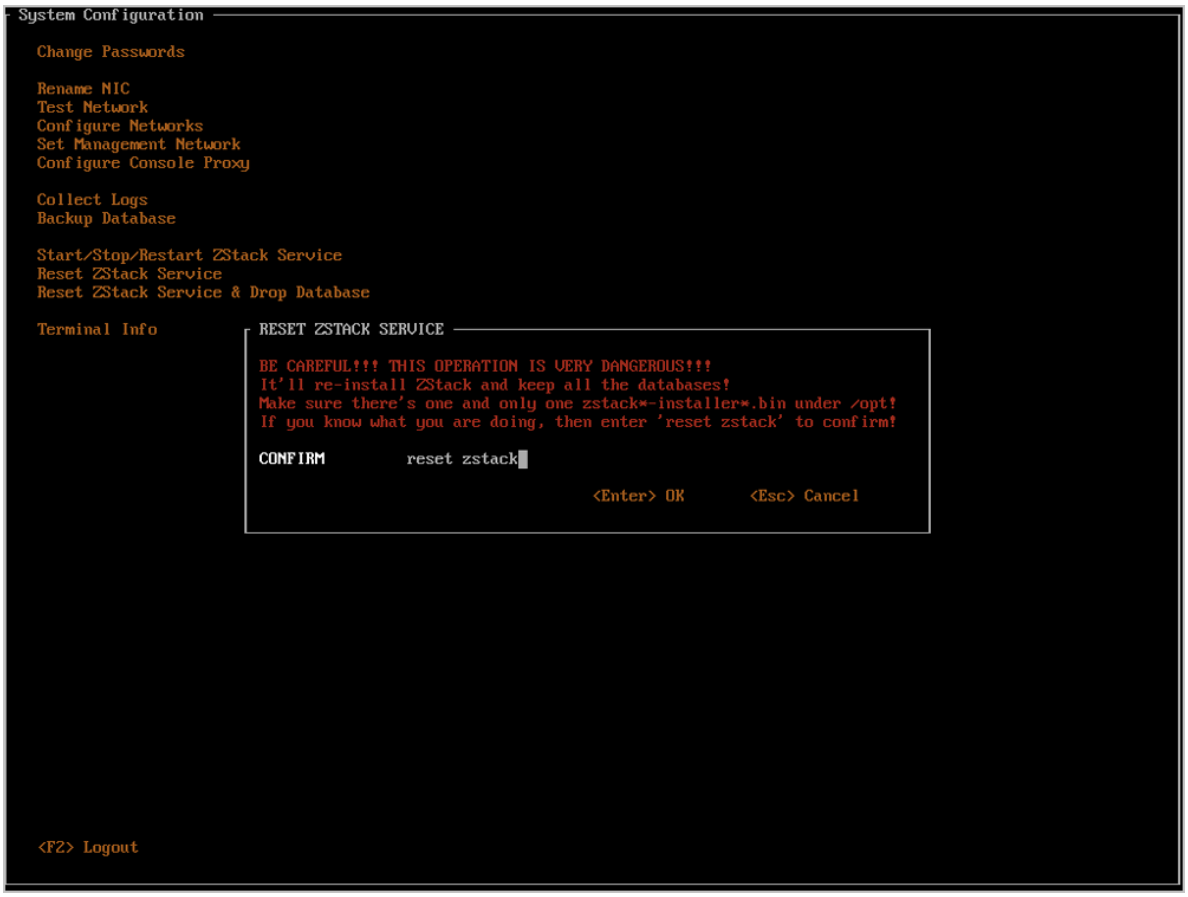
10.重装ZStack服务

将光标移动至**Reset ZStack Service**，按下回车，即可进入重装ZStack服务窗口。

该操作属于极其危险的操作，需要用户输入**reset zstack**，才能回车确认。

如图 *59:* 重装*ZStack*服务所示：

图 59: 重装ZStack服务



11.重装ZStack服务并删除数据库

将光标移动至**Reset ZStack Service&Drop Database**处，按下回车，即可进入重置ZStack和数据库窗口。

该操作与上一操作一样属于极其危险的操作，而且在重装ZStack的同时还会清空已有的数据库，需要用户输入**reset zstack drop database**，才能回车确认。

注: 请谨慎使用此功能！

如图 *60: 重装ZStack服务并删除数据库*所示

图 60: 重装ZStack服务并删除数据库

12.进入终端

ZStack TUI为用户保留了进入终端的入口。将光标移动至**Terminal Info**处，回车即可看到入口信息。

- 按下**Ctrl + Alt+ F2**可以进入保留终端，用户可以在里面执行常规命令 ，但是请谨慎使用，以免对系统造成破坏，影响ZStack服务运行。
- 按下**Ctrl + Alt + F3**可以进入*zstack-cli*命令行界面。
- 任何时候都可以通过按下**Ctrl + Alt + F1**返回ZStack TUI。

如图 *61:* 进入终端提示所示

图 61: 进入终端提示

重启/关机

在主界面按下**F12**即可进入重启/关机界面。

用户选择将光标移动至**Reboot**或**Poweroff**按钮，回车即可进入确认界面。

如图 *62:* 重启/关机所示：

图 62: 重启/关机

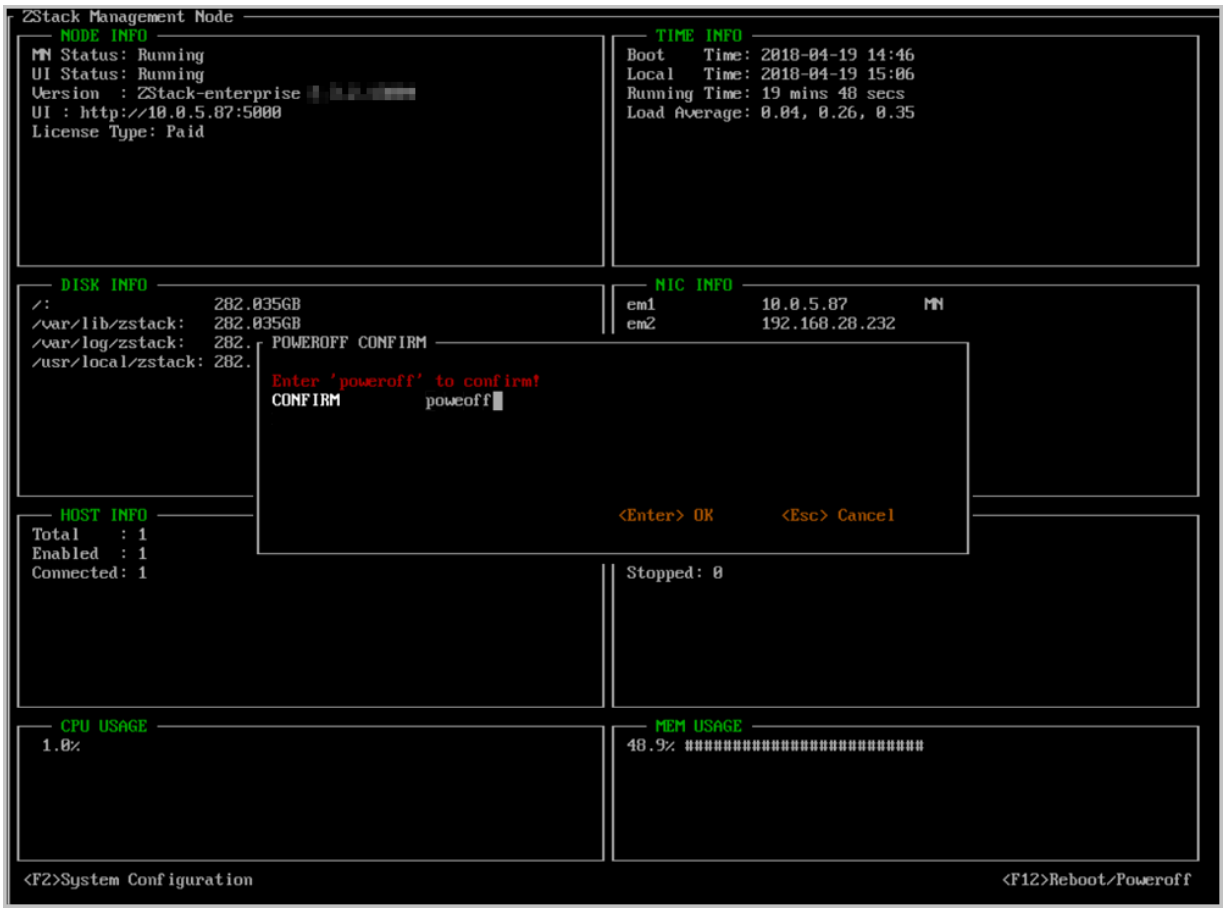
两种操作都需要用户根据提示输入**REBOOT**或**POWEROFF**才可以回车确认，以免误操作。

如图 *63:* 重启确认所示：

图 63: 重启确认

如图 *64: 关机确认*所示：

图 64: 关机确认



异常情况处理

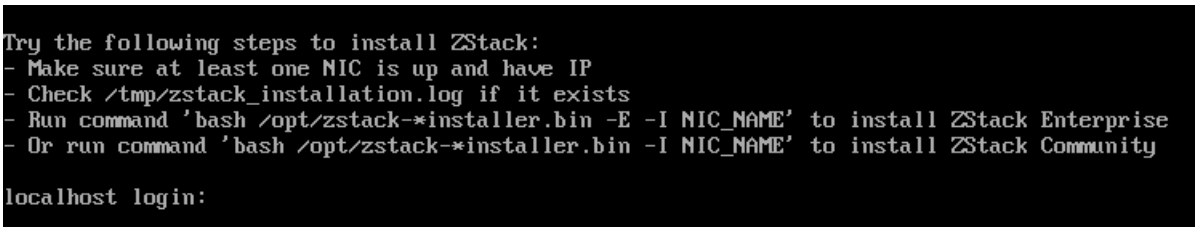
在安装管理节点模式下，如果由于缺少网卡配置或其他原因导致ZStack安装失败，都会退出到终端。

例如在安装ISO时，如果服务器没有可用IP，会导致无法正常安装ZStack管理节点。请先配置好网络，再执行以下命令安装ZStack安装包。

- ZStack企业版安装执行bash /opt/zstack*installer.bin -E
- ZStack社区版安装执行bash /opt/zstack*installer.bin

如图 *65:* 网卡异常情况处理所示：

图 65: 网卡异常情况处理



4.2.2 ZStack计算节点模式

如果用户选择计算节点模式，重启后会自动安装ZStack计算节点，安装完成后将自动进入TUI。

注: 部分场景下，需要all in one的模式来搭建ZStack，这时应选用ZStack管理节点模式安装。

计算节点TUI主界面

计算节点TUI拥有管理节点TUI的部分功能，可以视为精简版的管理节点TUI，使用方法与*ZStack管理节点模式(企业版/社区版)*相同。

- **VM_INFO**：

  列出了当前计算节点所运行的云主机信息，包括UUID、CPU核心数、内存容量和允许状态等。

- 其他信息模块与管理节点意义相同，不再赘述。

如图 *66: 计算节点TUI主界面*所示：

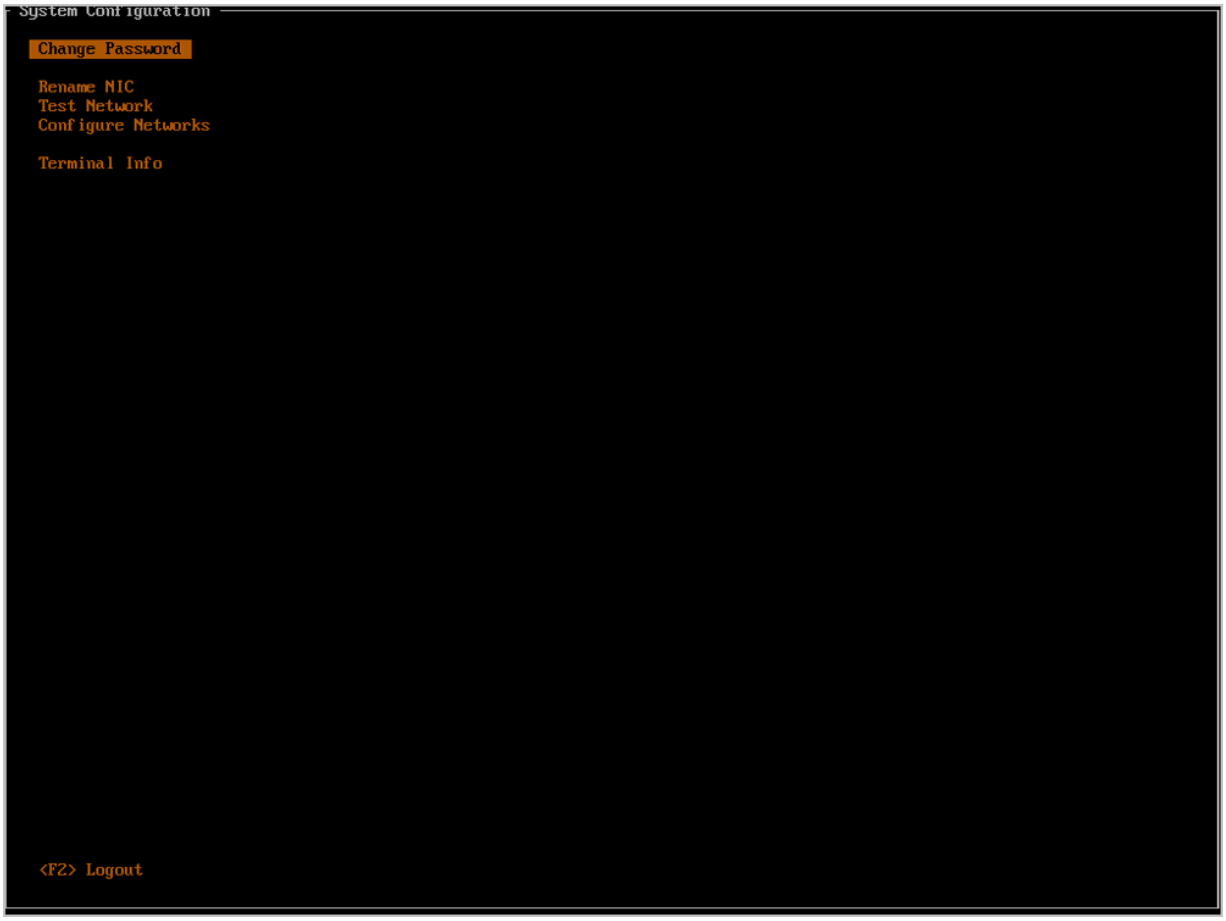
图 66: 计算节点TUI主界面

系统配置

计算节点系统配置与管理节点系统配置相比，仅拥有其中部分功能条目的配置。

如图 *67: 系统配置*所示：

图 67: 系统配置



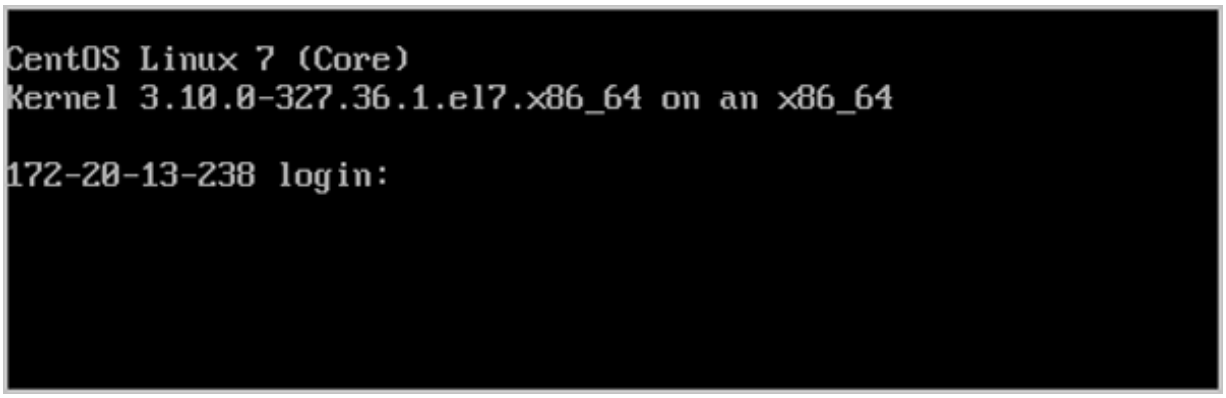
补充说明：管理节点可以添加计算节点的个数在技术上无限制，跟License有关。程序模拟过100万个计算节点。

4.2.3 ZStack专家模式

背景信息

如果用户选择专家模式，重启后会进入终端界面，如图 *68: 终端界面*所示：

图 68: 终端界面



安装完专家模式后，用户可根据实际场景需求，自定义安装所需ZStack环境。

4.3 管理ZStack

操作步骤

1. 首次安装后，系统将自动启动ZStack服务。
2. 管理节点重启后，ZStack服务将自动开机自启。
3. 在管理节点因维护或其他异常原因停止服务后，需手动启动服务。

   启动ZStack服务的方法为：

   ```
   [root@localhost ~]#zstack-ctl start
   #此命令将同时启动管理节点和WEB UI服务
   ```

4. 用户可以使用zstack-ctl status命令查看ZStack管理节点相关服务的运行状态。

   ```
   [root@10-0-5-87 ~]# zstack-ctl status
   ZSTACK_HOME: /usr/local/zstack/apache-tomcat/webapps/zstack
   zstack.properties: /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/
   zstack.properties
   log4j2.xml: /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/log4j2.xml
   PID file: /usr/local/zstack/management-server.pid
   log file: /usr/local/zstack/apache-tomcat/logs/management-server.log
   version: 2.4.0 (ZStack-enterprise 2.4.0.13004)
   MN status: Running [PID:3498]
   UI status: Running [PID:8459] http://10.0.5.87:5000
   ```

5. 用户也可以使用zstack-ctl ui_status命令单独查看Web UI服务状态。

   ```
   [root@172-20-12-20 ~]# zstack-ctl ui_status
   ```

```
UI status: Running [PID:8459] http://10.0.5.87:5000
```

6. 在使用过程中如需重启管理节点服务，则需执行：

```
zstack-ctl restart_node
```

7. 在使用过程中不建议全部停止及重启所有服务。如果确需重启所有服务，可执行以下命令进行重启：

```
zstack-ctl stop && zstack-ctl start
```

4.4 升级ZStack

4.4.1 c72版 升级

本章节主要介绍c72版的升级场景。

- 升级前，管理节点与计算节点均安装c72版操作系统，将管理节点升级至最新的c72版操作系统。
- 只需升级管理节点，计算节点会自动完成升级。
- 升级前，管理员需对数据库进行备份。
- 升级过程中，可访问管理平台界面和命令入口，运行状态的云主机服务不受升级影响。

支持**增量升级**和**离线升级**两种方案。

增量升级

为了提升用户的升级体验，ZStack支持**增量升级**方案。

相比**离线升级**方案（即：用户需下载相应版本的ISO并升级本地源，然后升级ZStack），**增量升级**方案，用户只需要下载最新的ZStack安装包，执行升级安装，该安装包会自动检测ISO版本。

1. 在线升级ZStack之前，请管理员准备好以下必要的软件包，且均存放在管理服务器目录*/opt/*下。
   - ZStack安装包
     - 文件名称：ZStack-installer-2.5.1.bin
     - 下载地址：点击这里
2. 在线升级ZStack之前，管理员需对数据库进行备份。

3. 管理员执行以下命令升级ZStack管理服务。

```
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u
```

注:

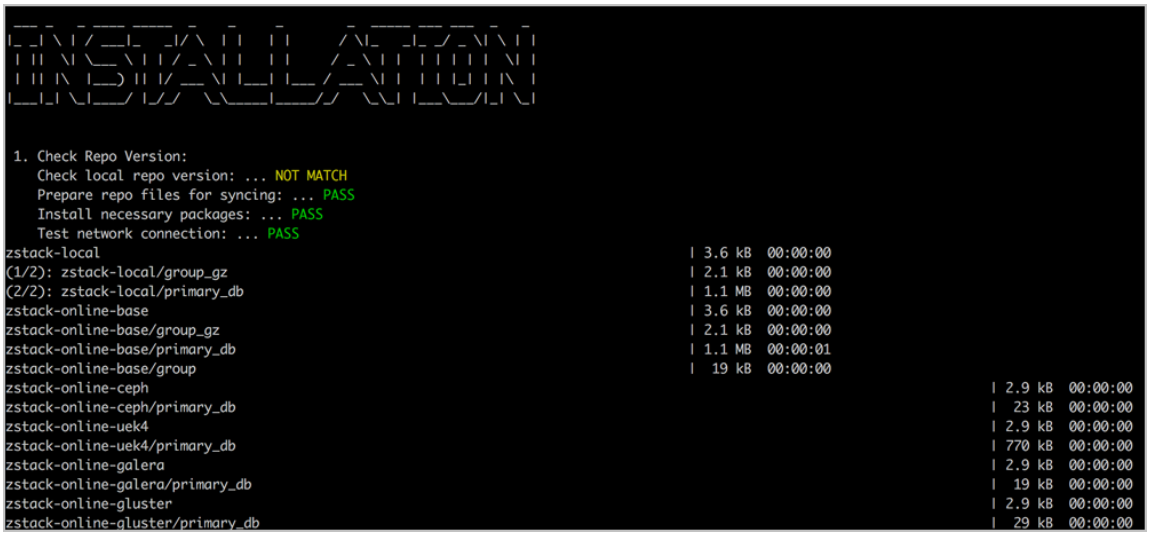
- 若数据库root密码采用系统默认的**zstack.mysql.password**，执行上述命令进行升级即可。
- 若数据库root密码采用自定义非空密码，需执行以下命令进行升级：

```
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u -P
 MYSQL_ROOT_PASSWORD
```

4. 执行升级安装，该安装包会自动检测ISO版本：

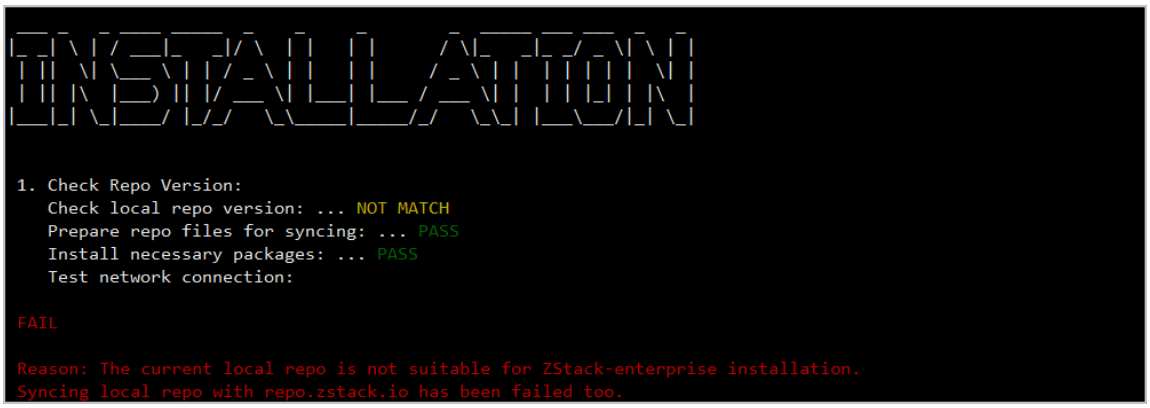
- 如果检测到ISO版本过低，会自动将本地源同步到最新，然后开始ZStack的安装，如图 *69:* 自动将本地源同步到最新所示。

图 69: 自动将本地源同步到最新



- 如果在同步本地源过程中报错，将会提示用户采用离线升级方案，如图 *70:* 同步本地源过程中报错所示。

图 70: 同步本地源过程中报错



注:

- 整个增量升级过程需在**联网状态**下进行。
- 支持采用增量升级方案无缝升级至最新版。

离线升级

1. 离线升级ZStack之前，请管理员准备好以下必要的软件包，且均存放在管理节点目录*/opt/*下。
   - ZStack定制版ISO
     - 文件名称：ZStack-x86_64-DVD-2.5.1-c72.iso
     - 下载地址：点击这里
   - ZStack安装包
     - 文件名称：ZStack-installer-2.5.1.bin
     - 下载地址：点击这里
   - 升级脚本
     - 文件名称：zstack-upgrade
     - 下载地址：点击这里

   注: 软件下载后，需通过MD5校验工具核对校验码，确认与发行信息一致。
2. 离线升级ZStack之前，管理员需对数据库进行备份。
3. 管理员执行以下命令升级ZStack管理服务。

```
#离线升级的两种方式:
# 1. 升级本地仓库和管理服务
[root@zstack-1 opt]# bash zstack-upgrade ZStack-x86_64-DVD-2.5.1-c72.iso
# 2. 如果先升级本地仓库再升级管理服务:
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-x86_64-DVD-2.5.1-c72.iso
```

```
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u
```

注:

- 若数据库root密码采用系统默认的**zstack.mysql.password**，执行上述命令进行升级即可。
- 若数据库root密码采用自定义非空密码，需执行以下命令进行升级：

```
#离线升级的两种方式:
# 1. 升级本地仓库和管理服务
[root@zstack-1 opt]# bash zstack-upgrade ZStack-x86_64-DVD-2.5.1-c72.iso
# 2. 如果先升级本地仓库再升级管理服务:
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-x86_64-DVD-2.5.1-c72.iso
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u -P
 MYSQL_ROOT_PASSWORD
```

4. 升级成功界面如图 *71:* 升级成功所示：

图 71: 升级成功

4.4.2 c74版 升级

本章节主要介绍c74版的升级场景。

- 升级前，管理节点与计算节点均安装c74版操作系统，将管理节点升级至最新的c74版操作系统。
- 只需升级管理节点，计算节点会自动完成升级。
- 升级前，管理员需对数据库进行备份。
- 升级过程中，可访问管理平台界面和命令入口，运行状态的云主机服务不受升级影响。

支持**增量升级**和**离线升级**两种方案。

增量升级

为了提升用户的升级体验，ZStack支持**增量升级**方案。

相比**离线升级**方案（即：用户需下载相应版本的ISO并升级本地源，然后升级ZStack），**增量升级**方案，用户只需要下载最新的ZStack安装包，执行升级安装，该安装包会自动检测ISO版本。

1. 在线升级ZStack之前，请管理员准备好以下必要的软件包，且均存放在管理服务器目录*/opt/*下。
   - ZStack安装包
     - 文件名称：ZStack-installer-2.5.1.bin
     - 下载地址：点击这里
2. 在线升级ZStack之前，管理员需对数据库进行备份。
3. 管理员执行以下命令升级ZStack管理服务。

```
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u
```

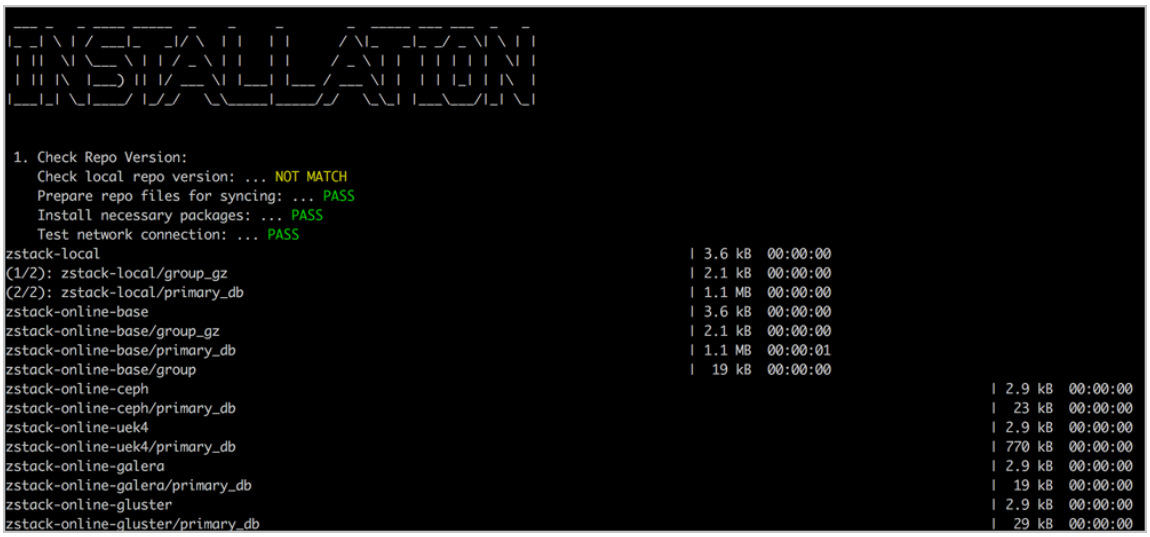
注:

- 若数据库root密码采用系统默认的**zstack.mysql.password**，执行上述命令进行升级即可。
- 若数据库root密码采用自定义非空密码，需执行以下命令进行升级：

```
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u -P
 MYSQL_ROOT_PASSWORD
```

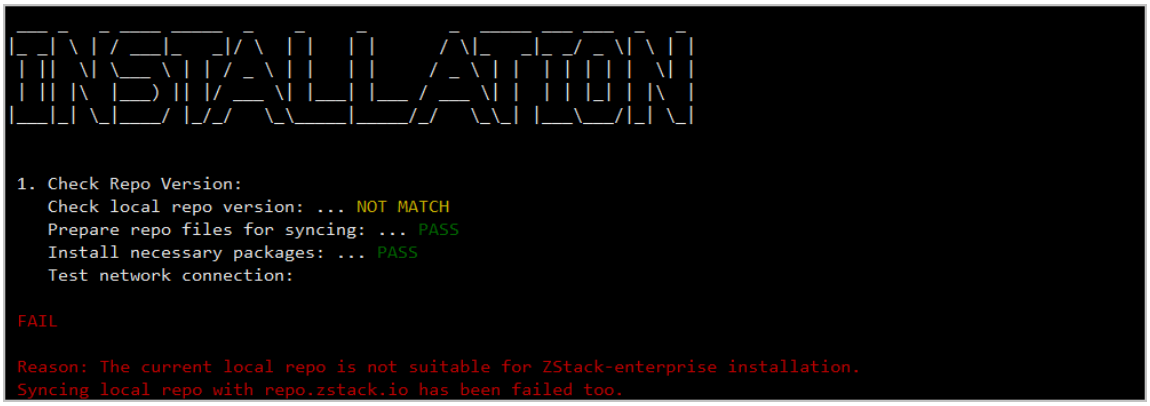
4. 执行升级安装，该安装包会自动检测ISO版本：
   - 如果检测到ISO版本过低，会自动将本地源同步到最新，然后开始ZStack的安装，如图 *72: 自动将本地源同步到最新*所示。

图 72: 自动将本地源同步到最新



- 如果在同步本地源过程中报错，将会提示用户采用离线升级方案，如图 *73:* 同步本地源过程中报错所示。

图 73: 同步本地源过程中报错



注:

- 整个增量升级过程需在**联网状态**下进行。
- 支持采用增量升级方案无缝升级至最新版。

离线升级

1. 离线升级ZStack之前，请管理员准备好以下必要的软件包，且均存放在管理节点目录*/opt/*下。
   - ZStack定制版ISO
     - 文件名称：ZStack-x86_64-DVD-2.5.1-c74.iso
     - 下载地址：点击这里
   - ZStack安装包

- 文件名称：ZStack-installer-2.5.1.bin
- 下载地址：点击这里

- 升级脚本
  - 文件名称：zstack-upgrade
  - 下载地址：点击这里

注: 软件下载后，需通过MD5校验工具核对校验码，确认与发行信息一致。

2. 离线升级ZStack之前，管理员需对数据库进行备份。
3. 管理员执行以下命令升级ZStack管理服务。

```
#离线升级的两种方式:
# 1. 升级本地仓库和管理服务
[root@zstack-1 opt]# bash zstack-upgrade ZStack-x86_64-DVD-2.5.1-c74.iso
# 2. 如果先升级本地仓库再升级管理服务:
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-x86_64-DVD-2.5.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u
```

注:

- 若数据库root密码采用系统默认的**zstack.mysql.password**，执行上述命令进行升级即可。
- 若数据库root密码采用自定义非空密码，需执行以下命令进行升级：

```
#离线升级的两种方式:
# 1. 升级本地仓库和管理服务
[root@zstack-1 opt]# bash zstack-upgrade ZStack-x86_64-DVD-2.5.1-c74.iso
# 2. 如果先升级本地仓库再升级管理服务:
[root@zstack-1 opt]# bash zstack-upgrade -r ZStack-x86_64-DVD-2.5.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-2.5.1.bin -u -P
 MYSQL_ROOT_PASSWORD
```

- 执行*zstack-upgrade*命令前需确认所准备的ISO是基于CentOS 7.4的，避免使用基于CentOS 7.2的ISO覆盖本地源！

4. 升级成功界面如图 *74:* 升级成功所示：

图 74: 升级成功

1. Check Repo Version:
Check local repo version: ... NOT MATCH
Prepare repo files for syncing: ... PASS
Install necessary packages: ... PASS
Test network connection: ..._PASS
Sync from repo.zstack.io: ... PASS
Update metadata: ... PASS
Update non-rpm archives: ... PASS
Update /opt/zstack-dvd/.repo_version: ... PASS
Cleanup: ... PASS
2. Check System:
Pre-Checking: ... PASS
Check System: ... PASS
Update Package Repository: ... PASS
3. Get ZStack:
Download ZStack package: ... PASS
Unpack ZStack package: ... PASS
4. Upgrade ZStack:
Upgrade apache-tomcat: ... PASS
Upgrade zstack-ctl: ... PASS
Install General Libraries (takes a couple of minutes): ... PASS
Stop ZStack: ... PASS
Upgrade ZStack: ... PASS
Add cronjob to clean logs: ... PASS
Enable ZStack bootstrap service: ... PASS
Enable NTP: ... PASS
Config zstack.properties: ... PASS
Append iptables: ... PASS
Install ZStack Web UI (takes a couple of minutes): ... PASS
Start ZStack management node (takes a couple of minutes): ... PASS
Start ZStack Web UI: ... PASS
ZStack in /usr/local/zstack has been successfully upgraded to version:
Management node has been started up again. You can use `zstack-ctl status` to check its status.
zstack-ui has been upgraded.
zstack-ui has been started up again.
Your old zstack was saved in /usr/local/zstack/upgrade/2018-02-09-13-52-22

5 系统登录

登录界面如图 *75:* 登录界面所示：

图 75: 登录界面

- 支持HTTP与HTTPS两种方式登录UI管理界面。
  - HTTP方式默认支持5000端口，输入相应的URL地址（*http://your_machine_ip:5000*），即可打开UI管理界面（建议使用Chrome或Firefox浏览，图示为Chrome浏览器）。
  - HTTPS方式默认不启用。如需启用，可参考*ZStack*官网教程《HTTPS方式登录UI 使用说明》。
- ZStack登录方式分为三种：账户登录、用户登录和AD/LDAP登录。
- 系统首次登录时，默认账户名：**admin** 默认初始密码：**password**。
- 点击登录即可进入系统。
- 首次登录成功后，可点击UI界面右上角的**个人中心** > **修改密码**。
- 默认登录时效为2小时，超时需重新登录。
  - **会话超时时间**可自定义设置，设置方法：在ZStack私有云主菜单，进入**设置** > **全局设置** > **基本设置**中设置。
- 点击**个人中心** > **相应语言按钮**，可切换UI界面语言，目前支持简体中文/英语/繁体中文。
- 点击**个人中心** > **登出**，即可退出ZStackUI管理界面。

注:

若已安装企业管理模块许可证，系统登录相关介绍可参考企业管理*(Plus)*章节，License相关介绍可参考关于章节。

6 Wizard引导设置

首次登录ZStack，系统界面将引导进行ZStack私有云平台基本的初始化环境配置。

注:

- 在系统使用中，如果中断Wizard引导设置或者删除了系统关键资源，**系统将不会再次进入引导界面。**
- 建议按照引导进行ZStack基本环境的配置。

6.1 创建区域

背景信息

区域：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。

如图 *76: 创建区域*所示：

图 76: 创建区域

可参考以下示例输入相应内容：

- **名称**：输入区域的名称
- **简介**：可选项，可留空不填

点击**下一步**按钮，完成区域创建。

6.2 创建集群

背景信息

集群：一组物理机（计算节点）的逻辑集合。

如图 77: 创建集群所示：

图 77: 创建集群

可参考以下示例输入相应内容：

- **名称**：输入集群的名称
- **简介**：可选项，可留空不填

点击**下一步**按钮，完成集群创建。

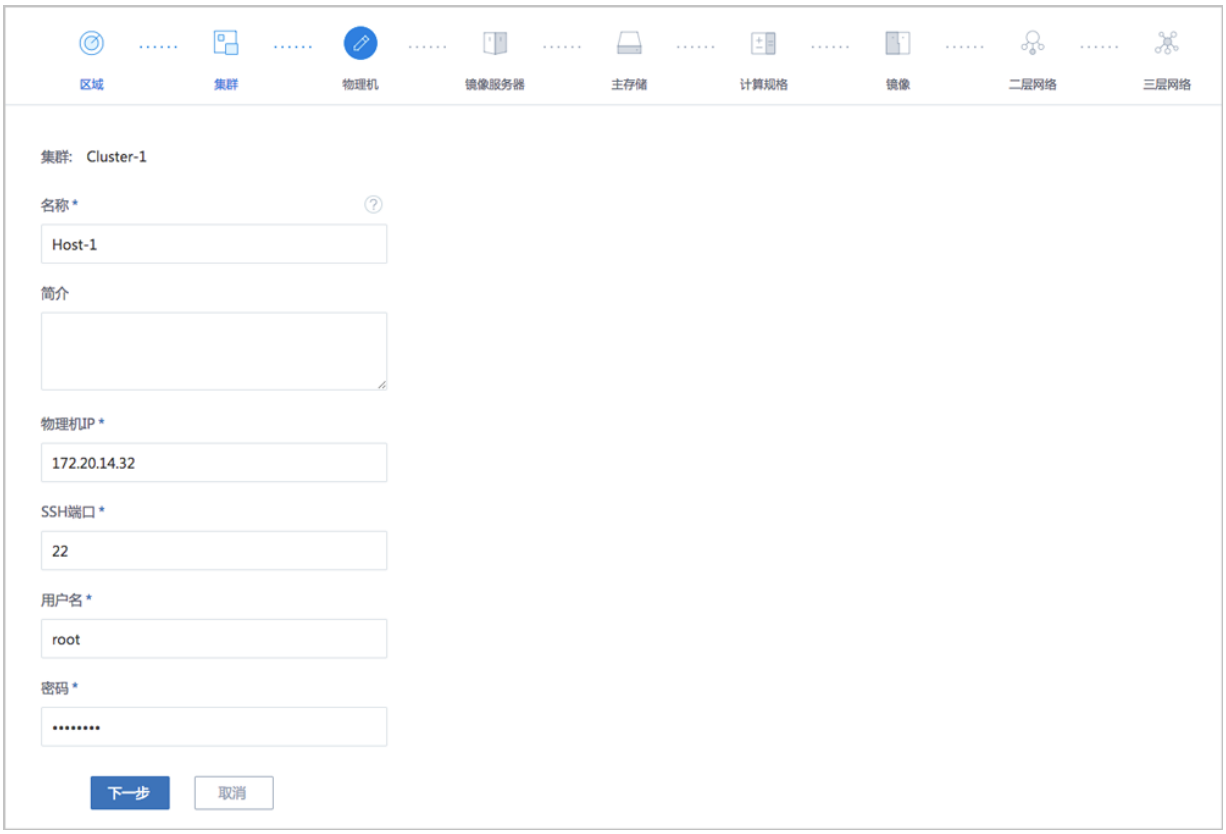
6.3 添加物理机

背景信息

物理机：也称之为计算节点，是云计算平台的核心资产，云主机将会运行在物理机之上。

如图 78: 添加物理机所示：

图 78: 添加物理机



操作步骤

1. 输入物理机的**名称**。
2. 输入物理机的**简介**。可简述物理机相关信息进行备注，可使用中文，也可留空不填。
3. 输入**物理机IP**地址，例如*172.20.14.32*。
   - 在生产环境中，出于安全和稳定性考虑，建议采用管理网络和公有网络分离的方案，即管理节点和计算节点采用独立的网络和IP。

     例如，使用eth0连接一套管理网络，ZStack通过管理网络与各计算节点通讯；使用eth1连接另外一套公有网络，可以通过顶层汇聚交换机与外界互联互通。
   - 使用管理网络和公有网络分离的方案，可以最大限度保障系统安全，以及保障足够的网络带宽供管理网络使用。
4. 输入物理机的**SSH端口**，默认为22，如果此物理机没有配置SSH端口，则可按照默认配置的22端口使用。
5. 输入物理机的**用户名**，默认为root用户，也可输入普通用户。
   - 如果此物理机没有添加普通用户，则可按照默认的root用户使用。
   - 普通用户要求拥有sudo权限。

- 建议在创建普通用户时，使用*adduser*命令。

  创建普通用户及修改用户sudo权限可参考以下样例：

```
#创建一个名为zstack的普通用户
[root@localhost ~]# adduser zstack
#授权zstack用户拥有sudo权限
[root@localhost ~]# echo "zstack    ALL=(ALL)    NOPASSWD: ALL" >>/etc/sudoers
```

6. 输入对应的用户**密码**，输入密码时请注意大小写。
7. 点击**下一步**，ZStack会调用后台作业来配置物理机。

   - 配置过程可能持续几分钟。
   - 若安装出错，会提示相应的错误信息。

后续操作

若Wizard引导设置结束后，要在同一区域的同一集群中再添加其它物理机，则对应主机需安装相同的CentOS系统。SSH端口、用户名、密码无须相同。

6.4 添加镜像服务器

镜像服务器：用于保存云主机的镜像模板或ISO的存储服务器。

镜像服务器支持以下类型：

1. **ImageStore（镜像仓库）**：以镜像切片方式存储镜像文件，支持增量存储；
2. **Sftp**：以文件方式存储镜像文件；
3. **Ceph镜像服务器**：以Ceph分布式块存储方式存储镜像文件；
4. **FusionStor镜像服务器**：以FusionStor分布式块存储方式存储镜像文件。

注:

企业版和混合云版支持ImageStore、Ceph和FusionStor类型，社区版支持Sftp、Ceph和FusionStor类型。

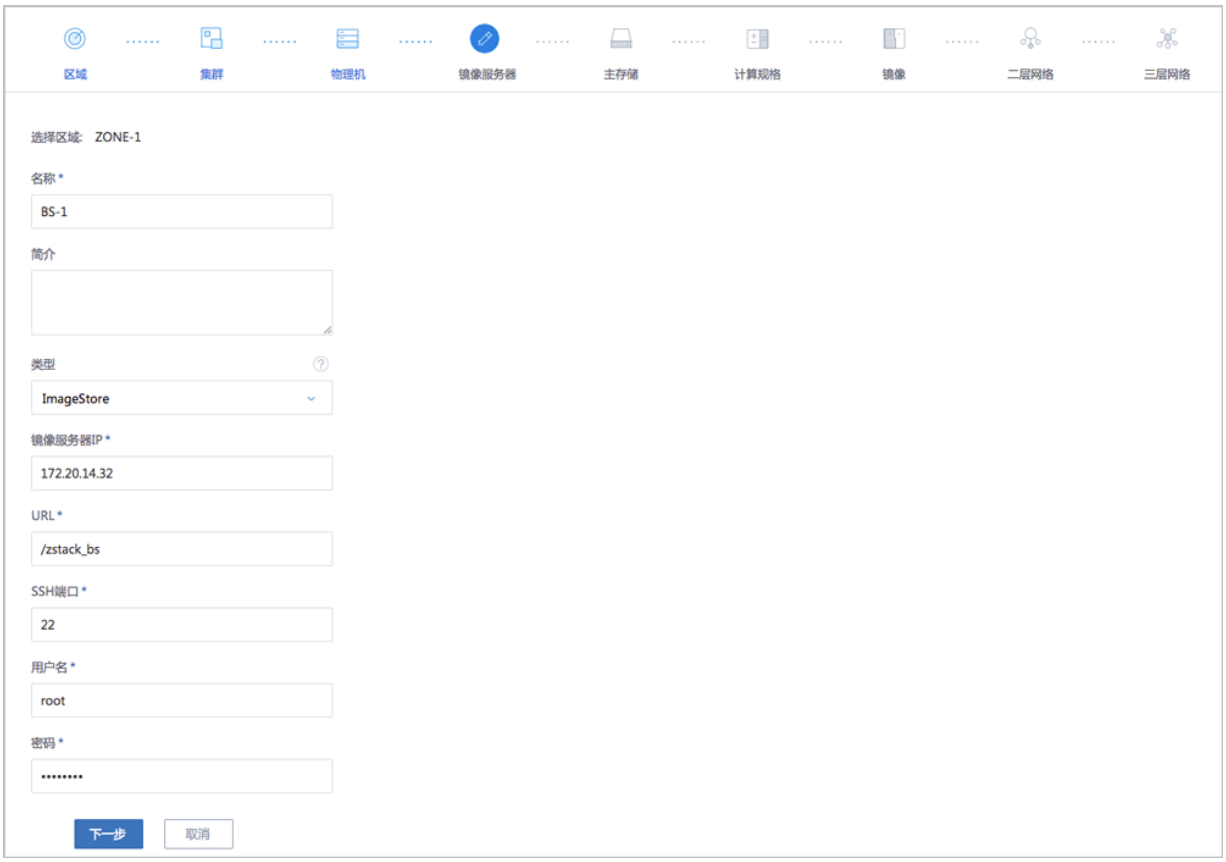
需根据环境需求，进行相关配置。

6.4.1 ImageStore（镜像仓库）

背景信息

如图 *79:* 添加镜像仓库所示：

图 79: 添加镜像仓库



操作步骤

1. 输入镜像服务器的**名称**。
2. 输入镜像服务器的**简介**。可简述镜像服务器相关信息进行备注，可使用中文，也可留空不填。
3. 镜像服务器**类型**选择ImageStore。
4. 输入**镜像服务器IP**地址。
    - 在生产环境中，出于安全和稳定性考虑，建议采用管理网络和公有网络分离的方案。
    - 镜像服务器IP地址可与管理网络共享，以节省公有网络带宽。
    - 当公有网络是万兆网络环境时，镜像服务器IP地址也可与公有网络共享，以提高镜像在镜像服务器和计算节点之间的传递速度。

      通常在添加镜像，保存镜像时，会占用较大网络带宽，如果与公有网络共享，建议选择网络空闲时段进行镜像相关操作。
    - 有条件的客户，可设置独立的存储网络。
5. 输入镜像服务器上挂载大容量存储的**URL**，例如输入*/zstack_bs*。
6. 输入**SSH端口**，默认为22，如果镜像服务器没有配置SSH端口，则可按照默认配置的22端口使用。

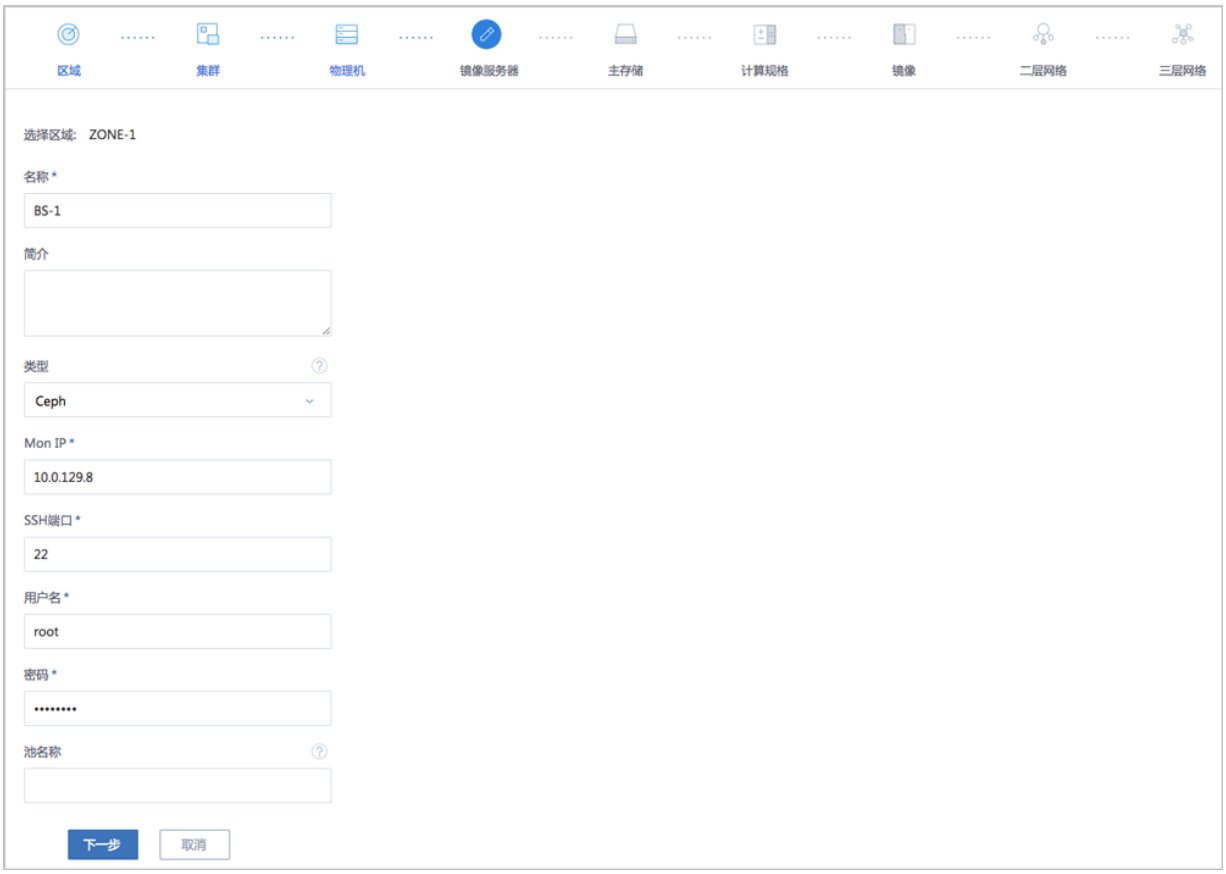
7. 输入**用户名**，默认为root用户，也可输入普通用户。
    - 如果镜像服务器没有添加普通用户，则可按照默认的root用户使用。
    - 普通用户要求拥有sudo权限。
8. 输入对应的用户**密码**，输入密码时请注意大小写。
9. 点击**下一步**，系统会配置ImageStore类型镜像服务器。

6.4.2 Ceph镜像服务器

背景信息

如图 *80: 添加Ceph镜像服务器*所示：

图 80: 添加Ceph镜像服务器



操作步骤

1. 输入镜像服务器的**名称**。
2. 输入镜像服务器的**简介**。可简述镜像服务器相关信息进行备注，可使用中文，也可留空不填。
3. 镜像服务器**类型**选择Ceph。

4. 输入Ceph监控节点的IP地址**Mon IP**。
5. 输入Ceph监控节点的**SSH端口**号，默认为22，如果此节点没有配置SSH端口，则可按照默认配置的22端口使用。
6. 输入Ceph监控节点的**用户名**，默认为root用户，也可输入普通用户。
   - 如果此Ceph监控节点没有添加普通用户，则可按照默认的root用户使用。
   - 普通用户要求拥有sudo权限。
7. 输入Ceph监控节点对应的用户**密码**，输入密码时请注意大小写。
8. 输入**池名称**，可选项，可对Ceph镜像服务器指定特定的存储池。
   - 如果指定，需提前在Ceph存储集群自行创建存储池。
   - 如果不指定，默认自动创建存储池。
9. 点击**下一步**，系统会配置Ceph类型镜像服务器。

6.4.3 FusionStor镜像服务器

背景信息

添加FusionStor镜像服务器的具体步骤，与添加Ceph镜像服务器的步骤类似。

操作步骤

1. 输入镜像服务器的**名称**。
2. 输入镜像服务器的**简介**。可简述镜像服务器相关信息进行备注，可使用中文，也可留空不填。
3. 镜像服务器**类型**选择FusionStor。
4. 输入FusionStor监控节点的IP地址**Mon IP**。
5. 输入FusionStor监控节点的**SSH端口**号，默认为22，如果此节点没有配置SSH端口，则可按照默认配置的22端口使用。
6. 输入FusionStor监控节点的**用户名**，默认为root用户，也可输入普通用户。
   - 如果此FusionStor监控节点没有添加普通用户，则可按照默认的root用户使用。
   - 普通用户要求拥有sudo权限。
7. 输入FusionStor监控节点对应的用户**密码**，输入密码时请注意大小写。
8. 点击**下一步**，系统会配置FusionStor类型镜像服务器。

6.5 添加主存储

主存储：用于存储云主机磁盘文件（包括：根云盘、数据云盘、根云盘快照、数据云盘快照、镜像缓存等）的存储服务器。

主存储的支持类型分为两大类：

1. 本地存储，使用物理机的硬盘进行存储；
2. 共享存储，又细分为NFS、Shared Mount Point、Ceph、FusionStor和Shared Block几种类型。
   - NFS为网络文件系统的存储方式。
   - Shared Mount Point支持常用的分布式文件系统提供的网络共享存储，支持的常见类型有MooseFS、GlusterFS、OCFS2、GFS2等。
   - Ceph采用了分布式块存储方式。
   - FusionStor采用了华云网际提供的分布式块存储方式。
   - Shared Block采用共享块存储方式。

注:

主存储类型与镜像服务器类型有关联性要求：

- 如果镜像服务器采用ImageStore（镜像仓库），主存储支持选择采用LocalStorage（本地存储）、NFS、Share Mount Point、Ceph或Shared Block类型。
- 如果镜像服务器采用Ceph类型，主存储支持采用Ceph类型。
- 如果镜像服务器采用FusionStor类型，主存储支持采用FusionStor类型。

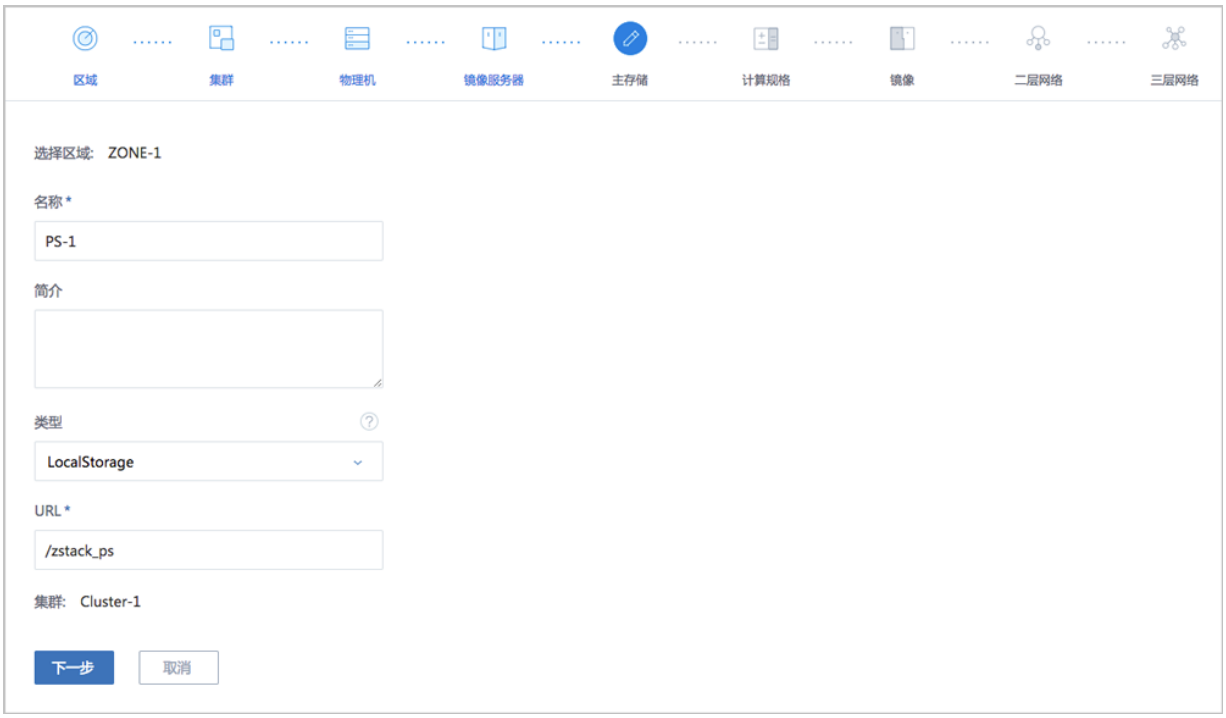
6.5.1 LocalStorage（本地存储）

背景信息

如果采用本地存储类型的主存储，所有物理机将会使用相同的目录进行配置。

如图 *81:* 添加本地存储所示：

图 81: 添加本地存储



可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择LocalStorage
- **URL**：输入本地存储的路径

  注:

  - 不能使用以下/、 /dev/、/proc/、/sys/、/usr/bin、/bin等系统目录。
  - 使用系统目录可能会导致物理机异常。
- **集群**：选择主存储需要挂载的集群

点击**下一步**按钮，完成LocalStorage添加。

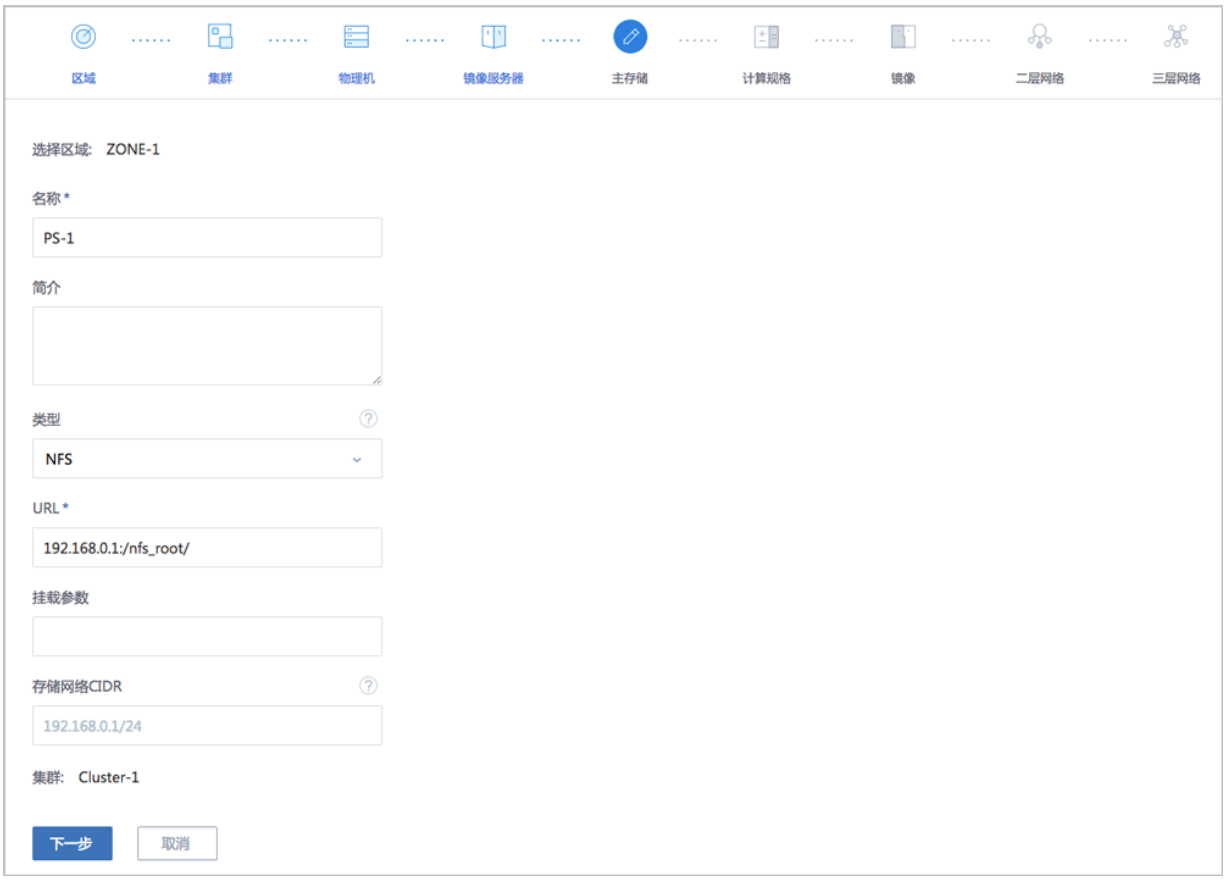
6.5.2 NFS

背景信息

如果采用了NFS，那么ZStack会在所有的物理机上自动挂载相同的NFS共享目录作为主存储。NFS Server的目录需提供读写权限。

如图 *82: 添加NFS主存储*所示：

图 82: 添加NFS主存储



可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择NFS
- **URL**：输入NFS Server的共享目录的URL

注:

- 输入格式为：*NFS_Server_IP:/NFS_Share_folder*
- 请提前在NFS Server端设置相应目录的访问权限。
- 为保证在NFS Server端的安全控制，建议配置相应安全规则，进行访问控制。
- 用户可以提前在NFS Server端通过showmount -e命令检查NFS Server已共享的目录。
- 不能使用以下/、 /dev/、/proc/、/sys/、/usr/bin、/bin等系统目录。
- 使用系统目录可能会导致物理机异常。

- **挂载参数**：可选项，需NFS Server端支持

注:

- 参数以逗号隔开。
- NFS的mount参数可以参考mount的 -o选项里的内容。
- 可根据常用的客户端mount命令参数进行设置。如果设置的参数与NFS Server端冲突，则以Server端为准。

- **存储心跳网络CIDR**：可选项，使用此存储网络来判断云主机健康状态，不填默认与管理网络共用
- **集群**：选择主存储需要挂载的集群

点击**下一步**按钮，完成NFS添加。

6.5.3 Shared Mount Point

前提条件

1. Shared Mount Point提供了对MooseFS，GlusterFS，OCFS2，GFS2等可以提供共享文件系统存储的支持。
2. 添加过程与本地存储类似，用户只需提供物理机挂载的本地目录，ZStack即可完成对各种分布式文件系统的对接。
3. 选择使用Shared Mount Point，用户需要提前配置好相应的分布式文件系统。并且根据不同存储系统的客户端配置，预先在每台物理机上把共享文件系统挂载在相同的文件路径。
4. 下面以MooseFS为例来配置主存储。

   假如MooseFS的master Server IP地址为*172.20.12.19*。用户需要下载并安装MooseFS的客户端工具mfsmount。并且创建相应目录作为mount节点。

   注:

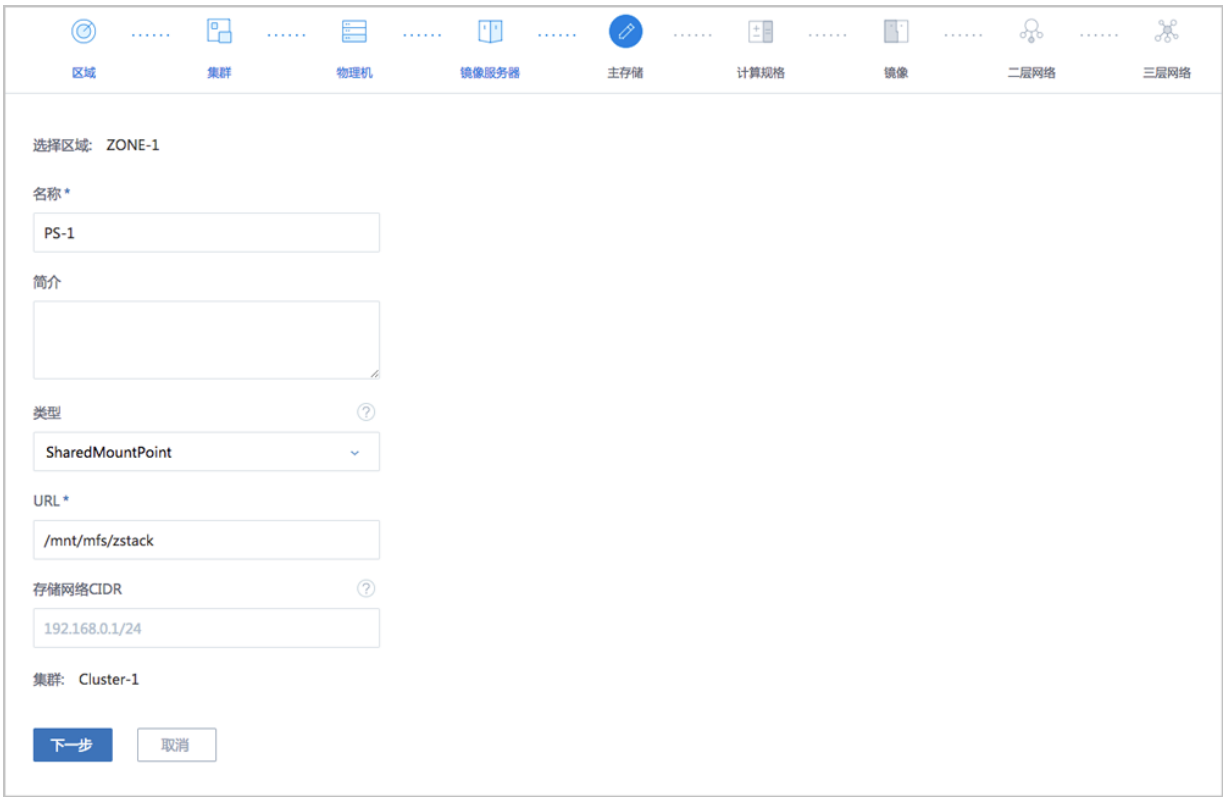
   例如，创建*/mnt/mfs*作为挂载点，使用*mfsmount*命令挂载MooseFS系统。用户也可以根据需要使用*mfssetgoal*命令设置相应的文件副本保存数量。

   ```
   [root@localhost ~]#mkdir /mnt/mfs
   [root@localhost ~]#mfsmount /mnt/mfs -H 172.20.12.19
   [root@localhost ~]#mkdir /mnt/mfs/zstack
   [root@localhost ~]#mfssetgoal -r 2 /mnt/mfs/zstack/
   #以上命令将/mnt/mfs/zstack/目录的文件挂载到远端172.20.12.19，MooseFS存储服务器保留两份拷贝。
   ```

背景信息

如图 *83: 添加Shared Mount Point主存储*所示：

图 83: 添加Shared Mount Point主存储



可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择SharedMountPoint
- **URL**：输入物理机已挂载的共享存储目录URL
- **存储心跳网络CIDR**：可选项，使用此存储网络来判断云主机健康状态，不填默认与管理网络共用
- **集群**：选择主存储需要挂载的集群

点击**下一步**按钮，完成Shared Mount Point添加。

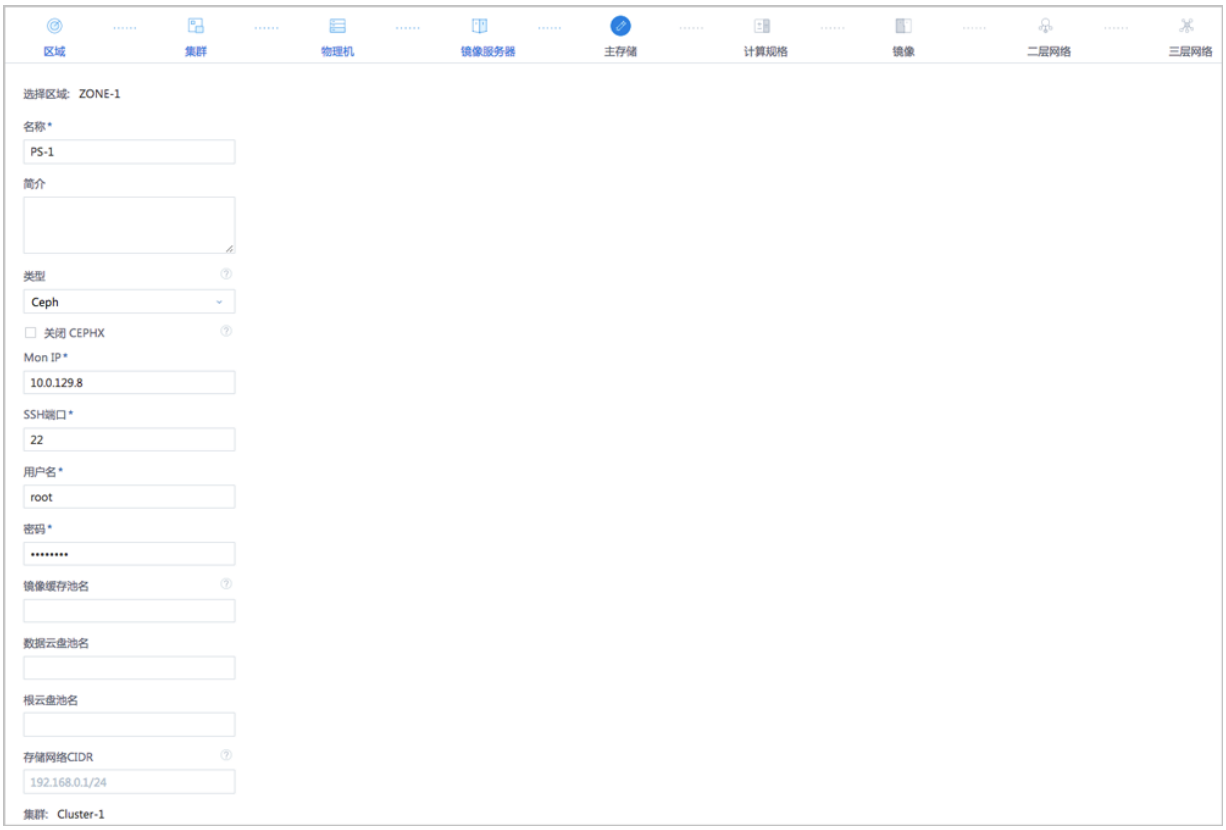
6.5.4 Ceph

背景信息

ZStack对Ceph的支持为块存储模式。如果主存储类型选择Ceph，则需要先添加一个Ceph类型或镜像仓库类型的镜像服务器，并且提前配置好Ceph分布式存储。

如图 *84: 添加Ceph主存储*所示：

图 84: 添加Ceph主存储



可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择Ceph
- **关闭CEPHX**：CEPHX代表Ceph密钥认证，默认关闭

  注:

  - 关闭CEPHX，代表关闭Ceph密钥认证；
  - 如果计算节点的网络较安全，可关闭此项，以避免Ceph的认证失败；
  - 需确保Ceph存储已关闭密钥认证，如果Ceph存储未关闭，此处勾选可能导致创建云主机失败。
- **管理IP**：输入Ceph监控节点的IP地址Mon IP
- **SSH端口**：输入Ceph监控节点的SSH端口，默认为22
- **用户名**：输入Ceph监控节点的用户名
- **密码**：输入Ceph监控节点的用户名对应的密码
- **继续添加**：点击加号按钮继续添加Ceph监控节点
- **镜像缓存池名**：输入镜像缓存池名，如果不填，系统会自动为用户创建这三个池

- **数据云盘池名**：输入数据云盘池名，如果不填，系统会自动为用户创建这三个池
- **根云盘池名**：输入根云盘池名，如果不填，系统会自动为用户创建这三个池
- **存储心跳网络CIDR**：可选项，使用此存储网络来判断云主机健康状态，不填默认与管理网络共用
- **集群**：选择主存储挂载的集群

点击**下一步**按钮，完成Ceph添加。

6.5.5 FusionStor

前提条件

FusionStor采用了华云网际提供的分布式块存储方式。如果主存储类型需要采用FusionStor，则需要先添加一个FusionStor类型的镜像服务器并且提前配置好FusionStor分布式存储。

背景信息

添加FusionStor存储具体步骤，与添加Ceph存储步骤类似。

操作步骤

1. 选择主存储的**类型**为FusionStor。
2. 输入FusionStor监控节点的IP地址**Mon IP**。
3. 输入FusionStor监控节点的**SSH端口**，默认为22，如果此节点没有配置SSH端口，则可按照默认配置的22端口使用。
4. 输入FusionStor监控节点的**用户名**，默认为root用户，也可输入普通用户（普通用户要求拥有sudo权限）。如果此FusionStor监控节点没有添加普通用户，则可按照默认的root用户使用。
5. 输入FusionStor监控节点的对应的用户**密码**，输入密码时请注意大小写。
6. 输入**镜像缓存池名**、**数据云盘池名**和**根云盘池名**，这三个都是选填项。

   注:

   - 如果用户需要填写，则必须先在FusionStor集群上创建这三个池成功后再进行填写。
   - 如果用户不填写，则系统会自动为用户创建这三个池。
7. 输入**存储心跳网络CIDR**，用于共享存储FusionStor指定存储网络。
8. 点击**下一步**，系统会配置FusionStor的块存储作为主存储。

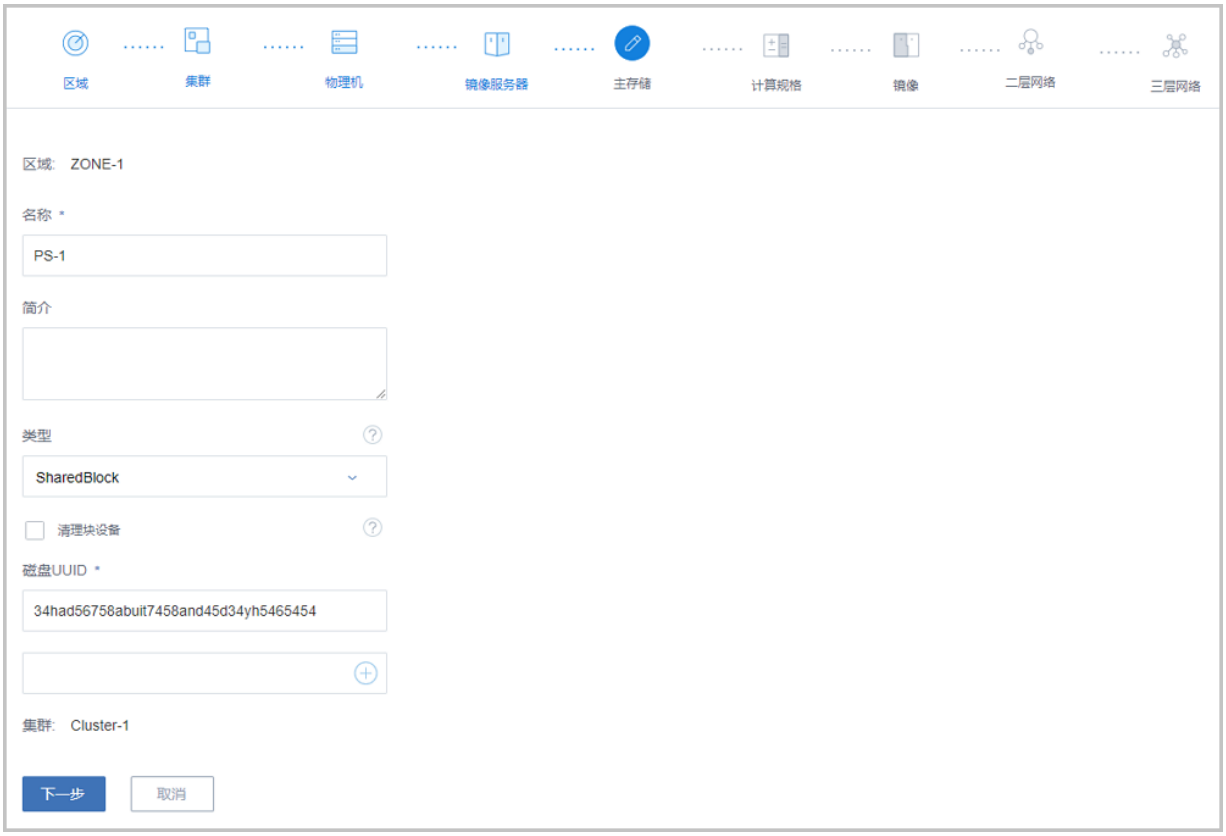
6.5.6 Shared Block

背景信息

Shared Block（共享块存储）是ZStack企业版新支持的一种主存储类型，可以将用户在SAN存储上划分的LUN设备直接作为存储池，再提供给业务云主机使用。与之前Shared Mount Point（SMP）主存储类型不同，**Shared Block**具备便捷部署、灵活扩展、性能优异等优势。

如果主存储类型采用Shared Block，那么使用共享块设备作为主存储，匹配镜像仓库，支持添加一个或多个共享块设备，需输入磁盘唯一标识，例如：磁盘UUID、WWN、WWID。

图 85: 添加Shared Block主存储



可参考以下示例输入相应内容：

- **名称**：输入主存储的名称
- **简介**：可选项，可留空不填
- **类型**：选择SharedBlock类型
- **清理块设备**：默认不勾选

注:

- 勾选后将强制清理LUN设备中的文件系统、RAID或分区表中的签名，请谨慎选择。
- 若LUN设备中未存放重要数据，可勾选此项。
- 添加的LUN设备中不能有分区，否则会添加失败。

- **磁盘UUID**：输入磁盘唯一标识，例如：磁盘UUID、WWN、WWID；支持添加多个共享块设备
- **集群**：可选项，选择加载的集群

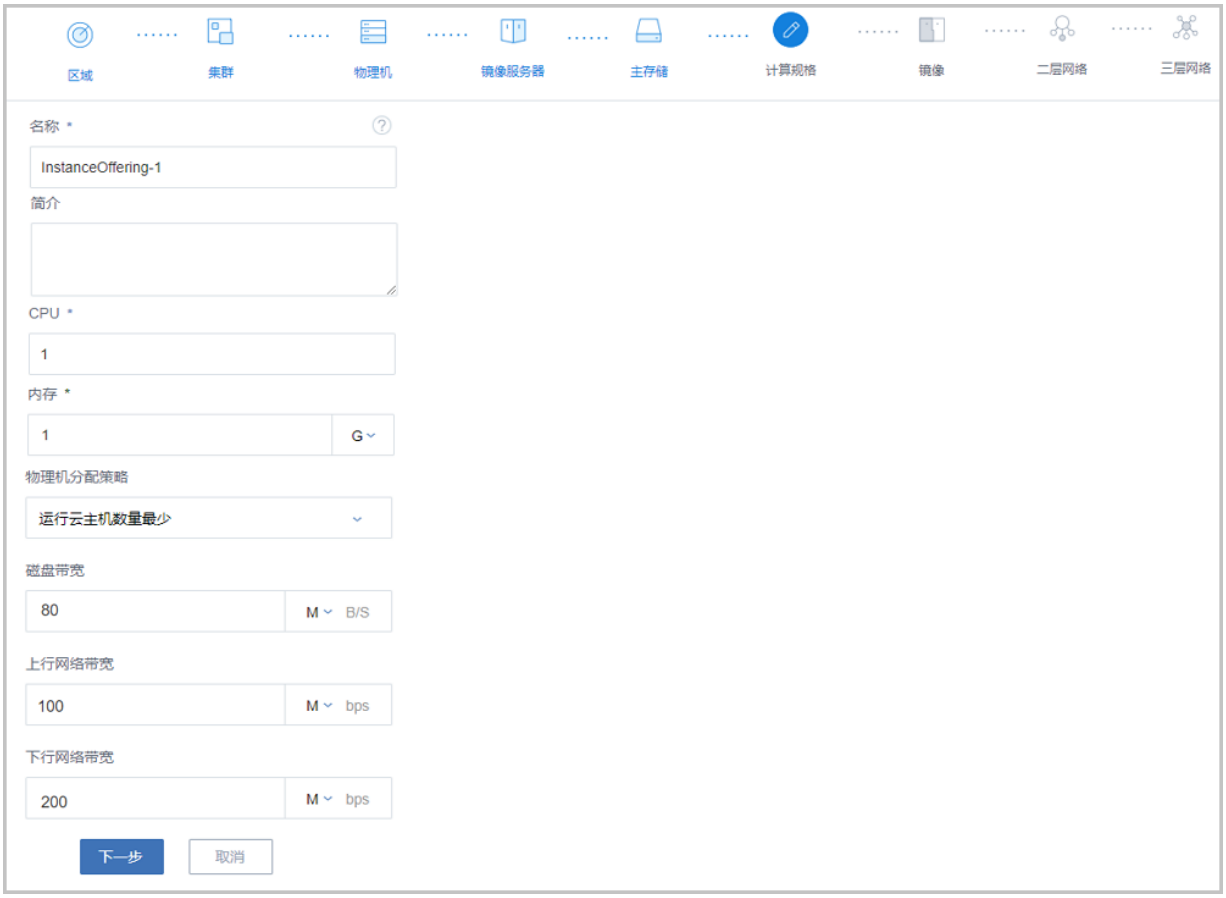
点击**下一步**按钮，完成Shared Block添加。

6.6 创建计算规格

背景信息

如图 *86: 创建计算规格*所示：

图 86: 创建计算规格



可参考以下示例输入相应内容：

- **名称**：设置计算规格的名称
- **简介**：可选项，可留空不填

- **CPU**：设置云主机CPU的核数
- **内存**：设置云主机内存的大小，基本单位包括：M/G/T
- **物理机分配策略**：选择物理机分配策略。包括：运行云主机数量最少、CPU使用率最低、内存使用率最低、运行云主机最大数量，默认为运行云主机数量最少策略
  - **运行云主机数量最少**：优先选择云主机最少的物理机来创建云主机
  - **CPU使用率最低**：优先选择CPU使用率最低的物理机来创建云主机

    注:

    - 系统会采集一段时间内物理机CPU负载数据，计算出这段时间的平均CPU使用率，然后优先选择CPU使用率最低的物理机来创建云主机。
    - 数据采集周期默认10分钟，在**设置** > **全局设置** > **高级设置**中，修改**物理机CPU使用率最低采集间隔**参数，更改数据采集时间。
  - **内存使用率最低**：优先选择内存使用率最低的物理机来创建云主机

    注:

    - 系统会采集一段时间内物理机内存负载数据，计算出这段时间的平均内存使用率，然后优先选择内存使用率最低的物理机来创建云主机。
    - 数据采集周期默认10分钟，在**设置** > **全局设置** > **高级设置**中，修改**物理机内存使用率最低采集间隔**参数，更改数据采集时间。
  - **运行云主机最大数量**：用户需要先设置物理机最多运行云主机的数量，然后系统会筛选出满足此要求的物理机来创建云主机。如果没有满足条件的物理机，那么云主机创建失败
- **策略模式**：物理机分配策略选择CPU使用率最低或内存使用率最低时需要选择该项，包括非强制和强制两种策略模式

  注:

  - **分配策略(非强制)**：若查询不到物理机负载信息，则随机分配资源足够的物理机创建云主机
  - **分配策略(强制)**：若查询不到物理机负载信息，则无法创建云主机
- **磁盘带宽**：可选项，可设置云主机根云盘的IO带宽上限。为空时，代表不限制IO带宽。基本单位包括：MB/s、GB/s、TB/s
- **上行网络带宽**：可选项，可设置从云主机上上传的网络带宽的上限。为空时，代表不限制上行网络带宽。基本单位包括：Kbps、Mbps、Gbps

- **下行网络带宽**：可选项，可设置从云主机上下载的网络带宽的上限。为空时，代表不限制下载网络带宽。基本单位包括：Kbps、Mbps、Gbps

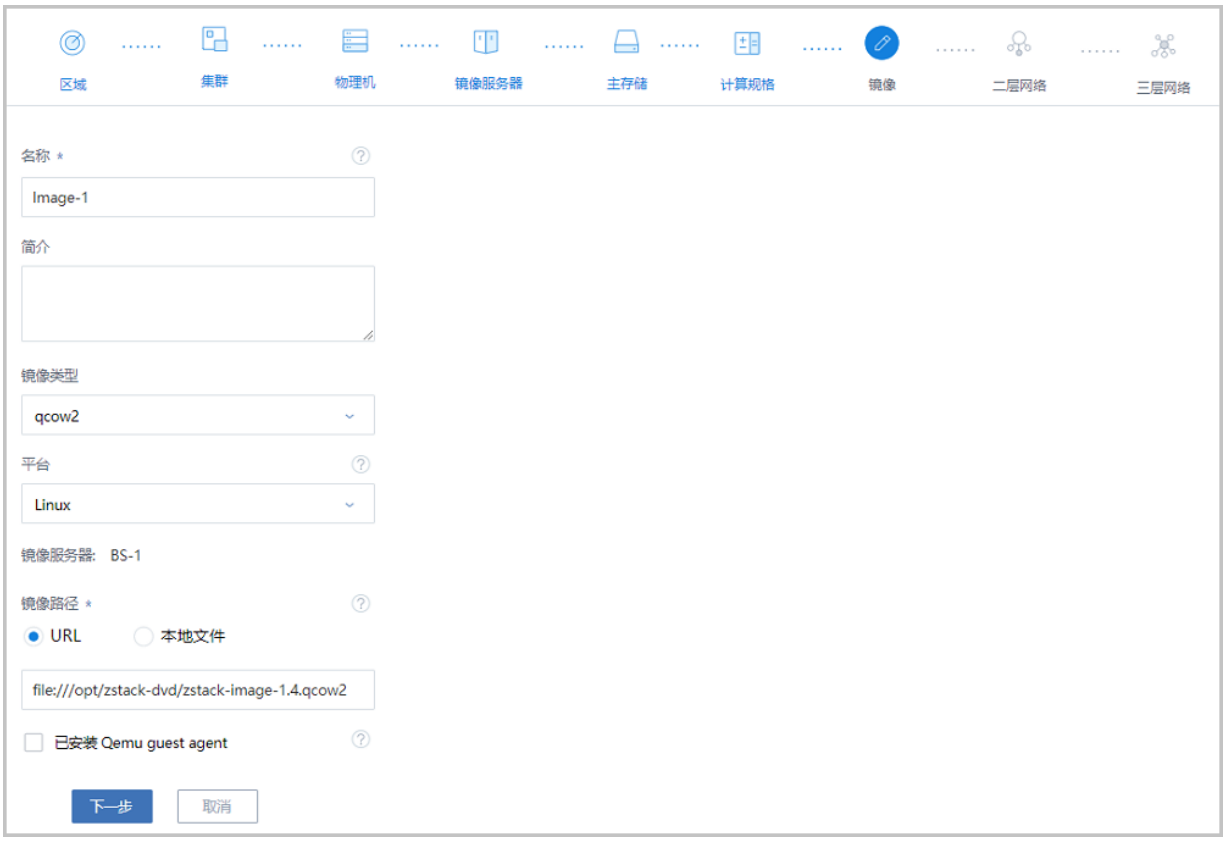
点击**下一步**按钮，完成计算规格创建。

6.7 添加镜像

背景信息

如图 *87: 添加镜像*所示：

图 87: 添加镜像



操作步骤

1. 输入云主机镜像的**名称**。
2. 输入云主机镜像的**简介**，可简述云主机镜像相关信息进行备注。
3. 在**镜像类型**的下拉框选择相应的镜像类型，包括qcow2、raw和ISO。需根据镜像的文件属性选择正确的选项。
4. 在**平台**的下拉框选择相应的平台类型，包括：
   Linux、Windows、WindowsVirtio、Other、Paravirtualization。

5. **镜像服务器**默认为本Wizard引导设置过程中创建的镜像服务器。

注:

- 请务必确保被导入的镜像已安装Qemu guest agent，并已设置为自启动。
- 满足以上条件后，勾选**Qemu guest agent**选项，则由添加的镜像创建出来的云主机，以及该云主机克隆生成的云主机或创建的镜像，可在运行状态下从外部修改云主机密码。

6. **镜像路径**中选择URL或本地文件方式上传镜像。

- **URL**：采用指定的URL路径来添加镜像。
  - 支持*HTTP/HTTPS*方式：
    - 填写格式为：*http://path/file*或*https://path/file*
    - 例如：*http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2*
  - 支持*FTP*方式：
    - 匿名模式：*ftp://hostname[:port]/path/file*

      例如：*ftp://172.20.0.10/pub/zstack-image.qcow2*
    - 非匿名模式：*ftp://user:password@hostname[:port]/path/file*

      例如：*ftp://zstack:password@172.20.0.10/pub/zstack-image.qcow2*
  - 支持*SFTP*方式：
    - 指定密码模式：*sftp://user:password@hostname[:port]/path/file*

      例如：*sftp://root:password@172.20.0.10/pub/zstack-image.qcow2*
    - 免密模式：*sftp://user@hostname[:port]/path/file*

      例如：*sftp://root@172.20.0.10/pub/zstack-image.qcow2*
  - 镜像服务器上的绝对路径，支持Sftp镜像服务器和镜像仓库

    例如：*file:///opt/zstack-dvd/zstack-image-1.4.qcow2*

注:

- 输入URL时，需确保可被镜像服务器访问，且存在此镜像文件。
- 使用*SFTP*免密模式上传镜像时，需提前确保镜像服务器与Sftp服务器可互相SSH免密登录。
- 关于平滑连续进度条显示和断点续传：

  - 若使用镜像仓库，支持平滑连续进度条显示，且支持断点续传；
  - 若使用Ceph或FusionStor镜像服务器，支持平滑连续进度条显示，不支持断点续传；
  - 若使用Sftp镜像服务器，不支持平滑连续进度显示，且不支持断点续传。
- 关于*file:///*方式上传镜像
  - 若使用Ceph或FusionStor镜像服务器，目前暂不支持*file:///*格式的输入；
  - *file:///*是三个/，对应的路径应为镜像服务器的**绝对路径**，例如*file:///opt/zstack-dvd/zstack-image-1.4.qcow2*，在镜像服务器的*/opt/zstack-dvd*目录下应存放有*zstack-image-1.4.qcow2*文件。

- **本地文件**：选择当前浏览器可访问的镜像直接上传，支持镜像仓库。

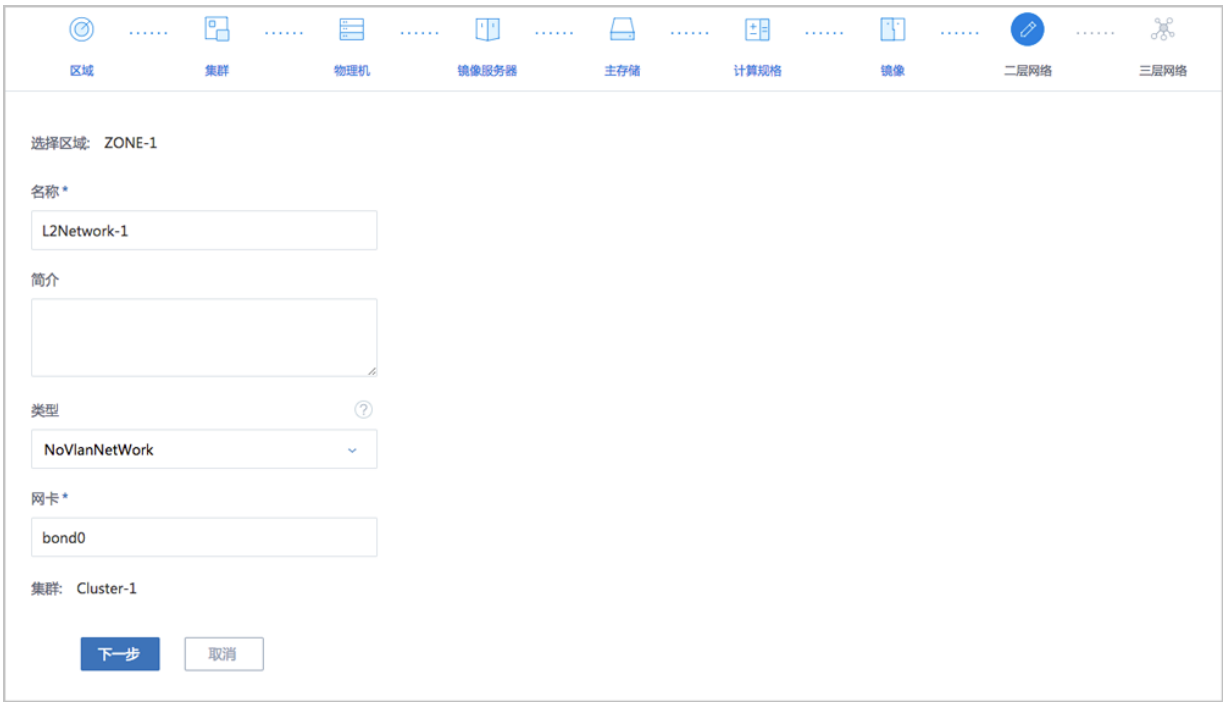
7. **已安装 Qemu guest agent**：勾选表示镜像已安装了qemu-guest-agent，创建出的云主机默认支持在线修改密码。
8. 点击**下一步**，系统会创建下载对应的云主机镜像文件，下载过程会在后台进行。

6.8 创建二层网络

背景信息

如图 *88:* 创建二层网络所示：

图 88: 创建二层网络



操作步骤

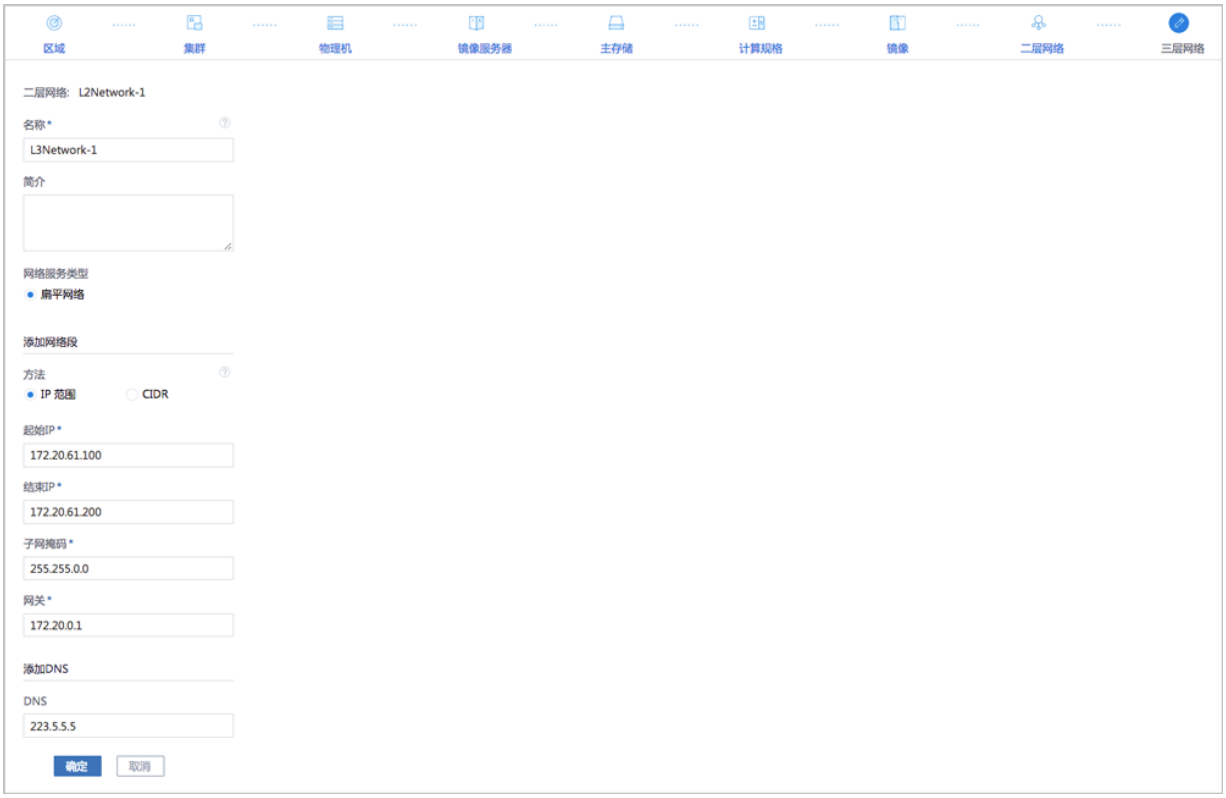
1. 输入二层网络的**名称**。
2. 输入二层网络的**简介**，可简述二层网络相关信息进行备注。
3. 在**类型**的下拉可选框，选择需要使用的网络类型。
   - **L2NoVlanNetwork**
     - 若不打算使用Vlan网络，则选择L2NoVlanNetwork。
     - NoVlaNetwork模式下，指定的网卡连接交换机网口必须是Access模式。
     - 在**网卡**输入框输入对应计算节点的网卡设备。
     - **集群**默认为本Wizard引导设置过程中创建的集群。
   - **L2VlanNetwork**
     - 若需要ZStack帮助配置VLAN网络，则需选择L2VlanNetwork。
     - VlanNetwork模式下，指定的网卡连接交换机网口必须是Trunk模式。
     - 输入**Vlan ID**，可输入1~4094之间的数字，需与交换机配置相同。
     - 在**网卡**输入框输入对应计算节点的网卡设备。
     - **集群**默认为本Wizard引导设置过程中创建的集群。
4. 点击**下一步**，创建二层网络。

6.9 创建三层网络

背景信息

如图 *89:* 创建三层网路所示：

图 89: 创建三层网路



操作步骤

1. **二层网络**默认为本Wizard引导设置过程中创建的二层网络。
2. 输入三层网络的**名称**。
3. **网络服务类型**默认为扁平网络类型。
4. **添加网络段**的方法有：**IP范围**和**CIDR**两种。
   - **IP范围**
     - 需要依次输入**起始IP**、**结束IP**、**子网掩码**、**网关**。例如可填写类似*172.20.61.100*到*172.20.61.200*，子网掩码填写*255.255.0.0*，网关填写*172.20.0.1*。
     - 添加**DNS**：添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*等。
   - **CIDR**
     - **CIDR**一般填写类似*192.168.1.0/24*。

- 添加**DNS**：添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*等。

5. 点击**下一步**，系统将创建三层网络。

后续操作

至此，Wizard引导设置全部完成。

7 云平台操作指南

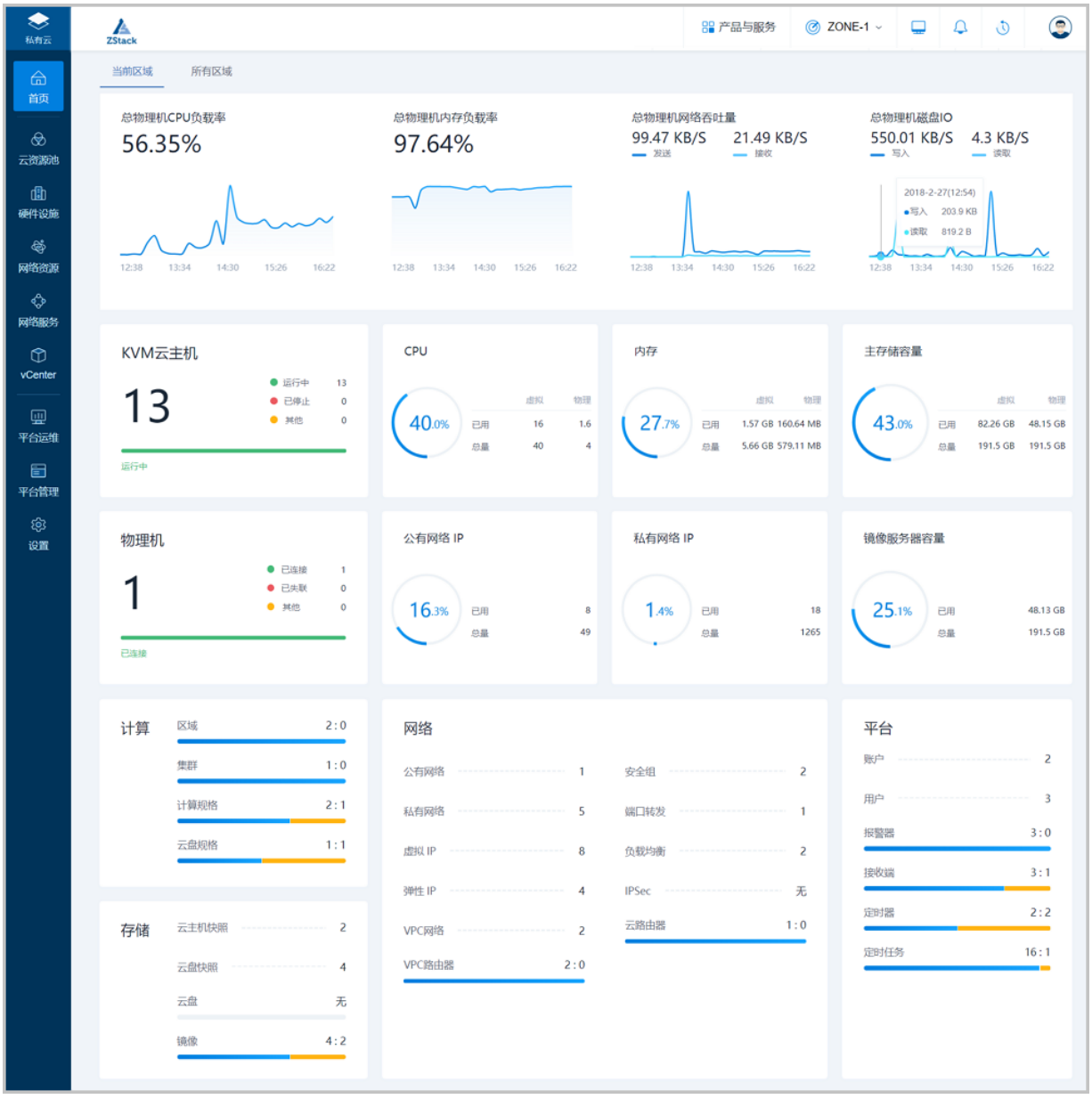
本章主要介绍admin对ZStack私有云平台进行管理运维的各种操作。

7.1 首页

在ZStack私有云主菜单，点击**首页**，进入**首页**界面。

如图 *90:* 首页所示：

图 90: 首页



首页主要对当前区域/所有区域的数据中心资源实时状态进行统一直观展示。

首页界面分为**当前区域**和**所有区域**两个子页面，可点击图标切换页面，查看所选区域物理机资源利用率及主要资源的使用情况。

首页主要分为四大部分：

- **总物理主机资源使用率及性能监控**

  通过对当前区域/所有区域的全部物理主机CPU、内存、磁盘、网络资源使用情况进行统计分析，以全部物理主机的总CPU负载压力、总内存负载压力、总网络吞吐性能、以及总磁盘IO性能为指标，分别进行实时展示监控。实时显示的数据结合动态曲线图，可直观告知用户当前全部物理主机的整体资源使用状态以及性能状态。

- **KVM云主机、物理主机的运行状态统计**

  通过对当前区域/所有区域的全部KVM云主机、物理主机运行状态进行统计分析，对处于各状态的资源数量进行实时展示监控，并结合进度条的绿、红、黄比例提示，可直观告知用户当前全部KVM云主机、物理主机的运行情况。

  - **绿色**：表示运行中状态。
  - **红色**：表示已停止状态。
  - **黄色**：表示其他状态。比如：KVM云主机的启动中、重启中；物理机的未知、已失联、进入维护模式等。

- **CPU、内存、主存储、镜像服务器、公网IP、私网IP的实时资源用量统计**

  通过对当前区域/所有区域的相关物理资源使用情况进行统计分析，挑选出CPU、内存、主存储、镜像服务器、公网IP、私网IP等资源，对它们的资源用量分别进行实时展示监控，实时显示的百分比结合进度条的蓝、黄、红三色提示可直观告知用户当前资源的使用量。同时提供详实的数据（已用/总量、虚拟/物理）供用户参考。

  - **蓝色**：小于60%时，显示为蓝色。
  - **黄色**：大于等于60%并且小于80%时，显示为黄色。
  - **红色**：大于等于80%时，显示为红色。

- **计算、存储、网络、平台的资源可用性统计**

  通过对当前区域/所有区域数据中心的计算、存储、网络、平台的相关资源可用性进行统计分析，对各资源以可用资源数量与不可用资源数量之比的形式进行实时展示监控，并结合进度条的蓝、黄比例提示，可直观告知用户当前资源的可用情况。

  - **蓝色**：表示可用资源。

- **黄色**：表示不可用资源。

在UI界面右上角从左到右的按钮依次为：产品与服务快速入口按钮、区域切换按钮、大屏监控入口按钮、工单消息按钮（Plus）、最近消息按钮、最近操作按钮、个人中心按钮，如图 *91: UI界面右上角按钮*所示（已安装企业管理模块许可证）：

图 91: UI界面右上角按钮

- **产品与服务快速入口**：基于UI Map为用户提供了ZStack私有云全局资源概览，详情可参考产品与服务快速入口章节。
- **区域切换**：可选择不同区域进行切换。
- **大屏监控入口**：可在新页面打开大屏监控，对所有区域的数据中心实时资源状态进行统一直观展示，详情可参考大屏监控章节。
- **工单消息**（Plus）：若已安装企业管理模块许可证，可查看未处理的工单信息，并可跳转至工单管理界面处理工单，详情可参考企业管理*(Plus)*的工单管理章节。
- **最近消息**：可查看最近消息，并可跳转至**消息中心**查看全部报警消息。
- **最近操作**：可查看最近进行中操作日志和已完成操作日志，并可跳转至**操作日志**查看全部操作日志。
- **个人中心**：支持修改登录密码、UI界面语言切换、跳转查看常见问题解答/关于界面、以及登出操作。
  - **常见问题解答**：跳转至ZStack官网常见问题界面，获取最新FAQ帮助。
  - **关于**：跳转至**关于**界面，显示了当前软件的授权协议、版本、授权状态和请求码等信息，并提供许可证本地上传以及删除功能，详情可参考关于章节。

7.1.1 产品与服务快速入口

在UI界面右上角点击**产品与服务**按钮，展开**产品与服务**界面，可以看到私有云快速导航入口。

私有云导航界面如图 *92: ZStack私有云快速导航*所示（已安装企业管理模块许可证）：

图 92: ZStack私有云快速导航

该界面基于UI Map提供了ZStack私有云全局资源概览，十分直观清晰。用户可点击某资源项快速跳转该资源主界面，同时每个资源项后的五角星可设置高亮，用户可按需进行高亮标注。

7.1.2 大屏监控

ZStack支持数据中心大屏监控功能。

如图 *93:* 大屏监控入口所示（已安装企业管理模块许可证），点击UI界面右上角的大屏监控入口按钮，可在新页面打开大屏监控，对所有区域的数据中心实时资源状态进行统一直观展示，如图 *94:* 大屏监控界面所示：

图 93: 大屏监控入口

图 94: 大屏监控界面

大屏监控主要分为四大部分：

1. 左侧：Top5云主机CPU负载、Top5云主机内存负载、Top5物理机CPU负载、Top5物理机内存负载

   通过对所有区域数据中心的云主机、物理机的CPU、内存资源使用情况进行统计分析，以云主机CPU负载、云主机内存负载、物理机CPU负载、物理机内存负载为指标，分别挑选出各指标下负载压力最高的前五台机器，进行实时展示监控。实时显示的百分比排行榜结合进度条的蓝、黄、红三色提示，可直观告知用户当前哪些机器资源告急。

   如图 *95: 云主机、物理机负载压力最高的实时Top5*所示：

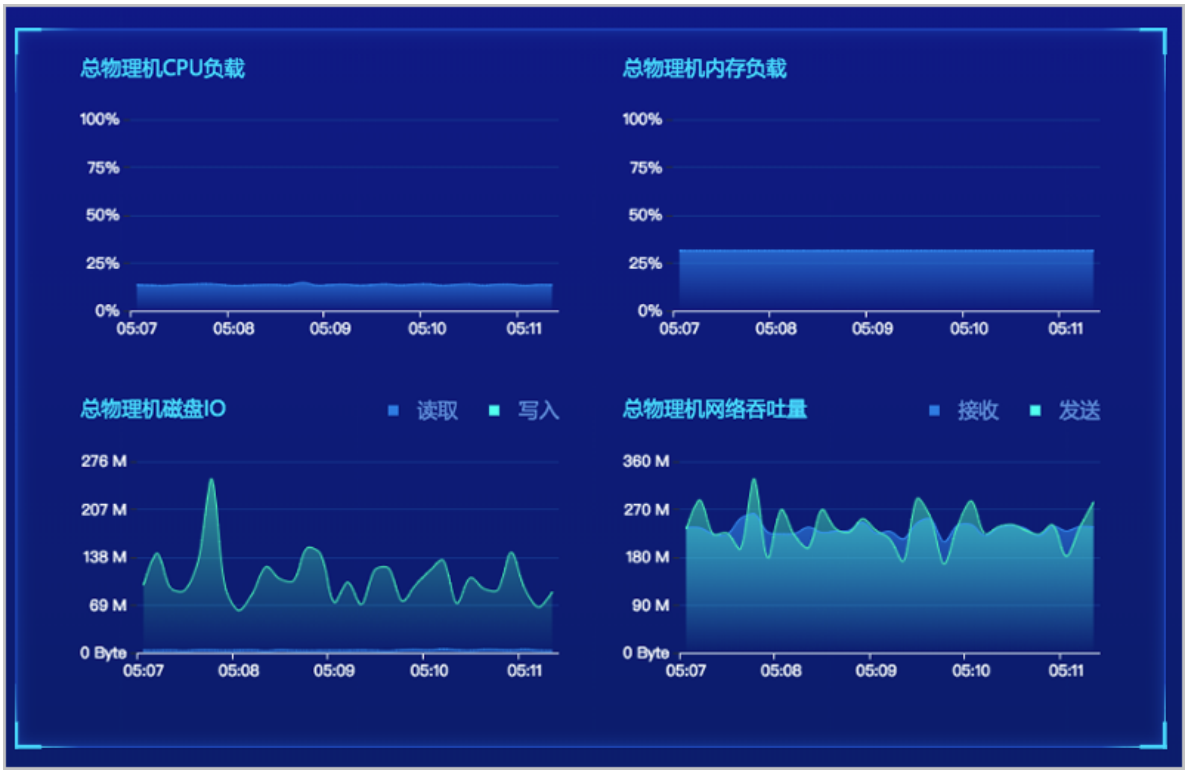
   图 95: 云主机、物理机负载压力最高的实时Top5

2. 中间上侧：总物理机的CPU负载、内存负载、磁盘IO、网络吞吐量

   通过对所有区域数据中心的全部物理机的CPU、内存、磁盘、网络资源使用情况进行统计分析，以全部物理机的总CPU负载压力、总内存负载压力、总磁盘IO性能、以及总网络吞吐性能为指标，分别进行实时展示监控。实时显示的动态曲线图结合不同监控项目的颜色区分，可直观告知用户当前全部物理机的整体资源使用状态以及性能状态。

   如图 *96:* 总物理机的实时资源使用率和性能监控所示：

   图 96: 总物理机的实时资源使用率和性能监控

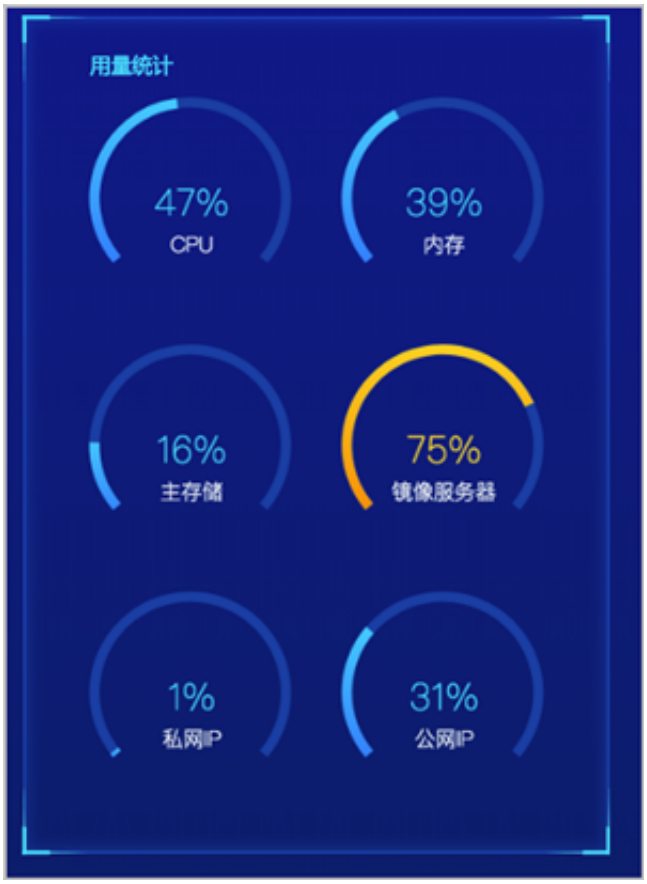


3. 右侧：CPU、内存、主存储、镜像服务器、私网IP、公网IP的实时资源用量统计

   通过对所有区域数据中心的相关物理资源使用情况进行统计分析，挑选出CPU、内存、主存储、镜像服务器、私网IP、公网IP等资源，对它们的资源用量分别进行实时展示监控，实时显示的百分比结合进度条的蓝、黄、红三色提示可直观告知用户当前资源的使用量。

   如图 *97: 物理资源实时用量统计*所示：

   图 97: 物理资源实时用量统计



4. 下侧：云主机、物理机、镜像、集群的实时资源总览

   通过对所有区域数据中心的云主机、物理机、镜像、集群等资源使用情况进行统计分析，对它们的资源总用量分别进行实时展示监控。

   如图 *98: 云主机、物理机、镜像、集群的实时资源总览*所示：

   图 98: 云主机、物理机、镜像、集群的实时资源总览

大屏标题支持自定义编辑，点击**设置 > 自定义UI**，在**自定义UI**界面编辑即可。详情请参考*自定义UI*章节。

注:

系统登入或登出，大屏不受影响，保持持续展示，数据实时刷新。

7.1.3 关于

如图 *99: 个人中心*所示（已安装企业管理模块许可证），在UI界面右上角点击**个人中心** > **关于**，展开**关于**界面，显示了当前软件的授权协议、版本、授权状态和请求码等信息，并提供许可证本地上传以及删除功能，如图 *100: 关于界面*所示：

图 99: 个人中心

图 100: 关于界面

授权协议说明

ZStack提供多种**授权协议**，主要分为云平台许可证（Base License）和模块许可证（Plus License）两大类。

- **云平台许可证**（Base **License**）：
  - 提供云平台核心基本功能，可满足用户主流业务场景需求；
  - 主要包括：企业版许可证、混合云版许可证。

- **模块许可证**（Plus **License**）：
  - 提供附加功能或功能强化，可满足用户特定业务场景需求；
  - 主要包括：企业管理模块、VMware管理模块许可证。

具体授权协议说明如表 *1:* 授权协议说明所示：

表 1: 授权协议说明

基本类型	授权协议		授权协议说明
——	社区版		• 免费使用； • 不限计算节点数量； • 不限授权期限； • 仅限使用ZStack私有云的部分功能； • 不提供官方售后技术支持服务； • 不适合用于企业生产环境，推荐社区爱好者做技术研究使用。
云平台许可证（Base **License**）	企业版	企业版（试用许可证）	• 免费使用； • 可以添加许可证指定数量CPU的物理机； • 在许可证授权期限内可使用ZStack私有云的全部功能； • 不提供官方售后技术支持服务。
		企业版（无限期免费许可证）	• 免费使用； • 可以免费添加1台物理机； • 可无限期使用ZStack私有云的全部功能； • 不提供官方售后技术支持服务。
		企业版（付费许可证）	• 付费授权使用； • 可管理的计算节点数量按购买的物理CPU颗数计算； • 在许可证授权期限内可使用ZStack私有云的全部功能； • 在售后服务期内可获得官方售后技术支持服务； • 适于企业部署生产环境的私有云。
	混合云版		• ZStack和阿里云联合推出的ZStack for Alibaba Cloud，付费授权使用；

基本类型	授权协议	授权协议说明
		• 可管理的计算节点数量按购买的物理CPU颗数计算； • 在许可证授权期限内可使用ZStack私有云的全部功能以及"阿里云-ZStack"混合云的全部功能； • 在售后服务期内可获得官方售后技术支持服务； • 适于企业部署生产环境的私有云和混合云。
模块许可证（Plus License）	企业管理	• 付费授权使用； • 需购买云平台许可证（Base License）基础上使用，不可单独使用； • 在许可证授权期限内可使用企业管理模块的全部功能，包括：管理项目、组织架构、用户、权限，以及云平台运营相关的功能； • 在售后服务期内可获得官方售后技术支持服务。
	VMware管理	• 付费授权使用； • 需购买云平台许可证（Base License）基础上使用，不可单独使用； • 在许可证授权期限内可为VMware计算节点提供独立的CPU授权，若未授权或超额，则使用KVM的授权CPU； • 在售后服务期内可获得官方售后技术支持服务。

注:

- 如您需要试用企业版或打算购买付费企业版，请点击**请求码**后面的 ，将您的请求码和您的需求发送电子邮件至 sales@zstack.io，我们将尽快与您联系。
- 欢迎您直接与**sales@zstack.io**咨询购买的相关事宜。
- 如您需要升级到其它版本或更新许可证，请将您的请求码和升级需求发送电子邮件至**sales@zstack.io**，我们将尽快与您联系。

导入许可证

如果您已获得新的许可证，可点击**关于**界面右上角的**上传许可证**按钮，弹出**上传许可证**界面，直接将获得的新许可证本地上传即可，如图 *101:* 本地上传许可证所示：

图 101: 本地上传许可证

注:

- 支持依次上传云平台许可证（Base License）以及模块许可证（Plus License）。
- 可点击**关于**界面右上角的刷新按钮，重新加载许可证。
- 可点击**关于**界面右上角的删除按钮，删除已加载的许可证。
- 仅admin拥有加载和删除许可证的权限。

许可证到期提醒

- 当许可证剩余使用期限不足14天时，登录云平台后智能操作助手将弹出**许可证即将过期**的提醒信息。
  - 点击**暂不处理**，提醒信息暂时关闭。
  - 点击**查看详情**，将直接跳转至**关于**界面。为不影响您的正常使用，请尽快联系云平台相关服务人员进行续费，以继续使用本产品。

  如图 *102:* 许可证即将过期所示：

  图 102: 许可证即将过期

- 当许可证已经过期，登录云平台后将自动跳转至**关于**界面。为不影响您的正常使用，请尽快联系云平台相关服务人员进行续费，以继续使用本产品。

  如图 *103:* 许可证已过期所示：

  图 103: 许可证已过期

注:

- 若您的云平台许可证（Base License）已过期，云平台上原有业务依然正常运行，但请勿做任何操作（如重连物理主机、重连镜像服务器、重连主存储等均无法重连成功），以免影响业务运行！
- 若您的模块许可证（Plus License）已过期，该模块提供的全部功能将不可使用。例如，若您的企业管理模块许可证已过期，项目登录界面将锁定，并提示：**许可证已过期，请联系云平台管理员。**
- 若您的云平台许可证（Base License）已过期，但模块许可证（Plus License）仍在授权期限内，您可查看该模块涉及的相关资源，但不可操作资源。例如，若您的企业版许可证已过期，但企业管理模块许可证仍在授权期限内，您可从项目登录入口登录云平台，但不可操作相关资源。

7.2 云资源池

在云资源池中，主要涉及以下内容：

- 云主机：在计算节点创建的虚拟机实例
- 云盘：云主机所使用的数据盘，可提供额外存储空间
- 镜像：云主机所使用的镜像模板文件
- 亲和组：云主机和物理机绑定关系的简单编排策略。
- 计算规格：指定云主机的CPU、内存、IO带宽等规格定义
- 云盘规格：指定云主机的数据云盘的容量大小定义

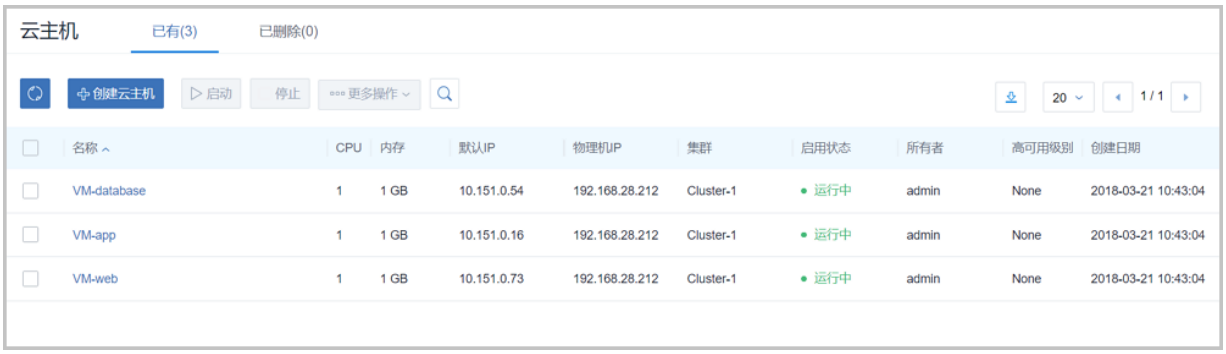
7.2.1 云主机

云主机：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，是ZStack的核心组成部分。

7.2.1.1 云主机管理

在ZStack私有云主菜单，点击**云资源池** > **云主机**按钮，可以进入**云主机**管理界面，如图 *104:* 云主机管理界面所示。

图 104: 云主机管理界面



云主机界面分为两栏：

- **已有**：在此界面，可以查看运行或者停止状态的云主机列表信息，并对云主机进行创建、启动、停止、重启和打开控制台等操作。
- **已删除**：在此界面，可以查看删除状态的云主机列表信息，并对云主机进行恢复或者彻底删除的操作。

云主机界面，支持以下操作：

- **搜索**：点击**搜索**按钮，用户可以根据云主机的名称、UUID、IP地址、物理机IP、用户标签、弹性IP、计算规格名称、所有者以及高级搜索进行快速搜索云主机。
- **导出csv**：点击右上方的**导出csv**图标，用户可按需导出当前页面或全部页面的云主机列表。
- **列表数**：点击**列表数**按钮，用户可以选择每一页显示的云主机数量。

7.2.1.2 创建云主机

7.2.1.2.1 创建单个云主机

背景信息

ZStack云管理平台支持云主机的单个/批量创建，本节主要介绍创建单个云主机。

在**云主机**管理界面，点击**创建云主机**按钮，弹出**创建云主机**界面，如图 *105:* 创建云主机所示，可快速创建单个云主机。

图 105: 创建云主机

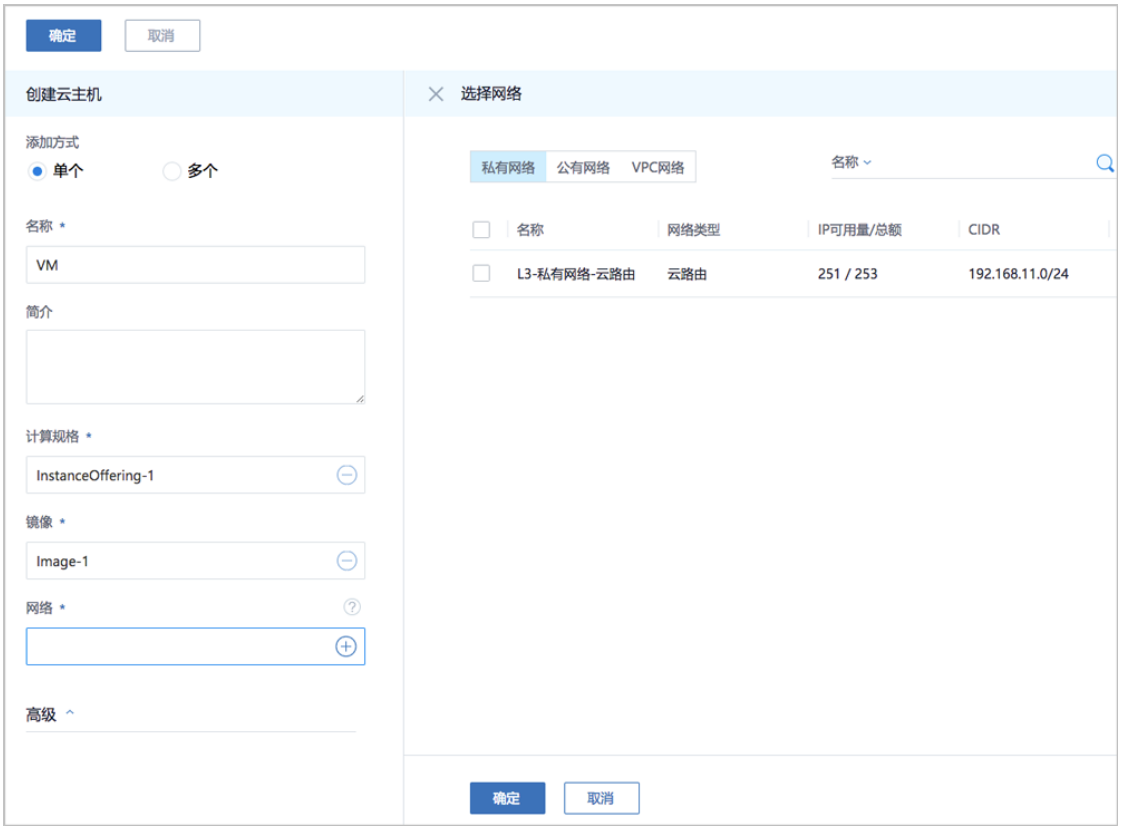
操作步骤

1. **添加方式**：单个
2. **名称**：输入云主机名称，支持重名
3. **简介**：可选项，可留空不填
4. **计算规格**：选择合适的计算规格
5. **镜像**：选择创建云主机的镜像
6. **根云盘规格**：选择创建云主机的根云盘容量。添加镜像为ISO类型时，需要选择根云盘规格；添加镜像为Image类型时，不出现此选项

7. **网络**：选择创建云主机的网络

   1. 支持使用私有网络、公有网络和VPC网络创建云主机，如图 *106: 支持私有网络、公有网络和VPC网络*所示：

      图 106: 支持私有网络、公有网络和VPC网络



   2. 选择镜像后，如果镜像所在集群只有一个网络可用，将默认选择此网络。
   3. 选择镜像后，如果镜像所在集群有多个网络可用，支持同时选择多个网络，如图 *107: 选择多个网络*所示。点击**确定**后，**网络**项将显示全部已选网络，此时可选择其中一个作为默认网络。

      图 107: 选择多个网络

4. 设置网卡：选定云主机网络后，系统支持设置云主机的静态IP地址和MAC地址。

   点击**网络**项下方的**设置网卡**按钮，可指定静态IP地址和MAC地址，如图 *108:* 设置网卡所示：

注: 设置静态IP地址时，系统会显示5个可用IP提示。如果当前IP段可用数量不足5个，则显示全部可用IP。

图 108: 设置网卡

8. 至此，创建云主机的基本设置已经完成，可点击**创建云主机**界面上方的**确定**按钮，创建云主机。

   云主机创建成功后，可在**云主机**界面选择该云主机，点击**更多操作** > **打开控制台**，访问云主机系统。

9. **高级设置**：创建云主机时，如希望配置高级设置，点击**高级**按钮进行配置，高级配置选项均为可选项。

   如图 *109:* 高级设置界面所示：

   图 109: 高级设置界面

确定
取消
创建云主机
高级
数据云盘规格
40G
亲和组
亲和组-1
集群
Cluster-1
数据云盘主存储
PS-1
根云盘主存储
PS-1
物理机
Host-1
GPU设备
Advanced Micro Devices, Inc. [AMD/ATI], D...
高可用级别
None
控制台密码
SSH 公钥
User Data
USB 重定向
控制台模式
vnc
spice

a) 数据云盘规格：

- 创建云主机时，给云主机直接创建并加载数据云盘。
- 点击数据云盘规格右侧的+按钮，在弹出的新界面中选择启动云主机使用的云盘规格。
- 如果云盘规格列表为空，则需参考创建云盘规格进行创建。

b) 亲和组：

- 创建云主机时，选择创建的亲和组。
- 点击亲和组右侧的+按钮，在弹出的新界面中选择可用亲和组。

c) 集群：

- 选择指定启动云主机的物理机所在的集群。
- 点击集群右侧的+按钮，在弹出的新界面中选择可用集群。

d) 数据云盘主存储：

- 指定云主机的数据云盘主存储。
- 点击数据云盘主存储右侧的+按钮，在弹出的新界面中选择可用的数据云盘主存储。

注:

ZStack支持一个集群挂载多个主存储，详情可参考集群章节的集群 | 主存储。

创建云主机时多主存储分配策略：

- 一个集群挂载多个本地主存储：
  - 创建云主机可指定任意的本地主存储。
  - 如不指定主存储，系统将自动选择可用容量最充足的本地主存储。
- 一个集群挂载多个共享主存储（目前支持多个NFS主存储、多个Shared Block主存储）：
  - 创建云主机可指定任意的NFS或Shared Block主存储。
  - 如不指定步主存储，系统将随机分配可用的NFS或Shared Block主存储。
- 一个集群挂载混合主存储（目前支持1个LocalStorage + 1个NFS、1个LocalStorage + 1个SMP、1个LocalStorage + 1个Shared Block）：
  - 创建云主机可指定任意的主存储。

- 如果创建云主机的同时创建并加载数据云盘，则需指定数据云盘所使用的主存储。
- 如不指定主存储，系统将默认使用本地主存储来创建云主机。

e) 根云盘主存储：

- 指定云主机的根云盘主存储。
- 点击根云盘主存储右侧的+按钮，在弹出的新界面中选择可用的根云盘主存储。

f) 物理机：

- 选择指定的物理机来启动云主机。
- 点击物理机右侧的+按钮，在弹出的新界面中选择启动云主机使用的物理机资源，如果已经选择了集群，只能选择该集群所在的物理机。

注: 建议单台物理机上所建云主机数量不要超过400台。

g) GPU设备:

- 创建云主机时，可选择物理机透传的GPU设备直接加载到云主机。
- 需提前在物理机BIOS中开启Intel VT-d或AMD IOMMU，且在物理机内核开启IOMMU支持，确保物理机可正常使用GPU设备透传功能。
- 支持加载多个不同类型的GPU设备到云主机。
- 不能跨物理机加载GPU设备到云主机。

注: 关于GPU透传功能的详情请参考《GPU及USB设备透传使用教程》的*GPU透传*章节。

h) 高可用级别：

高可用级别支持NeverStop、None两种模式设置。

- **None**：代表不设置高可用
- **NeverStop**：表示云主机永不停机

i) 控制台密码：

设置控制台密码（VNC密码），长度为6-18位。

j) SSH公钥：

如果预先制作了带有Cloud-init功能的镜像文件，还可输入SSH公钥，可实现创建云主机后，SSH免密码登录。详情请参考*SSH公钥管理*章节。

k) User Data：

支持导入User Data，即用户自定义数据，通过上传自定义的参数或脚本，对主机做一些定制化配置或完成特定任务。

注:

导入User Data前，需确保Userdata网络服务、DHCP网络服务均可正常使用。

- 默认情况下，扁平网络/云路由网络/VPC网络环境下，Userdata网络服务、DHCP网络服务均启用。

- Linux云主机导入User Data
  - Linux云主机导入User Data，云主机镜像需提前安装Cloud-Init；
  - Linux云主机导入User Data样例：

```
#cloud-config
users:
 - name: test
   shell: /bin/bash
   groups: users
   sudo: ['ALL=(ALL) NOPASSWD:ALL']
   ssh-authorized-keys:
       - ssh-rsa AAAAB3NzaC1LXCJfjroD1IT root@10-0-0-18
bootcmd:
 - mkdir /tmp/temp
write_files:
 - path: /tmp/ZStack_config
   content: |
       Hello,world!
   permissions: '0755'
hostname: Perf-test
disable_root: false
ssh_pwauth: yes
chpasswd:
  list: |
      root:word
  expire: False
runcmd:
 - echo ls -l / >/root/list.sh
```

上述样例脚本实现以下功能：

1. 创建云主机时，创建用户test，使用ssh-key；
2. 开机写入文件*/etc/hosts*，创建*/tmp/temp*目录，并创建文件写入内容；
3. 设置hostname，开启root用户，允许ssh密码登录，修改root密码；
4. 执行`echo ls -l /`命令。

  - Windows云主机导入User Data

- Windows云主机导入User Data，云主机镜像需提前安装Cloudbase-Init，具体安装方法可参考*Cloudbase*官方文档。
- Windows云主机导入User Data样例：

```
#cloud-config
write_files:
  - encoding: b64
    content: NDI=
    path: C:\b64
    permissions: '0644'
  - encoding: base64
    content: NDI=
    path: C:\b64_1
    permissions: '0644'
  - encoding: gzip
    content: !!binary |
      H4sIAGUfoFQC/zMxAgCIsCQyAgAAAA==
    path: C:\gzip
    permissions: '0644'
```

上述样例脚本实现以下功能：

- 云主机启动过程中，在c盘下创建**b64**、**b64_1**、**gzip**三个文件。

l) USB重定向：

ZStack兼容多种USB设备重定向，当用户需要使用VDI功能时，需要勾选此项，将VDI客户端的USB设备重定向给VDI云主机。

m) 控制台模式：

打开控制台使用的模式，可选项：vnc和spice。

7.2.1.2.2 批量创建云主机

操作步骤

1. 在**云主机**管理界面，点击**创建云主机**按钮，弹出**创建云主机**界面。

   如图 *110:* 批量创建云主机界面所示：

   图 110: 批量创建云主机界面

2. **添加方式**：多个。
3. **创建数量**：输入需要批量创建云主机的数量。
4. **名称**：输入云主机名称，多个云主机的名字以数字加后缀进行区分，例如，输入VM，则云主机名字以VM-1，VM-2依序排列。
5. **简介**：可选项，可留空不填。

6. **计算规格**：点击右侧+按钮选择合适的计算规格。
7. **镜像**：点击右侧+按钮选择合适的云主机镜像。
8. **网络**：点击右侧+按钮选择合适的云主机网络。
9. 点击**确定**按钮，进行批量创建云主机。

注:

- 需等待一段时间后，批量创建的云主机会在**云主机**管理界面以列表形式显示。
- 由于计算节点能力不同，并行创建大量云主机时，可能导致每一个云主机启动时间变得很长。
- 并发创建云主机的数量最好结合计算节点的数量以及计算节点的能力进行综合考虑。
- 如果创建的云主机数量所占用的资源超过系统可用资源（CPU、内存、存储、网络），则ZStack会根据系统中最少的资源量来并发创建云主机的数量。

7.2.1.3 云主机操作

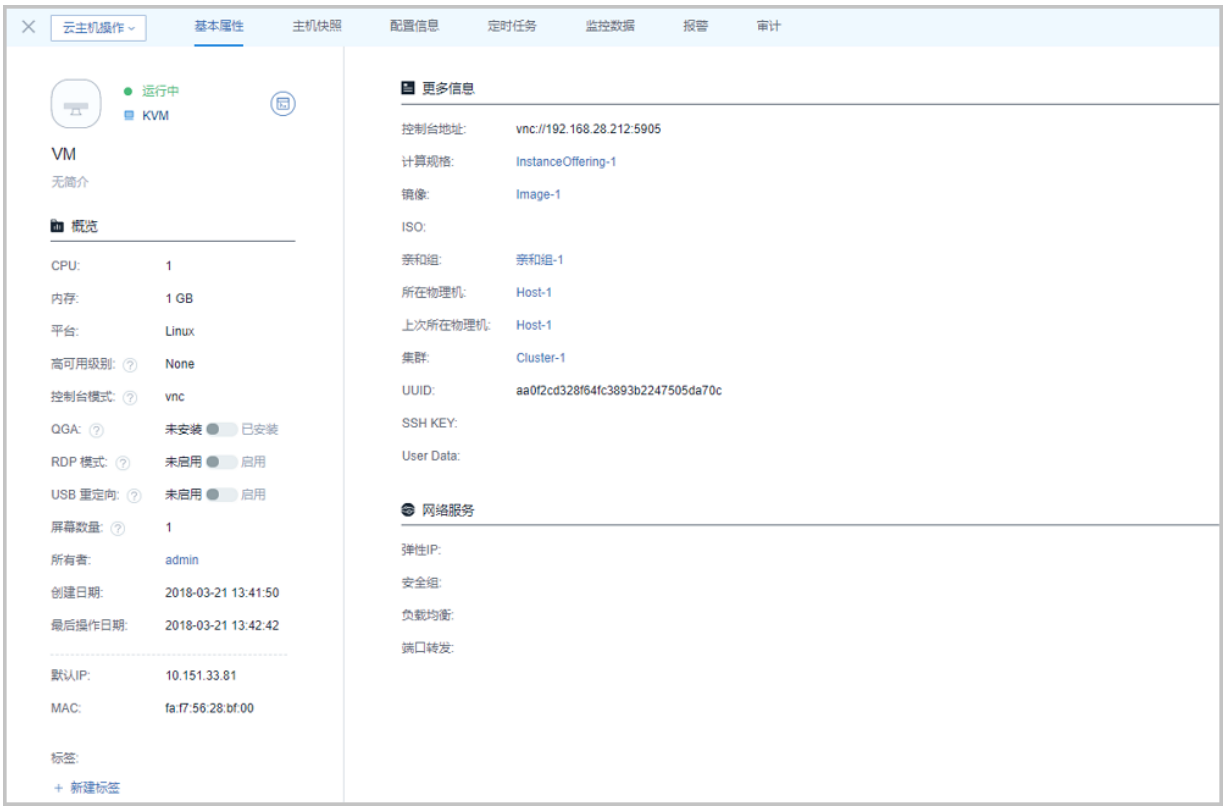
7.2.1.3.1 单个云主机操作

在**云主机**界面，点击相应云主机名称，可展开云主机详情页。

- 目前包括以下子栏：基本属性、主机快照、配置信息、定时任务、监控数据、报警和审计。
- 云主机详情页左上角有**云主机操作**按钮，可对当前云主机进行操作，所含操作菜单是云主机管理界面上对云主机所有操作的合集。

如图 *111:* 云主机详情页所示：

图 111: 云主机详情页



云主机支持多种操作，依据不同的约束条件可支持的操作不同

- **运行中**的云主机：

  停止、重启、暂停、恢复、关闭电源、打开控制台、克隆、创建镜像、创建快照、删除快照、创建灾备数据（混合云版支持）、创建云盘、加载云盘、卸载云盘、云盘扩容、创建云盘镜像、设置云盘QoS、取消云盘QoS、删除云盘、加载ISO、卸载ISO、添加SSH KEY、删除SSH KEY、设置高可用、修改计算规格、设置启动顺序、设置控制台密码、取消控制台密码、更改所有者、设置RDP模式、设置USB重定向、修改云主机密码、系统扩容、切换控制台模式、删除、绑定亲和组、解绑亲和组、设置名称和简介、设置平台类型、设置QGA状态、设置VDI设备最多支持的屏幕数量、设置用户标签、加载网卡、卸载网卡、设置静态IP、取消静态IP、设置网卡QoS、取消网卡QoS、加载GPU设备、卸载GPU设备、加载USB设备、卸载USB设备、加载其它外接设备、卸载其它外接设备、定时任务、报警和审计。

- **停止状态**的云主机：

  启动、克隆、迁移、创建云主机镜像、创建快照、恢复快照、删除快照、创建灾备数据（混合云版支持）、创建云盘、加载云盘、卸载云盘、云盘扩容、创建云盘镜像、设置云盘QoS、取消云盘QoS、删除云盘、加载ISO、卸载ISO、添加SSH KEY、删除SSH KEY、设置高可用、修改计算规格、设置启动顺序、启动（指定物理机）、设置控制台密码、取消控制台密码、重置云主机、更改所有者、设置RDP模式、设置USB重定向、系统扩容、切换控制台模式、存储迁

移、更换系统、删除、绑定亲和组、解绑亲和组、设置名称和简介、设置平台类型、设置QGA状态、设置VDI设备最多支持的屏幕数量、设置用户标签、加载网卡、卸载网卡、设置MAC、设置静态IP、取消静态IP、设置网卡QoS、取消网卡QoS、加载GPU设备、卸载GPU设备、加载USB设备、卸载USB设备、加载其它外接设备、卸载其它外接设备、定时任务、报警和审计。

- **删除状态**的云主机：

  支持恢复、彻底删除的操作

- **本地存储**的云主机：

  支持热迁移与冷迁移。

  注:

  - 热迁移指迁移运行状态下的云主机；冷迁移指迁移停止状态下的云主机。
  - 要使用热迁移功能，需在ZStack私有云主菜单，点击**设置** > **全局设置**按钮，在**基本设置**页面，将**在线迁移**设为true。

- **共享存储**的云主机：

  支持热迁移与冷迁移，其中冷迁移目前支持跨Ceph存储迁移、跨NFS存储迁移以及跨Shared Block迁移。

  注:

  - 热迁移：主要是为拷贝CPU相关寄存器的状态及内存的信息。
  - 云主机支持共享存储的冷迁移，目前支持跨Ceph存储迁移、跨NFS存储迁移以及跨Shared Block迁移。
    - 跨Ceph存储迁移：
      - 云主机进行跨Ceph存储迁移之前，需先卸载所有数据云盘。
      - 所涉及的两个Ceph存储所在集群需加载到相同的二层网络，且彼此的mon节点可以互通。
    - 跨NFS存储迁移：
      - 云主机进行跨NFS存储迁移之前，需先卸载所有数据云盘。
      - 所涉及的两个NFS存储所在集群需加载到相同的二层网络，且目标NFS存储能够被挂载到待迁移云主机所在集群。
    - 跨Shared Block存储迁移：
      - 支持挂载云盘（共享云盘除外）的云主机进行跨Shared Block存储迁移。

- 所涉及的两个Shared Block存储所在集群需加载到相同的二层网络，且目标Shared Block存储能够被挂载到待迁移云主机所在集群。

云主机的操作定义如下：

- **启动**：将处于停止状态的云主机启动。
- **停止**：将处于运行状态的云主机停止。
- **重启**：将处于运行状态的云主机重启。
- **暂停**：将处于运行状态的云主机暂停。

  注: 暂停云主机并非真正停止云主机，因此请不要关闭暂停的云主机所在的物理机。

- **恢复**：将处于暂停状态的云主机恢复。
- **关闭电源**：当云主机处于运行状态时，使云主机强制进入停止状态。

  在云主机详情界面，点击**云主机操作** > **关闭电源**。

  注: 正常状态下不建议执行此操作。

- **打开控制台**：打开当前云主机的控制台，可以登录云主机系统。

  注:

  - 在云主机控制台，支持开机时设置boot选项，点击**ESC**进入选项菜单。
  - 如果无法打开云主机控制台，可尝试在**properties**文件里将控制台代理IP地址改成当前管理节点。

- **克隆**：对云主机根云盘和数据云盘进行复制，根据此云主机的计算规格，克隆出与当前云主机系统相同的云主机。

  - 云主机配置、安装程序、密码等都会复制到新克隆出的云主机内，但并不考虑其他配置的复制，例如：用户标签、定时任务等。
  - 克隆出的云主机处于启动状态。重启后控制台密码才会生效。

  在云主机详情界面，点击**云主机操作** > **克隆**，弹出**克隆**界面，可参考以下示例输入相应内容：

  - **名称**：输入克隆后云主机的名称
  - **数量**：克隆云主机数量
  - **亲和组**：可选项，选择亲和组策略
  - **同时克隆已挂载的云盘**：默认不勾选。勾选表示整机克隆，将同时克隆已挂载的数据云盘

注: 挂载共享云盘的云主机不支持整机克隆。

如图 *112: 克隆云主机界面*所示，点击**确定**按钮，完成克隆。

图 112: 克隆云主机界面

- 不带数据云盘克隆时，仅复制根云盘内容。支持**ImageStore**或**Ceph**类型的镜像服务器，所有主存储类型的云主机支持在线/暂停/关机克隆。
- 整机克隆时，将同时复制根云盘和数据云盘内容。仅支持**ImageStore**类型的镜像服务器。
  - LocalStorage、NFS和SMP类型的主存储，支持在线/暂停/关机克隆。
  - Ceph类型的主存储，支持在线/暂停/关机克隆。
  - Shared Block类型的主存储，支持暂停/关机克隆。

- **迁移**：将云主机迁移到别的计算节点中。

  迁移的速度与两台主机的网络配置有关，如果网络配置较低，迁移速度可能较慢。

  - **共享存储**：该迁移操作支持共享存储的云主机的热迁移。
  - **本地存储**：该迁移操作支持本地存储的云主机的热迁移和冷迁移。
    - 热迁移：

注:

- 本地存储热迁移不支持带有数据云盘的云主机的迁移。
- 本地存储热迁移不支持Windows云主机的迁移。

热迁移具体步骤如下：

1. 需在私有云**设置** > **全局设置** > **基本设置**里，将**在线迁移**设为true。
2. 将数据云盘从云主机上卸载。
3. 将云主机、数据云盘分别迁移至其它相同的计算节点。
4. 将卸载的数据云盘重新加载到该云主机。

- 冷迁移具体步骤如下：

1. 停止云主机。
2. 卸载云主机上的数据云盘。
3. 将云主机、数据云盘分别迁移至其它相同的计算节点。
4. 将卸载的数据云盘重新加载到该云主机。

- **创建镜像**：系统可以对云主机进行定制并保存为镜像模板文件。

在**云主机**管理界面，选择某一云主机，点击**更多操作** > **创建镜像**，弹出**创建镜像**界面，填写镜像名称，选择平台和所在镜像服务器，点击**确定**按钮。

系统会在后台创建该镜像文件，创建成功后会显示在**镜像**管理界面的镜像列表中。

如图 *113:* 创建镜像所示：

图 113: 创建镜像

注:

- 运行状态的云主机：如果云主机的镜像使用**镜像仓库**/Ceph类型的镜像服务器，支持在线创建镜像，以保存云主机当时的应用场景。
- 停止状态的云主机：如果云主机的镜像使用**镜像仓库**/Sftp/Ceph/FusionStor类型的镜像服务器，支持关机创建镜像。
- ZStack 支持在Ceph主存储上的云主机（处于运行或停止状态）创建镜像到镜像仓库类型的镜像服务器。

- **创建快照**：系统支持对云主机的根云盘创建快照。

  在**云主机**管理界面，选择某一云主机，点击**更多操作** > **创建快照**按钮，弹出**创建快照**界面，填写快照名称，点击**确定**按钮。系统立即对根云盘当前状态创建快照。

  也可在云主机详情界面，点击**主机快照**进入**主机快照**页面，点击**+**号按钮，弹出**创建快照**界面以创建快照。

  在**主机快照**页面，快照信息显示，如图 *114:* 主机快照所示：

  图 114: 主机快照

注:

- 如果云主机正在进行大量的I/O并发，此时创建快照，可能会有数据丢失的风险，请谨慎操作。建议停止云主机后再创建快照。
- 如果需要恢复快照，先停止云主机。
- 本地存储、NFS和SMP上的云主机快照为树状结构，如果删除任意一个非叶子节点的快照，那么它的所有子节点快照都将被删除。
- Ceph上的云主机快照为星型结构，每个快照互不影响。

注:

- 如果云主机的镜像使用**镜像仓库**/Ceph/FusionStor类型的镜像服务器，支持在线创建快照。
- 如果云主机的镜像使用**镜像仓库**/Sftp/Ceph/FusionStor类型的镜像服务器，支持关机创建快照。

- **创建灾备数据**：混合云版支持，详情请参考《混合云使用教程》的灾备实践章节。
- **创建云盘**：创建一个新的云盘并添加给当前云主机。

  具体步骤如下：

  1. 在云主机详情界面，点击**配置信息**，进入**配置信息**页面，点击**云盘**右侧的**操作** > **创建**，进入**创建云盘**界面，如图 *115:* 创建云盘界面所示：

     图 115: 创建云盘界面

2. 输入云盘名称，选择创建方式。若基于云盘规格创建，选择对应的云盘规格、主存储（可选项）；若基于云盘镜像创建，需选择已有的云盘镜像、主存储（可选项），然后点击**确定**。

注:

- 若系统在初始化后没有添加过云盘规格，需提前在云盘规格界面创建云盘规格。详情请参考创建云盘规格。
- 支持基于云盘镜像创建云盘，若云盘镜像来自于镜像仓库类型的镜像服务器，支持创建云盘到Ceph主存储上。

- **加载云盘**：将一个可用的未加载的云盘加载到当前云主机。

注:

- 如果主存储为本地存储，该云盘须与云主机在同一台物理机上。如果该云盘和云主机不在同一个物理机上，需提前将该云盘迁移到云主机所在的物理机上。详情请参考云盘操作。

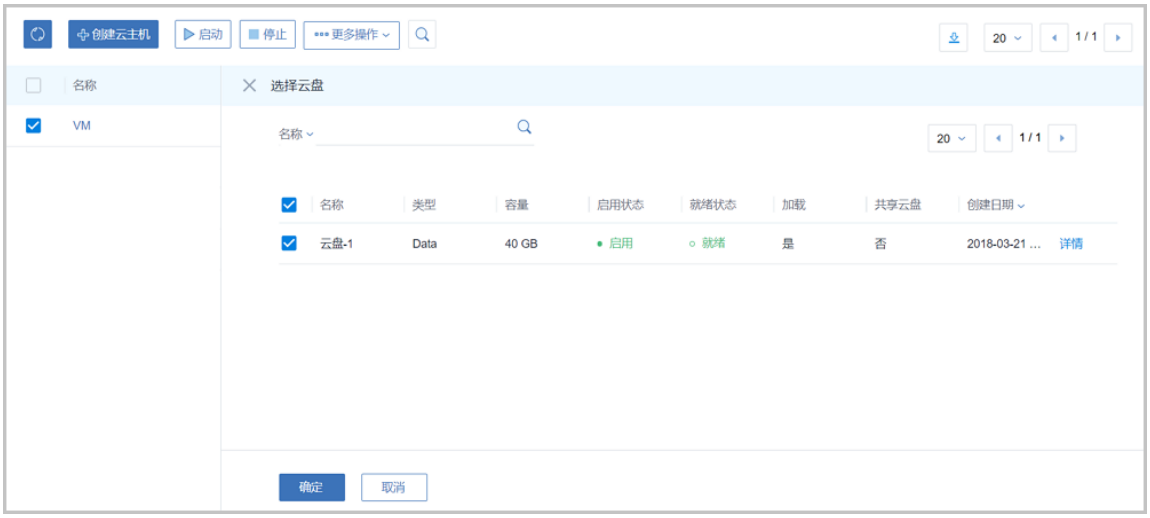
- **卸载云盘**：将之前添加的云盘从云主机卸载。

  具体步骤如下：

  1. 在**云主机**管理界面，选择某一云主机，点击**更多操作** > **卸载云盘**，进入选择卸载云盘界面。
  2. 从云盘列表选择需要卸载的云盘，点击**确认**。

     如图 *116:* 卸载云盘界面所示：

     图 116: 卸载云盘界面



- **云盘扩容**：

  在云主机运行或者停止状态下，在**配置信息**界面，选择需要扩容的根云盘/数据云盘，点击**云盘**右侧的**操作** > **云盘扩容**，弹出**云盘扩容**界面，如图 *117:* 根云盘/数据云盘扩容界面所示。可按需进行根云盘/数据云盘扩容，更改容量即时生效。

  图 117: 根云盘/数据云盘扩容界面

注:

- 扩容容量只增不减，增量不得小于4MB。单位包括：MB/GB/TB

- **创建云盘镜像**：

  在云主机运行或者停止状态下，在**配置信息**界面，点击网卡右侧的**操作** > **创建镜像**，弹出**创建镜像**界面，填写云盘镜像名称，选择所在镜像服务器，点击**确定**按钮。

  注:

  - ZStack 支持创建云盘镜像，且支持Ceph主存储上的云盘创建云盘镜像到镜像仓库类型的镜像服务器。

- **设置云盘QoS**：

  在云主机运行或者停止状态下，在**配置信息**界面，点击网卡右侧的**操作** > **设置云盘QoS**，弹出**设置云盘QoS**界面，可设置云盘带宽，单位为Mbps/Gbps。

- **取消云盘QoS**：可取消已设置的云盘带宽。
- **删除云盘**：删除云主机挂载的数据云盘。
- **加载ISO**：添加ISO镜像到云主机中。ZStack支持挂载多个ISO，最多支持添加3个，不支持批量加载。具体步骤如下：

  1. 在**云主机**管理界面，选择某一云主机，点击**更多操作** > **加载ISO**按钮，进入加载ISO界面。

2. 在**选择ISO**列表勾选需要加载的ISO，点击**确认**按钮，进行加载。
3. 重复上述操作加载其他ISO。

- **卸载ISO**：将已添加的ISO镜像从云主机中卸载，支持批量卸载。
  - 在**云主机**管理界面，选择某一云主机，点击**更多操作** > **卸载ISO**按钮，进入卸载ISO界面。
  - 在**选择ISO**列表勾选需要卸载的ISO，点击**确认**按钮，进行卸载。
- **添加SSH KEY**：

  在**云主机**管理界面，选择某一云主机，点击**更多操作添加SSH KEY**按钮，进入**添加SSH KEY**界面。在文本框中输入要添加的SSH KEY，点击**确认**，重启后生效。SSH KEY具体介绍请参考*SSH*公钥管理章节。

  注:

  - SSH KEY注入开机第一次生效，再次添加需在云主机中清理先前配置并重启。
  - 如果云主机之前已注入过SSH KEY，则需在云主机中手动执行`rm -rf /var/lib/cloud/instances`以清理先前配置。
- **删除SSH KEY**：可删除已添加的SSH KEY。
- **设置高可用**：高可用级别有NeverStop或None两种模式。
  - None：云主机关闭高可用功能
  - NeverStop：云主机开启高可用功能

  本地存储的云主机设置为NeverStop：

  - 当所在物理机处于**启用**和**已连接**状态时，该云主机会一直运行。即使强制关机，该云主机也会再次启动。

    注:

    如希望NeverStop云主机本次关机不自动启动，在弹出的**停止云主机**窗口，勾选**设置NeverStop的云主机**，**本次停止将不会自动启动**即可。
  - 当所在物理机异常断电/断网时，该云主机会进入**已停止**状态。

  共享存储的云主机设置为NeverStop：

  - 在已添加的物理机里，只要有任意一台资源允许，该云主机会一直运行。即使强制关机，该云主机也会再次启动。

    注:

如希望NeverStop云主机本次关机不自动启动，在弹出的**停止云主机**窗口，勾选**设置NeverStop的云主机**，**本次停止将不会自动启动**即可。

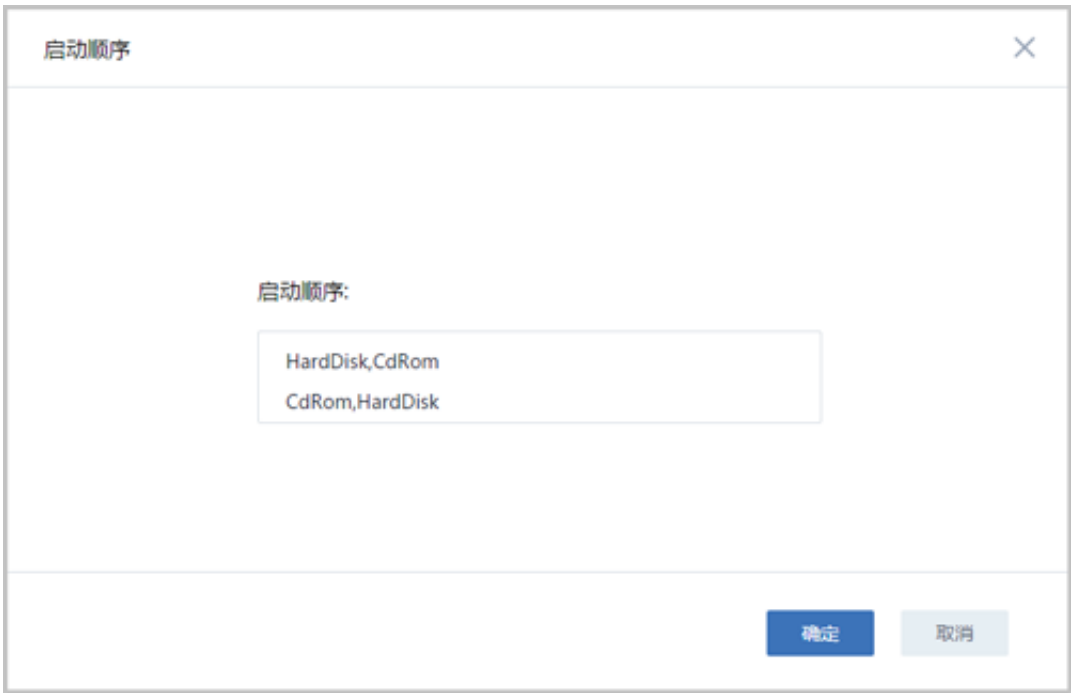
- 当所在物理机异常断电/断网时，只要资源允许，该云主机会迁移至其它物理机运行。

- **修改计算规格**：
  - Linux云主机支持在线/关机修改计算规格（CPU/内存）
    - **开机修改**：
      1. 在线修改云主机计算规格，需首先在私有云**设置** > **全局设置** > **基本设置**里，将**NUMA**设为true。
      2. 重启管理节点云主机。
      3. 在**云主机**界面，选择某一运行中的云主机，点击**更多操作** > **修改计算规格**，在打开的计算规格列表中选择。
    - **关机修改**：

      在**云主机**管理界面，选择某一已停止的云主机，点击**更多操作** > **修改计算规格**，在打开的计算规格列表中选择。
    - 也可在云主机详情界面直接修改CPU/内存，开启**NUMA**后支持在线修改；未开启时仅支持关机修改。
  - Windows云主机仅支持关机修改计算规格，不支持在线修改计算规格。
- **设置启动顺序**：
  - 如果在创建云主机时，镜像选择为ISO，云主机会首先从ISO启动。
  - 如果云主机创建之后加载ISO，云主机默认的启动顺序是：第一从硬盘引导，第二从ISO引导。
  - 如需更改启动顺序，例如通过ISO启动来修复硬盘，操作如下：

    在**云主机**管理界面，选择某一云主机，点击**更多操作** > **设置启动顺序**，以更改云主机启动顺序，如图 *118: 启动顺序界面*所示，其中CdRom代表ISO引导时的虚拟光驱。

    图 118: 启动顺序界面



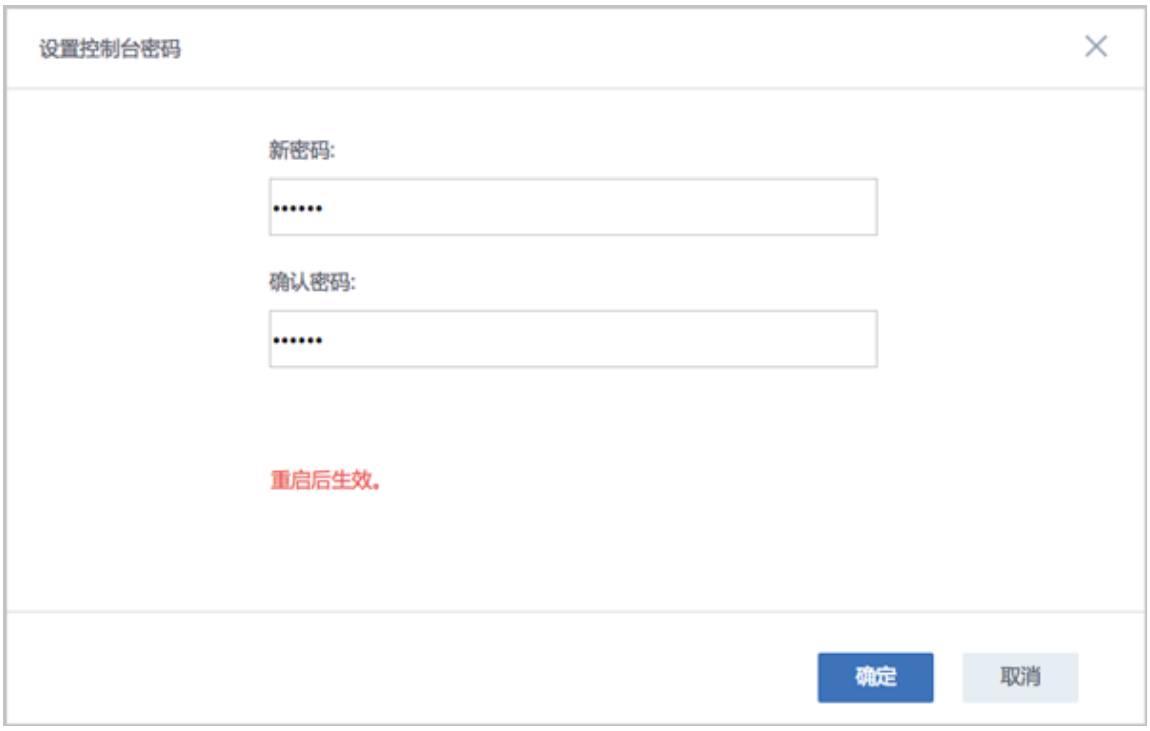
注:

- 如果选择CdRom是第一启动顺序，只有通过**停止**和**启动**操作，云主机才会从CdRom启动。
- 如果直接在云主机操作系统中通过*reboot*命令重启，云主机还是会从硬盘启动。

- **启动（指定物理机）**：
  - 使用**共享存储**的云主机停止后，可以选择在指定的物理机上重新启动。

    在**云主机**管理界面，选择某一云主机，点击**更多操作** > **启动（指定物理机）**，在打开的物理机列表中选定后，该云主机可直接从选择的物理机启动。
  - 使用**本地存储**的云主机停止后，只能从该云主机根云盘所在的物理机启动。
- **设置/取消控制台密码**：支持设置/取消云主机控制台密码。
  - 该密码为VNC协议的密码，不是云主机本身的密码。
  - 设置完成后，重启云主机才可生效，如图 *119:* 设置控制台密码界面所示：

    图 119: 设置控制台密码界面



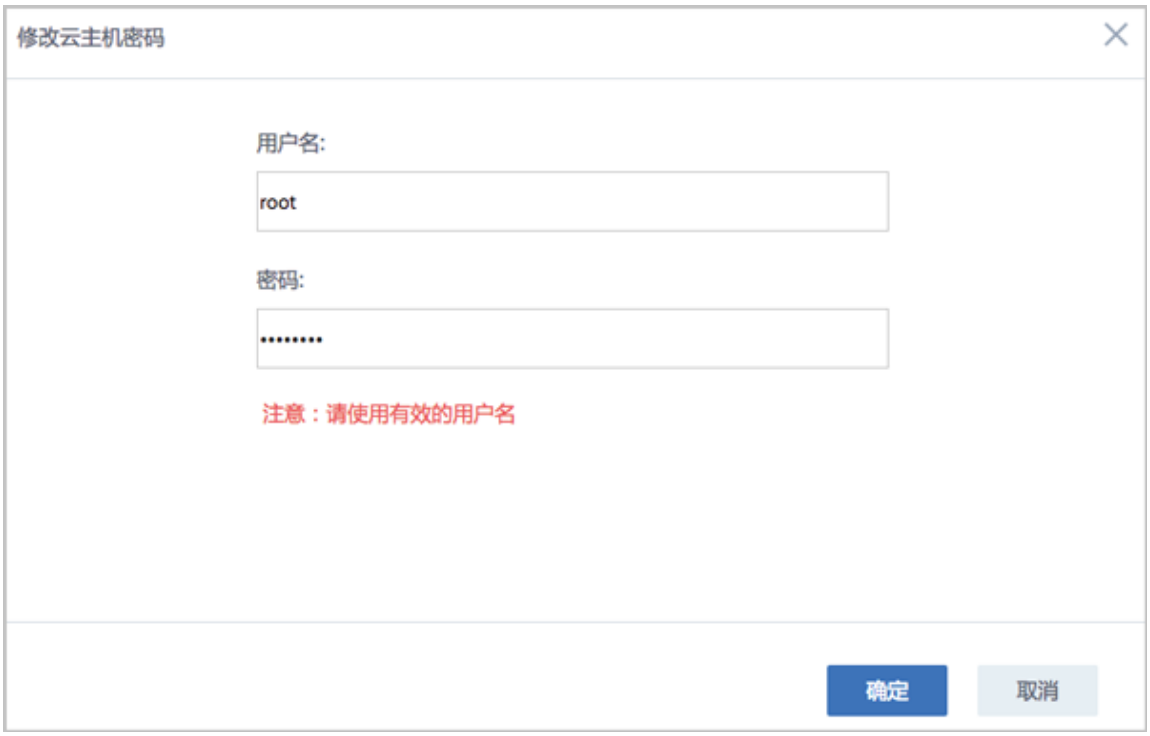
- **重置云主机**：如果云主机使用镜像创建，可重置该云主机到创建时的状态。

  注:

  - 云主机必须处于**已停止**状态。在**云主机**管理界面，选择某一已停止的云主机，点击**更多操作** > **重置云主机**，重启云主机后生效。
  - 使用ISO安装创建的云主机不支持重置功能。
- **更改所有者**： 将云主机的所有者更改。
- **设置RDP模式**：针对VDI用户界面，选择RDP模式后，默认以RDP模式打开控制台。
- **设置USB重定向**：当用户需要使用VDI功能时，需要开启此项，将VDI客户端的USB设备重定向给VDI云主机使用。
- **修改云主机密码**：

  - 在**云主机**管理界面，选择某一运行中的云主机，点击**更多操作** > **修改云主机密码**，弹出**修改云主机密码**界面，如图 *120:* 修改云主机密码界面所示。输入用户名，密码，点击**确定**后生效。

    图 120: 修改云主机密码界面



- 使用已修改密码的云主机创建的镜像，创建出的新云主机或者克隆出的新云主机均支持该功能。
- 目前已支持修改云主机密码的镜像类型有：
  - CentOS 7.x\6.x（32位\64位\）；
  - Ubuntu 16.x\15.x\14.x\13.x\12.x\（64位）；
  - Windows 2003\2008\7\10\2012\2016（64位）

注:

- 使用Sftp/Ceph类型镜像服务器添加镜像，已勾选**支持修改密码**的qcow2镜像所创建的云主机，也支持该功能。Sftp类型镜像服务器仅在社区版支持。
- 如果修改云主机密码失败，请先检查云主机中是否已安装Qemu Guest Agent，在终端手动检查QGA的运行状态是否正常。

- **系统扩容**：在云主机运行或者停止状态下，点击**系统扩容**，可按需进行根云盘扩容，更改容量及时生效。

  在**云主机**管理界面，选择某一运行中/已停止的云主机，点击**更多操作** > **系统扩容**，弹出**系统扩容**界面，如图 *121: 系统扩容界面*所示。可按需进行根云盘扩容，更改容量即时生效。

图 121: 系统扩容界面

注:

- 扩容容量只增不减，增量不得小于4MB。单位包括：MB/GB/TB

系统扩容具体介绍请参考系统扩容教程。

- **切换控制台模式**：支持云主机控制台模式在VNC和SPICE之间切换。
- **存储迁移**：云主机支持关机状态下跨共享存储的数据迁移，目前支持跨Ceph存储迁移、跨NFS存储迁移以及跨Shared Block迁移。
  - 跨Ceph存储迁移：
    - 云主机进行跨Ceph存储迁移之前，需先卸载所有数据云盘。
    - 所涉及的两个Ceph存储所在集群需加载到相同的二层网络，且彼此的mon节点可以互通。
  - 跨NFS存储迁移：
    - 云主机进行跨NFS存储迁移之前，需先卸载所有数据云盘。
    - 所涉及的两个NFS存储所在集群需加载到相同的二层网络，且目标NFS存储能够被挂载到待迁移云主机所在集群。
  - 跨Shared Block存储迁移：
    - 支持挂载云盘（共享云盘除外）的云主机进行跨Shared Block存储迁移。

- 所涉及的两个Shared Block存储所在集群需加载到相同的二层网络，且目标Shared Block存储能够被挂载到待迁移云主机所在集群。

- **绑定亲和组**：绑定云主机到亲和组，组策略对该云主机即时生效。

  目前ZStack提供针对云主机与物理机的两种亲和组策略：反亲和组(非强制)、反亲和组(强制)。

  - 反亲和组(非强制)：

    将亲和组内的云主机尽量分配到不同物理机上，当没有更多物理机可分配时，回归普通分配策略。

  - 反亲和组(强制)：

    将亲和组内的云主机严格分配到不同物理机上，当没有更多物理机可分配时，则分配失败。

- **解绑亲和组**：将云主机从从亲和组解绑，组策略对该云主机即时失效。
- **更换系统**：将云主机停止后，点击**更换系统**，在弹出的**选择镜像**界面，选择目标镜像即可，目标镜像需为Image类型。更换系统后，云主机保持关机状态。

  注:

  - 更换系统操作，会彻底删除原系统盘及其快照，务必确认更换系统前做好相关备份，以免丢失数据。
  - 创建云主机快照的定时任务会失效，需要重新设置。
  - 云主机挂载数据盘时，支持更换不同类型的操作系统，例如从Linux更换为Windows。
  - 在做跨平台的操作系统更换时，数据盘的分区格式可能会无法识别。

- **删除**：

  ZStack支持三种云主机删除模式：

  - **立刻删除**（Direct）：

    删除云主机后，云主机相关资源立刻被删除。

  - **延时删除**（Delay）：

    删除云主机后，云主机的**启用状态**会被标记为**已删除**，并移至**已删除**页面。系统默认使用此种删除策略，如图 *122:* 已删除云主机页面所示：

    图 122: 已删除云主机页面

注:

- 系统默认24小时后才会彻底删除这些云主机。
- 可在私有云的**设置** > **全局设置** > **基本设置**页面，更改**彻底删除时延**的时间。

- **永不删除**（Never）：

  删除云主机后，云主机相关资源永远不删除。

注:

- 可在私有云的**设置** > **全局设置** > **基本设置**页面，通过修改**删除策略**的值来设置默认的云主机删除模式。
- 在删除云主机弹出的确认窗口，若勾选**同时删除云盘**，会同时删除此云主机已加载的所有普通云盘，不会删除共享云盘。

- **彻底删除/恢复**：将已删除栏中的云主机彻底删除或恢复。
  - **彻底删除**：

    选择彻底删除后，云主机相关资源会被彻底删除，不可逆转，请谨慎操作。
  - **恢复**：

    恢复后的云主机回到**可用**页面，且**启用状态**为**已停止**，用户可以重新启动该云主机。

    注: 删除云主机后，其IP地址会返回IP地址池中。恢复云主机，会为其重新分配IP地址。

  云主机、镜像、云盘均支持恢复和彻底删除。
- **修改名称和简介**：修改云主机的名称和简介。

  注: 云主机的名称可以重复，但建议使用易于区分的名称。UUID为系统中唯一确定云主机身份的标识。
- **QGA**：只有云主机使用的镜像中已经安装了QGA服务，相应的云主机才可以使用它。
  - 开启QGA前，需确保云主机已安装并运行Qemu guest agent。

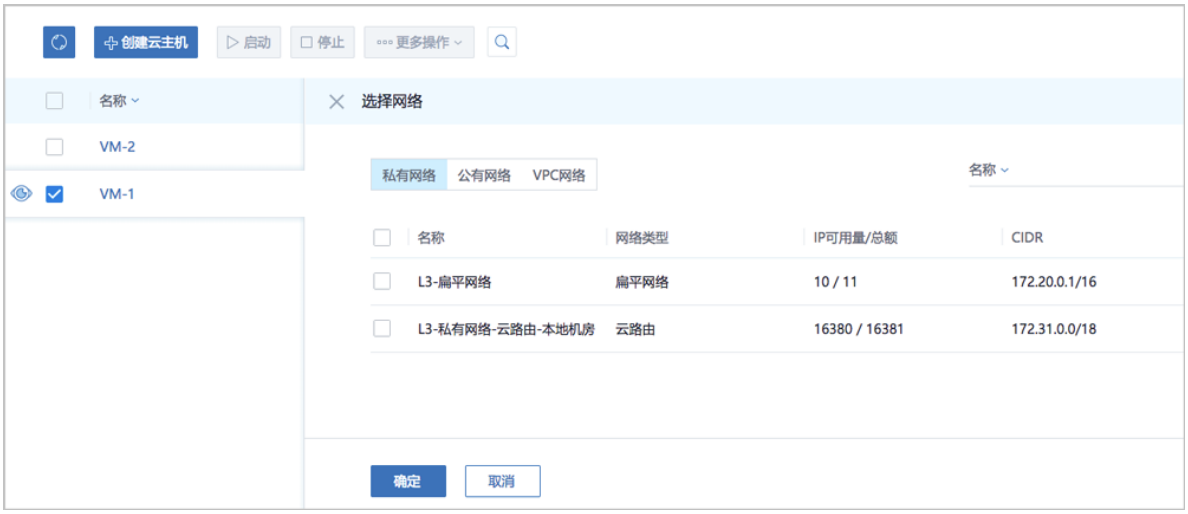
- 开启QGA后，云主机默认支持在线修改密码。

- **屏幕数量**：可设置VDI设备最多支持的屏幕数量，支持SPICE模式。
- **标签**：可对云主机设置用户标签，方便用户搜索查询云主机。可创建多个用户标签。也可点击右侧**X**删除。
- **加载网卡**：支持对云主机动态加载网络，例如：新增一个云路由网络到云主机。

  在**云主机**管理界面，选择某一云主机，打开其详情页，点击**配置信息**，进入**配置信息**页面，点击网卡右侧的**操作** > **加载**，弹出可选网络列表界面，支持加载私有网络、公有网络和VPC网络，支持批量加载，点击**确定**按钮。加载成功后的网络会显示在云主机网络列表。

  如图 *123:* 云主机加载网卡可选网络列表界面所示：

  图 123: 云主机加载网卡可选网络列表界面



- **卸载网卡**：支持对云主机动态卸载网络，例如从云主机移除一个网络。

  在**配置信息**界面，选择需卸载的网络，点击网卡右侧的**操作** > **卸载**，可将选中的网络从云主机卸载。

- **更改默认网络**：

  在**配置信息**界面，网络列表中选择某一网络，点击**默认**按钮，确认后需重启网络服务生效。

- **设置MAC** ：

  创建云主机时可以指定MAC地址。停止云主机后，可在**配置信息**界面，点击网卡右侧的**操作** > **设置MAC**来设置或更改MAC地址。

- **设置静态IP**：

创建云主机时可以指定静态IP地址。停止云主机后，可在**配置信息**界面，点击网卡右侧的**操作** > **设置IP**来设置或更改静态IP地址。

注: 需避免与其它IP地址冲突。

- **取消静态IP**：

  支持取消静态IP。停止云主机后，在**配置信息**界面，点击网卡右侧的**操作** > **取消静态IP**即可。

- **设置网卡QoS**：

  在云主机停止或者运行状态下，在**配置信息**界面，点击网卡右侧的**操作** > **设置网卡QoS**，弹出**设置网卡QoS**界面，可设置上行网络带宽和下行网络带宽，单位为Kbps/Mbps/Gbps。

- **取消网卡QoS**：可取消已设置的网卡QoS。
- **加载GPU设备**：开启物理机GPU透传功能，云主机可加载物理机GPU设备。
- **卸载GPU设备**：云主机卸载物理机GPU设备，支持热插拔。

注: 关于GPU透传功能的详情请参考《GPU及USB设备透传使用教程》的*GPU透传*章节。

- **加载USB设备**：开启USB透传功能，云主机可加载USB设备。
- **卸载USB设备**：云主机卸载USB设备。

注: 关于USB透传功能的详情请参考《GPU及USB设备透传使用教程》的*USB透传*章节。

- **加载其他设备**：开启其他外接设备透传功能，云主机可加载其他外接设备。
- **卸载其他设备**：云主机卸载其他外接设备。
- **定时任务**：定时任务能够帮助用户完成周期性的资源操作任务，比如根据业务需要定时启动云主机、停止云主机、重启云主机、为云主机根云盘创建快照等。详情请参考云主机定时任务章节。
- **报警**：支持云主机报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加云主机CPU、磁盘、网卡、内存相关的多项报警条目，以邮件/钉钉/HTTP POST方式发送报警信息。详情请参考云主机报警章节。
- **审计**：支持对云主机的所有操作行为审计，有效保障云环境下核心数据的安全。

7.2.1.3.2 批量云主机操作

已有页面

在**云主机**管理界面，**已有**页面支持的批量操作有：启动、停止、重启、暂停、关闭电源、设置高可用、修改计算规格、更改所有者、设置RDP模式、设置USB重定向、切换控制台模式、删除等操作，如图 *124:* 已有页面批量操作云主机所示：

图 124: 已有页面批量操作云主机

注:

批量操作会过滤掉已经处于目标状态下的云主机。例如，用户想停止批量选中的云主机，系统会自动跳过已停止的云主机。

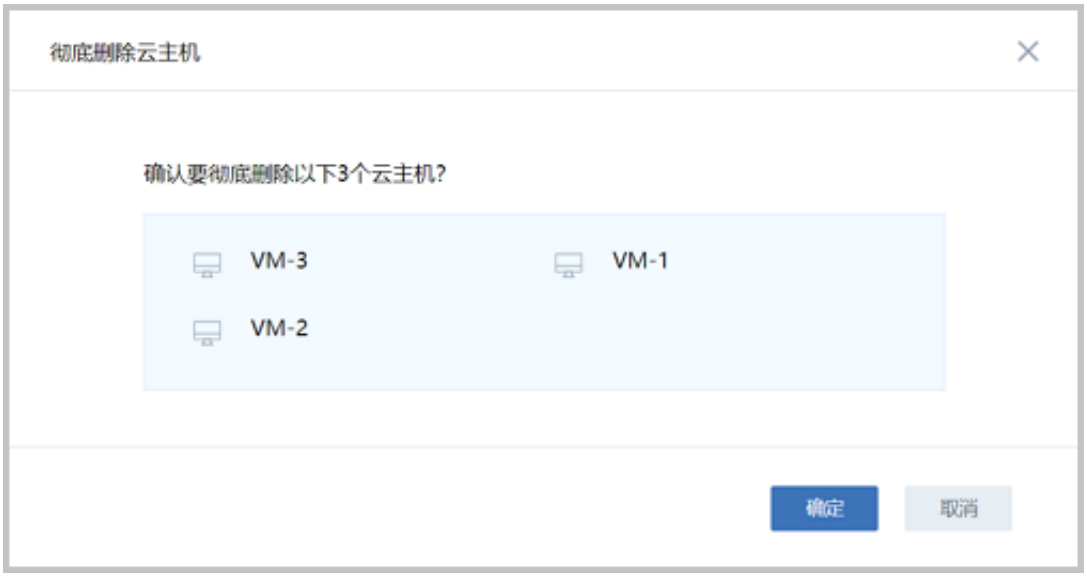
已删除页面

在**云主机**管理界面，**已删除**页面支持的批量操作有：恢复和彻底删除，如图 *125:* 已删除页面批量操作云主机所示：

图 125: 已删除页面批量操作云主机

批量勾选需彻底删除的云主机，点击**彻底删除**，弹出确认界面如图 *126:* 批量彻底删除云主机确认界面所示。

图 126: 批量彻底删除云主机确认界面



7.2.1.3.3 SSH公钥管理

注入SSH公钥可以给云主机的root用户设置SSH公钥，云主机启动后，用户可用对应的SSH私钥进行SSH无密码登录。

SSH公钥目前使用cloud-init注入方式实现，采用Amazon AWS的标准用法，使用该功能云主机模板需要预装cloud-init。

注: 使用cloud-init镜像，默认情况下不支持用户名/密码登录，需要使用SSH公钥登录。

具体操作：

1. 生成SSH公钥。

   SSH公钥由*ssh-keygen*命令生成，默认会存放在*/root/.ssh/id_rsa.pub*文件。将此文件内容贴入SSH公钥输入框即可。

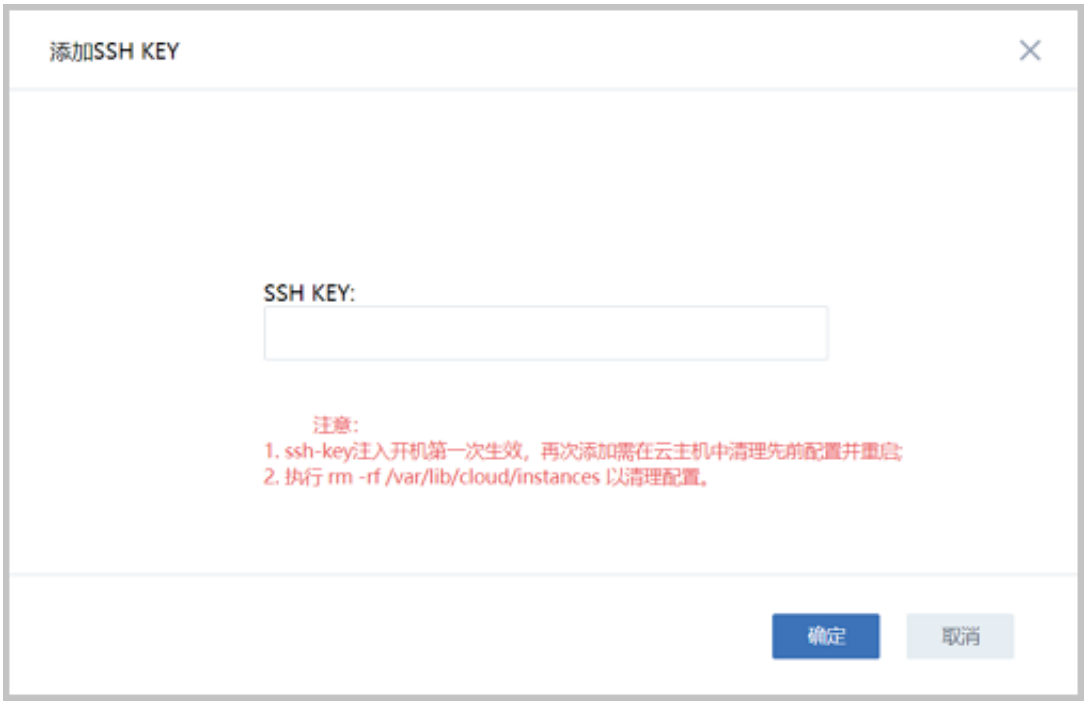
   注:

   1. 在CentOS的云主机里可以通过yum install cloud-init直接安装cloud-init，安装完毕后保存为镜像。

2. 使用此镜像的云主机在启动时，如果输入SSH公钥，云主机启动后，拥有对应SSH公钥和私钥的主机即可无密码登录此云主机。

2. 在创建云主机时，**高级**选项中，输入SSH KEY。
3. 也可在云主机操作中使用**添加SSH KEY**输入SSH公钥，如图 *127: 为云主机注入SSH公钥*所示。

图 127: 为云主机注入SSH公钥



4. 添加SSH公钥后，可在云主机详情界面查看对应SSH公钥的基本信息，例如对应公钥的用户名或主机信息。

用户可登录CentOS、Ubuntu官网直接下载相应的镜像测试使用，下载链接如下：

- CentOS 7.2 ： 点击这里。
- Ubuntu 14.04 ：点击这里。

7.2.1.3.4 系统扩容教程

ZStack支持云主机在运行或者停止状态下进行根云盘扩容。

云主机根云盘扩容

可通过以下三种方式进行云主机根云盘扩容：

1. 在**云主机**管理界面，选择某一运行中/已停止的云主机，点击**更多操作** > **系统扩容**，弹出**系统扩容**界面，如图 *128:* 系统扩容界面所示。可按需进行根云盘扩容，更改容量即时生效。

图 128: 系统扩容界面

注:

- 扩容容量只增不减，增量不得小于4MB。单位包括：MB/GB/TB

2. 选择某一运行中/已停止的云主机，进入云主机详情页的**配置信息**页面，选择需要扩容的根云盘，点击**云盘**右侧的**操作** > **云盘扩容**，弹出**云盘扩容**界面，如图 *129:* 云盘扩容界面所示。可按需进行根云盘扩容，更改容量即时生效。

图 129: 云盘扩容界面

注:

- 扩容容量只增不减，增量不得小于4MB。单位包括：MB/GB/TB

3. 选择某一运行中/已停止的云主机，进入云主机详情页的**配置信息**页面，点击需要扩容的根云盘，进入根云盘详情页，按需修改根云盘**容量**，更改容量即时生效。

上述步骤仅实现将云主机的根云盘容量扩大，需在云主机的操作系统里对硬盘进行分区扩容，才可使得云主机识别。

云主机操作系统硬盘分区扩容

针对不同类型、不同分区、不同文件系统的云主机，扩容方式均不相同。

注:

- 进行根云盘扩容前，默认对当前系统进行了快照备份，以增强数据安全性。
- 扩容存在风险。安全的扩容方式是对扩容的新容量，规划新的分区。
- 扩容只能增加容量，不能减少容量。
- 扩容增加的容量可以合并到最后一个分区，将其连续使用。
  - 如果最后一个分区是系统备份分区（Windows），则只能对新增容量规划新的分区方式使用。

- 如果最后一个分区是swap分区，则swap分区可以删除，将新增容量扩容至swap分区前一分区后，再重建swap分区。

以下分三种不同的应用场景来介绍：

1. 使用GParted开源工具针对ext4+swap分区扩容ext4根分区实例。

   注:

   - 此方式需借助Live CD方式对当前分区进行重新规划。
   - 调整分区时需谨慎操作，以防止数据丢失。

   假定云主机采用了ext4根分区+swap分区，其中ext4根分区35G，swap分区5G，总容量40G，将系统从40G扩容至50G后，打算将新增容量扩容至ext4根分区。

   操作步骤如下：

   1. 添加GParted ISO，下载路径可参考GPared官网*https://gparted.org/download.php*，建议下载amd64的iso表示支持64位系统。
   2. 添加ISO后，设置启动顺序为cdrom harddisk，表示下次启动，以cdrom优先。
   3. 使用GParted Live CD引导系统，打开云主机控制台，GParted引导后，按照引导一直执行Enter键直至进入图形界面。
   4. 在GParted界面，右击删除原本的swap分区，扩展ext4将其从35G扩展至46G，针对unallocated的4G分区，新建swap分区，如图 *130: 删除原本的swap分区*、图 *131: 扩展ext4从35G至46G*和图 *132: 新建4G swap分区*所示：

      图 130: 删除原本的swap分区

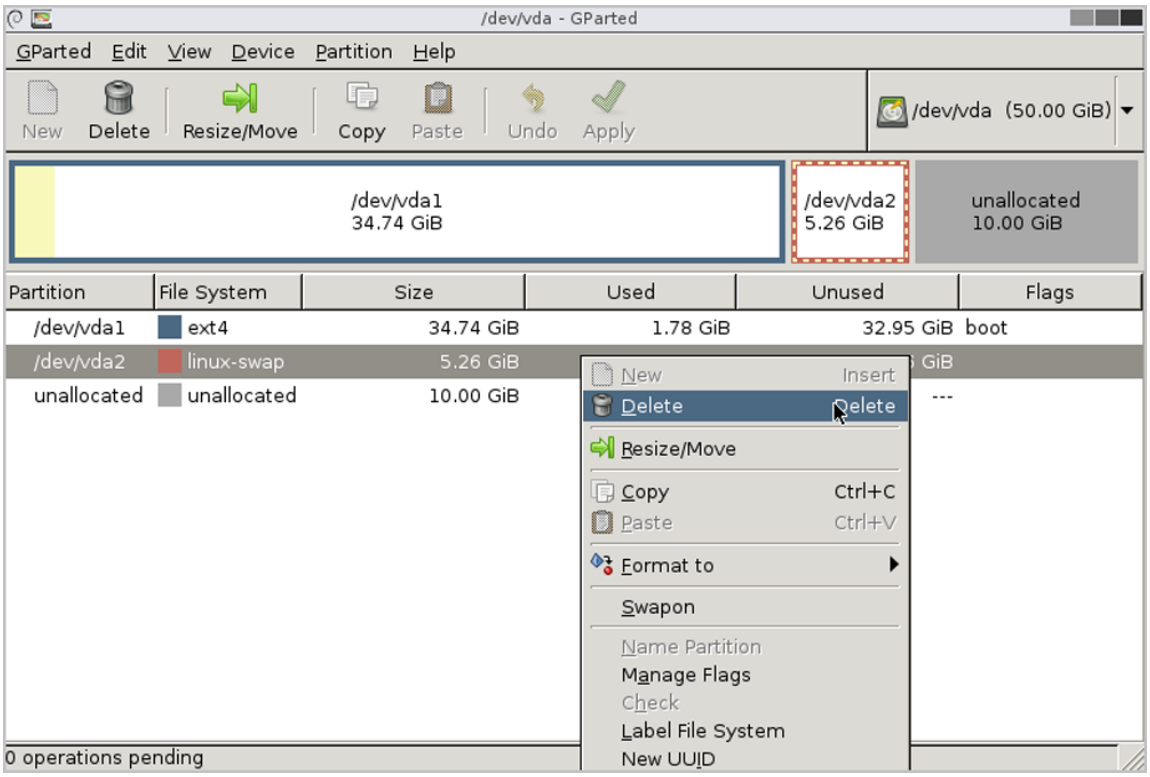
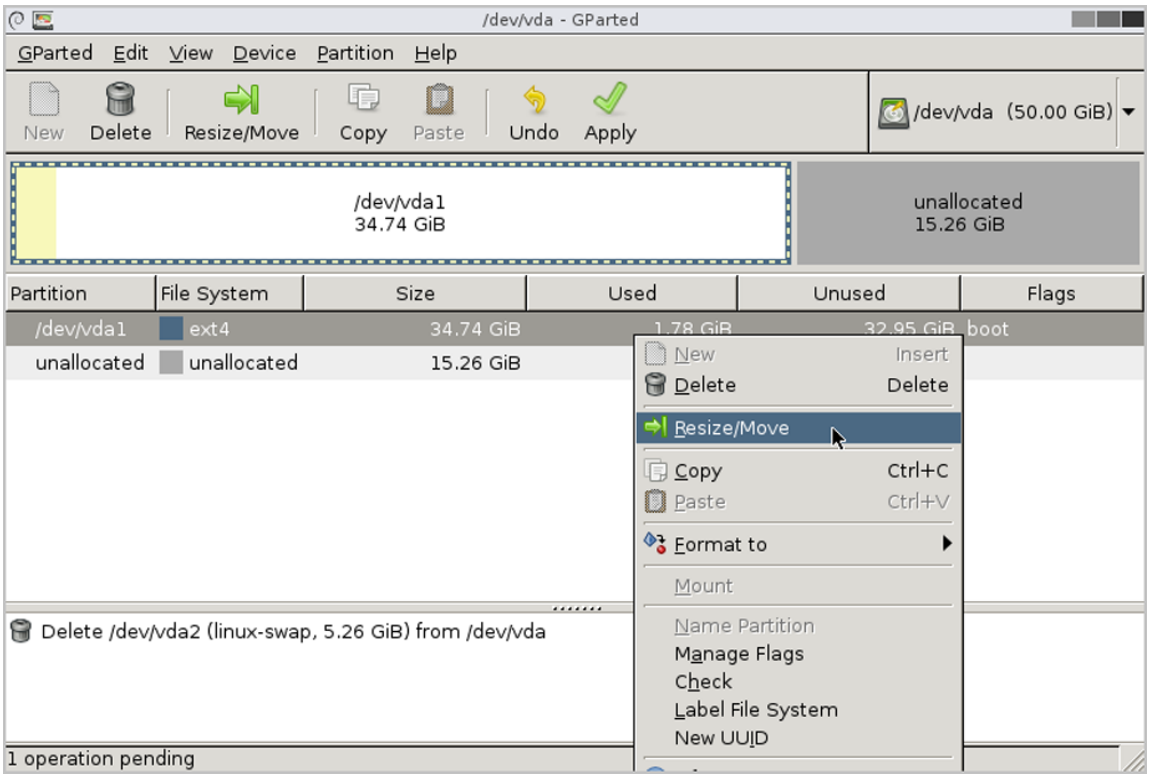


图 131: 扩展ext4从35G至46G



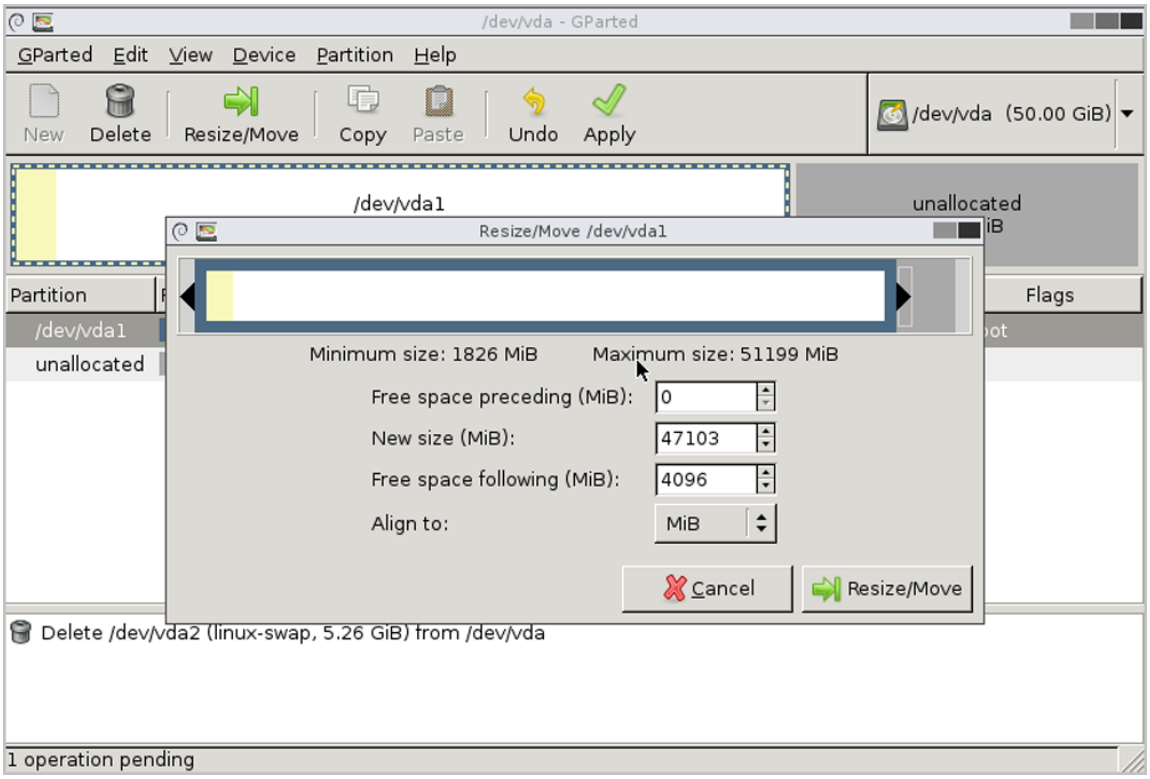
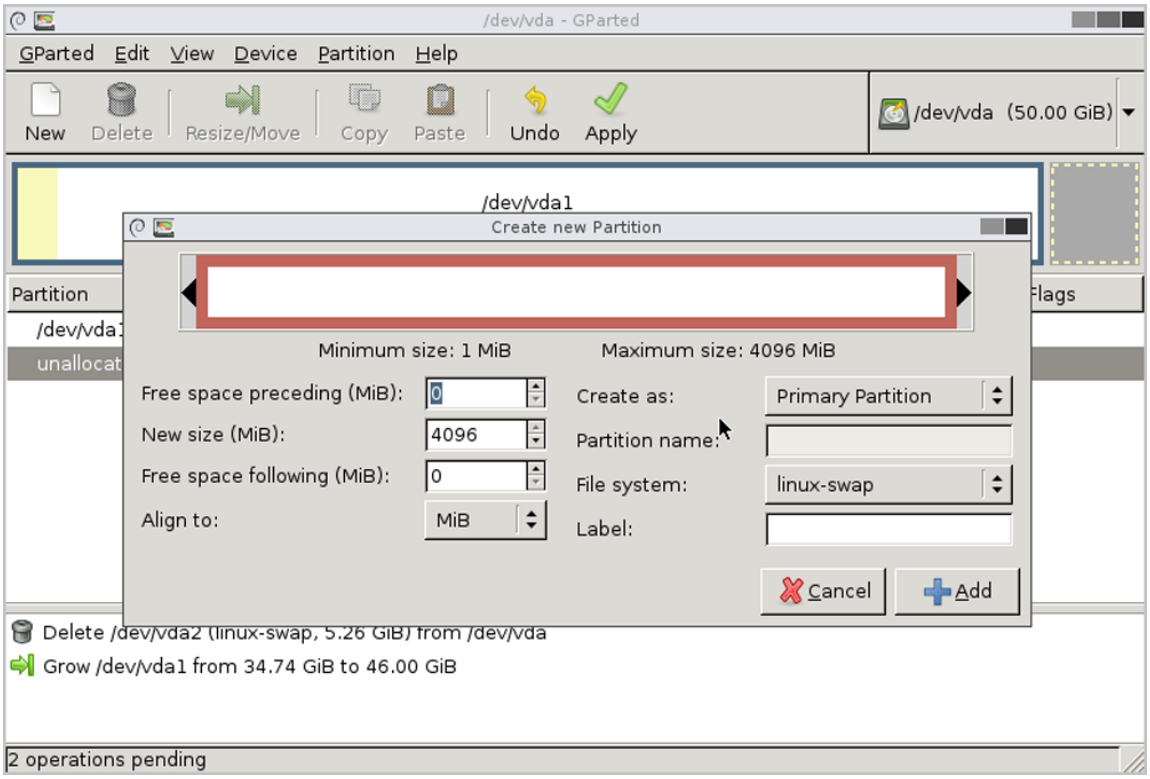
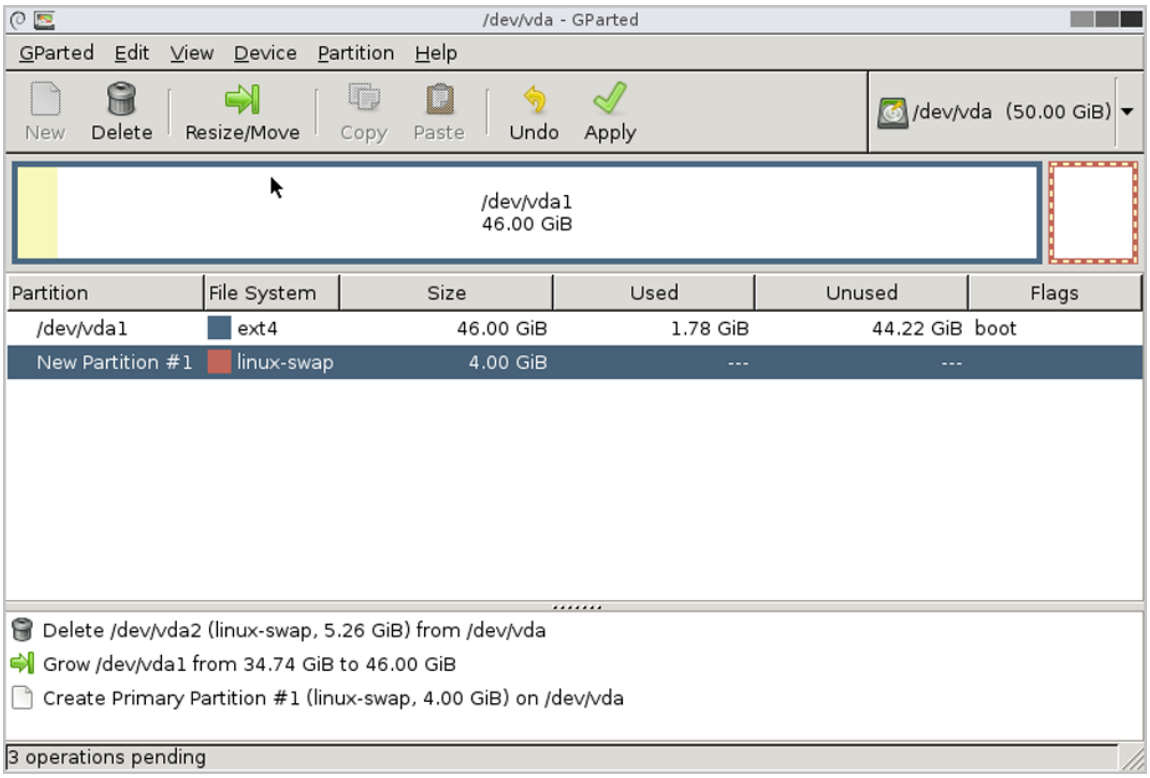


图 132: 新建4G swap分区





5. 关闭云主机，卸载ISO，启动云主机。

6. 打开云主机控制台，执行df -h，可见云主机根分区容量已扩展至46G。

```
[root@10-58-21-213 ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/vda1 46G 1.2G 42G 3% /
```

7. 开启swap分区并修改*/etc/fstab*磁盘分区表。

```
[root@10-58-21-213 ~]# fdisk -l|grep vda
Disk /dev/vda: 53.7 GB, 53687091200 bytes, 104857600 sectors
/dev/vda1 * 2048 96468991 48233472 83 Linux
/dev/vda2 96468992 104857599 4194304 82 Linux swap / Solaris

[root@10-58-21-213 ~]# mkswap /dev/vda2
mkswap: /dev/vda2: warning: wiping old swap signature.
Setting up swapspace version 1, size = 4194300 KiB
no label, UUID=ed99f72b-aafb-43ad-be8f-fcd09794beb0
#可知此swap分区的UUID为ed99f72b-aafb-43ad-be8f-fcd09794beb0

[root@10-58-21-213 ~]# swapon /dev/vda2
#开启swap分区

[root@10-58-21-213 ~]# free -m
 total used free shared buff/cache available
Mem: 911 106 671 6 133 657
Swap: 4095 0 4095

[root@10-58-21-213 ~]# sed -i '/swap/d' /etc/fstab
echo "UUID=ed99f72b-aafb-43ad-be8f-fcd09794beb0 swap swap defaults 0 0"
```

```
#将swap的设置写入磁盘分区表，以便开机自启。
```

8. 关机重启后，此云主机根云盘ext4分区成功扩容，swap分区也保留4G使用。

2. 使用LVM分区工具针对xfs+swap分区扩容LVM分区实例。

注: 此方式适用于LVM分区动态扩容，无须借助其他工具。

假定云主机采用了LVM分区，并格式化为boot分区、xfs根分区和swap分区。其中xfs根分区94G，swap分区6G，总容量100G，将系统从100G扩容至120G后，打算将新增容量扩容至xfs根分区。

操作步骤如下：

1. 查看当前分区和LVM逻辑分区，其中boot分区为500M，使用了*/dev/vda1*，LVM分区为94G，使用了*/dev/vda2*，路径为*/dev/vg/root*，swap分区为6G，路径为*/dev/vg/swap*。

```
[root@10-0-44-221 ~]# df -h
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vg-root 94G 6.5G 88G 7% /
/dev/vda1 477M 104M 344M 24% /boot
#boot分区为500M，使用了/dev/vda1
#LVM分区为94G，使用了/dev/vda2，路径为/dev/vg/root
#swap分区为6G，路径为/dev/vg/swap

[root@10-0-44-221 ~]# fdisk -l |grep vda
Disk /dev/vda: 128.8 GB, 128849018880 bytes, 251658240 sectors
/dev/vda1 * 2048 1026047 512000 83 Linux
/dev/vda2 1026048 209715199 104344576 8e Linux LVM

[root@10-0-44-221 ~]# pvdisplay |egrep "Name|Size"
 PV Name /dev/vda2
 VG Name vg
 PV Size 99.51 GiB / not usable 3.00 MiB
 PE Size 4.00 MiB
#物理卷使用/dev/vda2

[root@10-0-44-221 ~]# vgdisplay |egrep "Name|Size"
 VG Name vg
 VG Size 99.51 GiB
 PE Size 4.00 MiB
 alloc PE / Size 25463 / 99.46 GiB
 Free PE / Size 11 / 44.00 MiB
#卷组信息，卷组名称为vg，会针对此卷组扩容

[root@10-0-44-221 ~]# lvdisplay |egrep "Name|Size"
 LV Name root
 VG Name vg
 LV Size 93.59 GiB
 LV Name swap
 VG Name vg
 LV Size 5.88 GiB
```

```
#逻辑卷信息
```

2. 扩容后，执行fdisk /dev/vda对新增容量分区，使用n建立新分区，使用t将其分区为LVM格式，使用w使修改生效，使用partprobe使其立刻生效。

```
[root@10-0-44-221 ~]# fdisk /dev/vda
Welcome to fdisk (util-linux 2.23.2).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.
Command (m for help): p
Disk /dev/vda: 128.8 GB, 128849018880 bytes, 251658240 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0008168e
 Device Boot Start End Blocks Id System
/dev/vda1 * 2048 1026047 512000 83 Linux
/dev/vda2 1026048 209715199 104344576 8e Linux LVM
Command (m for help): n
Partition type:
 p primary (2 primary, 0 extended, 2 free)
 e extended
Select (default p):
Using default response p
Partition number (3,4, default 3):
First sector (209715200-251658239, default 209715200):
Using default value 209715200
Last sector, +sectors or +size{K,M,G} (209715200-251658239, default 251658239):
Using default value 251658239
Partition 3 of type Linux and of size 20 GiB is set
Command (m for help): t
Partition number (1-3, default 3):
Hex code (type L to list all codes): 8e
Changed type of partition 'Linux' to 'Linux LVM'
Command (m for help): p
Disk /dev/vda: 128.8 GB, 128849018880 bytes, 251658240 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0008168e
 Device Boot Start End Blocks Id System
/dev/vda1 * 2048 1026047 512000 83 Linux
/dev/vda2 1026048 209715199 104344576 8e Linux LVM
/dev/vda3 209715200 251658239 20971520 83 Linux LVM
Command (m for help): w
The partition table has been altered!
Calling ioctl() to re-read partition table.
WARNING: Re-reading the partition table failed with error 16: Device or resource busy.
The kernel still uses the old table. The new table will be used at
the next reboot or after you run partprobe(8) or kpartx(8)
Syncing disks.

[root@10-0-44-221 ~]# partprobe
```

3. 针对新格式化的分区，创建物理卷。

```
[root@10-0-44-221 ~]# pvcreate /dev/vda3
 Physical volume "/dev/vda3" successfully created
```

```
#创建物理卷
```

4. 针对卷组，进行扩展。

```
[root@10-0-44-221 ~]# vgextend vg /dev/vda3
  Volume group "vg" successfully extended
#卷组名称为vg，将新分区扩展至卷组vg
```

5. 关闭swap，删除原本的swap逻辑卷。

```
[root@10-0-44-221 ~]# swapoff -a
[root@10-0-44-221 ~]# lvremove /dev/vg/swap
Do you really want to remove active logical volume swap? [y/n]: yes
  Logical volume "swap" successfully removed
```

6. 将逻辑卷*/dev/vg/root*扩容20G。

```
[root@10-0-44-221 ~]# lvextend -L +20G /dev/vg/root
  Size of logical volume vg/root changed from 93.59 GiB (23959 extents) to 113.59 GiB
  (29079 extents).
  Logical volume root successfully resized.
#对/dev/vg/root 扩容20G

[root@10-0-44-221 ~]# lvdisplay
  --- Logical volume ---
  LV Path /dev/vg/root
  LV Name root
  VG Name vg
  LV UUID UkyCVW-gd5E-Z4Q2-bVHv-T84e-c3GH-ZMiUdF
  LV Write Access read/write
  LV Creation host, time localhost, 2017-07-26 13:18:40 +0800
  LV Status available
  # open 1
  LV Size 113.59 GiB
  Current LE 29079
  Segments 2
  allocation inherit
  Read ahead sectors auto
  - currently set to 8192
  Block device 253:0
```

7. 执行xfs_growfs进行xfs文件系统扩容，使其生效，并检查新分区。

```
[root@10-0-44-221 ~]# xfs_growfs /dev/vg/root
meta-data=/dev/mapper/vg-root isize=256 agcount=4, agsize=6133504 blks
  = sectsz=512 attr=2, projid32bit=1
  = crc=0 finobt=0
data = bsize=4096 blocks=24534016, imaxpct=25
  = sunit=0 swidth=0 blks
naming =version 2 bsize=4096 ascii-ci=0 ftype=0
log =internal bsize=4096 blocks=11979, version=2
  = sectsz=512 sunit=0 blks, lazy-count=1
realtime =none extsz=4096 blocks=0, rtextents=0
data blocks changed from 24534016 to 29776896

[root@10-0-44-221 ~]# df -h|grep vg-root
Filesystem Size Used Avail Use% Mounted on
/dev/mapper/vg-root 114G 6.5G 108G 6% /
```

```
#新分区扩容已生效
```

8. 从逻辑卷组划分新容量给swap分区，并启动swap分区，写入磁盘配置。

```
[root@10-0-44-221 ~]# lvcreate -L 4G -n swap vg
 Logical volume "swap" created.
#从卷组vg创建4G分区命名为swap

[root@10-0-44-221 ~]# mkswap /dev/vg/swap
Setting up swapspace version 1, size = 4194300 KiB
no label, UUID=bfc8a843-c758-4665-adfe-e32752ceda44
#创建swap分区，可知此swap分区的UUID为bfc8a843-c758-4665-adfe-e32752ceda44

[root@10-0-44-221 ~]# swapon /dev/mapper/vg-swap
#开启swap分区

[root@10-58-21-213 ~]# sed -i '/swap/d' /etc/fstab
echo "UUID=bfc8a843-c758-4665-adfe-e32752ceda44 swap swap defaults 0 0"
#将swap的设置写入磁盘分区表，以便开机自启。
```

9. 关机重启后，此云主机LVM分区的xfs系统成功扩容，swap分区也保留了4G使用。

3. Windows分区扩容实例

Windows分区可以在磁盘管理界面直接进行磁盘扩容。

注: Windows在线扩容后需重新扫描磁盘，如图 *133:* 重新扫描磁盘所示：

图 133: 重新扫描磁盘

7.2.1.4 云主机详情

7.2.1.4.1 云主机定时任务

定时任务能够帮助用户完成周期性的资源操作任务，比如根据业务需要定时开关云主机、重启云主机、为云主机根云盘创建快照等。ZStack支持定时器与定时任务实现松耦合，支持在不同的定时器上创建不同的定时任务，具体参考定时器章节。

点击云主机名称进去云主机详情页，点击**定时任务**，如图 *134:* 云主机定时任务界面所示：

图 134: 云主机定时任务界面

注: 更改云主机所有者后，定时任务会自动变为**停用**状态。

已创建的定时任务可以手动启用、停用和删除。当用户对ZStack中的资源创建了定时任务后，如果出现突发情况需要暂时停用此任务，此时可以停用定时任务功能，而不需要删除或修改已设定好的任务。当恢复正常任务周期，重新启用定时任务即可。

提示: 用户在创建了中午12：00（第一次执行）开始的根云盘快照任务，设定次数为10次，间隔时间为1小时，于下午14：30**停用**定时任务，此时已创建根云盘快照3次。

- 若用户在18：30启用定时任务，系统将继续执行剩下的3次任务，到21：00结束。
- 若用户在第二天启用此定时任务，则任务过期则不再执行。

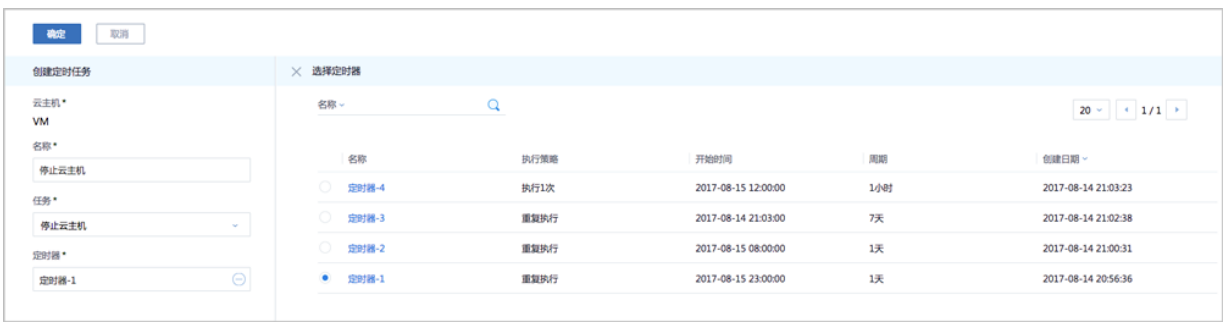
当恢复正常任务周期后，点击**启用**，所选定时任务就可以恢复正常使用了。

注: 若任务已经正常执行完毕，或者在暂停的过程中已经超出设定时间。定时任务状态自动变为**已完成**，所有定时任务以系统时间为准。

创建定时任务

在**云主机详情**的**定时任务**子页面，点击定时任务旁的**操作**按钮，选择**创建**，弹出**创建定时任务**界面，如图 *135:* 创建定时任务所示：

图 135: 创建定时任务



可参考示例输入相应内容：

- **名称**：自定义定时任务名称
- **任务**：选择任务类型

  目前云主机支持的定时任务类型包括：

  - 启动云主机
  - 停止云主机
  - 重启云主机
  - 创建云主机快照
- **定时器**：选择需要绑定的定时器

  注: 定时器需提前在**定时器**界面里设置好，具体参考定时器章节。

7.2.1.4.2 云主机监控数据

ZStack支持对云主机的实时性能监控，包括：CPU、内存、磁盘、网卡，监控数据自动实时更新。

CPU

支持选择不同的时间跨度来监控云主机CPU的实时使用率（单位：%）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年
- 监控条目：
  - All：将total和所有单个CPU的实时情况全部显示
  - total：显示云主机所有CPU的实时使用率的迭加
  - 单个CPU：单个CPU的实时使用率，例如：0、1、2号CPU

如图 *136: CPU实时监控*所示：

图 136: CPU实时监控

内存

支持选择不同的时间跨度来监控云主机内存的实时使用情况（单位：M）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年
- 监控条目：
  - All：同时实时显示云主机内存已使用和未使用的使用情况
  - used：实时显示云主机内存的已使用量
  - free：实时显示云主机内存的未使用量

如图 *137: 内存实时监控*所示：

图 137: 内存实时监控

注:

也可通过libvirt提供的virsh dommemstat命令来监控云主机内存的实时使用情况：

```
# 获取云主机ID
[root@localhost ~]# virsh list
```

```
 Id    名称                           状态
----------------------------------------------------
 1     fe3790c408204c9998ccd6b54272fab1 running

# 获取云主机内存的实时使用情况，单位为KB
[root@localhost ~]# virsh dommemstat 1
actual 2097152
swap_in 0
swap_out 16
major_fault 698
minor_fault 686260
unused 23876
available 2048544
rss 2147224
```

磁盘

支持选择不同的时间跨度来监控云主机磁盘的实时读/写情况（单位：B/S）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年
- 支持监控：
  - read+disk_octets：磁盘读速度
  - read+disk_ops：磁盘读IOPS
  - write+disk_octets：磁盘写速度
  - write+disk_ops：磁盘写IOPS
- 监控条目：
  - All：将hdc和vda分区的实时情况全部显示
  - 单个磁盘：显示单个磁盘的实时读/写速度，例如：vda磁盘

如图 *138: 磁盘实时监控*所示：

图 138: 磁盘实时监控

网卡

可选择不同的时间跨度来监控云主机网卡的实时情况（单位：B/s）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年。
- 支持监控：
  - rx+if_octets：网卡入包速度
  - rx+if_packets：网卡入包速率
  - rx+if_errors：网卡入包错误速率
  - tx+if_octets：网卡出包速度
  - tx+if_packets：网卡出包速率
  - tx+if_errors：网卡出包错误速率
- 监控条目：
  - All：将所有单个云主机网卡的使用情况全部显示
  - 单个网卡：显示单个云主机网卡的实时上行/下行速度，例如：网卡vnic7.0

如图 *139:* 网卡实时监控所示：

图 139: 网卡实时监控

7.2.1.4.3 云主机报警

背景信息

ZStack支持云主机报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加云主机CPU、磁盘、网卡、内存相关的多项报警条目，以邮件/钉钉/HTTP POST方式发送报警信息。

操作步骤

1. 进入**云主机详情**页的**报警**子页面，如图 *140:* 云主机报警界面所示。

图 140: 云主机报警界面

2. 创建报警器。

在云主机**报警**子页面，点击**操作**，在下拉菜单中选择**创建报警器**，弹出**创建报警器**界面，如图 *141:* 创建报警器界面所示：

图 141: 创建报警器界面

确定
取消
创建资源报警器
名称 *
VM
简介
资源类型 *
云主机
报警条目 *
CPU使用率
云主机 *
VM
CPU *
0
报警条件 *
大于
60
%
持续时间 *
10
秒
报警间隔时间
30
分
(系统默认报警间隔为30分钟)
接收端
钉钉类型接收端

3. 在云主机**报警**子页面，可对该云主机报警器进行管理。

后续操作

关于报警功能的详细介绍，请参考资源报警器章节。

7.2.2 云盘

云盘：为云主机提供存储。可分为：

- 根云盘：云主机的系统云盘，用于支撑云主机的系统运行。
- 数据云盘：云主机使用的数据云盘，一般用于扩展的存储使用。

云盘管理主要涉及数据云盘的管理。

注意事项

云盘使用时，需注意：

- 不同Hypervisor上的云盘不可挂载到不同类型的云主机上。例如，KVM云主机的云盘不能被VMWare云主机加载。
- 云盘占用空间采用虚拟容量来计算。创建云盘时扣除的是云盘的虚拟容量大小，而本身只占用少量实际容量。随着写入文件额增加，实际容量会逐步增加。
- （非共享）云盘同一时间只能挂载到一个云主机。Ceph类型的主存储支持共享云盘，共享云盘可被多个云主机识别并同时访问。
- 根云盘作为云主机的附属，不能卸载。
- 数据云盘可在相同类型Hypervisor的不同云主机之间挂载和卸载。
- 多个主存储环境下，可以指定主存储创建云盘。如果未指定主存储：
  - 针对本地主存储，云盘默认会从容量大的主存储创建。
  - 针对NFS主存储，云盘默认会随机选择一个主存储创建。
  - 针对本地主存储+NFS/Shared Mount Point类型主存储，默认会选择与当前根云盘不在同一个主存储的存储来创建。
- 数据云盘可设置QoS进行磁盘带宽限速，需注意限速不可过低，过低的QoS可能导致IO性能过低。

7.2.2.1 云盘操作

在ZStack私有云主菜单，点击**云资源池** > **云盘**，进入**云盘**管理界面，如图 *142:* 云盘管理界面所示：

图 142: 云盘管理界面

云盘管理界面，分为三栏：

- **已有**：系统当前可用的云盘列表。
- **未实例化**：未实例化云盘列表。
  - 未实例化主要指没有实际占用任何空间，只是一个概念性的设备，当挂载到云主机后，才会实例化。
  - 在创建云盘时，如果只选择云盘规格，不选择其他选项，创建出来的就是未实例化的云盘。
- **已删除**：已被删除但尚未彻底删除的云盘列表。可以执行恢复和彻底删除。

系统对云盘操作的定义如下：

- **创建云盘**：基于云盘规格创建一个新的云盘。
- **启用**：将处于停用状态的云盘启用。**支持批量操作。**
- **停用**：停止使用某个云盘。**支持批量操作。**
- **加载**：将选中的云盘作为数据云盘加载到指定的云主机。**只支持单一操作。**
  - 若主存储为本地存储，如果加载一个卸载过的云盘，需要保证该云盘和目标云主机在同一台物理机上。如果该云盘和目标云主机不在同一台物理机上，需将云盘和云主机迁移到同一台物理机上。
    - 云主机迁移请参考云主机迁移。
    - 云盘迁移请参考云盘迁移
- **卸载**：卸载云主机的云盘。**只支持单一操作。**

- **迁移**：云盘迁移到其他物理机。**只支持单一操作。**

  注: 该**迁移**操作只针对本地主存储。

- **创建灾备数据**：对当前云主机、镜像或云盘进行灾备备份；云主机和镜像会备份成镜像进行保存；云盘会备份成云盘备份进行保存。
- **创建镜像**：对当前云盘进行创建镜像操作，此镜像可用于创建新的云盘。

  注:

  - ZStack 支持创建云盘镜像，且支持Ceph主存储上的云盘创建云盘镜像到镜像仓库类型的镜像服务器。
- **创建快照**：对云盘支持在线快照操作。**只支持单一操作。**
  - 快照可以保存当前云盘的所有数据，用户可以使用快照快速的把云盘的状态恢复到历史的某个状态。
  - 首次创建快照，可能需较久时间来进行快照存储。
- **删除快照**：删除当前快照。**只支持单一操作**

  具体操作：云盘详情界面，点击**云盘快照**栏，选择需要删除的快照，进入**快照详情**界面，点击**快照操作** > **删除**，可将此快照删除。
- **恢复快照**：只能操作一个已卸载或已停止的云主机上的云盘。**只支持单一操作。**

  具体操作：云盘详情界面，点击**云盘快照**栏，选择需要恢复的快照，进入**快照详情**界面，点击**快照操作** > **恢复**，就可以把该云盘还原到当前快照状态。
- **更改所有者**：可以更改云盘的所有者。**支持批量操作。**
- **云盘扩容**：在云主机运行或者停止状态下，支持对根云盘/数据云盘扩容，扩容容量只增不减，增量不得小于4MB。更改容量即时生效。
- **存储迁移**：云盘支持跨网络共享存储的迁移，目前支持跨Ceph存储迁移、跨NFS存储迁移以及跨Shared Block迁移

  注:

  - 跨Ceph存储迁移：
    - 云盘进行跨Ceph存储迁移之前，需先确认该云盘没有被挂载到任何云主机上或挂载该云盘的云主机已停止。
    - 所涉及的两个Ceph存储，要求彼此的mon节点可以互通。

  - 跨NFS存储迁移：
    - 云盘进行跨NFS存储迁移之前，需先确认该云盘没有被挂载到任何云主机上或挂载该云盘的云主机已停止。
    - 所涉及的两个NFS存储，要求目标NFS存储能够被挂载到待迁移云盘所在集群。
  - 跨Shared Block存储迁移：
    - 云盘进行跨Shared Block存储迁移之前，需先确认该云盘没有被挂载到任何云主机上或挂载该云盘的云主机已停止。
    - 所涉及的两个Shared Block存储，要求目标Shared Block存储能够被挂载到待迁移云盘所在集群。
- **删除**：将云盘删除后， 云盘会显示在**已删除**栏。**删除支持批量操作。**
- **恢复**：已删除的云盘支持恢复操作，恢复后镜像将显示在可用栏。**支持批量操作。**
- **彻底删除**：已删除的云盘彻底删除。**支持批量操作。**
- **搜索**：云盘资源的搜索目前支持名称、UUID、所有者以及高级搜索
- **定时任务**：云盘的定时任务，可以定时为数据云盘创建快照，详情参考云盘定时任务。**只支持单一操作**

7.2.2.2 创建云盘

在**云盘**管理界面，点击**创建云盘**按钮，弹出**创建云盘**界面，可以创建一个云盘并将其加载到云主机，创建云盘支持云盘规格方式和云盘镜像方式。

1. **基于云盘规格创建云盘**：

   如图 *143:* 云盘规格方式创建云盘所示：

   图 143: 云盘规格方式创建云盘

可参考以下示例输入相应内容：

- **名称**：输入云盘名称
- **简介**：可选项，可留空不填
- **创建方式**：选择云盘规格方式，并选择合适的云盘规格

- **主存储**和**云主机**：
  - 两个都不填写：创建的云盘为未实例化的云盘，显示在未实例化栏中。
  - 只填写云主机：创建的云盘会自动在云主机所在的主存储中创建成功。
  - 只填写主存储：创建的云盘会是可用状态，会占用真正的空间 。

  注:

  - 主存储选择**本地存储**：必须指定物理机
  - 主存储选择**Ceph**或者**FusionStor**：必须指定pool
- **物理机**：选择云盘要挂载的物理机
- **VirtioSCSI**：默认勾选此项。勾选此项后，并且初始化云盘，系统会自动给云盘创建唯一识别ID（WWN）。云主机（例如Linux）启动后，从*/dev/disk/by-id/*下可以查看WWN。WWN是为了方便用户加载和卸载数据云盘
- **共享云盘**：如果需要勾选此项，必须先勾选VirtioSCSI选项。勾选后，创建的云盘可以挂载到多个云主机上

  注:

  - 只有在Ceph、Shared Block或者FusionStor主存储的环境下才能实现共享云盘。
  - 同时读写云盘可能造成数据的不一致，请在明确需求的情况下使用此功能。禁止在写云盘的过程中，卸载对应的云主机。

2. **基于云盘镜像创建云盘**

   如图 *144:* 云盘镜像方式创建云盘所示：

   图 144: 云盘镜像方式创建云盘

可参考以下示例输入相应内容：

- **名称**：输入云盘名称
- **简介**：可选项，可留空不填
- **创建方式**：选择云盘镜像方式并选择合适的云盘镜像
- **云主机**：选择需要绑定的云主机
- **指定主存储**：可选项，若勾选此项，需指定主存储

注:

- ZStack 支持来自镜像仓库类型镜像服务器的云盘镜像，创建云盘到Ceph主存储上。

7.2.2.3 云盘详情

在**云盘**管理界面，点击云盘名称，打开云盘详情页，如图 *145: 云盘详情页*所示。可通过**云盘操作**按钮对当前云盘进行操作，所包含的操作菜单是云盘管理界面上所有操作的合集。

图 145: 云盘详情页

详情页分为以下4栏：

- **基本属性**：查看云盘的基本信息。在此栏可以更改云盘的名字、简介和磁盘带宽。
- **云盘快照**：对云盘支持在线快照操作。在云盘快照栏， 可以创建快照，以及显示已有快照的结构图， 最底下的是快照的起始，最上边的是当前最新的快照。 如图 *146: 云盘快照*所示。

  图 146: 云盘快照

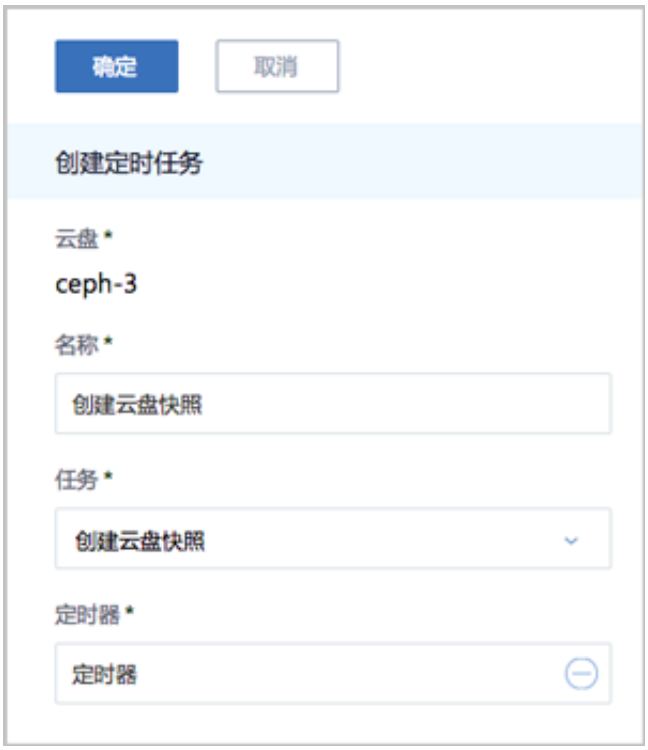
注: 本地存储、NFS、SMP和Shared Block存储创建的快照为树状模式，删除树根快照，树叶快照也会被删除；Ceph存储下创建的快照是独立的，删除某一快照，不影响其他快照。

- **定时任务**：云盘的定时任务，可以定时为数据云盘创建快照，详情参考云盘定时任务。
- **审计**：显示与此云盘相关的日志。

7.2.2.3.1 云盘定时任务

目前云盘定时任务只支持数据盘快照任务，支持创建、启用、停用、删除定时任务。如图 *147: 创建定时任务界面*所示：

图 147: 创建定时任务界面



云盘定时任务的设置与云主机定时任务设置方法完全一样，参照云主机定时任务章节。

7.2.3 镜像

镜像：云主机或云盘所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。
- 系统云盘镜像支持ISO和Image类型，数据云盘镜像支持Image类型。
- Image类型支持raw和qcow2两种格式。
- 镜像保存在镜像服务器上，首次创建云主机/云盘时，会下载到主存储上作为镜像缓存。

镜像平台类型决定了创建云主机时是否使用KVM Virtio驱动（包括磁盘驱动和网卡驱动），支持以下类型：

- Linux：使用Virtio驱动；
- Windows：不使用Virtio驱动，使用Qemu模拟设备。镜像操作系统是未安装Virtio的Windows；
- WindowsVirtio：使用Virtio驱动。镜像操作系统是已安装Virtio驱动（包括磁盘驱动和网卡驱动）的Windows；
- Other：不使用Virtio驱动，使用Qemu模拟设备。镜像操作系统可以是任何操作系统。
- Paravirtualization：使用Virtio驱动。镜像操作系统可以是已安装Virtio驱动的任何操作系统；

镜像路径支持添加URL路径或本地文件上传两种方式：

1. URL：采用指定的URL路径来添加镜像。

   - 支持*HTTP/HTTPS*方式：
     - 填写格式为：*http://path/file*或*https://path/file*
     - 例如：*http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2*
   - 支持*FTP*方式：
     - 匿名模式：*ftp://hostname[:port]/path/file*

       例如：*ftp://172.20.0.10/pub/zstack-image.qcow2*
     - 非匿名模式：*ftp://user:password@hostname[:port]/path/file*

       例如：*ftp://zstack:password@172.20.0.10/pub/zstack-image.qcow2*
   - 支持*SFTP*方式：
     - 指定密码模式：*sftp://user:password@hostname[:port]/path/file*

       例如：*sftp://root:password@172.20.0.10/pub/zstack-image.qcow2*
     - 免密模式：*sftp://user@hostname[:port]/path/file*

       例如：*sftp://root@172.20.0.10/pub/zstack-image.qcow2*
   - 镜像服务器上的绝对路径，支持Sftp镜像服务器和镜像仓库

     例如：*file:///opt/zstack-dvd/zstack-image-1.4.qcow2*

   注:

   - 输入URL时，需确保可被镜像服务器访问，且存在此镜像文件。
   - 使用*SFTP*免密模式上传镜像时，需提前确保镜像服务器与Sftp服务器可互相SSH免密登录。
   - 关于平滑连续进度条显示和断点续传：
     - 若使用镜像仓库，支持平滑连续进度条显示，且支持断点续传；
     - 若使用Ceph或FusionStor镜像服务器，支持平滑连续进度条显示，不支持断点续传；
     - 若使用Sftp镜像服务器，不支持平滑连续进度显示，且不支持断点续传。
   - 关于*file:///*方式上传镜像
     - 若使用Ceph或FusionStor镜像服务器，目前暂不支持*file:///*格式的输入；

- *file:///*是三个/，对应的路径应为镜像服务器的**绝对路径**，例如*file:///opt/zstack-dvd/zstack-image-1.4.qcow2*，在镜像服务器的*/opt/zstack-dvd*目录下应存放有*zstack-image-1.4.qcow2*文件。

2. 本地文件上传：表示选择当前浏览器可访问的镜像直接上传，支持镜像仓库和Ceph镜像服务器。

   如图 *148:* 支持浏览器本地上传镜像所示：

   图 148: 支持浏览器本地上传镜像

注:

添加本地文件作为镜像，采用了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。

7.2.3.1 镜像操作

在ZStack私有云主菜单，点击**云资源池** > **镜像**，进入**镜像**管理界面，如图 *149:* 镜像管理界面所示。在**镜像管理**界面，可以查看镜像列表信息，如：名称、镜像服务器、镜像类型、镜像格式、启用状态、就绪状、容量、平台、所有者、创建日期等。并可对镜像进行添加、启用、停用、导出、全局共享、全局召回、更改所有者、存储迁移、删除、彻底删除、恢复等操作。

从图 *149:* 镜像管理界面中可以看到，下载镜像时，就绪状态为**下载中**。

图 149: 镜像管理界面

镜像管理界面，分为三栏：

- **已有**：显示目前可用的镜像列表。
- **已删除**：显示目前已被删除但尚未彻底删除的镜像列表。
- **已导出**：显示导出的镜像列表。

注: 只有镜像仓库类型的镜像服务器上的镜像支持镜像导出及导出镜像删除功能。

ZStack对镜像操作的定义如下：

- **添加镜像**：添加一个新的镜像到镜像服务器。

注:

- ZStack 支持添加云盘镜像。

- **启用**：将处于停用状态的镜像启用。**支持批量操作。**
- **停用**：停止使用某个镜像，停止后不能再用其创建云主机，但不影响之前已创建的云主机。**支持批量操作。**
- **导出**：选中一个镜像，点击**导出**按钮，后台会进入导出镜像操作。由于镜像可能较大，导出的时间会较长。导出后的镜像显示在**已导出**栏。**只支持单一操作。**

注: 只有镜像仓库类型的镜像服务器上的镜像支持镜像导出及导出镜像删除功能。

- **全局共享**：将镜像进行全局共享后，所有的账户都可以使用此镜像。**支持批量操作。**
- **全局召回**：将已全局共享的镜像进行全局召回后，其他账户将看不见此镜像。**支持批量操作。**
- **更改所有者**：可以更改镜像的所有者。**支持批量操作。**
- **存储迁移**：镜像支持跨网络共享存储的数据迁移，目前支持跨Ceph类型镜像服务器的迁移

注:

    - 跨Ceph类型镜像服务器迁移：
        - 所涉及的两个Ceph存储，要求彼此的mon节点可以互通。
- **删除**：将镜像删除后， 镜像会显示在**已删除**栏。**支持批量操作。**
- **QGA**：修改Qemu guest agent的状态。
    - 开启QGA前，需确保该镜像已安装并运行Qemu guest agent。
    - 开启QGA后，该镜像创建的云主机默认支持在线修改密码。
- **恢复**：将已删除的镜像恢复，恢复后镜像将显示在**可用**栏。 **支持批量操作。**
- **彻底删除**：将已删除的镜像彻底删除。只有已删除的镜像才支持彻底删除。**支持批量操作。**
- **下载**：可下载已导出的镜像。点击**下载**按钮，会直接在使用的浏览器中开始下载。**支持批量操作。**
- **复制URL**：可以复制已导出镜像的URL。点击复制按钮，则将镜像的URL写入系统的剪贴板中，可以直接复制到浏览器或者下载工具中下载，也可以直接作为添加镜像的URL使用。**只支持单一操作。**
- **已导出**页面的**删除**：将已导出的镜像删除。**支持批量操作。**

  注:

  在镜像仓库中，镜像文件以差量形式存储，只有在使用时（例如创建云主机或者导出镜像）才会产生一个完整镜像文件。该删除操作只删除该完整镜像。镜像服务器中的原有镜像保持不变。
- **搜索**：支持名称，UUID，镜像服务器，所有者以及高级搜索。

7.2.3.2 添加镜像

1. 添加系统镜像

   在**镜像**管理界面，点击**添加镜像**按钮，弹出**添加镜像**界面，如图 *152:* 添加云盘镜像所示：

   图 150: 添加系统镜像

可参考以下示例输入相应内容：

- **名称**：设置镜像名称
- **简介**：可选项，可留空不填
- **镜像类型**：选择系统镜像，支持qcow2、iso和raw镜像格式。

- **平台**：镜像平台类型决定了创建云主机时是否使用KVM Virtio驱动（包括磁盘驱动和网卡驱动）

  支持以下类型：

  - Linux：使用Virtio驱动；
  - Windows：不使用Virtio驱动，使用Qemu模拟设备。镜像操作系统是未安装Virtio的Windows；
  - WindowsVirtio：使用Virtio驱动。镜像操作系统是已安装Virtio驱动（包括磁盘驱动和网卡驱动）的Windows；
  - Other：不使用Virtio驱动，使用Qemu模拟设备。镜像操作系统可以是任何操作系统。
  - Paravirtualization：使用Virtio驱动。镜像操作系统可以是已安装Virtio驱动的任何操作系统；
- **镜像服务器**：选择已创建的镜像服务器。
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

  1. URL：采用指定的URL路径来添加镜像。
     - 支持*HTTP/HTTPS*方式：
       - 填写格式为：*http://path/file*或*https://path/file*
       - 例如：*http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2*
     - 支持*FTP*方式：
       - 匿名模式：*ftp://hostname[:port]/path/file*

         例如：*ftp://172.20.0.10/pub/zstack-image.qcow2*
       - 非匿名模式：*ftp://user:password@hostname[:port]/path/file*

         例如：*ftp://zstack:password@172.20.0.10/pub/zstack-image.qcow2*
     - 支持*SFTP*方式：
       - 指定密码模式：*sftp://user:password@hostname[:port]/path/file*

         例如：*sftp://root:password@172.20.0.10/pub/zstack-image.qcow2*
       - 免密模式：*sftp://user@hostname[:port]/path/file*

         例如：*sftp://root@172.20.0.10/pub/zstack-image.qcow2*
     - 镜像服务器上的绝对路径，支持Sftp镜像服务器和镜像仓库

例如：*file:///opt/zstack-dvd/zstack-image-1.4.qcow2*

注:

- 输入URL时，需确保可被镜像服务器访问，且存在此镜像文件。
- 使用*SFTP*免密模式上传镜像时，需提前确保镜像服务器与Sftp服务器可互相SSH免密登录。
- 关于平滑连续进度条显示和断点续传：
  - 若使用镜像仓库，支持平滑连续进度条显示，且支持断点续传；
  - 若使用Ceph或FusionStor镜像服务器，支持平滑连续进度条显示，不支持断点续传；
  - 若使用Sftp镜像服务器，不支持平滑连续进度显示，且不支持断点续传。
- 关于*file:///*方式上传镜像
  - 若使用Ceph或FusionStor镜像服务器，目前暂不支持*file:///*格式的输入；
  - *file:///*是三个/，对应的路径应为镜像服务器的**绝对路径**，例如*file:///opt/zstack-dvd/zstack-image-1.4.qcow2*，在镜像服务器的*/opt/zstack-dvd*目录下应存放有*zstack-image-1.4.qcow2*文件。

2. 本地文件上传：表示选择当前浏览器可访问的镜像直接上传，支持镜像仓库和Ceph镜像服务器。

如图 *151:* 支持浏览器本地上传镜像所示：

图 151: 支持浏览器本地上传镜像

注:

添加本地文件作为镜像，采用了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。

- **Qemu guest agent**：

  注:

  - 请务必确保被导入的镜像已安装Qemu guest agent，并已设置为自启动。
  - 满足以上条件后，勾选**Qemu guest agent**选项，则由添加的镜像创建出来的云主机，以及该云主机克隆生成的云主机或创建的镜像，可在运行状态下从外部修改云主机密码。

2. 添加云盘镜像

   在**镜像**管理界面，点击**添加镜像**按钮，弹出**添加镜像**界面，如图 *152:* 添加云盘镜像所示：

   图 152: 添加云盘镜像

可参考以下示例输入相应内容：

- **名称**：设置镜像名称
- **简介**：可选项，可留空不填
- **镜像类型**：选择云盘镜像，支持qcow2、raw镜像格式。
- **平台**：镜像平台类型决定了创建云主机时是否使用KVM Virtio驱动（包括磁盘驱动和网卡驱动）
- **镜像服务器**：选择已创建的镜像服务器。
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

7.2.3.3 镜像详情

在**镜像**管理界面，点击镜像名称，打开镜像详情界面，如图 *153: 镜像详情界面*所示。还有一个**镜像操作**按钮可以对当前镜像进行操作，它里面的操作菜单是镜像管理界面上所有操作的合集。

图 153: 镜像详情界面

详情界面分为以下3栏：

- **基本属性**：概括了此镜像的基本信息。在此栏可以更改镜像的名称和简介。

  注: 系统会根据镜像平台的类型，给云主机使用不同的设备。例如，Linux和Windows Virtio平台使用快速的Virtio设备；Windows平台使用QEMU模拟的普通硬盘和Intel Pro\/MT 1000网卡设备。如果平台类型在添加时填写错误，可以在这里进行更改。

- **共享**：显示所有共享当前镜像的账户。
- **审计**：显示当前镜像相关的日志。

7.2.4 亲和组

7.2.4.1 介绍

亲和组（Affinity Group）是一种针对IaaS资源的简单编排策略，可用于保障用户业务的高性能或高可用。

亲和组策略

目前ZStack提供针对云主机与物理机的两种亲和组策略：反亲和组(非强制)、反亲和组(强制)。

- 反亲和组(非强制)：

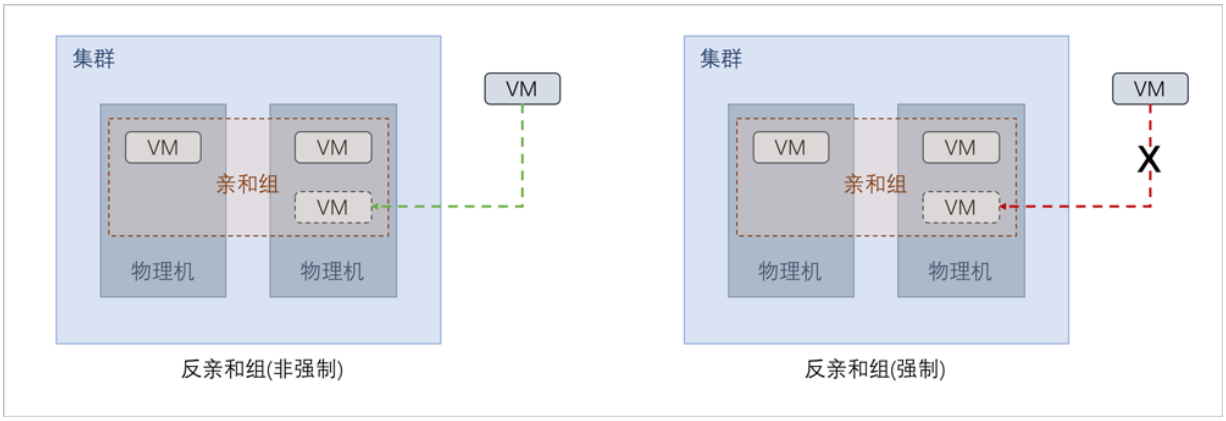
  将亲和组内的云主机尽量分配到不同物理机上，当没有更多物理机可分配时，回归普通分配策略。

- 反亲和组(强制)：

  将亲和组内的云主机严格分配到不同物理机上，当没有更多物理机可分配时，则分配失败。

如图 *154:* 反亲和组(非强制)与反亲和组(强制)所示：

图 154: 反亲和组(非强制)与反亲和组(强制)



应用场景

以下介绍反亲和组(非强制)和反亲和组(强制)策略的应用场景。

- 反亲和组(非强制)策略应用场景举例：

  希望Hadoop不同角色的节点尽量分散部署在不同的物理机上，提高系统整体性能。

  - 例如用户部署Hadoop系统，对于namenode、datanode、jobtracker、tasktracker等不同角色，事先并不能预知总共有多少个节点，但显然部署到不同物理机上效率更高。采用反亲和组(非强制)策略，可使Hadoop集群尽量分散部署在不同物理机上，分散IO压力提高系统整体性能。

- 反亲和组(强制)策略应用场景举例：

  承载主备数据库的两台云主机要求部署在不同的物理机上，保障业务高可用。

  - 例如用户部署两台业务云主机分别承载主备MySQL数据库，并要求主备数据库不能同时宕机，因此两台云主机必须部署在不同物理机上。由于部署自动化，用户事先并不能预知哪些物理机上有资源，采用反亲和组(强制)策略，可选出两个不同的物理机分别运行这两台云主机，保障业务高可用。

7.2.4.2 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。

本教程将详细介绍针对 云主机 | 物理机 的两种亲和组策略的使用方法。

7.2.4.3 使用入口

针对 云主机| 物理机 的亲和组策略的使用，主要涉及以下两个入口：

- **云资源池 > 亲和组**
- **云资源池 > 云主机**

7.2.4.3.1 亲和组

本节主要介绍从**云资源池 > 亲和组**入口，有关 云主机 | 物理机 的亲和组策略的使用。

亲和组管理界面

在ZStack私有云主菜单，点击**云资源池 > 亲和组**，进入**亲和组**管理界面。

在**亲和组**管理界面，可查看当前已有的全部亲和组信息，包括：亲和组名称、指定策略、绑定云主机数量、亲和组类型、所有者、创建日期，并可对亲和组进行创建、启用、停用、以及更多操作。

如图 *155:* 亲和组管理界面所示：

图 155: 亲和组管理界面

创建亲和组

在**亲和组**管理界面，点击**创建亲和组**，弹出**创建亲和组**界面，可参考以下示例输入相应内容：

- **名称**：设置亲和组名称
- **简介**：可选项，可留空不填
- **策略**：选择亲和组策略

目前ZStack提供针对云主机与物理机的两种亲和组策略：

- 反亲和组(非强制)：

  将亲和组内的云主机尽量分配到不同物理机上，当没有更多物理机可分配时，回归普通分配策略。

- 反亲和组(强制)：

  将亲和组内的云主机严格分配到不同物理机上，当没有更多物理机可分配时，则分配失败。

如图 *156:* 创建反亲和组(非强制)策略的亲和组所示：

图 156: 创建反亲和组(非强制)策略的亲和组

亲和组详情页

在**亲和组**管理界面，点击相应亲和组名称展开其详情页，如图 *157:* 亲和组详情页所示：

图 157: 亲和组详情页

亲和组详情页包含以下子页面：

- **基本属性**：

  显示当前亲和组的基本信息，包括：亲和组名称、简介、绑定云主机数量、指定策略、亲和组类型和UUID等。

  注: 亲和组创建后，必已指定策略和类型，且只可修改名称和简介，其它参数不可修改。

- **云主机**：

  显示当前亲和组绑定的全部云主机列表，支持绑定新的云主机到亲和组、或从亲和组解绑云主机。

- **审计**：

  显示当前亲和组的相关操作日志。

亲和组支持的操作

亲和组支持以下操作：

- 创建：在当前区域中创建一个新的亲和组。
- 启用：重新启用选中的亲和组，将检查组内云主机是否满足所属组策略，若均满足，亲和组成功启用，否则亲和组启用失败。
- 停用：停止使用选中的亲和组，组内云主机将停止遵循所属组策略。

- 绑定云主机：绑定新的云主机到亲和组，组策略即时生效。
- 解绑云主机：将云主机从从亲和组解绑，组策略即时生效。
- 更改所有者：更改亲和组的所有者。
- 删除：删除选中的亲和组，组内云主机下次启动时不再遵循组策略。

约束条件

- 亲和组策略目前支持反亲和组(非强制)和反亲和组(强制)，亲和组类型目前支持HOST，即云主机与物理机的亲和。
- 亲和组绑定的云主机数量可自行控制，没有上限限制。亲和组也没有配额限制，可创建无限个。
- 亲和组的作用域为整个区域，作用对象为区域内全部满足条件的物理机。
- 一个云主机同一时间只允许属于一个亲和组。
- 当云主机处于运行状态或已停止状态，才允许变更所属亲和组。
- 本地存储上的云主机变更所属亲和组后，将优先选择last host启动，而不是遵循新的组策略启动（避免不必要的迁移）。
- 共享存储上的云主机变更所属亲和组后，将遵循新的组策略启动。
- 绑定云主机/解绑云主机操作，组策略均即时生效；只有共享存储上处于已停止状态的云主机绑定到亲和组，组策略在云主机下次启动时生效。
- 迁移云主机也需遵循亲和组策略。
- 所有云路由器和VPC路由器默认都属于一个亲和组（可称之为系统组），该亲和组只允许启用和停用，不允许其它操作。
- admin账户以及普通账户均支持创建亲和组。
- admin账户可对所有亲和组进行操作，普通账户只能对本账户拥有的亲和组进行操作。

7.2.4.3.2 云主机

本节主要介绍从**云资源池** > **云主机**入口，有关 云主机 | 物理机 的亲和组策略的使用。

创建云主机 指定亲和组

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

- **添加方式**：选择单个
- **名称**：设置云主机名称
- **简介**：可选项，可留空不填

- **计算规格**：选择合适的计算规格
- **镜像**：选择创建云主机的镜像
- **网络**：选择创建云主机的网络
- **高级设置**：高级设置均为可选项，用户可按需设置

  如希望云主机遵循某亲和组策略创建：

  - **亲和组**：选择已有的某一亲和组（亲和组必已指定策略和类型）

如图 *158:* 创建云主机 指定亲和组所示：

图 158: 创建云主机 指定亲和组

确定
取消
创建云主机
添加方式
单个
多个
名称 *
云主机
简介
计算规格 *
InstanceOffering-1
镜像 *
Image-1
网络 *
L3-私有网络
默认网络
设置网卡
高级
数据云盘规格
亲和组
亲和组-反亲和组(强制)

云主机详情页 显示所属亲和组

在**云主机**管理界面，点击相应云主机名称展开其详情页，点击**基本属性**进入**基本属性**子页面，可见该云主机当前所属亲和组，点击该亲和组名称可跳转至亲和组详情页查看更多信息。

如图 *159:* 云主机详情页所示：

图 159: 云主机详情页

云主机支持关于亲和组的操作

云主机支持以下关于亲和组的操作：

- 创建云主机指定亲和组：创建云主机时可以指定一个亲和组，云主机将基于指定组策略创建。
- 克隆云主机指定亲和组：克隆云主机时可以指定一个亲和组，云主机将基于指定组策略克隆。
- 绑定亲和组：绑定云主机到亲和组，组策略对该云主机即时生效。
- 解绑亲和组：将云主机从从亲和组解绑，组策略对该云主机即时失效。

约束条件

创建云主机时，如果在高级设置中同时指定了亲和组和物理机：

- 指定亲和组策略为反亲和组(非强制)：

  - 当指定物理机满足创建云主机条件，但不满足指定亲和组策略时，云主机创建成功；
  - 当指定物理机不满足创建云主机条件时，云主机创建失败。
- 指定亲和组策略为反亲和组(强制)：
  - 当指定物理机满足创建云主机条件，但不满足指定亲和组策略时，云主机创建失败；
  - 当指定物理机不满足创建云主机条件时，云主机创建失败。

7.2.4.4 场景实践

以下主要介绍针对 云主机 | 物理机 的两种亲和组策略的场景实践。

- 云主机 | 物理机 反亲和组(非强制)
- 云主机 | 物理机 反亲和组(强制)

7.2.4.4.1 云主机 | 物理机 反亲和组(非强制)

背景信息

本节主要介绍 云主机 | 物理机 的反亲和组(非强制)策略的场景实践。

假定场景如下：在一个集群环境中，用户准备部署四台业务云主机，希望它们尽量分散部署在三台不同物理机上。

基本流程：

1. 创建一个反亲和组(非强制)策略的亲和组。
2. 创建四台业务云主机指定该亲和组。
3. 验证：四台业务云主机尽量分散部署在三台不同物理机上。

操作步骤

1. 创建一个反亲和组(非强制)策略的亲和组。

   在ZStack私有云主菜单，点击**云资源池** > **亲和组**，进入**亲和组**管理界面，点击**创建亲和组**，弹出**创建亲和组**界面，可参考以下示例输入相应内容：

   - **名称**：设置亲和组名称，例如亲和组-反亲和组(非强制)
   - **简介**：可选项，可留空不填
   - **策略**：指定亲和组策略：反亲和组(非强制)

   如图 *160:* 创建反亲和组(非强制)策略的亲和组所示：

   图 160: 创建反亲和组(非强制)策略的亲和组

2. 创建四台业务云主机指定该亲和组。

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

   - **添加方式**：选择多个
   - **创建数量**：4
   - **名称**：设置云主机名称
   - **简介**：可选项，可留空不填
   - **计算规格**：选择合适的计算规格
   - **镜像**：选择创建云主机的镜像
   - **网络**：选择创建云主机的网络
   - **高级设置**：高级设置均为可选项，用户可按需设置，本场景需设置以下内容：
     - **亲和组**：选择已创建的反亲和组(非强制)策略的亲和组

   如图 *161:* 创建云主机 指定亲和组所示：

   图 161: 创建云主机 指定亲和组

确定
取消
创建云主机
添加方式
单个
多个
创建数量 *
4
名称 *
业务云主机
简介
计算规格 *
InstanceOffering-1
镜像 *
Image-1
网络 *
L3-私有网络
默认网络
设置网卡
高级
数据云盘规格
亲和组
亲和组-反亲和组(非强制)

3. 验证：四台业务云主机尽量分散部署在三台不同物理机上。

   在**云主机**管理界面，可见四台业务云主机尽量分散部署在三台不同物理机上，反亲和组(非强制)策略生效。

   如图 *162:* 验证反亲和组(非强制)策略所示：

   图 162: 验证反亲和组(非强制)策略

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者
业务云主机-1	1	1 GB	192.168.82.251	10.0.41.182	Cluster-1	运行中	admin
业务云主机-4	1	1 GB	192.168.82.119	10.0.235.164	Cluster-1	运行中	admin
业务云主机-3	1	1 GB	192.168.82.205	10.0.41.182	Cluster-1	运行中	admin
业务云主机-2	1	1 GB	192.168.82.161	10.0.55.46	Cluster-1	运行中	admin

7.2.4.4.2 云主机 | 物理机 反亲和组(强制)

背景信息

本节主要介绍 云主机 | 物理机 的反亲和组(非强制)策略的场景实践。

假定场景如下：在一个集群环境中，用户准备部署三台业务云主机，要求它们必须分别部署在三台不同物理机上。

基本流程：

1. 创建一个反亲和组(强制)策略的亲和组。
2. 创建三台业务云主机指定该亲和组。
3. 验证：三台业务云主机必须分别部署在三台不同物理机上。

操作步骤

1. 创建一个反亲和组(强制)策略的亲和组。

   在ZStack私有云主菜单，点击**云资源池 > 亲和组**，进入**亲和组**管理界面，点击**创建亲和组**，弹出**创建亲和组**界面，可参考以下示例输入相应内容：

   - **名称**：设置亲和组名称，例如亲和组-反亲和组(强制)
   - **简介**：可选项，可留空不填
   - **策略**：指定亲和组策略：反亲和组(强制)

如图 *163:* 创建反亲和组(强制)策略的亲和组所示：

图 163: 创建反亲和组(强制)策略的亲和组

2. 创建三台业务云主机指定该亲和组。

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

   - **添加方式**：选择多个
   - **创建数量**：3
   - **名称**：设置云主机名称
   - **简介**：可选项，可留空不填
   - **计算规格**：选择合适的计算规格
   - **镜像**：选择创建云主机的镜像
   - **网络**：选择创建云主机的网络
   - **高级设置**：高级设置均为可选项，用户可按需设置，本场景需设置以下内容：
     - **亲和组**：选择已创建的反亲和组(强制)策略的亲和组

   如图 *164:* 创建云主机 指定亲和组所示：

   图 164: 创建云主机 指定亲和组

确定
取消
创建云主机
添加方式
单个
多个
创建数量 *
3
名称 *
业务云主机
简介
计算规格 *
InstanceOffering-1
镜像 *
Image-1
网络 *
L3-私有网络
默认网络
设置网卡
高级
数据云盘规格
亲和组
亲和组-反亲和组(强制)

3. 验证：三台业务云主机必须分别部署在三台不同物理机上。

   在**云主机**管理界面，可见三台业务云主机分别部署在三台不同物理机上，反亲和组(强制)策略生效。

   如图 *165:* 验证反亲和组(强制)策略所示：

   图 165: 验证反亲和组(强制)策略

名称	CPU	内存	默认IP	物理机IP	集群	启用状态	所有者
业务云主机-1	1	1 GB	192.168.82.237	10.0.41.182	Cluster-1	运行中	admin
业务云主机-2	1	1 GB	192.168.82.211	10.0.55.46	Cluster-1	运行中	admin
业务云主机-3	1	1 GB	192.168.82.84	10.0.235.164	Cluster-1	运行中	admin

后续操作

至此，针对 云主机 | 物理机 的两种亲和组策略的使用方法介绍完毕。

7.2.5 计算规格

计算规格：云主机的CPU、内存、物理机分配策略、磁盘带宽、网络带宽的数量或大小规格定义。

7.2.5.1 计算规格操作

在ZStack私有云主菜单，点击**云资源池** > **计算规格**，进入**计算规格**管理界面，如图 *166:* 计算规格管理界面所示。在**计算规格**管理界面，可以查看计算规格列表的信息，如：名称、CPU、内存、启用状态、物理机分配策略等。并可对计算规格进行创建、启用、停用、全局共享、全局召回、删除等操作。

图 166: 计算规格管理界面

计算规格支持以下操作：

- 创建计算规格：创建一个新的计算规格。

- 启用：将处于停用状态的计算规格启用。**支持批量操作。**
- 停用：停止使用某个计算规格，停止后不能再用其创建云主机，但不影响之前已创建的云主机。**支持批量操作。**
- 全局共享：将计算规格进行全局共享后，所有的账户都可以使用此计算规格。**支持批量操作。**
- 全局召回：将已全局共享的计算规格进行全局召回后，其他账户将看不见此计算规格。**支持批量操作。**
- 删除：删除计算规格时，会弹出确认删除窗口。**支持批量操作。**
- 搜索：计算规格的搜索目前支持名称，UUID，以及高级搜索。

7.2.5.2 创建计算规格

在**计算规格**管理界面，点击**创建计算规格**，可以创建一个计算规格，如图 *167:* 创建计算规格界面所示：

图 167: 创建计算规格界面

创建计算规格具体步骤如下：

- **名称**：设置计算规格的名称
- **简介**：可选项，可留空不填
- **CPU**：设置云主机CPU的核数
- **内存**：设置云主机内存的大小，基本单位包括：M/G/T

- **物理机分配策略**：选择物理机分配策略。包括：运行云主机数量最少、CPU使用率最低、内存使用率最低、运行云主机最大数量，默认为运行云主机数量最少策略
  - **运行云主机数量最少**：优先选择云主机最少的物理机来创建云主机
  - **CPU使用率最低**：优先选择CPU使用率最低的物理机来创建云主机

    注:

    - 系统会采集一段时间内物理机CPU负载数据，计算出这段时间的平均CPU使用率，然后优先选择CPU使用率最低的物理机来创建云主机。
    - 数据采集周期默认10分钟，在**设置** > **全局设置** > **高级设置**中，修改**物理机CPU使用率最低采集间隔**参数，更改数据采集时间。
  - **内存使用率最低**：优先选择内存使用率最低的物理机来创建云主机

    注:

    - 系统会采集一段时间内物理机内存负载数据，计算出这段时间的平均内存使用率，然后优先选择内存使用率最低的物理机来创建云主机。
    - 数据采集周期默认10分钟，在**设置** > **全局设置** > **高级设置**中，修改**物理机内存使用率最低采集间隔**参数，更改数据采集时间。
  - **运行云主机最大数量**：用户需要先设置物理机最多运行云主机的数量，然后系统会筛选出满足此要求的物理机来创建云主机。如果没有满足条件的物理机，那么云主机创建失败
- **策略模式**：物理机分配策略选择CPU使用率最低或内存使用率最低时需要选择该项，包括非强制和强制两种策略模式

  注:

  - **分配策略(非强制)**：若查询不到物理机负载信息，则随机分配资源足够的物理机创建云主机
  - **分配策略(强制)**：若查询不到物理机负载信息，则无法创建云主机
- **磁盘带宽**：可选项，可设置云主机根云盘的IO带宽上限。为空时，代表不限制IO带宽。基本单位包括：MB/s、GB/s、TB/s
- **上行网络带宽**：可选项，可设置从云主机上上传的网络带宽的上限。为空时，代表不限制上行网络带宽。基本单位包括：Kbps、Mbps、Gbps
- **下行网络带宽**：可选项，可设置从云主机上下载的网络带宽的上限。为空时，代表不限制下载网络带宽。基本单位包括：Kbps、Mbps、Gbps

注: 用户需完全理解磁盘带宽和网络带宽配置的含义后，才能进行对应的设置，否则可能会导致无法从云主机下载文件。

7.2.5.3 计算规格详情

在**计算规格**管理界面，点击计算规格的名称，打开计算规格详情页，如图 *168: 计算规格详情页*所示。可通过**计算规格操作**按钮对当前计算规格进行操作，所包含的操作菜单是计算规格管理界面上所有操作的合集。

图 168: 计算规格详情页

计算规格详情界面分为以下3栏：

- **基本属性**：概括了此计算规格的基本信息。在此栏可以修改计算规格的名称和简介。
- **共享**：显示所有共享当前计算规格的账户
- **审计**：显示与此计算规格相关的日志。

7.2.6 云盘规格

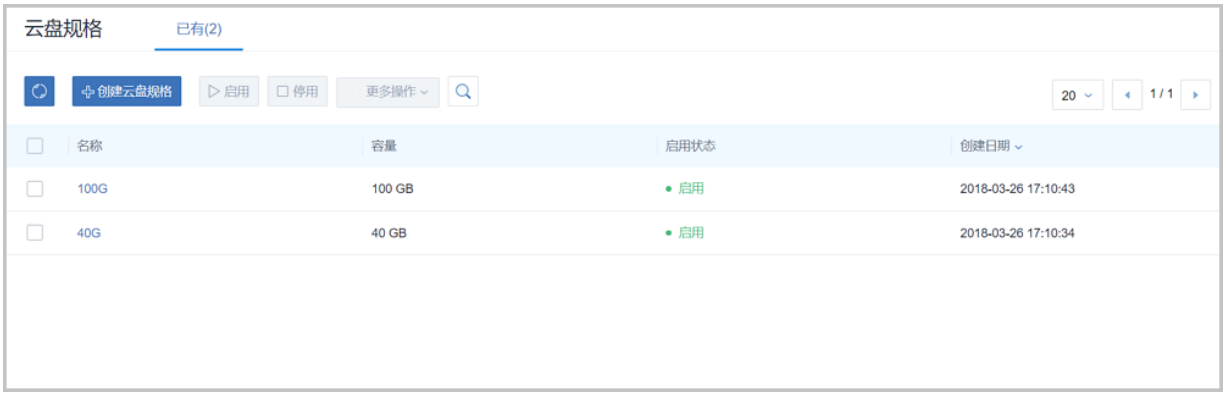
云盘规格：云主机使用的云盘的大小规格定义。

云盘规格可以用来创建根云盘和数据云盘。

7.2.6.1 云盘规格操作

在ZStack私有云主菜单，点击**云资源池** > **云盘规格**，进入**云盘规格**管理界面，如图 *169: 云盘规格管理界面*所示。在**云盘规格**管理界面，可以查看云盘规格列表的信息，如：名称，容量，启用状态等。并可对云盘规格进行创建、启用、停用、全局共享、全局召回、删除等操作。

图 169: 云盘规格管理界面



云盘规格支持操作如下：

- 创建云盘规格：创建一个新的云盘规格。
- 启用：将处于停用状态的云盘规格启用。**支持批量操作。**
- 停用：停止使用某个云盘规格，停止后不能再用其创建云盘，但不影响之前已创建的云盘。**支持批量操作。**
- 全局共享：将云盘规格进行全局共享后，所有的账户都可以使用此云盘规格。**支持批量操作。**
- 全局召回：将已全局共享的云盘规格进行全局召回后，其他账户将看不见此计算规格。**支持批量操作。**
- 删除：删除云盘规格时，会弹出确认删除窗口。**支持批量操作。**
- 搜索：云盘规格的搜索目前支持名称，UUID以及高级搜索。

7.2.6.2 创建云盘规格

在**云盘规格**管理界面，点击**创建云盘规格**，可以创建一个云盘规格，如图 *170: 创建云盘界面*所示：

图 170: 创建云盘界面

创建云盘规格具体步骤如下：

- **名称**：设置云盘规格的名称
- **简介**：可选项，可留空不填
- **容量**：设置云盘容量大小
- **磁盘带宽**：可选项，可设置云盘的IO带宽上限；为空时，代表不限制IO带宽；基本单位包括：MB/s、GB/s、TB/s

7.2.6.3 云盘规格详情

在**云盘规格**管理界面，点击云盘规格的名称，可以打开**云盘规格详情**界面，如图 *171:* 云盘规格详情界面所示。可通过**云盘规格操作**按钮对当前云盘规格进行操作，所包含的操作菜单是云盘规格管理界面上所有操作的合集。

图 171: 云盘规格详情界面

云盘规格详情界面分为以下3栏：

- **基本属性**：概括了此云盘规格的基本信息。在此栏可以修改云盘规格的名称和简介。
- **共享**：显示共享此云盘规格的账户。
- **审计**：显示与此云盘规格相关的日志。

7.3 硬件设施

硬件设施主要涉及了物理硬件环境相关的配置信息，主要包括：

- 区域：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。一般对应了数据中心的一个机房。
- 集群：一个集群是一组物理机的逻辑组合，一个集群一般对应了一个机架。
- 物理机：为云主机实例提供计算、网络、存储的物理机。
- 主存储：用于存储云主机磁盘文件（包括根云盘、数据云盘、快照、镜像缓存等）的存储服务器。支持LocalStorage、NFS、Ceph、FusionStor、Shared Mount Point类型。
- 镜像服务器：用于存储云主机的镜像模板（含ISO）。支持ImageStore、Sftp（ZStack社区版支持）、Ceph、FustionStor类型。

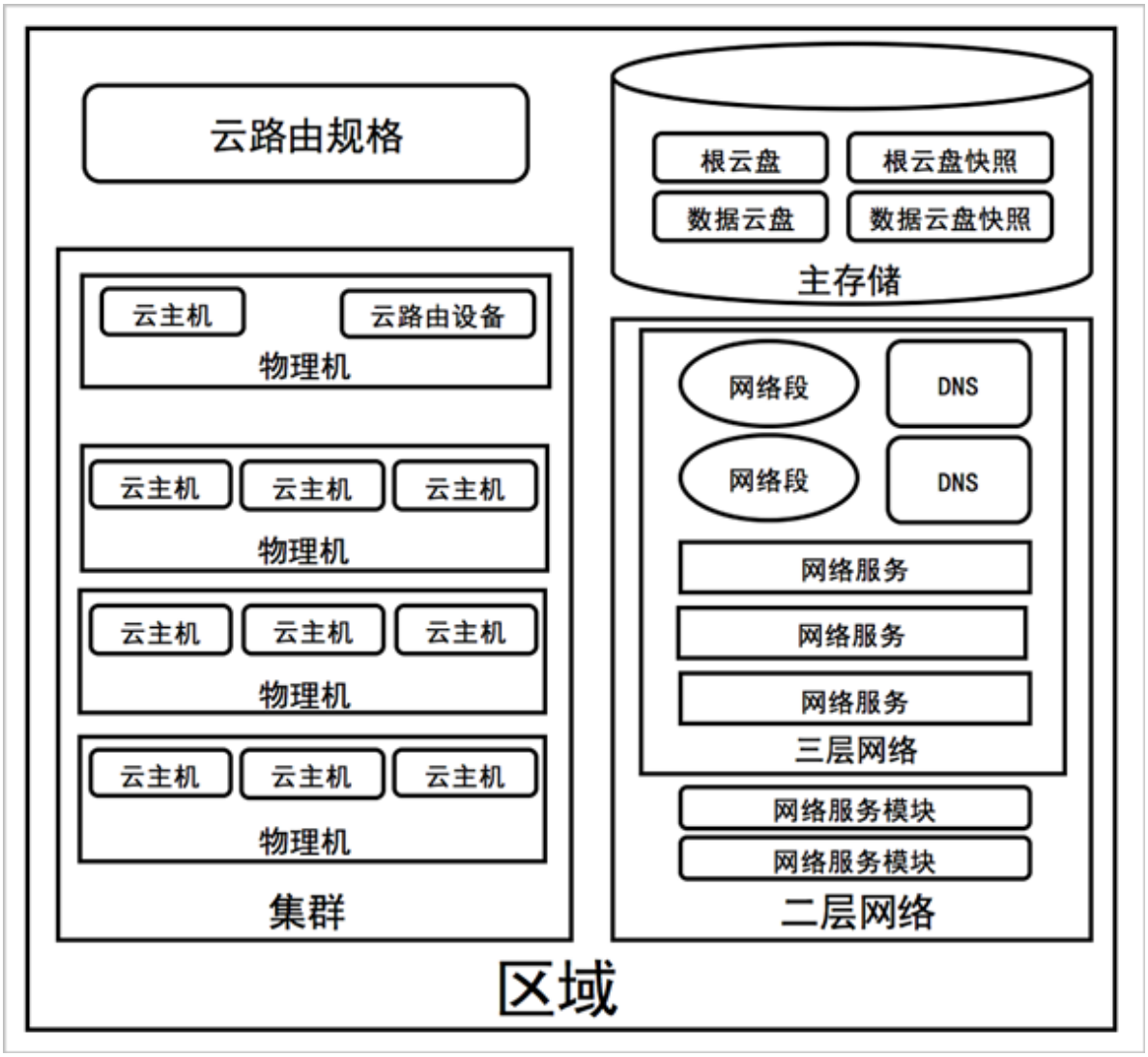
7.3.1 区域

区域：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。

- 在数据中心中，区域一般对应了一个机房。

- 区域定义了一个可见的边界，同一区域内的子资源互相可见并且可以形成某种关系，但不同区域内的子资源是不可见的，不能互相发生关系。
- 如图 *172:* 区域资源结构所示，区域中的资源以如下形式组织：

图 172: 区域资源结构



规划区域时，需注意：

1. 同一个物理二层广播域中的物理机应该在同一个区域，可属于同一个集群或分属于多个集群。
2. 同一个物理二层广播域不应该跨越多个区域，而应该映射为单个区域的二层网络。
3. 同一个主存储不应该跨越多个区域，而应该映射为单个区域的主存储。
4. 一个数据中心可以有多个区域。
5. 一个区域可以挂载一个或多个镜像服务器。
   - 一个区域中的资源， 例如主存储，只能访问挂载在同一区域中的镜像服务器。

- 一个镜像服务器可以从一个区域中卸载；卸载后，区域中的资源不能再看见该镜像服务器。
- 当数据中心的网络拓扑改变导致一个镜像服务器不能再被一个区域中的资源访问时，可以将镜像服务器从区域中卸载。
- UI界面为便于管理镜像服务器和区域的关系，特别设置了一个镜像服务器在同一时间内只能挂载到一个区域不能再挂载到其它区域。UI界面上，添加镜像服务器，默认会挂载到当前区域；删除区域的同时会直接删除挂载此区域的镜像服务器。

7.3.1.1 区域操作

在ZStack私有云主菜单，点击**硬件设施** > **区域**，进入**区域**管理界面，如图 *173:* 区域所示。在**区域**管理界面，可以查看系统中所有区域的信息，包括：区域名称、启用状态和创建日期。并可以对区域进行创建、启用、停用和删除等操作。

图 173: 区域

ZStack对区域操作定义如下：

- **搜索**：在区域管理界面上支持三种搜索方式：名称、UUID和高级搜索。
- **创建区域**：在系统中创建一个新的区域。

  点击**创建区域**按钮，弹出**创建区域**界面，输入区域的**名称**和**简介**（选填），点击**确定**按钮，如图 *174:* 创建区域所示：

  图 174: 创建区域

- **启用**：将选中的区域重新启用起来。**支持批量操作。**
- **停用**：停止使用选中的区域，同时会停用此区域上所有子资源。**支持批量操作。**但此时用户可以手动重新启用区域中的某些集群，也可以创建新的集群到当前的区域中，而不用重新启用整个区域。
- **删除**：删除选中的区域，同时也会删除区域中的所有子资源。**支持批量操作。**

注: 删除区域会删除所有子资源，并无法恢复！

7.3.1.2 区域详情

在**区域**管理界面，点击相应区域的名称，可以展开区域详情页。

它包含六栏：**基本属性**、**集群**、**主存储**、**二层网络**、**镜像服务器**和**审计**。

可通过**区域操作**按钮对当前区域进行操作，所包含的操作菜单是区域管理界面上所有区域操作的合集。点击左上角**X**按钮可以关闭区域详情页，如图 *175:* 区域详情所示：

图 175: 区域详情

- **基本属性**：

  基本属性栏为区域详情页的缺省栏，显示了当前区域的基本情况，包含：区域名称、简介、状态、概览和UUID等信息，如图 *175:* 区域详情所示。在此栏可以修改区域的名称和简介。

- **集群**：

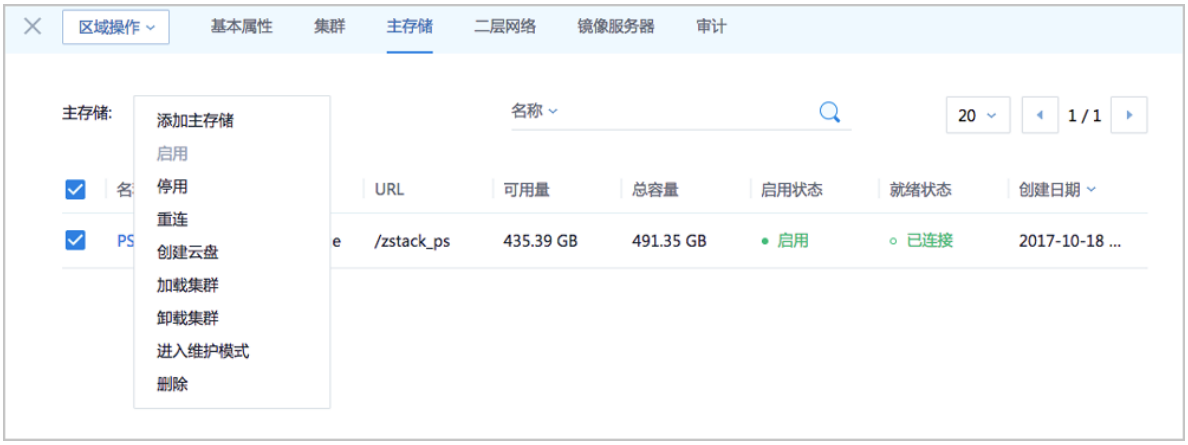
  集群栏列出了加载到当前区域中的集群列表。主要显示了集群的名称、虚拟化技术、物理机数量和状态等。在此栏可以点击集群后边的**操作**按钮来操作集群，包括：创建集群、启用集群、停用集群、加载二层网络到集群、从集群卸载二层网络、加载主存储到集群、从集群卸载主存储、删除集群。如图 *176:* 集群所示：

  图 176: 集群

- **主存储**：

主存储栏列出了当前区域中所加载的主存储列表。主要显示了主存储的名称、类型、URL、可用量、总容量、启用状态、就绪状态和创建日期等。在此栏可以点击主存储后边的**操作**按钮来操作主存储，包括：添加主存储、启用主存储、停用主存储、重连主存储、在主存储上创建云盘、为主存储加载集群、从主存储上卸载集群、将主存储进入维护模式、删除主存储。如图 *177:* 主存储所示：

图 177: 主存储



- **二层网络**：

二层网络栏列出了当前区域中所加载的二层网络列表。主要显示了二层网络的名称、网卡、VLAN号和类型等。在此栏可以点击二层网络后边的**操作**按钮来操作二层网络，包括：创建二层网络、为二层网络加载集群、从二层网络上卸载集群、删除二层网络。如图 *178:* 二层网络所示：

图 178: 二层网络

- **镜像服务器**：

镜像服务器栏列出了当前区域中所加载的镜像服务器列表。主要显示了镜像服务器的名称、类型、容量和状态等。在此栏可以点击镜像服务器后边的**操作**按钮来操作镜像服务器，包括：添加镜像服务器、启用镜像服务器、停用镜像服务器、重连镜像服务器、删除镜像服务器。如图 *179:* 镜像服务器所示：

图 179: 镜像服务器

- **审计**：

审计栏列出了当前区域的操作日志。如操作日志所示：

图 180: 操作日志

7.3.2 集群

集群：一组物理机（计算节点）的逻辑集合。

在数据中心中，一个集群一般对应了一个机架。

规划集群时，需注意：

1. 集群内所有物理机须拥有相同的操作系统；
2. 集群内所有物理机须拥有相同的网络配置；

3. 集群内所有物理机须能够访问相同的主存储；
4. 集群需挂载主存储、二层网络后，才可提供云主机服务；
5. 集群的规模，也就是每个集群中可以包含物理机的最大数量，没有限制。

集群和各个资源之间的关系定义如下：

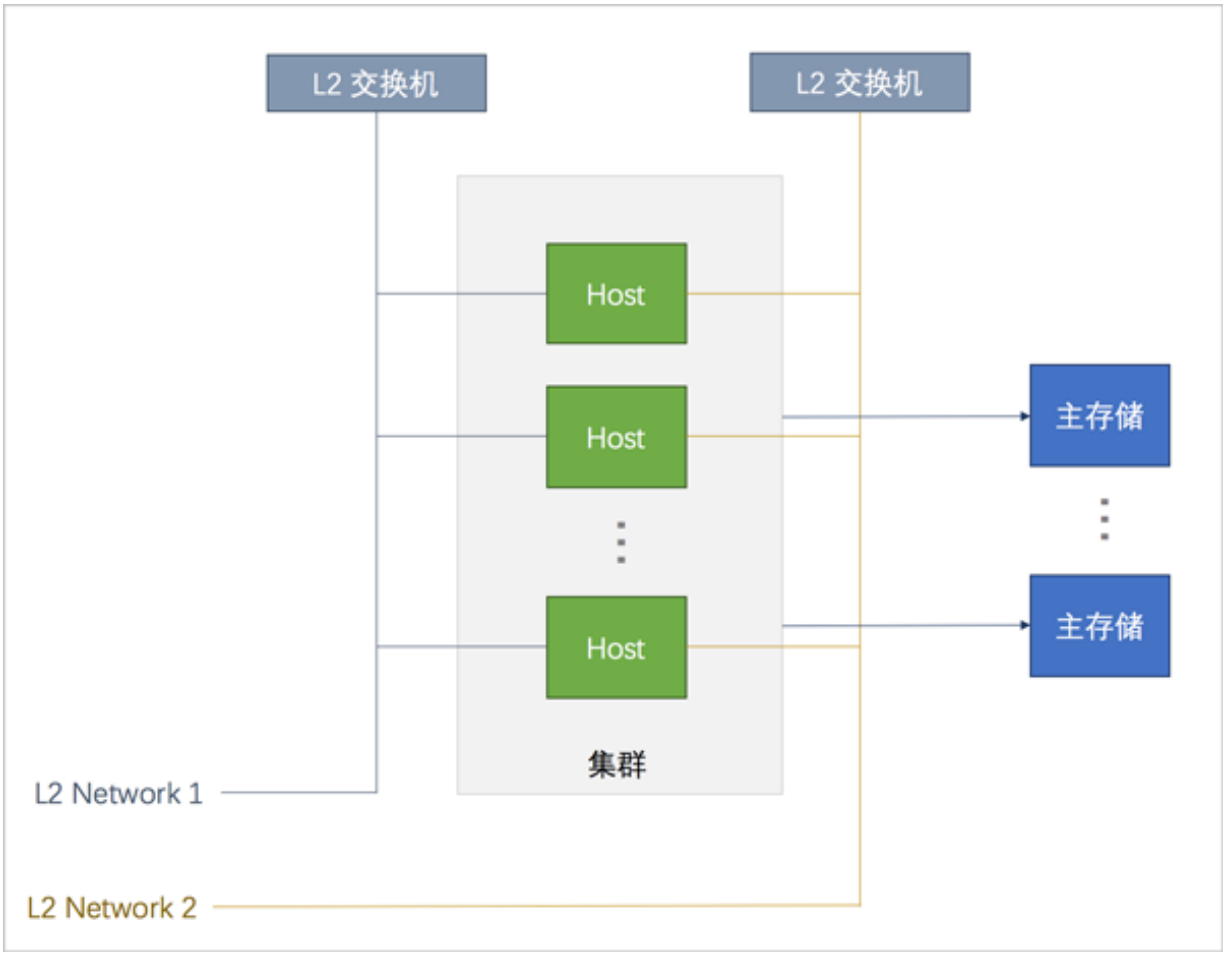
集群 | 区域

支持**多集群**操作。可在一个区域内创建多个集群，新增的物理机可以按需添加到不同的集群之中。

集群 | 主存储和二层网络

集群中可以加载或卸载主存储和二层网络，它们之间的结构关系如图 *181:* 集群、主存储、二层网络的关系所示：

图 181: 集群、主存储、二层网络的关系



注:

主存储和二层网络加载到集群时需注意：

1. 集群 | 主存储

   - 一个主存储可以加载到多个集群。
   - 一个集群可以挂载多个主存储。

     目前支持的场景有：

     - 一个集群可以挂载一个或多个本地主存储。
     - 一个集群可以挂载一个或多个NFS主存储。
     - 一个集群可以挂载一个或多个Shared Block主存储。
     - 一个集群可以挂载一个Shared Mount Point主存储。
     - 一个集群可以挂载一个本地主存储和一个NFS主存储。
     - 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
     - 一个集群可以挂载一个本地主存储和一个Shared Block主存储。
     - 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。
     - 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
     - 一个主存储可以挂载到多个集群 。

     主存储与集群的依赖关系如表 2: 主存储与集群关系所示：

     表 2: 主存储与集群关系

主存储	集群
LocalStorage	支持挂载一个或多个本地存储
NFS	支持挂载一个或多个NFS
Share Mount Point	支持挂载一个SMP
Shared Block	支持挂载一个或多个Shared Block
Ceph	为挂载到集群的Cpeh，有且仅有一个
FusionStor	为挂载到集群的FusionStor，有且仅有一个
LocalStorage + NFS	支持挂载1个LocalStorage + 1个NFS
LocalStorage + SMP	支持挂载1个LocalStorage + 1个SMP
LocalStorage + Shared Block	支持挂载1个LocalStorage + 1个Shared Block

- 集群挂载多个本地存储时，务必在添加物理机以及添加主存储之前，提前在物理机对应URL上做好分区，确保每个本地存储部署在独占的逻辑卷或物理磁盘上。
- 主存储可以被所在集群中的所有物理机访问。
- 如果数据中心的网络拓扑发生改变导致主存储不能被集群中的物理机继续访问时，主存储可以从集群卸载。

2. 集群 | 二层网络

- 一个集群可以加载一个或多个二层网络；一个二层网络可以挂载到多个集群。
- 集群可以挂载VXLAN Pool，VXLAN Pool下不同的Vni可用于创建不同的VxlanNetwork。
- 一个网卡只能创建一个NoVlanNetwork。
- 对于VlanNetwork，不同VLAN ID代表不同的二层网络。
- 如果数据中心的网络拓扑发生改变导致集群中的物理机不再在二层网络所代表的物理二层广播域中，二层网络也可以从集群卸载。

集群 | 镜像服务器

集群与镜像服务器没有直接依赖关系，一个镜像服务器可以为多个集群提供服务。

注:

- 集群中所加载的主存储和镜像服务器具有相关性。
- Ceph主存储支持与镜像仓库类型的镜像服务器一同工作。
- 主存储（PS）和镜像服务器（BS）的相关性如表 *3:* 主存储与镜像服务器的关系所示：

表 3: 主存储与镜像服务器的关系

PS\BS	ImageStore	Sftp	Ceph	FusionStor
LocalStorage	○	○	×	×
NFS	○	○	×	×
Shared Mount Point	○	○	×	×
Ceph	○	×	○	×
Shared Block	○	×	×	×
FusionStor	×	×	×	○

7.3.2.1 集群操作

在ZStack私有云主菜单，点击**硬件设施** > **集群**，进入**集群**管理界面，如图 *182: 集群*所示。在**集群**管理界面，可以查看当前区域内所有集群的列表及其信息，包括：集群名称、虚拟化技术、物理机数量、资源使用量和状态等。并可以对集群进行创建、启用、停用、加载资源、卸载资源和删除等操作。

图 182: 集群

ZStack对集群操作定义如下：

- **搜索**：在集群管理界面上支持三种搜索方式：名称、UUID和高级搜索。
- **创建集群**：在当前区域中创建一个新的集群。

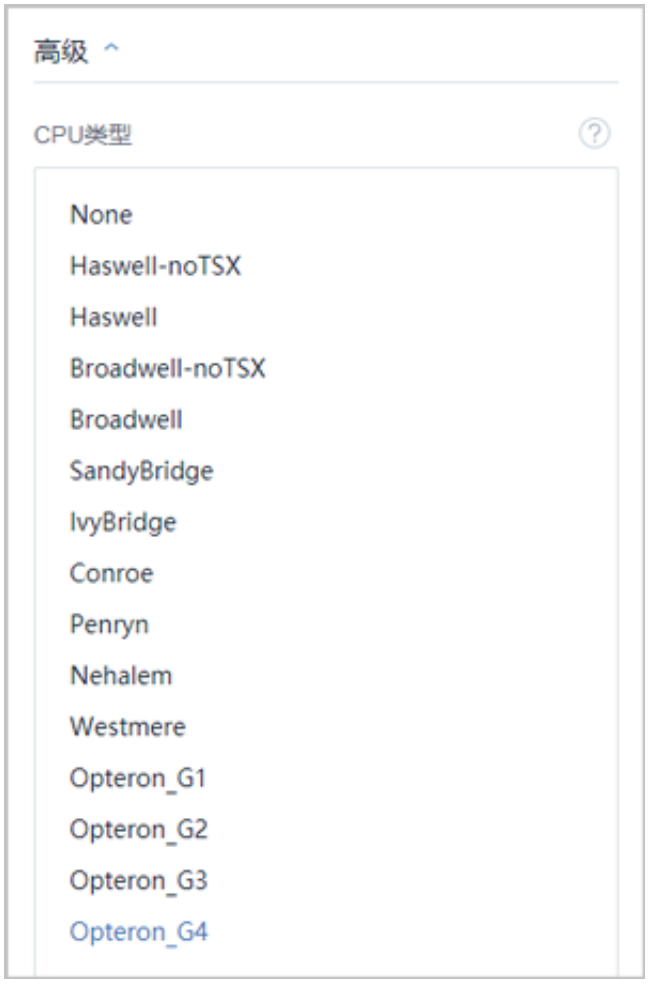
  点击**创建集群**按钮，弹出**创建集群**界面，可参考以下示例输入相应内容：

  - **名称**：设置集群名称
  - **简介**：可选项，可留空不填
  - **VDI网络**：可选项，如果已部署VDI单独使用的网络，需填写VDI网络CIDR
    - 通常VDI网络会占用较多带宽，ZStack支持VDI网络和管理网络分离。
    - 如果已部署VDI单独使用的网络，可直接将其添加到云平台中。
    - 如果不设置，VDI将默认使用管理网络。
  - **迁移网络CIDR**：可选项，如果已部署迁移云主机单独使用的网络，需填写迁移网络CIDR
    - 如果已部署迁移云主机单独使用的网络，可直接将其添加到云平台中。
    - 如果不设置，迁移云主机将默认使用管理网络。
  - **高级**
    - **CPU类型**：指定集群内CPU的类型，默认为None

      注:

- ZStack 支持KVM虚拟化定义集群的CPU模式，可选CPU类型如图 *183:* 可选*CPU*类型所示。

图 183: 可选CPU类型



- 此设置生效前提：在**设置** > **全局设置** > **高级设置**中将**物理机CPU型号检测**设置为**ture**。
- 集群指定CPU类型后，集群内只能添加所指定的CPU类型的物理机。
- 对于之前版本环境中已创建的集群，升级到2.3.2版本后，集群的CPU类型为None，不可更改。

如图 *184:* 创建集群所示：

图 184: 创建集群

- **启用**：将选中的集群重新启用起来。**支持批量操作。**
- **停用**：停止使用选中的集群，同时会停用此集群上所属物理机。**支持批量操作。**但此时用户也可以手动重新启用集群中的某些物理机，也可以添加新的物理机到集群，而不用重新启用整个集群。
- **加载/卸载二层网络**：可以将二层网络加载到集群中也可以将二层网络从集群中卸载。
- **加载/卸载主存储**：可以将主存储加载到集群中也可以将主存储从集群中卸载。
- **删除**：删除选中的集群，同时也会删除集群中的所有物理机，若主存储为本地存储（Local Storage），则同时删除物理机上的所有云主机。**支持批量操作。**

7.3.2.2 集群详情

在**集群**管理界面，点击相应集群的名称，可以展开集群详情页。包含：基本属性、物理机、主存储、二层网络、外接设备、监控数据和审计。

可通过**集群操作**按钮对当前集群进行操作，所包含的操作菜单是集群管理界面上所有集群操作的合集。点击左上角**X**按钮可以关闭集群详情页，如图 *185:* 集群详情所示：

图 185: 集群详情

- **基本属性**：

  基本属性栏为集群详情页的缺省栏，显示了当前集群的基本情况，包含：集群名称、简介、VDI网络CIDR、迁移网络CIDR、CPU类型、集群内资源使用情况、所在区域和UUID等信息，如图 *185:* 集群详情所示。在此页面可以修改集群的名称、简介、VDI网络CIDR、迁移网络CIDR、CPU类型。

- **物理机**：

物理机栏列出了加载到当前集群中的物理机列表。主要显示了物理机的名称、IP、虚拟化技术和状态等。在此栏可以点击物理机后边的**操作**按钮来操作物理机，包括：添加物理机、启用物理机、停用物理机、重连物理机、将物理机进入维护模式、删除物理机。如图 *186:* 物理机所示：

图 186: 物理机

- **主存储**：

主存储栏列出了当前集群中所加载的主存储列表。主要显示了主存储的名称、类型、URL、容量和状态等。在此栏可以点击主存储后边的**操作**按钮来操作主存储，包括：加载主存储到集群、从集群卸载主存储。

注: 从集群卸除主存储，将关闭所有使用本存储的云主机和云路由器，且此存储的所有云盘将不能正常使用。

如图 *187:* 主存储所示：

图 187: 主存储

- **二层网络**：

二层网络栏列出了当前集群中所加载的二层网络列表。主要显示了二层网络的名称、网卡、VLAN号和类型等。在此栏可以点击二层网络后边的**操作**按钮来操作二层网络，包括：加载二层网络到集群、从集群卸载二层网络。如图 *188:* 二层网络所示：

图 188: 二层网络

- **外接设备**：

外接设备栏显示了当前集群内物理机提供的外接透传设备列表，包括GUP设备、USB设备和其他设备。如图 *189:* 外接设备所示。关于外接透传功能的具体介绍请参考《外接设备透传教程》。

图 189: 外接设备

- **监控数据**：

监控数据页面显示了物理机或云主机的全部CPU使用率、全部内存使用百分比、全部网卡出入速度和全部磁盘读/写IOPS，可通过下拉菜单切换监控条目。

图 190: 监控数据

集群操作
基本属性
物理机
主存储
二层网络
外接设备
监控数据
审计
物理机
云主机
物理机全部CPU使用率:
15分钟
18.70%
14.03%
9.35%
4.68%
0%
16:55 16:56 16:57 16:58 16:59 17:00 17:01 17:02 17:03 17:04 17:05 17:06 17:07 17:09 17:10
物理机全部内存使用百分比:
15分钟
36.30%
27.23%
18.15%
9.08%
0%
16:55 16:56 16:57 16:58 16:59 17:00 17:01 17:03 17:04 17:05 17:06 17:07 17:08 17:09 17:10

物理机全部网卡出入速度:
15分钟
rx
2.3 MB/s
1.7 MB/s
1.1 MB/s
588.6 KB/s
0 B/s
20:05 20:06 20:07 20:08 20:09 20:10 20:11 20:13 20:14 20:15 20:16 20:17 20:18 20:19 20:20
物理机全部磁盘读/写IOPS:
15分钟
read
25 ops/s
19 ops/s
12.7 ops/s
6.3 ops/s
0 ops/s
20:05 20:06 20:07 20:08 20:09 20:10 20:11 20:13 20:14 20:15 20:16 20:17 20:18 20:19 20:20

- **审计**：

  审计栏列出了当前集群的操作日志。如操作日志所示：

  图 191: 操作日志

7.3.3 计算服务器

7.3.3.1 物理机

物理机：也称之为计算节点，主要为云主机实例提供计算、网络、存储等资源的物理服务器。

如图 *192:* 物理机所示：

图 192: 物理机

- 物理机是ZStack云管理平台里的核心资产，云主机运行在物理机之上。

7.3.3.1.1 物理机操作

在ZStack私有云主菜单，点击**硬件设施** > **物理机**，进入**物理机**管理界面，如图 *193:* 物理机所示。在**物理机**管理界面，可以查看当前区域中加载的所有物理机列表及其信息，包括：物理机名称、物理机IP、所在集群、启用状态、就绪状态和创建日期等。并可以对物理机进行添加、启用、停用、重连、进入维护模式和删除等操作。

图 193: 物理机

ZStack对物理机操作定义如下：

- **搜索**：在**物理机**管理界面上支持四种搜索方式：名称、UUID、IP和高级搜索。
- **添加物理机**：添加一个或多个物理机到系统中。

1. 添加单个物理机。

   点击**添加物理机**按钮，弹出**添加物理机**界面，可参考以下示例输入相应内容：

   - **名称**：设置物理机名称
   - **简介**：可选项，可留空不填
   - **集群**：选择物理机所在的集群
   - **物理机IP**：输入物理机IP地址

     注:

     在生产环境中，建议采用管理网络和公有网络分离的方案，可以最大限度保障系统安全，以及保障足够的网络带宽供管理网络使用。
   - **扫描物理机IOMMU设置**：如需使用GPU设备透传功能，可勾选此项，系统会遍历物理机可用的GPU设备。

     注:

     - 扫描后，需重启物理机以使得IOMMU配置在内核生效；
     - 需BIOS开启VT-d或IOMMU。
   - **SSH端口**：默认为22
   - **用户名**：默认为root用户，也可输入普通用户
   - **密码**：输入物理机对应的用户密码

   点击**确定**按钮后，ZStack会调用后台作业来配置物理机。配置过程可能持续几分钟。若安装出错，则会提示相应的错误信息。

   注:

   - 需使用定制版ISO安装CentOS 7.2系统；
   - BIOS需打开Intel VMX或AMD SVM的硬件虚拟化支持；
   - 需确保物理机IP地址、用户名、密码正确，用户名有sudo权限；
   - 管理节点的IP可达物理机的SSH端口以部署软件和代理程序。

   如图 *194:* 添加单个物理机所示：

   图 194: 添加单个物理机

2. 批量添加物理机。

在**添加物理机**界面，点击**添加更多物理机**下方的**+**号按钮，支持批量添加物理机。

注:

- 如果再添加区域内同一集群的其他主机，则对应主机需安装相同的CentOS系统。SSH端口、用户名、密码则无须相同。
- 如果错误填写物理机IP地址、SSH端口号、用户名、密码或用户名没有sudo权限，或防火墙策略设置了禁入规则，将会提示添加物理机失败。

如图 *195:* 批量添加物理机所示：

图 195: 批量添加物理机

确定
取消
添加物理机
名称 *
Host-2
简介
集群 *
Cluster-1
物理机IP *
172.20.14.33
扫描物理机IOMMU设置
SSH端口 *
22
用户名 *
root
密码 *
••••••••
添加更多物理机
已配置的物理机
名称: Host-1
简介:
集群: Cluster-1
物理机IP: 172.20.14.32
扫描物理机IOMMU设置: 停用
SSH端口: 22
用户名: root
密码: ********

物理机支持的操作：

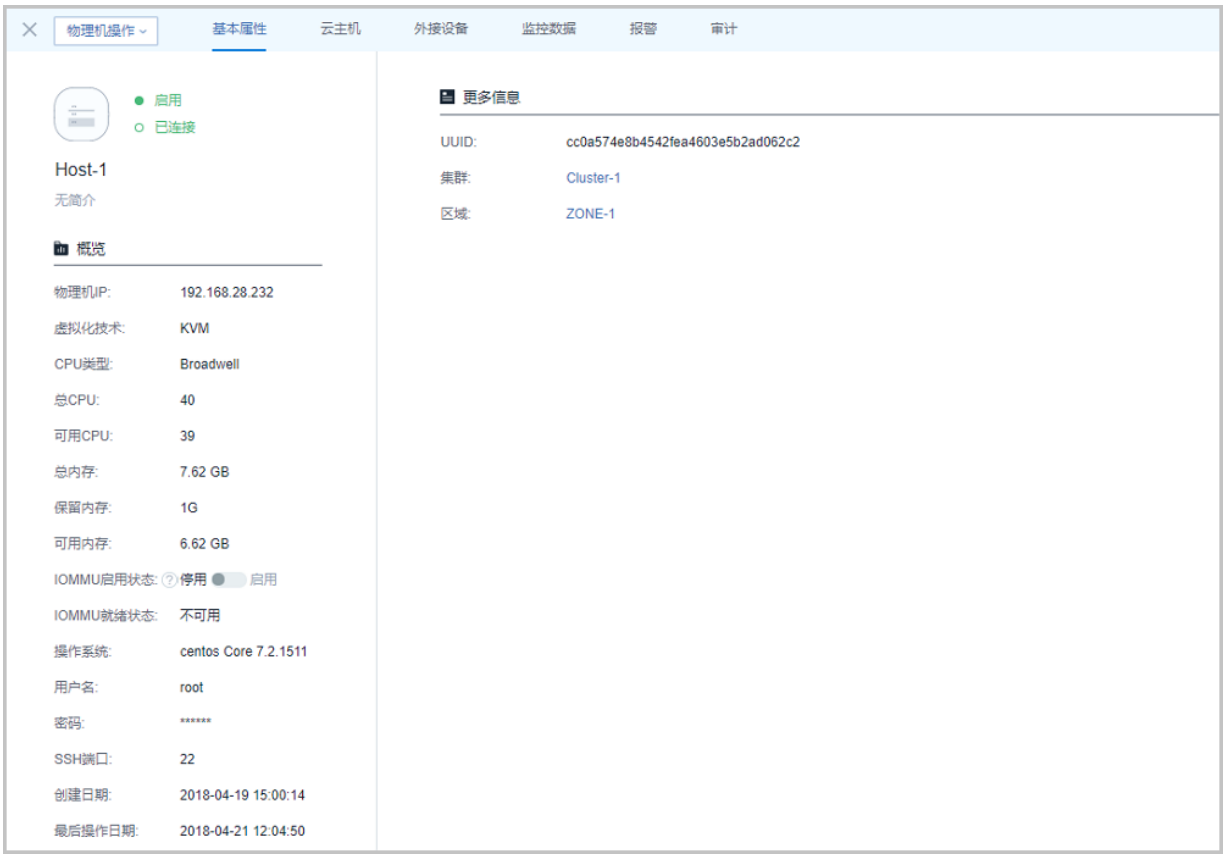
- **启用**：启用选中的物理机。**支持批量操作。**
- **停用**：停止使用选中的物理机，此物理机上所有的云主机也会被停用且停用后的物理机上将不能再创建云主机。**支持批量操作。**
- **重连**：重新连接选中的物理机，一般用于物理机的配置更新之后。例如：更新了物理机的内存或者硬盘，可以使用重连操作来更新ZStack的数据库。**支持批量操作。**
- **进入维护模式**：表示对物理机进行系统维护，可对此状态下的物理机进行物理停机，故障修复等操作。**支持批量操作。**
  - 若主存储为本地存储：物理机进入维护模式后，其上云主机会停止。
  - 若主存储为共享存储：物理机进入维护模式后，其上云主机会自动迁移。
- **删除**：只有物理机处于**维护模式**或者**失联**状态才能删除，否则无法删除。**支持批量操作。**
  - 若主存储为本地存储：
    - 删除物理机后，会自动删除该物理机上的云主机和数据云盘。
    - 即使重新添加此物理机，ZStack也将重新部署此物理机，之前的数据库资源将无法恢复。
  - 若主存储为共享存储：
    - 若云主机的**高可用级别**为**None**，删除它所在的物理机后，相应的云主机和数据云盘也会自动删除。与主存储为本地存储的情况一样。
    - 若云主机的**高可用级别**为**NeverStop**，删除它所在的物理机后，如果资源允许，相应的云主机会自动迁移至其他可用的物理机上且不会影响数据安全性；如果资源不足，相应的云主机会停止，在这种情况下，可能会出现一部分云主机因其他物理机满足资源条件已迁移，另外一部分云主机因资源不足而停止。
- **导出csv**：点击右上方的**导出csv**图标，用户可按需导出当前页面或全部页面的云主机列表。

7.3.3.1.2 物理机详情

在**物理机**管理界面，点击相应物理机的名称，可以展开物理机详情页。包含：基本属性、云主机、外接设备、监控数据、报警和审计。

可通过**物理机操作**按钮对当前物理机进行操作，所包含的操作菜单是物理机管理界面上所有物理机操作的合集。点击左上角**X**按钮可以关闭物理机详情页，如图 *196:* 物理机详情所示：

图 196: 物理机详情



- **基本属性**：

  基本属性栏为物理机详情页的缺省栏，显示了当前物理机的基本情况，包含：物理机名称、简介、物理机IP、虚拟化技术、CPU类型、物理机资源使用情况、IOMMU状态、当前操作系统版本信息、用户名、密码、SSH端口、所在集群、所在区域和UUID等信息，如图 *196: 物理机详情*所示。在此页面可以修改物理机的多项参数，具体如下：

  - **名称**和**简介**：支持对物理机的名称和简介进行修改。
  - **物理机IP**：如果物理机的IP地址发生了变化，可以点击物理机IP旁边的**编辑**按钮进行更改。IP地址更改后，ZStack会自动重连物理机。
  - **IOMMU启用状态**：IOMMU开启是使用GPU透传功能的必要条件之一。
  - **IOMMU就绪状态**：只有当 **1. IOMMU开启**；**2. BIOS中Intel VT-d或AMD IOMMU开启** 两点同时具备，IOMMU就绪状态才为**可用**，才能使用GPU透传功能。

    注: 关于GPU透传功能的具体介绍请参考*GPU透传使用教程*。

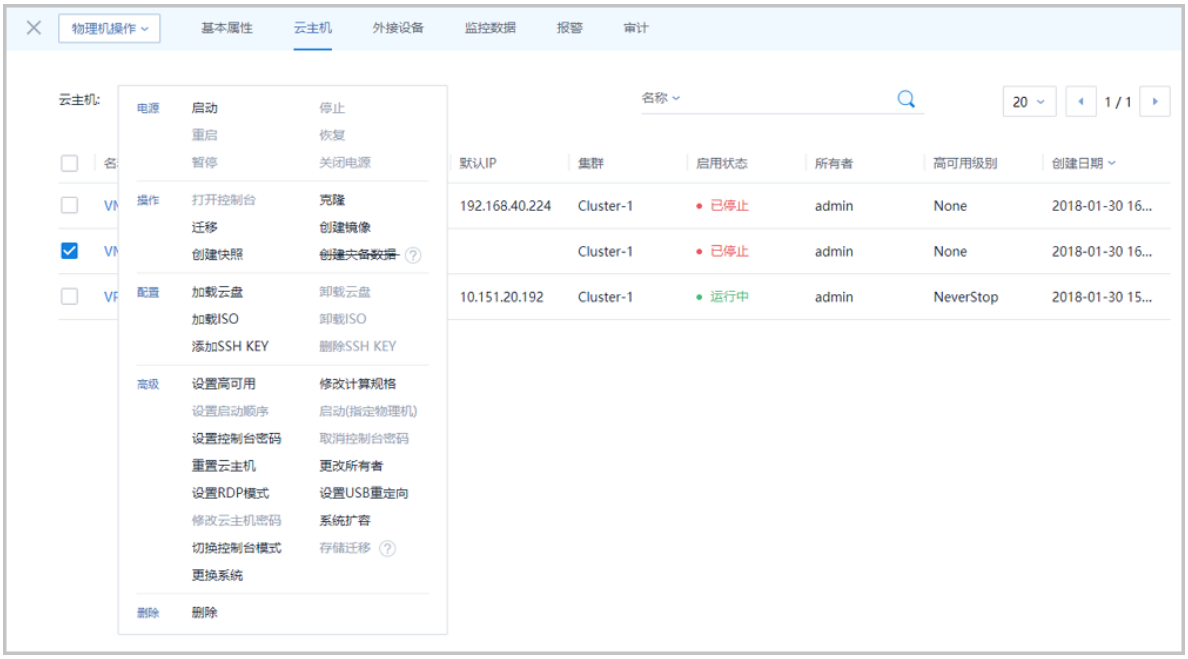
  - **用户名**：新更改的用户名需要拥有sudo权限，且更改完毕用户名后，请同时将密码修改成此用户名的密码。否则物理机可能重连失败。
  - **密码**：如果物理机的密码需要变更，可以点击密码旁边的**编辑**按钮进行更改。

- **SSH端口**：更改物理机SSH端口号。更改此端口号时，请确保新的端口号已生效，且物理机的防火墙对端口也允许访问。

- **云主机**：

  云主机栏列出了当前物理机中的所有云主机列表。主要显示了云主机的名称、CPU、内存、默认IP、集群、启用状态、所有者、高可用级别和创建日期等。在此栏可以点击云主机后边的**操作**按钮来操作云主机，如图 *197: 云主机*所示：

  图 197: 云主机



- **外接设备**：

  外接设备栏显示了当前物理机提供的GPU设备/USB设备/其他设备透传列表，如图 *198: 外接设备*所示。关于外接设备透传功能的具体介绍请参考《GPU及USB设备透传 使用教程》。

  图 198: 外接设备

- **监控数据**：

  监控数据栏显示了对物理机的实时性能监控，包括CPU、内存、磁盘、网卡，如图 *199:* 监控数据所示。监控数据自动实时更新。用户可以选择查看监控数据跨度的时间是15分钟，1小时，6小时，1天，2周，8周，甚至是1年的数据。用户还可以选择各个资源的不同监控指标。

  图 199: 监控数据

- **报警**：

  ZStack支持物理机报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加物理机CPU、内存、磁盘、网卡、其他相关的多项报警条目，以邮件/钉钉/HTTP POST方式发送报警信息。

  使用方法与云主机报警类似，具体可参考云主机报警章节。

- **审计**：

  审计栏显示了当前物理机的操作日志。如操作日志所示：

  图 200: 操作日志

7.3.3.1.3 物理机监控数据

ZStack支持对物理机的实时性能监控，包括CPU、内存、磁盘、网卡，监控数据自动实时更新。

CPU

支持选择不同的时间跨度来监控物理机CPU的实时资源使用率（单位：%）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年
- 支持监控的CPU：user、wait、system和idle。
- 监控条目：
  - All：将total和所有单个CPU的实时情况全部显示
  - total：显示物理机所有CPU的实时使用率的迭加
  - 单个CPU：0单个CPU的实时使用率，例如：0、1、2号CPU

如图 *201: CPU实时监控*所示：

图 201: CPU实时监控

内存

支持选择不同的时间跨度来监控物理机内存的实时使用情况（单位：MB）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年
- 监控条目：
  - All：同时实时显示物理机内存已使用和未使用的使用情况
  - used：实时显示物理机内存的使用量
  - free：实时显示物理机内存的未使用量

如图 *202: 内存实时监控*所示：

图 202: 内存实时监控

磁盘

支持选择不同的时间跨度来监控物理机磁盘的实时读/写速度（单位：B/S）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年
- 支持监控：
  - read+disk_octets：磁盘读速度
  - read+disk_ops：磁盘读IOPS
  - write+disk_octets：磁盘写速度
  - write+disk_ops：磁盘写IOPS
- 监控条目：
  - All：将hdc和vda分区的实时情况全部显示
  - 单个磁盘：显示单个磁盘的实时读/写速度，例如：vda磁盘

如图 *203: 磁盘实时监控*所示：

图 203: 磁盘实时监控

网卡

支持选择不同的时间跨度来监控物理机网络的实时上行/下行速度（单位：B/s）

- 可选择的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年。
- 支持监控：
  - rx+if_octets：网卡入包速度
  - rx+if_packets：网卡入包速率
  - rx+if_errors：网卡入包错误速率
  - tx+if_octets：网卡出包速度
  - tx+if_packets：网卡出包速率
  - tx+if_errors：网卡出包错误速率
- 监控条目：
  - All：将所有单个物理机网卡的使用情况全部显示
  - 单个网卡：显示单个物理机网卡的实时上行/下行速度，例如：网卡eth0

如图 *204: 网卡实时监控*所示：

图 204: 网卡实时监控

7.3.3.1.4 GPU及USB设备透传 使用教程

7.3.3.1.4.1 GPU透传

7.3.3.1.4.1.1 介绍

ZStack支持GPU透传功能，物理机GPU设备可直接透传到云主机，让云主机享有物理机强劲的GPU并行计算能力，不仅适用于3D渲染、高清转解码场景，还适用于诸多高性能计算（HPC）场景，如机器学习、医疗成像、石油勘探数据分析、比特币挖掘等具有大量密集运算特点的场景。

7.3.3.1.4.1.2 前提

- 本教程假定用户已安装最新版本ZStack，并部署完成创建云主机必要的资源。

  具体方式请参考用户手册安装部署章节。
- 本教程将从添加物理机的步骤开始，详细介绍GPU透传功能的使用方法。

7.3.3.1.4.1.3 添加物理机

操作步骤

1. 登录ZStack

   使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*http://your_machine_ip:5000/*），默认用户名和密码为：*admin/password*。

   如图 *205: ZStack登录界面*所示：

   图 205: ZStack登录界面

2. 进入**物理机**主界面

在ZStack私有云主菜单，点击**硬件设施** > **计算服务器** > **物理机**，进入**物理机**主界面。如图 *206: 物理机主界面*所示：

图 206: 物理机主界面

3. 添加物理机

点击**添加物理机**，弹出**添加物理机**界面，可参考以下示例输入相应内容：

- **名称**：设置物理机名称，例如Host-1
- **简介**：可选项，可留空不填
- **集群**：选择物理机所在集群，例如Cluster-1
- **物理机IP**：输入物理机IP地址，并勾选**扫描物理机IOMMU设置**。

注:

如果用户在创建物理机过程中未勾选**扫描物理机IOMMU设置**，则需在创建物理机后手动开启内核**IOMMU**，同时确保BIOS中**Intel VT-d或AMD IOMMU**开启，才能使用GPU透传功能，详情见下节。

- **SSH端口**：默认为22
- **用户名**：默认为root用户
- **密码**：输入物理机对应的用户**密码**，输入密码时请注意大小写

如图 *207:* 添加物理机所示：

图 207: 添加物理机

4. 点击**确定**，成功添加物理机Host-1

后续操作

添加物理机后，接下来需确认GPU设备启用。

7.3.3.1.4.1.4 确认GPU设备启用

操作步骤

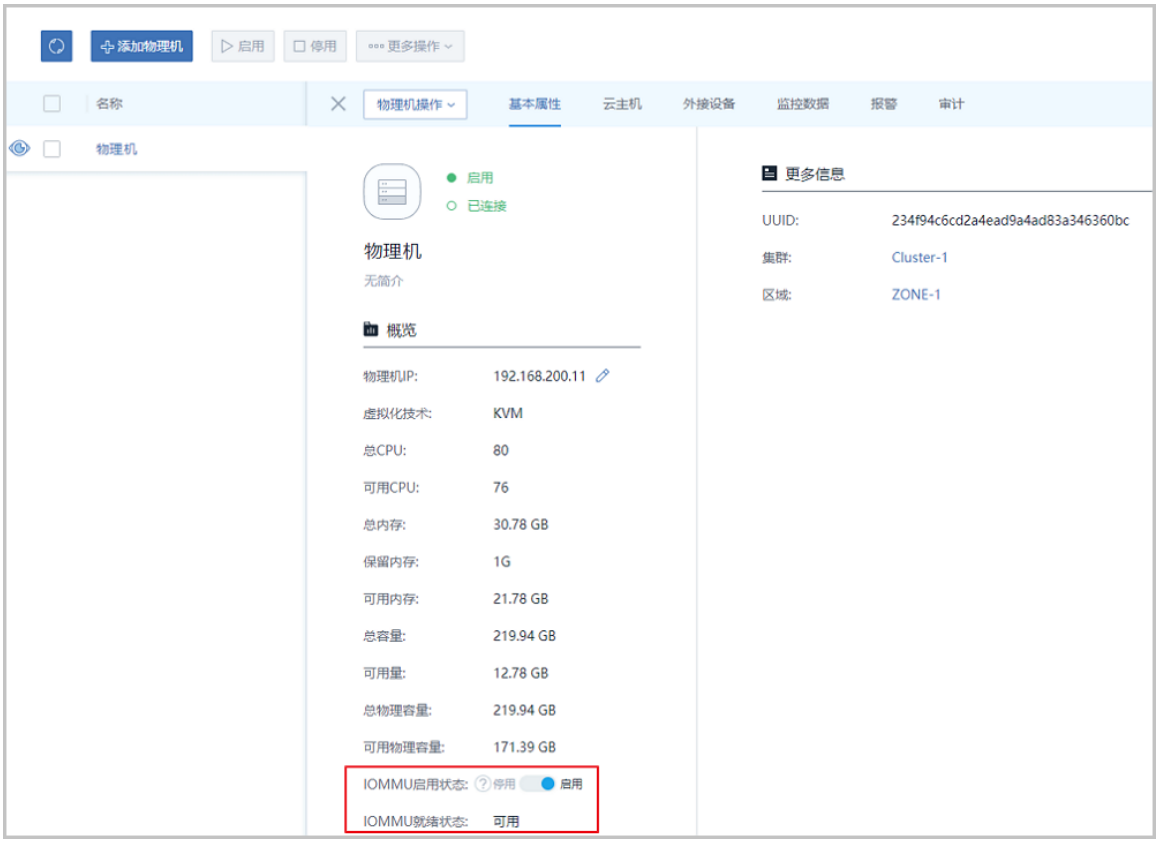
1. 确认IOMMU的启用状态和就绪状态

   在**物理机**界面，点击物理机名称进入**物理机详情**页面，在**基本属性**子页面，请确认：

   - IOMMU启用状态：**启用**
   - IOMMU就绪状态：**可用**

   如图 *208: 确认IOMMU启用和就绪状态*所示：

   图 208: 确认IOMMU启用和就绪状态



1. 要使用GPU透传功能，必须确保两点：

   - IOMMU开启（包括内核IOMMU开启，数据库中IOMMU状态为启用）
   - BIOS中Intel VT-d或AMD IOMMU选项开启

2. IOMMU启用状态：

   - **启用**：开关划至启用，表示IOMMU开启
   - **停用**：开关划至停用，表示IOMMU关闭

注:

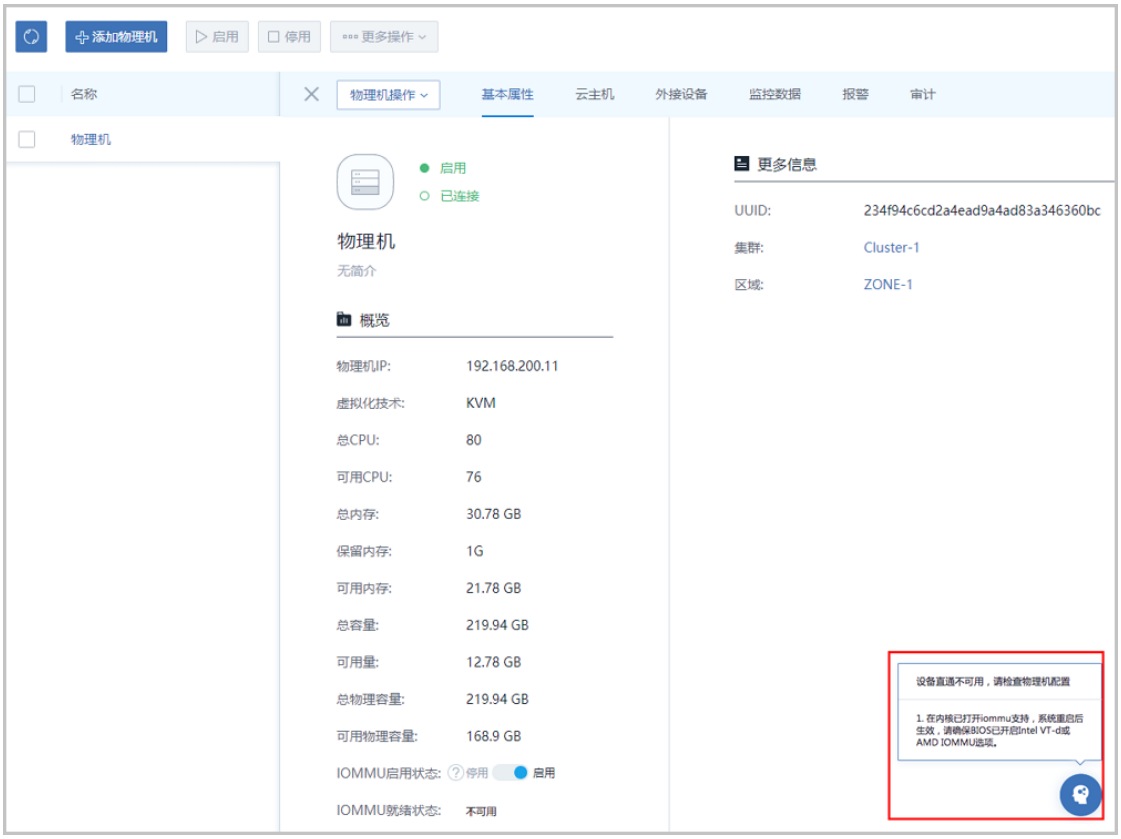
目前ZStack的**IOMMU启用状态**开关特性：

- 首次将**IOMMU启用状态**开关划至**启用**，内核IOMMU开启，需重启服务器生效，同时数据库中IOMMU状态为启用。
- 将**IOMMU启用状态**开关划至**停用**，内核IOMMU开启记录依然存在，但数据库中IOMMU状态变为停用，此时，GPU透传功能关闭。
- 目前ZStack的**IOMMU启用状态**开关，其**停用**仅支持修改IOMMU在管理节点的状态标签，不支持内核IOMMU参数的删除操作。

3. 如果用户将**IOMMU启用状态**开关划至**启用**，但发现**IOMMU就绪状态**为**不可用**：

- 此时页面右下角会弹出操作助手，如图 *209: 弹出操作助手*所示
- 此时内核IOMMU已开启，需重启服务器生效，同时，用户需进入BIOS开启Intel VT-d或AMD IOMMU选项

图 209: 弹出操作助手



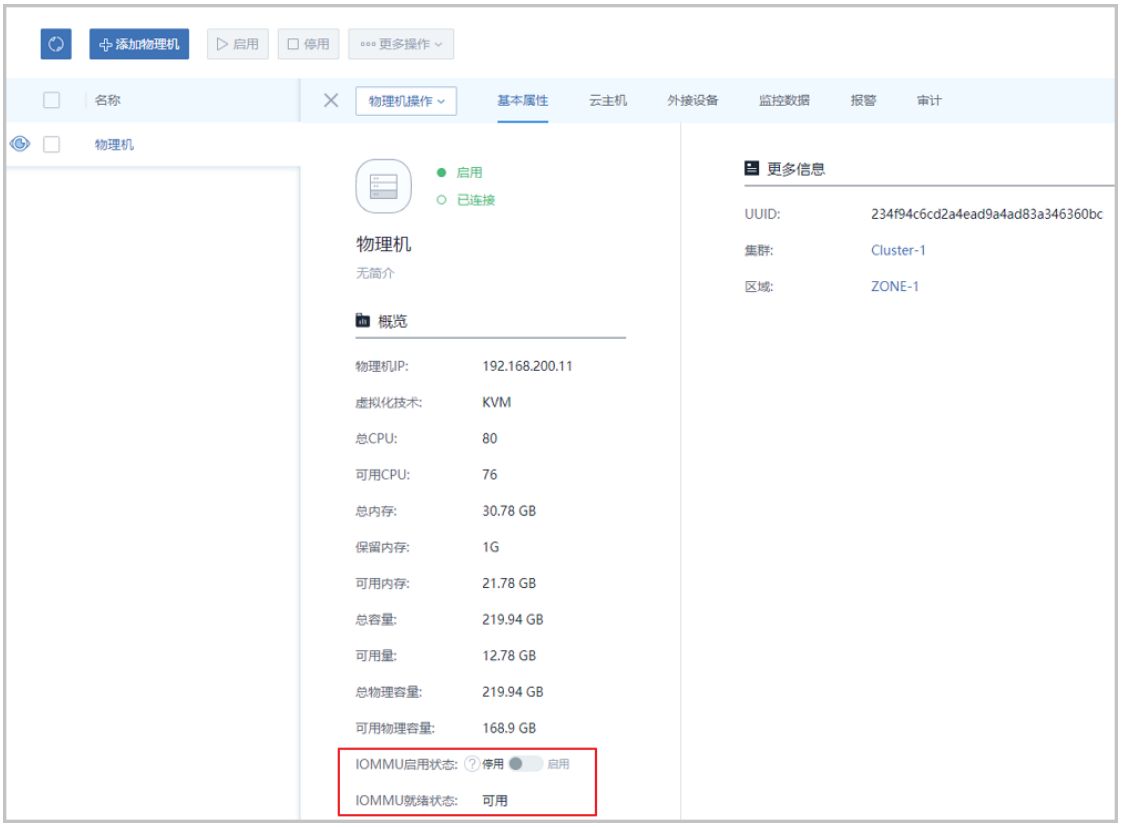
4. IOMMU就绪状态：

- 只有当 " **1. IOMMU开启**；**2. BIOS中Intel VT-d或AMD IOMMU选项开启** " 两点同时具备，IOMMU就绪状态才为**可用**，才能使用GPU透传功能。

5. 当IOMMU就绪状态已经为**可用**，用户希望暂时关闭该物理机的GPU透传功能，可将IOMMU启用状态的开关划至**停用**。

   如图 *210: IOMMU停用*所示：

   图 210: IOMMU停用



   此时：

   - 该物理机GPU设备已不能再加载到云主机。
   - 对于已加载该物理机GPU设备的云主机，透传不受影响，但GPU设备一旦卸载就无法再次加载。
   - 用户希望再次启用该物理机的GPU透传功能，只需将IOMMU启用状态的开关划至**启用**即可。

2. 查看物理机的GPU设备详情

点击物理机名称，在**物理机详情**页面，点击**外接设备** > **GPU设备**，进入**GPU设备**页面，展示了该物理机GPU设备的设备名、设备地址、类型、启用状态、就绪状态、加载到云主机的情况等，如图 *211: GPU设备详情*所示：

图 211: GPU设备详情

注:

- GPU设备需同时具备 " **1. 启用状态为启用**；**2. 就绪状态为就绪**" 两点，才能加载到云主机。
- GPU设备未加载到任何云主机，云主机状态为**未加载**；GPU设备加载到某个云主机，云主机状态将显示该云主机名，同时GPU设备**就绪状态**为**已加载**，如图 *212: GPU设备加载到某个云主机*所示。关于云主机加载GPU设备，详情见下节。
- 一旦GPU设备加载到某个云主机，该GPU设备就为该云主机独享。
- 云主机只能加载所在物理机的GPU设备，不支持跨物理机GPU设备的加载。

图 212: GPU设备加载到某个云主机

3. GPU设备支持的操作

- 启用：

  启用某个GPU设备，该设备的**启用状态**变为**启用**，如果此时**就绪状态**为**就绪**，表示云主机可加载该设备。

- 停用：

  停用某个GPU设备，该设备的**启用状态**变为**停用**，表示该设备暂时不可被加载到云主机。

- 全局共享：

  将已加载的GPU设备全局共享给普通账户。

- 全局召回：

  将共享给普通账户GPU设备全局召回。

- 删除：

  - 如果物理机异常掉电/断网，修复后重启物理机，重连过程中自动扫描GPU设备，由于GPU设备的BDF号很可能已更改，GPU设备状态在数据库中被刷新为**不可用**，此时用户可删除**就绪状态**为**不可用**的GPU设备。
  - 如果GPU设备从当前插槽拔出，重启物理机，重连过程中自动扫描GPU设备未找到，GPU设备状态在数据库中被刷新为**不可用**，此时用户可删除**就绪状态**为**不可用**的GPU设备。

如图 *213: GPU*设备支持的操作所示：

图 213: GPU设备支持的操作

4. 物理机所在集群的**集群详情**页，点击**外接设备** > **GPU设备**，进入**GPU设备**页面，可查看GPU设备详情，如图 *214: 集群详情页支持查看GPU设备详情*所示：

图 214: 集群详情页支持查看GPU设备详情

后续操作

确认GPU设备启用后，接下来需将GPU设备加载到云主机。

7.3.3.1.4.1.5 云主机加载GPU设备

操作步骤

1. 创建云主机。

a) 进入**云主机**界面

在ZStack私有云主菜单，点击**云资源池** > **云主机**，进入**云主机**界面，如图 *215: 云主机界面*所示：

图 215: 云主机界面

b) 点击**创建云主机**按钮，弹出**创建云主机**界面，如图 *216: 创建云主机*所示，可参考以下示例输入相应内容：

- **名称**：设置云主机名称
- **简介**：可选项，可留空不填
- **计算规格**：选择云主机的计算规格
- **镜像**：选择云主机的镜像
- **网络**：选择L3-私有网络
- **高级-GPU设备**：可选项，创建云主机时支持在高级操作中选择GPU设备；也可先创建云主机，然后在配置信息中加载GPU设备

注:

- 需提前在物理机BIOS中开启Intel VT-d或AMD IOMMU，且在物理机内核开启IOMMU支持，确保物理机可正常使用GPU设备透传功能。
- 支持加载多个不同类型的GPU设备到云主机
- 不能跨物理机加载GPU设备到云主机

图 216: 创建云主机

确定
取消
创建云主机
添加方式
单个
多个
名称 *
VM
简介
计算规格 *
1CPU-1G
镜像 *
Linux
网络 *
L3Network-1
默认网络
设置 IP

2. 云主机加载GPU设备

如果创建云主机时已添加GPU设备，可通过该方法继续加载或更换GPU设备。

a) 进入**云主机详情**的**配置信息**子页面。

在**云主机**界面点击云主机名称，显示**云主机详情**页面，点击**配置信息**进入**配置信息**子页面。在GPU设备处，点击**操作**，在下拉菜单中选择**加载**，如图 *217:* 配置信息所示：

图 217: 配置信息

b) 弹出**选择GPU设备**界面如所示，选择要加载到云主机VM上的GPU设备，如图 *218:* 选择要加载到云主机*VM*上的*GPU*设备所示：

图 218: 选择要加载到云主机VM上的GPU设备

c) 云主机成功加载GPU设备，如图 *219:* 云主机成功加载*GPU*设备所示：

图 219: 云主机成功加载GPU设备

3. 安装显卡驱动

加载GPU设备后，需要安装对应的驱动程序。请在AMD官网或NVIDIA官网获取官方驱动程序。

- Linux支持AMD的计算卡、游戏卡、专业卡。Linux自带社区驱动，如需支持计算加速和显示加速功能。请点击这里安装官方驱动。
- Linux支持NVIDIA的计算卡、游戏卡、专业卡。Linux自带社区驱动，如需支持计算加速和显示加速功能。请点击这里安装官方驱动。
- Windows支持AMD的计算卡、游戏卡、专业卡和NVIDIA的计算卡。请点击这里根据显卡类型和Windows操作系统版本下载合适的显卡驱动。
- Windows仅支持NVIDIA的计算卡。请点击这里根据显卡类型和Windows操作系统版本下载合适的显卡驱动。

后续操作

至此，GPU透传功能已成功开启。

7.3.3.1.4.1.6 典型应用场景

GPU透传功能通过云主机透传物理机强劲的GPU计算能力，可适用于3D渲染、人工智能、云游戏、VDI等典型应用场景。

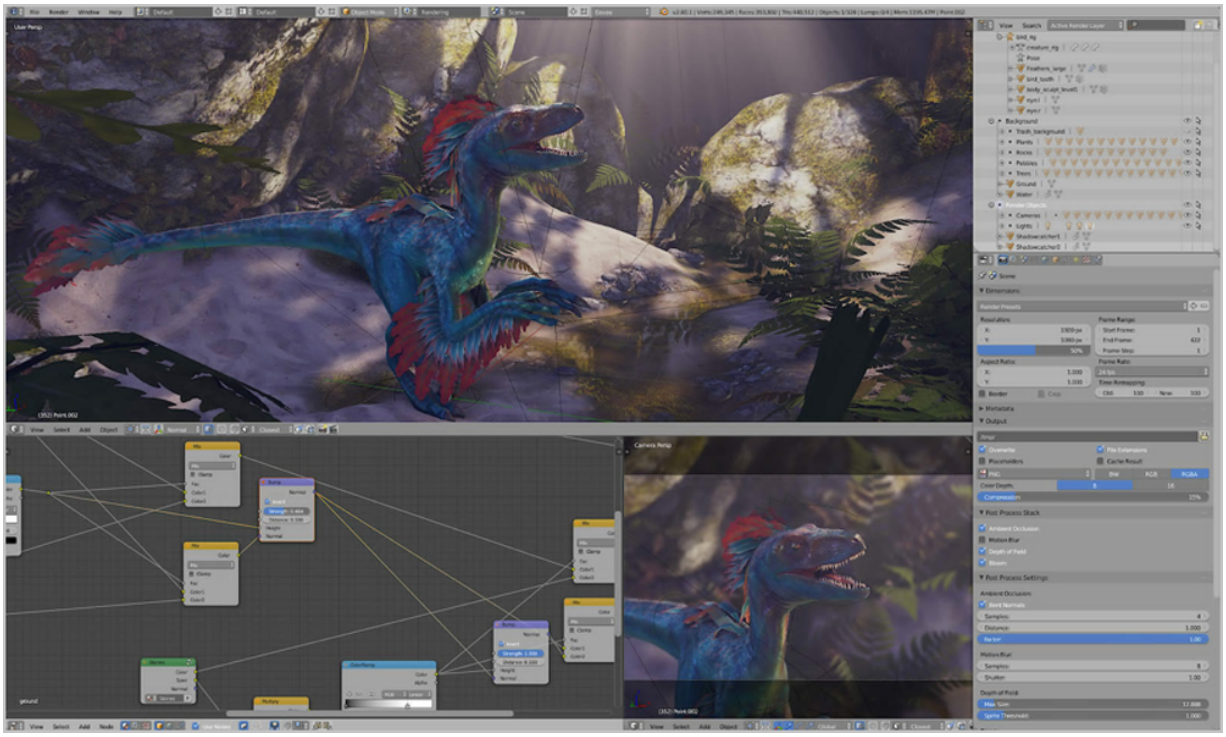
7.3.3.1.4.1.6.1 3D渲染

三维计算机图形的预渲染（Pre-rendering、Offline rendering）或实时渲染（Real-time rendering、Online rendering）速度都很缓慢。预渲染常用于电影制作，要求很高的计算强度，需要大量的服务器提供运算能力；实时渲染常用于三维视频游戏，通常依靠图形处理器（GPU）完成这个过程。

现在由于GPU的高速发展，已经有相当多的3D渲染是在GPU服务器集群中完成。结合ZStack的GPU透传功能，在性能损失极低的情况下（5%以内）同时可获得集中高效的集群管理功能，再配合智能监控软件以及ZStack自带的计费功能，可以形成一整套更便捷高效的渲染农场方案。

如图 *220: 3D渲染*所示：

图 220: 3D渲染



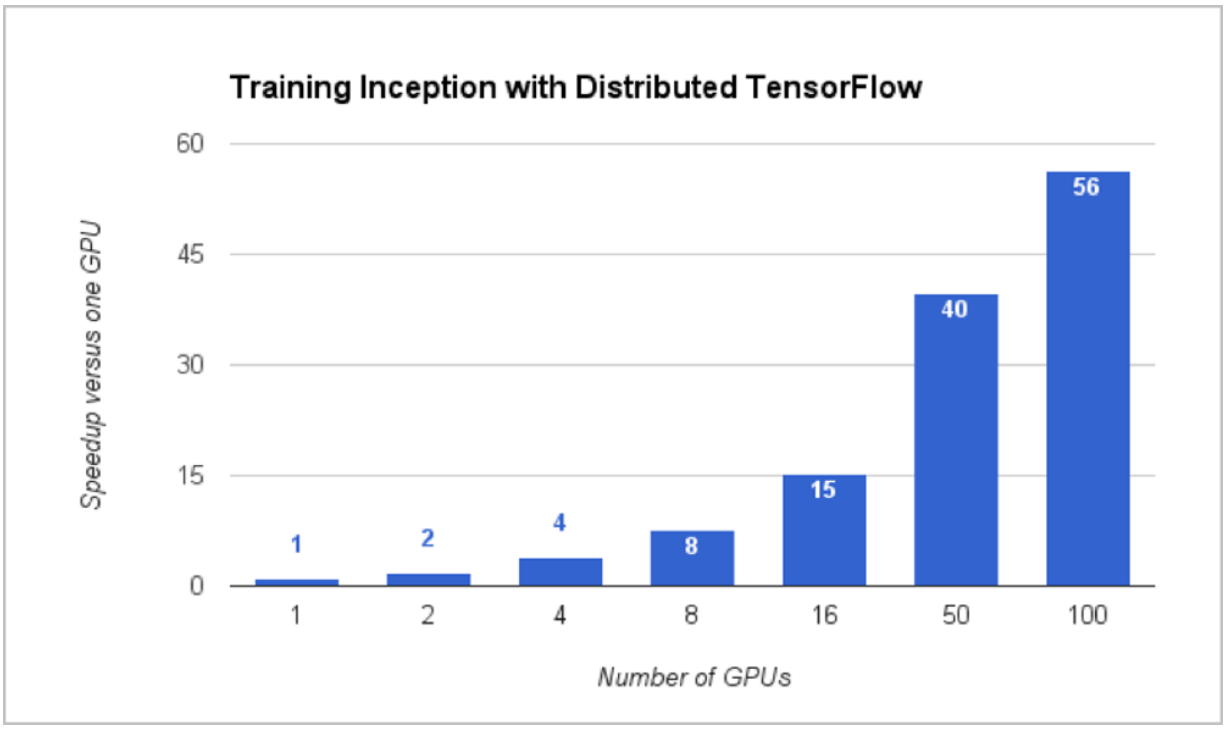
7.3.3.1.4.1.6.2 人工智能

GPU的计算能力可以应用于深度学习。自Google推出神经网络工具TensorFlow后，许多科研机构以及企业应用都日渐明显偏向使用GPU作为基础设施。

以规格较高的NVIDIA P100显卡为例，通过ZStack的GPU透传功能，将其透传至云主机后，性能测试结果显示，几乎与标称完全一致，能够充分满足大规模模型训练对基础设施的要求。

如图 *221: 人工智能*所示：

图 221: 人工智能



7.3.3.1.4.1.6.3 云游戏

随着宽带网络的发展，以及移动终端设备的普及，将游戏计算至于云端，客户端仅仅负责显示与控制的游戏模式也悄然开始流行。云端服务器上渲染3D游戏，即时为每一帧进行编码，将结果以流的形式传输至任何接驳有线或无线网络的设备。

这种云游戏模式，可以借助GPU以及服务器CPU能力，通过ZStack的GPU透传功能，为游戏创造隔离性更佳的虚拟环境，从而保证计算与渲染的流畅度，为用户提供更好的游戏体验。

如图 222: 云游戏所示：

图 222: 云游戏

7.3.3.1.4.1.6.4 VDI

GPU一直是VDI（桌面云）中非常重要的设备，它不仅能够改善桌面视觉体验，同时在特殊的应用程序中承担主力计算角色，从而完全代替传统PC图站，让用户在更为安全的环境中进行3D设计。

通过ZStack的GPU透传功能，以及配合RDP、PCoIP等协议，可充分利用显卡能力，比如3D设计、游戏等流畅运行，提供更逼近本地物理机的用户体验。

如图 *223: VDI*所示：

图 223: VDI

7.3.3.1.4.2 USB透传

7.3.3.1.4.2.1 介绍

ZStack支持USB透传功能，物理机USB设备可直接透传至该物理机上所运行的云主机，从而让云主机能够直接使用物理机上的USB设备。

7.3.3.1.4.2.2 前提

- 在此教程中，假定用户已安装最新版本ZStack，并部署完成创建云主机必要的资源。

  具体方式请参考用户手册安装部署章节。

- 本教程将从添加物理机的步骤开始，详细介绍USB透传功能的使用方法。

> **注:** USB透传功能需要ZStack管理员权限才可以操作。

7.3.3.1.4.2.3 添加物理机

操作步骤

1. 登录ZStack

   使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（http://your_machine_ip:5000/），默认用户名和密码为：admin/password，如登录界面所示：

   图 224: 登录界面

2. 进入**物理机**主界面

在ZStack私有云主菜单，点击**硬件设施** > **计算服务器** > **物理机**，进入**物理机**主界面。如图 *225: 物理机主界面*所示：

图 225: 物理机主界面

3. 添加物理机

点击**添加物理机**，弹出**添加物理机**界面，可参考以下示例输入相应内容：

- **名称**：设置物理机名称，例如Host-1
- **简介**：可选项，可留空不填
- **集群**：选择物理机所在集群
- **物理机IP**：输入物理机IP地址

注:

该USB透传功能无需IOMMU支持，无需勾选**扫描物理机IOMMU设置。**

- **SSH端口**：默认为22
- **用户名**：默认为root用户
- **密码**：输入物理机对应的用户**密码**，输入密码时请注意大小写

如图 *226:* 添加物理机所示：

图 226: 添加物理机

4. 点击**确定**，成功添加物理机

后续操作

添加物理机后，接下来可查看物理机上的USB设备详情。

7.3.3.1.4.2.4 查看USB设备详情

操作步骤

1. 查看物理机的USB设备详情

点击物理机名称，进入**物理机详情**页面，点击**外接设备** > **USB设备**，进入**USB设备**页面，展示了该物理机中可用的USB设备列表，包括：设备名、生产商、类型、启用状态、USB版本、加载到云主机的情况等，如图 *227: USB*设备详情所示：

图 227: USB设备详情

注:

- USB设备没有统一的命名规范，管理员需要通过生产商、类型、USB版本等信息建立起与实际USB设备之间的关联。支持修改设备名，进一步提高USB设备的辨识度。
- 当一个USB3.0设备插入一个USB2.0口时，对外表现为USB2.0设备，即**USB版本**显示**2.00**。
- USB设备未加载到任何云主机，云主机状态为**未加载**；USB设备加载到某个云主机，云主机状态将显示该云主机名，如图 *228: USB*设备加载到某个云主机所示。关于云主机加载USB设备，详情见下节。
- 一旦USB设备加载到某个云主机，该USB设备就为该云主机独享。
- 云主机处于**运行中**状态时：只能选择当前所在物理机的可用USB设备，不支持跨物理机USB设备的加载。
- 云主机处于**已停止**状态时：
  - 如果此前未挂载USB设备，可从所在集群的全部可用USB设备中选择；如果该云主机加载多个USB设备，需确保所有USB设备处于同一物理机上；
  - 如果此前已加载USB设备，只能从该USB设备所在物理机选择其它可用USB设备；

- 总原则：一台云主机加载的所有USB设备只能处于同一台物理机上。

注:

云主机加载USB设备，可能会影响其调度结果：该云主机只能在USB设备所在物理机上运行，如果物理机没有足够的资源，可能导致云主机无法开机！

图 228: USB设备加载到某个云主机

2. USB设备支持的操作

- **修改设备名**：修改设备名，进一步提高USB设备的辨识度。
- **启用**：启用某个USB设备，该设备的**启用状态**变为**启用**，表示云主机可加载该设备。
- **停用**：停用某个USB设备，该设备的**启用状态**变为**停用**，表示该设备暂时不可被加载到云主机。停用操作可用于过滤掉某些永远不会被加载的USB设备。
- **加载**：将某个USB设备加载到云主机。
- **卸载**：将某个USB设备从云主机上卸载。

如图 *229: USB*设备支持的操作所示：

图 229: USB设备支持的操作

3. 点击**硬件设施** > **集群**，在**集群**页面点击集群名称，进入物理机所在集群的**集群详情**页，点击**外接设备** > **USB设备**，进入**USB设备**页面，可查看USB设备详情，如图 *230:* 集群详情页支持查看*USB*设备详情所示：

图 230: 集群详情页支持查看USB设备详情

7.3.3.1.4.2.5 云主机加载USB设备

操作步骤

1. 创建云主机

   a) 进入**云主机**界面。

   在ZStack私有云主菜单，点击**云资源池** > **云主机**，进入**云主机**界面，如图 *231:* 云主机界面所示：

图 231: 云主机界面

b) 点击**创建云主机**按钮，弹出**创建云主机**界面，如图 *232: 创建云主机*所示，可参考以下示例输入相应内容：

- **名称**：设置云主机名称
- **简介**：可选项，可留空不填
- **计算规格**：选择云主机的计算规格
- **镜像**：选择云主机的镜像
- **网络**：选择云主机的网络

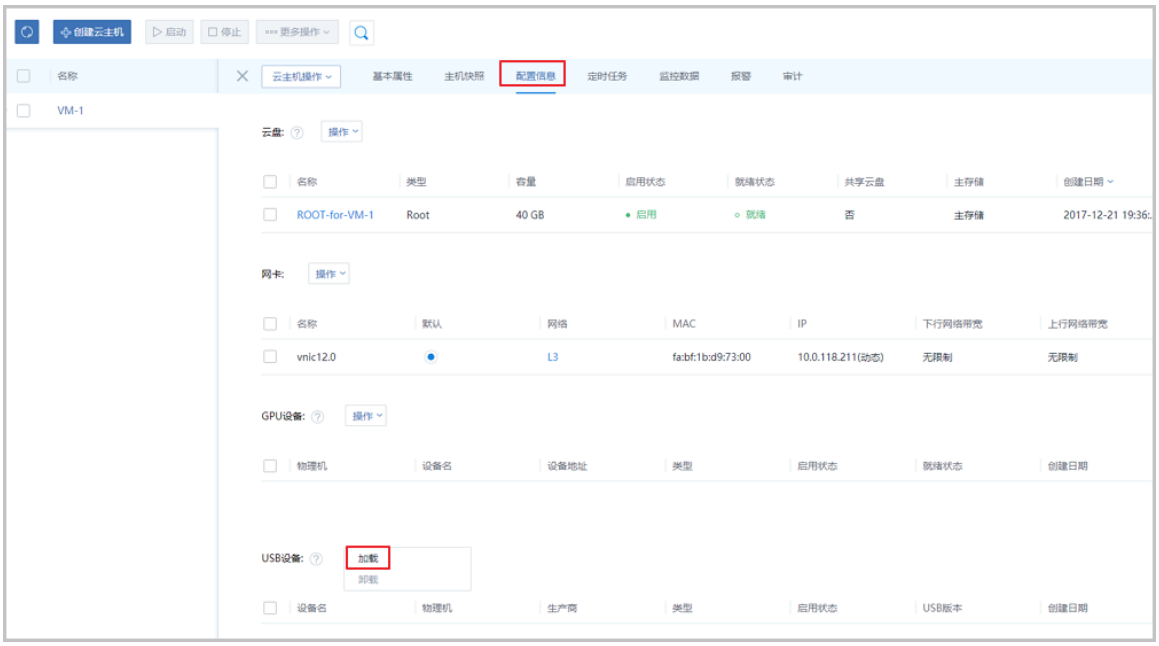
图 232: 创建云主机

2. 云主机加载USB设备

a) 点击云主机名称，进入**云主机详情**的**配置信息**子页面。

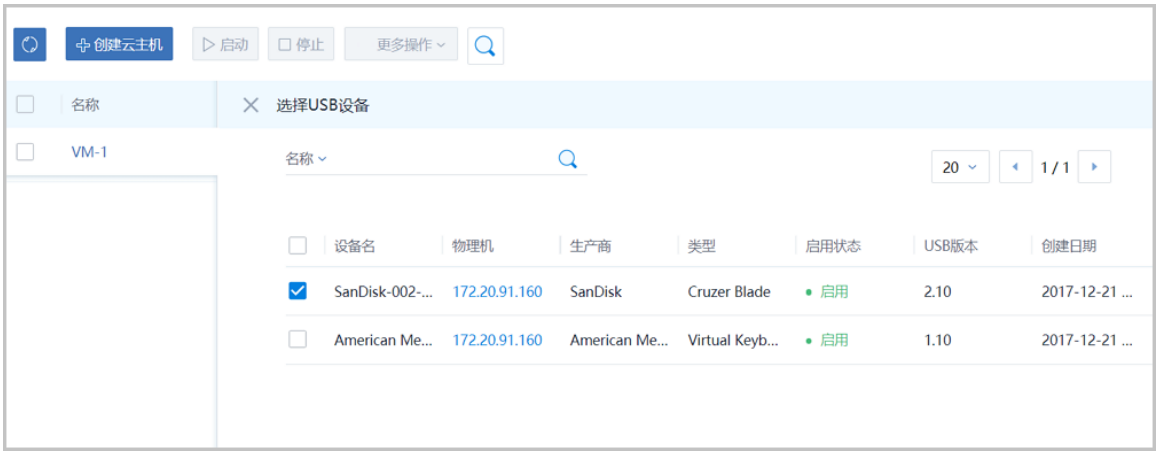
在**云主机**界面点击云主机名称进入**云主机详情**页面，点击**配置信息**进入**配置信息**子页面。在USB设备处，点击**操作**，在下拉菜单中选择**加载**，如图 *233:* 配置信息所示：

图 233: 配置信息



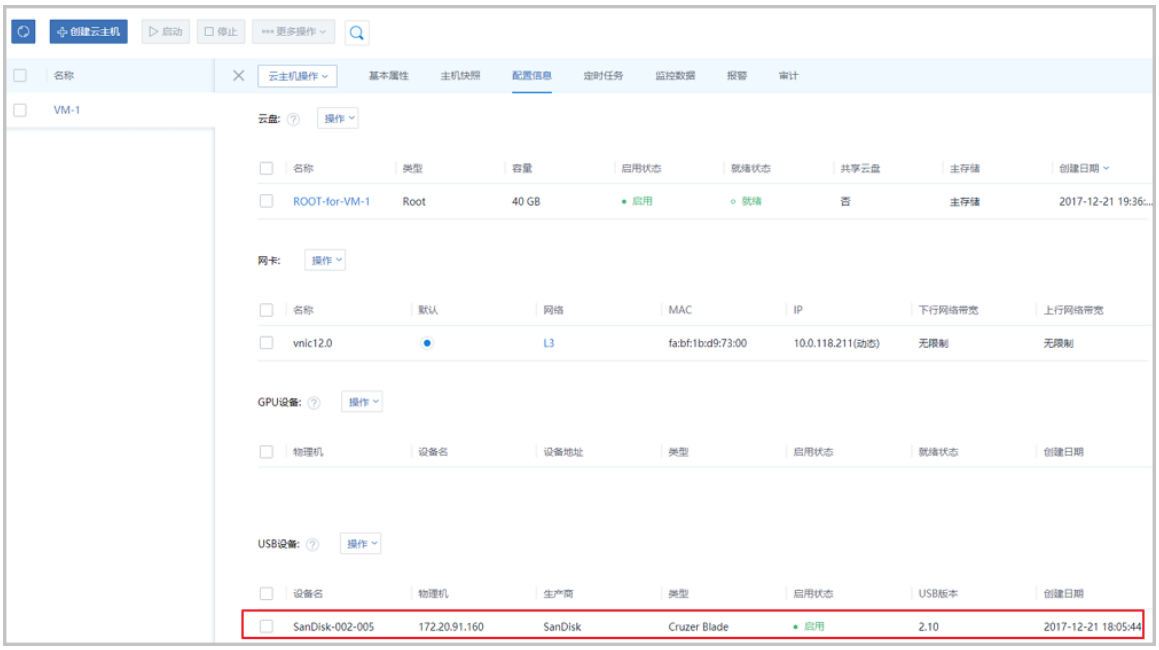
b) 弹出**选择USB设备**界面，选择要加载到云主机VM上的USB设备，如图 *234:* 加载*USB*设备所示：

图 234: 加载USB设备



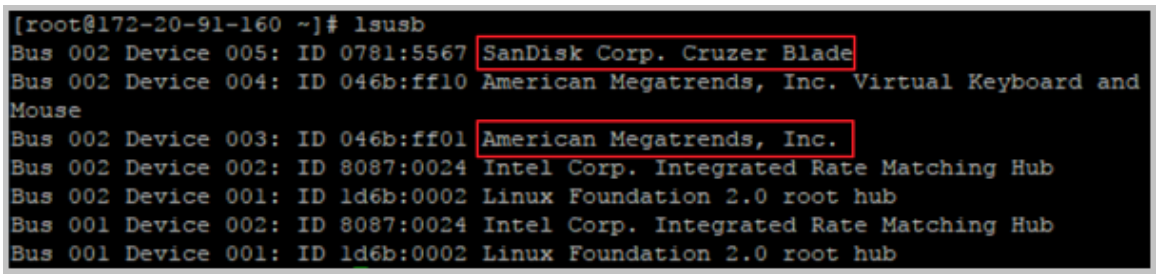
c) 云主机加载USB设备列表，如图 *235:* 云主机加载*USB*设备列表所示：

图 235: 云主机加载USB设备列表



3. 登入云主机控制台，执行lsusb命令，可查看已成功加载到云主机的USB设备。

图 236: 查看云主机加载的USB设备



注:

可使用yum install usbutils或apt install usbutils来安装lsusb命令。此时确保云主机可连接公网。

4. 安装USB3.0驱动

Windows 2003、Windows 2008和Windows 7系统，不支持USB 3.0设备的直接加载，需要手动安装驱动。

请在ZStack官方百度云盘获取驱动文件，地址：

https://pan.baidu.com/s/11T_qZ92JtBltcIKwcO1Dvg

提取码：mc7y，双击文件完成安装。

注:

- 对于USB2.0设备，Linux和Windows云主机均可加载并识别；
- 对于USB3.0设备，Linux云主机可加载并识别；Windows云主机中，Windows 2003、Windows 2008和Windows 7系统需要手动安装，或将USB3.0设备插在USB2.0口中，以提高识别率。
- 云主机加载USB设备的数量有上限限制：
  - USB1.0设备：最多支持加载1个
  - USB2.0设备：最多支持加载6个
  - USB3.0设备：最多支持加载4个

后续操作

至此，USB透传功能介绍完毕。

7.3.3.2 裸机部署教程

7.3.3.2.1 介绍

ZStack支持裸机部署功能。在完成基本的服务器上架以及相关准备工作后，管理员可在ZStack UI界面进行大规模批量部署，部署完成后的服务器可以直接添加到ZStack集群中，大幅缩短新设备上线流程。

根据实际情况，管理员可以选择半自动化或者自动化批量部署。

- 半自动化批量部署：

  当装机量较小，或者硬件不支持IPMI时，可以将ZStack管理节点视为PXE服务器，为物理机提供基于PXE环境的部署服务；管理员需手动开启每台物理机，选择PXE启动进入系统安装界面，然后手动配置物理机。
- 自动化批量部署：

  当装机量较大，并且硬件支持IPMI时，管理员可在ZStack UI界面上完成系统配置操作，并远程启动、部署众多物理机，无需进入机房。

本文档主要介绍自动化批量部署方法。

7.3.3.2.2 准备工作

批量部署的基本原理是：管理节点（PXE服务器）提供PXE服务，指示多台物理机（PXE客户端）由网络启动，从管理节点下载并安装相应的软件包。

为保证批量部署的顺利进行，需提前做好以下准备工作：

1. 手动安装管理节点
2. 进入物理机BIOS启用PXE
3. 规划裸机安装网络
4. 配置物理机IPMI

7.3.3.2.2.1 手动安装管理节点

首先，管理员需要使用最新的ZStack定制版ISO安装一台管理节点。

注: 务必使用ZStack定制版ISO来安装，否则管理节点无法通过TFTP服务为物理机提供软件包。

管理员可从*ZStack*官方网站下载并安装ZStack定制版ISO，安装时请选择企业版管理节点模式（ZStack Enterprise Management Node）。具体操作步骤可以参考用户手册安装部署章节。

注: 请获取ZStack定制版ISO，c74或c72版本。

- 文件名称：ZStack-x86_64-DVD-2.5.1-c74.iso
- 下载地址：点击这里
- 文件名称：ZStack-x86_64-DVD-2.5.1-c72.iso
- 下载地址：点击这里

7.3.3.2.2.2 进入物理机BIOS启用PXE

手动安装好一台管理节点后，管理员需要进入每台物理机的BIOS，**确认其首张网卡的PXE是Enable状态。**保险起见可以将所有网卡的PXE都设为Enable状态。

同时，由于管理节点提供长期的PXE服务，为防止物理机每次启动都进入PXE启动，**推荐将物理机的第一启动项设置为磁盘。**

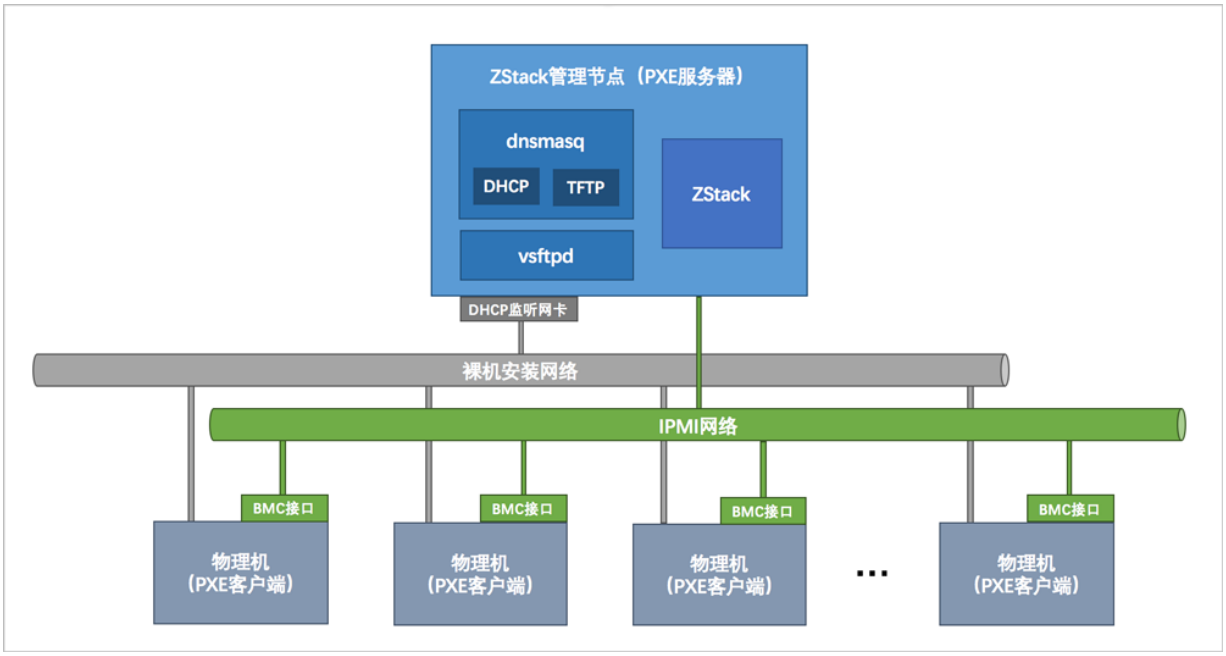
管理员可以通过快捷键或者IPMI临时修改启动顺序，使物理机按需PXE启动。

7.3.3.2.2.3 规划裸机安装网络

通常情况下，将物理机添加到ZStack集群时，需要输入物理机的IP地址；为了提高网络稳定性，在条件允许时还要配置网卡Bond。为了使批量部署后的物理机可以不加修改地直接添加到集群，管理员需要事先做好网络规划，并且在裸机部署过程中为每台物理机指定其网络配置。

参考如图 *237: 裸机安装网络(见灰色) 规划示意图*所示规划裸机安装网络：

图 237: 裸机安装网络(见灰色) 规划示意图



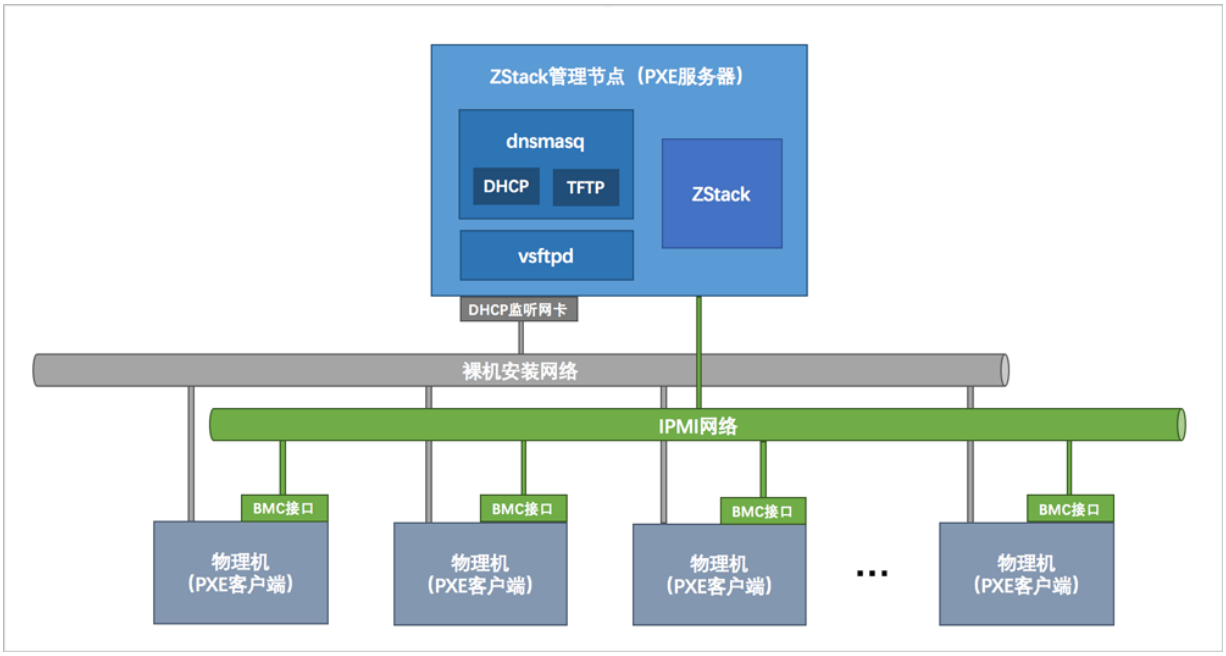
1. 要求管理节点DHCP接口是一个独立的、有IP地址的网卡，对外提供稳定的DHCP服务。
2. 用于裸机安装的网络，在各待部署物理机上均不能连接其他DHCP服务，以避免DHCP服务冲突。
3. 请根据实际生产环境，提前规划好每台物理机应该分配的IP地址，以及网卡绑定等细节问题。

7.3.3.2.2.4 配置物理机IPMI

如果物理机自带BMC管理口，应提前为每台物理机配置好IPMI地址、用户名和密码。

参考如图 *238: IPMI网络(见绿色) 规划示意图*所示规划IPMI网络：

图 238: IPMI网络(见绿色) 规划示意图



1. 管理节点通过IPMI网络连接到每台物理机的BMC接口，从而实现管理节点远程控制所有物理机。
2. 通过IPMI，管理员可在ZStack UI界面完成所有裸机的批量部署操作。
3. 如前文所述，如果硬件不支持IPMI，则在完成必要的准备工作，并创建PXE服务后，管理员需手动开启每台物理机，选择PXE启动进入系统安装界面，然后手动配置物理机。

7.3.3.2.3 自动化批量部署

准备工作完成后，管理员可以登录ZStack管理节点界面（http://your_management_node_ip:5000/），开始进行自动化批量部署物理机，主要有以下两大步骤：

1. 创建PXE服务：在管理节点安装并启动PXE服务
2. 裸机安装：批量添加裸机并自动化部署系统

注:

首次登录ZStack，系统界面将引导进行ZStack私有云平台基本的初始化环境配置；在本场景下（自动化批量部署物理机），请跳过Wizard初始化引导设置。

7.3.3.2.3.1 安装服务

操作步骤

1. 进入**安装服务**界面。

在ZStack私有云主菜单，点击 **硬件设施** > **计算服务器** > **安装服务**，进入**安装服务**界面，如图 *239: 安装服务界面*所示：

图 239: 安装服务界面

2. 创建PXE服务。

点击**创建PXE服务**，弹出**创建PXE服务**界面，可参考以下示例输入相应内容：

- **名称**：例如PXE服务
- **简介**：可选项，可留空不填
- **DHCP监听网卡**：管理节点上的裸机安装网络的网卡设备编号。

注:

- 此网卡要求连接到裸机安装网络，且已配置IP地址。
- 该监听网卡所在网络不能存在已有的DHCP服务。

- **起始IP**和**结束IP**：可选项，可留空不填

注:

- 如果管理员不指定**起始IP**和**结束IP**，ZStack会自动根据DHCP监听网卡推断出最大的动态分配地址范围
- 管理员可以根据实际情况缩小地址范围

如图 *240: 创建PXE服务*所示，点击**确定**按钮，PXE服务将成功创建。

图 240: 创建PXE服务

3. PXE服务支持的操作。

在**安装服务**主界面，成功创建的PXE服务处于**运行中**状态，PXE环境已准备就绪。这时管理员可通过**启用**、**停用**按钮按需启用/停用PXE服务。

如图 *241: 启用/停用PXE服务*所示：

图 241: 启用/停用PXE服务

如果需要变更DHCP监听网卡，需删除后重建PXE服务。选中PXE服务名称，点击**删除**按钮，删除PXE服务。如图 *242: 删除PXE服务*所示：

图 242: 删除PXE服务

注: 删除PXE服务会删除裸机管理中的所有资源，需谨慎操作！

7.3.3.2.3.2 裸机管理

前提条件

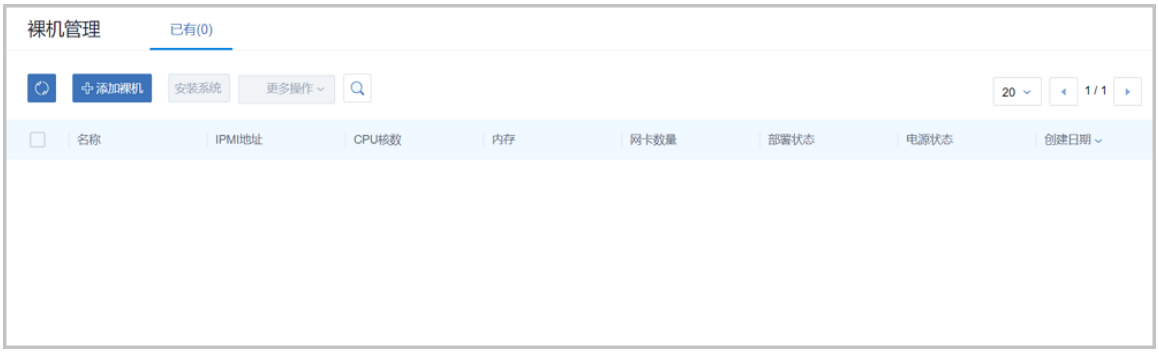
在保证PXE服务存在且处于运行状态的前提下，可以进入**裸机管理**界面，开始批量部署裸机。

操作步骤

1. 进入**裸机安装**界面。

   在ZStack私有云主菜单，点击**硬件设施** > **计算服务器** > **裸机管理**，进入**裸机管理**界面，如图 *243: 裸机管理界面*所示：

   图 243: 裸机管理界面



2. 添加裸机。

   添加裸机，主要负责将裸机的IPMI配置信息录入ZStack。

   如前文所述，在准备工作中，管理员已提前为每台物理机配置好IPMI地址、用户名和密码，而通过该IPMI配置可以唯一地确定一台物理机。

ZStack支持批量添加裸机。

点击**添加裸机**，弹出**添加裸机**界面，可参考以下示例输入相应内容：

- **名称**：例如Host-1
- **简介**：可选项，可留空不填
- **IPMI地址**：填写已为物理机配置好的IPMI地址
- **IPMI用户名**：填写已为物理机配置好的IPMI用户名
- **IPMI密码**：填写已为物理机配置好的IPMI密码
- **重启裸机**：重启裸机，可自动获取裸机硬件信息

  注:

  - 勾选后，会进行裸机重启，可自动获取裸机的硬件信息。
  - 默认不勾选，需手动重启获取裸机硬件信息。
- **添加更多裸机**：点击加号按钮，支持批量添加裸机

如图 *244:* 添加裸机界面和图 *245:* 支持批量添加裸机所示：

图 244: 添加裸机界面

图 245: 支持批量添加裸机

确定
取消
添加裸机
名称 *
Host-3
简介
IPMI地址 *
10.0.0.5
IPMI用户名 *
root
IPMI密码 *
••••••••
重启裸机
添加更多裸机
已配置裸机信息
名称: Host-1
简介:
IPMI地址: 10.0.0.3
IPMI用户名: root
IPMI密码: ******
名称: Host-2
简介:
IPMI地址: 10.0.0.4
IPMI用户名: root
IPMI密码: ******

3. 安装系统。

安装系统，主要负责完善裸机的ks.cfg配置文件，实现无人值守的自动化批量部署操作。

a) 进入**安装系统**界面。

成功获取硬件配置后，选中一台裸机，例如：Host-1，可以看到**安装系统**按钮由灰色点亮，点击**安装系统**按钮，如图 *246:* 点击安装系统按钮所示：

图 246: 点击安装系统按钮

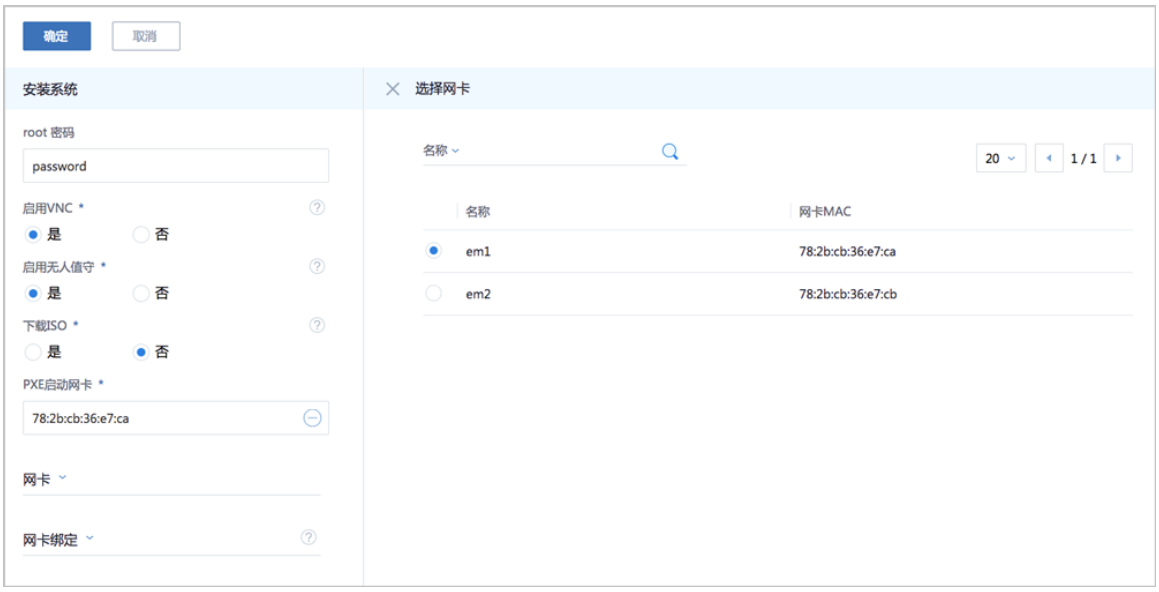
注:

- 安装系统：裸机的ks.cfg配置文件需要逐一完善，因此**安装系统**操作需要单台裸机逐一进行；如果选中多台裸机，**安装系统**按钮变灰
- 重装系统：由于裸机尚未安装系统，**重装系统**按钮为灰色
- 开机、关机、重启、删除操作：支持单台裸机或批量裸机的开机、关机、重启、删除操作

b) 完善裸机Host-1的ks.cfg配置文件。

弹出**安装系统**界面，如图 *247:* 安装系统界面所示：

图 247: 安装系统界面



可参考以下示例输入相应内容：

- **root密码**：管理员可以配置root密码
- **启用VNC**：建议选择**是**，表示启用VNC界面，可打开裸机控制台查看安装过程
- **启用无人值守**：
  - 选择**是**：

    表示进行自动分区模式，默认采取全盘LVM分区策略，并将大部分容量分配给根分区，以保证系统安装过程能够自动完成
  - 选择**否**：

    表示需自定义磁盘分区

    关闭无人值守，裸机从PXE自动重启后，进入系统安装界面将暂停，等待管理员进行手动配置
- **下载ISO**：
  - 选择**是**：

    表示将ISO拷贝至裸机的*/opt/zstack-dvd*目录，并创建YUM本地源
  - 选择**否**：

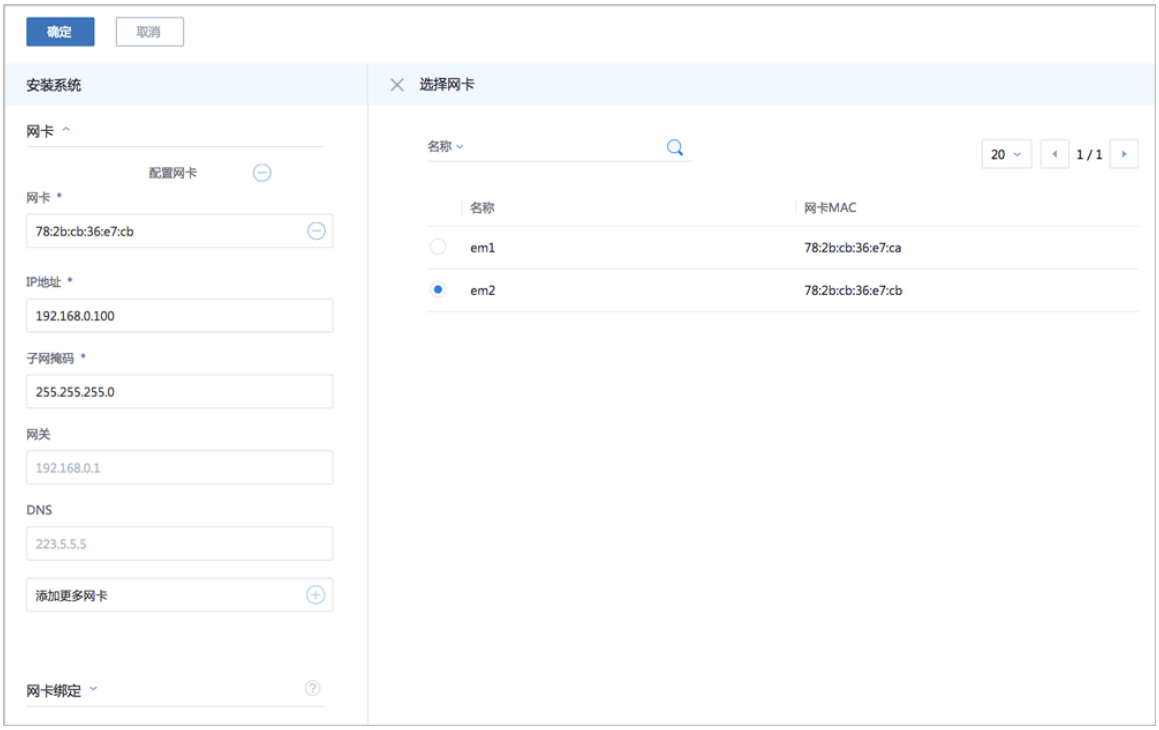
    表示不下载ISO至裸机的*/opt/zstack-dvd*目录

    注:

    - 在裸机部署过程中，考虑到网络负载压力，默认不下载ISO至裸机的*/opt/zstack-dvd/*目录
    - 但在某些特殊场景下，比如需在多台裸机上部署Ceph存储时，就可选择下载ISO，从而利用该本地源安装Ceph软件包
- **PXE启动网卡**：物理机上开启PXE功能的网卡
    - 必须接入裸机安装网络
    - 必须在BIOS中设置PXE为Enable状态
- **网卡**：管理员可以根据网络规划，为每台裸机中的多张网卡配置网络
- **网卡绑定**：支持创建网卡Bond

展开**网卡选项**，如图 *248:* 展开网卡选项所示：

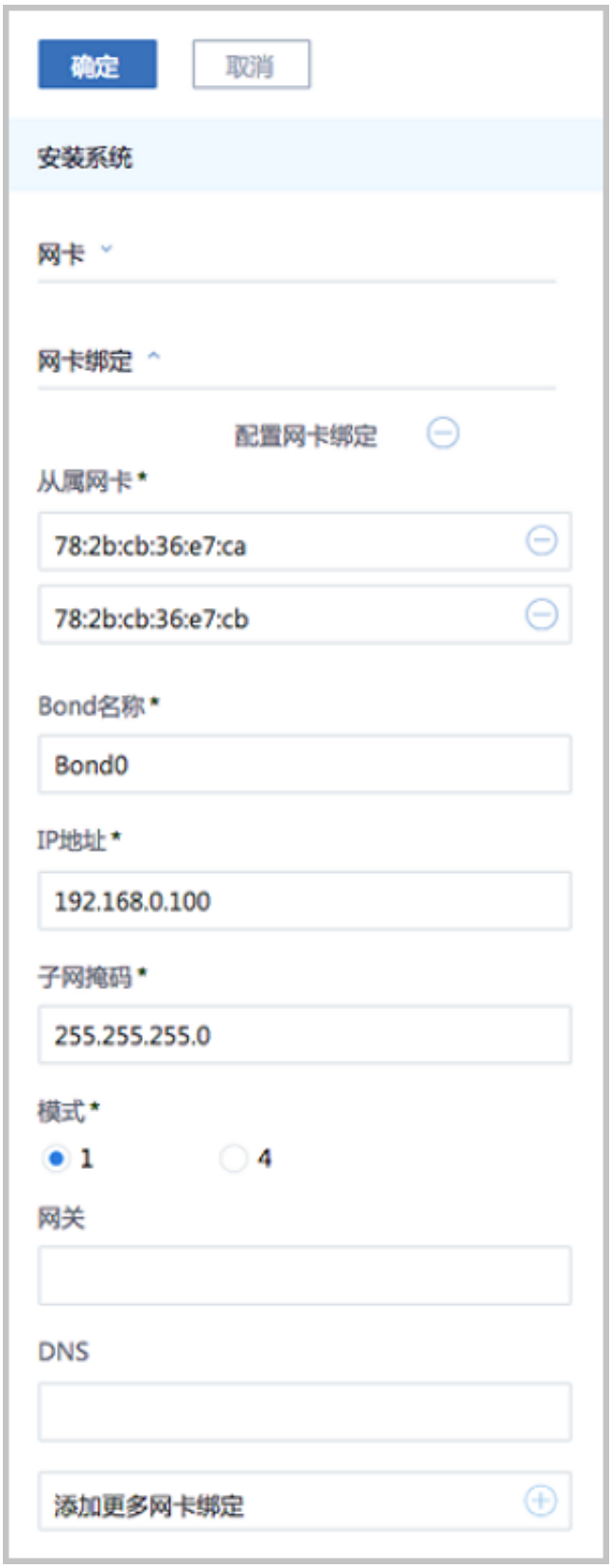
图 248: 展开网卡选项



展开**网卡绑定**选项，如图 *249:* 展开网卡绑定选项所示。

注: 默认选择模式**1**，如果选择模式**4**，需要交换机支持。

图 249: 展开网卡绑定选项



c）点击**确定**，回到**裸机安装**主界面，可以看到裸机Host-1的**电源状态**变为**重启中。**

如图 *250:* 重启中所示：

图 250: 重启中

d) 裸机Host-1重启后，在已完善的ks.cfg配置文件指导下执行自动化部署，**部署状态**变为**部署中。**

如图 *251:* 部署中所示：

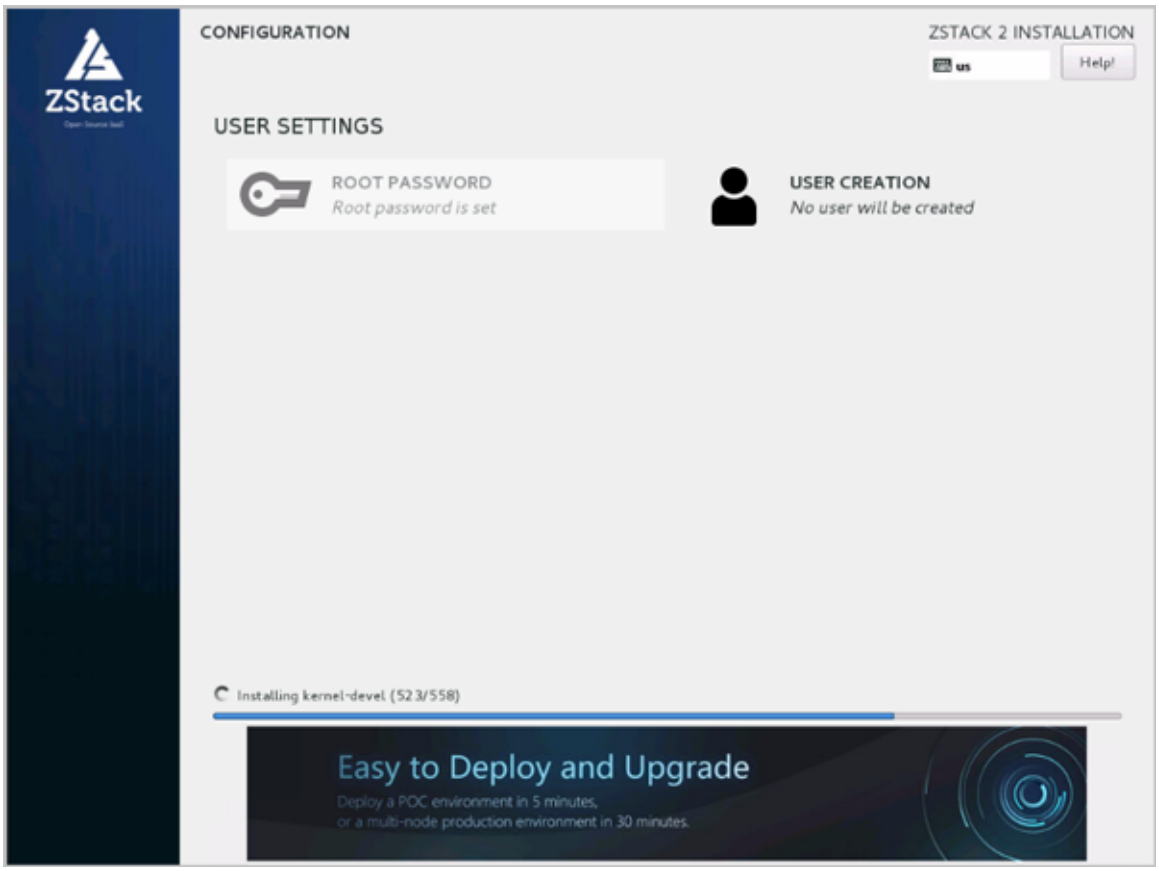
图 251: 部署中

e) 对于处于**部署中**的裸机Host-1，进入其**裸机详情**页，点击控制台按钮，可以实时观察系统安装过程。

如图 *252:* 处于部署中状态的裸机详情页和图 *253:* 进入控制台观察系统安装过程所示：

图 252: 处于部署中状态的裸机详情页

图 253: 进入控制台观察系统安装过程



注:

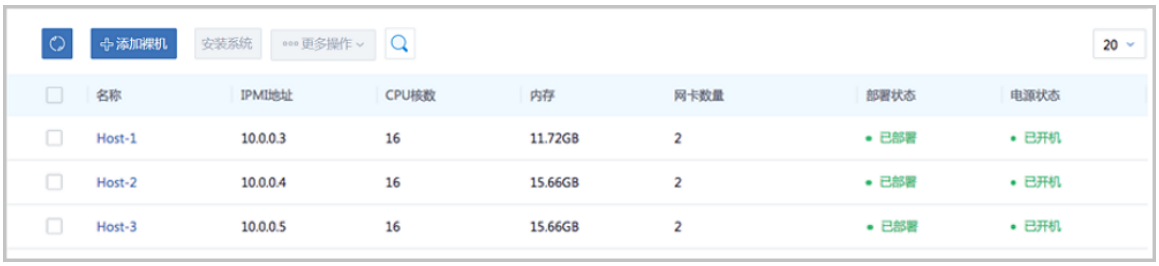
如果该裸机的ks.cfg配置文件中将VNC关闭，就不能进入控制台查看系统安装过程了，而且在**裸机详情**页里没有控制台按钮，如图 *254: VNC关闭*所示：

图 254: VNC关闭

f) 系统安装结束后，返回**裸机安装**主界面，可以看到裸机Host-1已经处于**已部署**状态。

如图 *255: 已部署*所示：

图 255: 已部署



g) 同裸机Host-1，可自动化批量部署其他裸机。

4. 查看网卡配置信息。

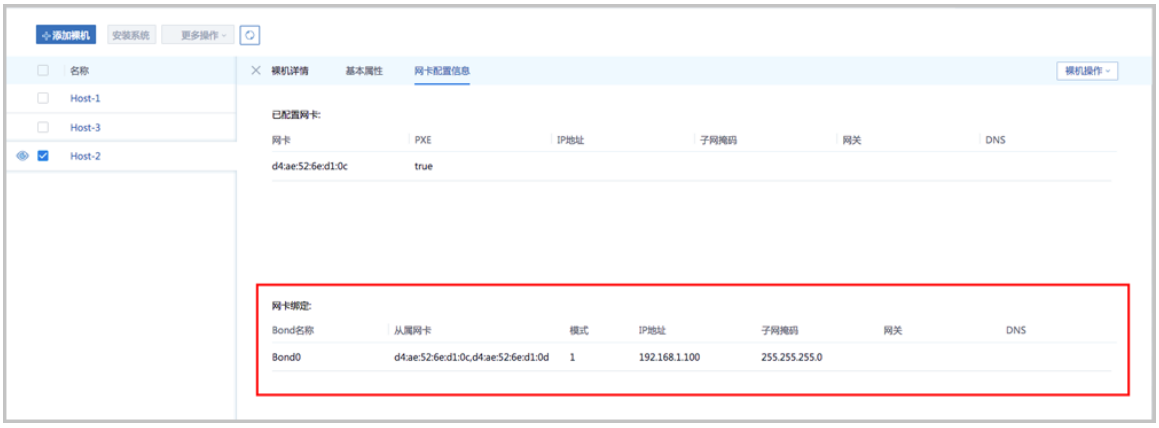
对于已部署的裸机，可以进入其**裸机详情**页的**网卡配置信息**子页面，查看已生效的网络配置，包括普通网络配置以及网卡绑定信息等。

此时，该裸机已经可以直接添加至ZStack集群。

如图 *256: 普通网络配置*和图 *257: 网卡绑定配置*所示：

图 256: 普通网络配置

图 257: 网卡绑定配置



5. 重装系统。

   如果希望为某台裸机重装系统，可以进入其**裸机详情**页，点击**重装系统**。

   注：重装系统会清空裸机内容，请谨慎操作。

   如图 *258:* 重装系统和图 *259:* 重装系统确认窗口所示：

图 258: 重装系统

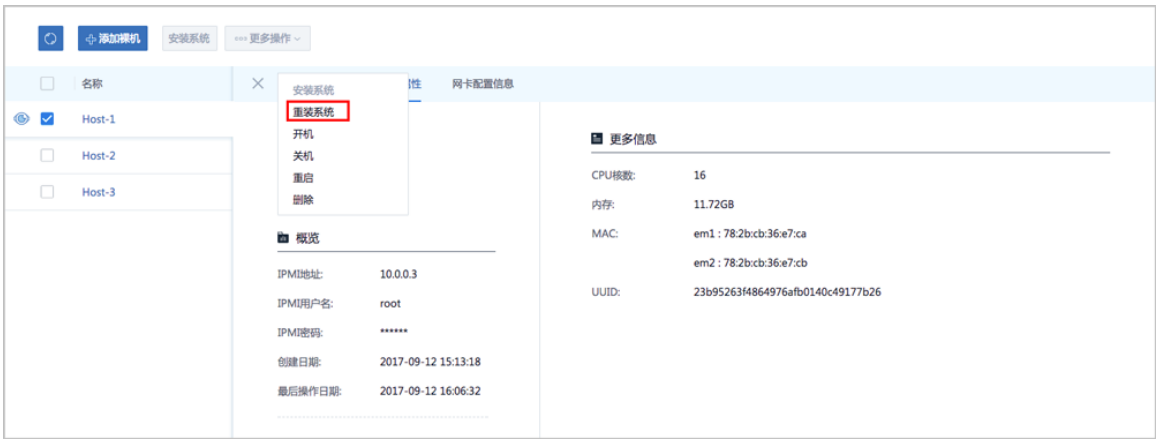
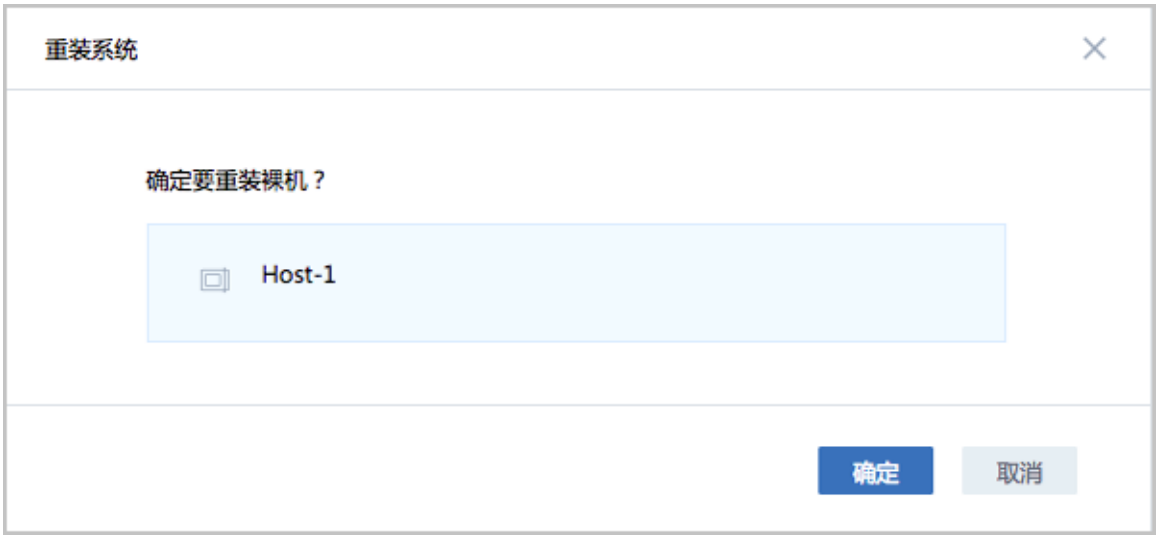


图 259: 重装系统确认窗口



6. 开机、关机、重启和删除。

   对于已部署的裸机，支持对单个裸机或批量裸机的开机、关机、重启和删除操作。

后续操作

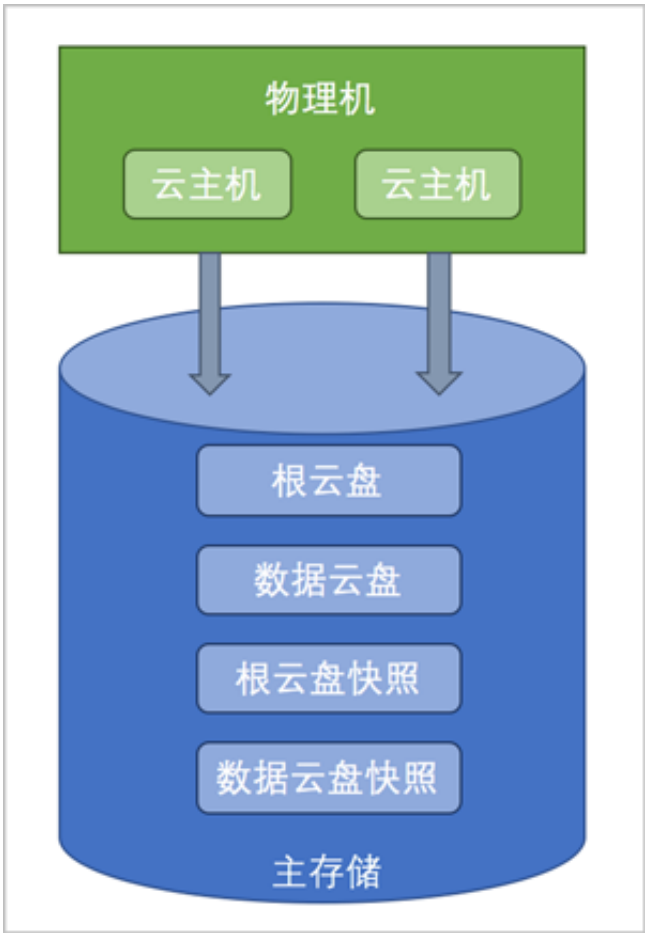
至此，ZStack成功完成自动化批量部署物理机。

7.3.4 主存储

主存储：用于存储云主机磁盘文件（包括：根云盘、数据云盘、根云盘快照、数据云盘快照、镜像缓存等）的存储服务器。

如图 *260:* 主存储所示：

图 260: 主存储



主存储支持类型分为两大类：

- **本地存储**（Local Storage）：使用物理机的硬盘进行存储。不带数据云盘克隆云主机时，支持ImageStore或Ceph类型的镜像服务器，在线/暂停/关机克隆；整机克隆时，支持ImageStore类型的镜像服务器，在线/暂停/关机克隆。
- **网络共享存储**：支持NFS、Shared Mount Point、Ceph、Shared Block和FusionStor类型。
  - NFS为网络文件系统的存储方式。
  - Shared Mount Point支持常用的分布式文件系统提供的网络共享存储， 支持的常见类型有MooseFS，GlusterFS，OCFS2，GFS2等。
  - Ceph采用了分布式块存储方式。
  - Shared Block采用了共享块存储方式。
  - FusionStor采用了华云网际提供的分布式块存储方式。

注:

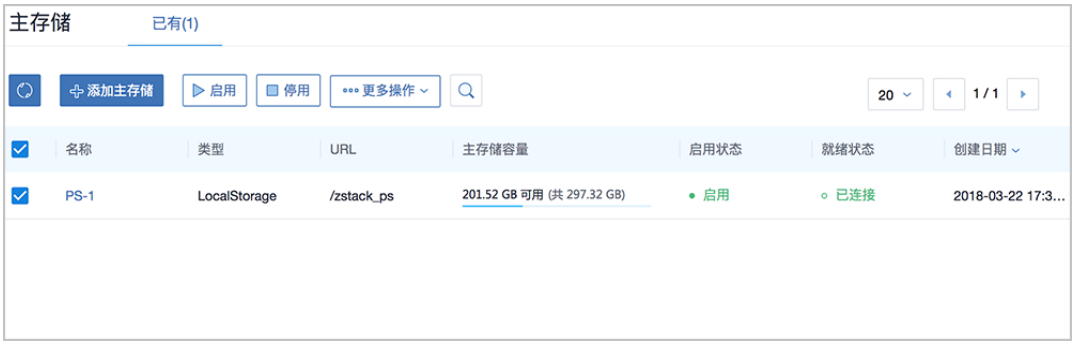
- 不带数据云盘克隆时，所有主存储类型，支持在ImageStore或Ceph类型的镜像服务器情况下，云主机在线/暂停/关机克隆。

- 整机克隆时，LocalStorage、NFS、SMP和Ceph类型的主存储，支持在ImageStore类型的镜像服务器情况下，云主机在线/暂停/关机克隆；Shared Block类型的主存储，支持在ImageStore类型的镜像服务器情况下，云主机暂停/关机克隆。

7.3.4.1 主存储操作

在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**管理界面，如图 *261: 主存储*所示。在主存储管理界面，可以查看当前区域内加载的所有主存储的信息，包括：主存储名称、类型、URL、容量和状态等等。并可以对主存储进行添加、启用、停用和删除等操作。

图 261: 主存储



ZStack对主存储操作的定义如下：

- **搜索**：在主存储管理界面上支持三种搜索方式：名称、UUID和高级搜索。
- **添加主存储**：添加一个主存储到系统中。因为主存储类型较多，每种类型主存储添加界面稍有差异，下面的章节会详细介绍。
- **启用**：将选中的处于停用状态的主存储启用。**支持批量操作。**
- **停用**：将选中的主存储停用。停用主存储后，此主存储上的所有云盘被停用并且新的云主机、云盘、快照将无法创建。**支持批量操作。**
- **重连**：重新连接选中的主存储。重连主存储会更新主存储相关的存储信息。**支持批量操作。**

  注: 如果有任意一台物理机正常连接到主存储，该主存储的就绪状态就会显示为**已连接。**

- **创建云盘**：在选中的主存储上面创建一个云盘出来，此云盘为实例化云盘。**只支持单一主存储操作。**
- **加载集群**：将选中的主存储加载到指定的集群上。一个集群可以挂载多个主存储，目前支持的场景有：
  - 一个集群可以挂载一个或多个本地主存储。

  - 一个集群可以挂载一个或多个NFS主存储。
  - 一个集群可以挂载一个或多个Shared Block主存储。
  - 一个集群可以挂载一个Shared Mount Point主存储。
  - 一个集群可以挂载一个本地主存储和一个NFS主存储。
  - 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
  - 一个集群可以挂载一个本地主存储和一个Shared Block主存储。
  - 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。
  - 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
  - 一个主存储可以挂载到多个集群 。
- **卸载集群**：将选中的主存储从指定的集群上卸载。
- **进入维护模式**：主存储进入维护模式后，会停止所有使用该主存储的云主机（包括NeverStop）。**支持批量操作。**
- **删除**：将选中的主存储删除掉。执行删除操作前请从所有集群卸载该主存储否则不能删除。删除主存储后，此主存储上的所有云主机和云盘都会被删除。**支持批量操作。**

注: 删除主存储是非常危险的操作，此操作会直接删除该主存储上的所有云主机和云盘。即使重新添加此主存储，也无法自动识别原有的文件。

7.3.4.2 主存储类型--本地存储

如果主存储类型采用本地存储（Local Storage），那么使用各物理机的本地硬盘目录作为主存储，匹配镜像仓库或Sftp镜像服务器，容量由各物理机的目录容量累加。

在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**页面，点击**添加主存储**按钮，可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择LocalStorage
- **URL**：输入本地存储的路径

注:

  - 不能使用以下/、 /dev/、/proc/、/sys/、/usr/bin、/bin等系统目录。
  - 使用系统目录可能会导致物理机异常。

- **集群**：选择主存储需要挂载的集群

如图 *262: 本地存储*所示，点击**确定**按钮，完成LocalStorage添加。

图 262: 本地存储

ZStack支持一个集群挂载多个主存储，目前支持的场景有：

- 一个集群可以挂载一个或多个本地主存储。
- 一个集群可以挂载一个或多个NFS主存储。
- 一个集群可以挂载一个或多个Shared Block主存储。
- 一个集群可以挂载一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个NFS主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Block主存储。

- 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。
- 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
- 一个主存储可以挂载到多个集群 。

注:

如果挂载多个本地存储，请确保每个本地存储必须部署在独占的逻辑卷或物理磁盘上。

7.3.4.3 主存储类型--NFS

如果主存储类型采用NFS，那么ZStack会在所有的物理机上自动挂载相同的NFS共享目录作为主存储。匹配镜像仓库或Sftp镜像服务器，会在所有物理机上自动挂载此目录。

在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**页面，点击**添加主存储**按钮，可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择NFS
- **URL**：输入NFS Server的共享目录的URL

注:

- 输入格式为：*NFS_Server_IP:/NFS_Share_folder*
- 请提前在NFS Server端设置相应目录的访问权限。
- 为保证在NFS Server端的安全控制，建议配置相应安全规则，进行访问控制。
- 用户可以提前在NFS Server端通过showmount -e命令检查NFS Server已共享的目录。
- 不能使用以下/、 /dev/、/proc/、/sys/、/usr/bin、/bin等系统目录。
- 使用系统目录可能会导致物理机异常。

- **挂载参数**：可选项，需NFS Server端支持

注:

- 参数以逗号隔开。
- NFS的mount参数可以参考mount的 -o选项里的内容。
- 可根据常用的客户端mount命令参数进行设置。如果设置的参数与NFS Server端冲突，则以Server端为准。

- **存储心跳网络CIDR**：可选项，使用此存储网络来判断云主机健康状态，不填默认与管理网络共用
- **集群**：选择主存储需要挂载的集群

如图 *263: NFS存储*所示，点击**确定**按钮，完成NFS添加。

图 263: NFS存储

ZStack支持一个集群挂载多个主存储，目前支持的场景有：

- 一个集群可以挂载一个或多个本地主存储。
- 一个集群可以挂载一个或多个NFS主存储。
- 一个集群可以挂载一个或多个Shared Block主存储。
- 一个集群可以挂载一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个NFS主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Block主存储。
- 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。
- 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
- 一个主存储可以挂载到多个集群 。

7.3.4.4 主存储类型--Shared Mount Point

1. Shared Mount Point提供了对MooseFS，GlusterFS，OCFS2，GFS2等可以提供共享文件系统存储的支持。
2. 添加过程与本地存储类似，用户只需提供物理机挂载的本地目录，ZStack即可完成对各种分布式文件系统的对接。
3. 选择使用Shared Mount Point，用户需要提前配置好相应的分布式文件系统。并且根据不同存储系统的客户端配置，预先在每台物理机上把共享文件系统挂载在相同的文件路径。
4. 下面以MooseFS为例来配置主存储。

   假如MooseFS的master Server IP地址为*172.20.12.19*。用户需要下载并安装MooseFS的客户端工具mfsmount。并且创建相应目录作为mount节点。

   注:

   例如，创建*/mnt/mfs*作为挂载点，使用*mfsmount*命令挂载MooseFS系统。用户也可以根据需要使用*mfssetgoal*命令设置相应的文件副本保存数量。

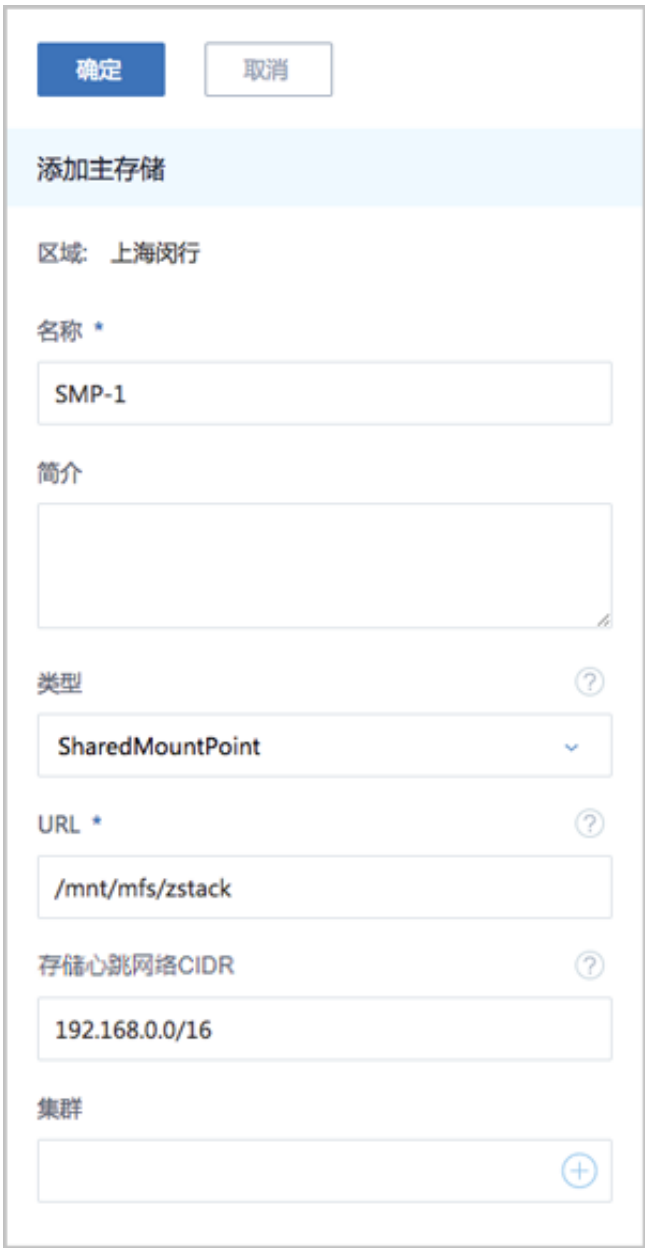
   ```
   [root@localhost ~]#mkdir /mnt/mfs
   [root@localhost ~]#mfsmount /mnt/mfs -H 172.20.12.19
   [root@localhost ~]#mkdir /mnt/mfs/zstack
   [root@localhost ~]#mfssetgoal -r 2 /mnt/mfs/zstack/
   #以上命令将/mnt/mfs/zstack/目录的文件挂载到远端172.20.12.19，MooseFS存储服务器保留两份拷贝。
   ```

在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**页面，点击**添加主存储**按钮，可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择SharedMountPoint
- **URL**：输入物理机已挂载的共享存储目录URL
- **存储心跳网络CIDR**：可选项，使用此存储网络来判断云主机健康状态，不填默认与管理网络共用
- **集群**：选择主存储需要挂载的集群

如图 *264: Shared Mount Point存储*所示，点击**确定**按钮，完成Shared Mount Point添加。

图 264: Shared Mount Point存储



ZStack支持一个集群挂载多个主存储，目前支持的场景有：

- 一个集群可以挂载一个或多个本地主存储。
- 一个集群可以挂载一个或多个NFS主存储。
- 一个集群可以挂载一个或多个Shared Block主存储。
- 一个集群可以挂载一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个NFS主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Block主存储。
- 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。

- 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
- 一个主存储可以挂载到多个集群 。

7.3.4.5 主存储类型--Ceph

ZStack对Ceph的支持为块存储的模式。如果主存储类型选择Ceph，则需要先添加一个Ceph类型的镜像服务器或镜像仓库类型的镜像服务器，并且提前配置好Ceph分布式存储。

在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**页面，点击**添加主存储**按钮，可参考以下示例输入相应内容：

- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择Ceph
- **关闭CEPHX**：CEPHX代表Ceph密钥认证，默认关闭

  注:

  - 关闭CEPHX，代表关闭Ceph密钥认证；
  - 如果计算节点的网络较安全，可关闭此项，以避免Ceph的认证失败；
  - 需确保Ceph存储已关闭密钥认证，如果Ceph存储未关闭，此处勾选可能导致创建云主机失败。
- **管理IP**：输入Ceph监控节点的IP地址Mon IP
- **SSH端口**：输入Ceph监控节点的SSH端口，默认为22
- **用户名**：输入Ceph监控节点的用户名
- **密码**：输入Ceph监控节点的用户名对应的密码
- **继续添加**：点击加号按钮继续添加Ceph监控节点
- **镜像缓存池名**：输入镜像缓存池名，如果不填，系统会自动为用户创建这三个池
- **数据云盘池名**：输入数据云盘池名，如果不填，系统会自动为用户创建这三个池
- **根云盘池名**：输入根云盘池名，如果不填，系统会自动为用户创建这三个池
- **存储心跳网络CIDR**：可选项，使用此存储网络来判断云主机健康状态，不填默认与管理网络共用
- **集群**：选择主存储挂载的集群

如图 *265: 添加Ceph主存储*所示，点击**确定**按钮，完成Ceph添加。

图 265: 添加Ceph主存储

ZStack支持一个集群挂载多个主存储，目前支持的场景有：

- 一个集群可以挂载一个或多个本地主存储。
- 一个集群可以挂载一个或多个NFS主存储。
- 一个集群可以挂载一个或多个Shared Block主存储。
- 一个集群可以挂载一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个NFS主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Block主存储。
- 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。
- 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
- 一个主存储可以挂载到多个集群 。

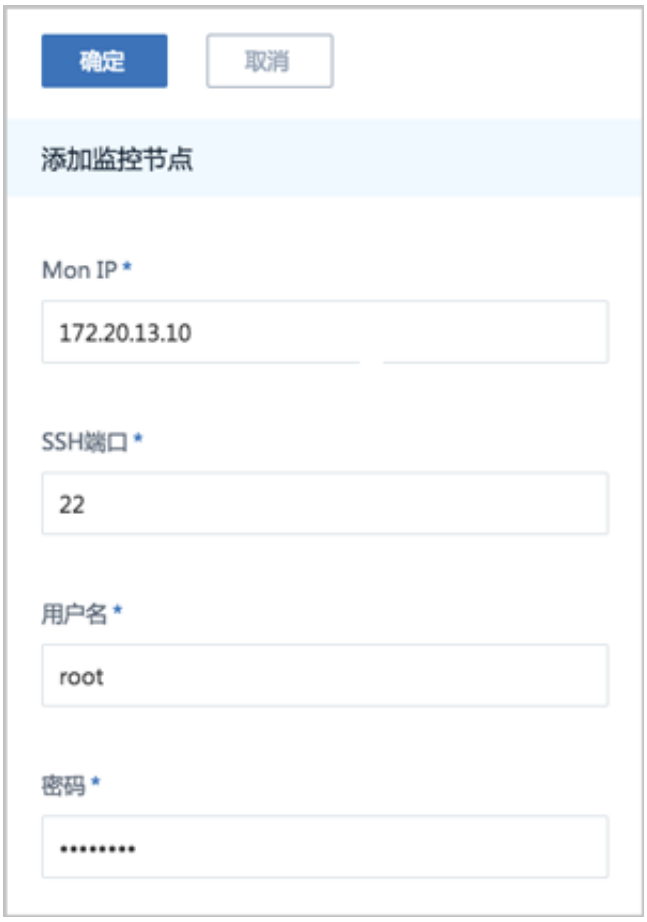
一般Ceph集群会配置多个监控节点。

1. 进入Ceph主存储详情页，点击**监控节点**，进入**监控节点**子页面，支持添加多个Ceph监控节点。如图 *266: 添加监控节点-1*所示：

   图 266: 添加监控节点-1

2. 点击**监控节点**右边的**操作** > **添加监控节点**，弹出**添加监控节点**界面，输入新增监控节点的Mon IP、SSH端口号、用户名和密码，如图 *267: 添加监控节点-2*所示：

   图 267: 添加监控节点-2



注:

- 请确保至少输入一个可用的Ceph监控节点。
- 建议在初始化引导界面，只添加一个Ceph监控节点以快速完成基本的初始化，其他监控节点也可在主存储界面再次挂载添加。
- 如果用户对Ceph的相关配置不熟悉，建议选择其他主存储类型进行配置。

7.3.4.6 主存储类型--Shared Block

Shared Block（共享块存储）是ZStack企业版新支持的一种主存储类型，可以将用户在SAN存储上划分的LUN设备直接作为存储池，再提供给业务云主机使用。与之前Shared Mount Point（SMP）主存储类型不同，**Shared Block**具备便捷部署、灵活扩展、性能优异等优势。

如果主存储类型采用Shared Block，那么使用共享块设备作为主存储，匹配镜像仓库，支持添加一个或多个共享块设备，需输入磁盘唯一标识，例如：磁盘UUID、WWN、WWID。

在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**界面，点击**添加主存储**按钮，可参考以下示例输入相应内容：

- **名称**：输入主存储的名称
- **简介**：可选项，可留空不填
- **类型**：选择SharedBlock类型
- **清理块设备**：默认不勾选

  注:

  - 勾选后将强制清理LUN设备中的文件系统、RAID或分区表中的签名，请谨慎选择。
  - 若LUN设备中未存放重要数据，可勾选此项。
  - 添加的LUN设备中不能有分区，否则会添加失败。
- **磁盘UUID**：输入磁盘唯一标识，例如：磁盘UUID、WWN、WWID；支持添加多个共享块设备
- **集群**：可选项，选择加载的集群

如图 *268: 添加Shared Block主存储*所示，点击**确定**按钮，添加Shared Block主存储。

图 268: 添加Shared Block主存储

ZStack支持一个集群挂载多个主存储，目前支持的场景有：

- 一个集群可以挂载一个或多个本地主存储。
- 一个集群可以挂载一个或多个NFS主存储。
- 一个集群可以挂载一个或多个Shared Block主存储。
- 一个集群可以挂载一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个NFS主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Block主存储。
- 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。

- 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
- 一个主存储可以挂载到多个集群 。

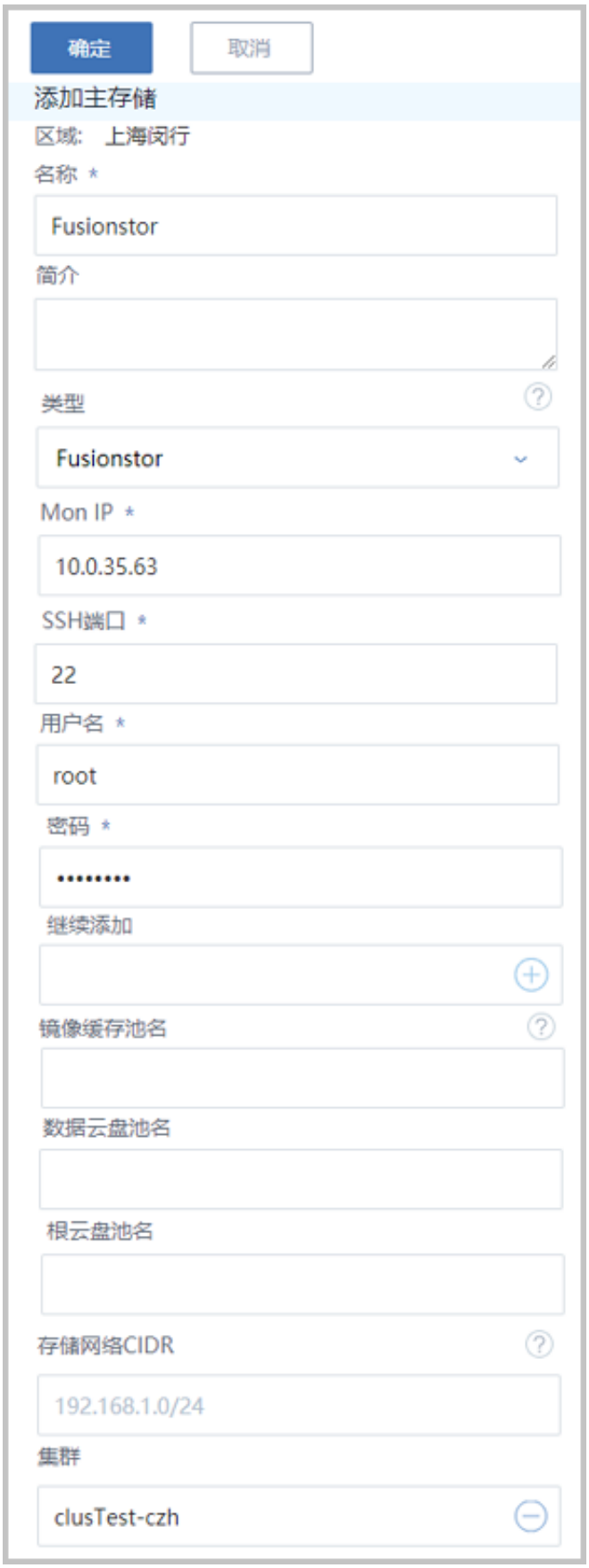
7.3.4.7 主存储类型--FusionStor

背景信息

FusionStor采用了华云网际提供的分布式块存储方式。如果主存储类型需要采用FusionStor，则需要先添加一个FusionStor类型的镜像服务器并且提前配置好FusionStor分布式存储。

添加FusionStor存储具体步骤，与添加Ceph存储步骤类似。如图 *269: FusionStor存储*所示：

图 269: FusionStor存储


确定
取消
添加主存储
区域: 上海闵行
名称 *
Fusionstor
简介
类型
Fusionstor
Mon IP *
10.0.35.63
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
clusTest-czh

操作步骤

1. 输入主存储的**名称**和**简介**（可选项）。
2. 选择主存储的类型为**FusionStor**。
3. 输入FusionStor监控节点的IP地址**Mon IP**。
4. 输入FusionStor监控节点的**SSH端口**，默认为22，如果此节点没有配置SSH端口，则可按照默认配置的22端口使用。
5. 输入FusionStor监控节点的**用户名**，默认为root用户，也可输入普通用户（普通用户要求拥有sudo权限）。如果此FusionStor监控节点没有添加普通用户，则可按照默认的root用户使用。
6. 输入FusionStor监控节点的对应的用户**密码**，输入密码时请注意大小写。
7. 可点击**继续添加**下方的**+**号按钮继续添加其它FusionStor主存储。
8. 输入**镜像缓存池名**、**数据云盘池名**和**根云盘池名**，这三个都是选填项。

   注:

   - 如果用户需要填写，则必须先在FusionStor集群上创建这三个池成功后再进行填写。
   - 如果用户不填写，则系统会自动为用户创建这三个池。
9. 输入**存储心跳网络CIDR**，用于共享存储FusionStor指定存储网络。
10. 选择主存储挂载的**集群**。
11. 点击**确定**按钮，系统会配置FusionStor的块存储作为主存储。

后续操作

一般FusionStor集群也会配置多个监控节点，配置方法与Ceph集群相似，可以参考主存储类型--*Ceph*章节。

7.3.4.8 主存储详情

在**主存储**管理界面，点击相应主存储的名称，可以展开主存储详情页。

主存储操作里所包含的操作是主存储管理界面上所有主存储操作的合集。不同类型主存储的主存储详情页存在差异，但均包括：**基本属性**、**云主机**、**云盘**、**集群**、**监控数据**、**报警**和**审计**。下面将分章节进行说明。

7.3.4.9 主存储详情--本地存储

本地存储类型的主存储详情页包括：基本属性、云主机、云盘、集群、物理机、监控数据、报警和审计。

- **基本属性**

  基本属性栏为主存储详情界面的缺省栏。它显示了当前本地存储的基本情况，例如：类型显示的是LocalStorage，URL显示的是已添加的各物理机的绝对路径信息，还显示了各种容量大小和UUID等。在此栏可以修改本地存储的名称、简介和URL。如图 *270:* 基本属性所示。

  图 270: 基本属性

- **云主机**

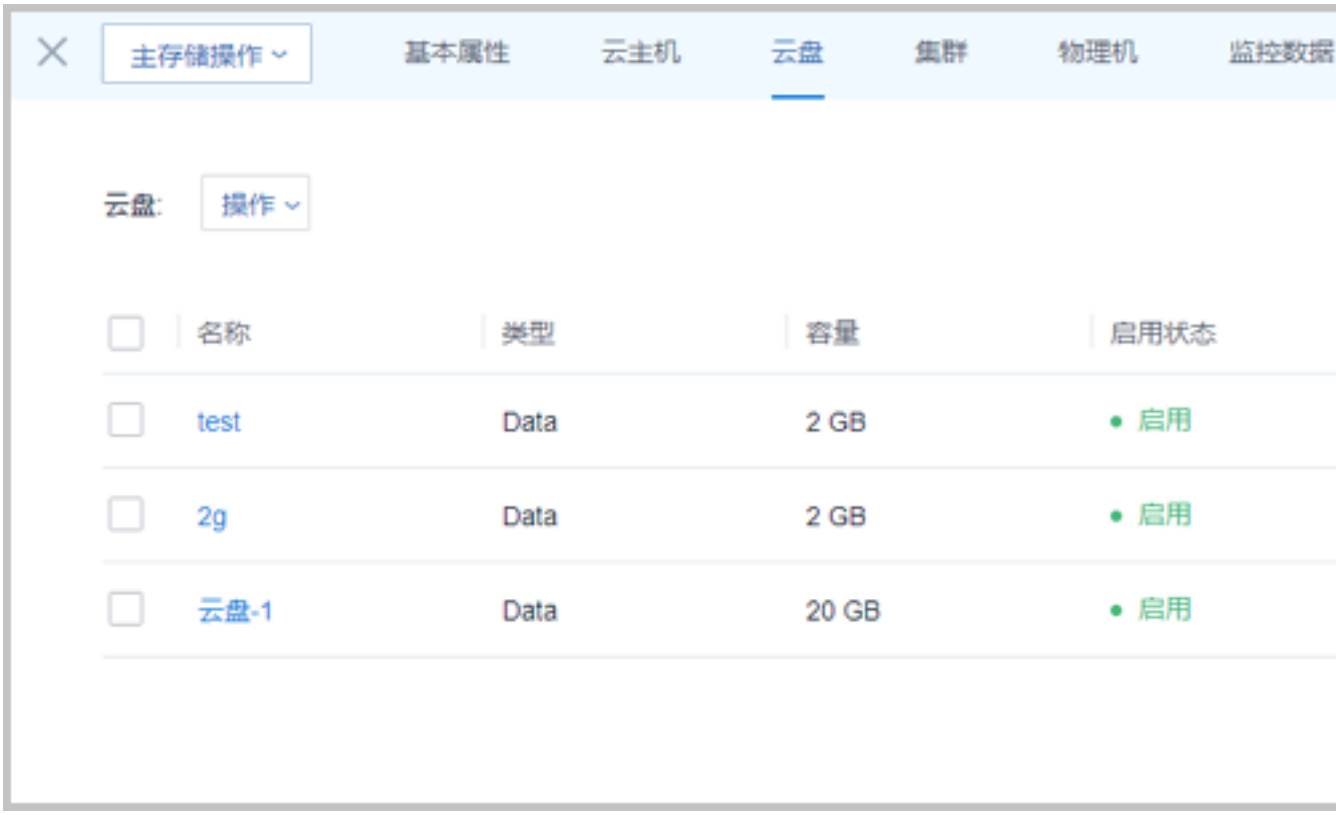
  云主机栏列出了在当前主存储上创建的所有云主机列表，显示了云主机的名称、计算规格、默认IP、所属集群、状态等。在此栏可以点击**操作**按钮来操作云主机，如图 *271:* 云主机所示：

  图 271: 云主机

- **云盘**

  云盘栏显示在当前主存储上创建的所有云盘列表，包括根云盘和数据云盘。显示了云盘的名称、类型、容量、状态和加载情况等等。在此栏可以点击云盘：操作按钮来操作这些云盘，如图 *272:* 云盘所示：

  图 272: 云盘



- **集群**

  集群栏显示的是加载了当前主存储的集群列表。显示了这些集群的名称、虚拟化技术、物理机数量和状态等等。在此栏可以点击集群：操作按钮来操作这些集群，如图 *273:* 集群所示。

  图 273: 集群

- **物理机**

  物理机栏显示的是提供当前主存储的物理机的列表。显示了这些物理机的名称、URL、容量和状态等信息。如果物理机失联，在此栏可以点击物理机：操作按钮来重连这些物理机，如图 *274: 物理机*所示。

图 274: 物理机

- **监控数据**

  监控数据页面显示了对主存储已用容量百分比的实时性能监控，如图 *275: 监控数据*所示：

图 275: 监控数据

- **报警**

  支持主存储报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加主存储相关的多项报警条目，以邮件/钉钉/HTTP 应用方式发送报警信息。

- **审计**

  审计栏显示了当前主存储的操作日志。如操作日志所示。

  图 276: 操作日志

7.3.4.10 主存储详情--NFS

NFS类型的主存储详情页包括：基本属性、云主机、云盘、集群、监控数据、报警和审计。

- **基本属性**

  基本属性栏为主存储详情界面的缺省栏。它显示了当前NFS存储的基本信息。例如，类型是NFS，URL是已添加的NFS服务器的共享目录，当前主存储的各种容量、存储心跳网络CIDR和UUID等。在此栏可以修改NFS存储的名称、简介、URL和存储心跳网络CIDR。如图 277: 基本属性所示：

  图 277: 基本属性

注:

如需将旧的NFS主存储上运行的云主机迁移至新的NFS主存储上，此时在UI界面更改NFS的URL就很方便。具体操作如下：

1. 关闭需要迁移的云主机。
2. 在第一个计算节点，挂载新的NFS存储到*/mnt/new-nfs/*目录。例如：

```
[root@localhost ~]#mount -t nfs 172.20.12.28:/share/new-ps /mnt/new-nfs/
```

3. 通过*rsync*命令同步数据。例如：

```
[root@localhost ~]#rsync -avu /opt/zstack/nfsprimarystorage/prim-45d5405
2761e4dacaa336415d9bfda8b/* /mnt/new-nfs/
```

4. 数据同步完成后，执行卸载新的NFS。例如：

```
[root@localhost ~]#umount /mnt/new-nfs
```

5. 在基本属性栏上，将原来的NFS的URL修改为新NFS的URL。例如：*172.20.12.28:/share/new-ps*

- **云主机**

云主机栏列出了在当前主存储上创建的所有云主机列表，显示了云主机的名称、计算规格、默认IP、所属集群、状态等。在此栏可以点击**操作**按钮来操作云主机。请参考本地存储详情界面的云主机栏。

- **云盘**

  云盘栏显示在当前主存储上创建的所有云盘列表，包括根云盘和数据云盘。请参考本地存储详情界面的云盘栏。

- **集群**

  集群栏显示的是加载了当前主存储的集群列表。请参考本地存储详情界面的集群栏。

- **监控数据**

  监控数据页面显示了对主存储已用容量百分比的实时性能监控。请参考本地存储详情界面的监控数据栏。

- **报警**

  支持主存储报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加主存储相关的多项报警条目，以邮件/钉钉/HTTP 应用方式发送报警信息。

- **审计**

  审计栏显示了当前主存储的操作日志。请参考本地存储详情界面的操作日志栏。

7.3.4.11 主存储详情--Shared Mount Point

Shared Mount Point类型的主存储详情页包括：基本属性、云主机、云盘、集群、监控数据、报警和审计。

- **基本属性**

  基本属性为主存储详情界面的缺省栏。它显示了当前Shared Mount Point存储的基本信息，例如，类型是Shared Mount Point，当前存储的各种容量、存储心跳网络CIDR和UUID等。在此栏可以修改Shared Mount Point存储的名称、简介、URL和存储心跳网络CIDR。如图 *278:* 基本属性所示：

  图 278: 基本属性

- **云主机**

  云主机栏列出了在当前主存储上创建的所有云主机列表，显示了云主机的名称、计算规格、默认IP、所属集群、状态等。在此栏可以点击**操作**按钮来操作云主机。请参考本地存储详情界面的云主机栏。

- **云盘**

  云盘栏显示在当前主存储上创建的所有云盘列表，包括根云盘和数据云盘。请参考本地存储详情界面的云盘栏。

- **集群**

  集群栏显示的是加载了当前主存储的集群列表。请参考本地存储详情界面的集群栏。

- **监控数据**

  监控数据页面显示了对主存储已用容量百分比的实时性能监控。请参考本地存储详情界面的监控数据栏。

- **报警**

  支持主存储报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加主存储相关的多项报警条目，以邮件/钉钉/HTTP 应用方式发送报警信息。

- **审计**

审计栏显示了当前主存储的操作日志。请参考本地存储详情界面的操作日志栏。

7.3.4.12 主存储详情--Ceph

Ceph类型的主存储详情页包括：基本属性、监控节点、云主机、云盘、集群、存储池、监控数据、报警和审计。

- **基本属性**：

  基本属性为主存储详情界面的缺省栏。它显示了当前Ceph存储的基本信息，例如：类型是Ceph、当前主存储的各种容量、存储心跳网络CIDR、CephX开关、池名和UUID等。在此页面可修改Ceph主存储的名称、简介、存储心跳网络CIDR、CephX开关状态。如图 *279:* 基本属性所示。

  图 279: 基本属性

- **监控节点**：

监控节点栏显示了当前Ceph存储的所有监控节点的基本信息。包含：Mon IP、节点管理IP、SSH用户名 、SSH用户端口、Mon端口和链接状态等。在此栏可以点击监控节点后边的**操作**按钮来操作监控节点，如图 *280:* 监控节点所示：

图 280: 监控节点

- **云主机**：

  云主机栏列出了在当前主存储上创建的所有云主机列表，显示了云主机的名称、计算规格、默认IP、所属集群、状态等。在此栏可以点击**操作**按钮来操作云主机。请参考本地存储详情界面的云主机栏。

- **云盘**：

  云盘栏显示在当前主存储上创建的所有云盘列表，包括根云盘和数据云盘。请参考本地存储详情界面的云盘栏。

- **集群**：

  集群栏显示的是加载了当前主存储的集群列表。请参考本地存储详情界面的集群栏。

- **存储池**：

  存储池栏显示Ceph主存储中每个存储池的显示名、池名称、池已用容量、池可用容量、池副本数、类型和创建日期等信息。

  点击**存储池**后面的**操作**按钮可对存储池进行相关操作，包括：添加数据云盘池、设置显示名、删除数据云盘池。如图 *281:* 存储池所示：

图 281: 存储池

注:

- 存储池，是一个Ceph存储的逻辑分区概念。添加Ceph存储到云平台时，如果没有指定存储池，系统会自动创建出相应的存储池：
  - 主存储：镜像缓存池，云主机根云盘池，云主机数据云盘池
  - 镜像服务器：镜像服务器存储池
- 用户也可以创建自己的新存储池（针对数据云盘指定的特定存储池）。新存储池创建完成后，可在**云盘**子页面创建出该存储池的云盘并加载到云主机中。
- 支持自定义设置存储池的显示名。
- 用户可直观查看各存储池当前的已用容量、可用容量、副本数以及存储池类型。

- **监控数据**

  监控数据页面显示了对主存储已用容量百分比的实时性能监控。请参考本地存储详情界面的监控数据栏。

- **报警**：

  ZStack支持主存储报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加主存储相关的多项报警条目，以邮件/钉钉/HTTP应用方式发送报警信息。

- **审计**：

  审计栏显示了当前主存储的操作日志。请参考本地存储详情界面的操作日志栏。

7.3.4.13 主存储详情--Shared Block

Shared Block类型的主存储详情页包括：基本属性、云主机、云盘、集群、共享块、监控数据、报警和审计。

- **基本属性**

  基本属性为主存储详情界面的缺省栏。它显示了Shared Block存储的基本信息，例如：类型、主存储的各种容量、所属区域和UUID等。在此栏可以修改Shared Block存储的名称、简介。如图 *282:* 基本属性所示：

  图 282: 基本属性

- **云主机**：

  云主机栏列出了在当前主存储上创建的所有云主机列表，显示了云主机的名称、计算规格、默认IP、所属集群、状态等。在此栏可以点击**操作**按钮来操作云主机。请参考本地存储详情界面的云主机栏。

- **云盘**：

  云盘栏显示在当前主存储上创建的所有云盘列表，包括根云盘和数据云盘。请参考本地存储详情界面的云盘栏。

- **集群**：

  集群栏显示的是加载了当前主存储的集群列表。请参考本地存储详情界面的集群栏。

- **共享块**：

共享块页面显示了共享块名称、磁盘和状态等信息。可以点击**操作**按钮继续添加共享块设备。如图 *283: 共享块*所示：

图 283: 共享块

- **监控数据**：

  监控数据页面显示了对主存储已用容量百分比的实时性能监控。请参考本地存储详情界面的监控数据栏。

- **报警**：

  支持主存储报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加主存储相关的多项报警条目，以邮件/钉钉/HTTP 应用方式发送报警信息。

- **审计**：

  审计栏显示了当前主存储的操作日志。请参考本地存储详情界面的操作日志栏。

7.3.4.14 主存储详情--FusionStor

FusionStor类型的主存储详情页包括：**基本属性**、**监控节点**、**云主机**、**云盘**、**集群**和**审计**。

- **基本属性**

  基本属性为主存储详情界面的缺省栏。它显示了当前FusionStor存储的基本信息，例如：类型是FusionStor，当前存储的各种容量、存储心跳网络CIDR和UUID等等。在此栏可以修改FusionStor存储的名称、简介和存储心跳网络CIDR。

- **监控节点**

  监控节点栏显示了当前FusionStor存储的所有监控节点的基本信息。请参考Ceph存储详情界面的监控节点栏。

- **云主机**

  云主机栏列出了在当前主存储上创建的所有云主机列表，显示了云主机的名称、计算规格、默认IP、所属集群、状态等。在此栏可以点击**操作**按钮来操作云主机。请参考本地存储详情界面的云主机栏。

- **云盘**

  云盘栏显示在当前主存储上创建的所有云盘列表，包括根云盘和数据云盘。请参考本地存储详情界面的云盘栏。

- **集群**

  集群栏显示的是加载了当前主存储的集群列表。请参考本地存储详情界面的集群栏。

- **审计**

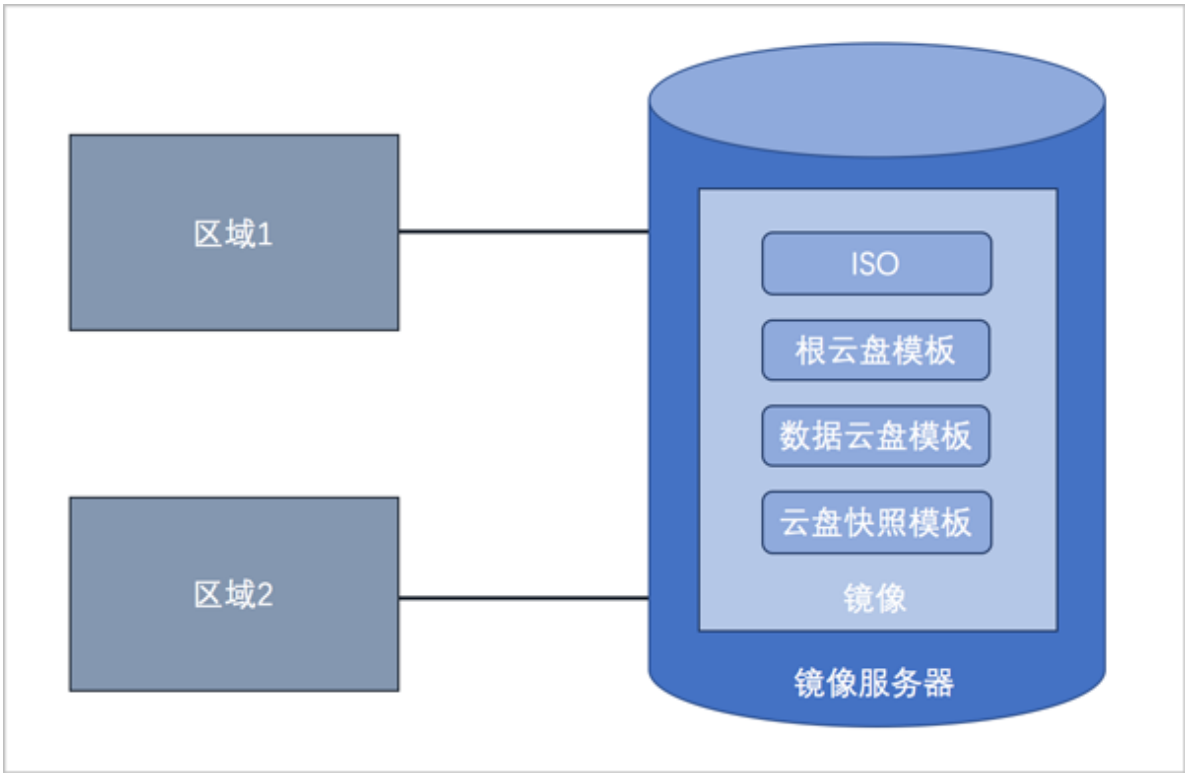
  审计栏显示了当前主存储的操作日志。请参考本地存储详情界面的操作日志栏。

7.3.5 镜像服务器

镜像服务器：用于保存镜像模板的存储服务器。

- 镜像服务器必须挂载到区域之后，区域中的资源才能访问它。通过镜像服务器，可在多个区域之间共享镜像。
- 如图 *284:* 镜像服务器所示：

  图 284: 镜像服务器



注:

UI界面为便于管理镜像服务器和区域的关系，特别设置了一个镜像服务器只能对应一个区域。UI界面上，添加镜像服务器，默认会挂载到当前区域；删除区域的同时会直接删除挂载此区域的镜像服务器。

镜像服务器的类型

镜像服务器支持以下类型：

1. **ImageStore（镜像仓库）**：
   - 以镜像切片方式存储镜像文件，支持增量存储；
   - 支持云主机的在线/关机快照、在线/关机创建镜像；
   - 不带数据云盘克隆云主机时，支持在线/暂停/关机克隆；
   - 整机克隆时，LocalStorage、NFS、SMP和Ceph类型的主存储，支持在线/暂停/关机克隆；Shared Block类型的主存储，支持暂停/关机克隆；
   - ImageStore类型的镜像服务器间支持镜像同步。
2. **Sftp**：
   - 仅社区版本支持；

- 以文件方式存储镜像文件；
- 支持云主机的关机快照、关机创建镜像。
- 创建的镜像可以在镜像服务器上，以对应的镜像路径访问，拷贝到其他云环境可直接使用。

3. **Ceph镜像服务器**：

- 以Ceph分布式块存储方式存储镜像文件；
- 支持云主机的在线/关机快照、在线/关机创建镜像；
- 支持不带数据云盘在线/暂停/关机克隆；不支持整机克隆。
- 导出镜像需在镜像服务器上导出。

  假定使用的镜像路径为：*ceph://bak-t-c9923f9821bf45498fdf9cdfa1749943/61ece0adc7244b0cbd12dafbc5494f0c*

  则需镜像服务器执行：

```
rbd export -p bak-t-c9923f9821bf45498fdf9cdfa1749943 --image 61ece0adc7244b
0cbd12dafbc5494f0c /root/export-test.image

# bak-t-c9923f9821bf45498fdf9cdfa1749943表示镜像所在的pool的名字
# 61ece0adc7244b0cbd12dafbc5494f0c表示镜像的名字
# /root/export-test.image表示导出的目标文件名字
```

4. **FusionStor镜像服务器**：

- 以FusionStor分布式块存储方式存储镜像文件；
- 支持云主机的在线/关机快照、关机创建镜像，不支持在线创建镜像和在线/关机克隆。
- 导出镜像需要在镜像服务器上执行类似命令：

```
lichbd export bak-t-8e694c40cf214db1af9e5d641b2e792d/8f1e0debfae042e5ae074
133a59c0622 /root/test.img -p nbd
```

注:

企业版和混合云版支持ImageStore、Ceph和FusionStor类型，社区版支持Sftp、Ceph和FusionStor类型。

镜像服务器 | 主存储

镜像服务器的类型与主存储的类型有关联性要求，如主存储与镜像服务器关系所示：

表 4: 主存储与镜像服务器的关系

PS\BS	ImageStore	Sftp	Ceph	FusionStor

LocalStorage	○	○	×	×
NFS	○	○	×	×
Shared Mount Point	○	○	×	×
Ceph	○	×	○	×
Shared Block	○	×	×	×
FusionStor	×	×	×	○

- 当主存储为本地存储（LocalStorage）、NFS、Share Mount Point或Shared Block类型时，镜像服务器的默认类型为ImageStore（企业版）或Sftp（社区版）。
- 当主存储为NFS或Shared Mount Point类型时，可将相应共享目录手动挂载到相应镜像服务器的本地目录上，从而使主存储和镜像服务器均能使用网络共享存储方式。
- 当主存储为Ceph类型时，镜像服务器可以使用同一个Ceph集群作为镜像服务器，也可以使用镜像仓库类型的镜像服务器。Ceph集群提供分布式块存储方式存储镜像文件。
- 当主存储为FusionStor类型时，镜像服务器必须使用同一个FusionStor集群作为镜像服务器。FusionStor集群提供分布式块存储方式存储镜像文件。

7.3.5.1 镜像服务器操作

在ZStack私有云主菜单，点击**硬件设施** > **镜像服务器**按钮，进入**镜像服务器**管理界面，如图 *285:* 镜像服务器所示。在**镜像服务器**管理界面，可以查看当前区域内加载的所有镜像服务器列表及其信息，包括：镜像服务器名称、类型、URL、容量和状态等，并可以对镜像服务器进行添加、启用、停用、重连和删除等操作，如图 *285:* 镜像服务器所示:

图 285: 镜像服务器

系统对镜像服务器操作的定义如下：

- **搜索**：在镜像服务器管理界面上支持三种搜索方式：名称、UUID和高级搜索。

- **添加镜像服务器**：即添加一个新的镜像服务器到系统中。在镜像服务器管理界面点击**添加镜像服务器**按钮后，打开**添加镜像服务器**界面，用户按照要求填写必要的信息后，点击**确定**按钮后，此过程可能需要等待几分钟。

  镜像服务器的类型有四种，添加镜像服务器的界面稍有差异：

  - **ImageStore**：是正式版支持的类型。类型选择**ImageStore**，输入名称、主机IP、URL、SSH端、用户名和密码等必填信息，点击**确定**即可创建，如图 *286: ImageStore*类型所示。
  - **Sftp**：是开源版支持的类型。类型选择**Sftp**，其他信息的填写和ImageStore存储相似。
  - **Ceph存储**：类型选择**Ceph**，其他信息的填写和ImageStore存储相似，当然用户也可以指定Ceph的池名称，如图 *287: Ceph*类型所示。
  - **FusionStor存储**：类型选择**FusionStor**，其他信息的填写和Ceph存储相似。

  图 286: ImageStore类型

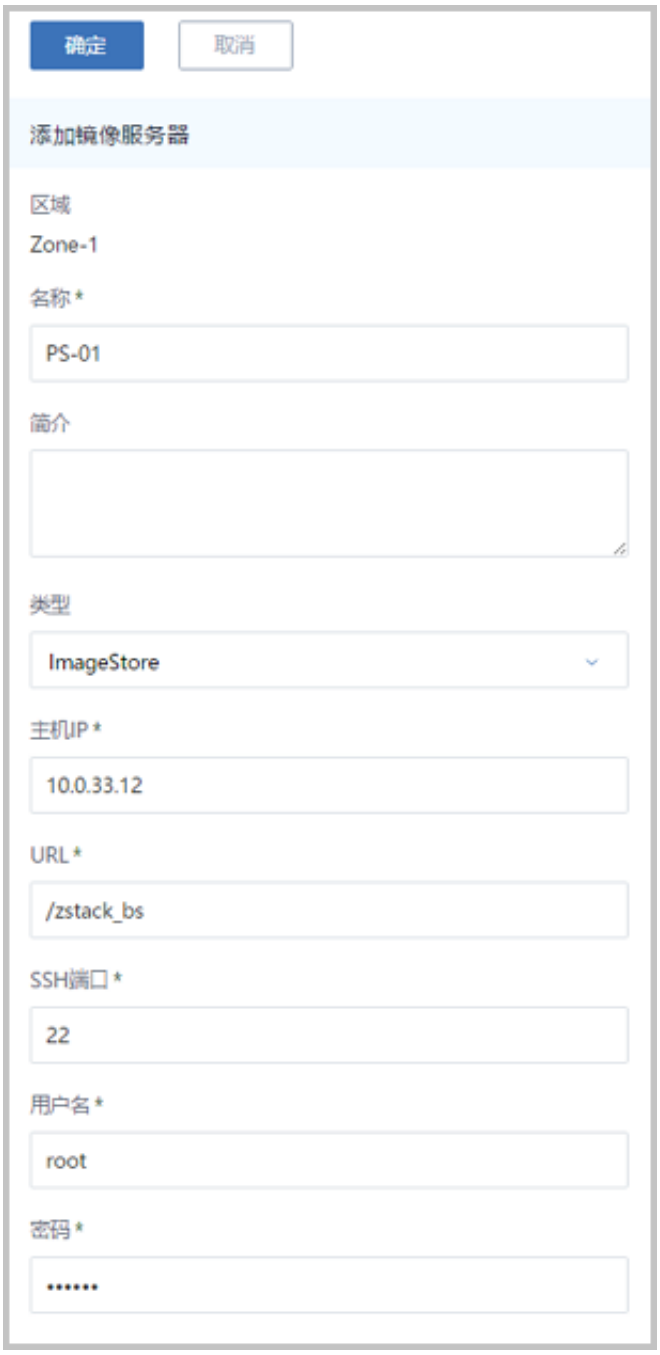
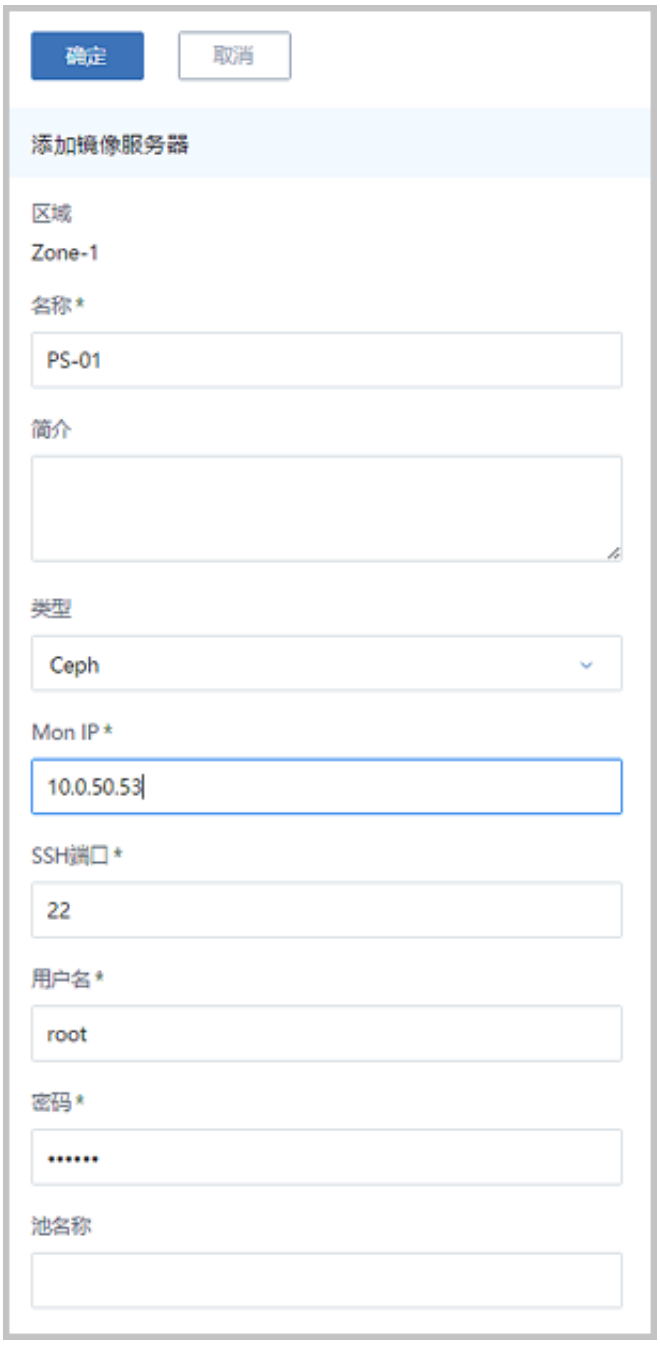

确定
取消
添加镜像服务器
区域
Zone-1
名称 *
PS-01
简介
类型
ImageStore
主机IP *
10.0.33.12
URL *
/zstack_bs
SSH端口 *
22
用户名 *
root
密码 *
••••••

图 287: Ceph类型



- **启用**：启用选中的镜像服务器。**支持批量操作。**
- **停用**：停止使用选中的镜像服务器。**支持批量操作。**
- **重连**：重新连接选中的镜像服务器，重连镜像服务器会更新镜像服务器上相关的存储信息。**支持批量操作。**
- **删除**：删除选中的镜像服务器。**支持批量操作。**

注:

- 删除镜像服务器会删除此镜像服务器中的所有镜像文件，且无法恢复，需谨慎操作。

- 这里的删除，只是移除镜像服务器和镜像在ZStack中的记录，并不删除真实的数据。

7.3.5.2 镜像服务器详情

在**镜像服务器**管理界面，点击相应镜像服务器的名字，可以展开镜像服务器详情页。不同类型的镜像服务器的详情页稍有差异，下边会详细介绍。不同类型的镜像服务器都有一个**镜像服务器操作**按钮可以对当前的镜像服务器进行操作，它里面的操作菜单是镜像服务器管理界面上所有区域操作的合集。点击左上角**X**按钮可以关闭镜像服务器详情界面。

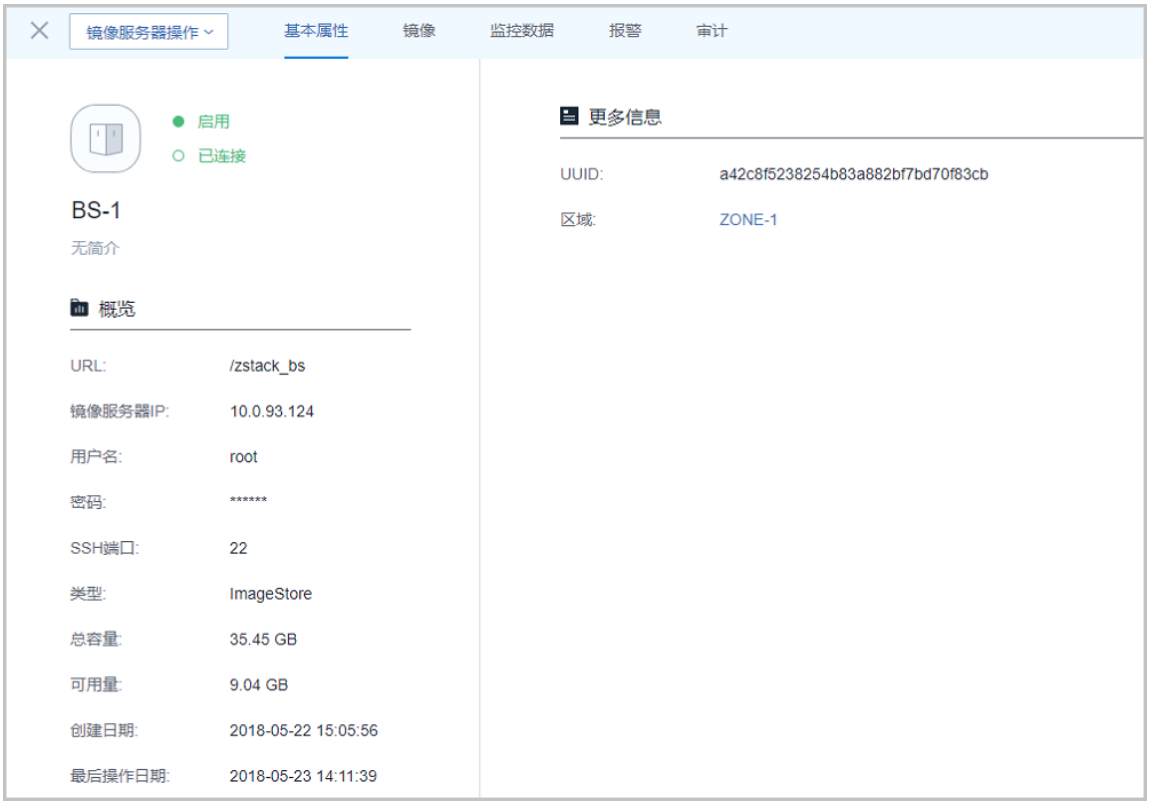
不同类型的镜像服务器的详情页简述：

- ImageStore 和Sftp相似，包含：基本属性、镜像、监控数据、报警和审计。
  - **基本属性**

    基本属性栏为镜像服务器详情界面的缺省栏。它显示了当前镜像服务器的基本信息，例如，类型、主机IP、容量和UUID等。在此栏可以修改镜像服务器的名称、简介、主机IP、SSH端口、用户名和密码，如图 *288: 基本属性--ImageStore*所示。

    - ImageStore ：类型显示为ImageStore；
    - Sftp：类型显示为Sftp。

    图 288: 基本属性--ImageStore



- **镜像**

镜像栏显示了当前镜像服务器上所加载的镜像，分为云主机镜像和云路由镜像两个子栏进行显示。显示镜像的基本信息：镜像名称、所在镜像服务器、镜像类型、镜像格式、镜像状态、平台类型、容量等，可以点击镜像后边的**操作**按钮来操作这些镜像，如图 *289: 镜像*所示。

图 289: 镜像

- **监控数据**

监控数据页面显示了对镜像服务器已用容量百分比的实时性能监控，如图 *290: 监控数据*所示：

图 290: 监控数据

- **报警**

ZStack支持镜像服务器报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加镜像服务器可用容量、可用容量百分比等多项报警条目，以邮件/钉钉/HTTP应用方式发送报警信息。

使用方法与云主机报警类似，具体可参考云主机报警章节。

- **审计**

审计栏显示了当前镜像服务器的操作日志。如操作日志所示。

图 291: 操作日志

- Ceph和FusionStor相似，包含：基本属性、监控节点、镜像、监控数据、报警和审计。

  - **基本属性**

  基本属性栏为镜像服务器详情界面的缺省栏。它显示了当前镜像服务器的基本信息，例如类型、容量和UUID等。在此栏可以修改镜像服务器的名称和简介、以及存储心跳网络CIDR，如图 *292: 基本属性--Ceph*所示。

  - Ceph：类型显示为Ceph；
  - FusionStor：类型显示为FusionStor；

  图 292: 基本属性--Ceph

- **监控节点**

监控节点栏显示了当前分布式存储的所有监控节点的基本信息。包含：Mon IP、节点管理IP、SSH用户名、SSH用户端口、Mon端口、链接状态和创建日期等。在此栏可以点击监控节点后的**操作**按钮来操作此这些监控节点，如图 *293:* 监控节点所示。

图 293: 监控节点

- **镜像**

镜像栏显示的是加载了当前镜像服务器的镜像列表。包括云主机镜像和云路由镜像。如图 *294:* 镜像所示：

图 294: 镜像

- **监控数据**

  监控数据页面显示了对镜像服务器已用容量百分比的实时性能监控，如图 *295:* 监控数据所示：

  图 295: 监控数据

- **报警**

  ZStack支持镜像服务器报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加镜像服务器可用容量、可用容量百分比等多项报警条目，以邮件/钉钉/HTTP 应用方式发送报警信息。

- **审计**

  审计栏显示了当前镜像服务器的日志。

7.4 网络资源

ZStack网络资源主要涉及以下内容：

- 网络拓扑

- 二层网络资源
- 三层网络
- 路由资源
- VPC

网络拓扑

不仅支持云平台全局网络拓扑的直观展示，助力分析网络问题，而且支持用户自定义生成拓扑，快速定位资源状态。

二层网络资源

二层网络资源包括VXLAN Pool和二层网络。

- 二层网络对应于一个二层广播域，支持L2NoVlanNetwork、L2VlanNetwork、VxlanNetwork类型。
- L2NoVlanNetwork和L2VlanNetwork作为一组，与计算节点的端口在交换机端的设置应相同。
- VXLAN Pool和VxlanNetwork共同提供了VxlanNetwork类型的配置，在使用VxlanNetwork前，需要先建立VXLAN Pool。创建完毕VXLAN Pool后，可指定或随机选择Vni来创建VxlanNetwork。

三层网络

三层网络作为二层网络的子资源，主要基于二层网络提供给云主机的网络配置，包括IP地址范围，网关，DNS，网络服务。

路由资源

ZStack使用定制的Linux云主机作为路由设备提供云主机网络服务。相关路由资源主要包括：云路由器、云路由镜像、云路由规格、路由表。

VPC

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具有灵活的网络配置、安全可靠的隔离、东西向网络流向优化等特点。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。

ZStack网络使用流程

先创建二层网络，再创建三层网络，最后使用这些网络提供的各种网络服务。

ZStack网络架构模型

ZStack支持三种基本网络架构模型：扁平网络、云路由网络、VPC

1. **扁平网络**

   - 扁平网络支持以下网络服务：DHCP、弹性IP、安全组、User Data等；
   - 扁平网络的网络服务采用分布式的DHCP、分布式的EIP结构；
   - 扁平网络的DHCP服务也包含了DNS的功能；
   - 初始化引导设置使用的网络模型就是采用了扁平网络。
   - 支持基于VXLAN的扁平网络架构。

2. **云路由网络**

   - 云路由网络支持以下网络服务：DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等；
   - 云路由网络的DHCP服务默认采用分布式的DHCP；
   - 云路由网络主要使用定制的Linux云主机作为路由设备提供网络服务。
   - 支持基于VXLAN的云路由网络架构。

3. **VPC**

   - VPC支持以下网络服务：DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等；
   - VPC的DHCP服务默认采用分布式的DHCP；
   - VPC主要使用定制的Linux云主机作为VPC路由器提供网络服务。
   - 网络服务（端口转发、负载均衡、IPsec隧道、路由表等）可以同时作用在一个VPC的多个子网上，进一步提升网络效率。
   - 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。

关于网络服务的详细介绍请参考网络服务章节。

7.4.1 网络拓扑

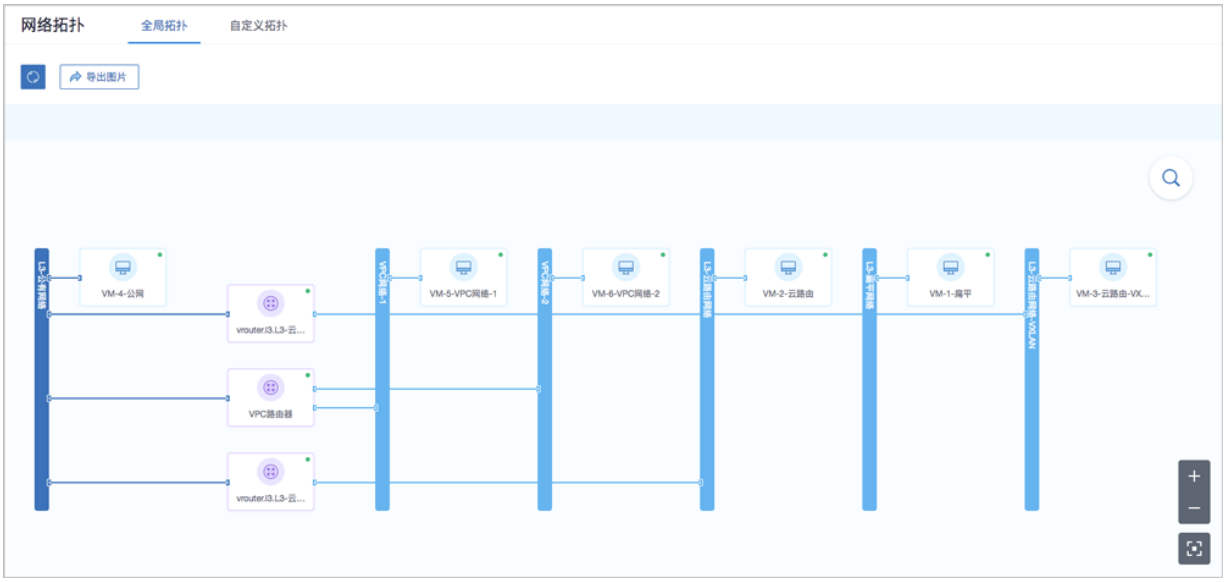
ZStack 支持网络拓扑功能。不仅支持云平台的全局拓扑，还支持针对自定义资源生成拓扑图，快速定位资源状态。

7.4.1.1 全局拓扑

全局拓扑界面

在ZStack私有云主菜单，点击**网络资源** > **网络拓扑**，直接进入**全局拓扑**界面，如图 *296:* 全局拓扑所示：

图 296: 全局拓扑



全局拓扑支持的操作

全局拓扑支持以下操作：

- 查看：支持对整个云平台网络拓扑的直观查看。
- 刷新：点击界面左上方刷新按钮，可显示当前最新全局拓扑。
- 导出图片：点击界面左上方导出图片按钮，支持当前全局拓扑以**png**格式图片导出。
- 搜索：点击界面右上方搜索按钮，弹出搜索框，支持按资源类别以及资源属性进行搜索。
  - 资源类别目前支持：云主机、路由器（云路由器/VPC路由器）、私有网络、公有网络。
  - 资源属性目前支持：资源名称、资源UUID、IP地址、弹性IP。
- 放大/缩小：点击界面右下方放大/缩小按钮，可将网络拓扑进行放大/缩小查看。
- 还原：点击界面右下方还原按钮，可将放大/缩小的网络拓扑还原至默认尺寸查看。
- 选中资源高亮显示：当选中某一资源，可对该资源及其关联资源进行高亮突出。
- 资源信息悬浮显示：当鼠标悬浮至某一资源上，该资源相关信息将自动浮现。
- 打开控制台：当鼠标悬浮至某一资源上，该资源相关信息自动浮现，点击右上角控制台按钮，可进入控制台。

- 路由器/云主机状态显示：通过路由器/云主机右上角圆点的颜色变化可实时掌握其运行状态，详情请参考表 5: 路由器/云主机状态显示定义。

表 5: 路由器/云主机状态显示定义

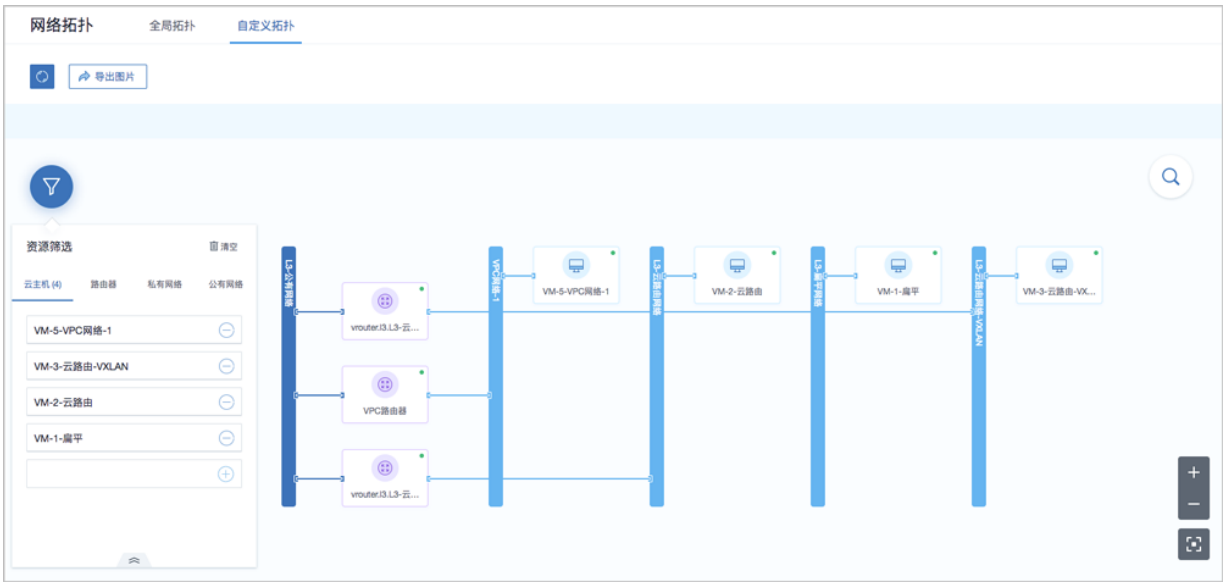
路由器/云主机状态	右上角圆点颜色
启动中	蓝色
运行中	绿色
停止中	蓝色
已停止	红色
重启中	蓝色
删除中	蓝色
已删除	灰色
迁移中	蓝色
彻底删除中	蓝色
暂停中	蓝色
已暂停	灰色
恢复中	蓝色
未知	黄色

7.4.1.2 自定义拓扑

自定义拓扑界面

在ZStack私有云主菜单，点击**网络资源** > **网络拓扑** > **自定义拓扑**，进入**自定义拓扑**界面，如图 297: 自定义拓扑所示：

图 297: 自定义拓扑



自定义拓扑支持的操作

自定义拓扑支持以下操作：

- 指定资源生成拓扑并查看：通过指定资源【目前包括：云主机、路由器（云路由器/VPC路由器）、私有网络、公有网络】，生成相应的拓扑，并直观查看。
- 刷新：点击界面左上方刷新按钮，可显示当前最新拓扑。
- 导出图片：点击界面左上方导出图片按钮，支持当前拓扑以**png**格式图片导出。
- 搜索：点击界面右上方搜索按钮，弹出搜索框，支持按资源类别以及资源属性进行搜索。
  - 需提前生成自定义拓扑，该搜索操作针对当前自定义拓扑上的资源进行搜索。
  - 资源类别目前支持：云主机、路由器（云路由器/VPC路由器）、私有网络、公有网络。
  - 资源属性目前支持：资源名称、资源UUID、IP地址、弹性IP。
- 放大/缩小：点击界面右下方放大/缩小按钮，可将当前拓扑进行放大/缩小查看。
- 还原：点击界面右下方还原按钮，可将放大/缩小的拓扑还原至默认尺寸查看。
- 选中资源高亮显示：当选中某一资源，可对该资源及其关联资源进行高亮突出。
- 资源信息悬浮显示：当鼠标悬浮至某一资源上，该资源相关信息将自动浮现。
- 打开控制台：当鼠标悬浮至某一资源上，该资源相关信息自动浮现，点击右上角控制台按钮，可进入控制台。
- 路由器/云主机状态显示：通过路由器/云主机右上角圆点的颜色变化可实时掌握其运行状态，详情请参考表 *5:* 路由器/云主机状态显示定义。

7.4.2 二层网络资源

二层网络资源包括VXLAN Pool和二层网络。

7.4.2.1 VXLAN Pool

VXLAN Pool表示使用UDP进行报文封装的VXLAN类型的集合，是基于IP网络组建的大二层网络，可满足大规模云计算中心的需求，最大支持16M个逻辑子网。

- VXLAN Pool和VxlanNetwork共同提供了VxlanNetwork类型的配置，使用VxlanNetwork需先创建VXLAN Pool，VxlanNetwork对应了VXLAN Pool里的一个虚拟网络。
- VXLAN Pool最大可支持16777216（16M）个虚拟网络。其Vni（VXLAN网络ID）范围可从1-16777216设置。
- 在创建VXLAN Pool时，如果需要加载到相应集群，则需设置相应的VTEP（VXLAN隧道端点）。
- VTEP一般对应于集群内计算节点中的某一网卡的IP地址，ZStack对VTEP的设置基于相应的CIDR进行配置，例如：
  - 假定计算节点某网卡的IP为*10.12.0.8*，子网掩码为*255.0.0.0*，网关为*10.0.0.1*，则VTEP输入的CIDR应为*10.0.0.1/8*；
  - 假定计算节点某网卡的IP为*172.20.12.13*，子网掩码为*255.255.0.0*，网关为*172.20.0.1*，则VTEP输入的CIDR应为*172.20.0.1/16*。
- VXLAN Pool与集群进行挂载时，检查的是VTEP相关的IP地址，与物理的二层设备无关。

创建VXLAN Pool

在ZStack私有云主菜单，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，可参考以下示例输入相应内容：

- **名称**：设置VXLAN Pool名称
- **简介**：可选项，可留空不填
- **起始Vni**：VxlanNetwork的起始ID，可输入1-16777214之间的数字
- **结束Vni**：VxlanNetwork的结束ID，可输入1-16777214之间的数字，需大于或等于起始Vni

  注: ZStack将最后两个Vni（即：16777215、16777216）作为系统保留。

- **集群**：可选项，选择需要加载的集群

注:

- 可在创建VXLAN Pool时加载集群，也可在创建VXLAN Pool后再加载集群；
- 加载集群时，集群内计算节点上应该存在VTEP对应的子网内IP。

- **VTEP CIDR**：输入VTEP对应的CIDR

如图 *298: 创建VXLAN Pool*所示：

图 298: 创建VXLAN Pool

VXLAN Pool支持的操作

VXLAN Pool支持以下操作：

- 修改名称：修改VXLAN Pool的名称。
- 修改简介：修改VXLAN Pool的简介。
- 加载集群：加载VXLAN Pool到集群，需指定VTEP对应的CIDR，请确保此CIDR在集群内各物理机均存在对应的IP，否则加载会失败。
- 卸载集群：从集群卸载VXLAN Pool。
- 删除：删除VXLAN Pool，其对应的子资源VxlanNetwork将被删除，相关的三层网络和云主机的网卡也将被删除。
- 共享：将此VXLAN Pool共享给指定的普通账户使用。
- 召回：将此VXLAN Pool从普通账户召回，使其不可见。
- 全局共享：将此VXLAN Pool共享给全部普通账户使用。
- 全局召回：将此VXLAN Pool从全部普通账户召回，使其不可见。
- 创建Vni范围：创建一个Vni范围给VXLAN Pool。
- 删除Vni范围：从VXLAN Pool中删除一个Vni范围。
- 创建VXLAN网络：基于VXLAN Pool创建VxlanNetwork，每个VxlanNetwork对应了VXLAN Pool中的一个Vni。
- 删除VXLAN网络：删除VxlanNetwork，其对应的子资源三层网络将被删除，使用此三层网络的云主机的网卡也将被删除。
- 审计：查看VXLAN Pool的相关操作。

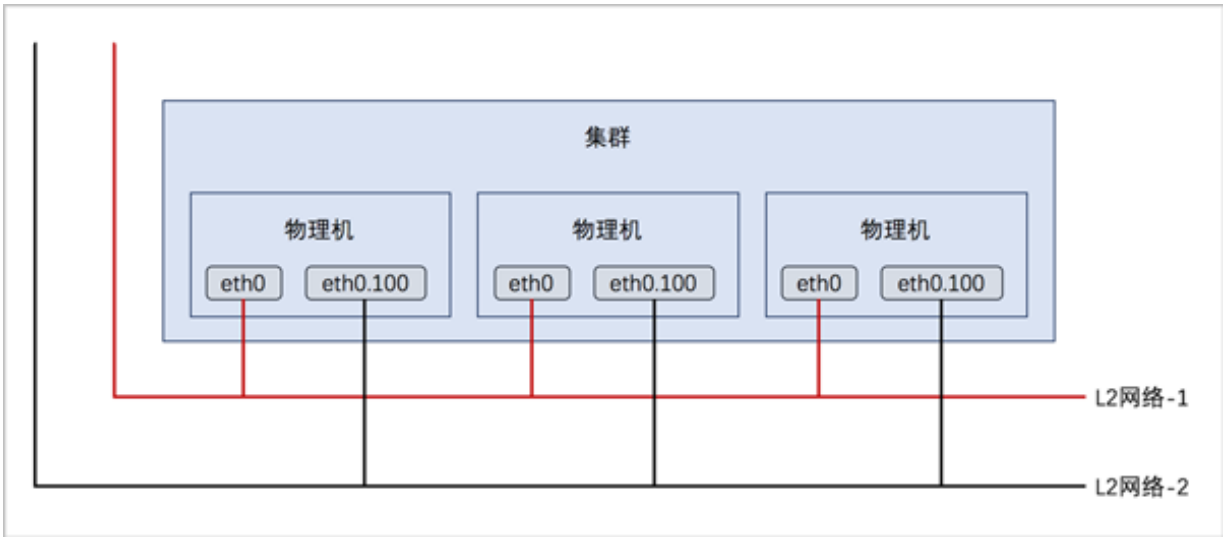
7.4.2.2 二层网络

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。

- VLAN、VXLAN、或者SDN等能提供二层隔离技术都可作为二层网络。
- 二层网络负责为三层网络提供二层隔离。

如图 *299:* 二层网络所示：

图 299: 二层网络



二层网络主要支持的三种类型

二层网络主要支持以下三种类型：

1. **L2NoVlanNetwork**

   NoVlanNetwork类型表示相关的物理机对应的网络设备不设置VLAN

   - 如果交换机端口设置了VLAN，则需在交换机端配置Access模式
   - 如果交换机端口没有设置VLAN, 则无须特别设置

2. **L2VlanNetwork**

   VlanNetwork类型表示相关的物理机对应的网络设备需设置VLAN

   - 从逻辑上划分虚拟局域网，支持1- 4094个子网
   - 此类型需在物理机接入的交换机端进行Trunk设置

3. **VxlanNetwork**

   VxlanNetwork类型表示使用VXLAN的子网进行网络配置，需要先建立VXLAN Pool，再建立VxlanNetwork。

注:

- 在添加NoVlanNetWork和VlanNetwork时，需要输入网卡设备名称。
- 在CentOS 7系列系统中，ethx格式的网卡名称会在系统重启后导致网卡顺序随机改变，建议将各计算节点的网卡设备名称修改成非ethx格式，例如，可修改成em01格式。尤其是带多网卡的云主机环境中。

二层网络与集群、三层网络、云主机之间的关系

二层网络与集群、三层网络、云主机之间存在以下关系：

- 同一个集群不能挂载两个相同的二层网络。
- 如果集群已挂载二层网络，但物理机不存在此二层设备，则物理机不能添加进入对应集群。
- 如果集群未挂载二层网络，但物理机不存在此二层设备，则集群不能挂载此二层网络。
- 如果某物理机存在此二层设备，但设备接线与集群内其他物理机接线不一致，则创建出的云主机IP不能正常工作。
- 删除二层网络，其对应的子资源三层网络将被删除，使用此三层网络的云主机的网卡也将被删除，请慎重操作！
- 删除二层网络，会删除使用此二层网络的云路由器/VPC路由器和云路由规格。
- 删除公有网络对应的二层网络，其对应的云路由的一切服务均会被删除，包括云路由器/VPC路由器、云路由规格、虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道等。
- VxlanNetwork下的云主机无法被外部的网络直接访问，需要通过弹性IP或者端口转发等服务进行间接访问。
- 一个VXLAN Pool可以创建多个VxlanNetwork，这些VxlanNetwork可以分别应用于扁平网络、云路由网络或VPC网络。
- ZStack支持一个二层网络可用于创建多个三层网络。其中，二层网络涵盖L2NoVlanNetwork、L2VlanNetwork、VxlanNetwork类型，三层网络涵盖公有网络、私有网络 / 扁平网络、云路由网络、VPC。

7.4.2.2.1 L2NoVlanNetwork

L2NoVlanNetwork表示二层网络不使用VLAN模式，如果不打算使用VLAN网络时，则应选择L2NoVlanNetwork。

注:

当交换机接入口配置为Access模式时，用户需设置L2NoVlanNetwork。

创建L2NoVlanNetwork

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**创建二层网络**，在弹出的**创建二层网络**界面，可参考以下示例输入相应内容：

- **名称**：设置二层网络名称
- **简介**：可选项，可留空不填

- **类型**：选择L2NoVlanNetwork
- **网卡**：输入二层网络设备名称，例如em01
- **集群**：选择需要加载的集群

如图 *300: 创建L2NoVlanNetwork*所示：

图 300: 创建L2NoVlanNetwork

7.4.2.2.2 L2VlanNetwork

L2VlanNetwork表示二层网络使用VLAN模式，如果打算使用VLAN网络时，则应选择L2VlanNetwork。

注:

- Vlan ID输入1-4094之间的数字。

- 如需云主机网络和物理机网络互通，则需在交换机端设置Trunk模式。

创建L2NoVlanNetwork

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**创建二层网络**，在弹出的**创建二层网络**界面，可参考以下示例输入相应内容：

- **名称**：设置二层网络名称
- **简介**：可选项，可留空不填
- **类型**：选择L2VlanNetwork
- **VLAN ID**：输入VLAN ID，可选1-4094之间的数字，需与实际网络配置相匹配
- **网卡**：输入二层网络设备名称，例如em01
- **集群**：选择需要加载的集群

如图 *301: 创建L2VlanNetwork*所示：

图 301: 创建L2VlanNetwork

7.4.2.2.3 VxlanNetwork

VXLAN Pool创建完毕后，可基于VXLAN Pool创建VxlanNetwork，每个VxlanNetwork对应了VXLAN Pool里面的一个Vni。

VXLAN网络特性

- VXLAN网络是建立在物理IP网络之上的虚拟网络，使用UDP封装五十个字节的报文头。
- 使用24位VXLAN网络标识符， 最大支持16M个逻辑网络。
- 使用UDP封装在三层物理网络上建立的二层逻辑网络。
- VXLAN可跨越物理三层网络。
- 使用IP多播封装广播和多播报文。

创建VxlanNetwork

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**创建二层网络**，在弹出的**创建二层网络**界面，可参考以下示例输入相应内容：

- **名称**：设置VxlanNetwork名称
- **简介**：可选项，可留空不填
- **类型**：选择VxlanNetwork
- **VXLAN网络池**：选择所在的VXLAN Pool
- **Vni**：可选项，可从VXLAN Pool中选择指定的Vni，若留空不填，则由ZStack动态随机分配

如图 *302: 创建VxlanNetwork*所示：

图 302: 创建VxlanNetwork

7.4.2.3 二层网络操作

L2NoVlanNetwork和L2VlanNetwork类型

L2NoVlanNetwork和L2VlanNetwork类型的网络支持以下操作：

- 修改名称：修改二层网络的名称。
- 修改简介：修改二层网络的简介。
- 加载集群：挂载网络到集群。
- 卸载集群：从集群卸载网络。
- 删除：删除二层网络，其对应的子资源三层网络将被删除，使用此三层网络的云主机的网卡也将被删除。
- 审计：查看L2NoVlanNetwork和L2VlanNetwork的相关操作。

VxlanNetwork类型

VxlanNetwork类型的网络支持以下操作：

- 修改名称：修改VxlanNetwork的名称。
- 修改简介：修改VxlanNetwork的简介。
- 共享：将此VxlanNetwork共享给指定的普通账户使用。
- 召回：将此VxlanNetwork从普通账户召回，使其不可见。
- 全局共享：将此VxlanNetwork共享给全部普通账户使用。
- 全局召回：将此VxlanNetwork从全部普通账户召回，使其不可见。
- 删除：删除VxlanNetwork，其对应的子资源三层网络将被删除，使用此三层网络的云主机的网卡也将被删除。
- 审计：查看VxlanNetwork的相关操作。

7.4.3 三层网络

三层网络：云主机使用的网络配置，包含了IP地址范围、网关、DNS、网络服务等。

- IP地址范围包含起始和结束IP地址、子网掩码、网关等，例如可指定*172.20.12.2*到*172.20.12.255*，子网掩码指定*255.255.0.0*，网关指定*172.20.0.1*。也可使用CIDR无域间路由来表示，例如*192.168.1.0/24*。
- DNS用于设置云主机网络的DNS解析服务。

公有网络

可直接连通互联网的网络，在云路由网络、VPC中可以提供网络服务。

- 可用于扁平网络创建使用公网的云主机；
- 可用于云路由网络环境，单独创建使用公网的云主机。
- 可用于VPC网络环境，单独创建使用公网的云主机。

系统网络

管理节点用于特定用途的网络。

- 可用于部署配置相关资源的管理网络，例如部署物理机、主存储、镜像服务器、云路由等资源；
- 可用于云主机迁移的迁移网络；
- 如果网络资源不足，可与公有网络共用；
- 独立的系统网络用于特定用途，例如管理云路由器的网络；
- 系统网络不能用于创建普通云主机。

私有网络

可称之为业务网络或接入网络，云主机使用的网络，一般情况下设置为私网。私有网络指定为云主机使用的网络，支持三种网络架构模型：扁平网络、云路由网络、VPC。

特定场景网络

- 管理网络

  作为系统网络的一种，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；
  - 创建云路由器/VPC路由器时需要云路由器/VPC路由器存在管理节点互通的IP，以便部署agent及agent代理消息返回。
- 存储网络

  特指在进行分布式存储部署时，底层存储系统通信使用的网络。在添加主存储时，可标识存储网络的CIDR，表示使用此网络来判断云主机健康状态。
- VDI网络

  在创建集群时，可以指定VDI网络的CDIR，此网络用于VDI连接的协议流量。

注意事项

- 创建云主机时，可指定多个网络。可指定多个扁平网络、或多个云路由网络、或多个VPC网络，或指定扁平网络、云路由网络、VPC网络的混合使用。
- 支持多级网络，而且多级网络的二层网络可以实际通信，需要特别避免IP地址空间冲突的问题。
- 一个二层网络可用于创建多个三层网络。其中，二层网络涵盖L2NoVlanNetwork、L2VlanNetwork、VxlanNetwork类型，三层网络涵盖公有网络、私有网络 / 扁平网络、云路由网络、VPC。

7.4.3.1 公有网络

公有网络表示可直接连通互联网的网络，在云路由网络/VPC中可以提供网络服务，既可用于扁平网络创建使用公网的云主机，也可用于云路由网络环境和VPC环境，单独创建使用公网的云主机。

创建公有网络

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，可参考以下示例输入相应内容：

- **名称**：设置公有网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择公有网络对应的二层网络

注:

ZStack支持一个二层网络可用于创建多个三层网络。

- 在**选择二层网络**界面，有两个子页面：**默认**和**全部**。
  - **默认**子页面：列出当前区域内尚未挂载三层网络的二层网络列表
  - **全部**子页面：列出当前区域内全部二层网络列表
- 用户可按需选择使用。

如图 *303:* 一个二层网络可用于创建多个三层网络所示：

图 303: 一个二层网络可用于创建多个三层网络

- **关闭DHCP服务**：选择是否需要DHCP服务
  - 若关闭DHCP服务，该网络创建的云主机需要手动配置IP
  - 若需要DHCP服务，在创建云主机时会分配一个IP给DHCP服务器，DHCP服务器会自动给云主机分配IP
- **添加网络段**：

  添加网络段有两种方法：IP范围、CIDR
  - 如选择IP范围，需设置以下内容：
    - **起始IP**：例如*172.20.108.200*
    - **结束IP**：例如*172.20.108.220*
    - **子网掩码**：例如*255.255.0.0*
    - **网关**：例如*172.20.0.1*
  - 如选择CIDR，需设置以下内容：
    - **CIDR**：例如*192.168.1.1/24*
- **添加DNS**：添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*

如图 *304:* 创建公有网络所示：

图 304: 创建公有网络

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
网络服务
关闭DHCP服务
添加网络段
方法
IP 范围
CIDR
起始IP *
172.20.108.200
结束IP *
172.20.108.220
子网掩码 *
255.255.0.0
网关 *
172.20.0.1
添加DNS
DNS

注意事项

请确保此公有网络的网络段可达外部网络，否则会导致云路由器或VPC路由器不能正常工作。

7.4.3.2 系统网络

系统网络表示管理节点用于特定用途的网络。例如，可用于部署配置相关资源的管理网络，包括部署物理机、主存储、镜像服务器、云路由等资源，也可用于云主机迁移的迁移网络。如果网络资源不足，可与系统网络共用。独立的系统网络仅用于特定用途，不能用于创建普通云主机。

创建系统网络

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，可参考以下示例输入相应内容：

- **名称**：设置系统网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择系统网络对应的二层网络

  注: 创建系统网络需使用单独的二层网络，不支持已挂载其它三层网络的二层网络用于创建系统网络。
- **关闭DHCP服务**：选择是否需要DHCP服务
  - 若关闭DHCP服务，该网络创建的云主机需要手动配置IP
  - 若需要DHCP服务，在创建云主机时会分配一个IP给DHCP服务器，DHCP服务器会自动给云主机分配IP
- **添加网络段**：

  添加网络段有两种方法：IP范围、CIDR
  - 如选择IP范围，需设置以下内容：
    - **起始IP**：例如*172.20.108.100*
    - **结束IP**：例如*172.20.108.120*
    - **子网掩码**：例如*255.255.0.0*
    - **网关**：例如*172.20.0.1*
  - 如选择CIDR，需设置以下内容：
    - **CIDR**：例如*192.168.1.1/24*
- **添加DNS**：添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*

如图 *305:* 创建系统网络所示：

图 305: 创建系统网络

确定
取消
创建系统网络
名称 *
L3-系统网络
简介
二层网络 *
L2-公有网络
添加网络段
方法
IP 范围
CIDR
起始IP *
172.20.108.100
结束IP *
172.20.108.120
子网掩码 *
255.255.0.0
网关 *
172.20.0.1
添加DNS
DNS
223.5.5.5

注意事项

创建云路由规格时，选择的公有网络和系统网络不能是同一个网段。

7.4.3.3 私有网络

私有网络表示云主机使用的网络，一般为内部网络，支持三种网络架构模型：扁平网络、云路由网络、VPC

- 云主机使用的私有网络，用于创建云主机，一般为内网。
- 用于扁平网络时，作为大二层网络，可与物理机网络直通。
- 用于云路由网络时，此网络可通过云路由器访问互联网。
- 用于VPC网络时，此网络可通过VPC路由器访问互联网。

本章主要介绍扁平网络和云路由网络类型，VPC相关介绍请参考*VPC*章节。

从**网络资源** > **三层网络** > **私有网络**入口创建私有网络，支持选择扁平网络和云路由网络类型，根据其支持的不同服务，分别配置相关的服务。

- **扁平网络**
  - 扁平网络支持以下网络服务：DHCP、弹性IP、安全组、UserData等；
  - 扁平网络的网络服务采用分布式的DHCP、分布式的EIP结构；
  - 扁平网络的DHCP服务也包含了DNS的功能；
- **云路由网络**
  - 云路由网络支持以下网络服务：DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec、安全组等；
  - 云路由网络的DHCP服务默认采用分布式的DHCP；
  - 云路由网络主要使用定制的Linux云主机作为路由设备提供网络服务。

创建私有网络（扁平网络/云路由网络类型）

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，可参考以下示例输入相应内容：

- **名称**：设置网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择私有网络对应的二层网络

注: ZStack支持一个二层网络可用于创建多个三层网络。

- **关闭DHCP服务**：选择是否需要DHCP服务
  - 若关闭DHCP服务，该网络创建的云主机需要手动配置IP
  - 若需要DHCP服务，在创建云主机时会分配一个IP给DHCP服务器，DHCP服务器会自动给云主机分配IP
- **选择网络架构模型**：**扁平网络**、**云路由**
  - 如选择扁平网络，请直接跳转到添加网络段。
  - 如选择云路由，需设置以下内容：
    - **云路由规格**：选择已创建的云路由规格。

      如果不存在云路由规格，则需在**云路由规格**界面创建云路由规格。详情请参考云路由规格章节。
- **添加网络段**：添加网络段有两种方法：IP范围、CIDR
  - 如选择IP范围，需设置以下内容：
    - **起始IP**：例如*172.20.108.150*
    - **结束IP**：例如*172.20.108.170*
    - **子网掩码**：例如*255.255.0.0*
    - **网关**：例如*172.20.0.1*
  - 如选择CIDR，需设置以下内容：
    - **CIDR**：例如*192.168.10.0/24*
- **添加DNS**：添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*

如图 *306:* 创建私有网络所示：

图 306: 创建私有网络

确定
取消
创建私有网络
名称 *
L3-私有网络
简介
二层网络 *
L2-私有网络
网络服务
关闭DHCP服务
扁平网络
云路由
云路由规格 *
云路由规格
添加网络段
方法
IP 范围
CIDR
CIDR *
192.168.10.0/24
添加DNS
DNS
223.5.5.5

7.4.3.4 三层网络操作

公有网络、系统网络和私有网络均支持的操作

三层网络的公有网络和私有网络均支持以下操作：

- 修改名称：修改三层网络的名称。
- 修改简介：修改三层网络的简介。
- 修改MTU：支持自定义限制网络传输数据包的大小，MTU参数的范围在68字节 ~ 9216字节，通常设置为1500。
- 添加网络段：给三层网络添加一段新的IP范围。
- 删除网络段：将三层网络的IP范围删除。
- 共享：将此三层网络共享给指定的普通账户使用。
- 召回：将此三层网络从普通账户召回，使其不可见。
- 全局共享：将此三层网络共享给全部普通账户使用。
- 全局召回：将此三层网络从全部普通账户召回，使其不可见。
- 添加DNS：添加一个DNS服务器地址。
- 删除DNS：删除一个DNS服务器地址。
- 创建报警器：为三层网络创建一个报警器并添加相关报警条目，系统可自动监控三层网络的多项报警条目，以邮件/钉钉/HTTP POST方式发送报警信息。
- 启用报警器：将已停用的报警器启用。
- 停用报警器：将正在使用的报警器停用。
- 删除报警器：删除一个报警器。
- 删除：删除三层网络。
- 查看监控数据：实时监控三层网络已用IP百分比情况。
- 审计：查看三层网络的相关操作。

私有网络下云路由类型的网络支持的操作

私有网络下云路由类型的网络还支持以下操作：

- 卸载云路由规格：加载云路由规格到云路由网络。
- 加载云路由规格：将云路由网络的云路由规格卸载掉。

VPC相关介绍请参考*VPC*章节。

7.4.4 路由资源

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。

云路由主要包括云路由镜像、云路由规格和云路由器。

- 云路由镜像：封装多种网络服务，只为创建云路由提供服务。
- 云路由规格：定义云路由器使用的CPU、内存、云路由镜像、公有网络、管理网络等。
- 云路由器：作为定制的Linux云主机提供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：

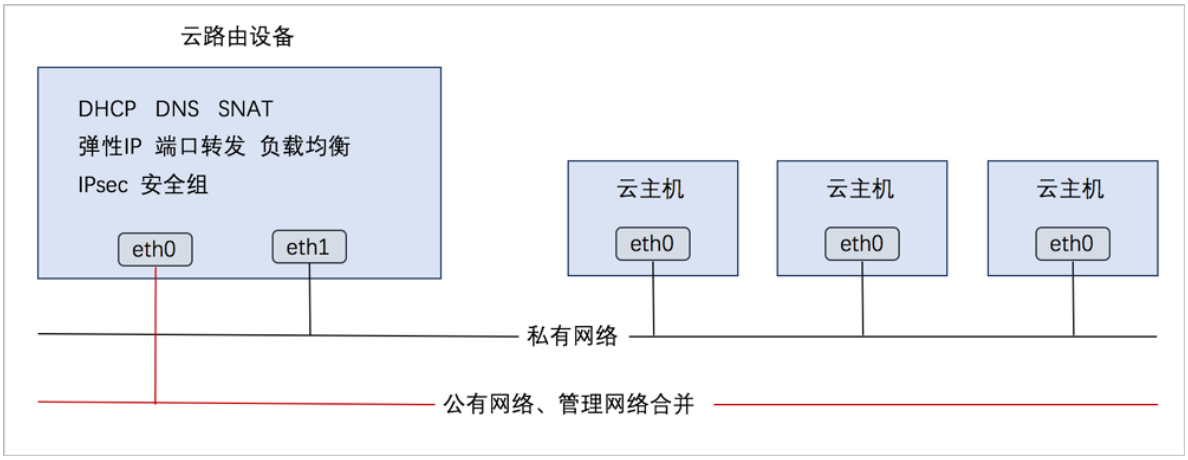
  也称之为业务网络或接入网络，是云主机使用的内部网络。

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 *307: 部署方式-1*所示：

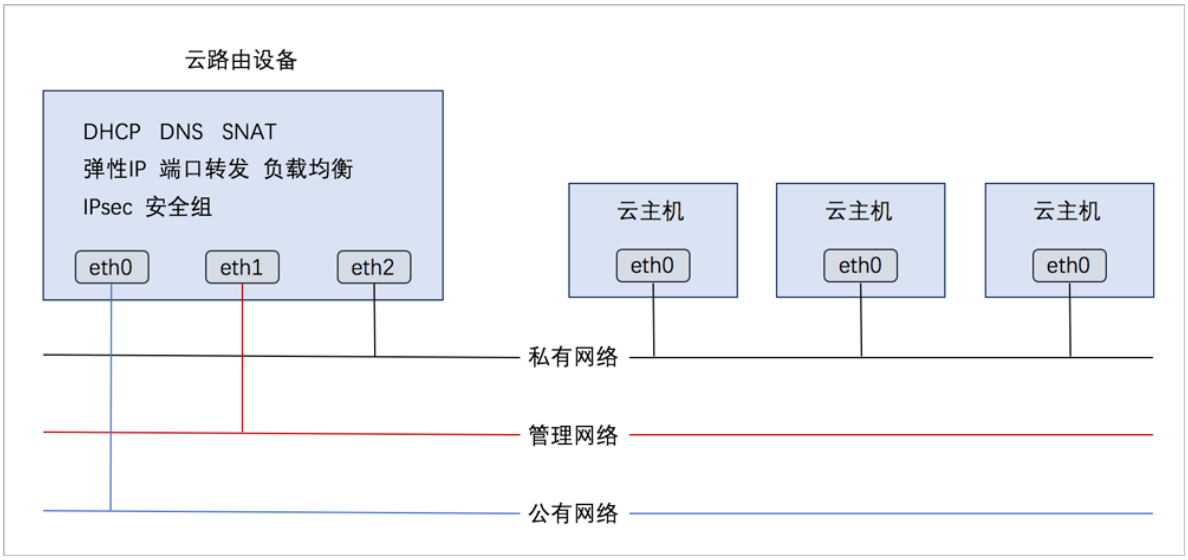
  图 307: 部署方式-1



- 公有网络、管理网络、私有网络均独立部署

  如图 *308:* 部署方式-2所示：

  图 308: 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、弹性IP、端口转发、负载均衡、IPsec隧道，将在专门章节中介绍。

云路由网络的基本部署流程

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。

注:

- 如果条件有限，管理网络可以与公有网络使用同一个网络。
- 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。

7.4.4.1 云路由器

云路由器：作为定制的Linux云主机提供分布式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。

- 云路由器由首次使用此网络的云主机同步创建。首次创建云路由器，启动时间可能较长。
- 云路由器必须存在公有网络、管理网络和私有网络。
- 同一个云路由规格只可创建一个云路由器。
- 云路由器需处于运行中和已连接的状态才可正常提供网络服务，如果处于其他状态，需检查相关资源是否异常。

云路由器详情页

- **基本属性**：

  云路由器**基本属性**显示了云路由器的概览信息和更多详细信息，并可在本页面对CPU、内存和平台信息进行修改。如图 *309:* 基本属性所示：

  图 309: 基本属性

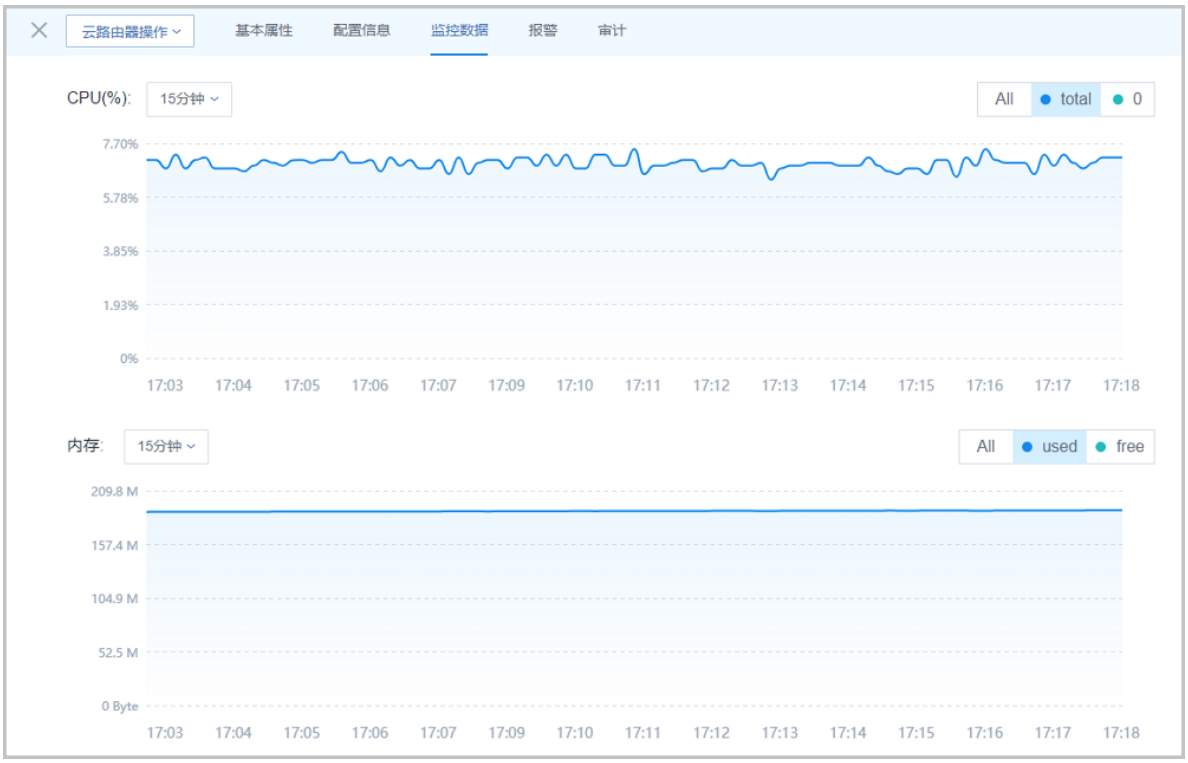
- **配置信息**：

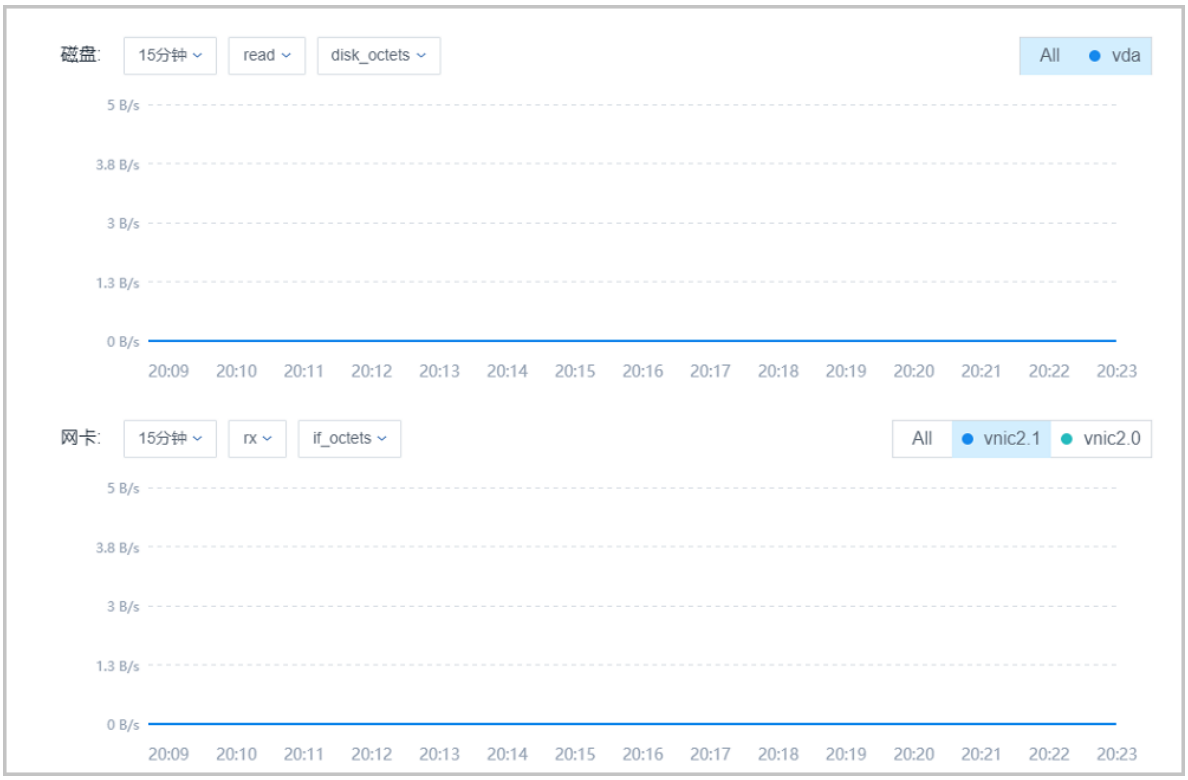
  云路由器**配置信息**页面显示了网卡信息，可在本页面对云路由器上的网卡进行加载和卸载操作。

- **监控数据**：

  监控数据页面显示了对云路由器的实时性能监控，包括：CPU、内存、磁盘、网卡，如图 *310:* 监控数据所示：

  图 310: 监控数据





- **报警**：

  ZStack支持云路由器报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加云路由器CPU、磁盘、网卡、内存相关的多项报警条目，以邮件/钉钉/HTTP 应用方式发送报警信息。

  使用方法与云主机报警类似，具体可参考云主机报警章节。

- **审计**：

  审计页面显示了当前云路由器的操作日志。

云路由器支持的操作

云路由器支持以下操作：

- 修改名称和简介：支持修改云路由器的名称和简介。
- 修改CPU/内存：支持开机/关机修改云路由器的CPU/内存。
- 修改平台：支持修改云路由器运行的平台类型。
- 启动：将停止状态的云路由器启动。
- 重启：重启云路由器。
- 重连：重连云路由器。

  注:

  - 目前ZStack管理节点升级重启后，云路由器需手动重连升级。
  - 云路由器手动重连升级后，虚拟IP设置QoS、IPsec隧道服务才可正常使用。
- 迁移：云路由器支持在线迁移。本地存储上的云路由器在线迁移，需在私有云**设置** > **全局设置** > **基本设置**里，将**在线迁移**设为true。
- 打开控制台：通过终端访问云路由器。
- 设置/删除控制台密码：支持设置/删除云路由器的控制台密码，重启生效。
- 删除：删除云路由器，会导致相关的云主机网络服务不可用，需重启云主机才可恢复网络服务。
- 加载/卸载网卡：
  - 支持加载/卸载新的公有网络。
  - 不可卸载云路由规格里定义的公有网络和管理网络。
  - 不支持加载/卸载私有网络。

7.4.4.2 云路由镜像

云路由镜像：封装多种网络服务，只为创建云路由提供服务。

- 云路由镜像是由ZStack定制进行封装的镜像，可从ZStack官方网站指定的URL下载。
- 云路由镜像不能直接用于创建云主机。

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*官方网站上找到最新的云路由镜像下载地址。

   - 文件名称：zstack-vrouter-2.5.1.qcow2
   - 下载地址：点击这里查看

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 *311:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 311: 添加云路由镜像

云路由镜像支持的操作

云路由镜像支持以下操作：

- 启用：创建云路由器时，此镜像可作为候选使用。
- 停用：停用后，创建云路由器时，此镜像将不再作为候选使用。
- 导出：如果镜像服务器类型是镜像仓库类型，那么此镜像支持导出功能。
- 删除：将云路由镜像删除掉。
- 恢复：将云路由镜像从删除状态恢复。
- 彻底删除：将云路由镜像从删除状态彻底删除。
- 审计：查看云路由镜像的相关操作。

已导出的云路由镜像支持以下操作：

- 下载：直接将云路由镜像下载下来。
- 复制URL：复制导出镜像的URL。
- 删除：将导出的镜像删除。

7.4.4.3 云路由规格

云路由规格：定义普通云路由器或VPC路由器使用的CPU、内存、云路由镜像、管理网络、公有网络等。

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 *312:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 312: 创建云路由规格

云路由规格支持的操作

云路由规格支持以下操作：

- 修改名称和简介：支持修改云路由规格的名称和简介。
- 启用：创建云路由器时，此规格可作为候选使用。
- 停用：停用后，创建云路由器时，此规格将不再作为候选使用。
- 共享：将此规格共享给指定的普通账户使用。

- 召回：将此规格从普通账户召回，使其不可见。
- 全局共享：将此规格共享给全部普通账户使用。
- 全局召回：将此规格从全部普通账户召回，使其不可见。
- 删除：将此云路由规格删除。
- 审计：查看此云路由规格的相关操作。

7.4.4.4 路由表

ZStack支持自定义配置虚拟路由器的路由表和路由条目，从而满足丰富的网络应用场景需求。

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**：可选项，可在创建路由表时指定待挂载的路由设备，也可创建路由表后再挂载路由设备

如图 *313:* 创建路由表所示：

图 313: 创建路由表

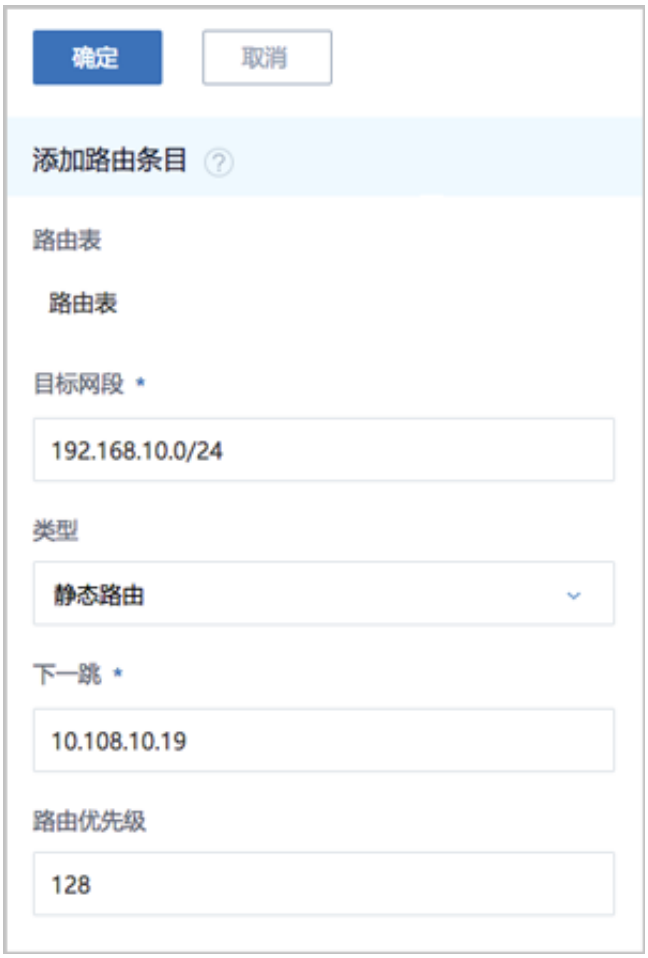
添加路由条目

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，可参考以下示例输入相应内容：

- **目标网段**：设置目标网段
- **类型**：路由类型一般设置静态路由，为防止环路，可设置黑洞路由，丢弃匹配的数据包
- **下一跳**：输入下一跳的地址，确保下一跳可达
- **优先级**：路由优先级设置范围为：1~254，数据越大，表示优先级越低

如图 *314:* 添加路由条目所示：

图 314: 添加路由条目



路由表支持的操作

路由表支持以下操作：

- 创建路由表：可在创建路由表时指定待挂载的路由设备，也可创建路由表后再挂载路由设备。
- 添加路由条目：自定义添加路由条目到路由表。
- 删除路由条目：删除路由表里的路由条目。
- 加载路由设备：支持路由表加载普通云路由器和VPC路由器。
- 卸载路由设备：支持路由表卸载普通云路由器和VPC路由器。
- 删除：将此路由表删除。
- 审计：查看此路由表的相关操作。

7.4.5 VPC

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。

- 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网络：作为VPC的私有网络，可挂载至VPC路由器。

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。

专有网络VPC的基本部署流程

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. 基于云路由规格创建VPC路由器。VPC路由器可提供各种网络服务。
8. 创建二层私有网络（用于创建三层的VPC网络），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，注意网络段不可重叠。
10. 使用VPC网络创建云主机。

注:

- 如果条件有限，管理网络可以与公有网络使用同一个网络。
- 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。
- 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。

7.4.5.1 VPC路由器

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。

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路由器名称
- **简介**：可选项，可留空不填
- **云路由规格**：选择已创建好的云路由规格

  需提前创建好云路由规格，详情请参考云路由规格章节。
- **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 *315: 创建VPC路由器*所示：

图 315: 创建VPC路由器

VPC路由器详情页

在**VPC路由器**管理界面，点击相应VPC路由器的名称，可展开其详情页。包含以下子页面：基本属性、网络、DNS、虚拟IP、弹性IP、IPsec隧道、端口转发、负载均衡、监控数据、报警和审计。

可通过**VPC路由器操作**对当前VPC路由器进行操作，所包含的操作菜单是VPC路由器管理界面上所有操作的合集。

如图 *316: VPC路由器详情页*所示：

图 316: VPC路由器详情页

- **基本属性**：

  基本属性页面为VPC路由器详情页的缺省栏，显示了当前VPC路由器的基本情况，包含：名称、简介、状态、概览和UUID等信息，如图 *316: VPC路由器详情页*所示。在此栏可修改VPC路由器的多项参数，具体如下：

  - **名称**和**简介**：支持修改VPC路由器的名称和简介
  - **CPU**和**内存**：支持开机/关机修改CPU/内存
  - **平台**：支持修改所运行的平台类型
  - **分布式路由**：分布式路由功能开关，默认**未开启**
    - 向右划至**开启**即生效，前提确保二层网络的MTU值一致。
    - 打开分布式路由功能，系统会尝试优化东西向网络流量，以提高吞吐量和降低网络延迟。
    - 分布式路由功能还可加强云主机之间通信的可靠性，内网跨三层流量不会因为云路由故障而失效。
- **网络**：

  网络页面列出了加载到当前VPC路由器的三层网络列表，主要分为VPC网络、公有网络和系统网络，如图 *317: 网络*所示：

  图 317: 网络

点击网络右侧的**操作**按钮，支持以下操作：

- VPC网络：
  - 创建：支持创建VPC网络并加载到VPC路由器。
  - 加载：支持加载VPC网络到VPC路由器。
  - 卸载：支持从VPC路由器卸载VPC网络，前提该VPC网络未挂载到任何云主机。
  - 删除：支持删除VPC路由器挂载的VPC网络。
- 公有网络：
  - 加载：支持加载公有网络到VPC路由器。
  - 卸载：支持从VPC路由器卸载其他公有网络，不支持卸载云路由规格定义的公有网络。
- 系统网络：不支持任何操作。

- **DNS**：

  VPC的DNS配置在VPC路由器上，VPC网络不能配置DNS地址。添加、删除DNS以后实时生效。

  DNS页面，显示了VPC路由器上的DNS列表，这些DNS按添加时间的先后顺序自顶向下依次排列生效。如图 *318: DNS*所示：

  图 318: DNS

- **虚拟IP**：

  虚拟IP页面列出了当前VPC路由器提供的虚拟IP列表，主要分为自定义虚拟IP和系统虚拟IP两个子栏。如图 *319: 虚拟IP*所示：

  图 319: 虚拟IP

  - 自定义虚拟IP：
    - 创建：用户手动创建。
    - 提供网络服务：

      VPC路由器可通过自定义虚拟IP提供弹性IP、端口转发、负载均衡、IPsec隧道服务。

      - 一个自定义虚拟IP仅用于一个弹性IP服务实例。
      - 一个自定义虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

        注: 不同类型服务不能使用相同的端口号。

      - 自定义虚拟IP不支持跨VPC路由器使用。
    - 删除：

- 删除自定义虚拟IP，将自动删除其上绑定的所有服务。
- 删除自定义虚拟IP的某一服务，并不影响其上绑定的其它服务运行。

- 系统虚拟IP：
  - 创建：VPC路由器成功创建后，由系统自动创建，该系统虚拟IP地址就是VPC路由器默认公网IP地址。
  - 提供网络服务：

    VPC路由器可通过系统虚拟IP提供端口转发、负载均衡、IPsec隧道服务。

    - 一个系统虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

      注: 不同类型服务不能使用相同的端口号。

    - 系统虚拟IP与VPC路由器一一对应。
  - 删除：
    - 删除系统虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
    - 删除VPC路由器，将自动删除相应的系统虚拟IP以及其上绑定的所有服务。

- **弹性IP**：

  弹性IP页面列出了当前VPC路由器提供的弹性IP列表，如图 *320: 弹性IP*所示。关于VPC下弹性IP的具体使用方法请参考《专有网络VPC 使用教程》弹性*IP*章节。

  图 320: 弹性IP

- **IPsec隧道**：

IPsec隧道页面列出了当前VPC路由器提供的IPsec隧道列表，如图 *321: IPsec隧道*所示。关于VPC下IPsec隧道的具体使用方法请参考《专有网络VPC 使用教程》*IPsec隧道*章节。

图 321: IPsec隧道

- **端口转发**：

端口转发页面列出了当前VPC路由器提供的端口转发列表，如图 *322:* 端口转发所示。关于VPC下端口转发的具体使用方法请参考《专有网络VPC 使用教程》端口转发章节。

图 322: 端口转发

- **负载均衡**：

负载均衡页面列出了当前VPC路由器提供的负载均衡列表，如图 *323:* 负载均衡所示。关于VPC下负载均衡的具体使用方法请参考《专有网络VPC 使用教程》负载均衡章节。

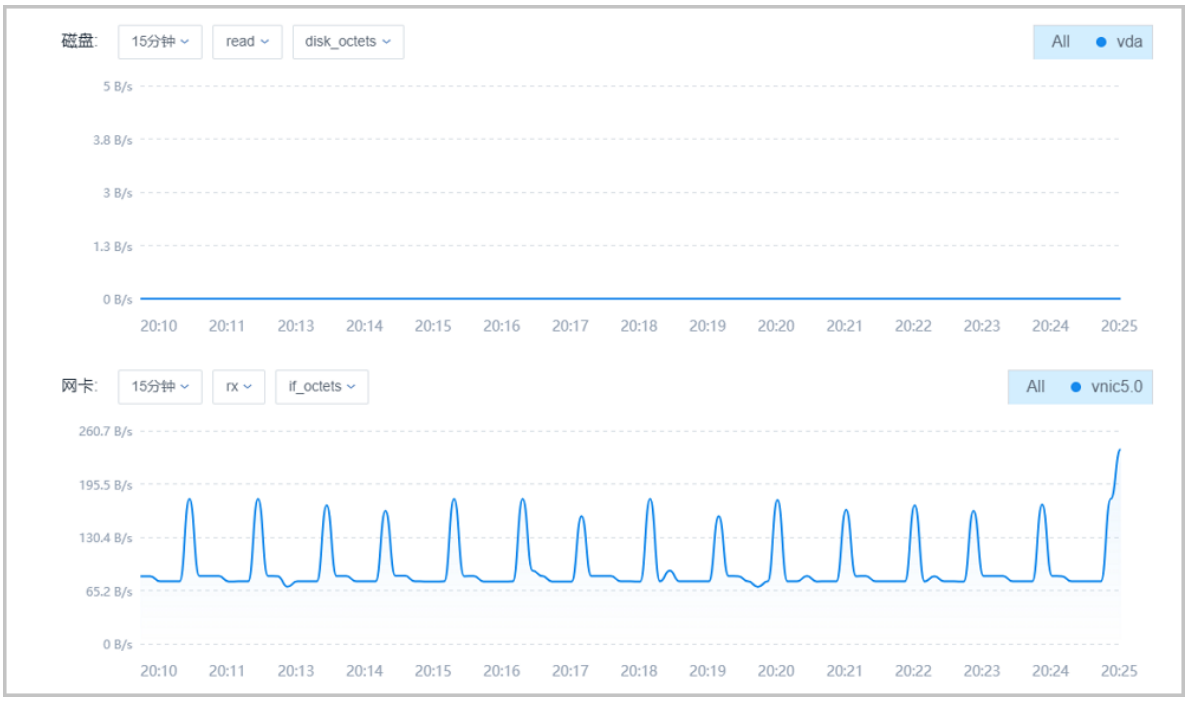
图 323: 负载均衡

- **监控数据**：

  监控数据页面显示了对VPC路由器的实时性能监控，包括：CPU、内存、磁盘、网卡，如图 *324:* 监控数据所示。

  - 监控数据自动实时更新。
  - 可选择查看监控数据的时间跨度：15分钟、1小时、6小时、1天、2周、8周、1年
  - 可选择磁盘和网络资源的不同监控指标。

图 324: 监控数据



- **报警**：

  ZStack支持VPC路由器报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加VPC路由器CPU、磁盘、网卡、内存相关的多项报警条目，以邮件/钉钉/HTTP 应用方式发送报警信息。

  使用方法与云主机报警类似，具体可参考云主机报警章节。

- **审计**：

  审计页面显示了当前VPC路由器的操作日志。

VPC路由器支持的操作

VPC路由器支持以下操作：

- 启动：将停止状态的VPC路由器启动。
- 重启：重启VPC路由器。
- 重连：重连VPC路由器。

  注:

  - 目前管理节点升级重启后，VPC路由器需手动重连升级。
  - VPC路由器手动重连升级后，虚拟IP设置QoS、VPC IPsec隧道服务才可正常使用。

- 迁移：VPC路由器支持在线迁移。本地存储上的VPC路由器在线迁移，需在私有云**设置** > **全局设置** > **基本设置**里，将**在线迁移**设为true。

- 打开控制台：通过终端访问VPC路由器。
- 设置/删除控制台密码：支持设置/删除VPC路由器的控制台密码，重启生效。
- 创建或删除DNS/弹性IP/IPsec隧道/端口转发/负载均衡器/虚拟IP：支持在当前VPC路由器下创建或删除DNS/弹性IP/IPsec隧道/端口转发/负载均衡器/自定义虚拟IP。
- 删除：删除VPC路由器，会导致相关的云主机网络服务不可用，需重新创建VPC路由器，并加载云主机使用的VPC网络，重启云主机才可恢复网络服务。

使用VPC路由器的注意事项

使用VPC路由器时，需注意：

- 不同VPC路由器下的VPC网络在二层默认互相隔离。
- 同一个VPC路由器下不同VPC网络的IP地址段不可重叠，任意两个VPC网络的网关不可相同。
- 普通账户创建VPC路由器前，需admin共享云路由规格，否则无法创建VPC路由器和VPC网络。
- VPC路由器需处于运行中和已连接的状态才可正常提供网络服务，如果处于其他状态，需检查相关资源是否异常。

7.4.5.2 VPC网络

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。

创建VPC网络

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，可参考以下示例输入相应内容：

- **名称**：设置VPC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
- **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
- **DHCP服务**：选择是否需要DHCP服务
- **添加网络段**：有IP范围和CIDR两种方式，本示例选择CIDR
- **CIDR**：填写CIDR范围，例如*192.168.10.0/24*

注: VPC路由器下所有VPC网络（子网）的网络段不可重叠。

如图 *325: 创建VPC网络*所示：

图 325: 创建VPC网络

VPC网络支持的操作

VPC网络支持以下操作：

- 修改名称和简介：支持修改VPC网络的名称和简介。
- 修改MTU：支持自定义限制网络传输数据包的大小，MTU参数的范围在68字节 ~ 9216字节，通常设置为1500。
- 添加网络段：给VPC网络添加一段新的IP范围。
- 删除网络段：将VPC网络的IP范围删除。
- 共享：将此VPC网络共享给指定的普通账户使用。
- 召回：将此VPC网络从普通账户召回，使其不可见。
- 全局共享：将此VPC网络共享给全部普通账户使用。
- 全局召回：将此VPC网络从全部普通账户召回，使其不可见。
- 创建报警器：为VPC网络创建一个报警器并添加相关报警条目，系统可自动监控VPC网络的多项报警条目，以邮件/钉钉/HTTP POST方式发送报警信息。
- 启用报警器：将已停用的报警器启用。
- 停用报警器：将正在使用的报警器停用。
- 删除报警器：删除一个报警器。
- 删除：删除VPC网络
- 查看监控数据：实时监控VPC网络已用IP百分比情况。
- 审计：查看VPC网络的相关操作。
- 加载VPC路由器：加载VPC路由器到VPC网络。
- 卸载VPC路由器：将VPC网络的VPC路由器卸载。

VPC详细部署实践请参考《专有网络VPC使用教程》。

7.5 网络服务

ZStack给云主机提供各种网络服务，主要包括安全组、虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道等。

支持以下三种网络架构模型：

- 扁平网络
- 云路由网络
- VPC

网络服务模块

网络服务模块：用于提供网络服务的模块。在UI界面已隐藏。

主要有以下四种：

1. VirtualRouter（虚拟路由器网络服务模块，不建议使用）

   提供以下网络服务：DNS、SNAT、负载均衡、端口转发、弹性IP、DHCP

2. Flat Network Service Provider（扁平网络服务模块）

   提供以下网络服务：

   - Userdata：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。

   - VipQos：虚拟IP限速，限制上行及下行带宽。仅作用于弹性IP。

3. vrouter（云路由网络服务模块）

   提供以下网络服务：

   - IPsec：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。
   - VRouterRoute：通过云路由路由表，用户可管理自定义路由。
   - CentralizedDNS：在启用分布式DHCP服务的场景下，提供DNS服务。
   - VipQos：虚拟IP限速，限制上行及下行带宽。
   - DNS：使用云路由器提供DNS服务。
   - SNAT：云主机使用SNAT可以直接访问外部互联网。
   - 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。
   - 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。
   - 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。
   - DHCP：集中式DHCP服务

4. SecurityGroup（安全组网络服务模块）

   提供以下网络服务：

   - 安全组：使用iptables进行云主机防火墙的安全控制。

扁平网络实践

生产环境中，一般建议使用以下网络服务的组合：

- 扁平网络服务模块：
  - Userdata：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实现的动态获取IP地址。

    注: DHCP服务包含了DNS的功能。
- 安全组网络服务模块：
  - 安全组：使用iptables进行云主机防火墙的安全控制。

云路由网络实践

生产环境中，一般建议使用以下网络服务的组合：

- 扁平网络服务模块：
  - Userdata：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。
  - DHCP：分布式DHCP实现的动态获取IP地址。
- 云路由网络服务模块：
  - DNS：使用云路由器提供DNS服务。
  - SNAT：云主机使用SNAT可以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。
- 安全组网络服务模块：
  - 安全组：使用iptables进行云主机防火墙的安全控制。

VPC网络实践

生产环境中，一般建议使用以下网络服务的组合：

- 扁平网络服务模块：
  - Userdata：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。
  - DHCP：分布式DHCP实现的动态获取IP地址。

- 云路由网络服务模块：
  - DNS：使用VPC路由器提供DNS服务。
  - SNAT：云主机使用SNAT可以直接访问外部互联网。
  - 弹性IP：使用VPC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。
- 安全组网络服务模块：
  - 安全组：使用iptables进行云主机防火墙的安全控制。

7.5.1 安全组

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：

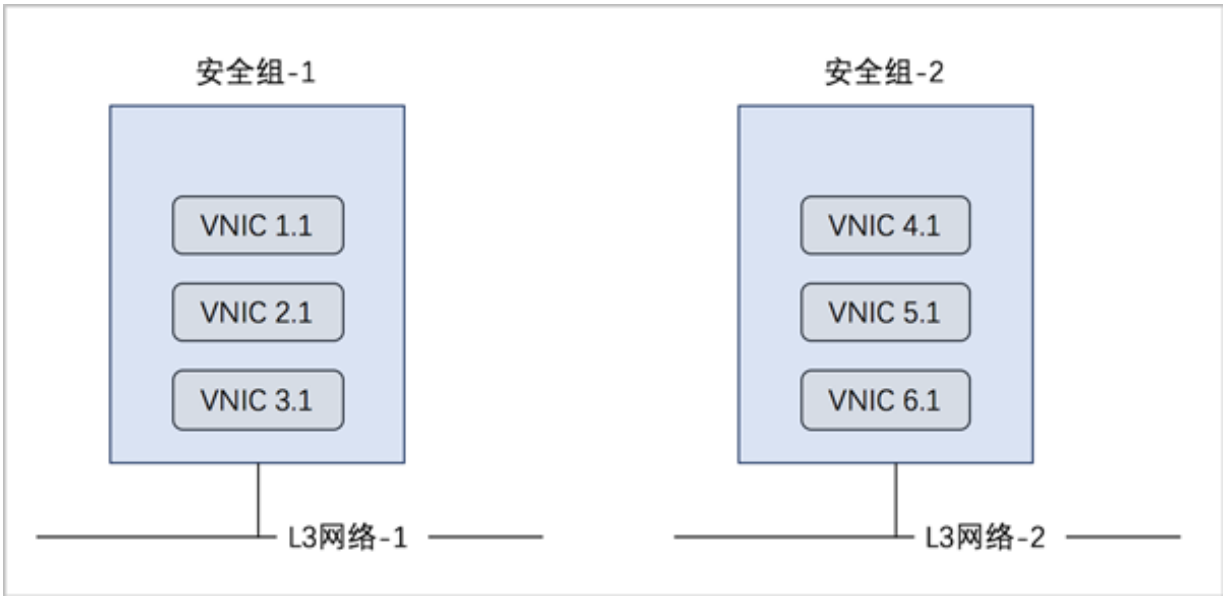
- 安全组规则按数据包的流向分为两种类型：
  - 入方向（Ingress）：代表数据包从外部进入云主机。
  - 出方向（Egress）：代表数据包从云主机往外部发出。
- 安全组规则对通信协议支持以下类型：
  - ALL：表示涵盖所有协议类型，此时不能指定端口。
  - TCP：支持1-65535端口。
  - UDP：支持1-65535端口。
  - ICMP：默认起始结束端口均为-1，表示支持全部的ICMP协议。
- 安全组规则支持对数据来源的限制，目前源可以设置为CIDR和安全组。
  - CIDR作为源：仅允许指定的CIDR才可通过

- 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 *326:* 安全组所示：

图 326: 安全组



安全组的使用方法

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。

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**：选择已创建的三层私有网络
- **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
- **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

如图 *327: 创建安全组*所示：

图 327: 创建安全组

设置安全组规则

以创建安全组时直接设置安全组规则为例。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**：选择安全组规则类型，例如入方向
- **协议**：选择协议类型，例如TCP
- **开始端口**：可从1-65535端口之间选择一个端口作为开始端口，例如23
- **结束端口**：可从1-65535端口之间选择一个端口作为结束端口，例如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 *328:* 设置规则所示：

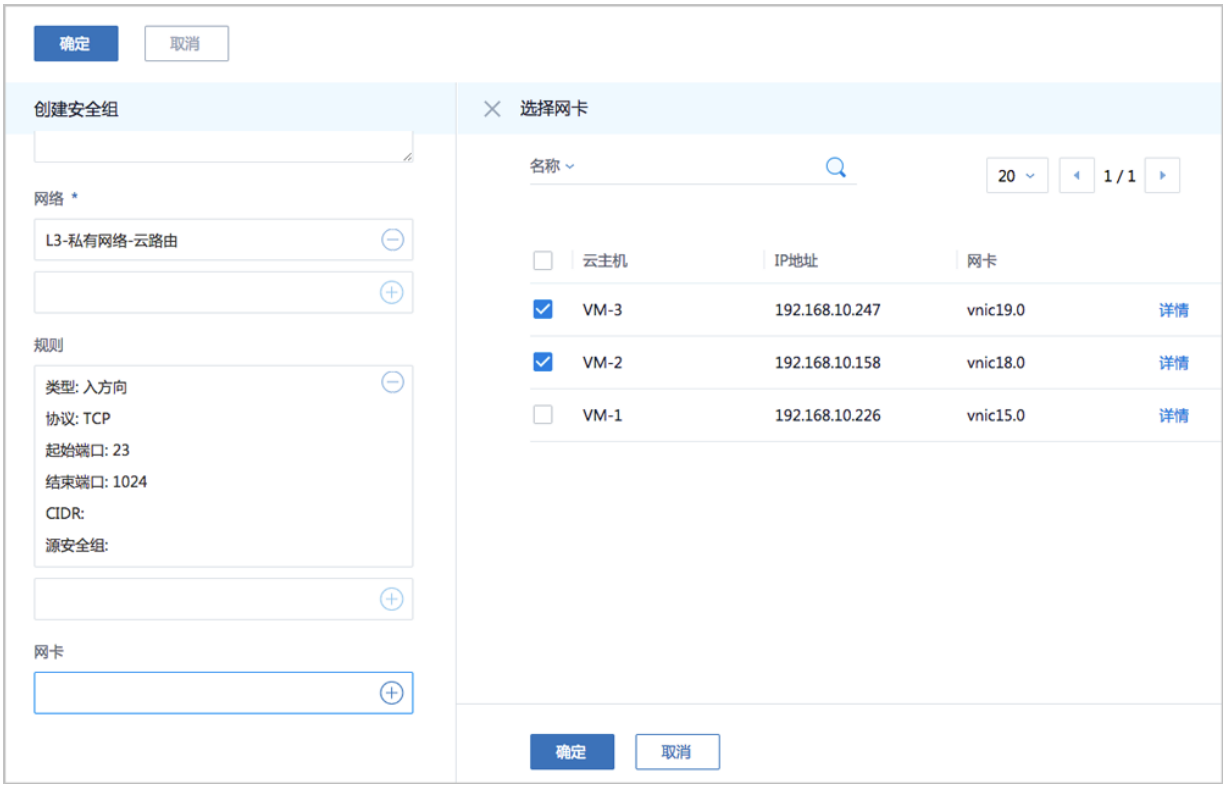
图 328: 设置规则

添加云主机网卡到安全组

以创建安全组时直接添加云主机网卡为例。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，选择需要添加的云主机网卡。

如图 *329: 添加云主机网卡到安全组*所示：

图 329: 添加云主机网卡到安全组



安全组支持的操作

安全组支持以下操作：

- 修改名称和简介：修改端口转发规则的名称和简介。
- 加载三层网络：安全组支持挂载到多个三层网络，它们会共享相同的安全组规则。
- 卸载三层网络：将安全组上的三层网络卸载。
- 添加规则：添加新的安全组规则到安全组。
- 删除规则：将安全组上的安全组规则删除。
- 绑定云主机网卡：安全组支持挂载到多个云主机，它们会共享相同的安全组规则。
- 解绑云主机网卡：将安全组上的云主机网卡解绑。
- 删除：删除安全组，将自动删除所有的安全组规则和相关安全组服务。

- 审计：查看此安全组的相关操作。

安全组的约束条件

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。

7.5.2 虚拟IP

虚拟IP（VIP）：在桥接网络环境中，使用虚拟IP地址来提供弹性IP、端口转发、负载均衡、IPsec隧道等网络服务，数据包会被发送到虚拟IP，再路由至云主机网络。

- 虚拟IP一般是将可以访问互联网的公有IP地址，路由到云主机的私有网络。
- 虚拟IP分为自定义虚拟IP和系统虚拟IP两类。

1. 自定义虚拟IP

    - 创建：由用户手动创建。
    - 提供网络服务：
        - 扁平网络下的自定义虚拟IP仅用于弹性IP服务。
        - 云路由网络/VPC下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务。
        - 一个自定义虚拟IP仅用于一个弹性IP服务实例。
        - 一个自定义虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

            注： 不同类型服务不能使用相同的端口号。

        - 自定义虚拟IP不支持跨普通云路由器/VPC路由器使用。
    - 删除：

- 删除自定义虚拟IP，将自动删除其上绑定的所有服务。
- 删除自定义虚拟IP的某一服务，并不影响其上绑定的其它服务运行。

2. 系统虚拟IP

- 创建：

  普通云路由器/VPC路由器成功创建后，由系统自动创建，该系统虚拟IP地址就是路由设备的默认公网IP地址。

- 提供网络服务：
  - 云路由网络/VPC下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务。
  - 一个系统虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

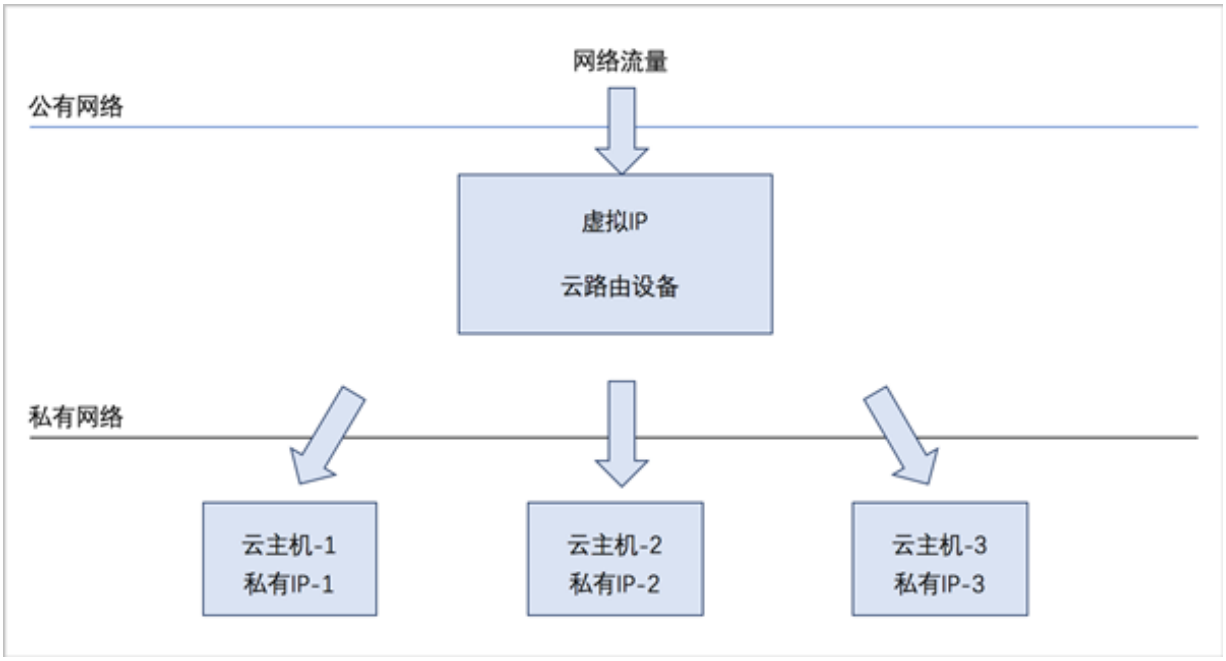
    注: 不同类型服务不能使用相同的端口号。

  - 系统虚拟IP与普通云路由器/VPC路由器一一对应。
- 删除：
  - 删除系统虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
  - 删除普通云路由器/VPC路由器，将自动删除相应的系统虚拟IP以及其上绑定的所有服务。

- 虚拟IP支持QoS：通过设置端口、限制上行及下行带宽，实现虚拟IP的端口流量控制。
  - 扁平网络下的自定义虚拟IP仅用于弹性IP服务，因此虚拟IP的QoS功能仅作用于弹性IP。
  - 云路由网络/VPC下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务，因此提供这四种服务的自定义虚拟IP均支持QoS设置。
  - 云路由网络/VPC下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务，因此提供这三种服务的系统虚拟IP均支持QoS设置。
  - 若使用VirtualRouter类型的云路由镜像创建云路由网络，不支持虚拟IP的QoS设置。
  - 同一虚拟IP可设置多个QoS规则，不设置端口的QoS规则优先级最低。

如图 *330: 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 330: 虚拟IP-负载均衡



虚拟IP的使用方法

- 自定义虚拟IP

  1. 扁平网络场景：

     扁平网络下的自定义虚拟IP仅用于弹性IP服务。使用方法有两种：

     - 在ZStack私有云主菜单，点击**网络服务** > **虚拟IP**，在**自定义虚拟IP**界面创建自定义虚拟IP后，在**弹性IP**界面，选择使用已有虚拟IP。
     - 点击**网络** > **网络服务** > **弹性IP**，在**弹性IP**界面选择新建虚拟IP。

  2. 云路由网络场景：

     云路由网络下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务。使用方法有两种：

     - 在ZStack私有云主菜单，点击**网络服务** > **虚拟IP**，在**自定义虚拟IP**界面创建自定义虚拟IP后，在**弹性IP**、**端口转发**、**负载均衡**、**IPsec隧道**界面，选择使用已有虚拟IP。
     - 在ZStack私有云主菜单，点击**网络服务** > **弹性IP/端口转发/负载均衡/IPsec隧道**，在**弹性IP**、**端口转发**、**负载均衡**、**IPsec隧道**界面，选择新建虚拟IP。

  3. VPC场景：

     VPC下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务。使用方法有四种：

- 在ZStack私有云主菜单，点击**网络** > **网络服务** > **虚拟IP**，在**自定义虚拟IP**界面创建自定义虚拟IP后，在**弹性IP**、**端口转发**、**负载均衡**、**IPsec隧道**界面，选择使用已有虚拟IP。
- 在ZStack私有云主菜单，点击**网络** > **网络服务** > **弹性IP/端口转发/负载均衡/IPsec隧道**，在**弹性IP**、**端口转发**、**负载均衡**、**IPsec隧道**界面，选择新建虚拟IP。
- 在ZStack私有云主菜单，点击**网络** > **VPC** > **VPC路由器**，在VPC路由器详情页的**虚拟IP**子页面创建自定义虚拟IP后，在**弹性IP**、**端口转发**、**负载均衡**、**IPsec隧道**子页面，选择使用已有虚拟IP。
- 在ZStack私有云主菜单，点击**网络** > **VPC** > **VPC路由器**，在VPC路由器详情页的**弹性IP/端口转发/负载均衡/IPsec隧道**子页面，选择新建虚拟IP。

- 系统虚拟IP

  1. 云路由网络场景：

     云路由网络下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务。使用方法有一种：

     - 在ZStack私有云主菜单，点击**网络** > **网络服务** > **端口转发/负载均衡/IPsec隧道**，在**端口转发**、**负载均衡**、**IPsec隧道**界面，选择使用已有虚拟IP。

  2. VPC场景：

     VPC下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务。使用方法有两种：

     - 在ZStack私有云主菜单，点击**网络** > **网络服务** > **端口转发/负载均衡/IPsec隧道**，在**端口转发**、**负载均衡**、**IPsec隧道**界面，选择使用已有虚拟IP。
     - 点击**网络** > **VPC** > **VPC路由器**，在VPC路由器详情页的**端口转发/负载均衡/IPsec隧道**子页面，选择使用已有虚拟IP。

创建自定义虚拟IP

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

- **名称**：设置虚拟IP名称
- **简介**：可选项，可留空不填
- **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
- **添加虚拟IP QoS**：支持对虚拟IP设置网络带宽限速，可在创建自定义虚拟IP时直接设置QoS，也可在创建自定义虚拟IP后再添加QoS

- **端口**：可选项，可指定某个端口设置QoS规则，支持端口范围：1-65535；若为空，表示该QoS规则对1-65535端口生效

  注: 不设置端口的QoS规则优先级最低。

- **上行网络带宽**：可选项，可按需设置虚拟IP的上行网络带宽上限，基本单位：Mbps；若为空，表示不限制上行网络带宽
- **下行网络带宽**：可选项，可按需设置虚拟IP的下行网络带宽上限，基本单位：Mbps；若为空，表示不限制下行网络带宽
- **添加更多QoS**：可选项，同一虚拟IP可设置多个QoS规则

如图 *331:* 创建虚拟*IP*所示：

图 331: 创建虚拟IP

虚拟IP支持的操作

虚拟IP支持以下操作：

- 创建虚拟IP：自定义虚拟IP由用户手动创建，系统虚拟IP由系统自动创建。

- 修改名称和简介：修改虚拟IP的名称和简介。
- 更改所有者：变更虚拟IP的所有者。
- 删除：
  - 自定义虚拟IP：
    - 删除自定义虚拟IP，将自动删除其上绑定的所有服务。
    - 删除自定义虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
  - 系统虚拟IP：
    - 删除系统虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
    - 删除普通云路由器/VPC路由器，将自动删除相应的系统虚拟IP以及其上绑定的所有服务。
- 添加/删除QoS：自定义虚拟IP和系统虚拟IP均支持添加/删除QoS。进入其详情页的QoS子页面进行添加/删除QoS即可。
- 报警：ZStack支持虚拟IP报警功能。创建报警器并添加相关报警条目，系统可自动监控已添加虚拟IP相关的多项报警条目，以邮件/钉钉/HTTP POST方式发送报警信息。
- 查看监控数据：实时显示虚拟IP的网络流量和网络包速率情况。
- 审计：查看此虚拟IP的相关操作。

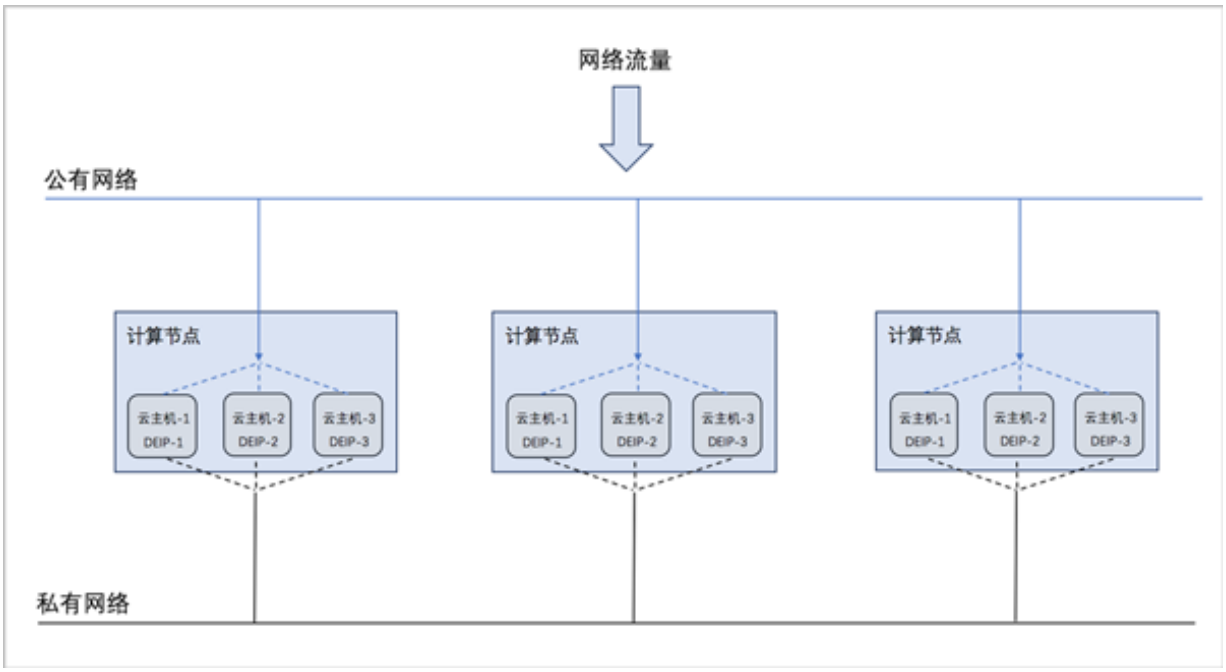
7.5.3 弹性IP

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。

扁平网络下弹性IP的应用场景，如图 *332: 扁平网络下弹性IP的应用场景*所示：

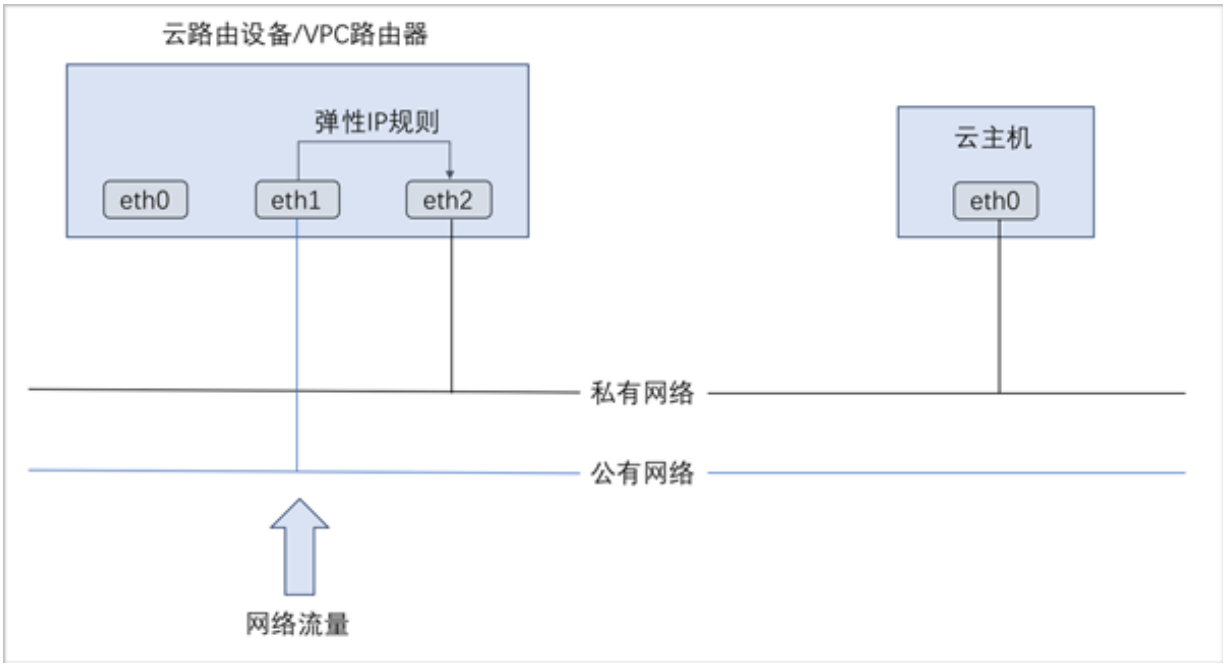
图 332: 扁平网络下弹性IP的应用场景



- 公有网络可通过防火墙连接到互联网。
- 私有网络为各个计算节点内云主机提供私有网络IP地址，此IP地址默认情况下无法连接到互联网。
- 每个计算节点分别部署分布式EIP，可分布独立实现公有网络与私有网络的绑定。

云路由网络/VPC下弹性IP的应用场景，如图 *333:* 云路由网络*/VPC*下弹性*IP*的应用场景所示：

图 333: 云路由网络/VPC下弹性IP的应用场景



创建弹性IP

在**私有云**界面，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
- **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 *334: 新建虚拟IP*所示：

    图 334: 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 *335: 已有虚拟IP*所示：

    图 335: 已有虚拟IP

如图 *336: 创建弹性IP*所示：

图 336: 创建弹性IP

弹性IP支持的操作

弹性IP支持以下操作：

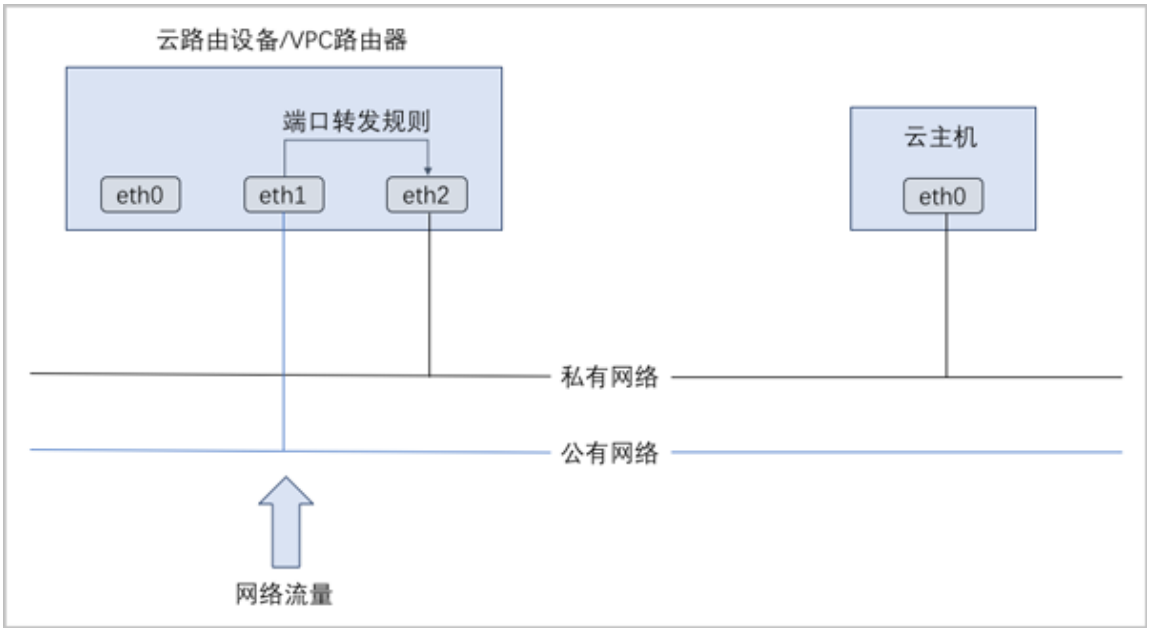
- 修改名称和简介：修改弹性IP的名称和简介。
- 绑定：将弹性IP绑定到云主机网卡。
- 解绑：将弹性IP与云主机网卡解绑。
- 更改所有者：变更弹性IP的所有者。
- 删除：删除弹性IP，将自动删除其提供的弹性IP服务。如需同时删除相应的虚拟IP，请勾选**删除虚拟IP**。
- 审计：查看此弹性IP的相关操作。

7.5.4 端口转发

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。

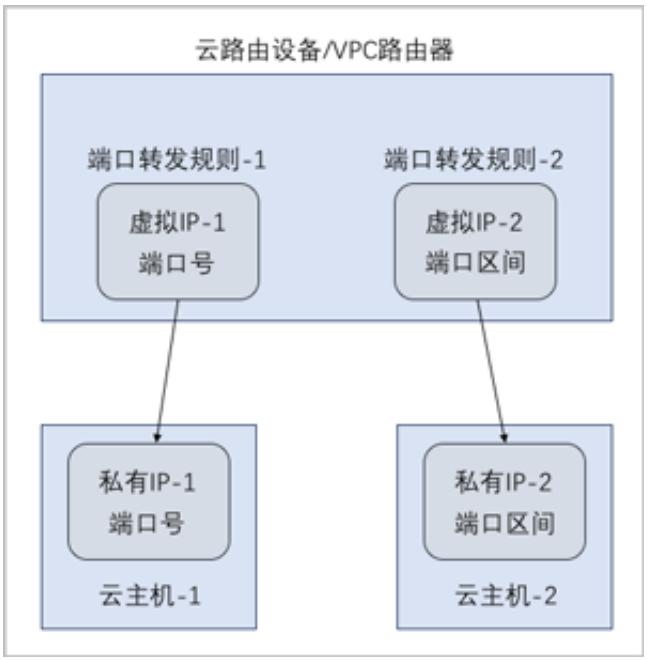
- 启用SNAT服务的私有网络中，云主机可访问外部网络但不能被外部网络所访问；使用端口转发规则，允许外部网络访问SNAT后面云主机的某些指定端口。
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *337:* 端口转发所示：

    图 337: 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 *338: 虚拟IP-端口转发*所示：

图 338: 虚拟IP-端口转发



创建端口转发规则

在**私有云**界面，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
- **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 *339: 新建虚拟IP*所示：

    图 339: 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 *340: 已有虚拟IP*所示：

    图 340: 已有虚拟IP

注: 云路由器/VPC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 *341:* 创建端口转发规则-指定端口所示：

    图 341: 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 *342:* 创建端口转发规则-端口区间所示：

  图 342: 创建端口转发规则-端口区间

创建的端口转发规则如图 *343:* 创建端口转发规则所示：

图 343: 创建端口转发规则

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

端口转发规则绑定云主机网卡

弹出**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，选择需绑定的云主机网卡，点击**确定**。

如图 *344:* 选择云主机网卡和图 *345:* 端口转发规则绑定云主机网卡所示：

图 344: 选择云主机网卡

图 345: 端口转发规则绑定云主机网卡

端口转发支持的操作

端口转发支持以下操作：

- 修改名称和简介：修改端口转发规则的名称和简介。
- 绑定：将端口转发规则绑定到云主机网卡。
- 解绑：将端口转发规则与云主机网卡解绑。
- 删除：删除端口转发规则，将自动删除其提供的端口转发服务。相应的虚拟IP以及其上绑定的其它服务不受影响。
- 审计：查看此端口转发的相关操作。

端口转发的约束条件

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。

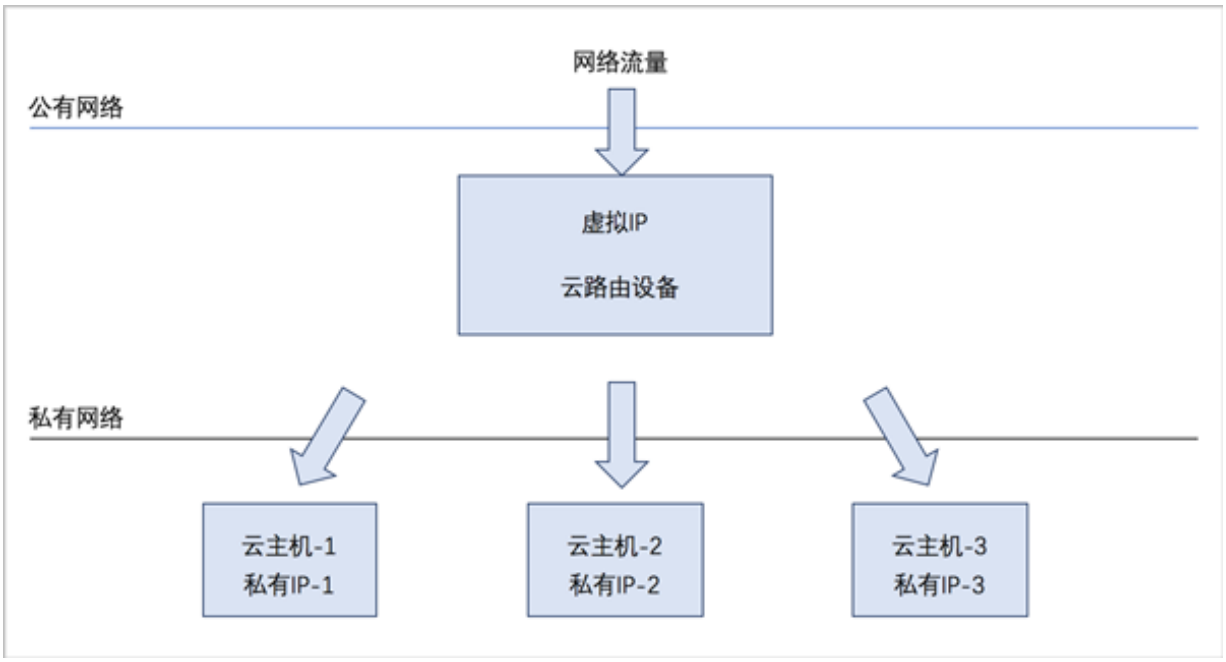
7.5.5 负载均衡

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三种协议。
- 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 *346: 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 346: 虚拟IP-负载均衡



负载均衡的使用方法

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。

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 *347: 新建虚拟IP*所示：

    图 347: 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 *348: 已有虚拟IP*所示：

  图 348: 已有虚拟IP

注: 云路由器/VPC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，可在创建负载均衡器时直接创建并添加监听器，也可在创建负载均衡器后再创建并添加监听器

如图 *349: 创建负载均衡器*所示：

图 349: 创建负载均衡器

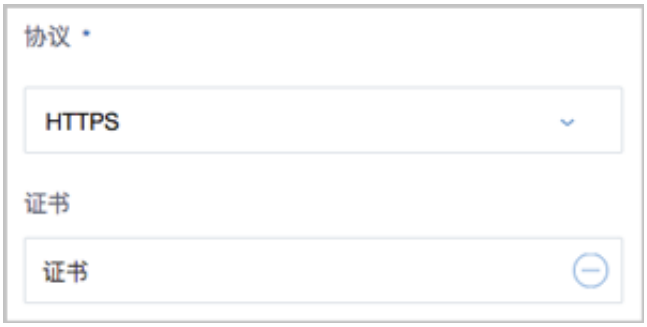
创建监听器

以创建负载均衡器过程中直接创建并添加监听器为例。

在**创建负载均衡器**界面，点击**监听器**下方的**创建监听器**，弹出**创建监听器**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
  - 如选择TCP/HTTP：支持1-65535端口
  - 如选择HTTPS：
    - 支持1-65535端口
    - 需绑定证书使用，支持上传证书和证书链，如何上传及管理证书可参考证书章节。
    - **证书**为可选项，可在创建监听器时直接绑定证书，也可在创建监听器后再绑定证书。
    - 如图 *350: HTTPS* 需绑定证书所示：

      图 350: HTTPS 需绑定证书

- **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 *351:* 创建监听器所示：

  图 351: 创建监听器

- **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
  - **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
  - **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 *352:* 创建监听器-高级选项所示：

图 352: 创建监听器-高级选项

绑定云主机网卡到监听器

在ZStack私有云主菜单，点击**网络服务** > **负载均衡** > **监听器**，进入**监听器**界面，选中已创建的监听器，点击**更多操作** > **绑定云主机网卡**，将弹出**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 *353:* 绑定云主机网卡到监听器所示，点击**确定**，绑定云主机网卡到监听器。

图 353: 绑定云主机网卡到监听器

负载均衡器将基于指定转发策略向三台云主机发送信息。

负载均衡支持的操作

负载均衡器支持以下操作：

- 修改名称和简介：修改负载均衡器的名称和简介。
- 创建监听器：创建一个新的监听器。

- 删除：删除负载均衡器，将自动删除所有的监听器和相关负载均衡服务。相应的虚拟IP以及其上绑定的其它服务不受影响。
- 审计：查看此负载均衡器的相关操作。

监听器支持以下操作：

- 修改名称和简介：修改监听器的名称和简介。
- 绑定云主机网卡：绑定云主机网卡到负载均衡器的某个监听器，使云主机成为监听器规则的一个负载均衡资源。
- 解绑云主机网卡：从监听器上解绑云主机网卡，将其从负载均衡池中移除。
- 绑定证书：当监听协议为HTTPS，需绑定证书使用，绑定一个证书或证书链到监听器。当监听协议为TCP/HTTP，该按钮禁用。
- 解绑证书：当监听协议为HTTPS，从监听器上解绑证书。当监听协议为TCP/HTTP，该按钮禁用。
- 删除：删除监听器，将自动删除其提供的负载均衡服务。
- 审计：查看此监听器的相关操作。

负载均衡的约束条件

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。

7.5.6 IPsec隧道

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。

IPsec隧道的特性：

- **IPsec连接模式**

基于安全考虑，只支持主动模式（Main Mode），不支持积极模式（Aggressive Mode）；仅支持ESP封装协议。

- **IPsec传输模式**

  仅支持站点到站点的隧道模式，不支持PC点对点模式（基于云端网络模型考虑），不支持两端存在NAT网络。

- **IPsec路由模型**

  仅支持基于对端网段配对模型，仅支持路由配对模式，不支持路由转发模式（不支持OSPF或BGP等动态路由协议）。

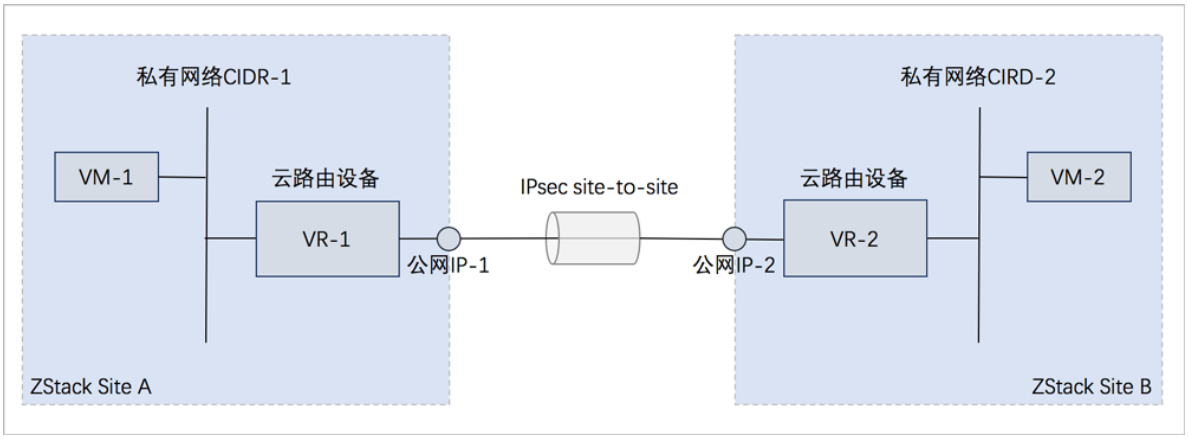
本章主要介绍云路由网络下IPsec隧道的使用，关于VPC下IPsec隧道的具体使用方法请参考《专有网络VPC使用教程》的*IPsec*隧道章节。

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。

  如图 *354:* 云路由网络下*IPsec*隧道应用场景所示：

  图 354: 云路由网络下IPsec隧道应用场景



云路由网络下IPsec隧道的使用方法

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。

在第一套ZStack中创建IPsec隧道

在ZStack私有云主菜单，点击**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 *355: 新建虚拟IP*所示：

    图 355: 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 *356: 已有虚拟IP*所示：

图 356: 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 *357: 创建IPsec隧道-1*所示：

图 357: 创建IPsec隧道-1

在第二套ZStack中创建IPsec隧道

在第二套ZStack中创建IPsec隧道的步骤与第一套步骤相同，只是参数存在差异，如图 *358: 创建IPsec隧道-2*所示：

图 358: 创建IPsec隧道-2

IPsec隧道搭建完毕后，两套ZStack的私网可以互通。

IPsec隧道支持的操作

云路由网络下IPsec隧道支持以下操作：

- 修改名称和简介：修改IPsec隧道的名称和简介。
- 删除：删除IPsec隧道，将自动删除其提供的IPsec隧道服务。相应的虚拟IP以及其上绑定的其它服务不受影响。
- 审计：查看此IPsec隧道的相关操作。

VPC下IPsec隧道支持以下操作：

- 修改名称和简介：修改IPsec隧道的名称和简介。
- 加载本地子网：VPC下IPsec隧道支持加载多个本地私有网络。
- 卸载本地子网：将IPsec隧道上的本地私有网络卸载。
- 添加远端网络CIDR：VPC下IPsec隧道支持加载多个远端网络CIDR。
- 删除远端网络CIDR：将IPsec隧道上的远端网络CIDR卸载。
- 删除：删除IPsec隧道，将自动删除其提供的IPsec隧道服务。相应的虚拟IP以及其上绑定的其它服务不受影响。
- 审计：查看此IPsec隧道的相关操作。

7.6 网络教程

网络教程主要包括：

- 扁平网络使用教程
- 云路由网络使用教程
- 专有网络VPC使用教程

7.6.1 扁平网络使用教程

7.6.1.1 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。

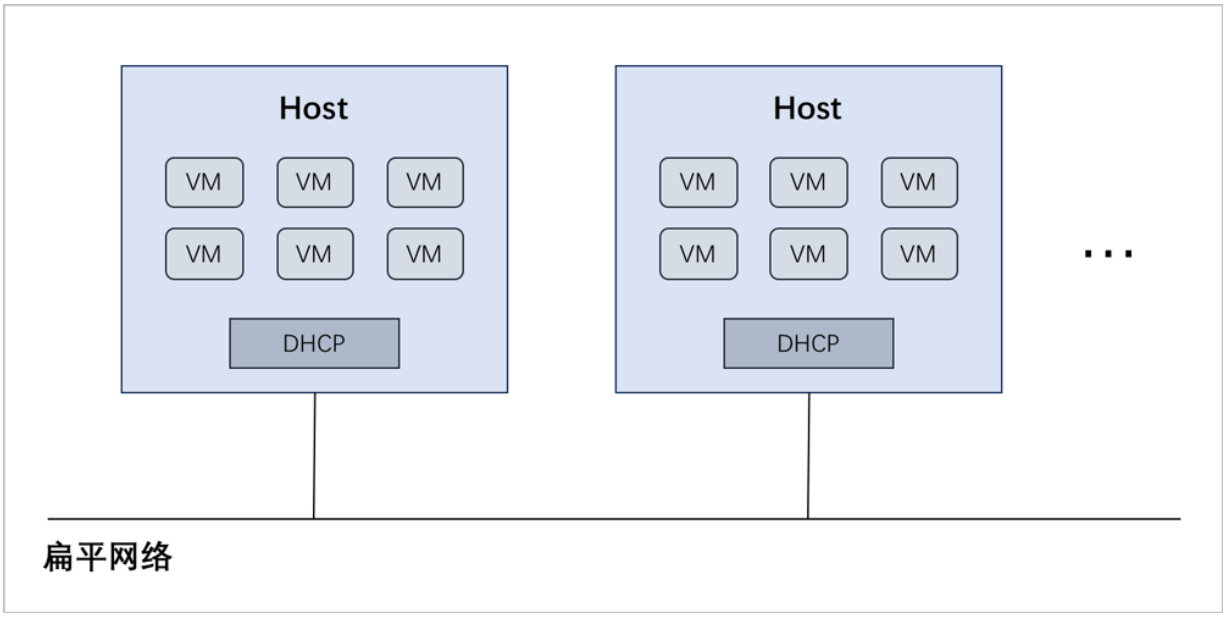
- DHCP：分布式DHCP实现动态获取IP地址。

  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 *359:* 扁平网络架构图所示：

图 359: 扁平网络架构图



7.6.1.2 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。

7.6.1.3 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 6: 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 *6:* 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 *360:* 创建*L2*-扁平网络所示，点击**确定**，创建L2-扁平网络。

   图 360: 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 *6: 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 *361:* 创建*L3*-扁平网络所示，点击**确定**，创建L3-扁平网络。

图 361: 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 *362: 创建云主机VM-1*所示，点击 **确定**，创建私有云云主机。

   图 362: 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 *363: VM-1 ping通 VM-2*所示：

        图 363: 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 *364: VM-2 ping通 VM-1*所示：

图 364: 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。

7.6.1.4 应用场景

扁平网络可用于以下典型应用场景：

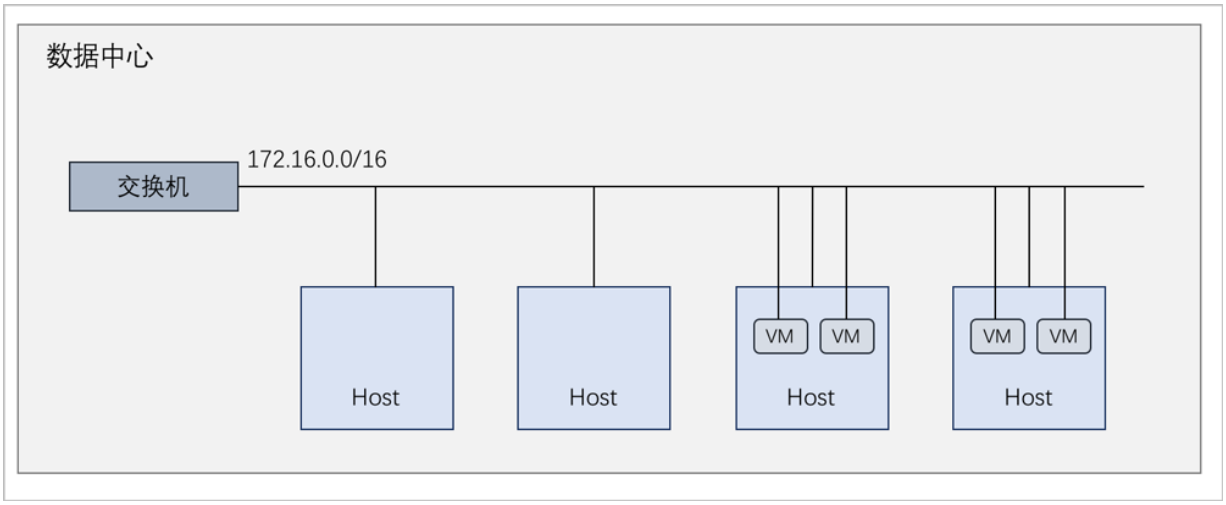
- 二层连通网络
- 安全组
- 弹性IP

7.6.1.4.1 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 *365: 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 365: 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。

7.6.1.4.2 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。

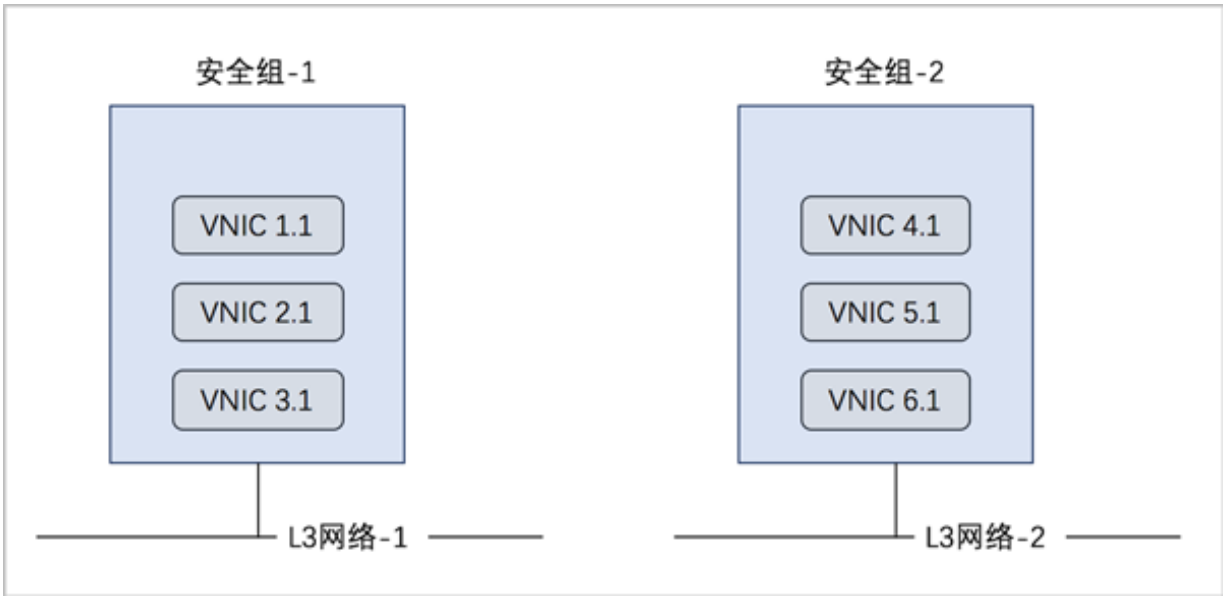
安全组规则：

- 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 *366:* 安全组所示：

图 366: 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：

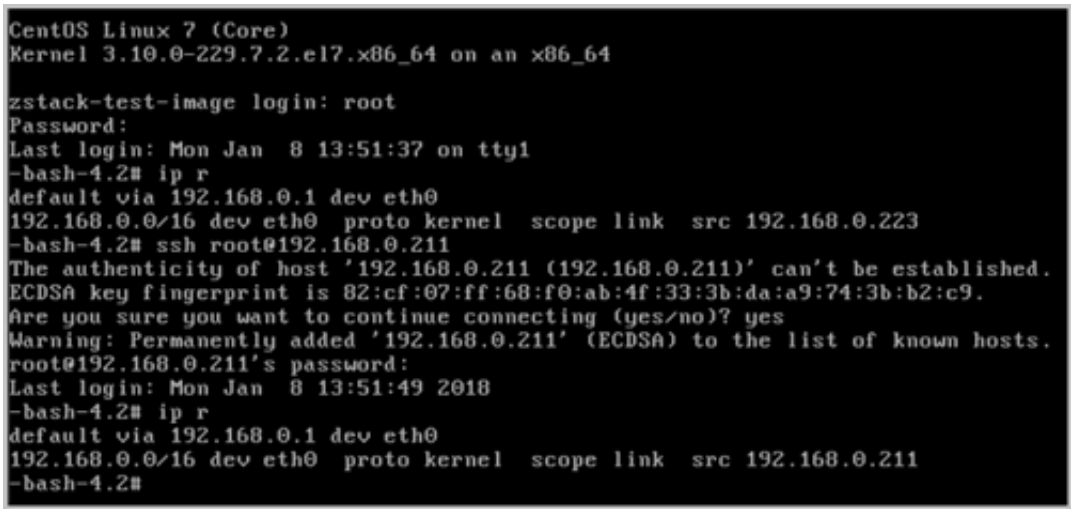
- 对云主机设置入方向规则。
- 对云主机设置出方向规则。

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 *367: SSH远程登录成功*所示：

   图 367: SSH远程登录成功



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 *368:* 创建安全组所示，点击**确定**，创建安全组。

图 368: 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

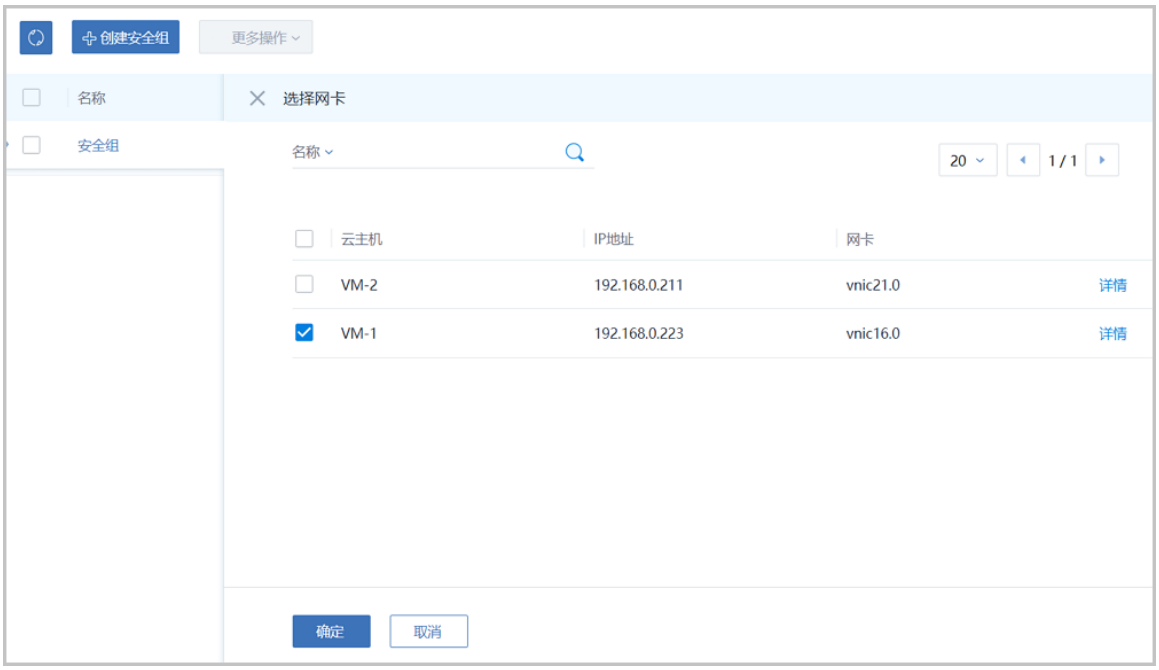
如图 *369:* 设置入方向规则所示，点击**确定**，设置入方向规则。

图 369: 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 *370:* 添加云主机网卡到安全组所示：

图 370: 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 *371: VM-2在端口10尝试连接VM-1失败*所示：

   图 371: 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 *372: VM-2在端口23向VM-1发送信息*和图 *373: VM-1在端口23接收信息成功*所示：

   图 372: VM-2在端口23向VM-1发送信息

图 373: 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 *374:* 设置出方向规则所示，点击**确定**，设置出方向规则。

图 374: 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。

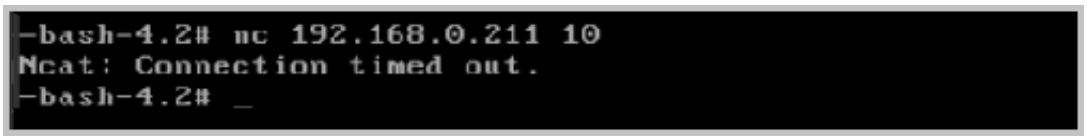
登录VM-2，尝试使用*nc*命令与VM-1建立通信连接。

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 *375: VM-1在端口10尝试连接VM-2失败*所示：

   图 375: VM-1在端口10尝试连接VM-2失败



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 *376: VM-1*在端口*200*向*VM-2*发送信息和图 *377: VM-2*在端口*200*接收信息成功所示：

   图 376: VM-1在端口200向VM-2发送信息

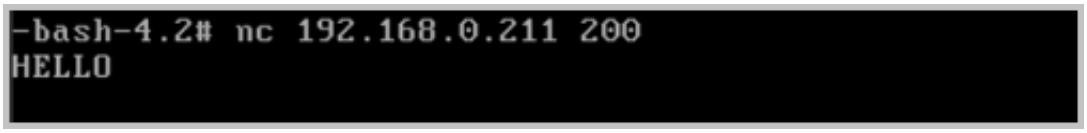


   图 377: VM-2在端口200接收信息成功

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。

7.6.1.4.3 弹性IP

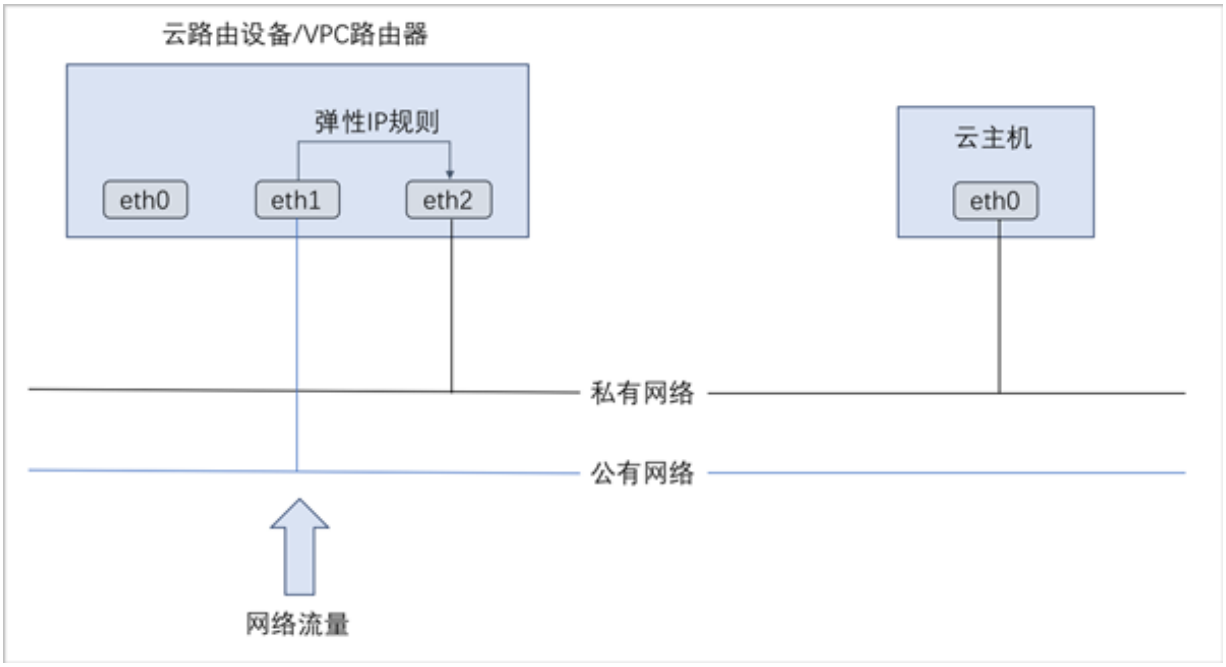
前提条件

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 *378: 云路由网络/VPC下弹性IP的应用场景*所示：

图 378: 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 *379: 新建虚拟IP*所示：

    图 379: 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 *380: 已有虚拟IP*所示：

    图 380: 已有虚拟IP

如图 *381: 创建弹性IP*所示：

图 381: 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 *382: 选择VM-1*和图 *383: 将EIP-1绑定VM-1*所示：

图 382: 选择VM-1

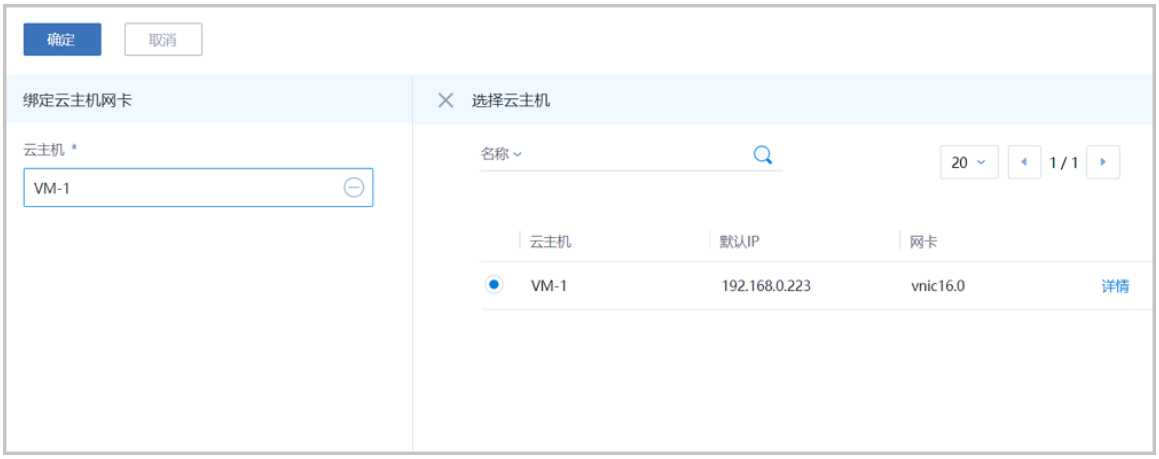
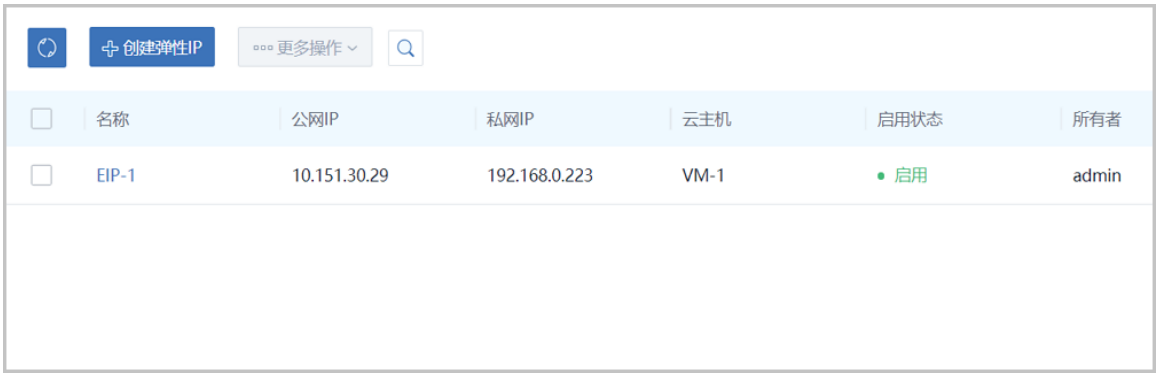


图 383: 将EIP-1绑定VM-1



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 *384: 通过EIP-1登录VM-1*所示：

图 384: 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 *385: 将EIP-1从VM-1解绑*所示：

   图 385: 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。

7.6.2 云路由网络使用教程

7.6.2.1 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：

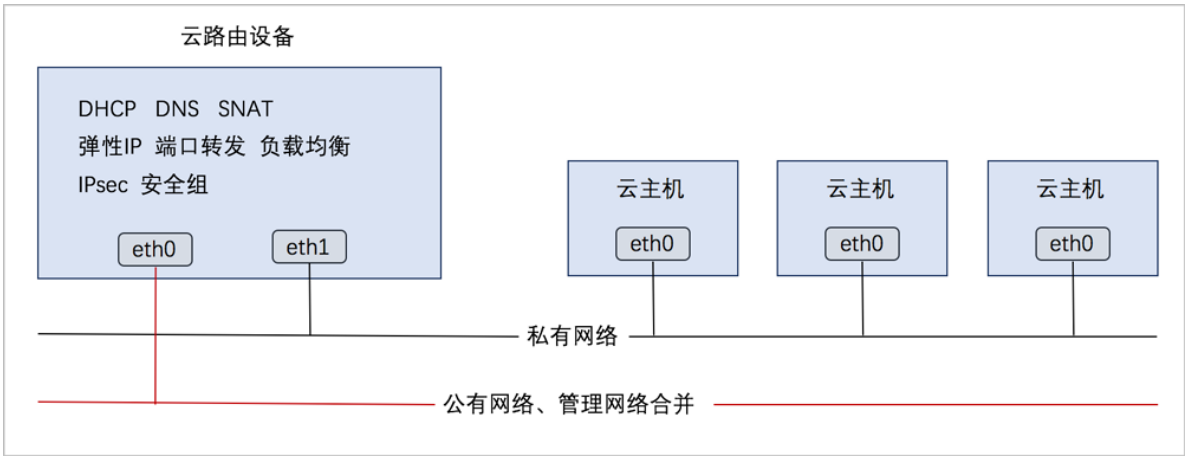
  也称之为业务网络或接入网络，是云主机使用的内部网络。

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 *386: 部署方式-1*所示：

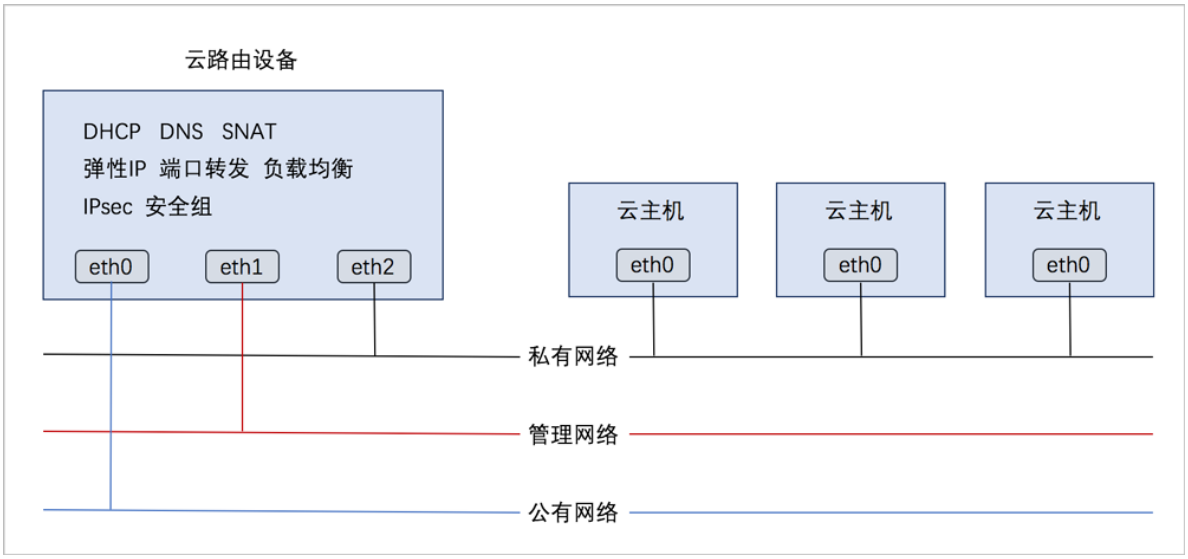
  图 386: 部署方式-1



- 公有网络、管理网络、私有网络均独立部署

  如图 *387: 部署方式-2*所示：

  图 387: 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原网络地址转换；
  - 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。

7.6.2.2 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。

7.6.2.3 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 7: 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*

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

2. 管理网络

表 8: 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。

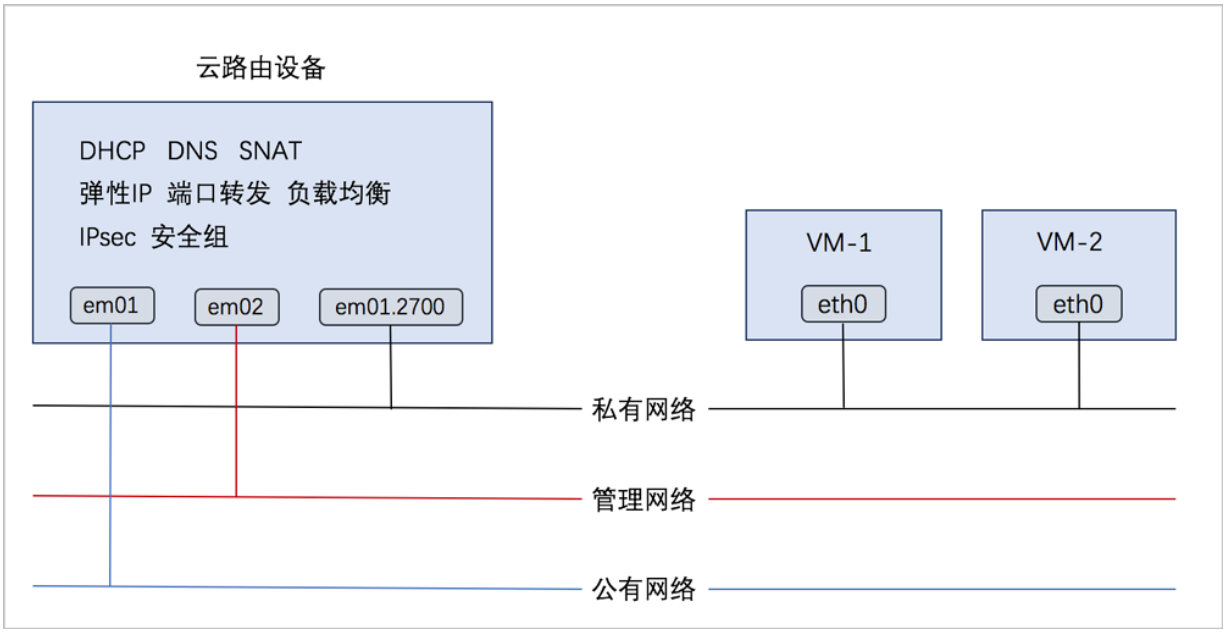
3. 私有网络

表 9: 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*

云路由网络架构如图 *388:* 云路由网络架构图所示：

图 388: 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 *7:* 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 *389:* 创建*L2*-公有网络所示，点击**确定**，创建L2-公有网络。

   图 389: 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 7: 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
   - **网络服务**：选择是否需要DHCP服务
   - **添加网络段**：选择IP范围
   - **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*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *390:* 创建*L3*-公有网络所示，点击**确定**，创建L3-公有网络。

图 390: 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
添加网络段
方法
IP 范围
CIDR
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
添加DNS
DNS
223.5.5.5

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 *8:* 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 *391:* 创建*L2*-管理网络所示，点击**确定**，创建L2-管理网络。

图 391: 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 *8:* 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
   - **DHCP服务**：选择是否需要DHCP服务
   - **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*
   - **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

   如图 *392:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

   图 392: 创建L3-管理网络

确定
取消
创建系统网络
名称 *
L3-管理网络
简介
二层网络 *
L2-管理网络
添加网络段
方法
IP 范围
CIDR
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
添加DNS
DNS
223.5.5.5

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*官方网站上找到最新的云路由镜像下载地址。

   - 文件名称：zstack-vrouter-2.5.1.qcow2
   - 下载地址：点击这里查看

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 *393:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 393: 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 *394:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 394: 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 *9:* 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 *395: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 395: 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 9: 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
- **DHCP服务**：选择是否需要DHCP服务
- 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*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *396:* 创建*L3*-私有网络所示，点击**确定**，创建L3-私有网络。

图 396: 创建L3-私有网络

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**：从网络列表中选择已创建的L3-私有网络（云路由网络）

如图 *397:* 创建私有云云主机所示，点击 **确定**，创建私有云云主机。

图 397: 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 *398: VM-1 ping*通公网所示：

  图 398: VM-1 ping通公网

```
[root@192-168-10-226 ~]# ip r
default via 192.168.10.1 dev eth0
169.254.0.0/16 dev eth0  scope link  metric 1002
192.168.10.0/24 dev eth0  proto kernel  scope link  src 192.168.10.226
[root@192-168-10-226 ~]# 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=51 time=26.0 ms
64 bytes from 220.181.57.217: icmp_seq=2 ttl=51 time=26.8 ms
64 bytes from 220.181.57.217: icmp_seq=3 ttl=51 time=26.0 ms
64 bytes from 220.181.57.217: icmp_seq=4 ttl=51 time=26.5 ms
64 bytes from 220.181.57.217: icmp_seq=7 ttl=51 time=26.1 ms
^C
--- baidu.com ping statistics ---
```

- 内网连通性验证：

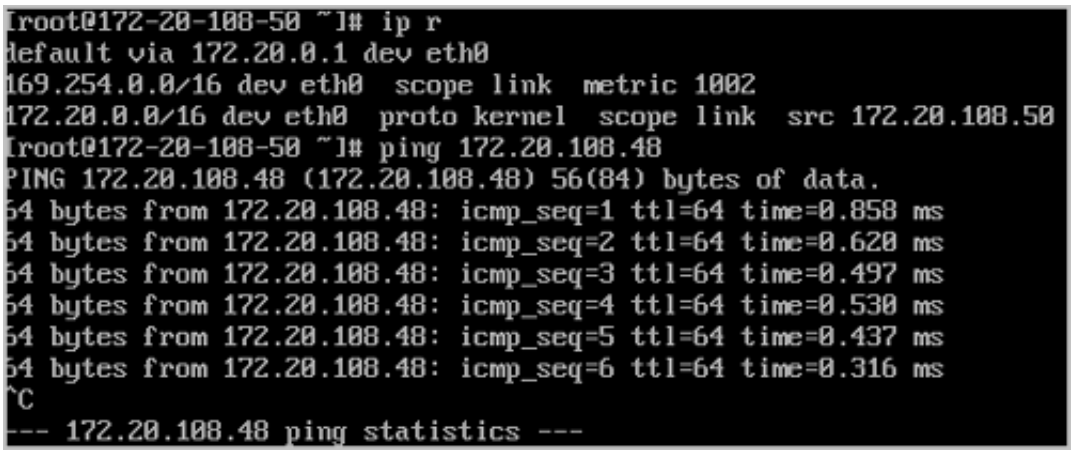
  1. 使用该云路由网络创建另一台私有云云主机，例如VM-2。
  2. 登录VM-1，检查是否能够ping通VM-2，如图 *399: VM-1 ping通 VM-2*所示：

     图 399: 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 *400: VM-2 ping通 VM-1*所示：

     图 400: VM-2 ping通 VM-1



至此，云路由网络的基本部署实践介绍完毕。

7.6.2.4 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

7.6.2.4.1 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 10: 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

VLAN	VXLAN
	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 11: 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 12: 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 13: 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 14: 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*

5. 私有网络2

表 15: 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*

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 *11:* 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 *401:* 创建*L2-*公有网络所示，点击**确定**，创建L2-公有网络。

   图 401: 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 *11:* 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
   - **DHCP服务**：选择是否需要DHCP服务
   - **添加网络段**：选择IP范围
   - **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*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *402:* 创建*L3*-公有网络所示，点击**确定**，创建L3-公有网络。

图 402: 创建L3-公有网络

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 *12:* 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 *403:* 创建*L2*-管理网络所示，点击**确定**，创建L2-管理网络。

图 403: 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 *12:* 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
- **DHCP服务**：选择是否需要DHCP服务
- **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*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *404:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 404: 创建L3-管理网络

确定
取消
创建系统网络
名称 *
L3-管理网络
简介
二层网络 *
L2-管理网络
添加网络段
方法
IP 范围
CIDR
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
添加DNS
DNS
223.5.5.5

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*官方网站上找到最新的云路由镜像下载地址。

   - 文件名称：zstack-vrouter-2.5.1.qcow2
   - 下载地址：点击这里查看

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 *405:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 405: 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 *406:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 406: 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 *13: 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 *407: 创建VXLAN网络池*所示，点击**确定**，创建VXLAN网络池。

图 407: 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）。

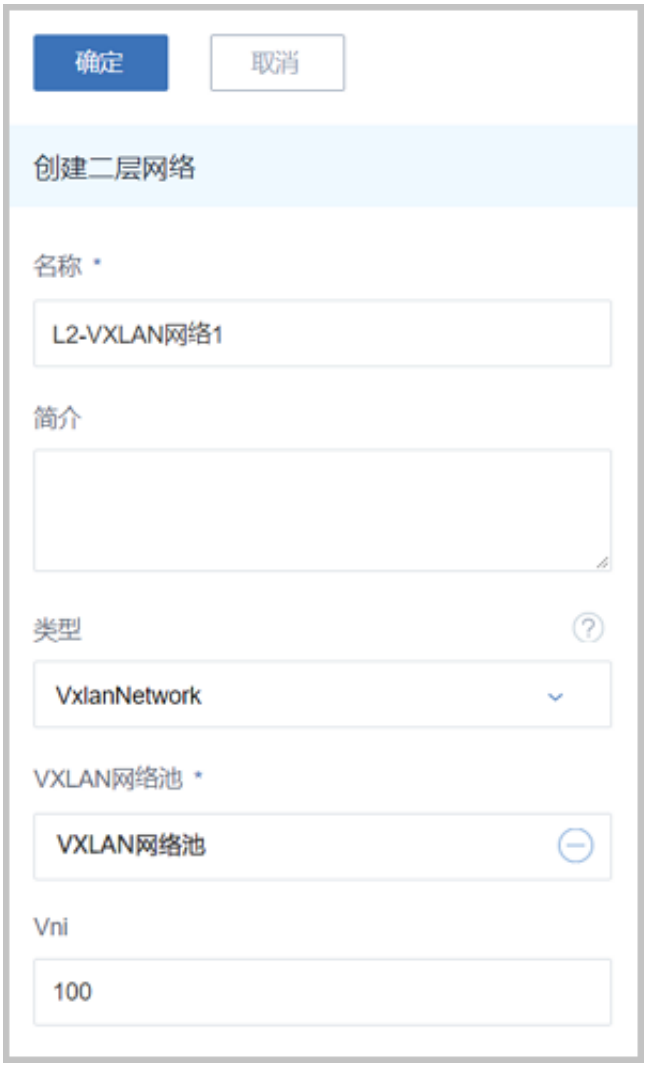
   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网络**，在弹出的**创建二层网络**界面，参考上述表 *14: 私有网络1*配置信息填写如下：

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

图 408: 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 *14: 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
- **DHCP服务**：选择是否需要DHCP服务

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

如图 *409: 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 409: 创建L3-VXLAN-云路由网络1

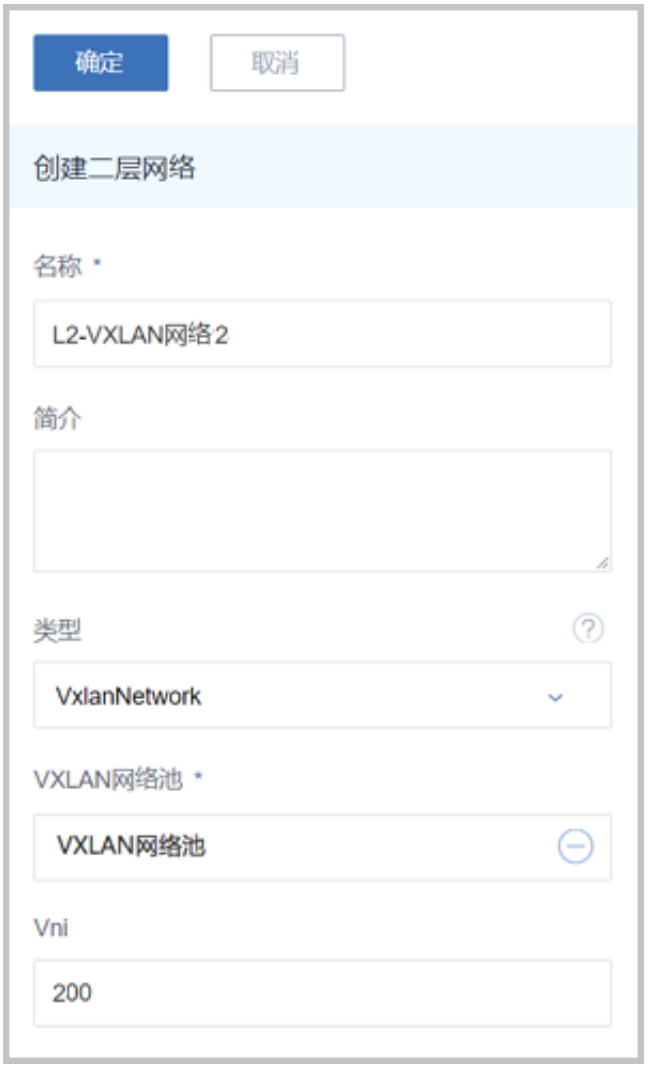
10.基于VXLAN网络池创建VXLAN网络2（虚拟的L2-私有网络）。

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 *15:* 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 *410:* 创建*L2-VXLAN*网络*2*所示，点击**确定**，创建L2-VXLAN网络2。

图 410: 创建L2-VXLAN网络2



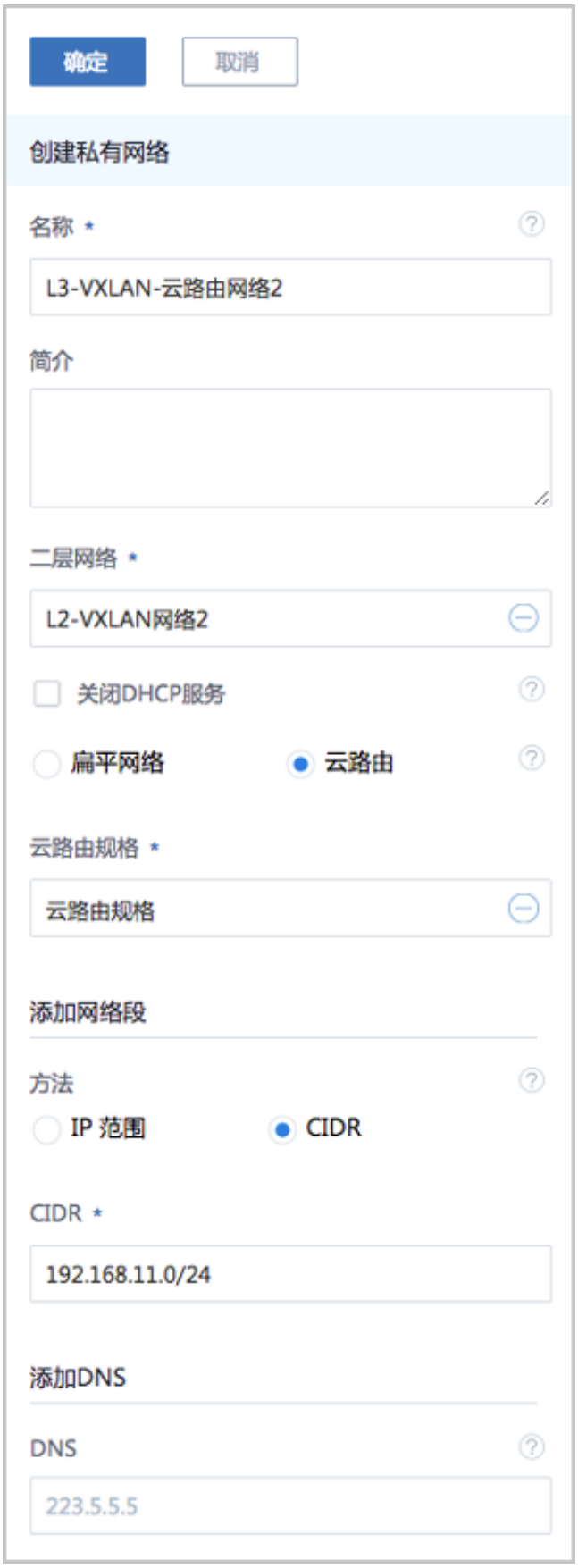
11.使用L2-VXLAN网络2创建云路由类型的L3-私有网络2。

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 *15:* 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
- **DHCP服务**：选择是否需要DHCP服务
- 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*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *411:* 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 411: 创建L3-VXLAN-云路由网络2



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 *412: VM-1、VM-2*所示：

图 412: 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）

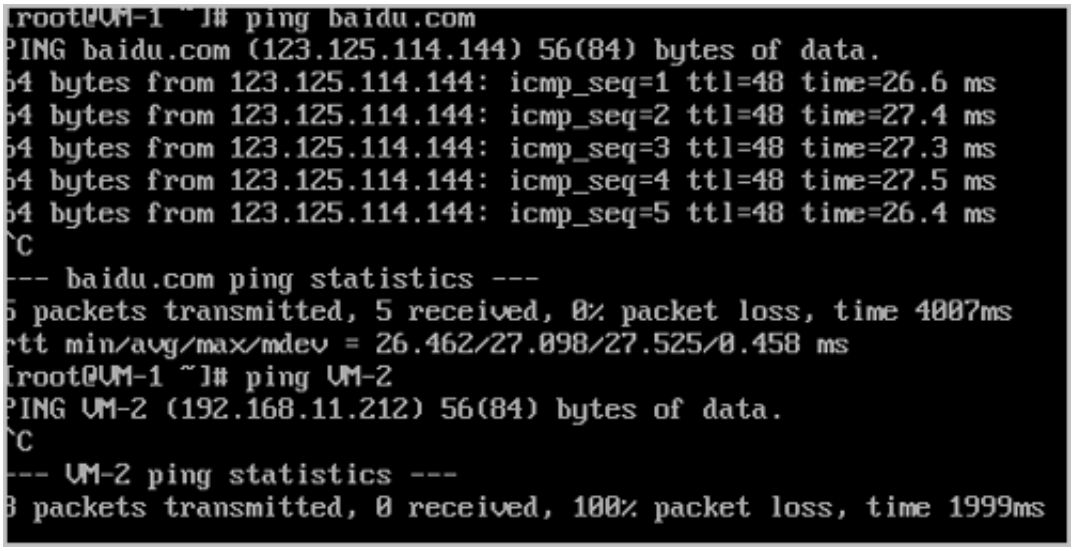
   注:

   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 *413: 验证VM-1网络连通性*所示：

   图 413: 验证VM-1网络连通性



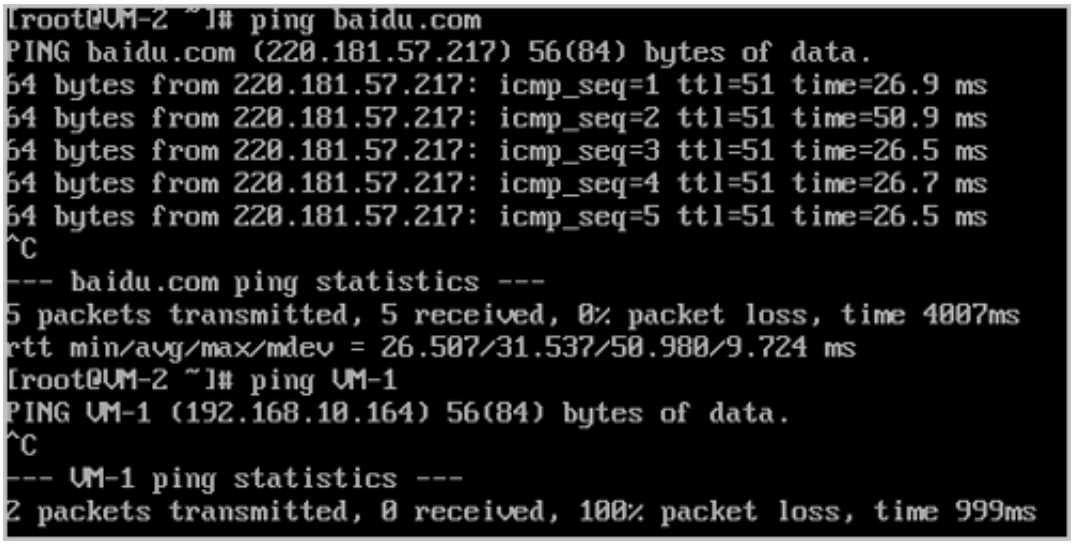
2. 登录VM-2，用*ping*命令验证网络连通性：

   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 *414: 验证VM-2网络连通性*所示：

   图 414: 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 *415: 创建路由表*所示：

图 415: 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 *416:* 添加两条自定义路由条目所示：

图 416: 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。

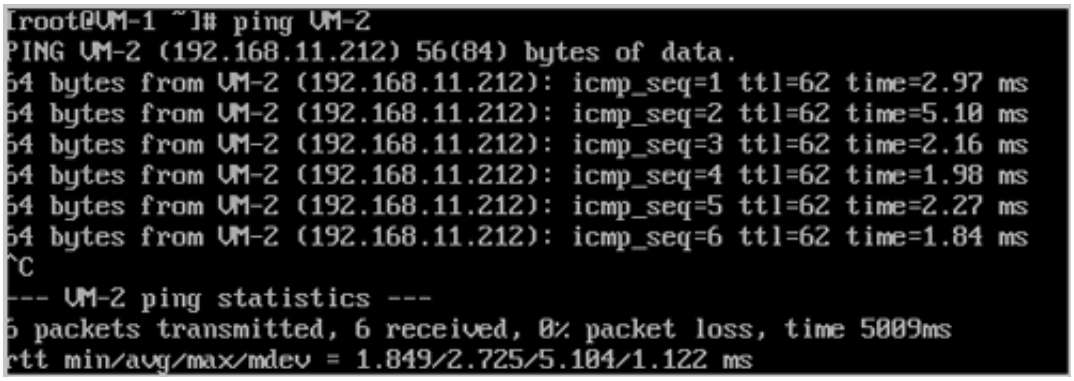
1. 登录VM-1，验证是否*ping*通VM-2：

   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 *417: VM-1 ping通 VM-2*所示：

   图 417: 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 *418: VM-2 ping通 VM-1*所示：

   图 418: 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。

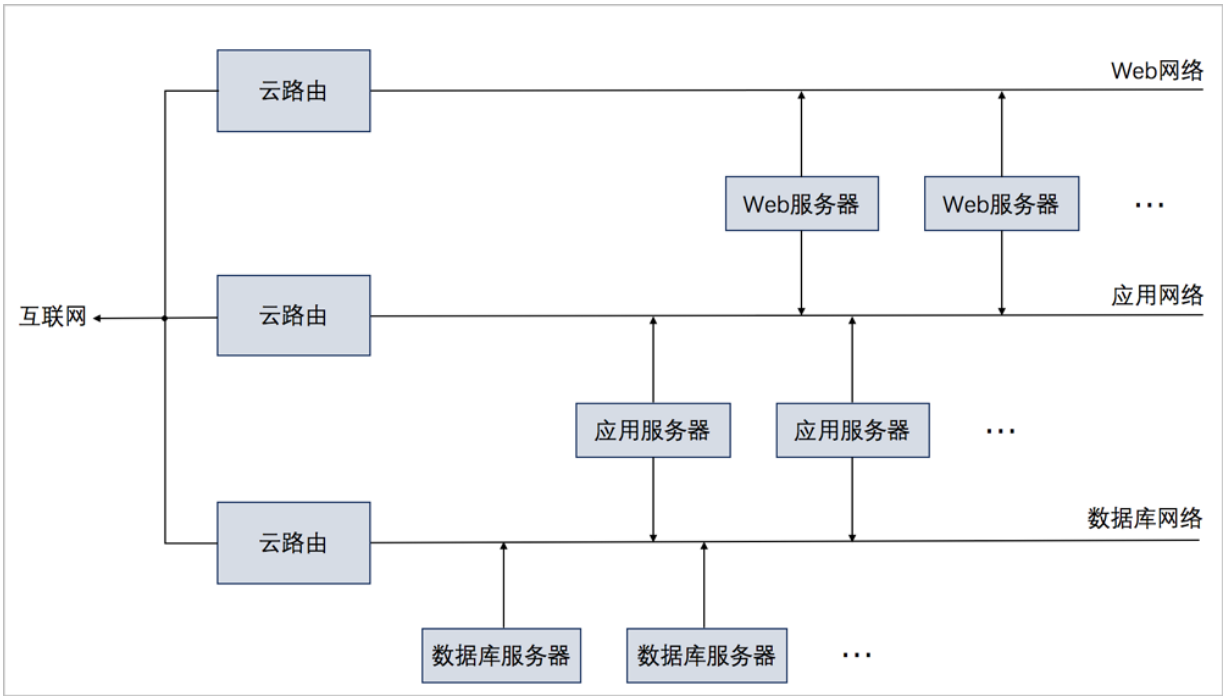
7.6.2.4.2 多层Web服务器

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 *419: 多层Web服务器网络架构图*所示：

图 419: 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 16: 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 17: 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 18: 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 19: 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 20: 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 *420:* 三个云路由网络所示：

图 420: 三个云路由网络

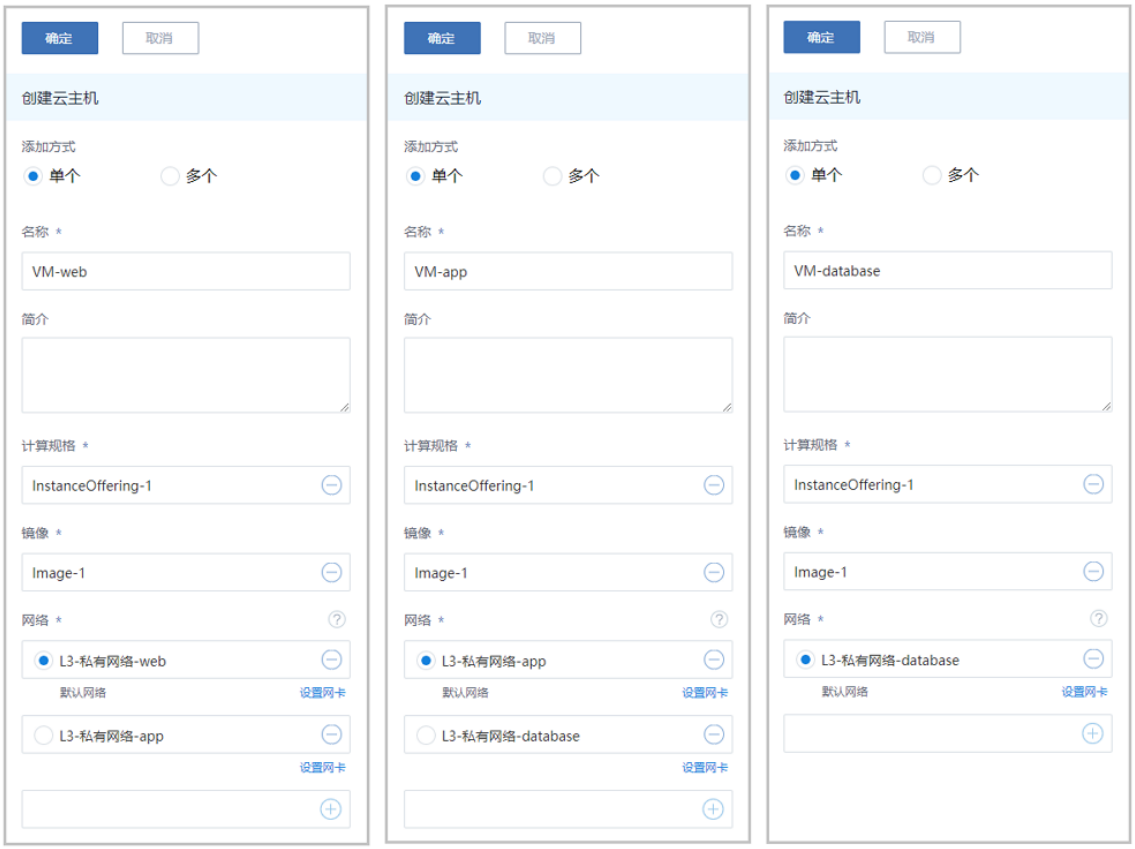
名称	网络类型	IP可用量/总额	CIDR	DHCP IP
L3-私有网络-database	云路由	250 / 253	192.168.12.0/24	192.168.12.196
L3-私有网络-app	云路由	250 / 253	192.168.11.0/24	192.168.11.187
L3-私有网络-web	云路由	251 / 253	192.168.10.0/24	192.168.10.93

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 *421:* 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 421: 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 *422: VM-web、VM-app、VM-database*所示：

图 422: 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 *423: 验证VM-web网络连通性*所示：

        图 423: 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 *424: 验证VM-app网络连通性*所示：

图 424: 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
```

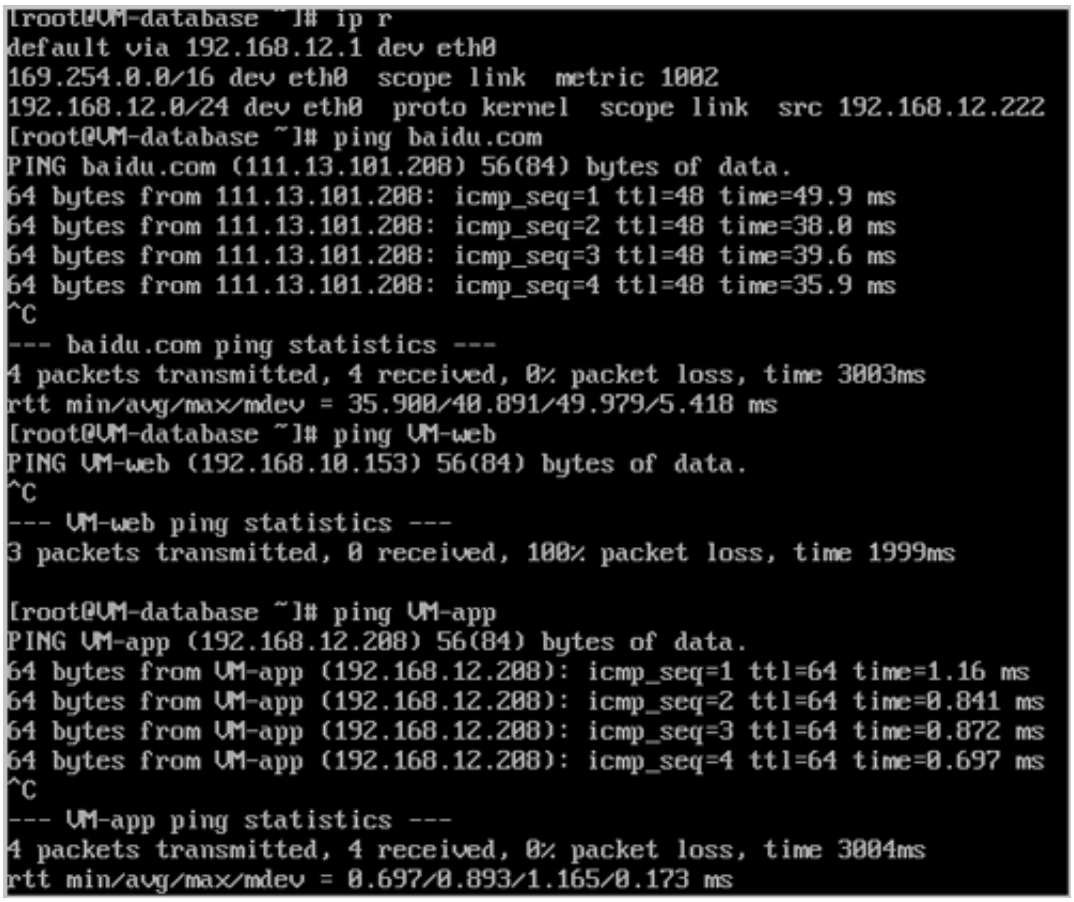
3. 登录VM-database，用*ping*命令验证网络连通性：

   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 *425: 验证VM-database网络连通性*所示：

图 425: 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。

7.6.2.4.3 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 21: 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 22: 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 23: 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 24: 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 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	*10.0.108.100~10.0.108.110*
子网掩码	*255.255.0.0*
网关	*10.0.0.1*

2. 管理网络

表 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	*192.168.29.30~192.168.29.40*
子网掩码	*255.255.255.0*
网关	*192.168.29.1*

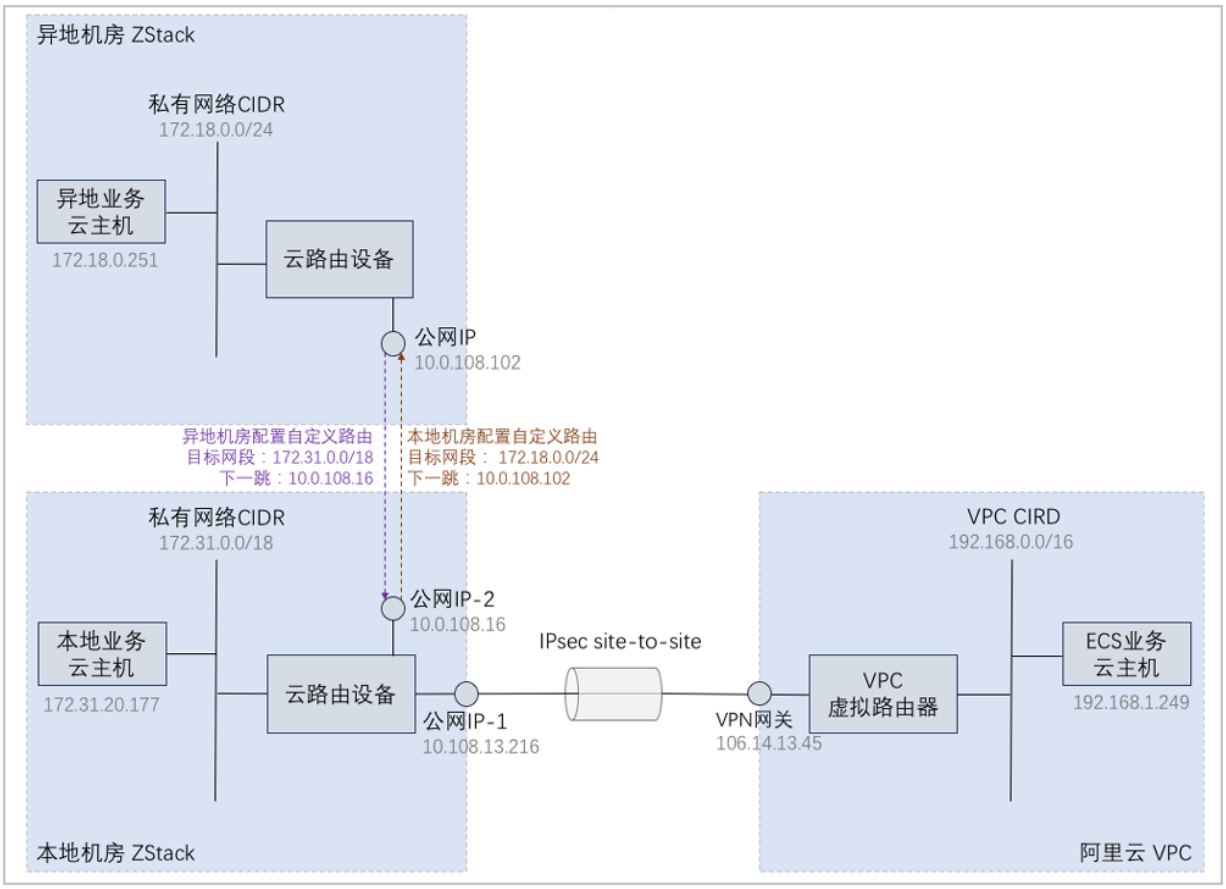
3. 私有网络

表 27: 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 *426:* 多公网场景网络架构图所示：

图 426: 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 *427:* 公有网络-用于与阿里云互通、图 *428:* 管理网络和图 *429:* 云路由网络所示：

   图 427: 公有网络-用于与阿里云互通

   图 428: 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 429: 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 *430: 本地业务云主机*所示：

   图 430: 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 *431: ECS业务云主机*所示：

   图 431: ECS业务云主机

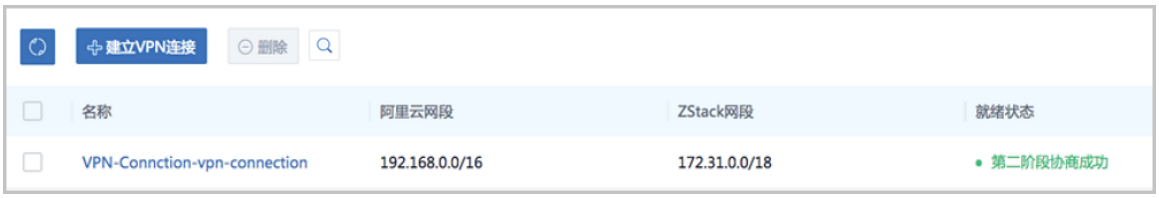
名称	ECS云主机ID	处理器	内存	私网IP	公网IP	付费信息	VPC	可用区	安全组	启用状态
ECS-业务-阿里云	i-uf6a0elu320ruf8...	1	1G	192.168.1.249		后付费	test-for-ipsec	华东 2 可用区 D	安全组-允许所有	运行中

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 *432: IPsec VPN隧道搭建完成*所示：

   图 432: IPsec VPN隧道搭建完成



注:

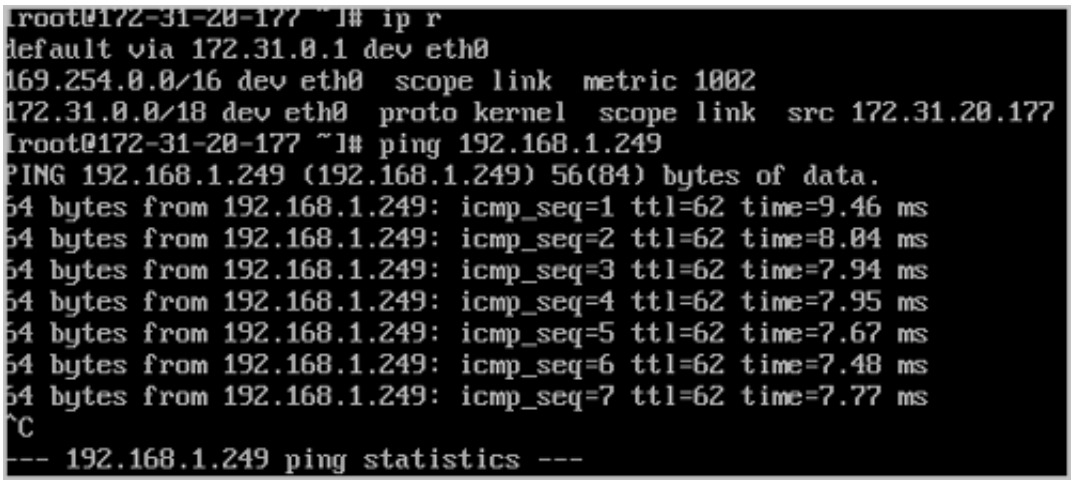
VPN连接的**就绪状态**显示为**第二阶段协商成功**，表示IPsec VPN隧道搭建完成，只有互通验证通过，IPsec VPN隧道才创建成功。

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 *433: 本地业务云主机 ping通 ECS业务云主机*所示：

   图 433: 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 *434: ECS业务云主机 ping通 本地业务云主机*所示：

   图 434: 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 *435:* 公有网络-用于与异地机房互通所示：

   图 435: 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 *436:* 云路由器加载多公网所示：

   图 436: 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 *437:* 公有网络-用于与本地机房互通、图 *438:* 管理网络和图 *439:* 云路由网络所示：

图 437: 公有网络-用于与本地机房互通

图 438: 管理网络

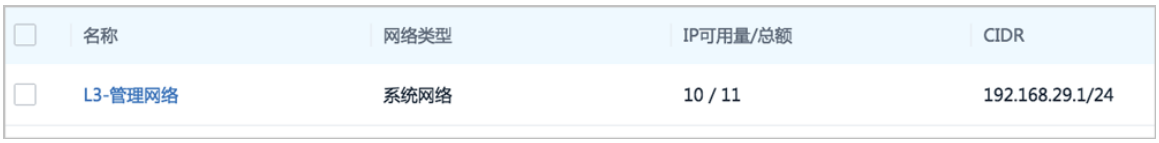


图 439: 云路由网络

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 *430:* 本地业务云主机所示：

图 440: 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 *441:* 本地机房配置路由所示：

   图 441: 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 *442:* 异地机房配置路由所示：

   图 442: 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 *443:* 本地业务云主机 *ping*通 异地业务云主机所示：

图 443: 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 *444:* 异地业务云主机 *ping*通 本地业务云主机所示：

图 444: 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。

7.6.2.4.4 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。

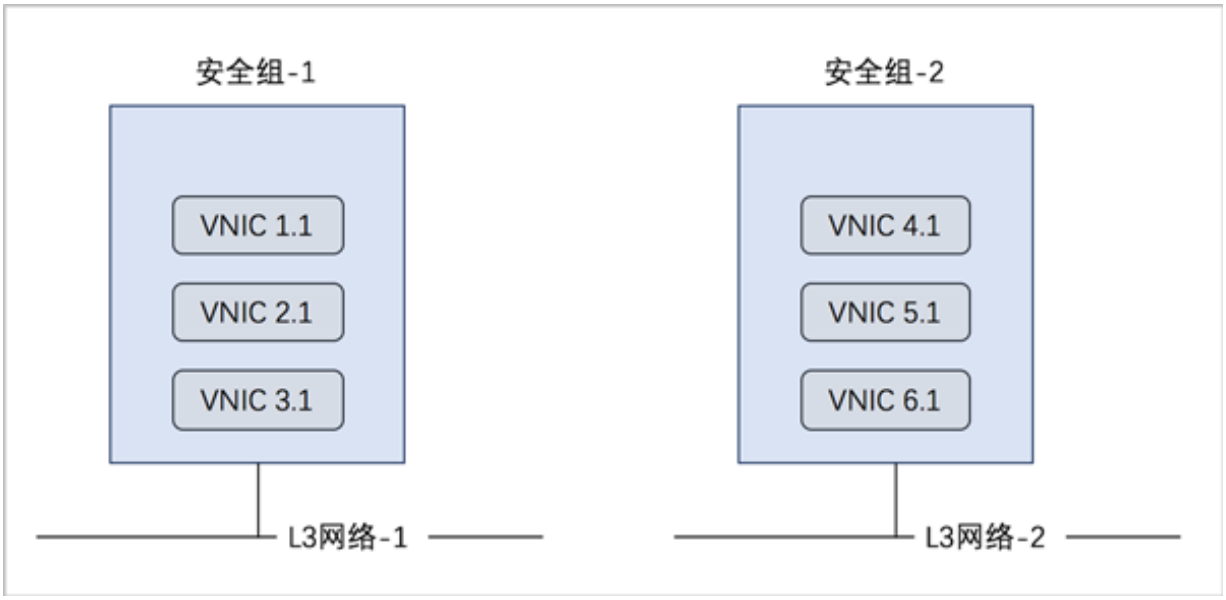
安全组规则：

- 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 *445:* 安全组所示：

图 445: 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。

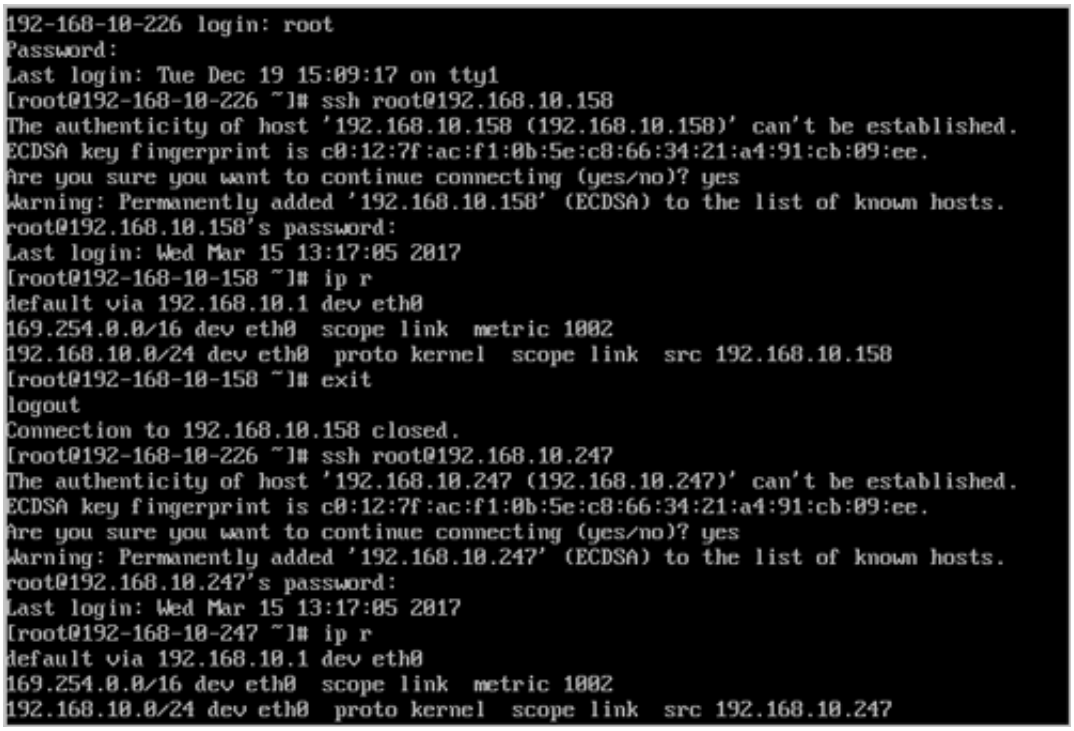
   创建的云主机如图 *446: VM-1、VM-2、VM-3*所示：

   图 446: 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 *447: SSH远程登录成功*所示：

图 447: 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 *448:* 创建安全组所示：

图 448: 创建安全组

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 *449:* 设置规则所示，点击**确定**，设置入方向规则。

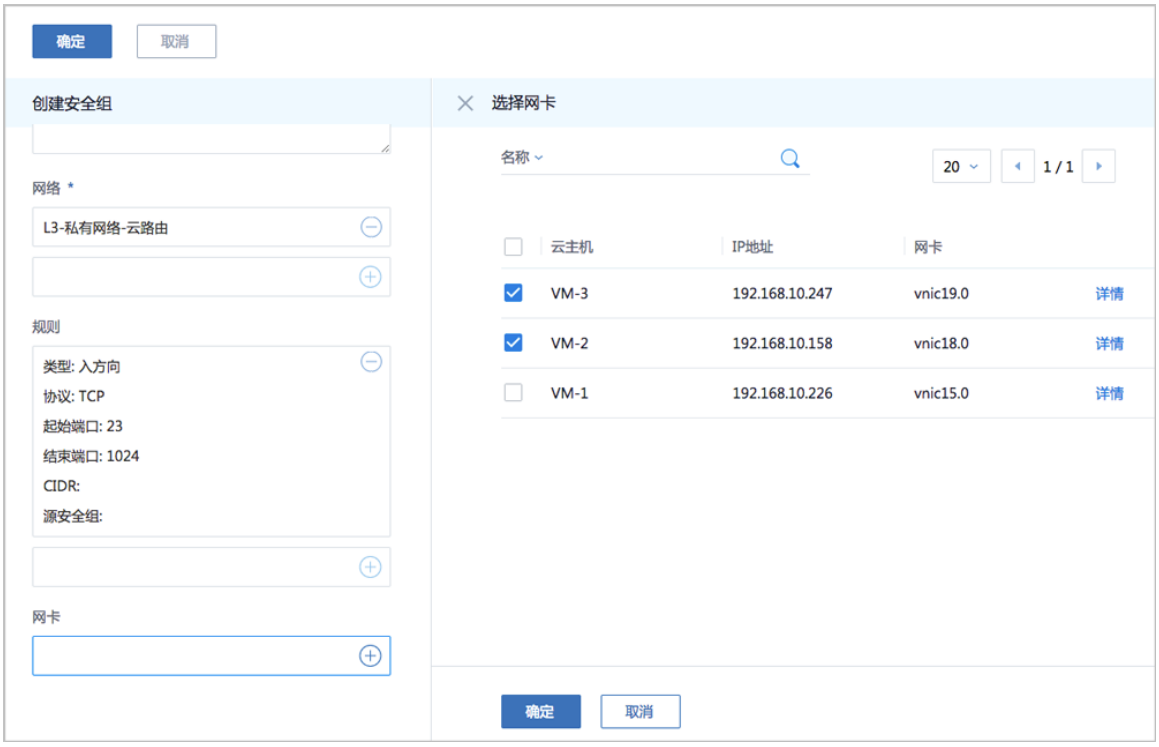
图 449: 设置规则

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 *450: 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 450: 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 *451: VM-1在端口23向VM-2发送信息*和图 *452: VM-2在端口23接收信息成功*所示：

   图 451: VM-1在端口23向VM-2发送信息

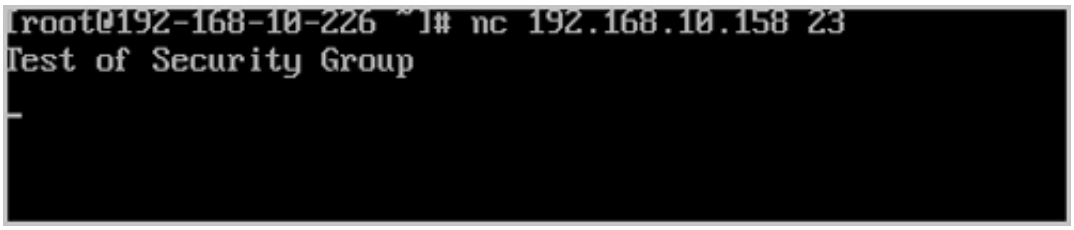
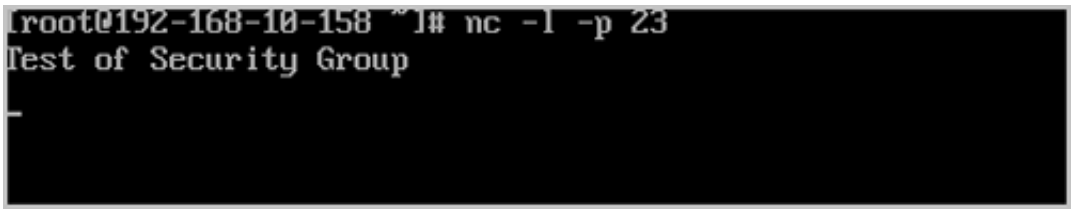


图 452: VM-2在端口23接收信息成功



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 *453:* 添加出方向规则所示：

图 453: 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 *454: 设置规则*所示，点击**确定**，设置出方向规则。

图 454: 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 *455: VM-2在端口21尝试连接VM-1失败*和图 *456: VM-1在端口21接收信息失败*所示：

   图 455: VM-2在端口21尝试连接VM-1失败

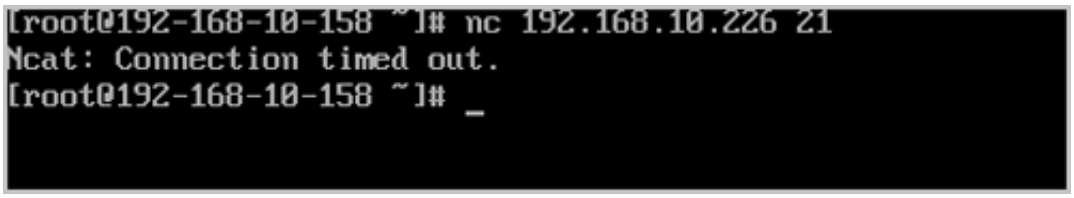


图 456: VM-1在端口21接收信息失败

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 *457: VM-2在端口23向VM-1发送信息*和图 *458: VM-1在端口23接收信息成功*所示：

   图 457: VM-2在端口23向VM-1发送信息

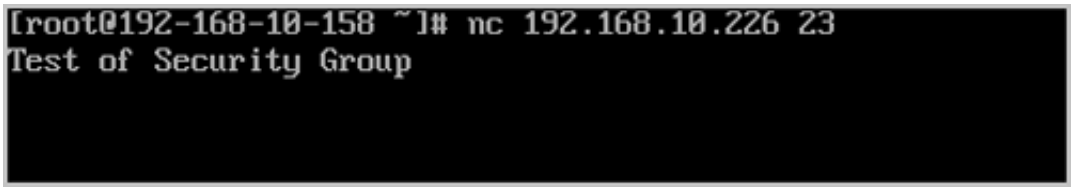


   图 458: VM-1在端口23接收信息成功

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。

7.6.2.4.5 弹性IP

前提条件

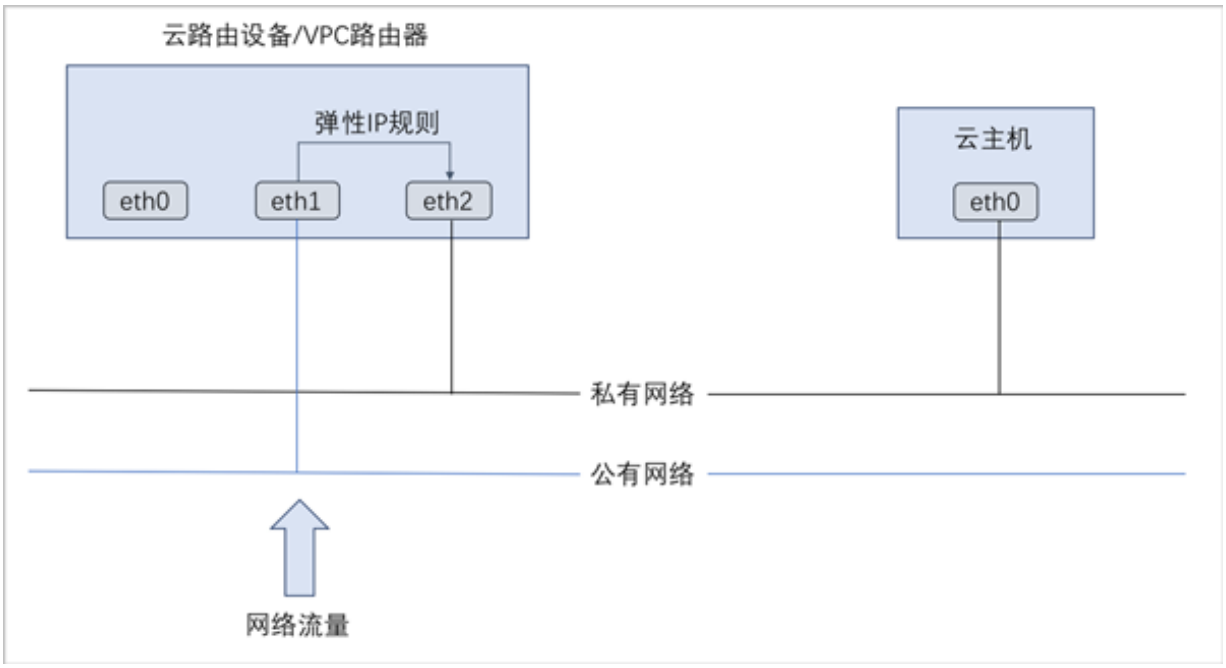
弹性IP（EIP）：定义了通过公有网络访问内部私有网络的方法。

- 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 *459: 云路由网络/VPC下弹性IP的应用场景*所示：

图 459: 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 *460: VM-1、VM-2*所示：

   图 460: 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 *461: 新建虚拟IP*所示：

    图 461: 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 *462: 已有虚拟IP*所示：

    图 462: 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 *463: 创建弹性IP*所示：

图 463: 创建弹性IP

b) 点击**确定**，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 *464: 选择VM-1*和图 *465: 将EIP-1绑定VM-1*所示：

图 464: 选择VM-1

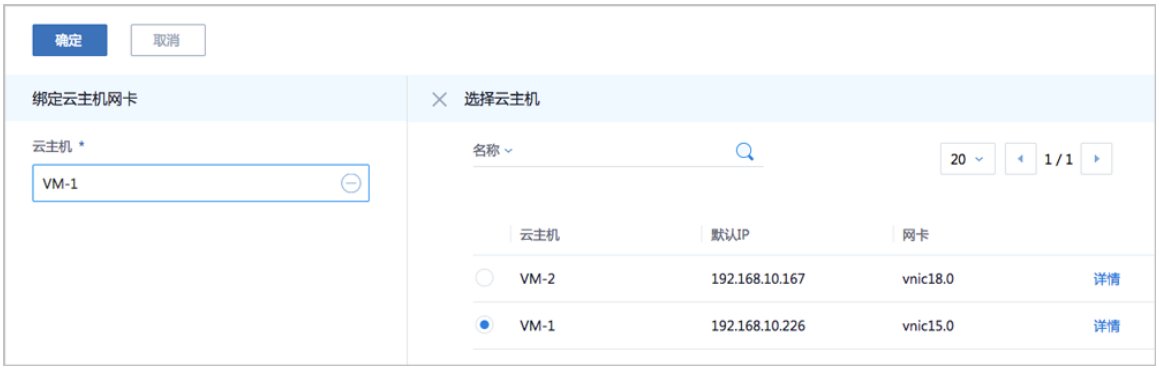
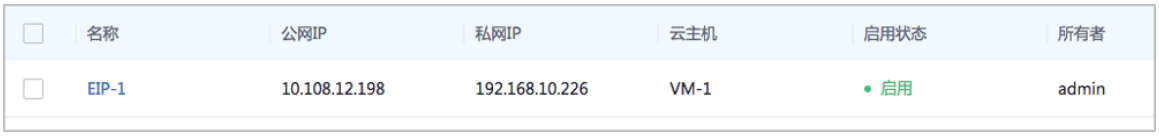


图 465: 将EIP-1绑定VM-1



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 *466: 通过EIP-1登录VM-1*所示：

图 466: 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 *467: 将EIP-1从VM-1解绑*所示：

图 467: 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 *468: 选择VM-2*和图 *469: 将EIP-1绑定VM-2*所示：

图 468: 选择VM-2

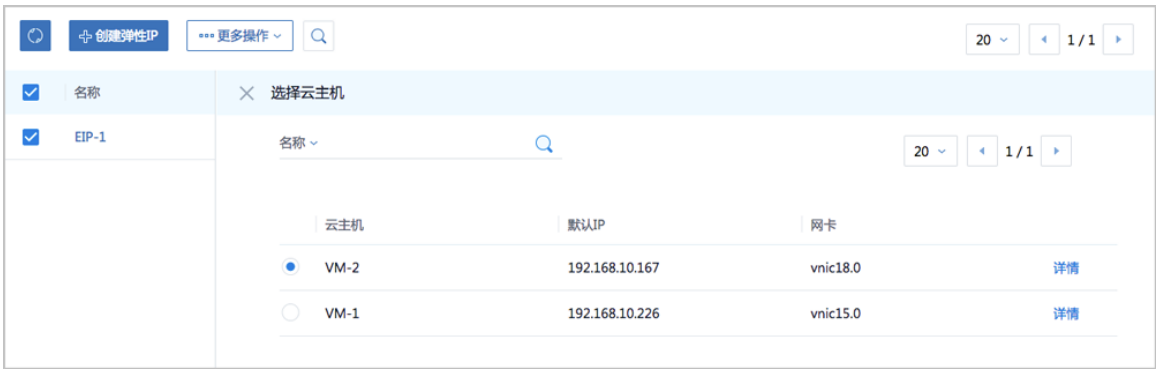
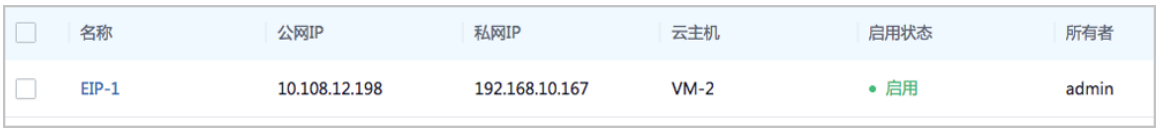


图 469: 将EIP-1绑定VM-2

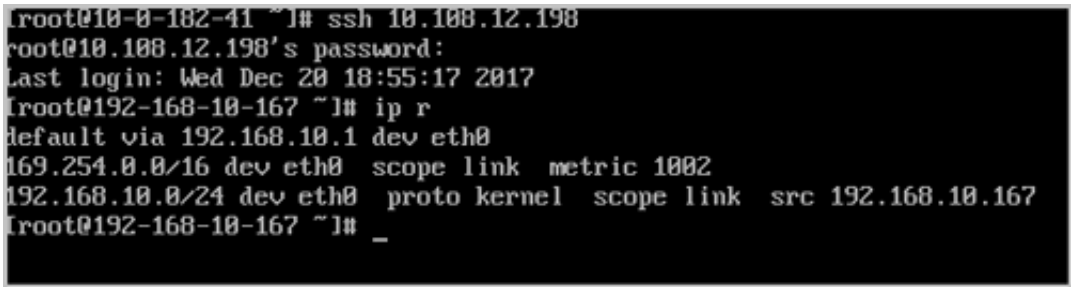


c) 通过EIP-1登录VM-2。

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 *466: 通过EIP-1登录VM-1*所示：

图 470: 通过EIP-1登录VM-2



至此，弹性IP的使用方法介绍完毕。

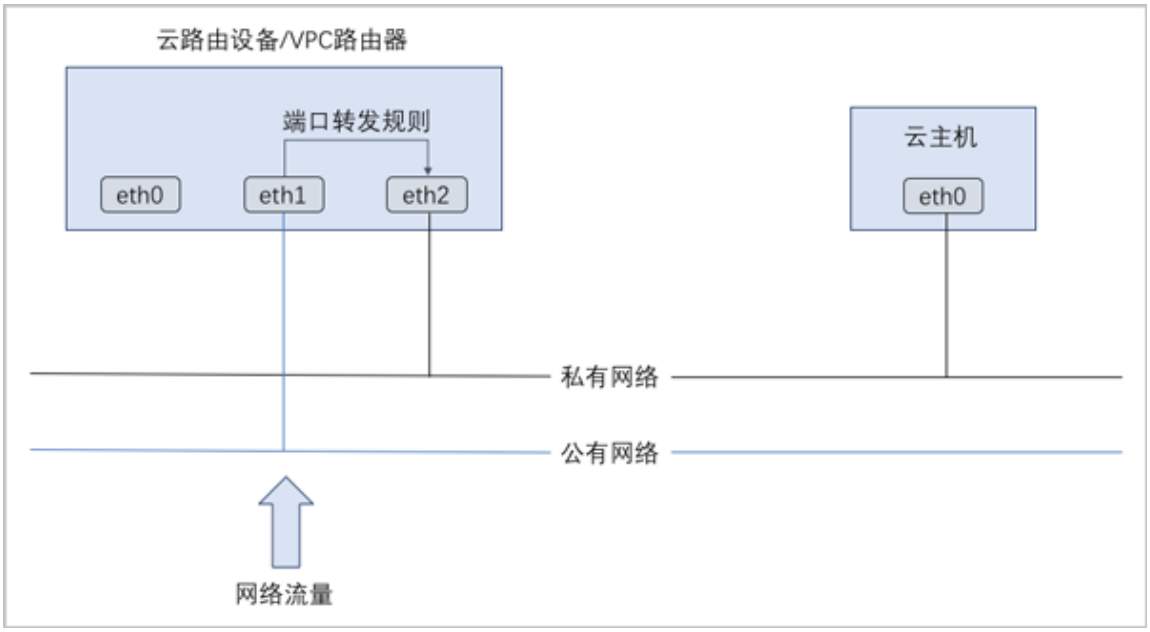
7.6.2.4.6 端口转发

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。

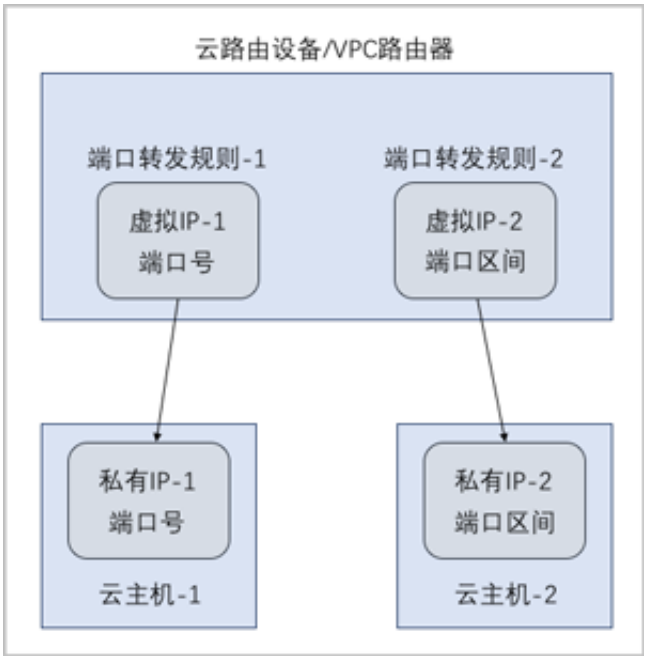
- 启用SNAT服务的私有网络中，云主机可访问外部网络但不能被外部网络所访问；使用端口转发规则，允许外部网络访问SNAT后面云主机的某些指定端口。
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *471: 端口转发*所示：

图 471: 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 *472: 虚拟IP-端口转发*所示：

图 472: 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 *473: VM-1、VM-2*所示：

   图 473: 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 *474: 新建虚拟IP*所示：

       图 474: 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 *475: 已有虚拟IP*所示：

  图 475: 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 *476:* 创建端口转发规则-指定端口所示：

图 476: 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 *477:* 创建端口转发规则-端口区间所示：

图 477: 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 *478:* 创建端口转发规则*PF-1*所示：

图 478: 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 *479: 选择VM-1*和图 *480: 将PF-1绑定VM-1*所示：

图 479: 选择VM-1

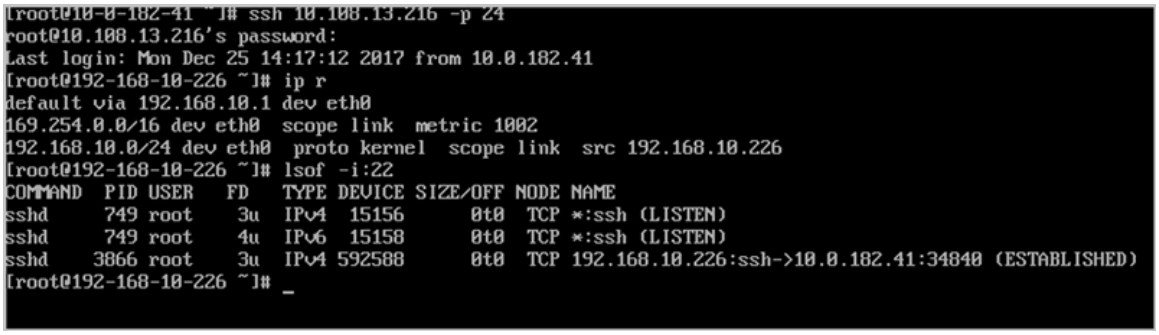
图 480: 将PF-1绑定VM-1

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 *481: 通过PF-1登录VM-1*所示：

图 481: 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 *482: 将PF-1从VM-1解绑*所示：

图 482: 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 *483: 选择VM-2*和图 *484: 将PF-1绑定VM-2*所示：

图 483: 选择VM-2

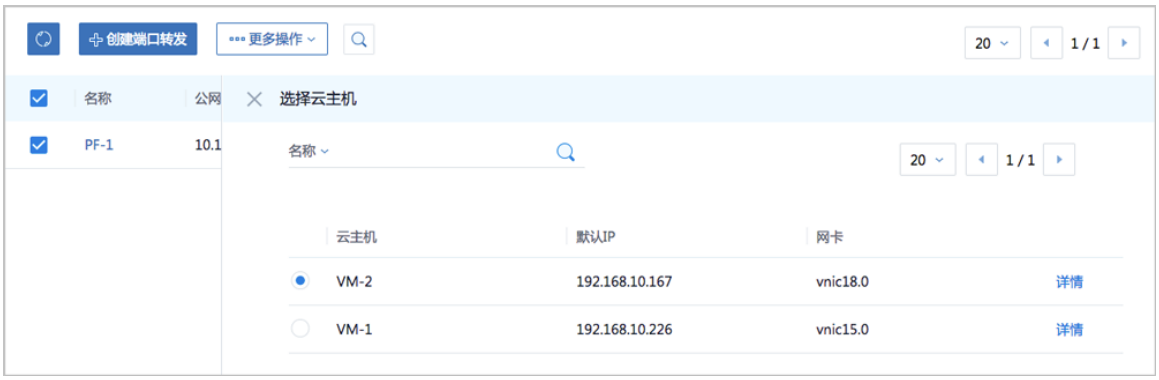


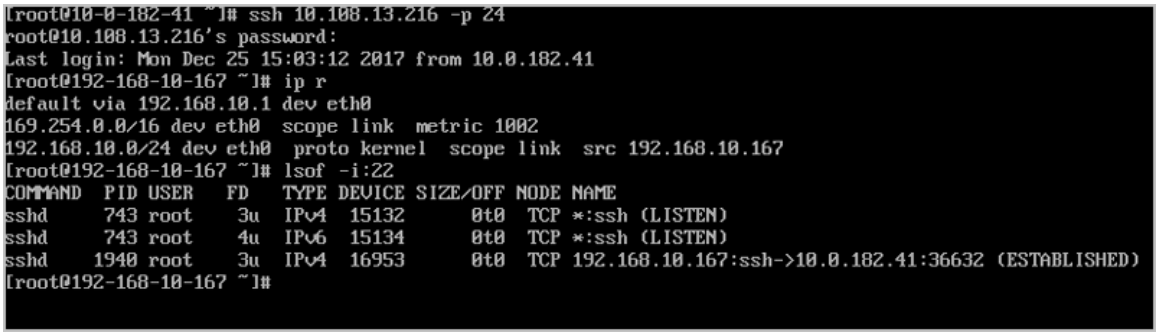
图 484: 将PF-1绑定VM-2

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 *485: 通过PF-1登录VM-2*所示：

图 485: 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 *478: 创建端口转发规则PF-1*所示：

图 486: 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 *487: 选择VM-1*和图 *488: 将PF-2绑定VM-1*所示：

图 487: 选择VM-1

图 488: 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 *489: 在源端口5900发送信息*和图 *490: 在VM-1的端口5900接收信息*所示：

图 489: 在源端口5900发送信息

图 490: 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。

7.6.2.4.7 负载均衡

前提条件

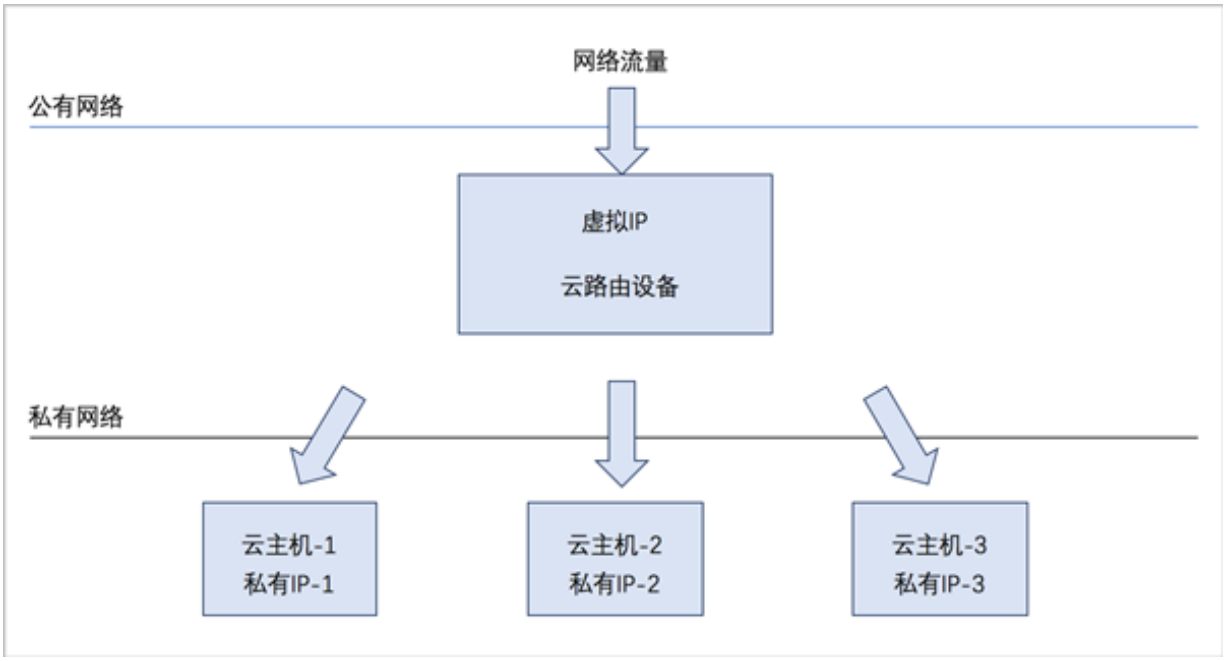
负载均衡（LB）：将公网地址的访问流量分发到一组后端的云主机， 并支持自动检测并隔离不可用的云主机，从而提高业务的服务能力和可用性。

- 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三种协议。

- 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 *491: 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 491: 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 *492: VM-1、VM-2、VM-3*所示：

图 492: 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 *493: 新建虚拟IP*所示：

    图 493: 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 *494: 已有虚拟IP*所示：

  图 494: 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 *495: 创建负载均衡器*所示：

图 495: 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
  - TCP：支持1-65535端口
  - HTTP：支持1-65535端口
  - HTTPS：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 *496:* 添加监听器所示：

图 496: 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
  - **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
  - **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 *497: 添加监听器-高级选项*所示：

图 497: 添加监听器-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 *498:* 进入监听器详情页所示：

   图 498: 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 *499: 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 499: 绑定云主机网卡到监听器

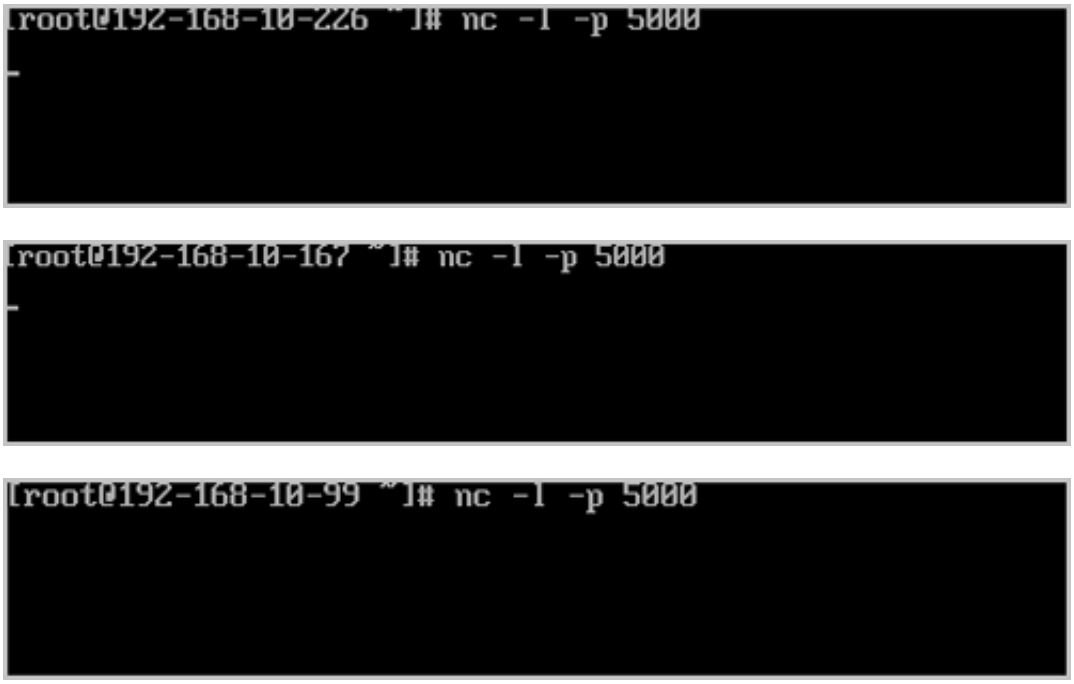
6. 负载均衡器以默认的轮询方式向三台云主机发送信息。

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

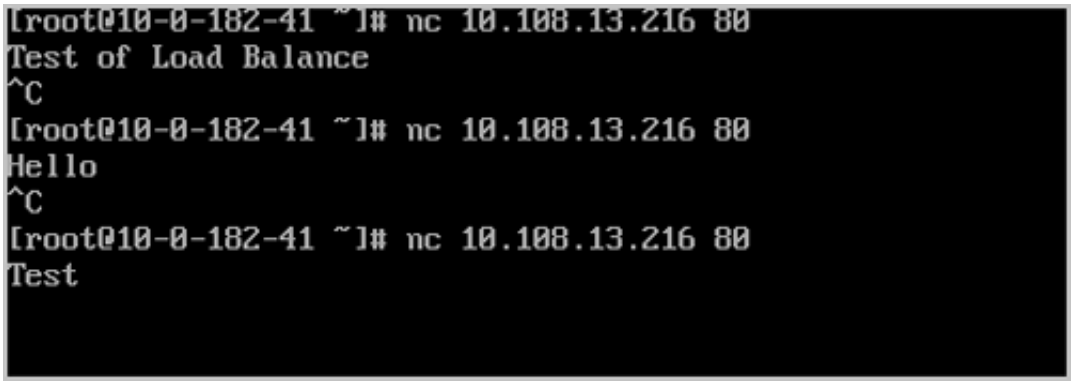
1. 开启VM-1、VM-2、VM-3的5000端口侦听，如图 *500:* 开启三台云主机的*5000*端口侦听所示：

图 500: 开启三台云主机的5000端口侦听



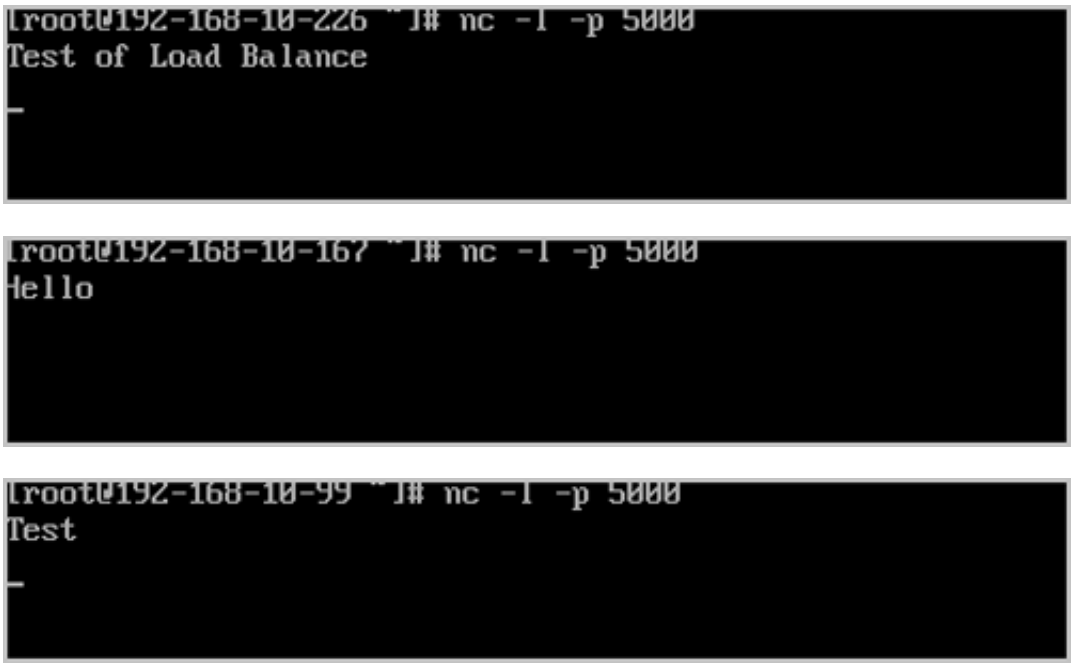
2. 向负载均衡器公网IP的80端口发送三条信息，如图 *501:* 向负载均衡器公网*IP*的*80*端口发送三条信息所示：

图 501: 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 *502:* 三台云主机的*5000*端口分别接收到一条信息所示：

图 502: 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。

7.6.2.4.8 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 28: 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 29: 管理网络配置信息

管理网络	配置信息
网卡	em02
VLAN ID	非VLAN

管理网络	配置信息
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 30: 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 31: 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 32: 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*

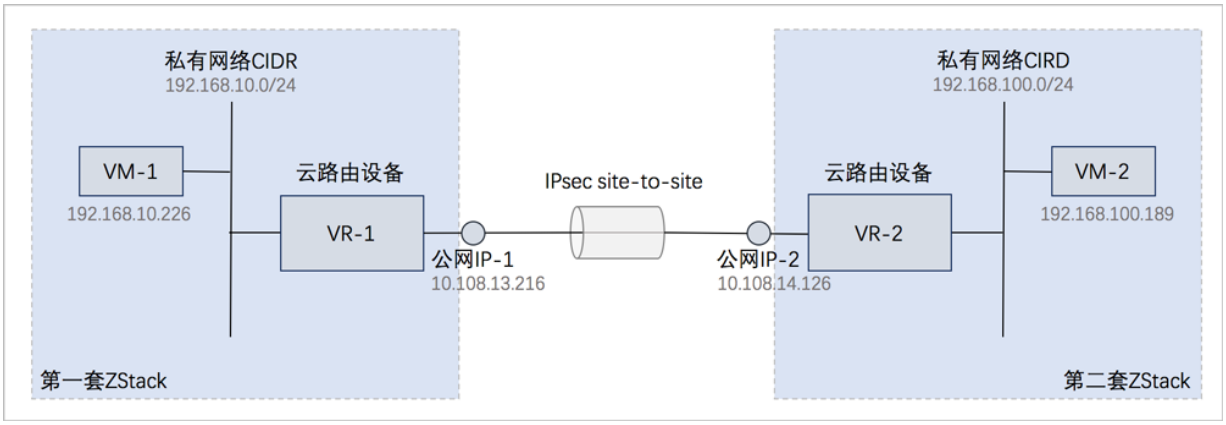
3. 私有网络

表 33: 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 *503: IPsec隧道网络架构图*所示：

图 503: 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 *504: VM-1*所示：

图 504: 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 *505: VM-2*所示：

   图 505: 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 *506: VM-1尝试连通VM-2失败*所示：

     图 506: 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 *507: 新建虚拟IP*所示：

    图 507: 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 *508: 已有虚拟IP*所示：

    图 508: 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 *509: 创建IPsec隧道-1*所示：

图 509: 创建IPsec隧道-1

b) IPsec隧道-1创建完成。

如图 *510: IPsec隧道-1*所示：

图 510: 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 *511: 创建IPsec隧道-2*所示：

图 511: 创建IPsec隧道-2

b）IPsec隧道-2创建完成。

如图 *512: IPsec隧道-2*所示：

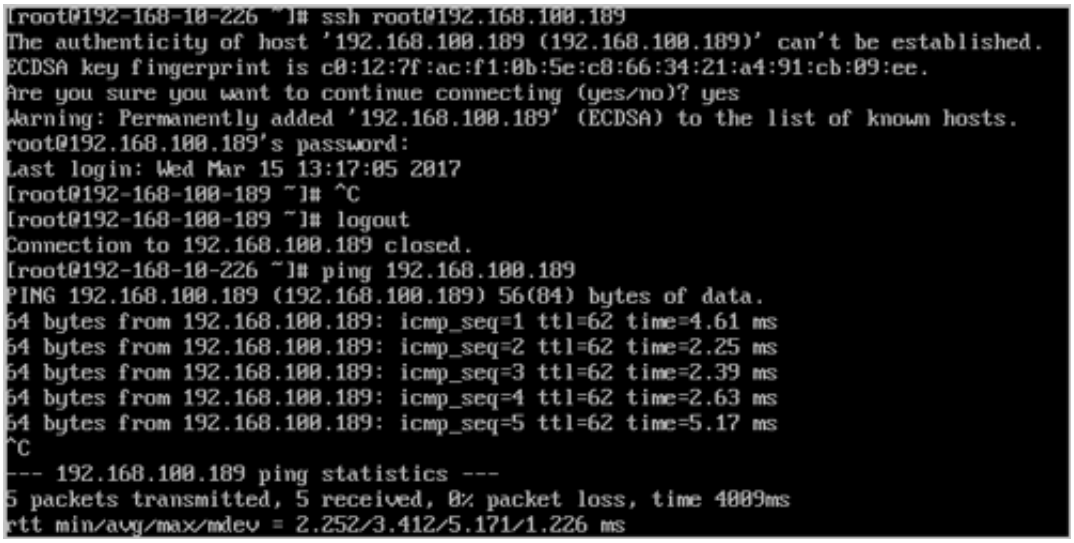
图 512: IPsec隧道-2

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 *513: VM-1成功连通VM-2*所示：

     图 513: 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。

7.6.3 专有网络VPC使用教程

7.6.3.1 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。

7.6.3.2 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、主存储等基本硬件资源的添加，以及计算规格的创建。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。

本教程将详细介绍专有网络VPC的基本部署。

7.6.3.3 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 34: 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*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

表 35: 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 36: 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*

4. VPC网络2

表 37: 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*

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 *34:* 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 *514:* 创建*L2*-公有网络所示，点击**确定**，创建L2-公有网络。

   图 514: 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 *34:* 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
   - **DHCP服务**：选择是否需要DHCP服务
   - **添加网络段**：选择IP范围
   - **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*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *515:* 创建*L3*-公有网络所示，点击**确定**，创建L3-公有网络。

图 515: 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
添加网络段
方法
IP 范围
CIDR
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
添加DNS
DNS
223.5.5.5

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 *35:* 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 *516:* 创建*L2*-管理网络所示，点击**确定**，创建L2-管理网络。

图 516: 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 *35:* 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
   - **DHCP服务**：选择是否需要DHCP服务
   - **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*
   - **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

   如图 *517:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

   图 517: 创建L3-管理网络

确定
取消
创建系统网络
名称 *
L3-管理网络
简介
二层网络 *
L2-管理网络
添加网络段
方法
IP 范围
CIDR
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
添加DNS
DNS
223.5.5.5

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*官方网站上找到最新的云路由镜像下载地址。

   - 文件名称：zstack-vrouter-2.5.1.qcow2
   - 下载地址：点击这里查看

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 *518:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 518: 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 *519:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 519: 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 *520: 创建VPC路由器*所示，点击**确定**，创建VPC路由器。

图 520: 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 *36: 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 *521: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 521: 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 36: 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

- **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
- **DHCP服务**：选择是否需要DHCP服务
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.10.0/24*

注: 网络段不可重叠。

如图 *522: 创建VPC网络1*所示，点击**确定**，创建VPC网络1。

图 522: 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）。

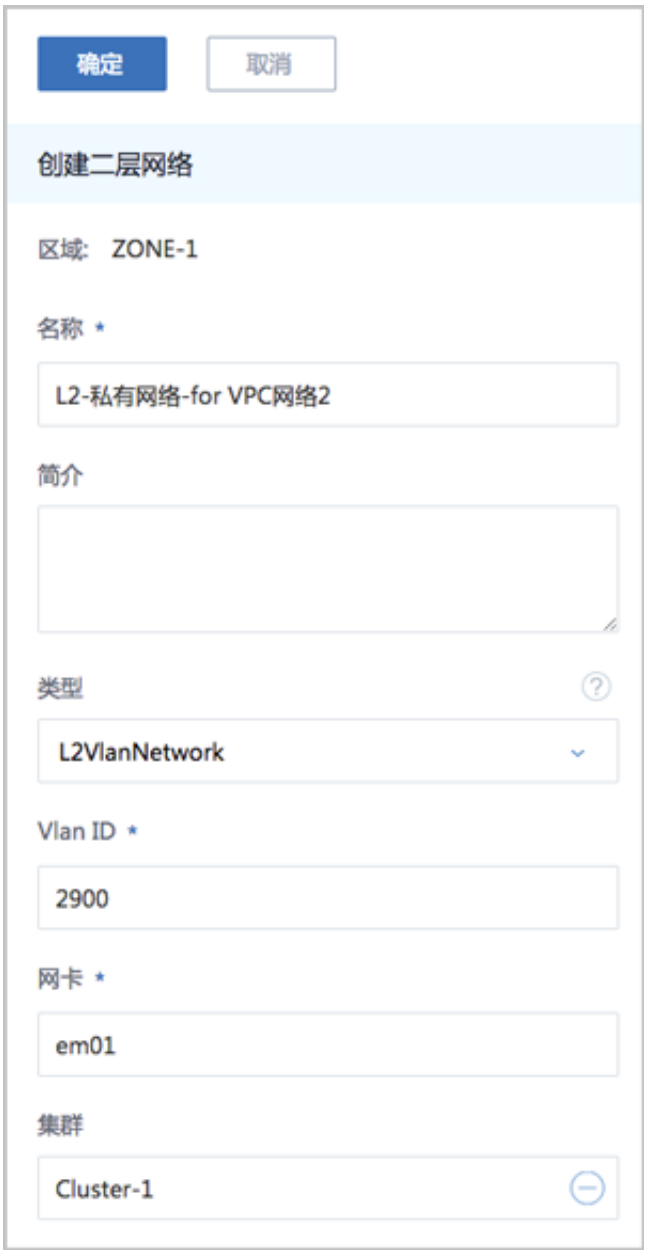
在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *37: VPC*网络2配置信息填写如下：

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

图 523: 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 *37: 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
- **DHCP服务**：选择是否需要DHCP服务
- **添加网络段**：选择CIDR
- **CIDR**：*192.168.11.0/24*

注: 网络段不可重叠。

如图 *524: 创建VPC网络2*所示，点击**确定**，创建VPC网络2。

图 524: 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**：从VPC网络列表中选择已创建的VPC网络1

如图 *525: 创建私有云云主机1*所示，点击 **确定**，创建私有云云主机1。

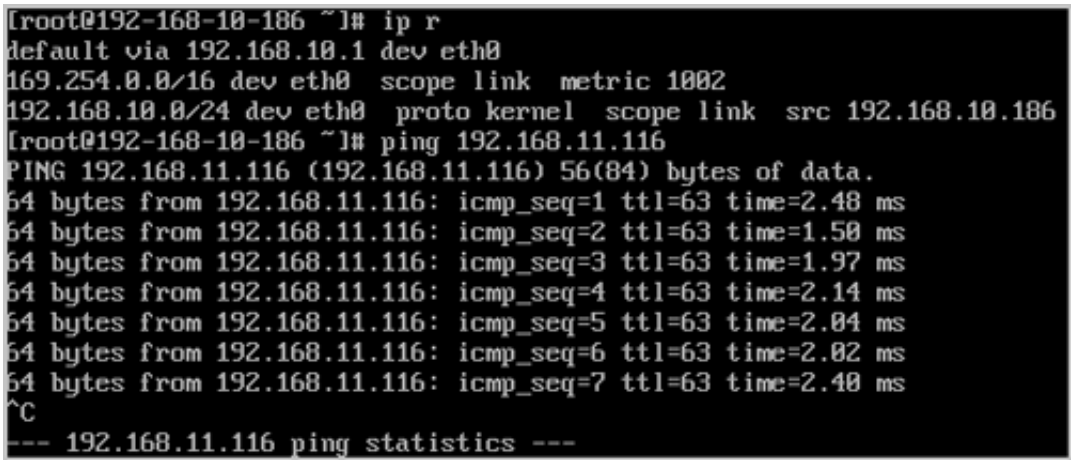
图 525: 创建私有云云主机1

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。

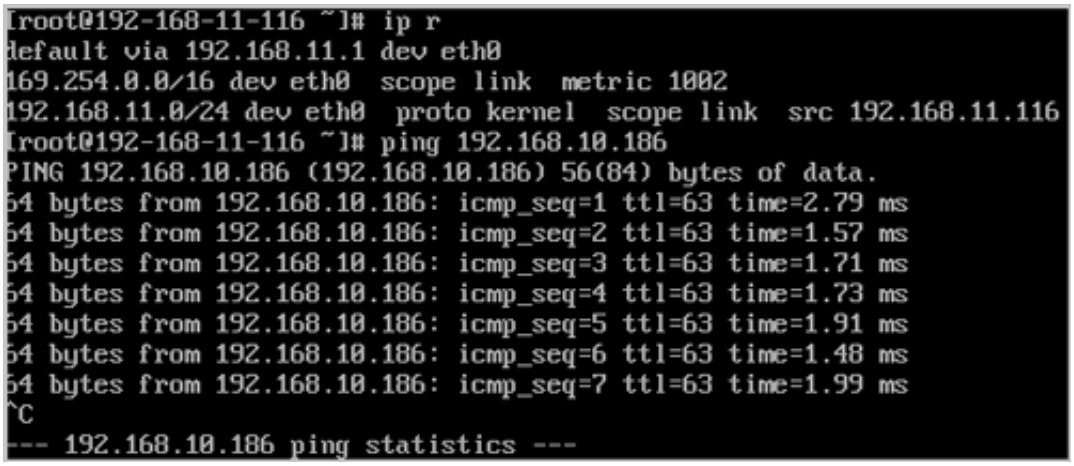
1. 登录VM-1，检查是否能够ping通VM-2，如图 *526: VM-1 ping通 VM-2*所示：

图 526: VM-1 ping通 VM-2



2. 登录VM-2，检查是否能够ping通VM-1，如图 *527: VM-2 ping通 VM-1*所示：

图 527: 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。

7.6.3.4 应用场景

专有网络VPC可用于以下典型应用场景：

- 多层Web服务器
- 安全组
- 弹性IP

- 端口转发
- 负载均衡
- IPsec隧道

7.6.3.4.1 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 38: 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-VPC网络提供多租户隔离的实践。

搭建多租户隔离VXLAN-VPC网络的基本流程：

1. 在admin账户下创建两个普通账户，账户A和账户B。
2. 在admin账户下创建二层公有网络，并加载此二层网络到相应集群。
3. 在admin账户下创建三层公有网络。
4. 在admin账户下创建二层管理网络，并加载此二层网络到相应集群。
5. 在admin账户下创建三层管理网络，用于与物理资源通信，例如，物理机、主存储、镜像服务器等。
6. 在admin账户下添加云路由镜像。
7. 在admin账户下创建云路由规格，并共享给账户A和账户B。
8. 在admin账户下创建VXLAN网络池，加载到相应集群，并共享给账户A和账户B。

9. 基于云路由规格在账户A和账户B分别创建一个VPC路由器。例如：VPC路由器-A和VPC路由器-B。
10. 基于VXLAN网络池在账户A和账户B分别创建两个VXLAN网络（虚拟的二层网络），例如：L2-VXLAN-A1和L2-VXLAN-A2、L2-VXLAN-B1和L2-VXLAN-B2。
11. 使用四个VXLAN网络分别在各自账户创建VPC网路，例如：VPC网络-A1和VPC网络-A2、VPC网络-B1和VPC网络-B2。
12. 使用四个VPC网络分别在各自账户创建一个云主机，例如：VM-A1、VM-A2、VM-B1和VM-B2。
13. 验证四台云主机之间的连通性。
14. 从admin账户共享三层公有网络给账户A和账户B。
15. 给VM-A1和VM-B1添加路由表。
16. 验证云主机VM-A1和VM-B1之间的连通性。

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 39: 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	*10.151.10.100~10.151.10.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

表 40: 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	*192.168.28.100~192.168.28.200*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

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 41: VXLAN网络池配置信息

VXLAN网络池	配置信息
Vni范围	20-1200
VTEP CIDR	192.168.28.1/24

4. VPC网络-A1

表 42: VPC网络-A1配置信息

VPC网络	配置信息
网卡	em01
IP CIDR	*192.168.21.0/24*

5. VPC网络-A2

表 43: VPC网络-A2配置信息

VPC网络	配置信息
网卡	em01

VPC网络	配置信息
IP CIDR	*192.168.22.0/24*

6. VPC网络-B1

表 44: VPC网络-B1配置信息

VPC网络	配置信息
网卡	em01
IP CIDR	*192.168.23.0/24*

7. VPC网络-B2

表 45: VPC网络-B2配置信息

VPC网络	配置信息
网卡	em01
IP CIDR	*192.168.24.0/24*

以下介绍搭建VXLAN-VPC网络的实践步骤。

操作步骤

1. 在admin账户下创建两个普通账户，账户A和账户B。

   在ZStack私有云界面，点击**平台管理** > **用户管理** > **账户**按钮，在**账户**页面点击**创建账户**按钮，在**创建账户**窗口，可参考以下示例输入相应内容：

   - **名称**：设置账户名称，不区分大小写，例如：账户A
   - **简介**：可选项，可留空不填
   - **新密码**：设置登录该账户的密码
   - **确认密码**：重复输入密码，避免误输

   如图 *528:* 创建账户所示，点击**确定**按钮，完成账户A创建。

   图 528: 创建账户

同理，创建账户B，创建完成后如图 *529:* 账户创建完成所示：

图 529: 账户创建完成

2. 在admin账户下创建二层公有网络，并加载此二层网络到相应集群。

   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 *39:* 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 *530: 创建L2-公有网络*所示，点击**确定**，创建L2-公有网络。

图 530: 创建L2-公有网络

3. 在admin账户下创建三层公有网络。

   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 39: 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
- **DHCP服务**：选择是否需要DHCP服务
- **添加网络段**：选择IP范围
- **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*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *531:* 创建*L3-*公有网络所示，点击**确定**，创建L3-公有网络。

图 531: 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
添加网络段
方法
IP 范围
CIDR
起始IP *
10.151.10.100
结束IP *
10.151.10.200
子网掩码 *
255.0.0.0
网关 *
10.0.0.1
添加DNS
DNS
223.5.5.5

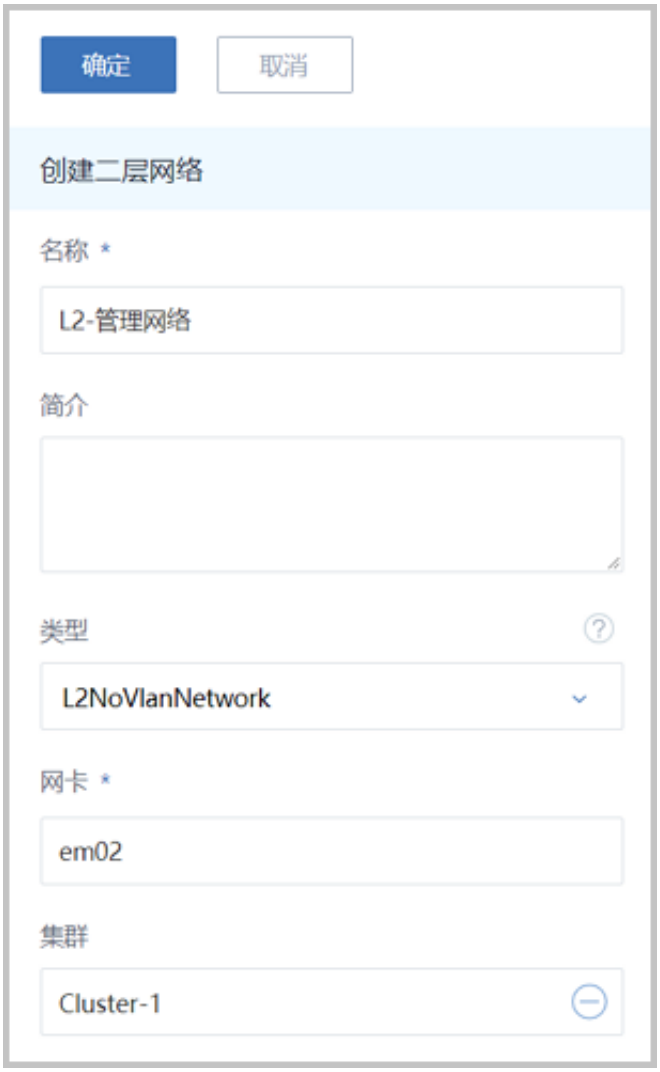
4. 在admin账户下创建二层管理网络，并加载此二层网络到相应集群。

   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 *40:* 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 *532:* 创建*L2*-管理网络所示，点击**确定**，创建L2-管理网络。

图 532: 创建L2-管理网络



5. 在admin账户下创建三层管理网络，用于与物理资源通信，例如，物理机、主存储、镜像服务器等。

   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 *40:* 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
   - **DHCP服务**：选择是否需要DHCP服务
   - **添加网络段**：选择IP范围
   - **起始IP**：*192.168.28.100*
   - **结束IP**：*192.168.28.200*
   - **子网掩码**：*255.255.255.0*
   - **网关**：*192.168.28.1*
   - **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

   如图 *533:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

   图 533: 创建L3-管理网络

确定
取消
创建系统网络
名称 *
L3-管理网络
简介
二层网络 *
L2- 管理网络
添加网络段
方法
IP 范围
CIDR
起始IP *
192.168.28.100
结束IP *
192.168.28.200
子网掩码 *
255.255.255.0
网关 *
192.168.28.1
添加DNS
DNS
223.5.5.5

6. 在admin账户下添加云路由镜像。

   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*官方网站上找到最新的云路由镜像下载地址。

        - 文件名称：zstack-vrouter-2.5.1.qcow2
        - 下载地址：点击这里查看

     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。

7. 在admin账户下创建云路由规格，并共享给账户a和账户b。

   a) 在admin账户下创建云路由规格。

   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 *534:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 534: 创建云路由规格

b) 将云路由规格共享给账户A和账户B。

在ZStack私有云主菜单，点击**网络资源** > **路由资源** > **云路由规格**按钮，在**云路由规格**页面点击云路由规格名称，点击**共享** > **操作** > **共享**按钮，选择账户A和账户B，点击**确定**完成共享。如图 *535: 共享云路由规格*所示：

图 535: 共享云路由规格

8. 在admin账户下创建VXLAN网络池，加载到相应集群，并共享给账户A和账户B。

   a) 在admin账户下创建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 41: 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1-16777214。
   - **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192.168.28.1/24

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，ZStack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 *536: 创建VXLAN网络池*所示，点击**确定**，创建VXLAN网络池。

图 536: 创建VXLAN网络池

b) 将VXLAN网络池共享给账户A和账户B。

在ZStack私有云主菜单，点击**网络资源** > **二层网络资源** > **VXLAN Pool**按钮，在**VXLAN Pool**页面点击VXLAN网络池名称，点击**共享** > **操作** > **共享**按钮，选择账户A和账户B，点击**确定**完成共享。如图 *537: 共享VXLAN网络池*所示：

图 537: 共享VXLAN网络池

9. 基于云路由规格在账户A和账户B分别创建一个VPC路由器。例如：VPC路由器-A和VPC路由器-B。

   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，例如：VPC路由器-A
   - **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 *538: 创建VPC路由器-A*所示，点击**确定**按钮，完成VPC路由器-A创建。

   图 538: 创建VPC路由器-A

同理，在账户B，创建VPC路由器-B。

10.基于VXLAN网络池在账户A和账户B分别创建两个VXLAN网络（虚拟的二层网络），例如：L2-VXLAN-A1和L2-VXLAN-A2、L2-VXLAN-B1和L2-VXLAN-B2。

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，可参考以下示例输入相应内容：

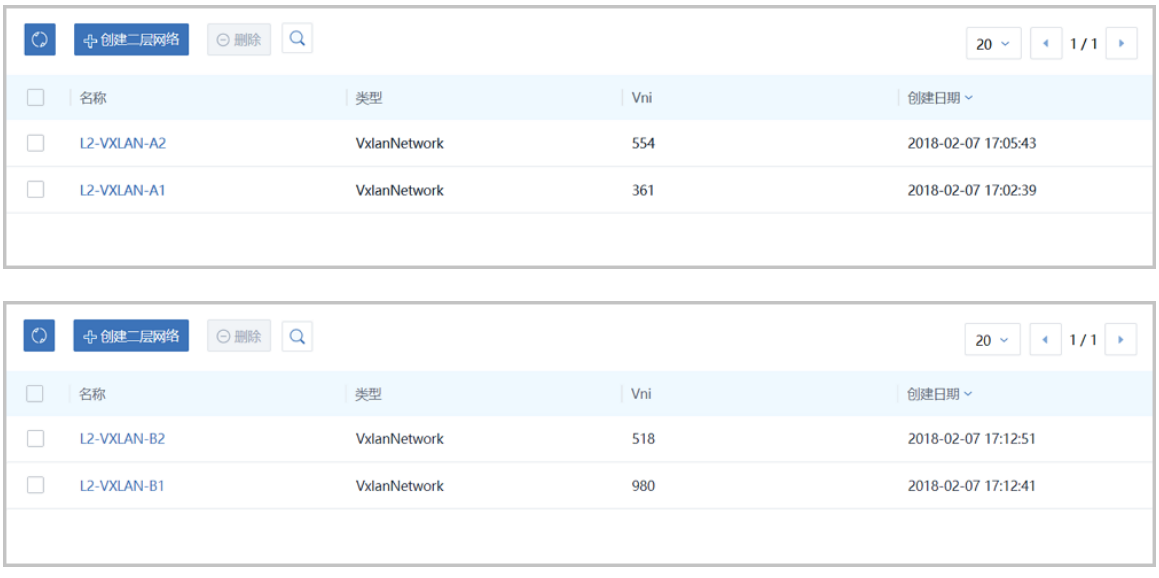
- **名称**：设置VXLAN网络名称，例如：L2-VXLAN-A1
- **简介**：可选项，可留空不填
- **类型**：选择VxlanNetwork
- **VXLAN网络池**：选择已创建的VXLAN网络池

如图 *539: 创建L2-VXLAN-A1*所示，点击**确定**，创建L2-VXLAN-A1。

图 539: 创建L2-VXLAN-A1

同理，创建L2-VXLAN-A2、L2-VXLAN-B1和L2-VXLAN-B2。VXLAN网络，创建完成后如图 *540: VXLAN网络*所示：

图 540: VXLAN网络



11. 使用四个VXLAN网络分别在各自账户创建VPC网路，例如：VPC网络-A1和VPC网络-A2、VPC网络-B1和VPC网络-B2。

    在ZStack私有云界面，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 *42: VPC网络-A1*配置信息填写如下：

    - **名称**：设置VPC网络名称，例如：VPC网络-A1
    - **简介**：可选项，可留空不填
    - **二层网络**：选择已创建的L2-VXLAN-A1
    - **VPC路由器**：选择已创建的VPC路由器
    - **关闭DHCP服务**：选择是否需要DHCP服务
    - **添加网络段**：选择CIDR
    - **CIDR**：*192.168.21.0/24*
    - **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

    如图 *541: 创建VPC网络-A1*所示，点击**确定**，创建L3-VXLAN-云路由网络1。

    图 541: 创建VPC网络-A1

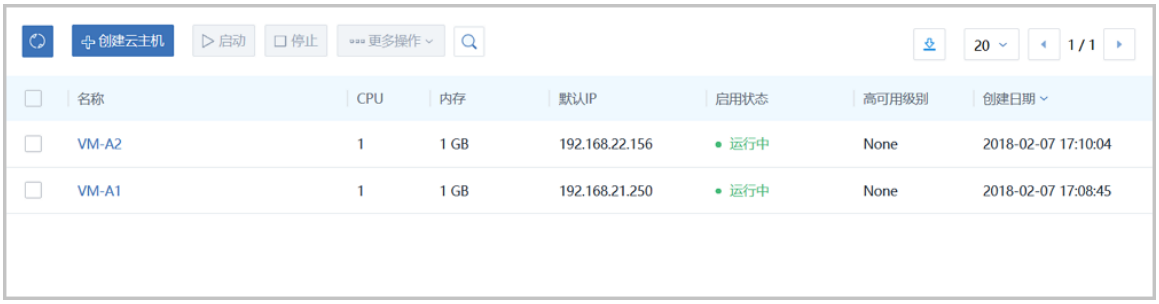
同理，创建VPC网络-A2、VPC网络-B1和VPC网络-B2，创建完成后如图 *542: VPC网络*所示：

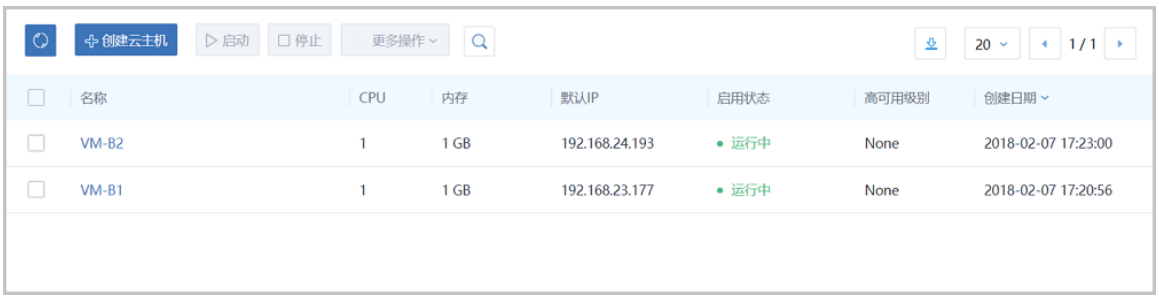
图 542: VPC网络

12.使用四个VPC网络分别在各自账户创建一个云主机，例如：VM-A1、VM-A2、VM-B1和VM-B2。

参考本教程基本部署章节的使用*VPC*网络创建云主机，使用四个VPC网络分别在各自账户创建一个云主机，VM-A1、VM-A2、VM-B1和VM-B2。创建的云主机如图 *543:* 创建云主机所示：

图 543: 创建云主机





13.验证四台云主机之间的连通性。

1. 登录VM-A1，用*ping*命令验证网络连通性：

   预期结果：

- ping baidu.com：可以成功
- ping VM-A2：可以成功
- ping VM-B1：会失败（两套VXLAN-VPC环境二层隔离）
- ping VM-B2：会失败（两套VXLAN-VPC环境二层隔离）

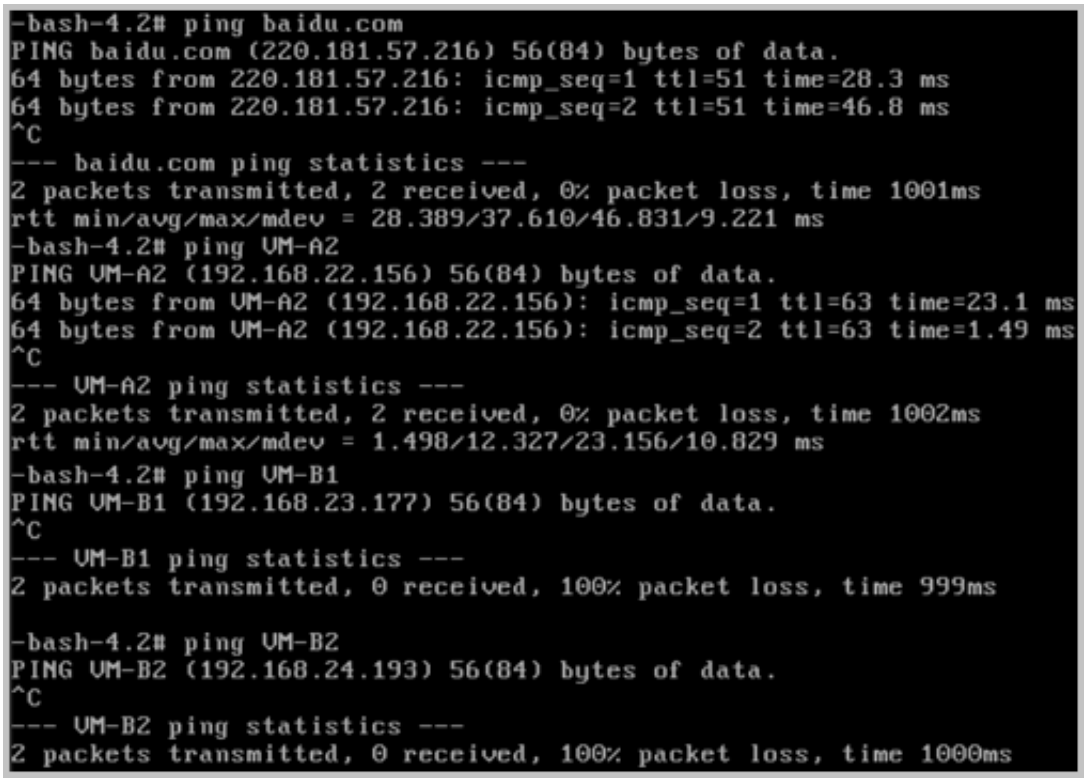
注:

在VM-A1系统中，手动添加其他VM的IP地址到*/etc/hosts*文件路径下。

```
[root@VM-web ~]# vim /etc/hosts
...
192.168.22.156 VM-A2
192.168.23.177 VM-B1
192.168.24.193 VM-B2
...
```

实际结果如图 *544:* 验证*VM-A1*网络连通性所示：

图 544: 验证VM-A1网络连通性



2. 同理，VM-A2的网络连通性和VM-A1相同。
3. 登录VM-B1，用*ping*命令验证网络连通性：

   预期结果：

- ping baidu.com：可以成功
- ping VM-A1：会失败（两套VXLAN-VPC环境二层隔离）
- ping VM-A2：会失败（两套VXLAN-VPC环境二层隔离）
- ping VM-B2：可以成功

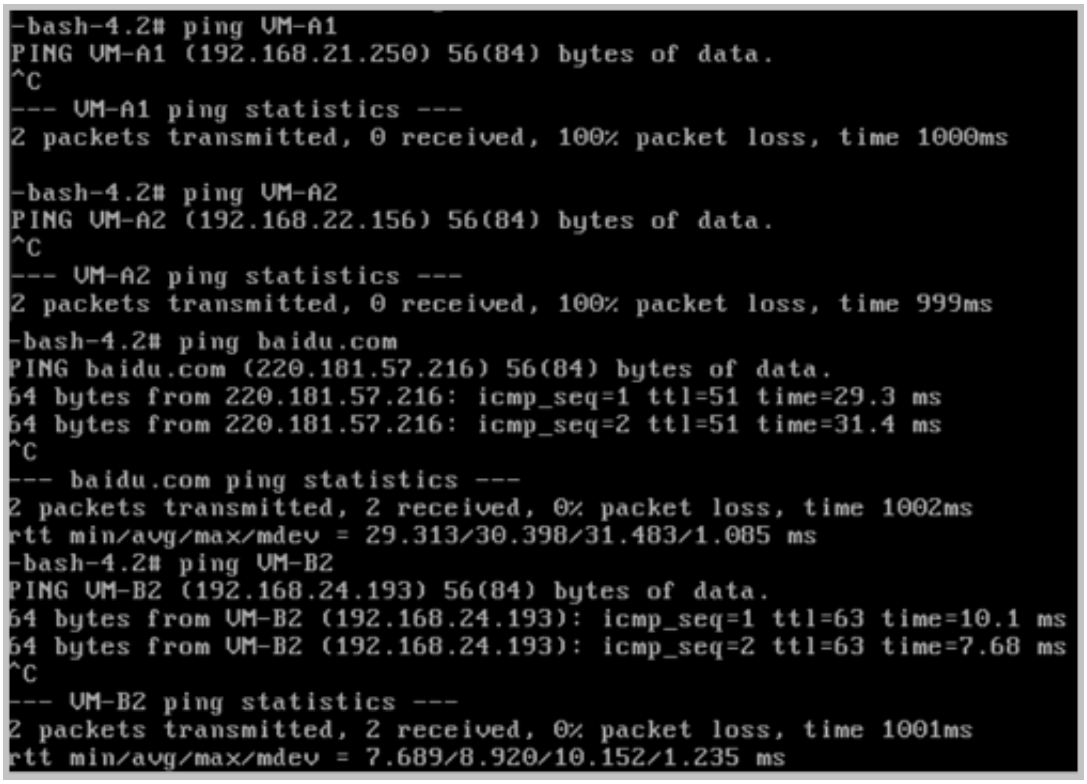
注:

在VM-B1系统中，手动添加其他VM的IP地址到*/etc/hosts*文件路径下。

```
[root@VM-web ~]# vim /etc/hosts
...
192.168.21.250 VM-A1
192.168.22.156 VM-A2
192.168.24.193 VM-B2
...
```

实际结果如图 *545:* 验证*VM-B2*网络连通性所示：

图 545: 验证VM-B2网络连通性



4. 同理，VM-B2的网络连通性和VM-B1相同。

14.从admin账户共享三层公有网络给账户A和账户B。

在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，再**公有网络**界面点击三层公网名称，点击**共享** > **操作** > **共享**按钮，勾选账户A和账户B，点击**确定**按钮完成共享。如图 *546: 共享三层公网*所示：

图 546: 共享三层公网

15.通过配置路由表，可让二层隔离的云主机VM-A1和VM-B1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-A1、VM-B1对应的云路由器

如图 *547: 创建路由表*所示：

图 547: 创建路由表

b) 添加两条自定义路由条目。

表 46: 自定义路由条目

	目标网段	下一跳
自定义路由条目1	VM-A1相应的云路由器的公网IP	VM-A1相应的云路由器的公网IP
自定义路由条目2	VM-B1相应的云路由器的公网IP	VM-B1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 *548:* 添加路由表条目所示：

图 548: 添加路由表条目

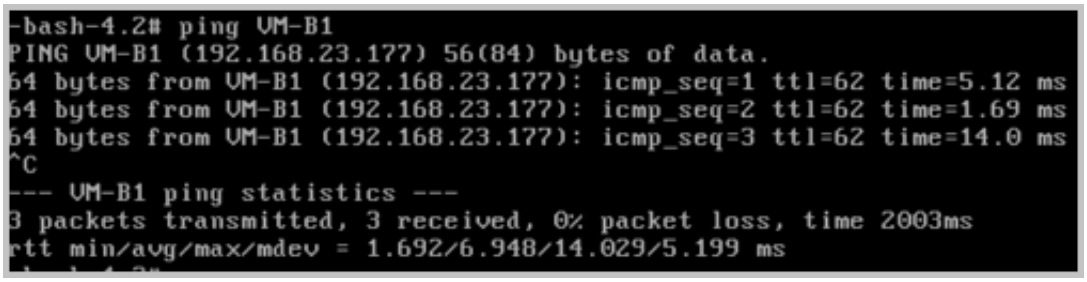
16.验证云主机VM-A1和VM-B1之间的连通性。

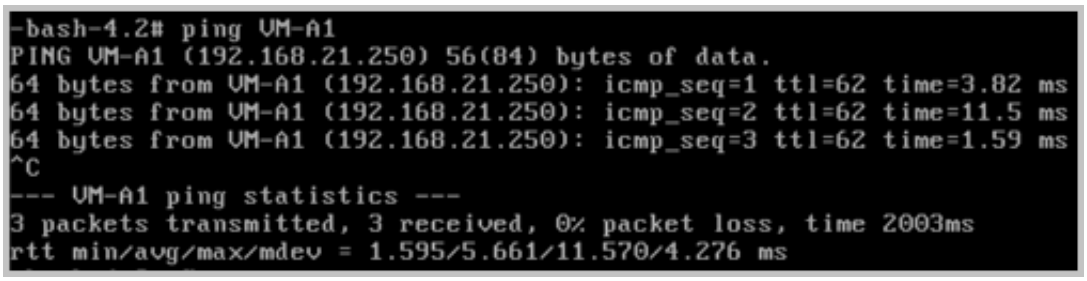
预期结果：

- 登录VM-A1，ping VM-B1：可以成功
- 登录VM-B1，ping VM-A2：可以成功

实际结果如图 *549: VM-A1和VM-B1互ping*所示：

图 549: VM-A1和VM-B1互ping





后续操作

至此，VPC网络多租户隔离部署实践介绍完毕。

7.6.3.4.2 多层Web服务器

背景信息

VPC下部署多层Web服务器的基本流程：

1. 在一个VPC下搭建三个VPC子网：Web网络、应用网络、数据库网络。

   注: 三个VPC子网的网络段不可重叠。

2. 基于三个VPC子网分别创建三台云主机：VM-web、VM-app、VM-database。
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 47: 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	*10.151.10.100~10.151.10.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

   表 48: 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	*192.168.28.100~192.168.28.200*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

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（VPC网络-1）

表 49: Web网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2017
IP CIDR	*192.168.10.0/24*

4. 应用网络（VPC网络-2）

表 50: 应用网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2020
IP CIDR	*192.168.20.0/24*

5. 数据库网络（VPC网络-3）

表 51: 数据库网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2050
IP CIDR	*192.168.50.0/24*
私有网络	配置信息

以下介绍VPC下部署多层Web服务器的实践步骤。

操作步骤

1. 在一个VPC下搭建三个VPC子网：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VPC子网的网络段不可重叠。

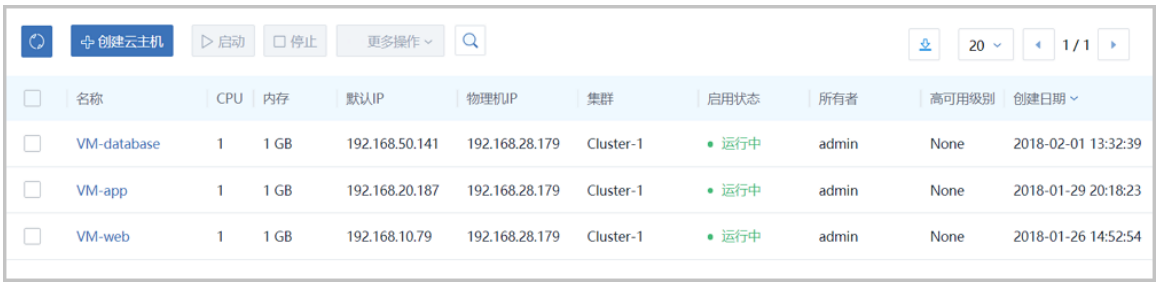
搭建的三个VPC子网如图 *550: 三个VPC子网*所示：

图 550: 三个VPC子网

2. 基于三个VPC子网分别创建三台云主机：VM-web、VM-app、VM-database。

   如图 *551: VM-web、VM-app、VM-database*所示：

   图 551: VM-web、VM-app、VM-database



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：可以成功

      注:

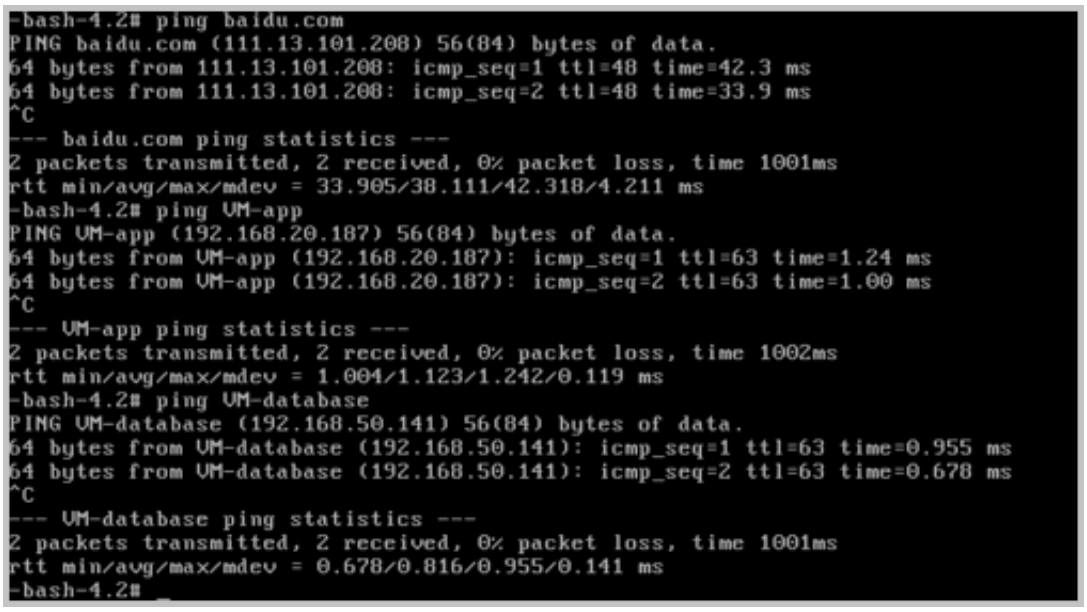
      在VM-web系统中，手动添加VM-app、VM-database的IP地址到*/etc/hosts*文件路径下。

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

```
...
```

实际结果如图 *552: 验证VM-web网络连通性*所示：

图 552: 验证VM-web网络连通性



2. 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

   注:

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

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

   实际结果如图 *553: 验证VM-app网络连通性*所示：

   图 553: 验证VM-app网络连通性

```
-bash-4.2# ping baidu.com
PING baidu.com (123.125.114.144) 56(84) bytes of data.
64 bytes from 123.125.114.144: icmp_seq=1 ttl=48 time=26.4 ms
64 bytes from 123.125.114.144: icmp_seq=2 ttl=48 time=26.5 ms
^C
--- baidu.com ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 26.461/26.497/26.534/0.166 ms
-bash-4.2# ping VM-web
PING VM-web (192.168.10.79) 56(84) bytes of data.
64 bytes from VM-web (192.168.10.79): icmp_seq=1 ttl=63 time=1.03 ms
64 bytes from VM-web (192.168.10.79): icmp_seq=2 ttl=63 time=1.05 ms
^C
--- VM-web ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 1.033/1.043/1.053/0.010 ms
-bash-4.2# ping VM-database
PING VM-database (192.168.50.141) 56(84) bytes of data.
64 bytes from VM-database (192.168.50.141): icmp_seq=1 ttl=63 time=0.886 ms
^C
--- VM-database ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.886/0.886/0.886/0.000 ms
-bash-4.2#
```

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-app：可以成功
   - ping VM-web：可以成功

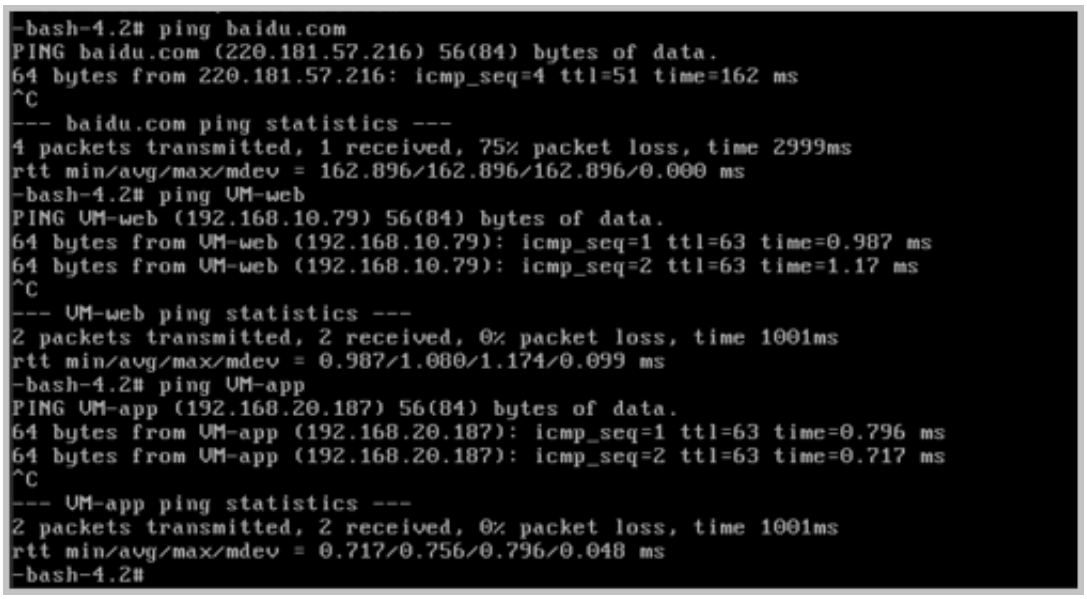
   注:

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

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

实际结果如图 *554: 验证VM-database网络连通性*所示：

图 554: 验证VM-database网络连通性



后续操作

至此，多层Web服务器的部署实践介绍完毕。

7.6.3.4.3 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：

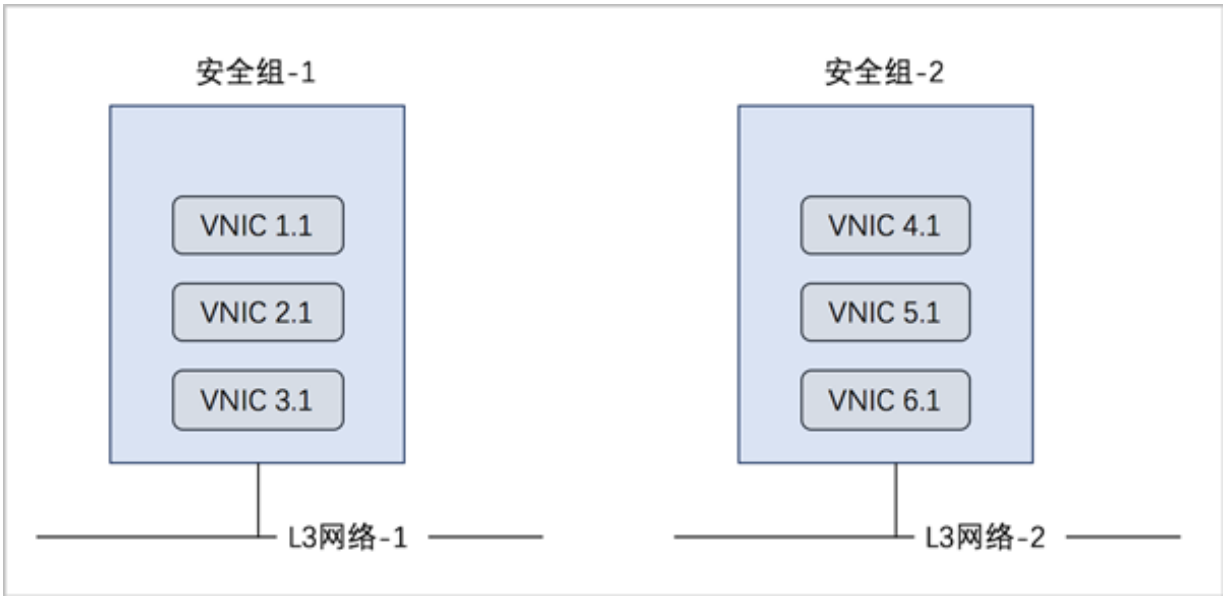
- 安全组规则按数据包的流向分为两种类型：
  - 入方向（Ingress）：代表数据包从外部进入云主机。
  - 出方向（Egress）：代表数据包从云主机往外部发出。
- 安全组规则对通信协议支持以下类型：
  - ALL：表示涵盖所有协议类型，此时不能指定端口。
  - TCP：支持1-65535端口。
  - UDP：支持1-65535端口。

  - 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 *555:* 安全组所示：

图 555: 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VPC下安全组的使用方法，包括两个场景：

- VPC下仅有一个VPC网络（VPC子网）：安全组使用方法与云路由网络场景的安全组使用方法相同。
- VPC下有多个VPC子网：
  - 对两个VPC子网下的云主机设置入方向规则；
  - 对两个VPC子网下的云主机设置出方向规则。

操作步骤

1. 在一个VPC下搭建两个VPC子网，例如：VPC网络-1和VPC网络-2，使用VPC网络-1创建云主机VM-1，使用VPC网络-2创建云主机VM-2。详情可参考本教程基本部署章节。
2. 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VPC网络，例如：VPC网络-1
   - **规则**：可选项，用于设置相应的防火墙规则

     注: 创建安全组的时候可点击**规则**后面的**+**进行添加，也可后续添加，详见设置入方向规则和设置出方向规则。
   - **网卡**：可选项，选择网卡加入安全组

     注: 创建安全组的时候可点击**网络**后面的**+**进行添加，也可后续添加，详见添加网卡到安全组。

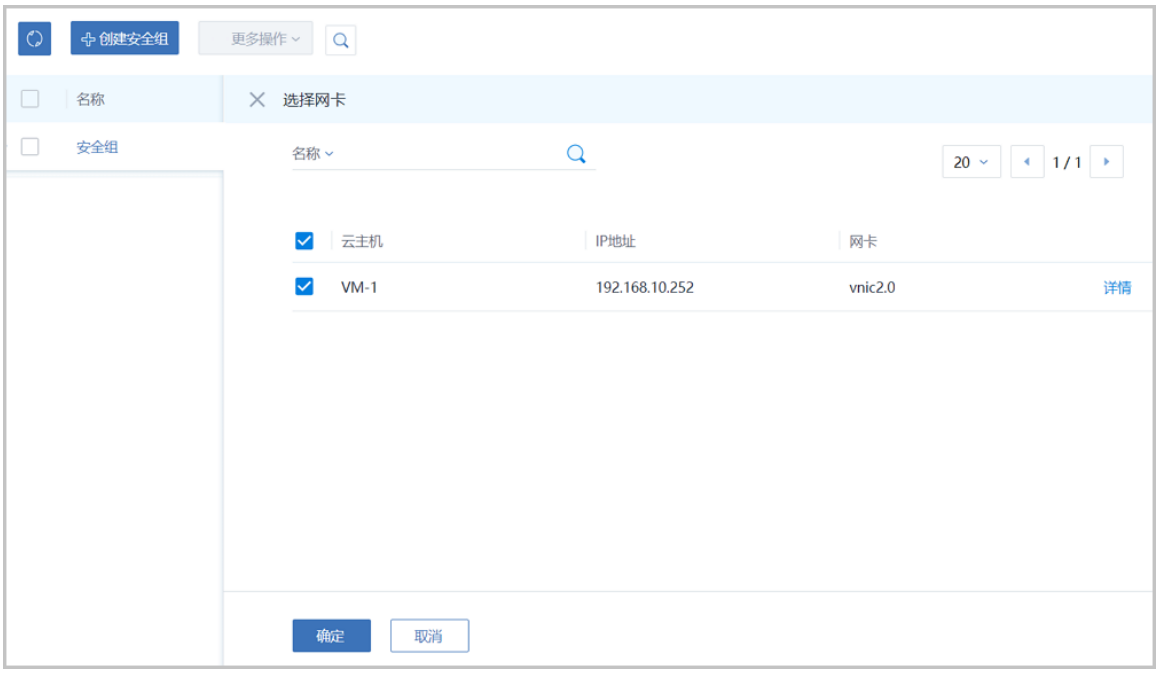
   如图 *556:* 创建安全组所示，点击**确定**完成安全组创建。

   图 556: 创建安全组

3. 添加网卡到安全组。

   在**安全组**界面，点击已创建的安全组名称，点击**云主机网卡**子页面的**操作** > **绑定云主机网卡**按钮，进入**选择网卡**界面，选择VM-1网卡，如图 *557:* 添加网卡所示，点击**确定**按钮完成网卡添加。

   图 557: 添加网卡



4. 设置入方向规则并验证。

a) 设置入方向规则。

在**安全组**界面，点击已创建的安全组名称，点击**规则**子页面的**操作** > **添加规则**按钮，进入**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 *558:* 设置入方向规则所示，点击**确定**，完成入方向规则设置。

图 558: 设置入方向规则

b) 入方向规则验证。

此时VM-1只允许外部通过端口20~100访问。

1. 登录VM-2，使用*nc*命令通过20端口与VM-1建立通信连接，可成功通信。

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

   如图 *559: VM-2在端口20向VM-1发送信息*和图 *560: VM-1在端口20接收信息成功*所示：

   图 559: VM-2在端口20向VM-1发送信息

图 560: VM-1在端口20接收信息成功

2. 登录VM-2，使用*nc*命令通过10端口与VM-1建立通信，通信会失败。如图 *561: VM-2在端口10尝试连接VM-1失败*所示：

图 561: VM-2在端口10尝试连接VM-1失败

5. 设置出方向规则并验证。

a) 设置出方向规则。

在**安全组**界面，点击已创建的安全组名称，点击**规则**子页面的**操作** > **添加规则**按钮，进入**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 *562: 设置出方向规则*所示，点击**确定**，完成入方向规则设置。

图 562: 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。

1. 登录VM-1，使用*nc*命令通过200端口与VM-2建立通信，可成功通信。

   注: 需将VM-2中原有的iptables规则清除，可使用命令iptables -F

   如图 *563: VM-1在端口200向VM-2发送信息*和图 *564: VM-2在端口200接收信息成功*所示：

   图 563: VM-1在端口200向VM-2发送信息

图 564: VM-2在端口200接收信息成功

2. 登录VM-1，使用*nc*命令通过10端口与VM-2建立通信，通信会失败。如图 *565: VM-1在端口10尝试连接VM-2失败*所示：

图 565: VM-1在端口10尝试连接VM-2失败

后续操作

至此，安全组的使用方法介绍完毕。

7.6.3.4.4 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。

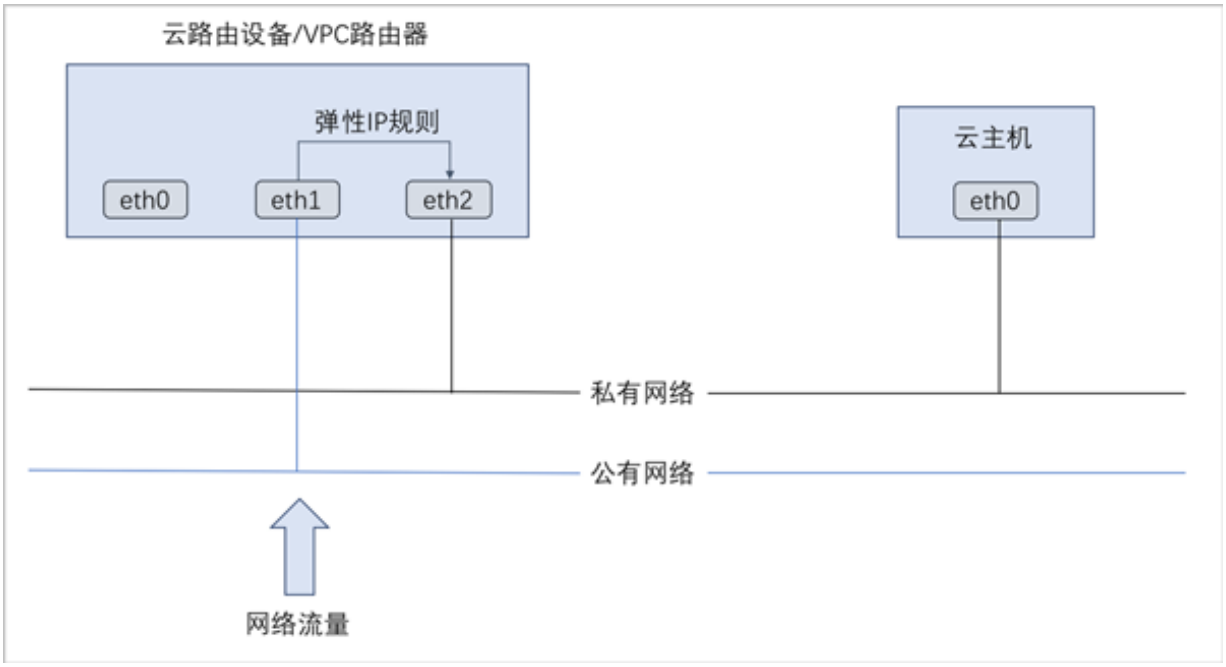
- 内部私有网络是隔离的网络空间，不能直接被外部网络访问。
- 弹性IP基于网络地址转换（NAT），将一个网络（通常是公有网络）的IP地址转换成另一个网络（通常是私有网络）的IP地址；通过弹性IP，可对公网的访问直接关联到内部私网的云主机IP。
- 弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
- 云主机使用的扁平网络、云路由网络、VPC均可使用弹性IP服务：
  - 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
  - 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。

- 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 *566: 云路由网络/VPC下弹性IP的应用场景*所示：

图 566: 云路由网络/VPC下弹性IP的应用场景



背景信息

以下介绍VPC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. 在一个VPC下搭建两个VPC子网，例如：VPC网络-1和VPC网络-2，使用VPC网络-1创建云主机VM-1，使用VPC网络-2创建云主机VM-2。详情可参考本教程基本部署章节。
2. 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 *567: 新建虚拟IP*所示：

       图 567: 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 *568: 已有虚拟IP*所示：

图 568: 已有虚拟IP

如图 *569: 创建弹性IP*所示：

图 569: 创建弹性IP

b) 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 *570: 选择VM-1*和图 *571: 将EIP-1绑定VM-1*所示：

图 570: 选择VM-1

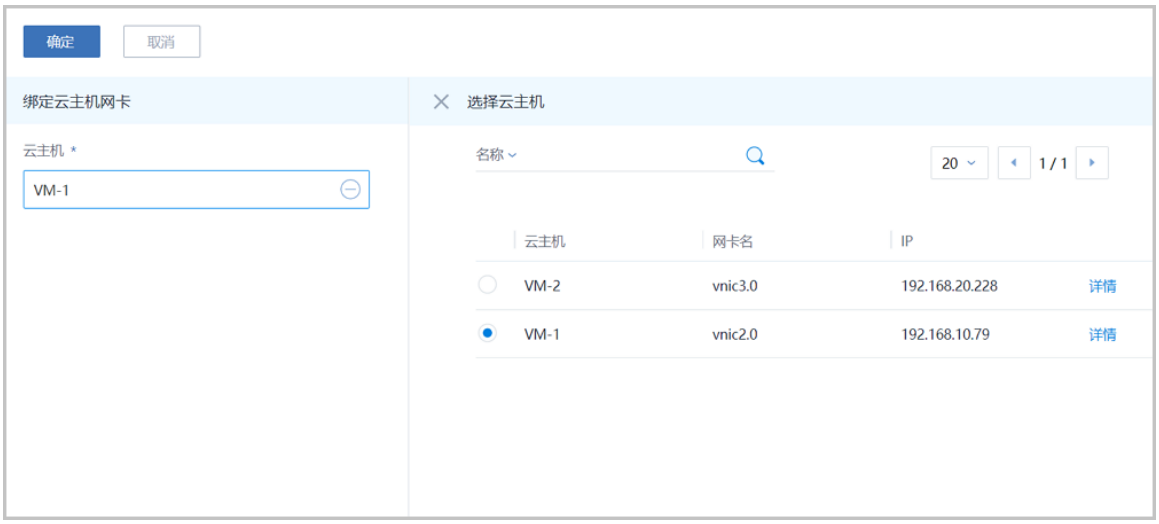


图 571: 将EIP-1绑定VM-1

c) 通过EIP-1登录VM-1。

使用某一可访问VPC网络公网网段的主机SSH登录EIP-1：*10.151.10.170*，也就是登录到私网IP为*192.168.10.79*的VM-1。

如所示：

图 572: 通过EIP-1登录VM-1

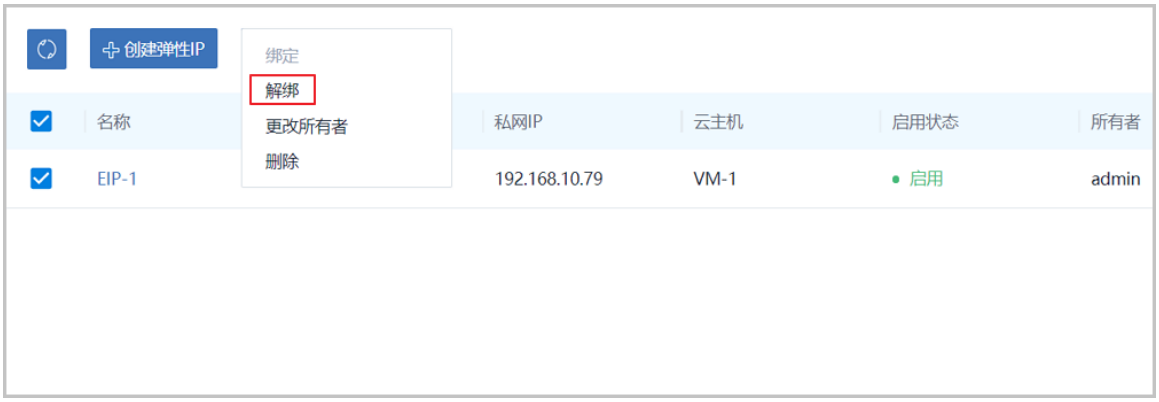
3. 将EIP-1绑定VM-2。

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 *573: 将EIP-1从VM-1解绑*所示：

图 573: 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 *574: 选择VM-2*和图 *575: 将EIP-1绑定VM-2*所示：

图 574: 选择VM-2

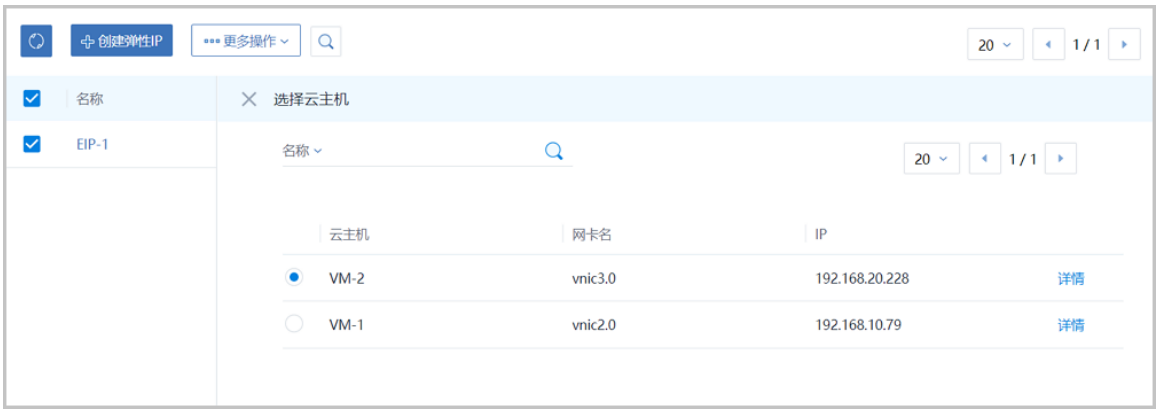


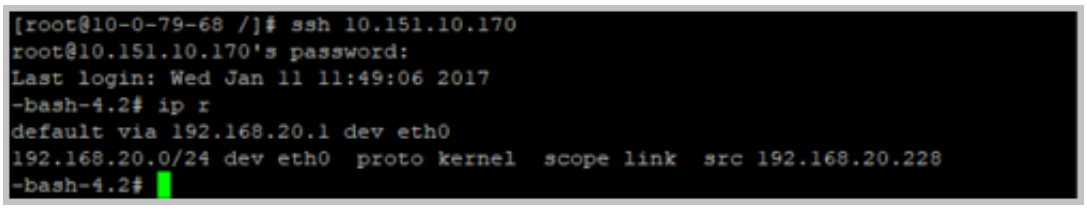
图 575: 将EIP-1绑定VM-2

c) 通过EIP-1登录VM-2。

再次SSH登录EIP-1：*10.151.10.170*，可发现此时登录到私网IP为*192.168.20.228*的VM-2。

如图 *576: 通过EIP-1登录VM-2*所示：

图 576: 通过EIP-1登录VM-2



后续操作

至此，弹性IP的使用方法介绍完毕。

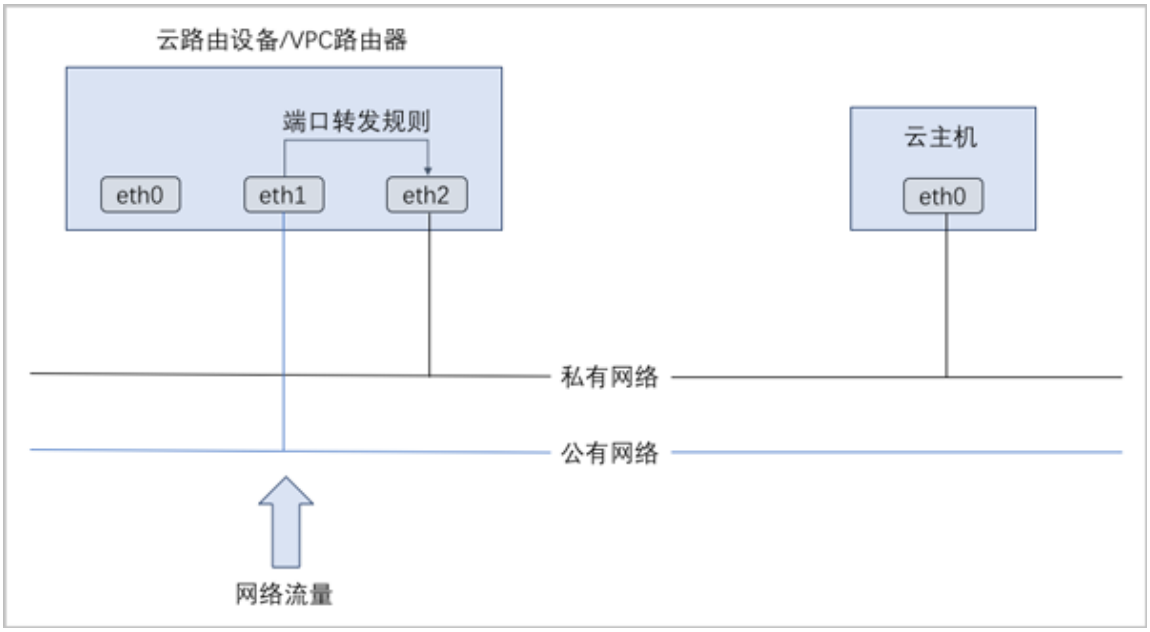
7.6.3.4.5 端口转发

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。

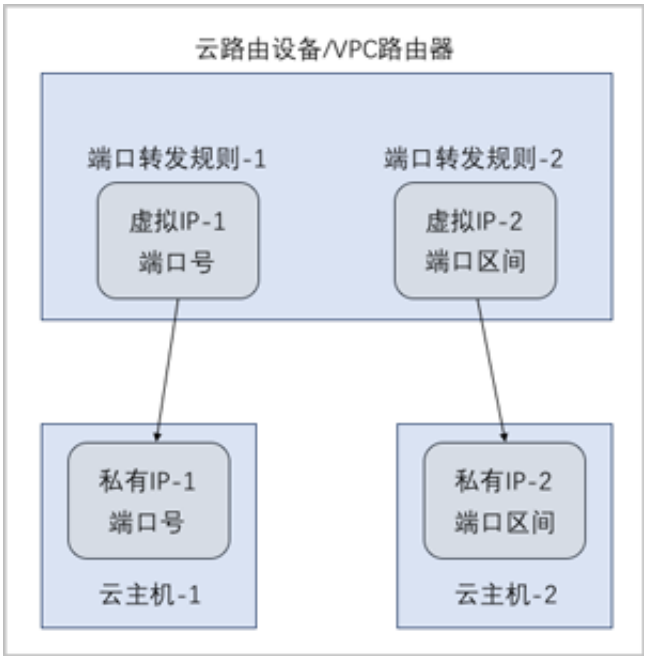
- 启用SNAT服务的私有网络中，云主机可访问外部网络但不能被外部网络所访问；使用端口转发规则，允许外部网络访问SNAT后面云主机的某些指定端口。
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *577: 端口转发*所示：

图 577: 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 *578: 虚拟IP-端口转发*所示：

图 578: 虚拟IP-端口转发



背景信息

以下介绍VPC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. 在一个VPC下搭建两个VPC子网，例如：VPC网络-1和VPC网络-2，使用VPC网络-1创建云主机VM-1，使用VPC网络-2创建云主机VM-2。详情可参考本教程基本部署章节。
2. 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，可选新建虚拟IP或已有虚拟IP方式添加
     - 新建虚拟IP方式，必须填写**网络**信息，可选填**指定IP**选项
     - 已有虚拟IP方式，必须填写**虚拟IP**信息

- **协议**：选择协议类型，包括：TCP、UDP
- **端口**：可选指定端口或端口区间方式添加，端口范围：1-65535
  - 指定端口方式，必须填写**源起始端口**和**云主机起始端口**，可选填**允许CIDR**
  - 端口区间方式，必须填写**源起始端口**和**源结束端口**，可选填**允许CIDR**

本场景下，使用指定端口方式（源起始端口：24，云主机起始端口：22）创建的端口转发规则PF-1如图 *579: 创建端口转发规则PF-1*所示，点击**确定**按钮完成端口转发创建。

图 579: 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-VPC路由器
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) 将PF-1绑定VM-1。

端口转发创建完成后会自动跳转到**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VM-1，点击**确定**。如图 *580: 选择VM-1*和图 *581: 将PF-1绑定VM-1*所示：

图 580: 选择VM-1

图 581: 将PF-1绑定VM-1

c) 通过PF-1登录VM-1。

使用某一可访问VPC网络公网网段的主机SSH登录公网IP：*10.151.10.174*的24端口，也就是登录到私网IP为*192.168.10.79*的VM-1的22端口。

如图 *582: 通过PF-1登录VM-1*所示：

图 582: 通过PF-1登录VM-1

```
login as: root
root@172.20.11.50's password:
Last login: Fri Jan 26 20:50:21 2018 from 172.31.253.12
[root@10-0-79-68 ~]# ssh 10.151.10.174 -p 24
root@10.151.10.174's password:
Last login: Fri Jan 26 12:51:39 2018 from 10.0.79.68
-bash-4.2# ip r
default via 192.168.10.1 dev eth0
192.168.10.0/24 dev eth0  proto kernel  scope link  src 192.168.10.79
-bash-4.2# lsof -i:22
COMMAND   PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd      860 root    3u  IPv4  13120      0t0  TCP *:ssh (LISTEN)
sshd      860 root    4u  IPv6  13129      0t0  TCP *:ssh (LISTEN)
sshd    26134 root    3u  IPv4  42006      0t0  TCP zstack-test-image:ssh->10.0.
79.68:39284 (ESTABLISHED)
-bash-4.2#
```

3. 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 *583: 将PF-1从VM-1解绑*所示：

图 583: 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 *584: 选择VM-2*和图 *585: 将PF-1绑定VM-2*所示：

图 584: 选择VM-2

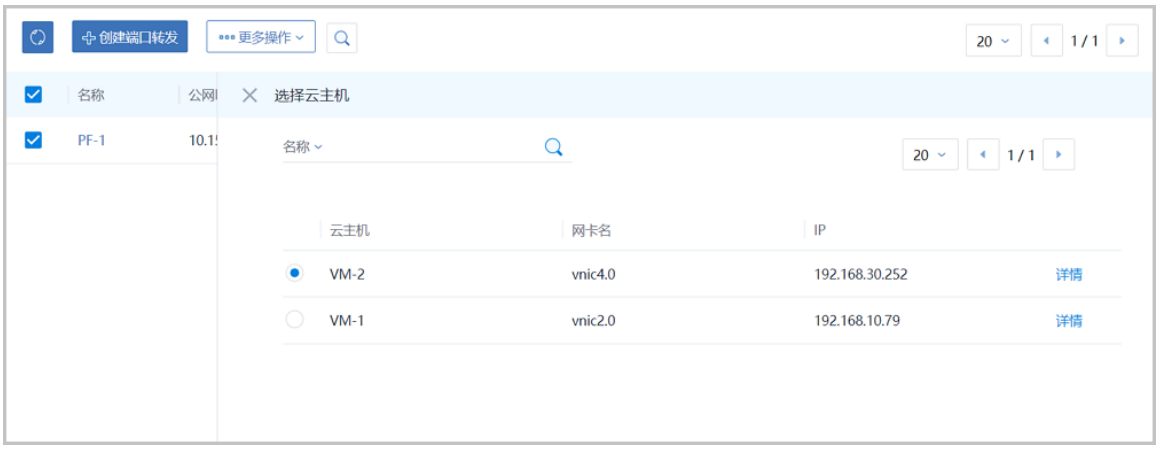


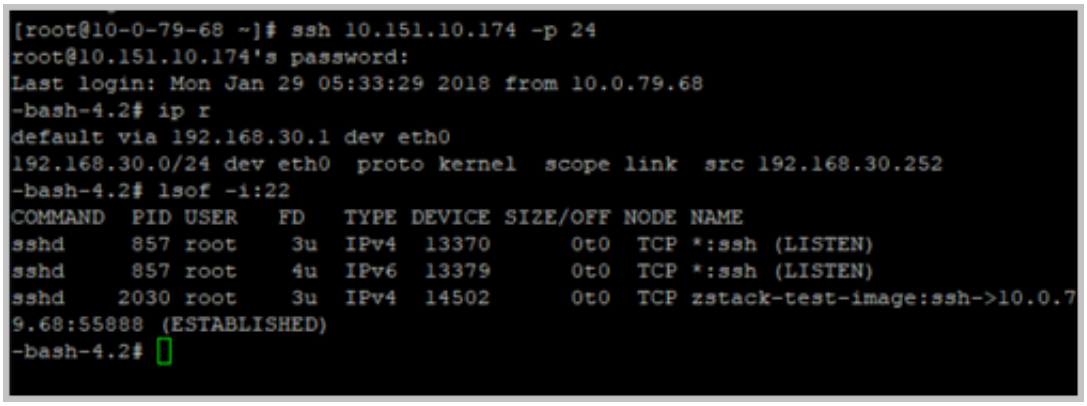
图 585: 将PF-1绑定VM-2

c) 通过PF-1登录VM-2。

再次SSH登录公网IP：*10.151.10.174*的24端口，可发现此时登录到私网IP为*192.168.30.252*的VM-2的22端口。

如图 *586: 通过PF-1登录VM-2*所示：

图 586: 通过PF-1登录VM-2



4. 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-2
- **简介**：可选项，可留空不填
- **选择虚拟IP**：选择已有虚拟IP
- **协议**：选择协议类型，包括：TCP、UDP
- **端口**：选择端口区间方式，端口范围：1-65535
  - **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30
  - **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40
  - **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 *587: 创建端口转发规则PF-2*所示，点击**确定**按钮完成端口转发创建。

图 587: 创建端口转发规则PF-2

确定
取消
创建端口转发
名称 *
PF-2
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-VPC路由器
协议 *
TCP
端口
指定端口
端口区间
源起始端口 *
30
源结束端口 *
40
云主机起始端口 *
30
云主机结束端口 *
40
允许CIDR:
192.168.1.0/24

b) 将PF-2绑定VM-1。

端口转发创建完成后会自动跳转到**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VM-1，点击**确定**。如图 *588: 选择VM-1*和图 *589: 将PF-2绑定VM-1*所示：

图 588: 选择VM-1

图 589: 将PF-2绑定VM-1

c) 可见，同一虚拟IP（*10.151.10.174*），通过不同的端口转发规则，绑定到不同云主机。

d) 通过PF-2向VM-1发送信息。

使用某一可访问VPC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 *590: 在源端口30发送信息*和图 *591: 在VM-1的端口5900接收信息*所示：

图 590: 在源端口30发送信息

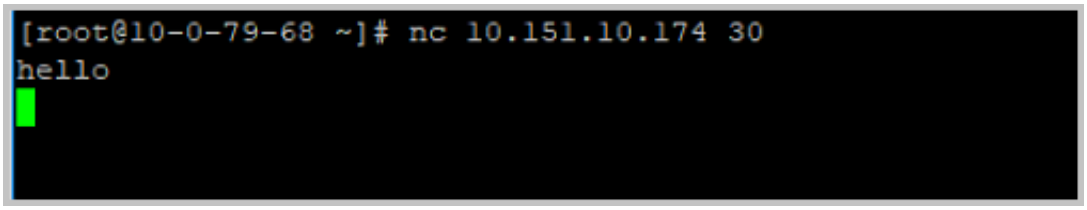


图 591: 在VM-1的端口5900接收信息

后续操作

至此，端口转发的使用方法介绍完毕。

7.6.3.4.6 负载均衡

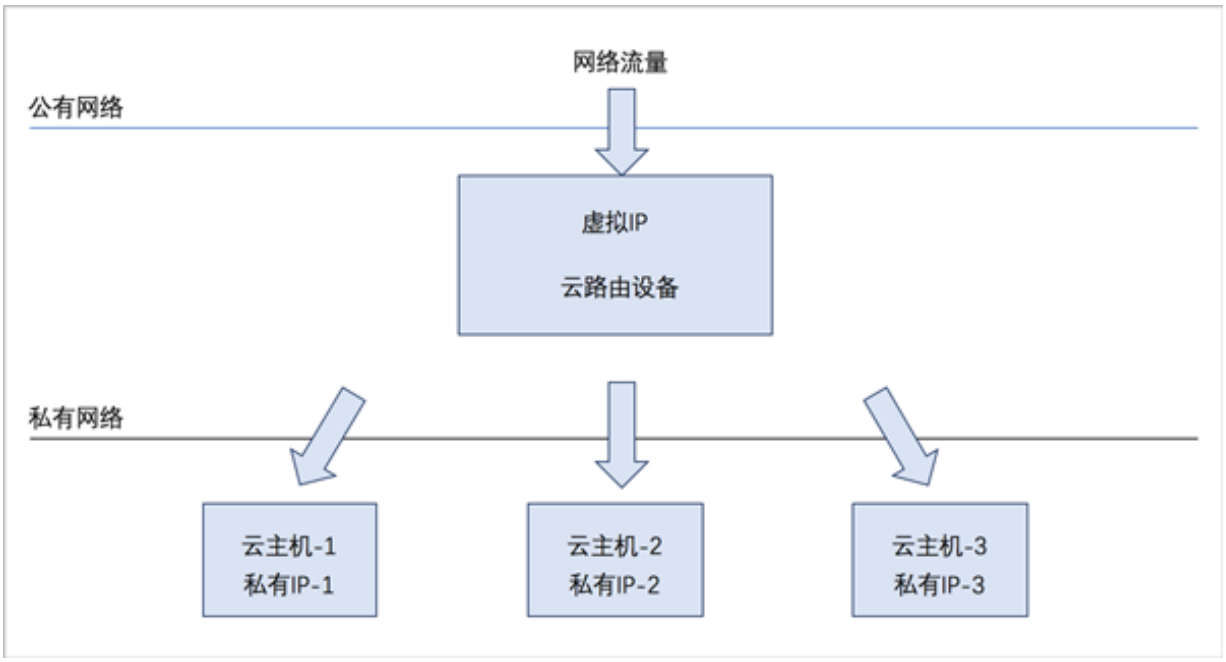
前提条件

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三种协议。
- 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 *592: 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 592: 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。

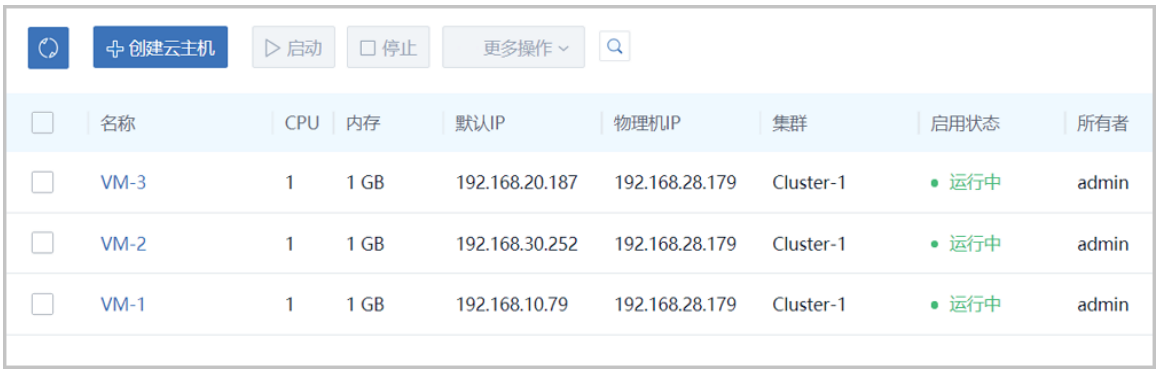
以下介绍VPC下负载均衡的使用方法，场景如下：

- 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. 搭建三个VPC子网，例如：VPC网络-1、VPC网络-2和VPC网络-3，并分别创建云主机VM-1、VM-2和VM-3。详情可参考本教程基本部署章节。如图 *593: VM-1、VM-2、VM-3*所示：

   图 593: VM-1、VM-2、VM-3



2. 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，可选新建虚拟IP或已有虚拟IP方式添加
  - 新建虚拟IP方式，必须填写**网络**信息，可选填**指定IP**选项
  - 已有虚拟IP方式，必须填写**虚拟IP**信息
- **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。

如创建负载均衡器所示：

图 594: 创建负载均衡器

3. 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
  - TCP：支持1-65535端口
  - HTTP：支持1-65535端口
  - HTTPS：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100，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100端口。

  如图 *595:* 添加监听器所示：

  图 595: 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
  - **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
  - **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 *596:* 添加监听器-高级选项所示：

图 596: 添加监听器-高级选项

4. 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 *597: 绑定云主机网卡*所示：

   图 597: 绑定云主机网卡

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**：选择云路由挂载的三层私有网络
- **云主机网卡**：选择网络对应的云主机

以VPC网络-3为例，如图 *598: 绑定VM-3网卡到监听器*所示，点击**确定**，绑定VM-3的云主机网卡到监听器。

图 598: 绑定VM-3网卡到监听器

重复此操作，绑定其他两个子网的网卡，绑定后如图 *599: 绑定云主机网卡到监听器*所示：

图 599: 绑定云主机网卡到监听器

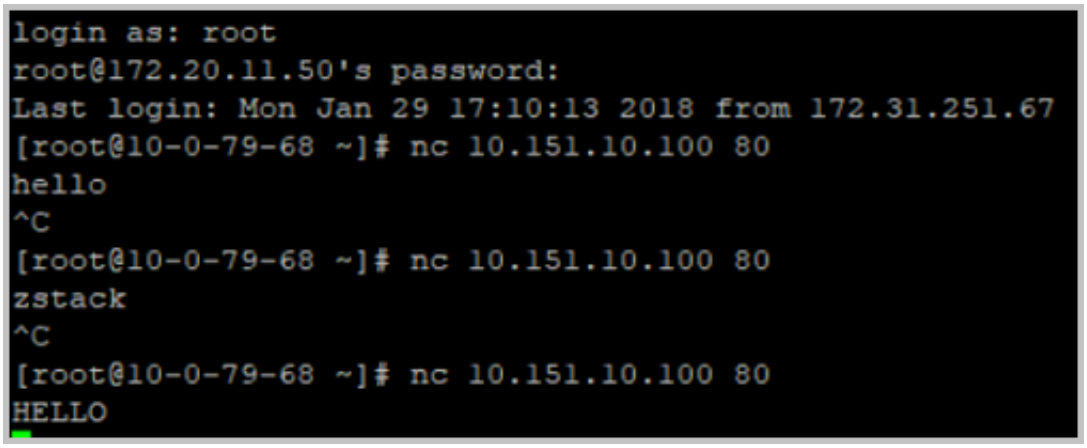
5. 负载均衡器以默认的轮询方式向三台云主机发送信息。

   使用某一可访问VPC网络公网网段的主机，通过*nc*命令向负载均衡器公网IP：*10.151.10.100*的80端口发送信息，可在VM-1（私网IP：*192.168.10.76*）、VM-2（私网IP：*192.168.30.252*）、VM-3（私网IP：*192.168.20.187*）的100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

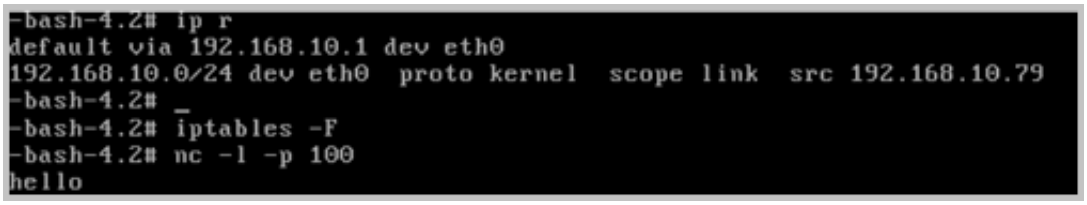
   1. 向负载均衡器公网IP的80端口发送三条信息，如图 *600:* 向负载均衡器公网*IP*的*80*端口发送三条信息所示：

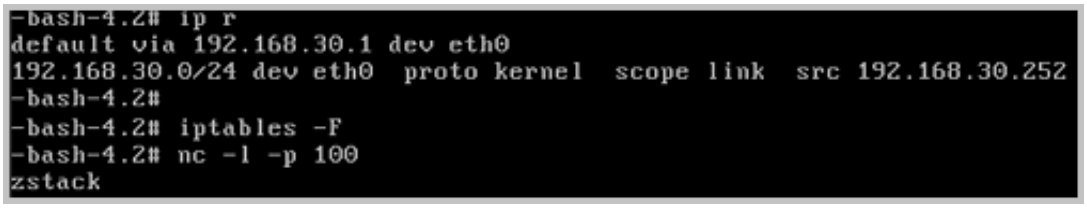
      图 600: 向负载均衡器公网IP的80端口发送三条信息

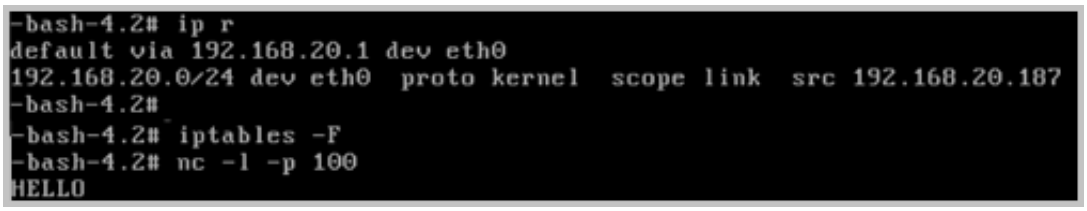
      

   2. VM-1、VM-2、VM-3的100端口分别接收到一条信息，如图 *601:* 三台云主机的*100*端口分别接收到一条信息所示：

      图 601: 三台云主机的100端口分别接收到一条信息



后续操作

至此，负载均衡的使用方法介绍完毕。

7.6.3.4.7 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。

VPC IPsec隧道的典型场景：

- 在两套隔离的ZStack私有云环境中，分别搭建两套VPC环境，在两套VPC环境中，分别创建两套VPC网络（VPC子网），两套VPC环境的子网间无法直接通信，使用IPsec隧道后，就可实现两套VPC环境的子网间互相通信。

背景信息

VPC IPsec隧道的使用流程：

1. 在第一套ZStack环境中，创建IPsec隧道，指定第一套VPC环境中的本地公网IP，并指定本地可用的一个或多个VPC子网，输入第二套VPC环境中的公网IP作为远端IP，并输入第二套VPC环境指定的一个或多个VPC子网作为远端网络；
2. 在第二套ZStack环境中，创建IPsec隧道，指定第二套VPC环境中的本地公网IP，并指定本地可用的一个或多个VPC子网，输入第一套VPC环境中的公网IP作为远端IP，并输入第一套VPC环境指定的一个或多个VPC子网作为远端网络。

注: 两套VPC环境中的所有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 52: 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	*10.151.10.100~10.151.10.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

2. 管理网络

表 53: 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	*192.168.28.100~192.168.28.200*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

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 54: VPC网络-1配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2018
IP CIDR	*192.168.10.0/24*

4. VPC网络-2

表 55: VPC网络-2配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2020
IP CIDR	*192.168.20.0/24*

- **第二套ZStack**：

  1. 公有网络

     表 56: 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	*10.151.20.100~10.151.20.200*
子网掩码	*255.0.0.0*
网关	*10.0.0.1*

  2. 管理网络

     表 57: 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	*192.168.28.10~192.168.28.90*
子网掩码	*255.255.255.0*
网关	*192.168.28.1*

  3. VPC网络-3

表 58: VPC网络-3配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2017
IP CIDR	*192.168.30.0/24*

4. VPC网络-4

表 59: VPC网络-4配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2030
IP CIDR	*192.168.40.0/24*

以下介绍搭建VPC IPsec隧道的实践步骤。

操作步骤

1. 在第一套ZStack中搭建VPC环境，并创建两套VPC网络（VPC子网），例如：VPC网络-1、VPC网络-2；使用VPC网络-1创建一台云主机VM-1，使用VPC网络-2创建一台云主机VM-2。详情可参考本教程基本部署章节。

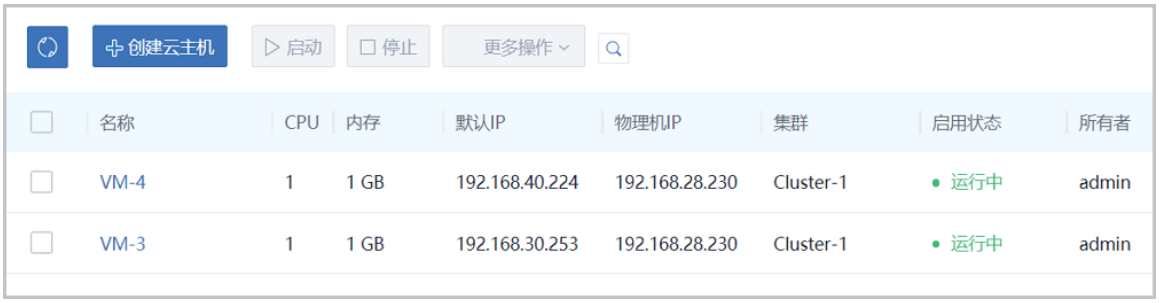
   创建的云主机如图 *602: VM-1、VM-2*所示：

   图 602: VM-1、VM-2

2. 同理，在第二套ZStack中搭建VPC环境，并创建两套VPC网络（VPC子网），例如：VPC网络-3、VPC网络-4；使用VPC网络-3创建云主机VM-3，使用VPC网络-4创建云主机VM-4。

创建的云主机如图 *603: VM-3、VM-4*所示：

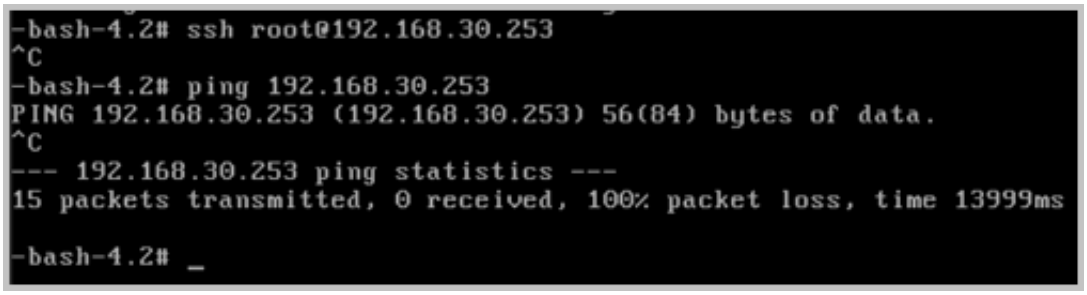
图 603: VM-3、VM-4



3. 检测第一套VPC环境中的云主机VM-1、VM-2与第二套VPC环境中的云主机VM-3、VM-4的连通性。

   - 登录VM-1，尝试SSH默认的22端口远程登录VM-3失败，也不能ping通VM-3。
   - 如图 *604: VM-1尝试连通VM-3失败*所示：

     图 604: VM-1尝试连通VM-3失败



   - 登录VM-1，尝试连通VM-4失败。
   - 登录VM-2，尝试连通VM-3、VM-4失败。
   - 登录VM-3，尝试连通VM-1、VM-2失败。
   - 登录VM-4，尝试连通VM-1、VM-2失败。

4. 在第一套ZStack中创建IPsec隧道。

   a) 创建IPsec隧道-1。

   在ZStack私有云主菜单，点击**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

  - **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

    注: VPC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VPC路由器挂载的两个VPC子网，如果VPC路由器仅挂载一个VPC子网则会默认选中该VPC网络
- **远端网络IP**：填写远端VPC环境中用于IPsec服务的公网IP
- **远端网络CIDR**：填写远端VPC环境中指定的一个或多个VPC子网CIDR（多个VPC子网CIDR用","隔开）
- **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VPC路由器与支持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 *605: 创建IPsec隧道-1*所示，点击**确定**按钮，创建IPsec隧道。

图 605: 创建IPsec隧道-1

确定
取消
创建IPsec隧道
名称 *
IPsec隧道-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-VPC路由器
本地子网 *
VPC网络-1
VPC网络-2
远端网络IP *
10.151.20.192
远端网络CIDR *
192.168.30.0/24,192.168.40.0/24
认证密钥 *
test1234

IPsec隧道-1创建完成，如图 *606: IPsec隧道-1*所示：

图 606: 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 *607: 创建IPsec隧道-2*所示：

   图 607: 创建IPsec隧道-2

确定
取消
创建IPsec隧道
名称 *
IPsec隧道-2
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-VPC路由器
本地子网 *
VPC网络-4
VPC网络-3
远端网络IP *
10.151.10.174
远端网络CIDR *
192.168.10.0/24,192.168.20.0/24
认证密钥 *
test1234

b) IPsec隧道-2创建完成。

如图 *608: IPsec隧道-2*所示：

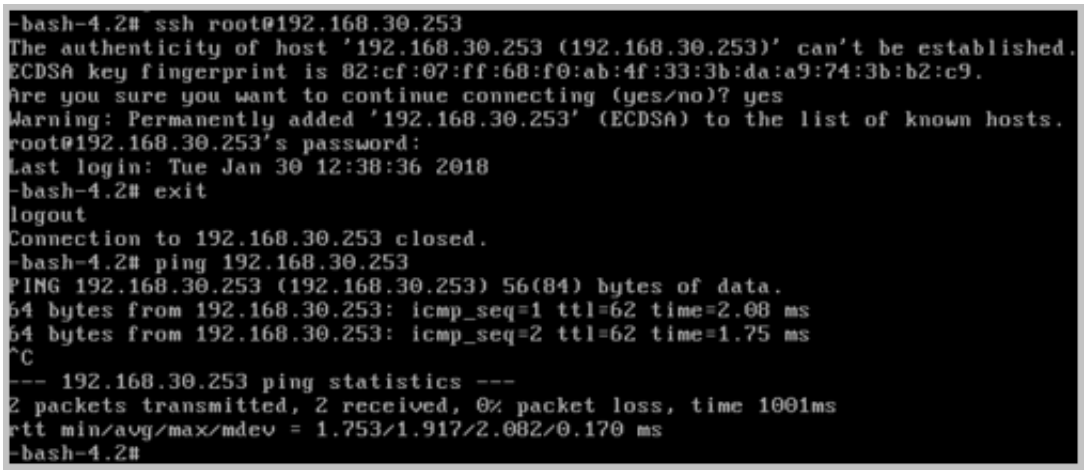
图 608: IPsec隧道-2

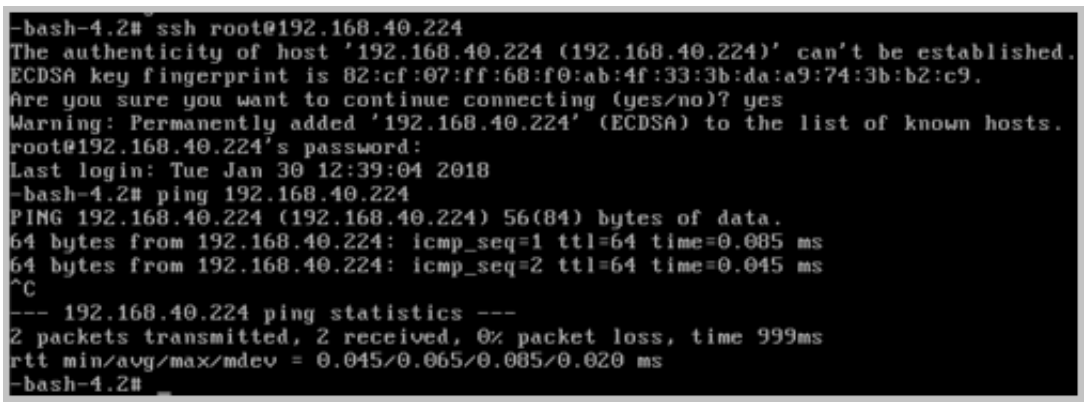
6. 检测第一套VPC环境中的云主机VM-1、VM-2与第二套VPC环境中的云主机VM-3、VM-4的连通性。

   - 登录VM-1，可通过SSH默认的22端口远程登录VM-3、VM-4，以及ping通VM-3、VM-4。

     如图 *609: VM-1成功连通VM-3、VM-4*所示：

     图 609: VM-1成功连通VM-3、VM-4

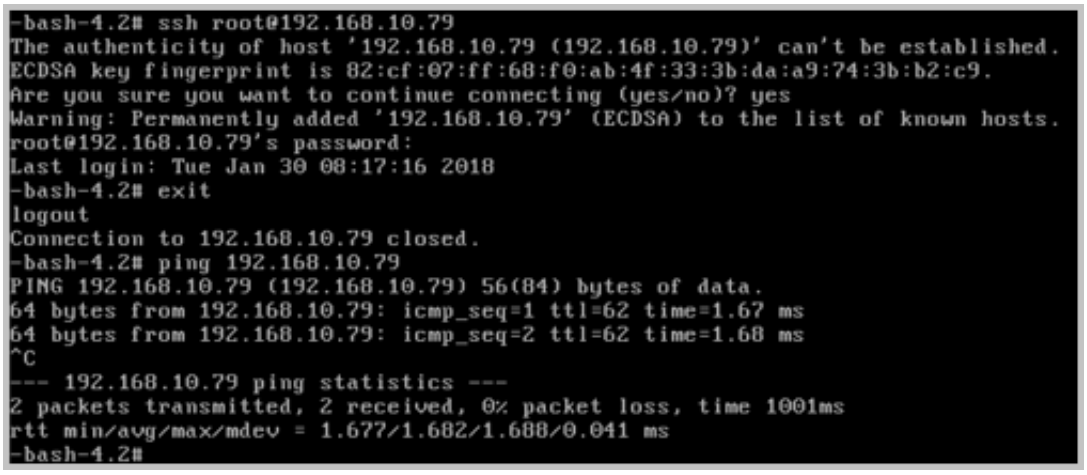


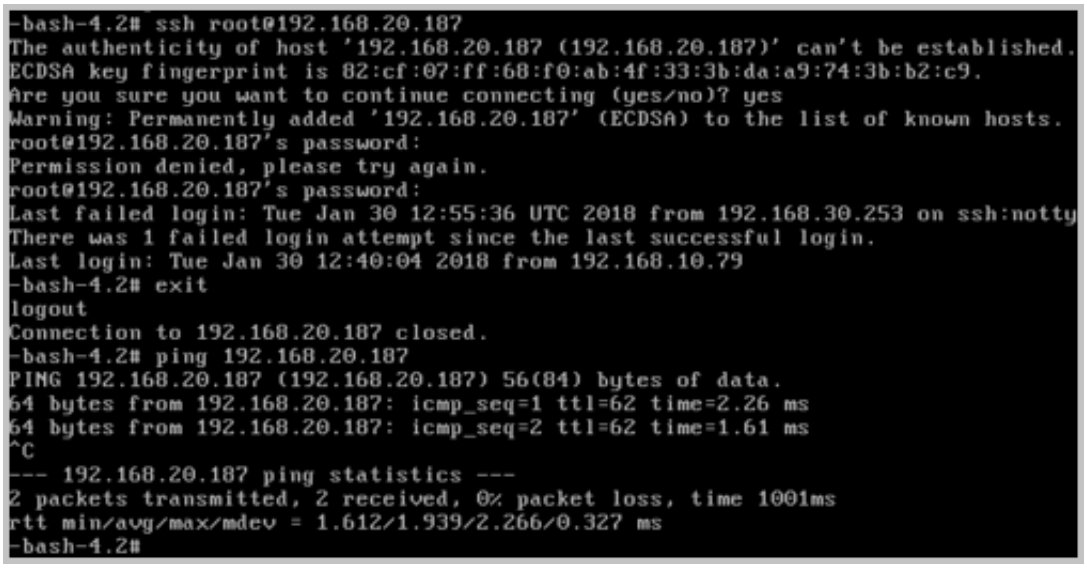


- 登录VM-2，可通过SSH默认的22端口远程登录VM-3、VM-4，以及ping通VM-3、VM-4。
- 登录VM-3，可通过SSH默认的22端口远程登录VM-1、VM-2，以及ping通VM-1、VM-2。

  如图 *610: VM-3成功连通VM-1、VM-2*所示：

  图 610: VM-3成功连通VM-1、VM-2





- 登录VM-4，可通过SSH默认的22端口远程登录VM-1、VM-2，以及ping通VM1、VM-2。

后续操作

至此，VPC IPsec隧道的使用方法介绍完毕。

7.7 vCenter

7.7.1 介绍

VMware vCenter Server是VMware vCenter的集中式管理平台。

针对用户已经部署VMware vCenter Server的应用场景，ZStack支持管纳VMware vCenter，可以通过VMware提供的公开API接口，良好地兼容和管理VMware vCenter Server虚拟化管理平台部分功能，实现多虚拟化平台的统一管理。

支持对现有数据中心中的VMware虚拟化环境进行管理，能够查看VMware vCenter Server所管理的vSphere服务器资源和虚拟机资源，能够在虚拟数据中心中使用VMware vSphere资源，并在VMware vCenter集群中完成对云主机的常用操作。

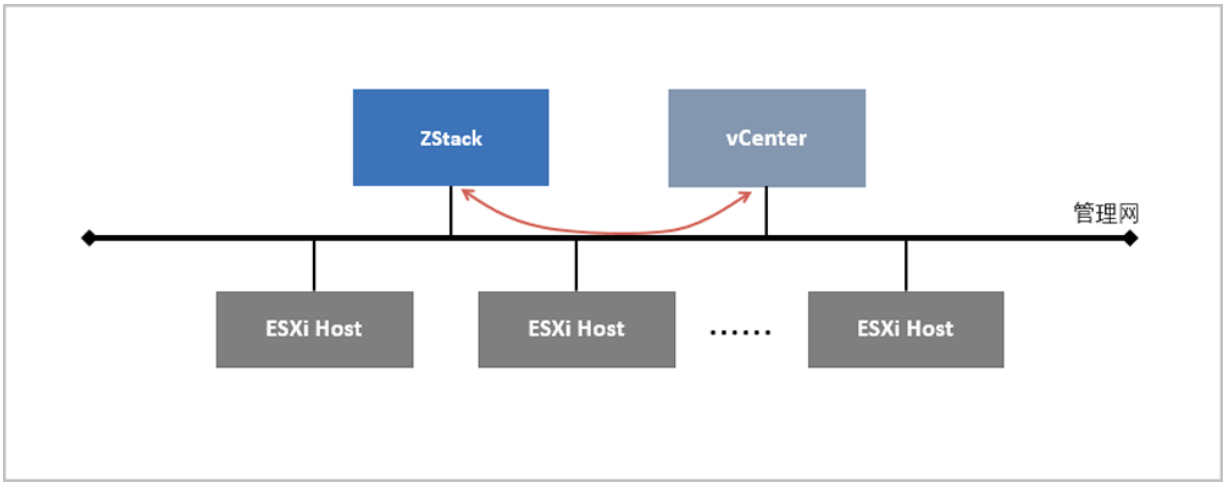
目前，ZStack支持的vCenter版本包括5.5、6.0和6.5。

外部访问原理

ZStack通过异步事件监听方式，发送云资源控制请求到vCenter，并接收返回的事件内容。ZStack支持接收vCenter主动推送内容，实现双向信息同步功能。

ZStack管控vCenter逻辑图如图 *611: ZStack管控vCenter逻辑图*所示：

图 611: ZStack管控vCenter逻辑图



7.7.2 环境准备

通过ZStack管理vCenter，需提前准备好ZStack私有云环境和vCenter环境。

ZStack私有云环境准备

管理员可通过单独的物理服务器部署ZStack管理节点，也可通过vCenter集群的虚拟机部署ZStack管理节点。

1. 软件准备

   - ZStack定制版ISO

  - 文件名称：ZStack-x86_64-DVD-2.5.1-c74.iso或ZStack-x86_64-DVD-2.5.1-c72.iso
  - 下载地址：点击这里
- ZStack安装包
  - 文件名称：ZStack-installer-2.5.1.bin
  - 下载地址：点击这里

注: 软件下载后，需通过MD5校验工具核对校验码，以确保软件完整无损。

2. 硬件准备

准备一台物理服务器，或vCenter集群的一台虚拟机，配置需求如下：

物理服务器 / vCenter虚拟机	参数
ZStack管理节点	• CPU支持64位，不低于4核心 • 内存不低于8GB • 至少1块硬盘，容量不低于500GB • 至少1块千兆网卡
网络	分配网络地址，并畅通访问vCenter服务器；

3. 安装ZStack

在物理服务器或vCenter虚拟机内，使用ZStack定制版ISO安装操作系统，请选择企业版管理节点模式（ZStack Enterprise Management Node），安装完成并重启系统后，将会自动安装ZStack。详情请参考用户手册安装部署章节。

注: vCenter虚拟机选择**CentOS 5/6/7 64位**操作系统类型。

4. 登录ZStack

使用Chrome或FireFox浏览器登录ZStack管理界面（*http://your_machine_ip:5000*），默认用户名为admin，密码为password。

图 612: 登录界面

注:

若使用vCenter虚拟机安装ZStack管理节点，建议此时创建快照（不包含内存），快照命名**初始化**。

vCenter环境准备

ZStack接管vCenter的虚拟化资源，vCenter必须满足以下特性：

- vCenter必须建立**数据中心**、**集群**和**物理机**的资源结构；
- 支持显示已经添加的本地存储和共享存储，包括FC、iSCSI和NFS存储；
- 目前不支持存储集群（Datastore Cluster）模式，建议分离使用；
- vCenter需配置分布式交换机（dvSwitch）或标准交换机（vSwitch）的端口组信息；
- vCenter已有的模板虚拟机，需要转换为【模板】类型。

如图 *613: vCenter显示集群和物理机信息*、图 *614: vCenter显示分布式交换机信息*和图 *615: vCenter显示模板信息*所示：

图 613: vCenter显示集群和物理机信息

图 614: vCenter显示分布式交换机信息

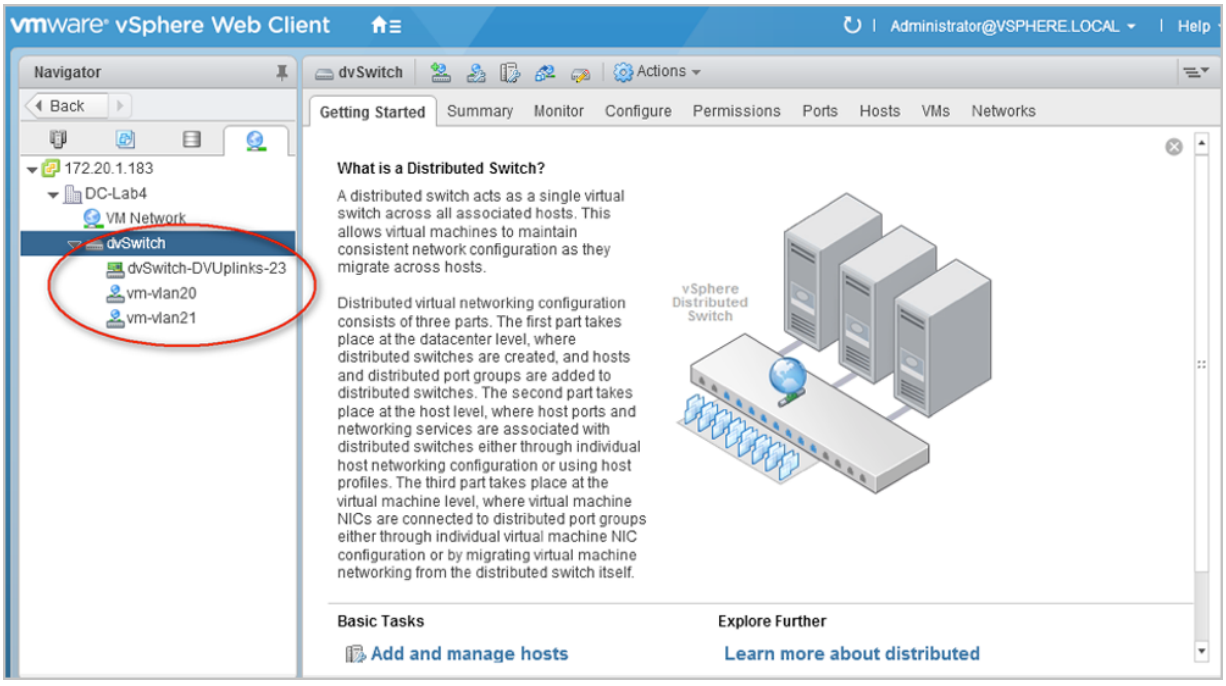
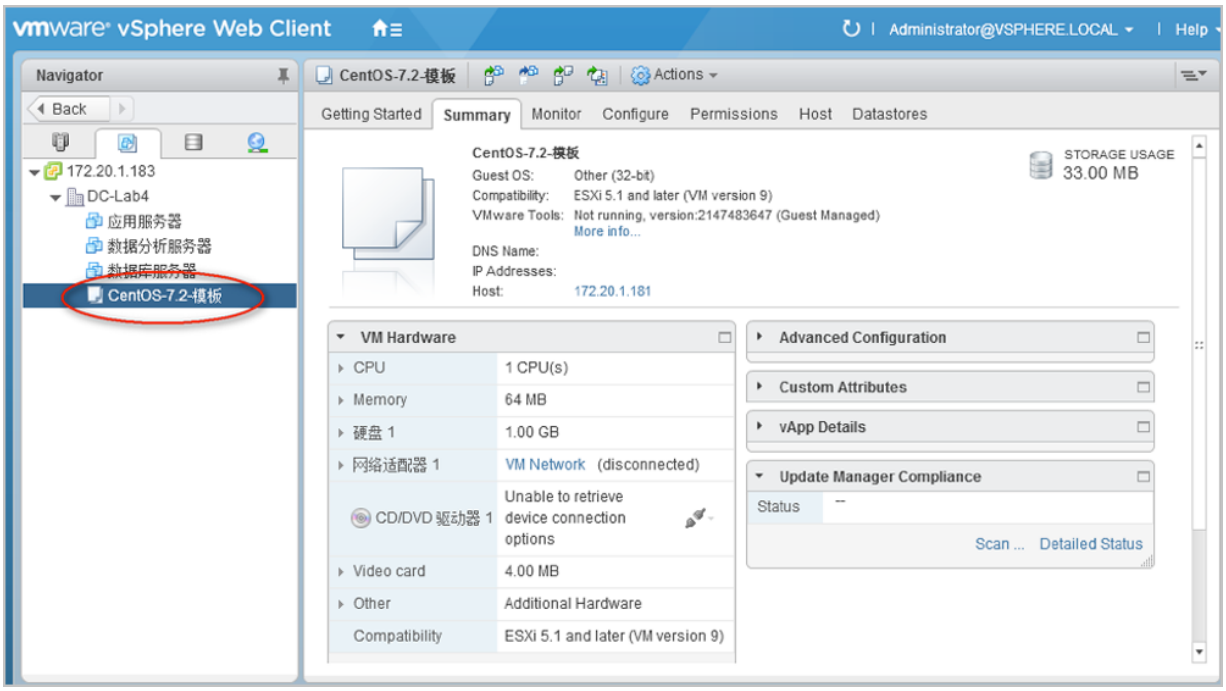


图 615: vCenter显示模板信息



7.7.3 基础资源

背景信息

vCenter的基础资源主要涉及ZStack对vCenter虚拟化资源的统一管理，目前包括：添加vCenter、同步数据和删除。

添加vCenter后，ZStack会自动同步vCenter的集群、物理机、虚拟机、模板、存储、网络等资源。也可通过点击**同步数据**按钮，将vCenter的资源实时同步至本地。相关资源均支持界面查看。

- 支持添加多个vCenter并进行管理；
- vCenter资源导入ZStack支持过滤。
  - dvSwitch场景：

    只有添加到dvSwitch中的物理机，其相关资源才能导入ZStack，未添加到dvSwitch中的物理机，其相关资源不能导入ZStack。
  - vSwitch场景：

    只有添加至少一个相同的vSwitch名称，且具备至少一个相同的端口组属性（包括：相同的网络标签和VLAN ID），满足以上条件的物理机，其相关资源（其上所有虚拟机、相同的端口组）才能导入ZStack。

注： ZStack仅接管虚拟机网络，不接管VMkernel或管理网络。

以下介绍ZStack添加vCenter的方法。

操作步骤

1. 需提前准备以下信息：

字段	意义	示例
访问域名	访问vCenter地址：域名或IP地址	• vc.test.com • 172.20.1.166
管理用户	vCenter管理员名称，包括完整域	administrator@vsphere.local
访问密码	vCenter管理员密码	Testing123

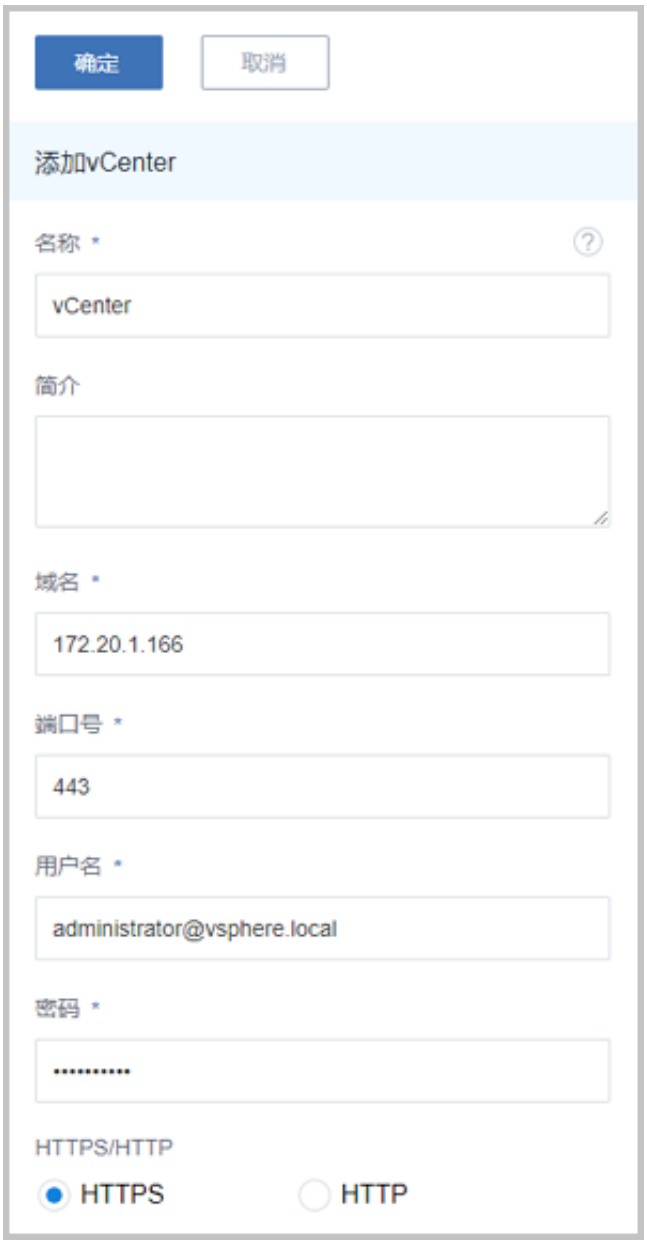
2. 添加vCenter。

   在ZStack私有云主菜单，点击 **vCenter** > **基础资源**，进入**基础资源**界面，点击**添加vCenter**，弹出**添加vCenter**界面，可参考以下示例输入相应内容：

   - **名称**：设置vCenter的名称
   - **简介**：作为可选项，可留空不填
   - **域名**：输入vCenter的域名
   - **端口号**：输入vCenter开放的端口号
   - **用户名**：输入vCenter的用户名
   - **密码**：输入vCenter用户名对应的密码，需与实际环境匹配，注意大小写
   - **HTTPS/HTTP**：选择同步vCenter时的传输协议，支持HTTPS和HTTP，默认HTTPS

   如图 *616: 添加vCenter*所示，点击**确定**，添加vCenter。

   图 616: 添加vCenter



3. 成功添加vCenter后，ZStack将导入vCenter已经存在的集群、物理机、虚拟机、模板、存储、网络等资源。

   vCenter详情页支持查看基本属性、集群、主存储、镜像服务器、物理机和审计。

   - 其中，**主存储**页面和**镜像服务器**页面均支持datastore列表查看，如图 *617: vCenter主存储*和图 *618: vCenter镜像服务器*所示：

     图 617: vCenter主存储

图 618: vCenter镜像服务器

- **物理机**页面支持查看维护模式状态。如图 *619: vCenter物理机*所示：

图 619: vCenter物理机

注:

- 如果远端vCenter上的物理机处于维护模式状态，通过同步数据，可在本地查看该资源状态。

- 在远端vCenter上，物理机进入维护模式前，需手动对云主机执行关机或迁移操作；如果远端vCenter环境已开启DRS（分布式资源调度）服务，物理机处于维护模式状态，云主机自动迁移。

- **审计**页面显示了vCenter的操作日志。

在vCenter详情页，点击**vCenter操作**，支持vCenter的同步数据和删除操作。

后续操作

vCenter基础资源支持的操作：

- 添加vCenter：添加vCenter后，ZStack会自动同步vCenter的集群、物理机、虚拟机、模板、存储、网络等资源，相关资源均支持界面查看。
- 同步数据：通过同步数据，可将vCenter的资源实时同步至本地。
- 删除：删除vCenter会删除vCenter相关资源的本地记录，远端vCenter上的真实资源不受影响。
- 查看集群：查看vCenter集群信息。
- 查看主存储：查看vCenter主存储信息，支持datastore列表查看。
- 查看镜像服务器：查看vCenter镜像服务器信息，支持datastore列表查看。
- 查看物理机：查看vCenter物理机信息。

7.7.4 云主机

背景信息

添加vCenter后，vCenter云主机自动同步至ZStack；也支持本地创建vCenter云主机。

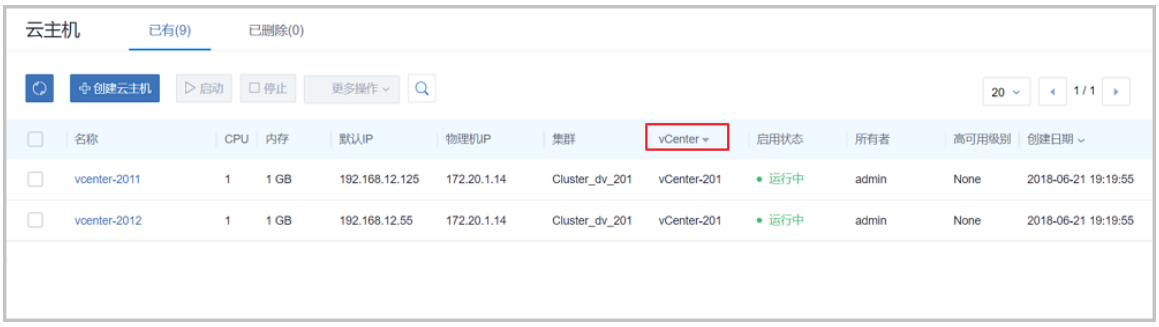
以下介绍ZStack本地创建vCenter云主机的方法。

操作步骤

1. 添加vCenter后，vCenter云主机自动同步至ZStack，在vCenter**云主机**界面可查看详情。

   在ZStack私有云主菜单，点击 **vCenter** > **云主机**，进入**云主机**界面，如图 *620: vCenter云主机界面*所示：

   图 620: vCenter云主机界面



注： ZStack支持多vCenter资源区分，点击**vCenter**按钮，可选择查看全部或某个vCenter下的资源。

2. 本地创建vCenter云主机。

本地创建vCenter云主机，需提前在ZStack中搭建好vCenter云路由网络或扁平网络，具体方法请参考网络章节。

vCenter云路由网络或扁平网络创建后，在vCenter**云主机**界面，点击**创建云主机**，弹出**创建云主机**界面，可参考以下示例输入相应内容：

- **添加方式**：支持创建单个或多个云主机
- **名称**：自定义vCenter云主机的名称
- **简介**：可选项，可留空不填
- **计算规格**：选择vCenter云主机的计算规格
- **镜像**：选择创建vCenter云主机所需要的vCenter镜像
- **网络**：选择已创建好的vCenter云路由网络或扁平网络
- **高级**：可选项，用户可指定填写，如不填写，系统将自动指定
  - **数据云盘规格**：选择挂载云主机上的数据云盘规格
  - **集群**：可指定vCenter的某个集群
  - **主存储**：可指定vCenter的某个主存储
  - **物理机**：可指定vCenter的某个物理机

如图 *621: 本地新建vCenter云主机*所示，点击**确定**，创建vCenter云主机。

图 621: 本地新建vCenter云主机

确定
取消
创建云主机
添加方式
单个
多个
名称 *
vCenter云主机
简介
计算规格 *
InstanceOffering-1
镜像 *
vCenter镜像
网络 *
vCenter扁平网络
默认网络
设置静态IP
高级
数据云盘规格
40G
集群
vc_cluster-165
主存储
datastore1
物理机
192.168.200.13

后续操作

vCenter云主机支持的操作：

- 创建：本地创建vCenter云主机。
- 启动：将停止状态的云主机启动。
- 停止：停止云主机。
- 重启：将云主机重启。
- 暂停：暂停云主机。
- 恢复：从暂停状态恢复云主机。
- 迁移：将云主机迁移到别的计算节点中。
  - 目前仅支持热迁移。
  - 共享存储支持带数据云盘的云主机热迁移。
  - 本地存储暂不支持迁移操作。
  - 迁移的速度与两台主机的网络配置有关，如果网络配置较低，迁移速度可能较慢。
  - 执行迁移操作前，需确保vMotion功能已开启。
    - vCenter 5.5版本，需配置专用的VMKernel网络并开启vMotion功能，且源端和目标端的VMkernel子接口vMotion的IP地址能互通。
    - vCenter 6.0版本及以上，开启管理网络中的vMotion功能即可。
- 克隆：对云主机根云盘进行复制，根据此云主机的计算规格，克隆出与当前云主机相同系统的云主机。
  - 云主机支持在线克隆、关机克隆。
  - 带数据云盘的云主机暂不支持整机克隆。
  - 云主机支持克隆为云主机（暂不支持克隆为模板）。
- 关闭电源：将云主机电源直接断电。
- 修改计算规格：支持离线修改云主机CPU/内存。
- 设置高可用：高可用级别有NeverStop或None两种模式。
  - None：云主机关闭高可用功能
  - NeverStop：云主机开启高可用功能

    本地存储的云主机设置为NeverStop：

    - 当所在物理机处于**启用**和**已连接**状态时，该云主机会一直运行。即使强制关机，该云主机也会再次启动。

注:

如希望NeverStop云主机本次关机不自动启动，在弹出的**停止云主机**窗口，勾选**设置NeverStop的云主机**，**本次停止将不会自动启动**即可。

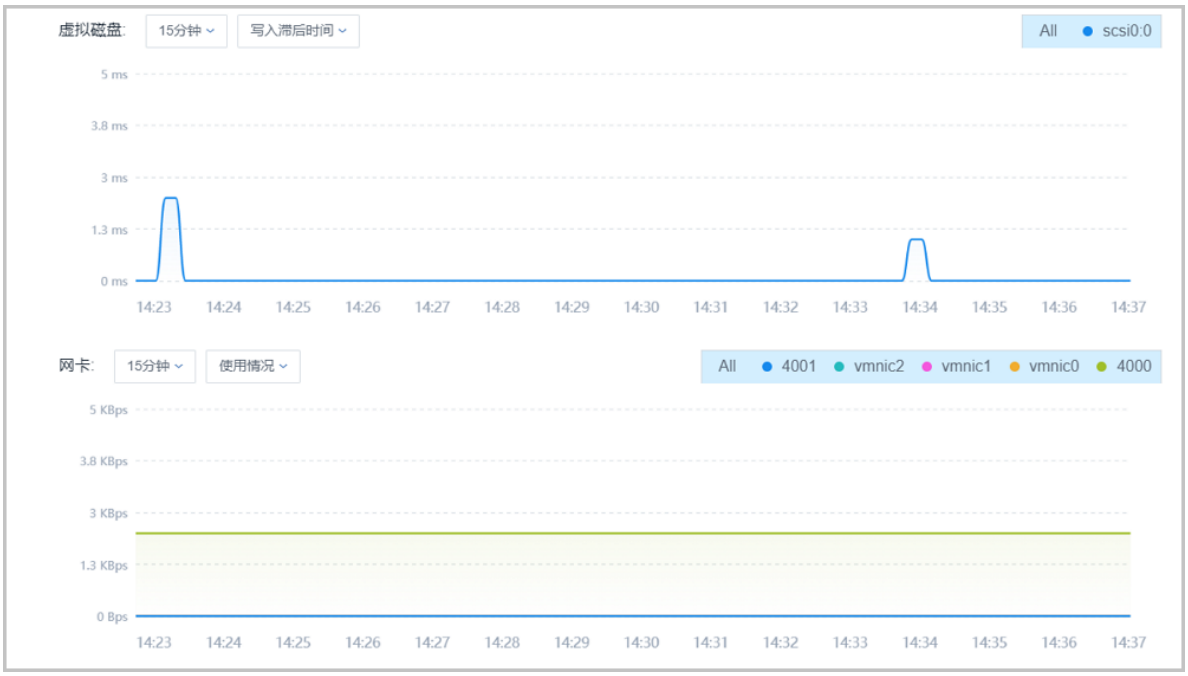
- 当所在物理机异常断电/断网时，该云主机会进入**已停止**状态。

- 如果远端vCenter环境已开启DRS（分布式资源调度）服务，为vCenter云主机提供高可用，ZStack的高可用设置与其无关，不受影响。

- 打开控制台：打开云主机的控制界面，可以登录控制云主机。
- 设置控制台密码：设置云主机的控制台密码。
- 取消控制台密码：取消云主机的控制台密码。
- 加载云盘：将一个可用的未加载的云盘加载到当前云主机。
- 卸载云盘：之前添加的云盘从云主机卸载。
- 删除：删除云主机，会删除本地记录，同时远端vCenter上的真实云主机停止。
- 恢复：从删除状态恢复云主机。
- 彻底删除：将删除状态的云主机彻底删除，会同时彻底删除本地记录和远端vCenter上的真实云主机资源。
- 查看监控数据：在vCenter云主机详情页，点击**监控数据**子页面，可查看vCenter云主机的CPU、内存、磁盘、虚拟磁盘和网卡的实时监控图，如图 *622:* 监控数据所示：

图 622: 监控数据

云主机操作
基本属性
配置信息
监控数据
审计
CPU:
15分钟
使用情况
5%
3.75%
2.5%
1.25%
0%
14:22 14:23 14:24 14:25 14:26 14:27 14:28 14:30 14:31 14:32 14:33 14:34 14:35 14:36 14:37
内存:
15分钟
已授权
939.4 M
704.6 M
469.7 M
234.9 M
0 Byte
14:22 14:23 14:24 14:25 14:26 14:27 14:28 14:30 14:31 14:32 14:33 14:34 14:35 14:36 14:37
磁盘:
15分钟
使用情况
18 KBps
13 KBps
9 KBps
4 KBps
0 Bps
14:22 14:23 14:24 14:26 14:27 14:28 14:29 14:30 14:31 14:32 14:33 14:34 14:35 14:36 14:37


虚拟磁盘:
15分钟
写入滞后时间
All
scsi0:0
5 ms
3.8 ms
3 ms
1.3 ms
0 ms
14:23 14:24 14:25 14:26 14:27 14:28 14:29 14:30 14:31 14:32 14:33 14:34 14:35 14:36 14:37
网卡:
15分钟
使用情况
All
4001
vmnic2
vmnic1
vmnic0
4000
5 KBps
3.8 KBps
3 KBps
1.3 KBps
0 Bps
14:23 14:24 14:25 14:26 14:27 14:28 14:29 14:30 14:31 14:32 14:33 14:34 14:35 14:36 14:37

7.7.5 网络

要在ZStack接管的vCenter环境中新建云主机，需提前搭建好vCenter中的云路由网络或扁平网络。

7.7.5.1 云路由网络

背景信息

搭建vCenter云路由网络，需提前确认ZStack管理节点与vCenter物理机能互相访问。

以下介绍搭建vCenter云路由网络的方法。

操作步骤

1. 在vCenter中创建公有网络（包括二层公有网络和三层公有网络）。

   在ZStack私有云主菜单，点击 **vCenter** > **网络**，进入**网络**主界面，点击**添加网络**，弹出**创建网络**界面，可参考以下示例输入相应内容：

   - **公有网络**：选择创建公有网络
   - **名称**：自定义vCenter公有网络名称
   - **简介**：作为可选项，可留空不填
   - **类型**：按实际情况选择需要搭建的二层公有网络类型
     - 支持L2NoVlanNetwork、L2VlanNetwork两种类型
     - 如选择L2VlanNetwork，需输入Vlan ID
   - **Switch**：按实际情况输入vCenter的dvSwitch或vSwitch名称
   - **集群**：选择vCenter的集群
   - **添加网络段**：选择**IP范围**或**CIDR**方式添加网络段：
     - **IP范围**

       使用IP范围方式可填写类似*172.20.58.200*到*172.20.58.220*，子网掩码填写*255.255.0.0*，网关填写*172.20.0.1*。
     - **CIDR**

       使用CIDR一般填写类似*192.168.1.1/24*。
   - **添加DNS**：添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*

   如图 *623: 创建vCenter公有网络*所示，点击**确定**，创建vCenter公有网络。

   图 623: 创建vCenter公有网络

确定
取消
创建网络
公有网络
私有网络
名称 *
vCenter公有网络
简介
类型
L2NoVlanNetwork
Switch *
DSwitch
集群
Cluster_188_2
添加网络段
方法
IP 范围
CIDR
起始IP *
172.20.58.200
结束IP *
172.20.58.220
子网掩码 *
255.255.0.0
网关 *
172.20.0.1

2. 在创建vCenter云路由网络前，需提前在**网络资源**中准备好云路由镜像和云路由规格。

   a) 添加vCenter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**主界面，点击**添加云路由镜像**，弹出**添加云路由镜像**界面，可参考以下示例输入相应内容：

   - **名称**：自定义云路由镜像名称
   - **简介**：作为可选项，可留空不填
   - **镜像服务器**：选择vCenter的镜像服务器
   - **镜像路径**：目前支持添加URL路径方式上传vCenter云路由镜像

     注:

     ZStack提供专用的vCenter云路由镜像供用户使用，可在*ZStack*官方网站上找到最新的云路由镜像下载地址。

     - 文件名称：zstack-vrouter-2.5.1.vmdk
     - 下载地址：点击这里查看

   如图 *624: 添加vCenter云路由镜像*所示：

   图 624: 添加vCenter云路由镜像

b) 添加vCenter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**主界面，点击**创建云路由规格**，弹出**创建云路由规格**界面，可参考以下示例输入相应内容：

- **名称**：自定义云路由规格名称
- **简介**：作为可选项，可留空不填
- **CPU**：设置云路由规格的CPU数目
- **内存**：设置云路由规格的内存大小，单位包括：M、G、T
- **镜像**：选择已添加好的vCenter云路由镜像
- **管理网络**：按实际情况选择管理网络，示例中管理网络与公有网络为同一网络
- **公有网络**：选择已创建好的vCenter公有网络

如图 *625: 创建vCenter云路由规格*所示：

图 625: 创建vCenter云路由规格

3. 创建vCenter云路由网络。

   在ZStack私有云主菜单，点击 **vCenter** > **网络**，进入**网络**主界面，点击**创建网络**，弹出**创建网络**界面，可参考以下示例输入相应内容：

   - **私有网络**：选择创建私有网络
   - **名称**：自定义vCenter云路由网络名称
   - **简介**：可选项，可留空不填

- **类型**：按实际情况选择需要搭建的二层公有网络类型
  - 支持L2NoVlanNetwork、L2VlanNetwork两种类型
  - 如选择L2VlanNetwork，需输入Vlan ID
- **Switch**：按实际情况输入vCenter的dvSwitch或vSwitch名称
- **集群**：选择vCenter的集群
- **云路由**：选择云路由网络架构类型
- **云路由规格**：选择已经创建好的vCenter云路由规格
- **添加网络段**：选择**IP范围**或**CIDR**方式添加网络段：

  1. **IP范围**

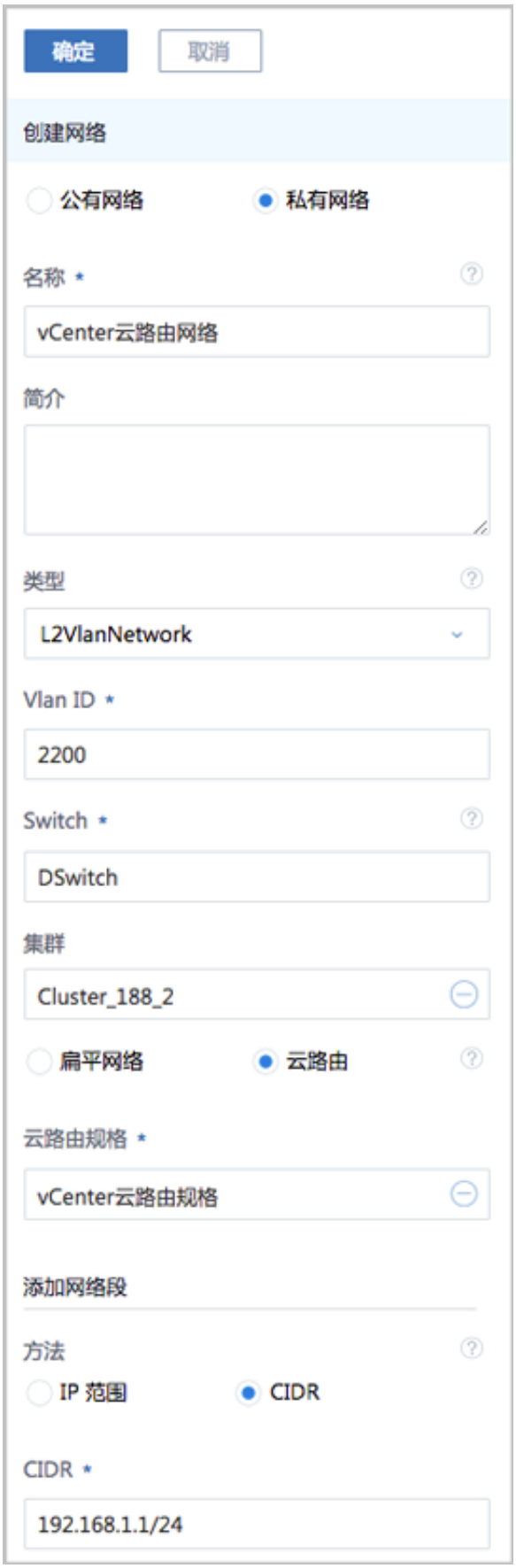
     使用IP范围方式可填写类似*172.20.58.200*到*172.20.58.220*，子网掩码填写*255.255.0.0*，网关填写*172.20.0.1*。

  2. **CIDR**

     使用CIDR一般填写类似*192.168.1.1/24*。
- **添加DNS**：可选项，添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*

如图 *626:* 创建*vCenter*云路由网络所示，点击**确定**，成功创建vCenter云路由网络。

图 626: 创建vCenter云路由网络


确定
取消
创建网络
公有网络
私有网络
名称 *
vCenter云路由网络
简介
类型
L2VlanNetwork
Vlan ID *
2200
Switch *
DSwitch
集群
Cluster_188_2
扁平网络
云路由
云路由规格 *
vCenter云路由规格
添加网络段
方法
IP 范围
CIDR
CIDR *
192.168.1.1/24

7.7.5.2 扁平网络

背景信息

以下介绍搭建vCenter扁平网络的方法。

操作步骤

1. 创建vCenter扁平网络。

   在ZStack私有云主菜单，点击 **vCenter** > **网络**，进入**网络**主界面，点击**添加网络**，弹出**创建网络**界面，可参考以下示例输入相应内容：

   - **私有网络**：选择创建私有网络
   - **名称**：自定义vCenter扁平网络名称
   - **简介**：可选项，可留空不填
   - **类型**：按实际情况选择需要搭建的二层私有网络类型
     - 支持L2NoVlanNetwork、L2VlanNetwork两种类型
     - 如选择L2VlanNetwork，需输入Vlan ID
   - **Switch**：按实际情况输入vCenter的dvSwitch或vSwitch名称
   - **集群**：选择vCenter的集群
   - **扁平网络**：选择扁平网络架构类型
     - **关闭DHCP服务**为灰色，不可设置
     - vCenter扁平网络不能给云主机自动分配IP，需手动配置，建议与预设的IP一致
   - **添加网络段**：选择**IP范围**或**CIDR**方式添加网络段：

     1. **IP范围**

        使用IP范围方式可填写类似*172.20.58.100*到*172.20.58.120*，子网掩码填写*255.255.0.0*，网关填写*172.20.0.1*。

     2. **CIDR**

        使用CIDR一般填写类似*192.168.1.1/24*。
   - **添加DNS**：添加DNS服务器，可指定*8.8.8.8*或*114.114.114.114*。

2. 点击**确定**，成功创建vCenter扁平网络。

   如图 *627: 创建vCenter扁平网络*所示：

   图 627: 创建vCenter扁平网络

确定
取消
创建网络
公有网络
私有网络
名称 *
vCenter扁平网络
简介
类型
L2NoVlanNetwork
Switch *
vSwitch0
集群
vc_cluster-165
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 *
172.20.58.100
结束IP *
172.20.58.120
子网掩码 *
255.255.0.0
网关 *
172.20.0.1

后续操作

vCenter网络支持的操作：

- vCenter公有网络：添加网络段、添加DNS、删除网络段、删除DNS、删除
- vCenter扁平网络：添加网络段、添加DNS、删除网络段、删除DNS、删除
- vCenter云路由网络：添加网络段、添加DNS、删除网络段、删除DNS、加载云路由规格、卸载云路由规格、删除

注: 删除vCenter网络资源，会删除本地记录，远端vCenter上的真实网络资源不受影响。（删除L3网络时，挂载该L3网络的vCenter云主机会将该L3网络卸载。）

7.7.5.3 网络服务

vCenter网络服务目前支持云路由网络架构模型。

vCenter云路由网络提供了DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道等网络服务。

- DNS：
  - vCenter云路由器可作为DNS服务器提供DNS服务；
  - 在vCenter云主机中看到的DNS地址默认为vCenter云路由器的IP地址，由用户设置的DNS地址由vCenter云路由器负责转发配置。
- SNAT：
  - vCenter云路由器向vCenter云主机提供原网络地址转换；
  - vCenter云主机使用SNAT可直接访问外部互联网。
- 弹性IP：使用vCenter云路由器可通过公有网络访问vCenter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vCenter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vCenter云主机，并自动检测并隔离不可用的vCenter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。

7.7.5.3.1 虚拟IP(ESX类型)

vCenter云路由网络是通过ESX类型的虚拟IP来提供弹性IP、端口转发、负载均衡、IPsec隧道等网络服务的。

ESX类型的虚拟IP也分为自定义虚拟IP和系统虚拟IP两类，与KVM类型的虚拟IP基本相同。

1. ESX类型的自定义虚拟IP

- 创建：由用户手动创建。
- 提供网络服务：
  - vCenter云路由网络下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务。
  - 一个自定义虚拟IP仅用于一个弹性IP服务实例。
  - 一个自定义虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

    注: 不同类型服务不能使用相同的端口号。

  - 自定义虚拟IP不支持跨vCenter云路由器使用。
- 删除：
  - 删除自定义虚拟IP，将自动删除其上绑定的所有服务。
  - 删除自定义虚拟IP的某一服务，并不影响其上绑定的其它服务运行。

2. ESX类型的系统虚拟IP

- 创建：

  vCenter云路由器成功创建后，由系统自动创建，该系统虚拟IP地址就是路由设备的默认公网IP地址。
- 提供网络服务：
  - vCenter云路由网络下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务。
  - 一个系统虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

    注: 不同类型服务不能使用相同的端口号。

  - 系统虚拟IP与vCenter云路由器一一对应。
- 删除：
  - 删除系统虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
  - 删除vCenter云路由器，将自动删除相应的系统虚拟IP以及其上绑定的所有服务。

虚拟IP(ESX类型)的使用方法

ESX类型的虚拟IP的使用方法，与KVM类型的虚拟IP的使用方法基本相同。

- ESX类型的自定义虚拟IP：

  vCenter云路由网络下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务。使用方法有两种：

  - 在ZStack私有云主菜单，点击**网络服务 > 虚拟IP**，在**自定义虚拟IP**界面创建自定义虚拟IP后，在**弹性IP**、**端口转发**、**负载均衡器**、**IPsec隧道**界面，选择使用已有虚拟IP。
  - 在ZStack私有云主菜单，点击**网络服务 > 弹性IP/端口转发/负载均衡器/IPsec隧道**，在**弹性IP**、**端口转发**、**负载均衡器**、**IPsec隧道**界面，选择新建虚拟IP。
- ESX类型的系统虚拟IP

  vCenter云路由网络下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务。使用方法有一种：

  - 在ZStack私有云主菜单，点击**网络服务 > 端口转发/负载均衡器/IPsec隧道**，在**端口转发**、**负载均衡器**、**IPsec隧道**界面，选择使用已有虚拟IP。

创建自定义虚拟IP(ESX类型)

ESX类型的自定义虚拟IP的创建方法，与KVM类型的自定义虚拟IP的创建方法基本相同。

在ZStack私有云主菜单，点击**网络服务 > 虚拟IP**，进入**自定义虚拟IP**界面，点击**创建虚拟IP**，在弹出的**创建虚拟IP**界面，依次输入相应内容即可。

注： **网络**项需选择提供虚拟IP的vCenter公有网络。

如图 *628: 创建自定义虚拟IP(ESX类型)*所示：

图 628: 创建自定义虚拟IP(ESX类型)

虚拟IP(ESX类型)支持的操作

ESX类型的虚拟IP支持的操作，与KVM类型的虚拟IP支持的操作基本相同。

- 创建虚拟IP：自定义虚拟IP由用户手动创建，系统虚拟IP由系统自动创建。
- 修改名称和简介：修改虚拟IP的名称和简介。
- 更改所有者：变更虚拟IP的所有者。
- 删除：
  - 自定义虚拟IP：
    - 删除自定义虚拟IP，将自动删除其上绑定的所有服务。
    - 删除自定义虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
  - 系统虚拟IP：
    - 删除系统虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
    - 删除vCenter云路由器，将自动删除相应的系统虚拟IP以及其上绑定的所有服务。

7.7.5.3.2 弹性IP

vCenter云路由网络通过ESX类型的自定义虚拟IP来提供弹性IP服务。

- 基于弹性IP服务，vCenter云路由器可通过公有网络访问vCenter云主机的私有网络。

创建弹性IP

vCenter云路由环境下创建弹性IP的方法，与KVM云路由环境下创建弹性IP的方法基本相同。

在**私有云**界面，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，依次输入相应内容即可。

注:

- 如选择新建虚拟IP提供弹性IP服务，**网络**项需选择提供虚拟IP的vCenter公有网络。

  如图 *629: 新建虚拟IP*所示：

  图 629: 新建虚拟IP

- 如选择已有虚拟IP提供弹性IP服务，**虚拟IP**项需选择已有的ESX类型的自定义虚拟IP。

  如图 *630: 已有虚拟IP*所示：

  图 630: 已有虚拟IP

弹性IP支持的操作

vCenter云路由环境下弹性IP支持的操作，与KVM云路由环境下弹性IP支持的操作基本相同。

- 修改名称和简介：修改弹性IP的名称和简介。
- 绑定：将弹性IP绑定到云主机网卡。
- 解绑：将弹性IP与云主机网卡解绑。
- 更改所有者：变更弹性IP的所有者。
- 删除：删除弹性IP，将自动删除其提供的弹性IP服务。如需同时删除相应的虚拟IP，请勾选**删除虚拟IP**。
- 审计：查看此弹性IP的相关操作。

7.7.5.3.3 端口转发

vCenter云路由网络通过ESX类型的自定义虚拟IP或系统虚拟IP来提供端口转发服务。

- 基于端口转发服务，vCenter云路由器可将指定公有网络的IP地址端口流量转发到vCenter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vCenter云主机对外服务，节省公网IP地址资源。

创建端口转发规则

vCenter云路由环境下创建端口转发规则的方法，与KVM云路由环境下创建端口转发规则的方法基本相同。

在**私有云**界面，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，依次输入相应内容即可。

注:

- 如选择新建虚拟IP提供端口转发服务，**网络**项需选择提供虚拟IP的vCenter公有网络。

  如图 *631: 新建虚拟IP*所示：

  图 631: 新建虚拟IP

- 如选择已有虚拟IP提供端口转发服务，**虚拟IP**项需选择已有的ESX类型的自定义虚拟IP或ESX类型的系统虚拟IP。

  如图 *632: 已有虚拟IP*所示：

  图 632: 已有虚拟IP

端口转发规则绑定云主机网卡

弹出**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，选择需绑定的vCenter云主机网卡，点击**确定**。

如图 *633: 选择云主机网卡*和图 *634: 端口转发规则绑定云主机网卡*所示：

图 633: 选择云主机网卡

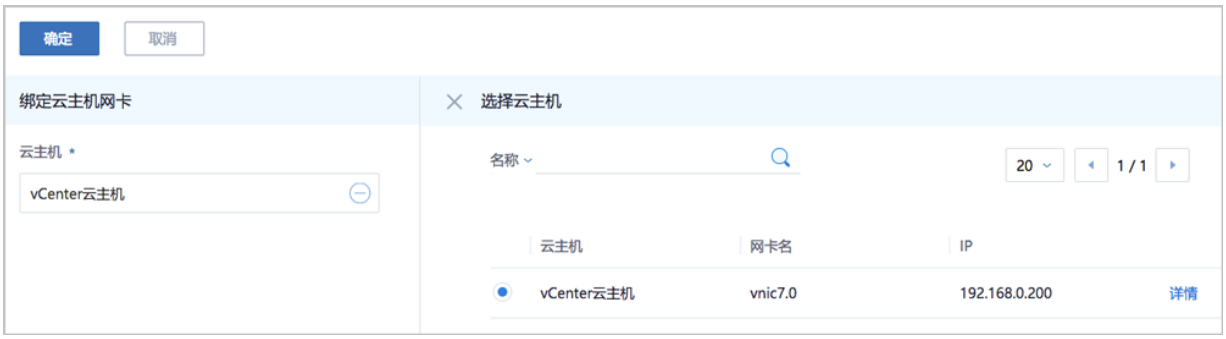


图 634: 端口转发规则绑定云主机网卡

端口转发支持的操作

vCenter云路由环境下端口转发支持的操作，与KVM云路由环境下端口转发支持的操作基本相同。

- 修改名称和简介：修改端口转发规则的名称和简介。
- 绑定：将端口转发规则绑定到云主机网卡。
- 解绑：将端口转发规则与云主机网卡解绑。
- 删除：删除端口转发规则，将自动删除其提供的端口转发服务。相应的虚拟IP以及其上绑定的其它服务不受影响。
- 审计：查看此端口转发的相关操作。

端口转发的约束条件

vCenter云路由环境下端口转发的约束条件，与KVM云路由环境下端口转发的约束条件基本相同。

- 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。

7.7.5.3.4 负载均衡

vCenter云路由网络通过ESX类型的自定义虚拟IP或系统虚拟IP来提供负载均衡服务。

- 基于负载均衡服务，可将vCenter公网地址的访问流量分发到一组后端的vCenter云主机， 并支持自动检测并隔离不可用的vCenter云主机，从而提高业务的服务能力和可用性。
- 负载均衡器支持HTTP/TCP两种协议。
- 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。

负载均衡的使用方法

vCenter云路由环境下负载均衡的使用流程，与KVM云路由环境下负载均衡的使用流程基本相同。

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。

创建负载均衡器

vCenter云路由环境下创建负载均衡器的方法，与KVM云路由环境下创建负载均衡器的方法基本相同。

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，依次输入相应内容即可。

注:

- 如选择新建虚拟IP提供负载均衡服务，**网络**项需选择提供虚拟IP的vCenter公有网络。

  如图 *635: 新建虚拟IP*所示：

  图 635: 新建虚拟IP

- 如选择已有虚拟IP提供负载均衡服务，**虚拟IP**项需选择已有的ESX类型的自定义虚拟IP或ESX类型的系统虚拟IP。

  如图 *636: 已有虚拟IP*所示：

  图 636: 已有虚拟IP

添加监听器

vCenter云路由环境下添加监听器的方法，与KVM云路由环境下添加监听器的方法基本相同。

绑定云主机网卡到监听器

在**负载均衡器**主界面，点击已创建的负载均衡器，进入其详情页，点击**监听器**，进入**监听器**子界面，点击已创建的监听器，进入其详情页，点击**云主机网卡**，进入**云主机网卡**子界面，点击**操作** > **绑定云主机网卡**，将弹出**绑定云主机网卡**界面。

如图 *637: 进入监听器详情页*所示：

图 637: 进入监听器详情页

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vCenter云路由器挂载的三层私有网络

- **云主机网卡**：选择vCenter云主机网卡

如图 *638:* 绑定云主机网卡到监听器所示，点击**确定**，绑定云主机网卡到监听器。

图 638: 绑定云主机网卡到监听器

负载均衡支持的操作

vCenter云路由环境下负载均衡器支持的操作，与KVM云路由环境下负载均衡器支持的操作基本相同。

- 修改名称和简介：修改负载均衡器的名称和简介。
- 创建监听器：创建一个新的监听器。
- 删除：删除负载均衡器，将自动删除所有的监听器和相关负载均衡服务。相应的虚拟IP以及其上绑定的其它服务不受影响。
- 审计：查看此负载均衡器的相关操作。

vCenter云路由环境下监听器支持的操作，与KVM云路由环境下监听器支持的操作基本相同。

- 修改名称和简介：修改监听器的名称和简介。
- 绑定云主机网卡：绑定云主机网卡到负载均衡器的某个监听器，使云主机成为监听器规则的一个负载均衡资源。
- 解绑云主机网卡：从监听器上解绑云主机网卡，将其从负载均衡池中移除。
- 绑定证书：当监听协议为HTTPS，需绑定证书使用，绑定一个证书或证书链到监听器。当监听协议为TCP/HTTP，该按钮禁用。

- 解绑证书：当监听协议为HTTPS，从监听器上解绑证书。当监听协议为TCP/HTTP，该按钮禁用。
- 删除：删除监听器，将自动删除其提供的负载均衡服务。
- 审计：查看此监听器的相关操作。

负载均衡的约束条件

vCenter云路由环境下负载均衡的约束条件，与KVM云路由环境下负载均衡的约束条件基本相同。

- 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。

7.7.5.3.5 IPsec隧道

vCenter云路由网络通过ESX类型的自定义虚拟IP或系统虚拟IP来提供IPsec隧道服务。

- 基于IPsec隧道服务，可实现站点到站点（site-to-site）的虚拟私有网络（VPN）连接。

云路由网络下IPsec隧道的使用方法

vCenter云路由环境下IPsec隧道的使用流程，与KVM云路由环境下IPsec隧道的使用流程基本相同。

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。

在第一套ZStack中创建IPsec隧道

vCenter云路由环境下创建IPsec隧道的方法，与KVM云路由环境下创建IPsec隧道的方法基本相同。

在ZStack私有云主菜单，点击**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，依次输入相应内容即可。

注:

- 如选择新建虚拟IP提供IPsec隧道服务，**网络**项需选择提供虚拟IP的vCenter公有网络。

  如图 *639: 新建虚拟IP*所示：

  图 639: 新建虚拟IP

- 如选择已有虚拟IP提供IPsec隧道服务，**虚拟IP**项需选择已有的ESX类型的自定义虚拟IP或ESX类型的系统虚拟IP。

  如图 *640: 已有虚拟IP*所示：

  图 640: 已有虚拟IP

- **本地子网**项需选择本地vCenter云路由器挂载的私有网络，如果vCenter云路由器仅挂载一个私网则会默认选中该私网。

如图 *641: 创建IPsec隧道-1*所示：

图 641: 创建IPsec隧道-1

确定
取消
创建IPsec隧道
名称 *
IPsec隧道-1
简介
选择虚拟IP
虚拟IP方法
新建虚拟IP
已有虚拟IP
网络 *
vCenter公有网络
指定IP
本地子网 *
vCenter云路由网络
远端网络IP *
10.108.14.126
远端网络CIDR *
192.168.100.0/24
认证密钥 *
test1234

在第二套ZStack中创建IPsec隧道

在第二套ZStack中创建IPsec隧道的步骤与第一套步骤相同，只是参数存在差异。

IPsec隧道搭建完毕后，两套ZStack的私网可以互通。

IPsec隧道支持的操作

vCenter云路由环境下IPsec隧道支持的操作，与KVM云路由环境下IPsec隧道支持的操作基本相同。

- 修改名称和简介：修改IPsec隧道的名称和简介。
- 删除：删除IPsec隧道，将自动删除其提供的IPsec隧道服务。相应的虚拟IP以及其上绑定的其它服务不受影响。
- 审计：查看此IPsec隧道的相关操作。

7.7.6 云盘

背景信息

vCenter云盘：为vCenter云主机提供存储。可分为：

- 根云盘：云主机的系统云盘，用于支撑云主机的系统运行。
- 数据云盘：云主机使用的数据云盘，一般用于扩展的存储使用。

vCenter云盘管理主要涉及vCenter数据云盘的管理。

以下介绍ZStack创建vCenter云盘的方法。

操作步骤

1. 创建vCenter云盘。

   在ZStack私有云主菜单，点击**vCenter** > **云盘**，进入**云盘**界面，如图 *642: vCenter云盘*所示：

   图 642: vCenter云盘

注： ZStack支持多vCenter资源区分，点击**vCenter**按钮，可选择查看全部或某个vCenter下的资源。

点击**创建云盘**按钮，弹出**创建云盘**界面，可参考以下示例输入相应内容：

- **名称**：自定义vCenter云盘的名称
- **简介**：可选项，可留空不填
- **创建方式**：创建vCenter云盘支持两种方式：基于云盘规格方式、基于云盘镜像方式
  - **云盘规格**：

    若选择基于云盘规格创建vCenter云盘，需设置以下内容：

    - **云盘规格**：选择合适的云盘规格
    - **主存储**和**云主机**：两项均为可选项
      - 两项均留空不填：创建的云盘为未实例化的云盘，显示在未实例化栏中

        注：

        未实例化云盘没有占用任何实际空间，只是一个概念性的设备，当挂载到云主机后，才会实例化。
      - 两项均填写：创建的云盘会在指定的主存储中创建，并绑定指定的云主机
      - 只填写**云主机**：创建的云盘会自动在指定云主机所在的主存储中创建
      - 只填写**主存储**：创建的云盘会在指定的主存储中创建，为可用状态，且占用真正的空间
  - **云盘镜像**：

    若选择基于vCenter云盘镜像创建vCenter云盘，需设置以下内容：

    - **云盘镜像**：选择合适的云盘镜像，需提前将所需云盘镜像上传至镜像服务器中

- **云主机**：选择需绑定的云主机，创建的云盘会自动在指定云主机所在的主存储中创建
- **指定主存储**：可选项，若勾选此项，云盘会在指定的主存储中创建

基于云盘规格创建vCenter云盘如图 *643: 基于云盘规格创建vCenter云盘*所示：

图 643: 基于云盘规格创建vCenter云盘

基于vCenter云盘镜像创建vCenter云盘如图 *644: 基于vCenter云盘镜像创建vCenter云盘*所示：

图 644: 基于vCenter云盘镜像创建vCenter云盘

2. 点击**确定**按钮，vCenter云盘成功创建。

后续操作

vCenter云盘与KVM环境下的云盘类似，分为已有云盘、未示例化云盘和已删除云盘三类。

已有云盘支持的操作：

- 创建：基于云盘规格或云盘镜像创建一个新的云盘。
- 启用：将处于停用状态的云盘启用。
- 停用：停止使用某个云盘。
- 加载：将选中的云盘作为数据云盘加载到指定云主机。
- 卸载：卸载云主机的云盘。

- 删除：将云盘删除后， 云盘会显示在**已删除**栏。
- 修改名称和简介：支持修改云盘名称和简介

未实例化云盘支持的操作：

- 启用：将处于停用状态的未实例化云盘启用。
- 停用：停止使用某个未实例化云盘。
- 加载：将选中的未实例化云盘作为数据云盘加载到指定云主机。
- 删除：将未实例化云盘删除后， 云盘会显示在**已删除**栏。
- 修改名称和简介：支持修改未实例化云盘名称和简介

已删除云盘支持的操作：

- 恢复：已删除云盘恢复后将显示在已有栏。
- 彻底删除：将已删除云盘彻底删除。

使用vCenter云盘，需注意：

- 不同Hypervisor上的云盘不可挂载到不同类型的云主机上。例如，KVM云主机的云盘不能被vCenter云主机加载。
- 云盘可在相同类型Hypervisor的不同云主机之间挂载和卸载。
- 云盘同一时间只能挂载到一个云主机。
- 云盘占用空间采用虚拟容量来计算。创建云盘时扣除的是云盘的虚拟容量大小，而本身只占用少量实际容量。随着写入文件额增加，实际容量会逐步增加。
- 根云盘作为云主机的附属，不能卸载。

7.7.7 镜像

背景信息

ZStack支持添加vmdk格式的本地镜像到vCenter。通过同步数据，vCenter镜像在本地和远端实现状态同步。支持添加两种镜像类型：系统镜像和云盘镜像。

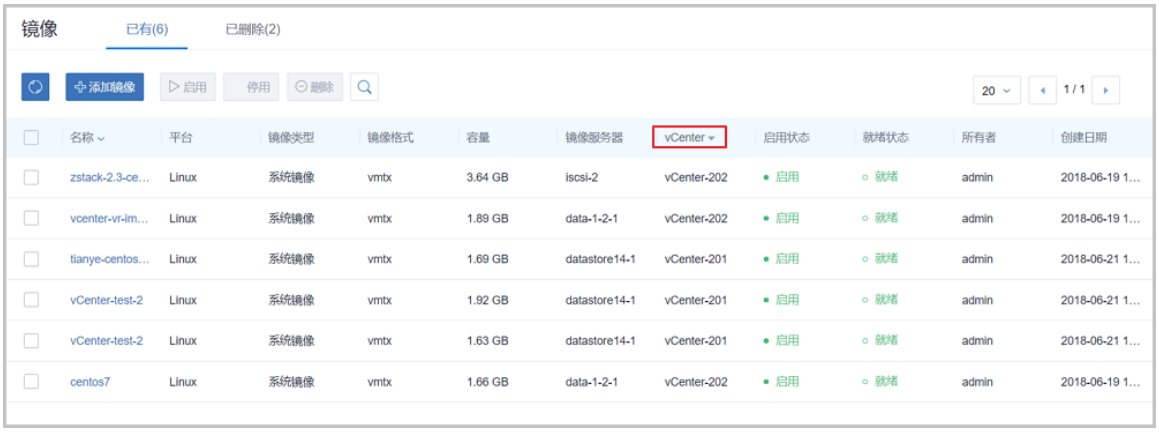
以下介绍ZStack添加vCenter镜像的方法。

操作步骤

1. 添加vCenter镜像。

在ZStack私有云主菜单，点击**vCenter** > **镜像**，进入**镜像**界面，如图 *645: vCenter镜像*所示：

图 645: vCenter镜像



注: ZStack支持多vCenter资源区分，点击**vCenter**按钮，可选择查看全部或某个vCenter下的资源。

点击**添加镜像**按钮，弹出**添加镜像**界面，可参考以下示例输入相应内容：

- **名称**：自定义vCenter镜像的名称
- **简介**：可选项，可留空不填
- **镜像类型**：支持添加两种镜像类型：系统镜像、云盘镜像
  - **系统镜像**：

    若选择添加vCenter系统镜像，需设置以下内容：

    - **平台**：选择vCenter系统镜像运行的平台类型，包括：Linux、Windows、Other

      注:

      平台类型决定创建虚拟机时是否使用Virtio驱动（包括磁盘驱动和网卡驱动）

      - Linux：使用Virtio
      - Windows：不使用Virtio，镜像操作系统是未安装Virtio的Windows
      - Other：不使用Virtio，镜像操作系统可以使任何操作系统
    - **镜像服务器**：选择vCenter镜像服务器
    - **URL**：输入vCenter系统镜像的可下载的路径
  - **云盘镜像**：

    若选择添加vCenter云盘镜像，需设置以下内容：

- **镜像服务器**：选择vCenter镜像服务器
- **URL**：输入vCenter云盘镜像的可下载的路径

添加vCenter系统镜像如图 *646: 添加vCenter系统镜像*所示：

图 646: 添加vCenter系统镜像

添加vCenter云盘镜像如图 *647: 添加vCenter云盘镜像*所示：

图 647: 添加vCenter云盘镜像

2. 点击**确定**按钮，vCenter镜像成功添加。

后续操作

vCenter中镜像支持的操作：

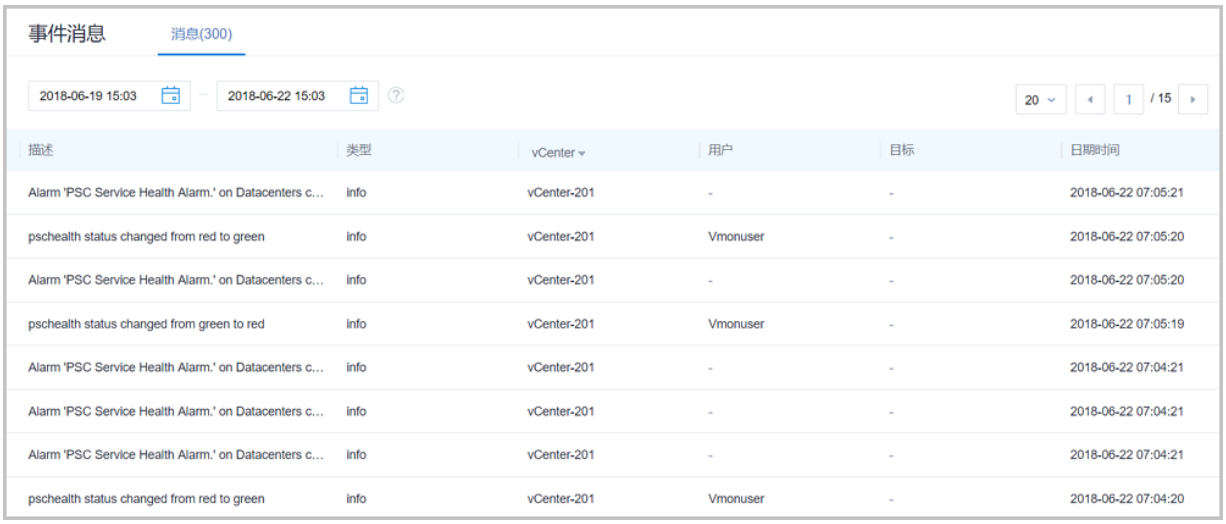
- 添加：支持添加vmdk格式的本地镜像到vCenter，目前不支持加添ISO格式。
- 启用：启用后，镜像可作为候选使用。
- 停用：停用后，镜像不可再作为候选使用。
- 删除：删除镜像，会同时删除本地记录和远端vCenter上的真实镜像资源。

至此，ZStack接管vCenter的使用方法介绍完毕。

7.7.8 事件消息

在ZStack私有云主菜单，点击**vCenter** > **事件消息**按钮，进入**事件消息**界面，如图 *648:* 事件消息所示：

图 648: 事件消息



事件消息提供vCenter报警消息的查看。可查看该报警的消息描述、类型、所属vCenter、触发用户、目标和日期时间信息。

- 界面最多显示300条事件消息。支持设置时间段，可调整合适的时间段查看所设时间段内的报警消息。
- 支持调整每页显示的报警消息数量，可选值为：10、20、50、100；且支持翻页操作。

7.8 企业管理(Plus)

企业管理主要为企业用户提供组织架构管理，以及基于项目的资源访问控制、工单审批、独立区域管理等功能。企业管理以单独的功能模块形式提供，需提前购买企业管理模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

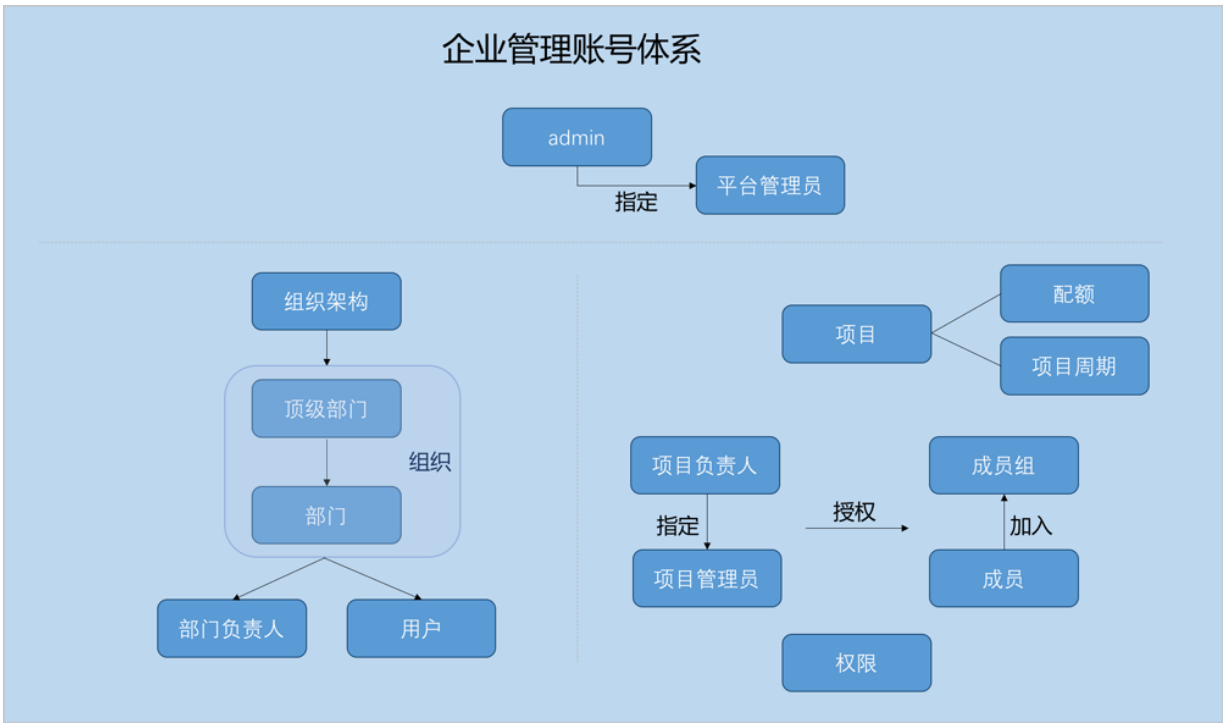
企业管理账号体系

企业管理账号体系主要涉及以下三类概念：

- 管理员账号：admin、平台管理员
- 未进入项目：用户、组织、部门负责人
- 已进入项目：项目负责人、项目管理员、成员、成员组、同时涉及项目、权限、配额等概念

企业管理账号体系如图 *649:* 企业管理账号体系所示：

图 649: 企业管理账号体系



相关定义：

- **admin**：

  admin不受权限控制，拥有超级权限，通常由IT系统管理员拥有。

- **平台管理员**：

  平台管理员主要是带有区域属性的管理员，admin可划分不同区域给不同平台管理员来管控不同区域的数据中心。

- **用户**：

  用户是企业管理中的最基本单位，admin/平台管理员可创建用户，并基于用户建立相应的组织架构。

- **组织**：

  组织是企业管理中组织架构的基本单位，admin/平台管理员可基于用户建立相应的组织架构，组织可分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门。

- **部门负责人**：

  创建组织，需指定相应的用户作为部门负责人。

- **项目**：

  项目用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务。企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。

- **项目负责人**：

  创建项目，需指定组织内的用户作为项目负责人。

- **项目管理员**：

  项目负责人可指定一个或多个成员作为项目管理员。

- **成员**：

  成员作为项目的基本组成人员，一般由admin/平台管理员/项目负责人/项目管理员添加进入项目；项目成员的权限可由admin/平台管理员/项目负责人/项目管理员进行相应控制。

- **成员组**：

  项目负责人/项目管理员可在项目中创建成员组，对成员进行分组管理；可以成员组为单位进行权限控制。

- **权限**：

  项目负责人/项目管理员可对成员赋予权限，获得权限的成员可调用相关API进行资源操作。

- **配额**：

  配额是admin/平台管理员对项目的资源总量进行控制的衡量标准。

  - 主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。
  - admin/平台管理员可修改以上各参数对各个项目进行资源总额的控制。

- **项目周期**：

  创建项目需指定项目周期，包括无限制和定时回收两种。

  - 无限制：创建项目后，项目内资源默认一直处于启用状态。
  - 定时回收：项目过期后，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。

企业管理各账号登录云平台

- admin从主登录界面登录云平台

  使用Chrome浏览器或FireFox浏览器打开主登录界面（*http://your_machine_ip:5000/#/login*），admin输入相应用户名和密码登录云平台。

  如图 *650:* 主登录界面所示：

  图 650: 主登录界面

- 平台管理员/项目负责人/项目管理员/项目成员从项目登录入口登录云平台

  使用Chrome浏览器或FireFox浏览器打开项目登录界面（*http://your_machine_ip:5000/#/project*），平台管理员/项目负责人/项目管理员/项目成员输入相应用户名和密码登录云平台。

  如图 *651:* 项目登录界面所示：

  图 651: 项目登录界面

企业管理的三个子功能

企业管理主要包括**项目管理**、**工单审批**、**独立区域管理**三个子功能。

- **项目管理**：

  以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。通过对项目生命周期进行管理（包括确定时间、确定配额、确定权限等），以更细粒度更自动化的方式提高云资源利用率，同时加强项目成员间的协作性。

  详情可参考*ZStack*官网教程《项目管理详解（企业管理模块）》。

- **工单审批**：

  为了更高效地为每个项目提供基础资源支持，项目成员可对云平台资源提出工单申请，管理员可进行一键审批，资源将自动部署成功并分发到项目中。

  详情可参考*ZStack*官网教程《工单管理详解（企业管理模块）》。

- **独立区域管理**：

区域通常对应某地的一个真实数据中心。在对区域进行资源隔离的基础上，可对每个区域指定相应的区域管理员，实现各地机房的独立管理，同时admin可对所有区域进行巡查和管理。

详情可参考*ZStack*官网教程《独立区域管理详解（企业管理模块）》。

以下介绍admin如何使用企业管理功能。

7.8.1 平台管理员

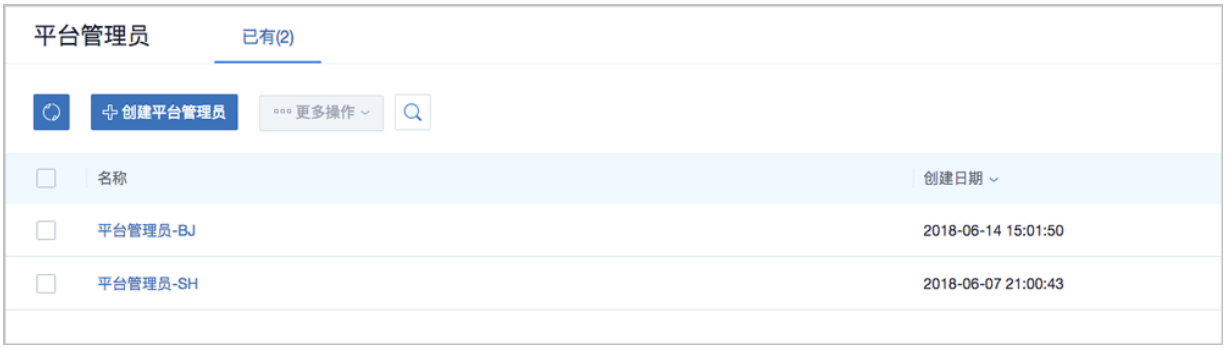
平台管理员主要是带有区域属性的管理员，admin可划分不同区域给不同平台管理员来管控不同区域的数据中心。

- 新建的平台管理员，未划分区域前，默认可管控所有区域；
- 平台管理员划分区域后，只可管控指定区域；
- 一个平台管理员可管控多个区域，一个区域可由多个平台管理员共同管控；
- 除admin可对平台管理员进行管控外，平台管理员拥有和admin相同的全部权限；
- 平台管理员需从项目登录入口登录云平台。

平台管理员界面

admin从主登录界面登录云平台后，在ZStack私有云主菜单，点击**企业管理** > **平台管理员**按钮，进入**平台管理员**界面，如图 *652:* 平台管理员界面所示：

图 652: 平台管理员界面



创建平台管理员

在**平台管理员**页面，点击**创建平台管理员**按钮，弹出**创建平台管理员**界面，可参考以下示例输入相应内容：

- **名称**：设置平台管理员名称，且作为登录名需全局唯一
- **简介**：可选项，可留空不填

- **密码**：设置平台管理员登录密码
- **确认密码**：再次输入登录密码
- **区域**：可选项，可为平台管理员划分管控区域，支持管控多个区域

如图 *653:* 创建平台管理员所示：

图 653: 创建平台管理员

admin对平台管理员支持的操作

admin对平台管理员支持以下操作：

- 创建平台管理员：创建一个平台管理员，可为其划分管控区域
- 修改名称和简介：修改平台管理员名称和简介，名称作为登录名需全局唯一
- 修改密码：修改平台管理员登录密码

- 添加区域：为平台管理员划分新的管控区域
- 移除区域：取消平台管理员对该区域的管控权限
- 删除：删除平台管理员
- 审计：查看admin对平台管理员的相关操作

7.8.2 组织架构

企业管理为企业用户提供组织架构管理功能。主要涉及以下概念：

- **用户**：

  用户是企业管理中的最基本单位，admin/平台管理员可创建用户，并基于用户建立相应的组织架构。

- **组织**：

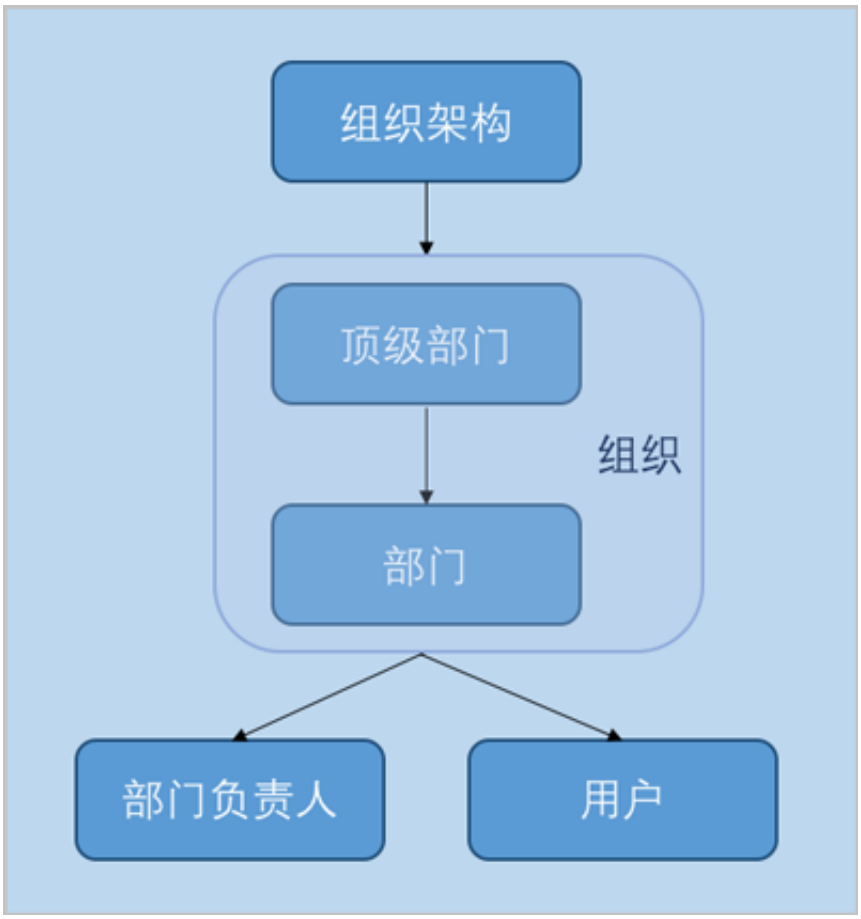
  组织是企业管理中组织架构的基本单位，admin/平台管理员可基于用户建立相应的组织架构，组织可分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门。

- **部门负责人**：

  创建组织，需指定相应的用户作为部门负责人。

组织架构示意图如图 *654:* 组织架构示意图所示：

图 654: 组织架构示意图



7.8.2.1 用户

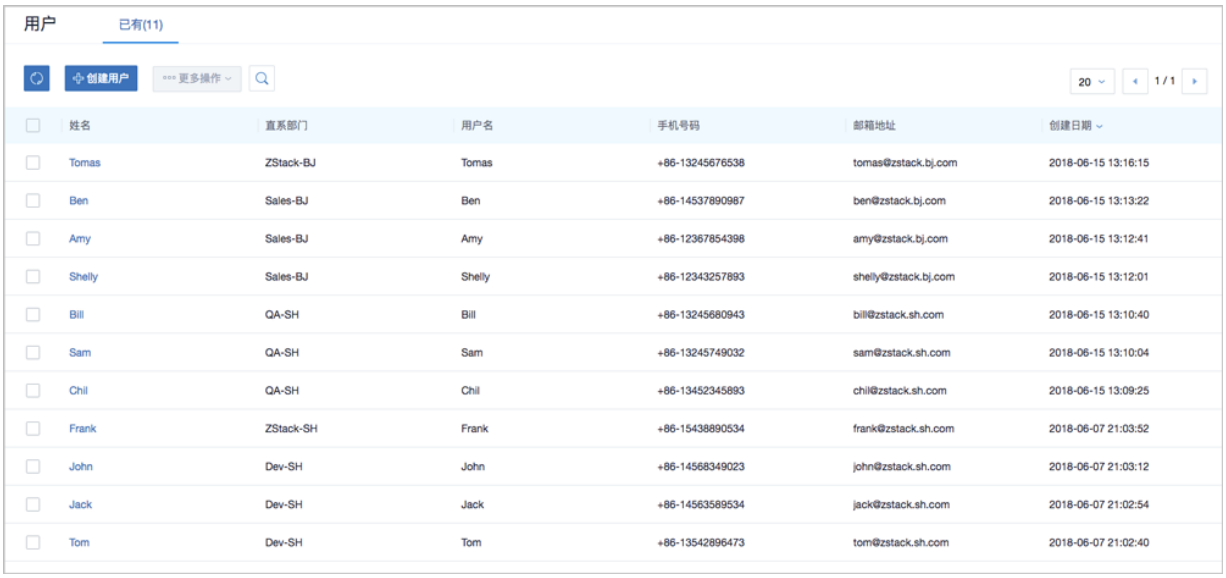
用户是企业管理中的最基本单位，admin/平台管理员可创建用户，并基于用户建立相应的组织架构。

- 创建用户时，需指定姓名和用户名，且用户名作为登录名需全局唯一；
- 用户需从项目登录入口登录云平台。

用户界面

admin/平台管理员从主登录界面登录云平台后，在ZStack私有云主菜单，点击**企业管理** > **组织架构** > **用户**按钮，进入**用户**界面，如图 *655:* 用户界面所示：

图 655: 用户界面



创建用户

在**用户**界面，点击**创建用户**按钮，弹出**创建用户**界面，可参考以下示例输入相应内容：

- **姓名**：输入用户姓名
- **用户名(用于登录)**：设置用户名，作为登录名需全局唯一
- **密码**：设置用户登录密码
- **确认密码**：再次输入登录密码
- **简介**：可选项，可留空不填
- **手机号码**：可选项，输入用户手机号码
- **邮箱地址**：可选项，输入用户邮箱地址
- **编号**：可选项，输入用户编号，例如工号
- **项目**：可选项，可将用户加入到一个或多个项目
- **组织**：可选项，可将用户加入到一个或多个组织

如图 *656: 创建用户*所示：

图 656: 创建用户

确定
取消
创建用户
姓名 *
Liz
用户名 (用于登录)*
Liz
密码 *
••••••••
确认密码 *
••••••••
简介
手机号码
+86
13425678767
邮箱地址
liz@zstack.bj.com
编号
24
项目
销售项目A-BJ
组织
Sales-BJ

admin/平台管理员对用户支持的操作

admin/平台管理员对用户支持以下操作：

- 创建用户：基于员工基本信息创建用户
- 修改姓名和简介：修改用户姓名和简介
- 查看组织架构路径：用户详情页支持查看组织架构路径
- 修改用户名：修改用户名，用户名作为登录名需全局唯一
- 修改密码：修改用户登录密码
- 修改个人信息：修改用户姓名、手机号码、邮箱地址和编号信息
- 加入部门：将用户加入到一个或多个部门
- 从部门移除：将用户从所选部门移除
- 加入项目：将用户加入到一个或多个项目
- 从项目移除：将用户从所选项目移除
- 删除：将用户从组织架构中删除

  注:

  - 若该用户为部门负责人/项目负责人，不允许直接删除；
  - admin/平台管理员需先更换部门负责人/项目负责人，再删除该用户。
- 审计：查看admin/平台管理员对用户的相关操作

7.8.2.2 组织

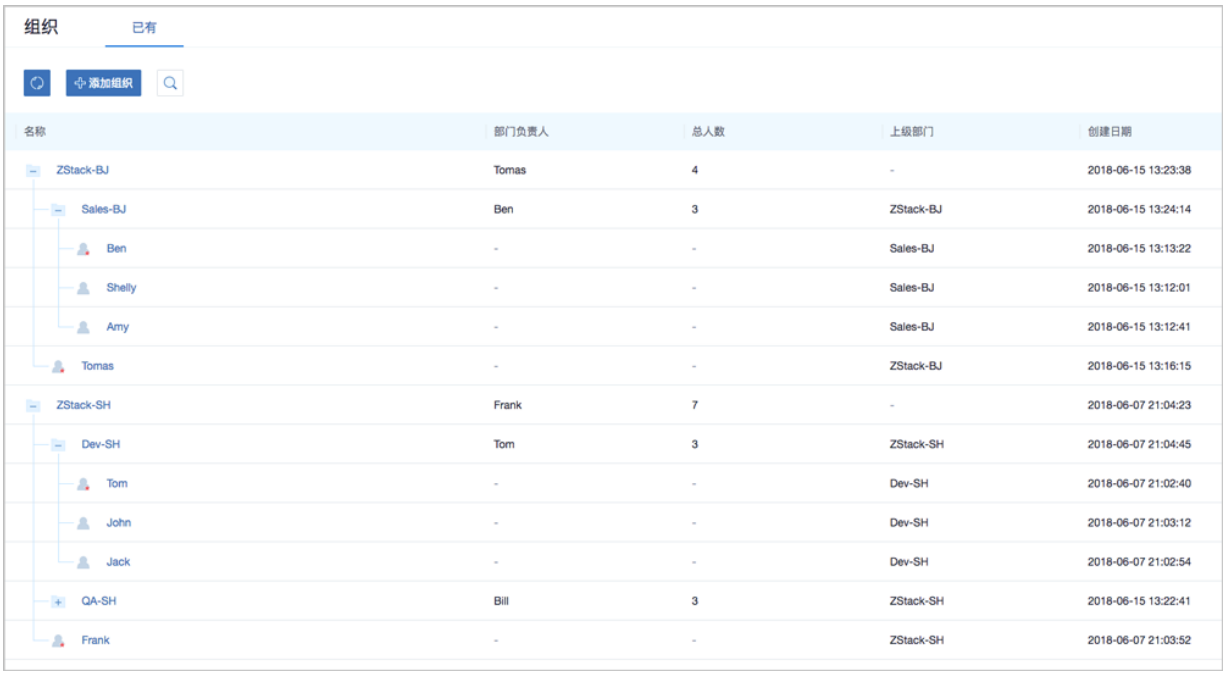
组织是企业管理中组织架构的基本单位，admin/平台管理员可基于用户建立相应的组织架构。

- 组织可分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门；
- 添加组织，需指定相应的用户作为部门负责人。

组织界面

admin/平台管理员从主登录界面登录云平台后，在ZStack私有云主菜单，点击**企业管理** > **组织架构** > **组织**按钮，进入**组织**界面，如图 *657:* 组织界面所示：

图 657: 组织界面



- 组织架构树以层级折叠方式展示，可直观查看企业组织架构全貌；
- 组织可分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门；
- 组织架构树中，顶级部门/部门的部门负责人图标右下角有红色五角星标识；
- 支持添加多个组织架构树。

添加组织

在**组织**界面，点击**添加组织**按钮，弹出**添加组织**界面，可参考以下示例输入相应内容：

- **名称**：输入组织名称
- **简介**：可选项，可留空不填
- **类型**：选择组织类型，可选择添加部门或顶级部门

  注: 添加部门，需指定**上级部门**，在已添加的顶级部门或部门中选择。

- **部门负责人**：需指定相应的用户作为部门负责人

  注: 组织架构树中，部门负责人图标右下角有红色五角星标识。

- **用户**：可选项，可将已有相关用户加入到该组织

如图 *658:* 创建组织所示：

图 658: 创建组织

admin/平台管理员对组织支持的操作

admin/平台管理员对组织支持以下操作：

- 添加组织：基于用户建立相应的组织架构
- 查看组织架构树：在**组织**界面，组织架构树以层级折叠方式展示，可直观查看企业组织架构全貌
- 修改名称和简介：修改组织名称和简介
- 更改上级部门：更改组织的上级部门；顶级部门不支持该操作
- 更改部门负责人：更改部门负责人
- 创建子部门：在该组织下创建一个子部门

- 删除子部门：删除该组织下的子部门；无子部门的组织不支持该操作
- 添加用户：添加新的用户到组织
- 移除用户：将用户从组织移除

注:

- 若该用户为部门负责人，无法被移除；
- admin/平台管理员需先更换部门负责人，再进行移除操作。

- 删除：删除指定组织

注: 删除组织时，其下所有子部门都会被删除，请谨慎操作。

- 审计：查看admin/平台管理员对组织的相关操作

7.8.3 项目管理

企业管理为企业用户提供项目管理功能。

项目管理：

以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。通过对项目生命周期进行管理（包括确定时间、确定配额、确定权限等），以更细粒度更自动化的方式提高云资源利用率，同时加强项目成员间的协作性。

主要涉及以下概念：

- **项目**：

  项目用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务。企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。

- **项目负责人**：

  创建项目，需指定组织内的用户作为项目负责人。

- **项目管理员**：

  项目负责人可指定一个或多个成员作为项目管理员。

- **成员**：

  成员作为项目的基本组成人员，一般由admin/平台管理员/项目负责人/项目管理员添加进入项目；项目成员的权限可由admin/平台管理员/项目负责人/项目管理员进行相应控制。

- **成员组**：

项目负责人/项目管理员可在项目中创建成员组，对成员进行分组管理；可以成员组为单位进行权限控制。

- **权限**：

  项目负责人/项目管理员可对成员赋予权限，获得权限的成员可调用相关API进行资源操作。

- **配额**：

  配额是admin/平台管理员对项目的资源总量进行控制的衡量标准。

  - 主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。
  - admin/平台管理员可修改以上各参数对各个项目进行资源总额的控制。

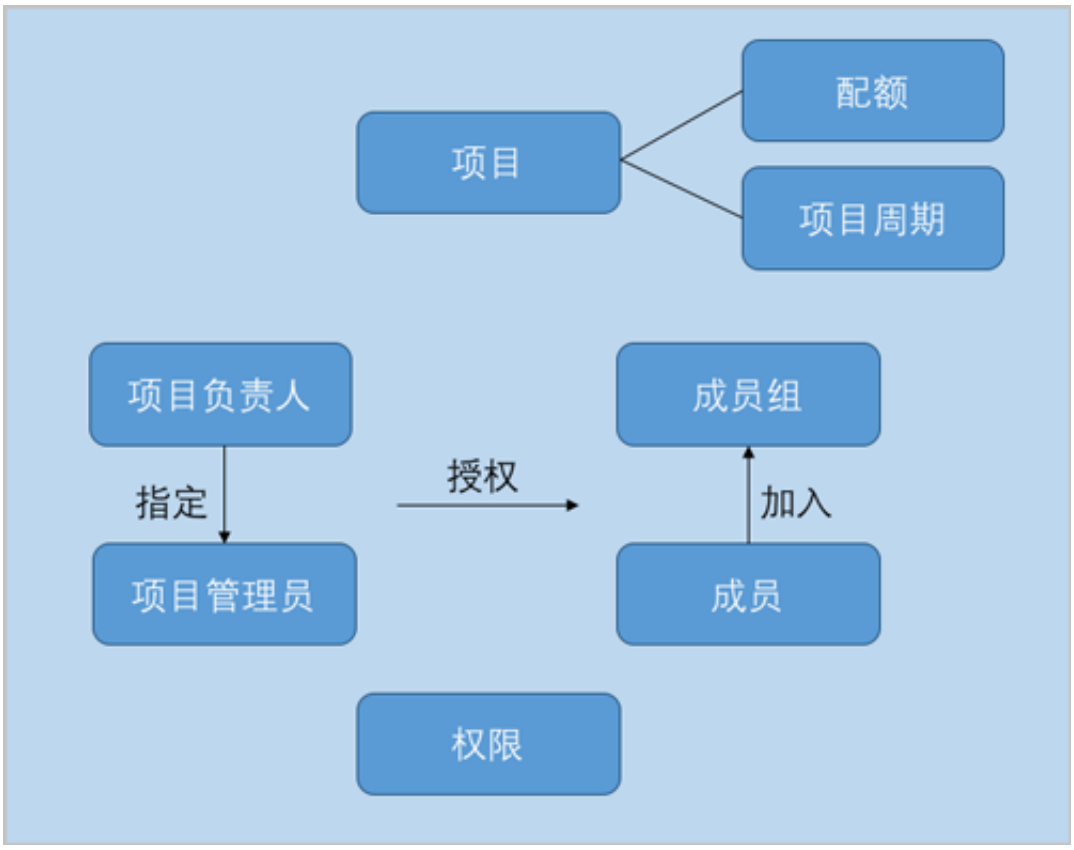
- **项目周期**：

  创建项目需指定项目周期，包括无限制和定时回收两种。

  - 无限制：创建项目后，项目内资源默认一直处于启用状态。
  - 定时回收：项目过期后，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。

项目管理示意图如图 *659:* 项目管理示意图所示：

图 659: 项目管理示意图



7.8.3.1 项目

项目用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务。企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。

- 基于组织内的用户创建项目，需指定资源配额，指定项目周期，指定项目负责人及成员等；
- 云平台内的基本资源（计算规格、镜像、网络等），建议提前共享或创建。

项目界面

admin/平台管理员从主登录界面登录云平台后，在ZStack私有云主菜单，点击**企业管理** > **项目管理** > **项目**按钮，进入**项目**界面，如图 *660:* 项目界面所示：

图 660: 项目界面

- 项目界面仅展示当前区域的项目列表信息；
- admin以及未划分区域的平台管理员，可对所有区域的项目进行管控；
- 平台管理员划分区域后，只可管控指定区域的项目。

创建项目

在**项目**界面，点击**创建项目**按钮，弹出**创建项目**界面。

注:

- 创建项目前，云平台内的基本资源（计算规格、镜像、网络等）建议提前共享或创建；
- 可按照弹出的智能操作助手进行相关操作，如图 *661:* 智能操作助手所示：

图 661: 智能操作助手

可参考以下示例输入相应内容：

- **名称**：设置项目名称
- **简介**：可选项，可留空不填
- **配额方式**：设置项目配额，对项目资源总量进行控制

  设置项目配额方式有以下两种：

  - **自定义**：

    如选择自定义方式设置项目配额，需设置以下内容：

- **计算资源**：包括云主机数量、运行中云主机数量、CPU数量、内存、亲和组数量的配额设置
- **存储资源**：包括云盘快照数量、数据云盘数量、可用存储容量、镜像数量、所有镜像容量的配额设置
- **网络资源**：包括VXLAN网络数量、三层网络数量、安全组数量、虚拟IP数量、弹性IP数量、端口转发数量、负载均衡器数量、监听器数量的配额设置
- **其他**：包括定时任务数量、定时器数量的配额设置

如图 *662:* 自定义配额方式所示：

图 662: 自定义配额方式

- **项目模板**：

  如选择项目模板方式设置项目配额，需设置以下内容：

  - **项目模板**：选择已有的项目模板，可直接使用模板定义的配额来配置项目

如图 *663: 项目模板配额方式*所示：

图 663: 项目模板配额方式

关于项目模板的更多介绍，详情可参考项目模板章节。

- **区域**：需指定项目所属的区域，一个项目只可归属于一个区域
- **项目周期**：可选项，默认为无限制，也可选择定时回收
  - **无限制**：

    创建项目后，项目内资源默认一直处于启用状态。
  - **定时回收**：

    项目过期后，项目内资源按照指定的控制策略回收。

    如选择定时回收，需设置以下内容：

    - **截止时间**：设置项目到期时间，支持秒级粒度
    - **回收策略**：提供以下三种回收策略
      - 禁止登录：过期后，项目相关人员均禁止登录此项目，项目内云主机仍将正常运行
      - 停止资源：过期后，项目内云主机会被停止，项目仍可正常登录
      - 删除项目：过期后，项目会被删除，处于“已删除”状态，项目禁止登录，云主机会被停止

    如图 *664: 定时回收*所示：

    图 664: 定时回收

- **项目负责人**：需指定相应的用户作为项目负责人
- **成员**：添加相关用户进入项目作为项目成员

如图 *665:* 创建项目所示：

图 665: 创建项目

确定
取消
创建项目
名称 *
开发项目C-SH
简介
配额方式 *
自定义
项目模板
项目模板 *
项目模板
区域 *
ZONE-SH
项目周期
定时回收
截止时间
2018-12-12 15:23
回收策略
禁止登录
项目负责人 *
John
成员
Jack
Tom

admin/平台管理员对项目支持的操作

admin/平台管理员对项目支持以下操作：

- 创建项目：创建一个项目
- 修改名称和简介：修改项目名称和简介
- 修改项目周期：项目详情页支持修改项目周期
- 修改项目配额：配额详情页支持修改项目配额
- 更换项目负责人：更换项目负责人
- 启用项目：将停用状态的项目启用，项目将允许正常登录
- 停用项目：将启用状态的项目停用，项目将禁止登录，项目内相关资源仍正常运行
- 生成项目模板：将已有项目生成模板，在创建项目时，可直接使用模板定义的配额来配置项目
- 添加成员：为项目添加成员
- 移除成员：将成员移除项目
- 停止项目资源：项目内相关资源将会停止，项目仍可正常登录
- 恢复过期项目：将已过期的项目恢复后，项目正常登录，项目内相关资源正常运行
- 删除：项目被删除后，处于已删除状态，项目禁止登录，项目内相关资源将会停止
- 恢复：将已删除状态的项目恢复为可用状态，需指定项目周期
- 彻底删除：将已删除状态的项目彻底删除，项目内相关资源将处于已删除状态，且归属于admin所有
- 审计：查看admin/平台管理员对项目的相关操作

7.8.3.2 项目模板

项目模板：主要用于标识各资源配额的模板。

- 在创建项目时，可直接使用模板定义的配额来配置项目；
- 可直接将已有项目生成模板。

创建项目模板

admin/平台管理员从主登录界面登录云平台后，在ZStack私有云主菜单，点击**企业管理** > **项目管理** > **项目模板**按钮，进入**项目模板**界面，点击**创建项目模板**按钮，可参考以下示例输入相应内容：

- **名称**：设置项目模板名称
- **简介**：可选项，可留空不填
- **配额**：设置模板中各资源配额

- **计算资源**：包括云主机数量、运行中云主机数量、CPU数量、内存、亲和组数量的配额设置
- **存储资源**：包括云盘快照数量、数据云盘数量、可用存储容量、镜像数量、所有镜像容量的配额设置
- **网络资源**：包括VXLAN网络数量、三层网络数量、安全组数量、虚拟IP数量、弹性IP数量、端口转发数量、负载均衡器数量、监听器数量的配额设置
- **其他**：包括定时任务数量、定时器数量的配额设置

如图 *666:* 创建项目模板所示：

图 666: 创建项目模板

admin/平台管理员对项目模板支持的操作

admin/平台管理员对项目模板支持以下操作：

- 创建项目模板：可通过自定义配额方式创建模板，也可直接将已有项目生成模板
- 修改名称和简介：修改项目模板名称和简介
- 修改配额：配额详情页支持修改项目模板配额
- 删除：删除项目模板
- 审计：查看admin/平台管理员对项目模板的相关操作

关于项目管理的更多详细介绍，可参考*ZStack*官网教程《项目管理详解（企业管理模块）》。

7.8.4 工单管理

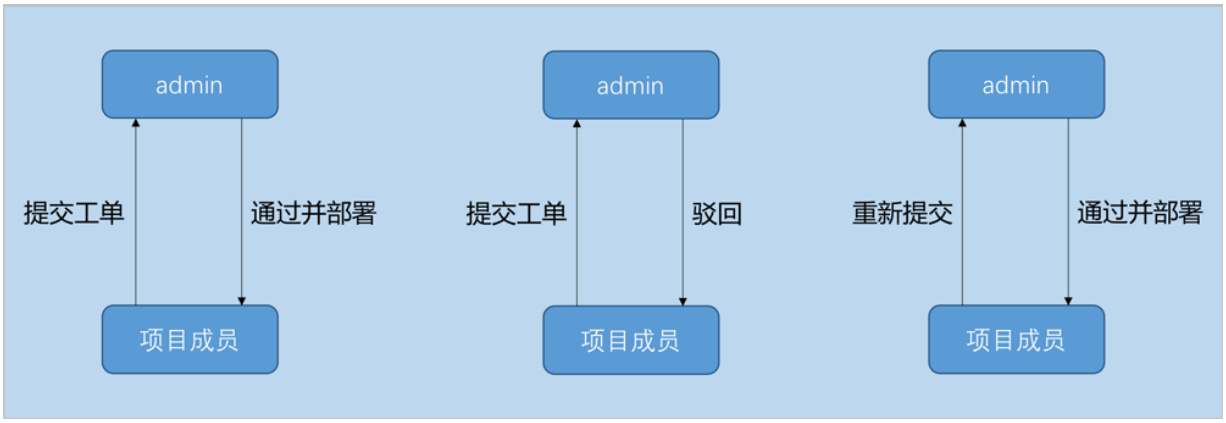
企业管理为企业用户提供工单管理功能。

工单管理：

为了更高效地为每个项目提供基础资源支持，项目成员可对云平台资源提出工单申请，管理员可进行一键审批，资源将自动部署成功并分发到项目中。

工单管理主要工作流如图 *667:* 工单管理工作流示意图所示：

图 667: 工单管理工作流示意图



以下介绍项目成员提交工单申请后，admin如何审批工单。

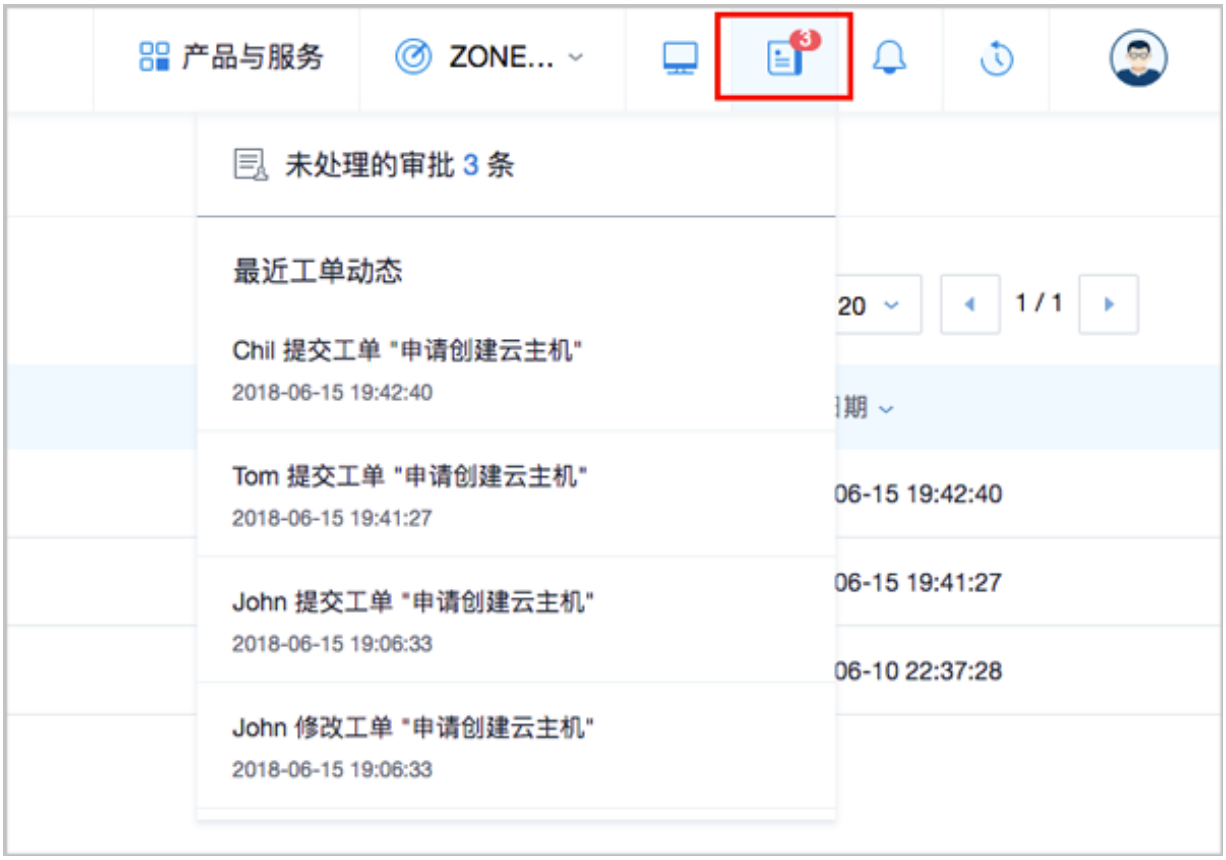
7.8.4.1 我的审批

admin需及时处理工单申请，可审批通过或驳回申请，审批通过后会自动部署，该项目下的资源会立即生效。

我的审批界面

admin从主登录界面（*http://your_machine_ip:5000/#/login*）登录云平台后，可从UI界面右上角的**工单消息**按钮处快速查看未处理的工单信息，并可跳转至**我的审批**界面处理工单，如图 *668:* 工单消息按钮所示：

图 668: 工单消息按钮



admin可在ZStack私有云主菜单，点击**企业管理** > **工单管理** > **我的审批**按钮，进入**我的审批**界面处理工单，如图 *669:* 我的审批界面所示：

图 669: 我的审批界面

我的审批界面分为**待审批**、**已处理**、**已归档**三个子页面：

- 待处理：该页面显示待处理的工单，可审批通过或驳回申请；
- 已处理：该页面显示已处理的工单，审批通过或驳回的工单均属于已处理工单；
- 已归档：该页面显示已归档的工单，项目成员删除已处理的工单后，admin可在已归档页面查看该条工单信息。

admin审批工单支持的操作

admin审批工单支持以下操作：

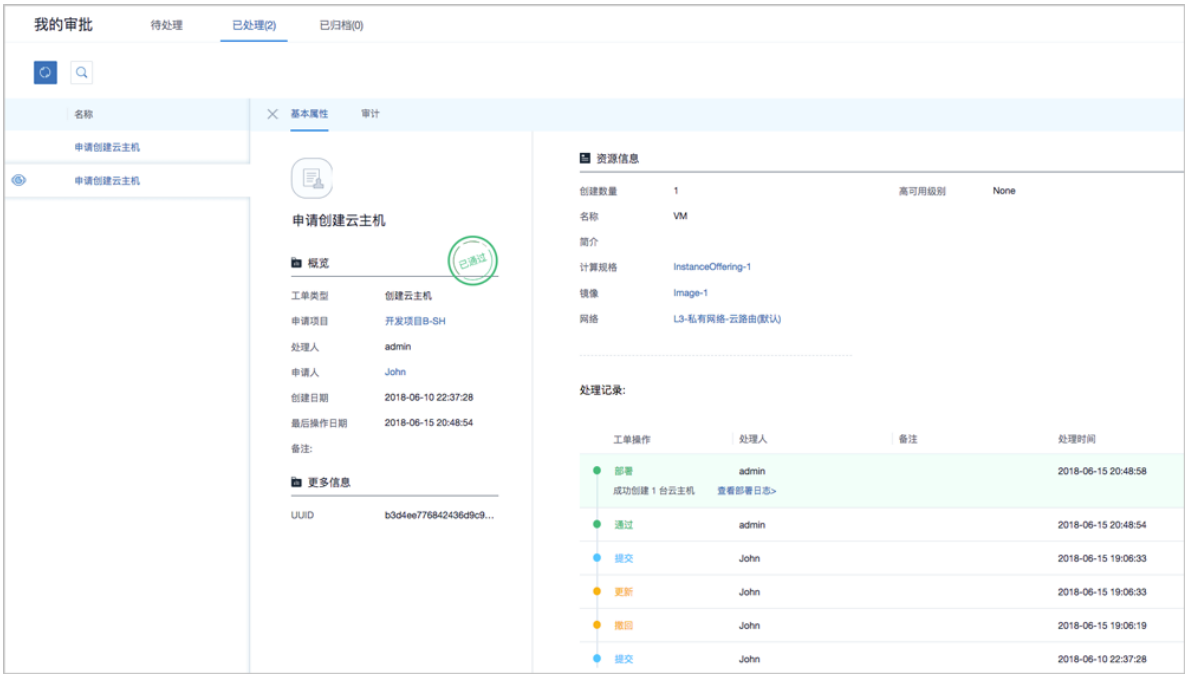
- 通过并部署：通过工单，系统将按配置自动创建资源给申请人

  注: 部署资源过程中，支持admin对资源进行高级设置。

- 驳回：驳回工单，可标注驳回原因
- 查看处理记录：工单详情页可实时查看处理记录

  如图 *670:* 查看处理记录所示：

  图 670: 查看处理记录



- 审计：查看admin审批工单的相关操作

关于工单管理的更多详细介绍，可参考*ZStack*官网教程《工单管理详解（企业管理模块）》。

7.9 平台运维

平台运维主要涵盖：性能统计、消息中心、操作日志、ZWatch监控报警、以及通知服务。

7.9.1 性能TOP5

性能TOP5是面向运维人员推出的可视化性能监控页面，在该页面可直观便捷查看物理机、云主机、路由器、虚拟IP、三层网络资源各种监控指标的TOP5信息，从而方便运维人员直观掌控云平台实时健康状态，以及快速定位问题。

在ZStack私有云主菜单，点击**平台运维** > **性能TOP5**，进入**性能TOP5**界面，包括五个子页面：物理机、云主机、路由器、虚拟IP、三层网络。

- 物理机页面：

  通过对当前区域全部物理机的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、磁盘读写IOPS、磁盘已使用容量百分比、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

  如图 *671:* 物理机性能*TOP5*所示：

  图 671: 物理机性能TOP5

- 云主机页面：

  同物理机页面类似，通过对当前区域全部云主机的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读写IOPS、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

- 路由器页面：

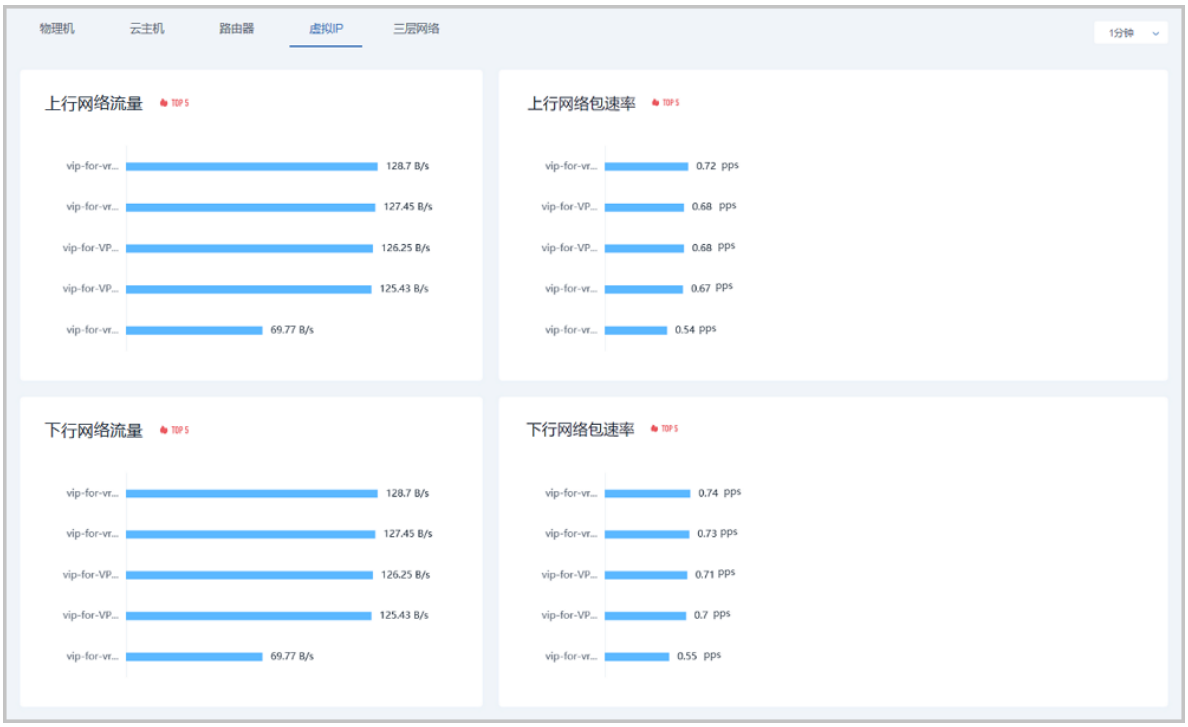
同云主机页面类似，通过对当前区域全部路由器（包括云路由器和VPC路由器）的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读写IOPS、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

- 虚拟IP页面：

  通过对当前区域全部虚拟IP的网络传输性能进行统计分析，以上行网络流量、下行网络流量、上行网络包速率、下行网络包速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的数值排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些虚拟IP出现传输性能瓶颈。

  如图 *672: 虚拟IP性能TOP5*所示：

  图 672: 虚拟IP性能TOP5

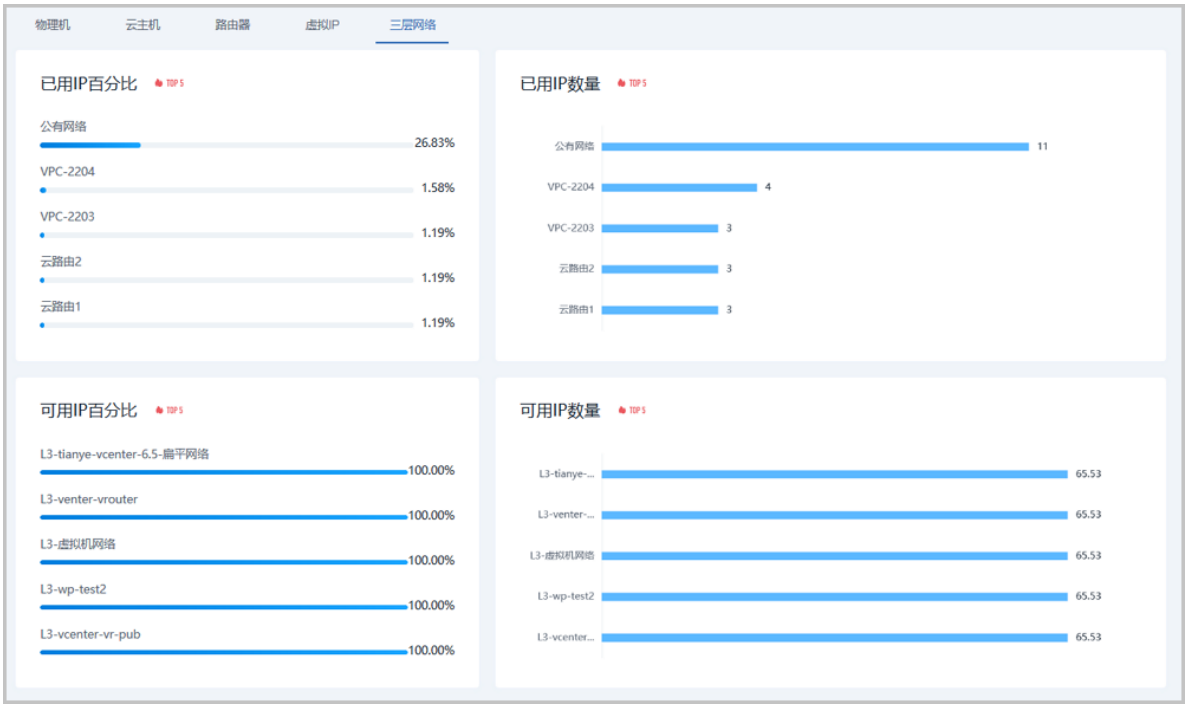


- 三层网络页面：

  通过对当前区域全部三层网络的IP资源使用情况进行统计分析，以已用IP百分比、已用IP数量、可用IP百分比、可用IP数量为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的数值排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些三层网络的IP资源出现告急。

如图 *673: 三层网络性能TOP5*所示：

图 673: 三层网络性能TOP5



补充说明

性能TOP5页面的右上角，点击时间下拉框，可对物理机、云主机、路由器、虚拟IP资源设置数据采样周期，可选：1分钟、1小时、1天、1周、1月。三层网络无采样周期设置。

7.9.2 性能分析

在ZStack私有云主菜单，点击**平台运维 > 性能分析**，进入**性能分析**界面。性能分析直观的显示了云主机、路由器、物理机、三层网络、虚拟IP、镜像服务器资源使用情况。其中：

- **云主机、路由器、物理机**：显示了名称、CPU平均使用率、内存使用率、磁盘读/写速度、网卡出/入速度信息，如图 *674: 云主机/路由器/物理机性能分析*所示：

图 674: 云主机/路由器/物理机性能分析

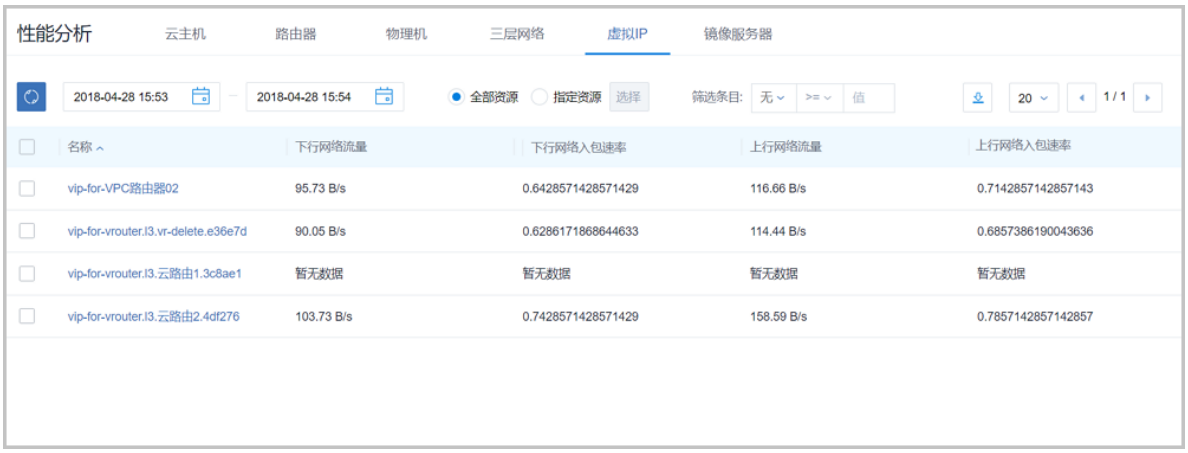
注: 点击左上角**停止**按钮，可以停止云主机。

- **三层网络**：显示了名称、已用IP数量、已用IP百分比、可用IP数量、可用IP百分比信息，如图 *675:* 三层网络性能统计所示：

图 675: 三层网络性能统计

- **虚拟IP**：显示了名称、下行网络流量、下行网络入包速率、上行网络流量、上行网络入包速率信息，如图 *676:* 虚拟*IP*性能分析所示：

图 676: 虚拟IP性能分析



- **镜像服务器**：显示了名称、镜像存储可用容量百分比信息，如图 *677:* 镜像服务器性能分析所示：

图 677: 镜像服务器性能分析

- **性能分析**页面支持全局资源和指定资源两种方式搜索，规定好搜索起止时间，填写筛选条目，系统会自动筛选出符合要求的信息。
- 每页默认显示20条信息，可点击旁边的下拉按钮切换10、20、50、100；点击右上角左右箭头按钮可进行翻页。
- 点击右上角下载按钮，可导出CSV文件。
- 如果存在多个CPU，CPU利用率可能会超过100%

7.9.3 ZWatch

ZStack支持ZWatch全新监控报警系统。

- 针对各种资源类型提供了多样化报警条目，支持的接收端类型有邮件/钉钉/HTTP应用。
- 设计原理：报警器或事件向SNS通知系统的主题发送消息，消息会自动推送到订阅该主题的接收端。发送到接收端的消息会以邮件/钉钉/HTTP POST方式发送到指定地址。

- 由于ZWatch监控系统与SNS通知系统完全松耦合，且基于开放式设计，用户可自定义报警器或事件，按需扩展更多资源类型以及更多报警条目，实现全方位、细粒度、灵活监控所有系统信息。

7.9.3.1 报警器

ZWatch监控系统支持对时序性数据和事件设置报警器，并通过SNS通知系统接收报警信息。

本章将分别介绍资源报警器和事件报警器的使用方法。

7.9.3.1.1 资源报警器

资源报警器，主要针对系统时序数据进行监控，例如云主机内存使用率、物理机CPU使用率等。支持用户自定义资源报警器。

创建资源报警器

在ZStack私有云主菜单，点击**平台运维 > ZWatch > 报警器**，直接进入**资源报警器**界面，点击**创建资源报警器**，在弹出的**创建资源报警器**界面，可参考以下示例输入相应内容：

- **名称**：设置资源报警器名称
- **简介**：可选项，可留空不填
- **资源类型**：按需选择资源类型， 可选项：云主机、镜像、镜像服务器、系统、物理机、三层网络、云盘、虚拟IP、主存储等
- **报警条目**：根据所选资源类型，按需选择报警条目

  注:

  每种资源类型对应多种报警条目，这里不一一列举，请按需选取。某些报警条目可能需要填写其他参数信息，请按要求设置。
- **报警条件**：选择报警判断类型并输入报警条件。可选项：大于、大于等于、小于、小于等于
- **持续时间**：阈值持续时间，单位包括：秒、分、时
- **报警间隔时间**：可选项，设置报警间隔时间，用于屏蔽重复报警，单位包括：秒、分、时；也可留空不填；系统默认报警间隔时间为30分钟
- **接收端**：可选项，不填表示不指定接收端；若填写，报警信息将会发送到指定接收端；支持添加多个接收端

  注: 用户可选择系统默认的接收端，也可用户自定义创建。创建接收端请参考接收端章节。

如图 *678:* 创建资源报警器所示：

图 678: 创建资源报警器

确定
取消
创建资源报警器
名称 *
云主机CPU使用率
简介
资源类型 *
云主机
报警条目 *
CPU使用率
云主机 *
VM
CPU *
0
报警条件 *
大于
60
%
持续时间 *
30
秒
报警间隔时间
30
分
(系统默认报警间隔为30分钟)
接收端
钉钉类型接收端

资源报警器支持的操作

资源报警器支持以下操作：

- 创建：创建一个资源报警器
- 启用：将已停用的资源报警器启用
- 停用：将正在使用的资源报警器停用
- 添加接收端：给选中的资源报警器添加接收端
- 移除接收端：将接收端从资源报警器移除
- 删除：删除一个资源报警器
- 修改名称和简介：修改资源报警器的名称和简介
- 修改报警条件、持续时间、报警间隔时间：修改资源报警器相关参数，包括报警条件、持续时间、报警间隔时间
- 查看报警记录：支持设置时间段，可查看所设时间段内资源报警器发出的报警记录
- 审计：查看此资源报警器的相关操作

7.9.3.1.2 事件报警器

事件报警器，主要针对系统事件进行监控，例如云主机状态变化事件、物理机失联事件等。支持用户自定义事件报警器。

创建事件报警器

在ZStack私有云主菜单，点击**平台运维 > ZWatch > 报警器 > 事件报警器**，进入**事件报警器**界面，点击**创建事件报警器**，在弹出的**创建事件报警器**界面，可参考以下示例输入相应内容：

- **资源类型**：按需选择资源类型，可选项：云主机、云路由、镜像服务器、物理机、主存储、vCenter等
- **报警条目**：根据所选资源类型，按需选择报警条目
- **接收端**：可选项，不填表示不指定接收端；若填写，报警信息将会发送到指定接收端；支持添加多个接收端

> **注:** 用户可选择系统默认的接收端，也可用户自定义创建。创建接收端请参考接收端章节。

如图 *679:* 创建事件报警器所示：

图 679: 创建事件报警器

事件报警器支持的操作

事件报警器支持以下操作:

- 创建：创建一个事件报警器
- 添加接收端：给选中的事件报警器添加接收端
- 移除接收端：将接收端从事件报警器移除
- 删除：删除一个事件报警器
- 查看报警记录：支持设置时间段，可查看所设时间段内事件报警器发出的报警记录
- 审计：查看此事件报警器的相关操作

7.9.3.2 报警消息模板

报警消息模板：报警器或事件向SNS系统的主题发送消息时使用的文本模板。

- 目前报警消息模板支持邮箱和钉钉两种接收端平台。使用报警消息模板，可将通知邮件或钉钉消息以统一格式发出。
- 系统自带一个默认模板，若用户没有创建模板，系统将使用自带模板。
- 用户可以创建多个模板，但只能指定一个为默认模板，发送消息时只会使用默认模板格式化信息。

- 模板中可以通过${}引用报警器或事件提供的变量。

创建报警消息模板

在ZStack私有云主菜单，点击**平台运维** > **ZWatch** > **报警消息模板**，进入**报警消息模板**界面，点击**创建报警消息模板**，在弹出的**创建报警消息模板**界面，可参考以下示例输入相应内容：

- **名称**：设置报警消息模板名称
- **简介**：可选项，可留空不填
- **平台**：选择接收端平台类型，目前报警消息模板支持邮箱和钉钉两种类型
- **文本**：用户可自定义模板，也可使用系统自带模板

  模板文本示例如下：

```
报警器 ${ALARM_NAME} 状态改变成 ${ALARM_CURRENT_STATUS}

报警器详情
UUID: ${ALARM_UUID}
资源名字空间: ${ALARM_NAMESPACE}
触发条件: ${ALARM_METRIC} ${ALARM_COMPARISON_OPERATOR} ${ALARM_T
HRESHOLD}
触发条件持续时间: ${ALARM_DURATION} seconds
先前状态: ${ALARM_PREVIOUS_STATUS}
当前值: ${ALARM_CURRENT_VALUE}
标签: ${ALARM_LABELS.join(",")}
```

  注:

  设置钉钉类型的报警消息模板，需遵循Markdown语法。目前钉钉只支持Markdown语法的子集，详情可查看钉钉官网文档**消息类型及数据格式**章节进行了解。

- **设为默认模板**：若勾选，会将当前创建的报警消息模板设置为默认模板

如图 *680:* 创建报警消息模板所示：

图 680: 创建报警消息模板

报警消息模板支持的操作

报警消息模板支持以下操作：

- 创建：创建一个报警消息模板
- 设为默认：将选中的报警消息模板设置为系统默认模板
- 取消默认：将已设置为系统默认的报警消息模板取消默认设置
- 删除：删除一个报警消息模板

- 修改名称和简介：修改报警消息模板的名称和简介
- 修改文本内容：修改报警消息模板的文本内容
- 审计：查看此报警消息模板的相关操作

7.9.4 通知服务

7.9.4.1 接收端

用户可以用不同的接收端订阅主题，接收端类型包括：邮箱、钉钉、HTTP应用。

创建邮箱类型接收端

- 发送到主题的消息都会以邮件方式通过邮箱服务器发送到指定的邮箱地址。
- 用户可提前创建报警消息模板，或使用系统自带模板，将通知邮件以统一格式发出。
- 需提前在当下区域内添加邮箱服务器，并测试邮箱服务器可用。

在ZStack私有云主菜单，点击**平台运维** > **通知服务** > **接收端**，进入**接收端**界面，点击**创建接收端**，在弹出的**创建接收端**界面，可参考以下示例输入相应内容：

- **名称**：设置接收端名称
- **简介**：可选项，可留空不填
- **接收端类型**：选择邮箱
- **邮箱地址**：输入邮箱地址
- **邮箱服务器**：输入已添加的邮箱服务器，添加邮箱服务器请参考邮箱服务器章节
- **测试**：需测试邮箱服务器可用

如图 *681:* 创建邮箱类型接收端所示：

图 681: 创建邮箱类型接收端

创建钉钉类型接收端

- 发送到主题的消息都会以钉钉方式发送到指定的钉钉机器人地址，若指定对象，会通过@电话号码通知相应的钉钉成员。
- 用户可提前创建报警消息模板，或使用系统自带模板，将钉钉消息以统一格式发出。
- 设置钉钉类型的报警消息模板，需遵循Markdown语法。目前钉钉只支持Markdown语法的子集，详情可登录钉钉官网进行了解。
- **名称**：设置接收端名称
- **简介**：可选项，可留空不填
- **接收端类型**：选择钉钉

- **地址**：输入钉钉机器人地址
- **对象**：可不指定，或指定群组所有人，或指定群组内成员

> **注:** 若指定成员，需以@电话号码的方式通知相应成员，示例：**+86-13800000000**

如图 *682:* 创建钉钉类型接收端所示：

图 682: 创建钉钉类型接收端

创建HTTP应用类型接收端

- 发送到主题的消息都会以HTTP POST方式发送到指定的HTTP地址。
- 若指定的HTTP应用已设置了用户名和密码才可访问，需按实填写用户名和密码。
- **名称**：设置接收端名称
- **简介**：可选项，可留空不填
- **接收端类型**：选择HTTP应用
- **地址**：输入HTTP服务地址
- **用户名**：可选项，若指定的HTTP应用已设置用户名和密码才可访问，需按实填写用户名
- **密码**：可选项，需按实填写相应密码

如图 *683:* 创建*HTTP*应用类型接收端所示：

图 683: 创建HTTP应用类型接收端

接收端支持的操作

接收端支持以下操作：

- 创建：创建一个接收端
- 启用：将已停用的接收端启用
- 停用：将正在使用的接收端停用
- 添加报警器：向选中的接收端中添加报警器
- 移除报警器：将报警器从接收端中移除
- 删除：删除一个接收端

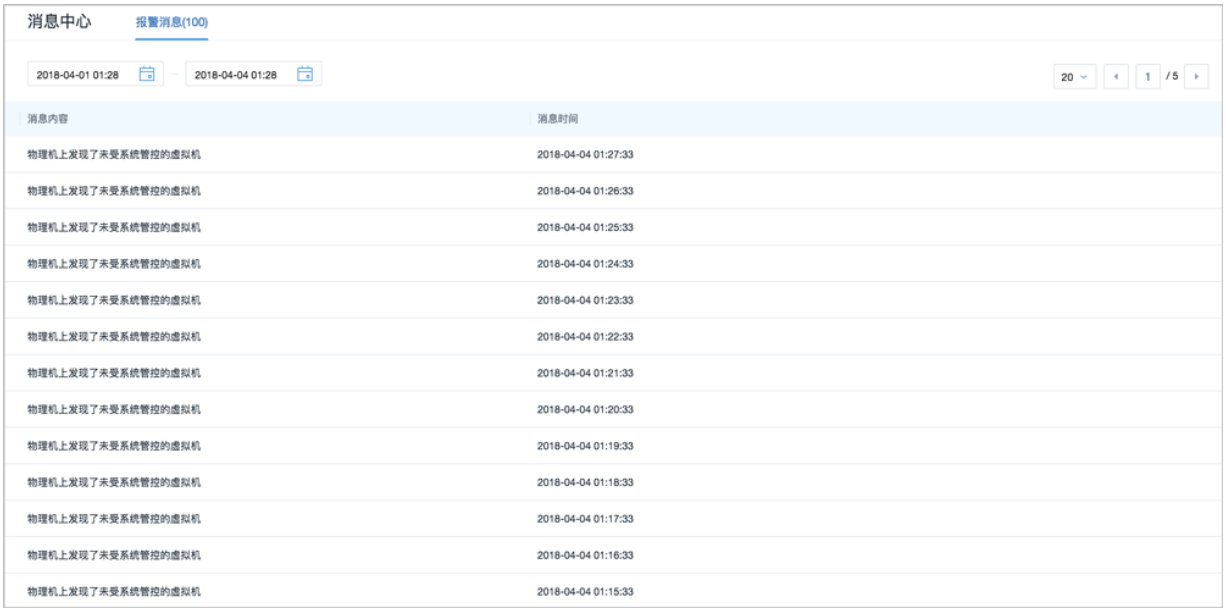
- 修改名称和简介：修改接收端的名称和简介
- 接收消息：支持设置时间段，可查看所设时间段内接收端的消息日志
- 审计：查看此接收端的相关操作

7.9.5 消息中心

消息中心界面

在ZStack私有云主菜单，点击**平台运维** > **消息中心**，进入**消息中心**管理界面，如图 *684:* 消息中心界面所示：

图 684: 消息中心界面



目前消息中心仅提供报警消息的查看。可查看该报警的消息内容、消息时间等信息。

- 支持设置时间段，可查看所设时间段内的报警消息，包括查看消息描述、消息时间、以及消息详情。
- 支持调整每页显示的报警消息数量，可选值为：10、20、50、100；且支持翻页操作。

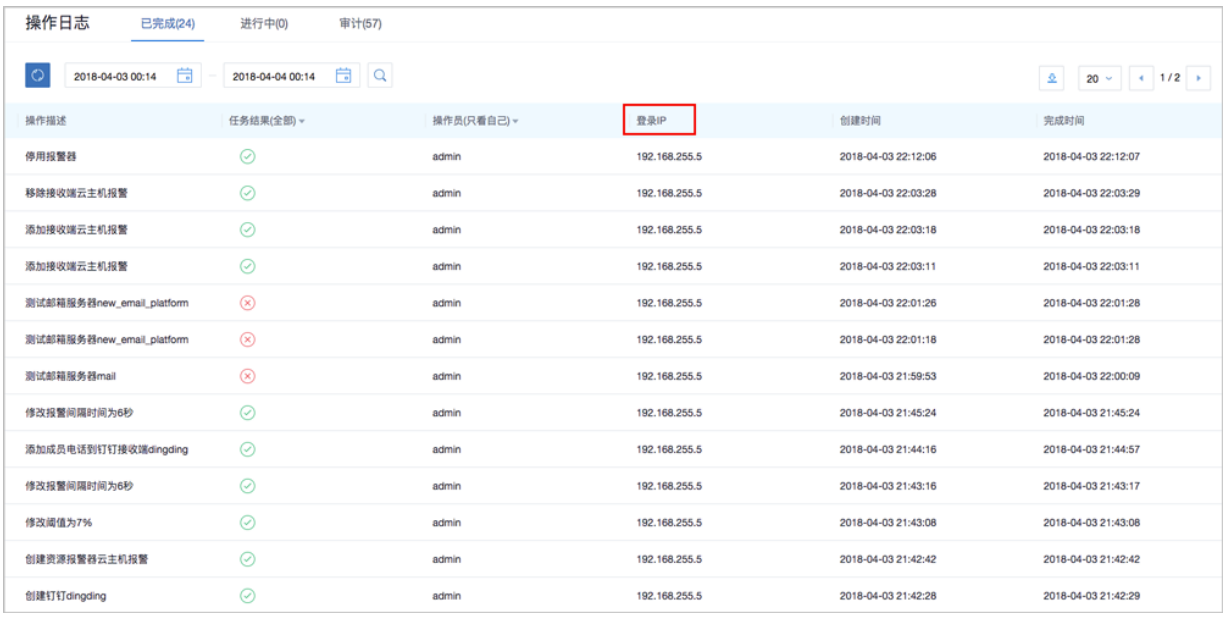
7.9.6 操作日志

操作日志界面包括三个子页面：已完成、进行中、审计。

操作日志界面：已完成

在**操作日志**界面，点击**已完成**，进入**已完成**子页面。如图 *685: 操作日志界面：已完成*所示：

图 685: 操作日志界面：已完成



已完成子页面针对已完成的操作提供日志查看，可查看该操作的操作描述、任务结果、操作员、登录IP、任务创建/完成时间，以及操作返回的消息详情，实现更细粒度管理。

- 支持设置时间段，可查看所设时间段内的已完成操作的日志。
- 支持通过输入操作描述/登录IP，搜索已完成的操作日志。
- 支持csv格式导出操作日志。
- 支持调整每页显示的已完成操作日志数量，可选值为：10、20、50、100；且支持翻页操作。
- 消息概览页增加创建时间和完成时间，更直观的显示信息详情。

操作日志界面：进行中

在ZStack私有云主菜单，点击**平台运维** > **操作日志**，直接进入**操作日志**的**进行中**子页面。如图 *686: 操作日志界面：进行中*所示：

图 686: 操作日志界面：进行中

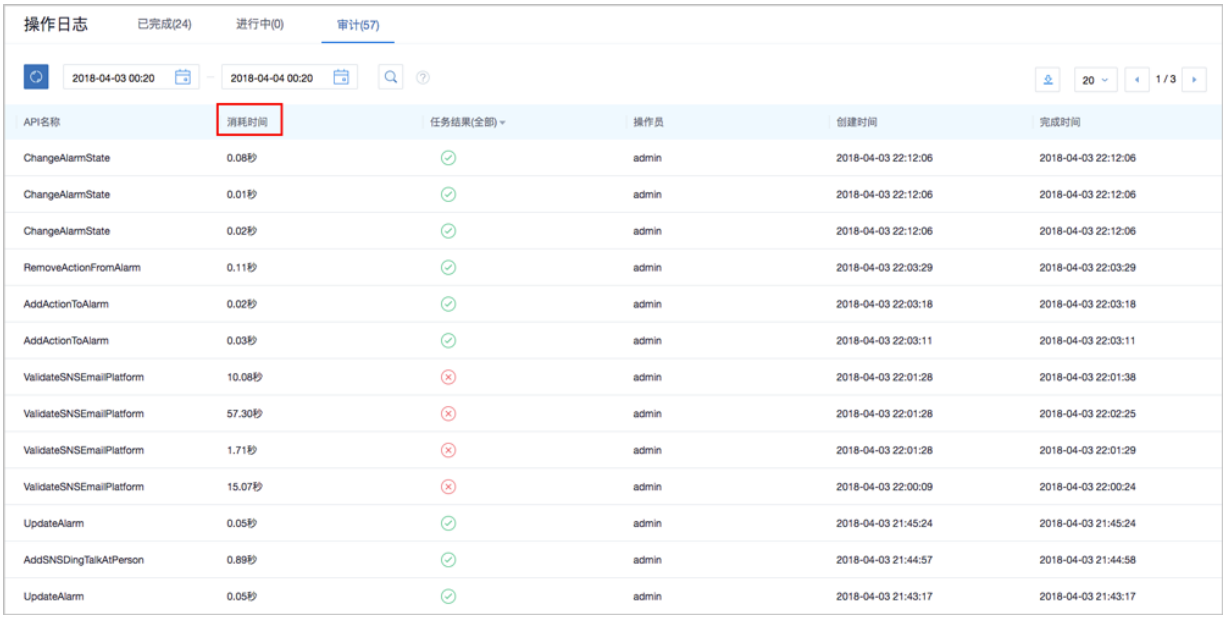
进行中子页面针对进行中的操作提供日志查看，可查看该操作的操作描述、任务结果、任务创建时间。

- 支持通过输入操作描述搜索正在进行的操作日志。
- 支持调整每页显示的进行中操作日志数量，可选值为：10、20、50、100；且支持翻页操作。
- 消息概览页增加创建时间和完成时间，更直观的显示信息详情。

操作日志界面：审计

在**操作日志**界面，点击**审计**，进入**审计**子页面。如图 *687: 操作日志界面：审计*所示：

图 687: 操作日志界面：审计



审计子页面针对调用API操作提供审计，可查看该调用API名称、消耗时间、任务结果、操作员，任务创建/完成时间，以及API行为的消息详情。

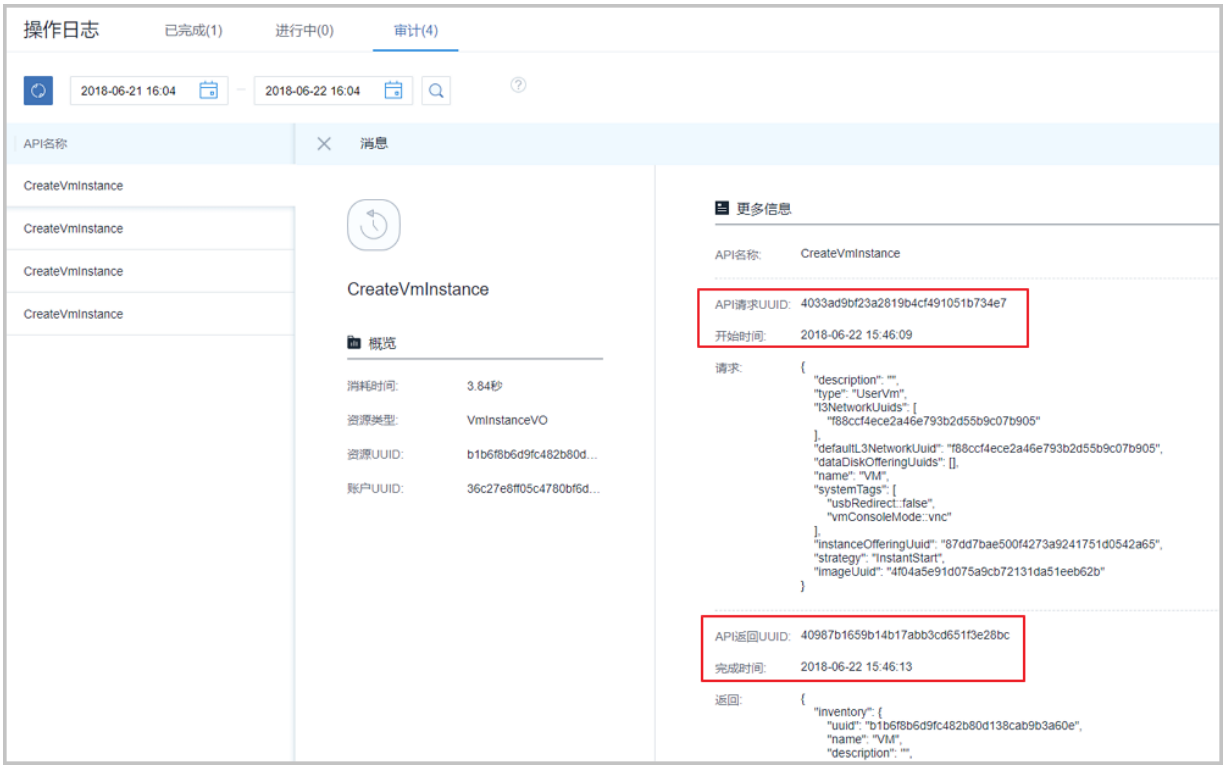
- 支持设置时间段，可查看所设时间段内调用API的审计信息。

注： 界面最多显示300条审计信息，请调整合适的时间段进行搜索。

- 支持通过输入资源类型/资源UUID/API名称/操作员，搜索调用API的审计信息。
- 支持csv格式导出审计信息。
- 支持调整每页显示的审计消息数量，可选值为：10、20、50、100；且支持翻页操作。

点击审计消息进入详情页，如图 *688:* 审计消息详情所示，新增显示开始/完成时间和API请求/返回UUID，更直观的显示审计信息详情。

图 688: 审计消息详情



7.9.7 资源编排

7.9.7.1 概述

资源编排服务是一款帮助云计算用户简化云资源管理和自动化部署运维的服务。通过资源栈模板，定义所需的云资源、资源间的依赖关系、资源配置等，可实现自动化批量部署和配置资源，轻松管理云资源生命周期，通过API和SDK集成自动化运维能力。

如图 *689:* 资源编排所示：

图 689: 资源编排

资源编排具有以下功能优势：

1. 用户只需创建资源栈模板或修改已有模板，定义所需的云资源、资源间的依赖关系、资源配置等，资源编排将通过编排引擎自动完成所有资源的创建和配置；
2. 可根据业务需要，动态调整资源栈模板，从而调整资源栈以灵活应对业务发展需要；
3. 如果不再需要某资源栈，可一键删除该栈及栈内所有资源；
4. 可重复使用已创建的资源栈模板快速复制整套资源，无需重复配置；
5. 可根据业务场景灵活组合云服务，以满足自动化运维的需求。

7.9.7.2 准备工作

admin请提前安装最新版本ZStack，并部署完成创建云主机必要的资源。

详情可参考用户手册安装部署章节。

本教程将详细介绍资源编排的使用方法。

7.9.7.3 典型使用流程

使用资源编排服务，用户可通过资源栈模板快速创建和配置一组资源，并便捷管理这组资源。

资源编排典型使用流程如下：

1. 准备资源栈模板。
   - 使用资源编排服务，首先需准备资源栈模板，资源编排将基于所准备的模板创建和配置相应资源栈；
   - 可先查看云平台提供的资源栈示例模板（即系统模板）是否满足业务需求，若满足，可直接使用示例模板创建资源栈；
   - 若示例模板不满足业务需求，可创建一个新模板或修改已有模板（即自定义模板）。如何创建自定义模板，请参考资源栈模板章节。
2. 通过模板创建资源栈。
   - 若示例模板满足业务需求，可直接使用示例模板创建资源栈。如何使用示例模板创建资源栈，请参考资源栈示例模板章节；
   - 用户也可使用自定义模板创建资源栈。如何使用自定义模板创建资源栈，请参考资源栈模板章节。
3. 管理资源栈。
   - 提供资源栈生命周期管理；
   - 可查看资源栈内所有资源的信息；
   - 删除资源栈时，默认会删除栈内编排创建的所有资源。
   - 管理资源栈的详细介绍，请参考资源栈章节。

7.9.7.4 资源栈

资源编排通过资源栈模板快速创建和配置一组资源，这组资源定义为一个资源栈，通过管理资源栈，维护这组资源。

资源栈支持以下操作：

- 创建资源栈
- 查看资源栈信息
- 删除资源栈

创建资源栈

在ZStack私有云主菜单，点击**平台运维** > **资源编排** > **资源栈**，进入**资源栈**界面，点击**创建资源栈**，弹出**创建资源栈**界面。

创建资源栈分为以下两步：

1. 可参考以下示例输入相应内容：

   - **区域**：自动显示当前区域
   - **名称**：设置资源栈名称
   - **简介**：可选项，可留空不填
   - **超时设置**：用于设置创建资源栈的超时时限，超时将失败，默认为60分钟
   - **失败回滚**：默认勾选，超时失败后将清理已创建的资源
   - **创建方式**：选择创建资源栈方式

     创建资源栈有以下三种方式：

     - **资源栈模板**：选择自定义模板或系统模板创建资源栈

       如图 *690:* 资源栈模板方式所示：

       图 690: 资源栈模板方式

       注: 如何创建自定义模板，请参考资源栈模板章节。

     - **上传文件**：直接上传已定义的UTF8编码格式的模板文件创建资源栈

       如图 *691:* 上传文件方式所示：

       图 691: 上传文件方式

注: 关于模板语法的详细介绍，请参考资源栈模板语法章节。

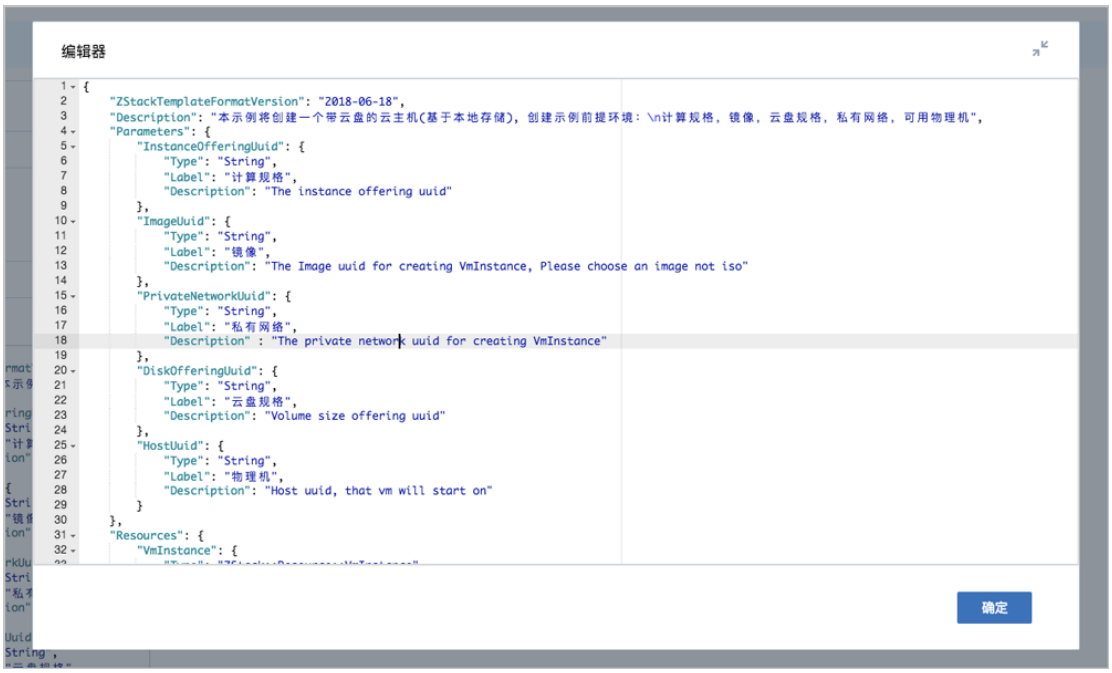
- **文本**：在文件编辑器中编辑模板创建资源栈

  如图 *692: 文本方式*：

图 692: 文本方式

可展开编辑器，如图 *693: 展开编辑器*所示：

图 693: 展开编辑器



注: 关于模板语法的详细介绍，请参考资源栈模板语法章节。

如图 *694: 创建资源栈1*所示，点击**下一步**。

图 694: 创建资源栈1

2. 根据需要的资源信息输入各个参数，不同类型的资源栈需要输入的参数不同。以上述创建云主机带云盘的资源栈为例，可参考以下示例输入相应内容：

   - **计算规格**：选择创建云主机的计算规格
   - **镜像**：选择创建云主机的镜像
   - **私有网络**：选择创建云主机的网络，本示例需选择创建云主机的私有网络
   - **云盘规格**：选择云主机所带云盘的规格
   - **物理机**：选择物理机以启动云主机

   如图 *695:* 创建资源栈2所示，点击**确定**，开始创建资源栈。

图 695: 创建资源栈2

注:

- 开始创建资源栈前，可点击**预览**查看将要创建的资源列表。
- 创建资源栈需要一定时长，请等待创建完成。

查看资源栈信息

在**资源栈**界面，选择某一资源栈，展开其详情页，可查看当前创建的资源栈状态和信息，包括：基本属性、资源栈内容、资源、事件、审计。

- 基本信息：显示资源栈当前状态、名称、简介、栈UUID等信息，其中名称和简介支持修改
- 资源栈内容：包括模板数据和参数配置
  - 模板数据：显示当前资源栈所对应的模板信息
  - 参数配置：创建资源栈时指定的参数信息
- 资源：显示资源栈所包括的全部资源信息
- 事件：显示资源栈生命周期中发生的每一个事件
- 审计：查看此资源栈的相关操作

删除资源栈

如果不再使用某一资源栈，可将该资源栈删除。

注:

- 删除资源栈默认会删除栈内编排创建的所有资源；
- 若资源栈所对应的模板事先已设置DeletionPolicy为Retain，栈内编排创建的所有资源将会被保留，详情可参考资源*(Resources)*章节。

7.9.7.5 资源栈模板

基于资源栈模板可快速创建资源栈。

资源栈模板分为系统模板和自定义模板，关于系统模板介绍，详情可参考章节，本章节主要介绍自定义模板。

资源栈模板支持以下操作：

- 创建资源栈模板
- 查看模板信息
- 启用模板
- 停用模板
- 创建资源栈
- 修改模板
- 删除模板

创建资源栈模板

在ZStack私有云主菜单，点击**平台运维** > **资源编排** > **资源栈模板**，进入**资源栈模板**界面，点击**创建资源栈模板**，弹出**创建资源栈模板**界面，可参考以下示例输入相应内容：

- **名称**：设置资源栈模板名称
- **简介**：可选项，可留空不填
- **创建方式**：选择创建资源栈模板方式

  创建资源栈模板有以下两种方式：

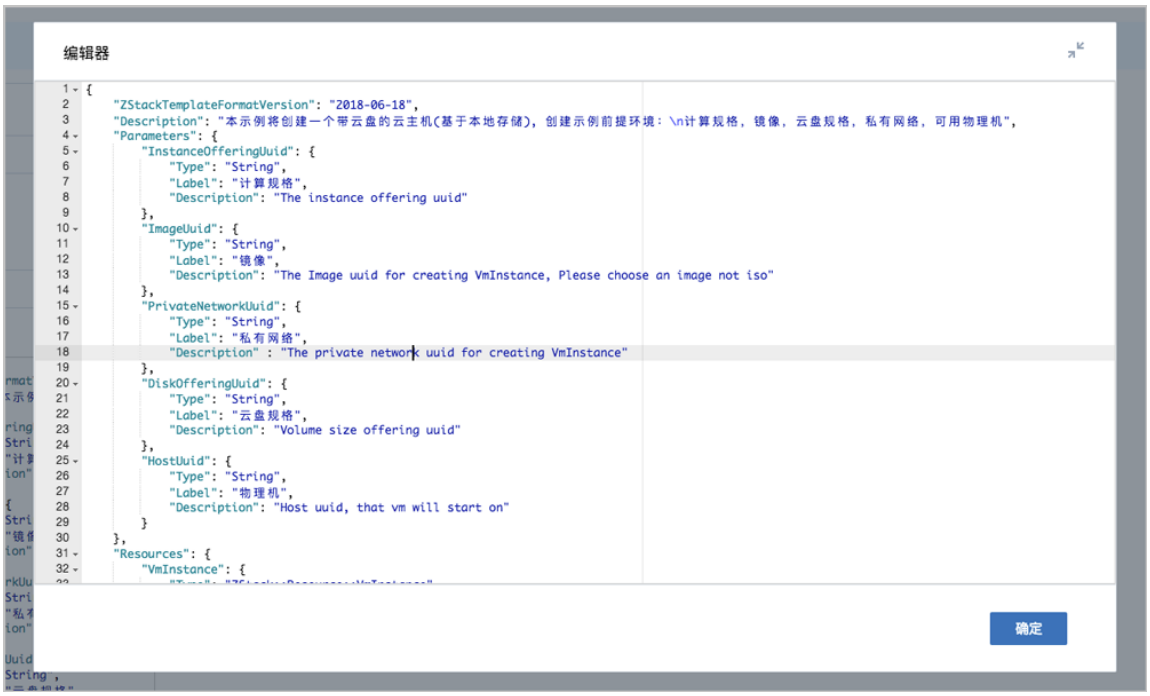
  - **文本**：在文件编辑器中编辑创建

如图 *696: 文本方式*：

图 696: 文本方式

可展开编辑器，如图 *697: 展开编辑器*所示：

图 697: 展开编辑器



注: 关于模板语法的详细介绍，请参考资源栈模板语法章节。

- **上传文件**：直接上传已定义的UTF8编码格式的文件创建

  如图 *698: 上传文件方式*所示：

图 698: 上传文件方式

注: 关于模板语法的详细介绍，请参考资源栈模板语法章节。

如图 *699: 创建资源栈模板*所示，点击**确定**。

图 699: 创建资源栈模板

查看模板信息

在**资源栈模板**界面，选择某一模板，展开其详情页，可查看当前创建的模板状态和信息，包括：基本属性、资源栈模板内容、审计。

- 基本信息：显示模板当前状态、名称、简介、模板UUID、MD5码等信息，其中名称和简介支持修改
- 资源栈模板内容：显示模板具体内容，关于模板语法的详细介绍，请参考资源栈模板语法章节
- 审计：查看此模板的相关操作

启用/停用模板

- 启用模板：将已停用的模板启用
- 停用模板：将模板停用，停用的模板不能创建资源栈

创建资源栈

在**资源栈模板**界面，选择某一模板，点击**更多操作 > 创建资源栈**，弹出**创建资源栈**界面。

使用自定义模板创建资源栈分为以下两步：

1. 可参考以下示例输入相应内容：

   - **区域**：自动显示当前区域
   - **名称**：设置资源栈名称
   - **简介**：可选项，可留空不填
   - **超时设置**：用于设置创建资源栈的超时时限，超时将失败，默认为60分钟
   - **失败回滚**：默认勾选，超时失败后将清理已创建的资源
   - **资源栈模板**：自动显示已选择的模板

   如图 *699:* 创建资源栈模板所示，点击**下一步**。

   图 700: 创建资源栈1

2. 根据需要的资源信息输入各个参数，不同类型的资源栈需要输入的参数不同。以上述创建云主机带云盘的资源栈为例，可参考以下示例输入相应内容：

   - **计算规格**：选择创建云主机的计算规格
   - **镜像**：选择创建云主机的镜像

- **私有网络**：选择创建云主机的网络，本示例需选择创建云主机的私有网络
- **云盘规格**：选择云主机所带云盘的规格
- **物理机**：选择物理机以启动云主机

如图 *701:* 创建资源栈2所示，点击**确定**，开始创建资源栈。

图 701: 创建资源栈2

注:

- 开始创建资源栈前，可点击**预览**查看将要创建的资源列表。
- 创建资源栈需要一定时长，请等待创建完成。

修改模板

支持在文件编辑器中修改模板。

删除模板

如果不再使用某一模板，可将该模板删除。

约束条件

需注意：

- 每个模板文件大小不超过4MB
- 若通过API提交，则参数大小不可超过64K

7.9.7.6 资源栈示例模板

云平台提供了常用的示例模板，用户可基于已有示例模板创建资源栈。

资源栈模板支持以下操作：

- 查看示例模板信息
- 使用示例模板创建资源栈

查看示例模板信息

在ZStack私有云主菜单，点击**平台运维 > 资源编排 > 资源栈示例模板**，进入**资源栈示例模板**界面，选择某一示例模板，展开其详情页，可查看模板状态和信息，包括：基本属性、资源栈模板内容、审计。

- 基本信息：显示示例模板的状态、名称、简介、模板UUID、MD5码等信息

  注: 示例模板一直处于启用状态，且不允许任何修改。

- 资源栈模板内容：显示示例模板具体内容，关于模板语法的详细介绍，请参考资源栈模板语法章节
- 审计：查看此模板的相关操作

使用示例模板创建资源栈

在**资源栈示例模板**界面，选择某一示例模板，点击**更多操作 > 创建资源栈**，弹出**创建资源栈**界面。

使用示例模板创建资源栈分为以下两步：

1. 可参考以下示例输入相应内容：
   - **区域**：自动显示当前区域
   - **名称**：设置资源栈名称
   - **简介**：可选项，可留空不填
   - **超时设置**：用于设置创建资源栈的超时时限，超时将失败，默认为60分钟
   - **失败回滚**：默认勾选，超时失败后将清理已创建的资源

- **资源栈模板**：自动显示已选择的模板

如图 *702: 创建资源栈1*所示，点击**下一步**。

图 702: 创建资源栈1

2. 根据需要的资源信息输入各个参数，不同类型的资源栈需要输入的参数不同。以上述模板**ZStack.System.v1.EIP**为例，通过该模板将创建一个弹性IP，并将弹性IP绑定到云主机上，可参考以下示例输入相应内容：

   - **计算规格**：选择创建云主机的计算规格
   - **镜像**：选择创建云主机的镜像
   - **私有网络**：选择创建云主机的网络，本示例需选择创建云主机的私有网络
   - **公有网络**：选择提供虚拟IP的公有网络，通过虚拟IP提供弹性IP服务

   如图 *703: 创建资源栈2*所示，点击**确定**，开始创建资源栈。

   图 703: 创建资源栈2

注:

- 开始创建资源栈前，可点击**预览**查看将要创建的资源列表。
- 创建资源栈需要一定时长，请等待创建完成。

7.9.7.7 快速实践

背景信息

本章节介绍如何使用一个资源栈示例模板**ZStack.System.v1.VPC**一键部署VPC网络。

操作步骤

1. 准备资源栈模板。

   本实践直接使用示例模板创建资源栈。

   在ZStack私有云主菜单，点击**平台运维** > **资源编排** > **资源栈示例模板**，进入**资源栈示例模板**界面，即可看到示例模板**ZStack.System.v1.VPC**，展开其详情页，查看资源栈模板内容，详情如下：

```
{
 "ZStackTemplateFormatVersion": "2018-06-18",
 "Description": "本示例会创建一个简单的VPC网络，需要用户提供下面正确的数据\n公有网络Uuid\n管理网络Uuid: 如果只有公有网络，则把公有网络当作管理网即可.\nVxlan网络的VTEP Cider",
```

```
 "Parameters": {
  "VrouterImageUrl": {
   "Type": "String",
                "Label":"云路由镜像链接地址",
   "Description":"云路由镜像链接地址",
   "DefaultValue": "http://cdn.zstack.io/product_downloads/vrouter/2.3/zstack-vrouter-2.3.2
.qcow2"
  },
  "VmImageUrl": {
   "Type": "String",
                "Label": "云主机镜像链接地址",
   "Description":"测试云主机镜像，请确定ZStack 可以下载下面链接的镜像",
   "DefaultValue": "http://cdn.zstack.io/zstack_repo/latest/zstack-image-1.4.qcow2"
  },
  "BackupStorage":{
   "Type": "CommaDelimitedList",
                "Label": "镜像服务器",
   "Description":"镜像服务器Uuid"
  },
  "ManagementNetworkUuid":{
   "Type": "String",
                "Label": "管理网络",
   "Description":"管理网络Uuid,如果只有公有网络填入公有网络Uuid即可"
  },
  "PublicNetworkUuid":{
   "Type": "String",
                "Label": "公有网络",
   "Description":"公有网络Uuid"
  },
  "ZoneUuid":{
   "Type": "String",
                "Label": "区域",
   "Description":"区域Uuid"
  },
  "ClusterUuid":{
   "Type": "String",
                "Label": "集群",
   "Description":"集群Uuid"
  },
  "Cidr":{
   "Type": "String",
   "Label": "VTEP CIDR",
                "Description":"VTEP Cider",
   "DefaultValue":"{10.0.0.0/8}"
  },
  "Vni":{
   "Type": "Number",
   "DefaultValue":222
  },
  "StartVni":{
   "Type": "Number",
                "Label": "起始Vni",
   "DefaultValue":100
  },
  "EndVni":{
   "Type": "Number",
                "Label": "结束Vni",
   "DefaultValue":300
  },
  "StartIp":{
   "Type": "String",
```

```
                "Label": "起始IP",
  "DefaultValue":"192.168.20.2"
 },
 "EndIp":{
  "Type": "String",
                "Label": "结束IP",
  "DefaultValue":"192.168.20.200"
 },
 "Netmask":{
  "Type": "String",
                "Label": "子网掩码",
  "DefaultValue":"255.255.255.0"
 },
 "Gateway":{
  "Type": "String",
                "Label": "网关",
  "DefaultValue":"192.168.20.1"
 }
},
"Resources": {
 "VrouterImage": {
  "Type": "ZStack::Resource::Image",
  "Properties": {
   "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, {"Ref":"ZStack::StackUuid"}, {"Ref
":"ZStack::AccountUuid"}, {"Ref":"ZStack::AccountName"}, "Vrouter-Image"]]},
   "url": {"Ref":"VrouterImageUrl"},
   "system": true,
   "format": "qcow2",
   "backupStorageUuids":{"Ref":"BackupStorage"}
  }
 },
 "VMImage": {
  "Type": "ZStack::Resource::Image",
  "Properties": {
   "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "VmImage"]]},
   "url": {"Ref":"VmImageUrl"},
   "format": "qcow2",
   "backupStorageUuids":{"Ref":"BackupStorage"}
  }
 },
 "VirtualRouterOffering":{
  "Type":"ZStack::Resource::VirtualRouterOffering",
  "Properties":{
   "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "Vrouter-Offering"]]},
   "zoneUuid":{"Ref":"ZoneUuid"},
   "managementNetworkUuid":{"Ref":"ManagementNetworkUuid"},
   "publicNetworkUuid":{"Ref":"PublicNetworkUuid"},
   "imageUuid":{"Fn::GetAtt":["VrouterImage", "uuid"]},
   "cpuNum":2,
   "memorySize":2147483648
  }
 },
 "VpcVRouter":{
  "Type":"ZStack::Resource::VpcVRouter",
  "Properties":{
   "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "VPC-Router"]]},
   "virtualRouterOfferingUuid":{"Fn::GetAtt":["VirtualRouterOffering","uuid"]}
  }
 },
 "L2VxlanNetworkPool":{
  "Type":"ZStack::Resource::L2VxlanNetworkPool",
  "Properties":{
```

```
  "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "L2VxlanNetworkPool"]]},
  "zoneUuid":{"Ref":"ZoneUuid"}
 }
},
"VniRange":{
 "Type":"ZStack::Resource::VniRange",
 "Properties":{
  "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "VniRange"]]},
  "startVni":{"Ref":"StartVni"},
  "endVni":{"Ref":"EndVni"},
  "l2NetworkUuid":{"Fn::GetAtt":["L2VxlanNetworkPool","uuid"]}
 }
},
"L2VxlanNetwork":{
 "Type":"ZStack::Resource::L2VxlanNetwork",
 "Properties":{
  "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "L2VxlanNetwork"]]},
  "poolUuid":{"Fn::GetAtt":["L2VxlanNetworkPool","uuid"]},
  "zoneUuid":{"Ref":"ZoneUuid"},
  "vni":{"Ref":"Vni"}
 }
},
"VpcL3Network":{
 "Type":"ZStack::Resource::L3Network",
 "Properties":{
  "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "VPC-Network"]]},
  "l2NetworkUuid":{"Fn::GetAtt":["L2VxlanNetwork","uuid"]},
  "category":"Private",
  "type":"L3VpcNetwork",
  "systemTags":["networkservices::VRouter"]
 }
},
"InstanceOffering":{
 "Type":"ZStack::Resource::InstanceOffering",
 "Properties":{
  "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "1cpu","4G"]]},
  "cpuNum": 1,
  "memorySize" : 4294967296
 }
},

"AttachL3ToVm":{
 "Type":"ZStack::Action::AttachL3NetworkToVm",
 "Properties":{
  "vmInstanceUuid": {"Fn::GetAtt":["VpcVRouter","uuid"]},
  "l3NetworkUuid":{"Fn::GetAtt":["VpcL3Network","uuid"]}
 },
 "DependsOn":[{"Ref":"AddIpRange"}]
},
"AddIpRange" :{
 "Type":"ZStack::Action::AddIpRange",
 "Properties":{
  "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "iprange"]]},
  "l3NetworkUuid":{"Fn::GetAtt":["VpcL3Network","uuid"]},
  "startIp":{"Ref":"StartIp"},
  "endIp":{"Ref":"EndIp"},
  "netmask":{"Ref":"Netmask"},
  "gateway":{"Ref":"Gateway"}
 }
},
"AttachL2NetworkToCluster":{
 "Type":"ZStack::Action::AttachL2NetworkToCluster",
```

```
    "Properties":{
     "l2NetworkUuid":{"Fn::GetAtt":["L2VxlanNetworkPool","uuid"]},
     "clusterUuid":{"Ref":"ClusterUuid"},
     "systemTags":[{"Fn::Join":["::",["l2NetworkUuid",{"Fn::GetAtt":["L2VxlanNetwork","uuid
"]},"clusterUuid",{"Ref":"ClusterUuid"},"cidr",{"Ref":"Cidr"}]]}]
    }
   },
   "TestVm":{
    "Type":"ZStack::Resource::VmInstance",
    "Properties":{
     "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"}, "TestVm"]]},
     "instanceOfferingUuid": {"Fn::GetAtt":["InstanceOffering","uuid"]},
     "l3NetworkUuids": [{"Fn::GetAtt":["VpcL3Network","uuid"]}],
     "imageUuid": {"Fn::GetAtt":["VMImage", "uuid"]}
    },
    "DependsOn":[{"Ref":"AttachL3ToVm"}]
   }
  },
  "Outputs": {
   "vpc": {
    "Value": {
     "Ref": "VpcL3Network"
    }
   }
  }
}
```

上述模板包含五个顶级字段：

- "ZStackTemplateFormatVersion": "2018-06-18"

  定义模板版本。

- "Description": "本示例会创建一个简单的VPC网络，需要用户提供下面正确的数据\n公有网络Uuid\n管理网络Uuid: 如果只有公有网络，则把公有网络当作管理网即可.\nVxlan网络的VTEP Cider"

  定义对模板的解释说明。

- "Parameters": { }

  定义模板的参数列表。

  本例中定义了以下参数：

  - 云路由镜像URL
  - 云主机镜像URL
  - 镜像服务器
  - 管理网络
  - 公有网络
  - 区域

- 集群
- VTEP CIDR
- Vni、起始Vni、结束Vni
- 起始IP、结束IP、子网掩码、网关

- "Resources": { }

  定义该模板将要创建的资源。

  本例中声明将要创建以下资源：

  - 添加一个云路由镜像
  - 添加一个云主机镜像
  - 创建一个云路由规格
  - 创建一个VPC路由器
  - 创建VXLAN网络池
  - 创建一个二层VXLAN网络
  - 创建一个VPC网络
  - 创建一个计算规格
  - 将VPC网络绑定到云主机
  - 配置VPC网络的IP范围
  - 将二层VXLAN网络加载到集群
  - 创建一个云主机

  这里声明的资源属性可以引用"Parameters": { }中定义的参数。

- "Outputs": { }

  定义资源创建完成后，通过资源栈输出资源属性等有用信息。

关于模板语法的详细介绍，请参考资源栈模板语法章节。

2. 通过示例模板创建资源栈。

   在**资源栈示例模板**界面，选择示例模板**ZStack.System.v1.VPC**，点击**更多操作** > **创建资源栈**，弹出**创建资源栈**界面。

   1. 可参考以下示例输入相应内容：

      - **区域**：自动显示当前区域
      - **名称**：设置资源栈名称

- **简介**：可选项，可留空不填
- **超时设置**：用于设置创建资源栈的超时时限，超时将失败，默认为60分钟
- **失败回滚**：默认勾选，超时失败后将清理已创建的资源
- **资源栈模板**：自动显示已选择的模板

如图 *704: 创建资源栈1*所示，点击**下一步**。

图 704: 创建资源栈1

2. 根据需要的资源信息输入各个参数，不同类型的资源栈需要输入的参数不同。本例中可参考以下示例输入相应内容：

- **云路由镜像URL**：添加云路由镜像以创建VPC路由器
- **云主机镜像URL**：添加创建云主机的镜像
- **镜像服务器**：选择合适的镜像服务器
- **管理网络**：选择已提前创建的管理网络

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。

- **公有网络**：选择已提前创建的公有网络
- **区域**：自动显示当前区域
- **集群**：可选项，可选择VXLAN网络池加载的集群
- **VTEP CIDR**：设置VTEP相应的CIDR
- **Vni**：可选项，可从VXLAN网络池中选择指定的Vni，若留空不填，则由系统动态随机分配
- **起始Vni**：设置VXLAN网络池的起始Vni
- **结束Vni**：设置VXLAN网络池的结束Vni
- **起始IP**：设置VPC网络的起始IP
- **结束IP**：设置VPC网络的结束IP
- **子网掩码**：设置VPC网络的子网掩码
- **网关**：设置VPC网络的网关

如图 *705:* 创建资源栈*2*所示，点击**确定**，开始创建资源栈。

图 705: 创建资源栈2

上一步
预览
确定
取消
创建资源栈
云路由镜像URL:
http://cdn.zstack.io/product_downloads/vrouter/2.3/zs
云主机镜像URL:
http://cdn.zstack.io/zstack_repo/latest/zstack-image-
镜像服务器: *
BS-1
管理网络: *
L3-管理网络
公有网络: *
L3-公有网络
区域: *
ZONE-1
集群: *
Cluster-1

注:

- 开始创建资源栈前，可点击**预览**查看将要创建的资源列表。
- 创建资源栈需要一定时长，请等待创建完成。

3. 管理资源栈。

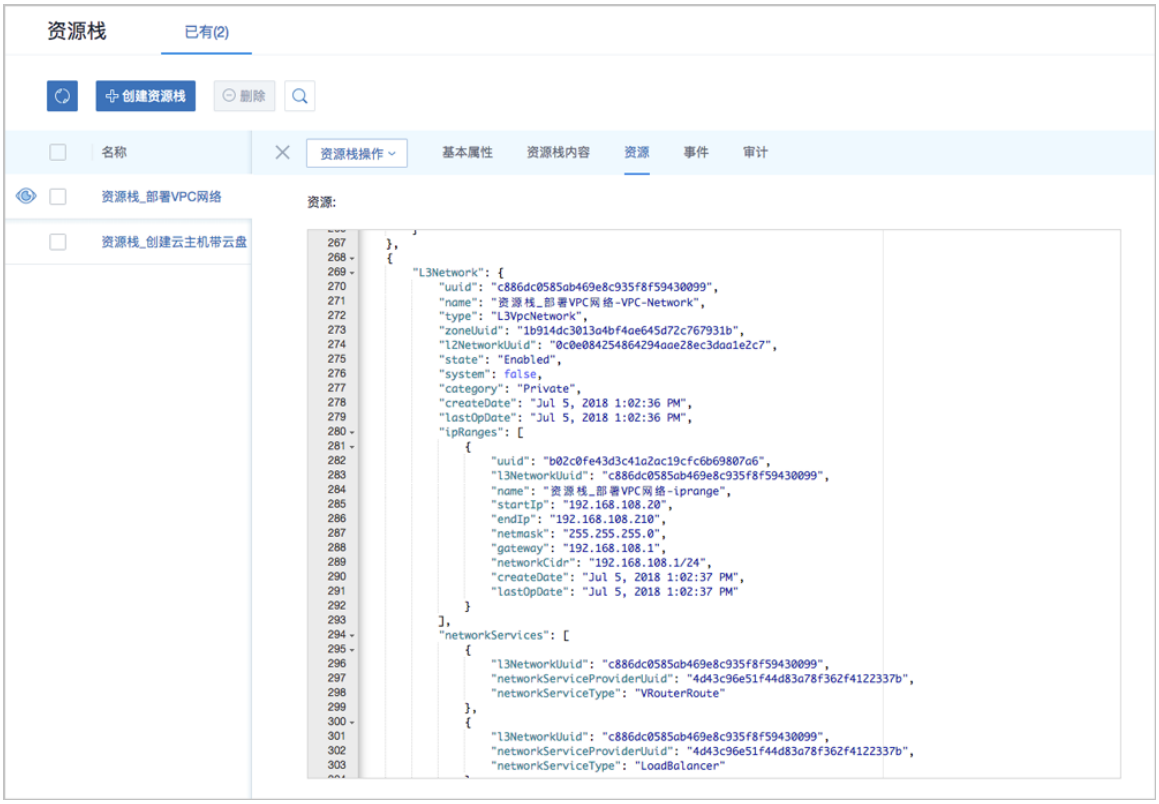
   资源栈创建成功后，可在**资源栈**界面，选中当前创建的资源栈，展开其详情页，查看栈状态和栈信息。

   - 基本信息：显示资源栈当前状态、名称、简介、栈UUID等信息，其中名称和简介支持修改
   - 资源栈内容：包括模板数据和参数配置
     - 模板数据：显示当前资源栈所对应的模板信息

  - 参数配置：创建资源栈时指定的参数信息
- 资源：显示资源栈所包括的全部资源信息
- 事件：显示资源栈生命周期中发生的每一个事件
- 审计：查看此资源栈的相关操作

本例中，资源栈内的全部资源信息如图 *706:* 资源栈输出资源信息所示：

图 706: 资源栈输出资源信息



如果不再使用该资源栈，可将栈删除。

7.9.7.8 附录

7.9.7.8.1 资源栈模板语法

资源栈模板是一个UTF8编码格式的文件。

基于模板可快速创建资源栈，用户在模板中定义所需的云资源、资源间的依赖关系、资源配置等，资源编排将解析模板，自动完成所有资源的创建和配置。

资源栈模板结构

资源栈模板结构如下：

```
{
  "ZStackTemplateFormatVersion" : "YYYY-MM-DD",
  "Description" : "模板描述信息，可用于说明模板的适用场景、架构说明等。",
  "Parameters" : {
    // 定义创建资源栈时，用户可以定制化的参数。
  },
  "Mappings" : {
    // 定义映射信息表，映射信息是一种多层的Map结构。
  },
  "Resources" : {
    // 所需资源的详细定义，包括资源间的依赖关系、配置细节等。
  },
  "Outputs" : {
    // 用于输出一些资源属性等有用信息，可以通过API获取输出的内容。
  }
```

- **ZStackTemplateFormatVersion(必需)**

  模板版本号。

  - 格式为：YYYY-MM-DD
- **Description(可选)**

  模板描述信息，可用于说明模板的适用场景、架构说明等。

  - 对模板进行详细描述，有利于用户理解模板内容。
- **Parameters(可选)**

  定义创建资源栈时，用户可以定制化的参数。

  - 例如，用户将创建云主机的计算规格设计成一个参数。
  - 参数支持默认值。
  - 使用参数可以增强模板的灵活性，提高复用性。
  - 关于**参数(Parameters)**的详细介绍，请参考*参数(Parameters)*章节。
- **Mappings(可选)**

  定义映射信息表，映射信息是一种多层的Map结构。

  - 可通过Fn::FindInMap函数选择key对应的值。
  - 可根据不同的输入参数值作为key查找映射表。
  - 例如，可根据区域不同，自动查找区域-镜像映射表，从而找到适用的镜像。
  - 关于**映射(Mappings)**的详细介绍，请参考*映射(Mappings)*章节。

- **Resources(可选)**

  所需资源的详细定义，包括资源间的依赖关系、配置细节等。

  - 关于**资源(Resources)**的详细介绍，请参考资源*(Resources)*章节。
- **Outputs(可选)**

  用于输出一些资源属性等有用信息，可以通过API获取输出的内容。

  - 关于**输出(Outputs)**的详细介绍，请参考输出*(Outputs)*章节。

7.9.7.8.1.1 参数(Parameters)

参数(Parameters)：定义创建资源栈时，用户可以定制化的参数。

- 创建资源栈模板时，使用参数可以增强模板的灵活性，提高复用性。
- 创建资源栈时，可根据实际情况替换模板中的某些参数值。

语法

参数由参数名称和参数属性组成。

- 参数名称必须为字母数字，同一个模板中不能与其它参数名称重复。
- 可以用Label字段定义友好的参数名。

参数属性列表：

属性	描述	是否必需	举例
Type	参数类型，默认支持： • String • Number(整数或浮点) • CommaDelimited List(相当于Java里的List<String>) • Boolean	是	"Type": "String"
Lable	参数别名，生成预览或正式表单时用	否	"Lable": "云主机密码"
Description	参数描述	否	"Description": "云主机登录密码"

属性	描述	是否必需	举例
NoEcho	该字段是否用*****替代，不填则不替代	否	"NoEcho": true **注:** 暂不支持
DefaultValue	参数默认值	否	"DefaultValue": "password"

资源编排还提供一些常量参数。

- 常量参数可直接引用，无需在Parameters中定义（也不可定义）。
- 其值在资源编排运行时确定。

常量参数列表

常量名	描述
ZStack::StackName	当前栈的名称
ZStack::StackUuid	当前栈的UUID
ZStack::AccountUuid	当前栈的AccountUuid
ZStack::AccountName	当前栈的AccountName

示例

代码段示例如下：

```
"Parameters" : {
  "username" : {
    "Label": "登录名",
    "Description" : "登录名",
    "DefaultValue": "root",
    "Type" : "String"
  },
  "password" : {
    "Label": "密码",
    "NoEcho" : "true",
    "Description" : "主机登录密码",
    "Type" : "String",
    "AllowedPattern" : "[a-zA-Z0-9]*"
  }
}
```

本例中Parameters声明两个参数：

- username
  - 参数属于**String**类型，默认值为**root**。

- 可指定的最小长度为**2**，可指定的最大长度为**12**。

注: username的默认值也必须符合长度限制和允许值限制。

- password
  - 参数属于**String**类型，无默认值。
  - 将NoEcho属性设置为**true**，可阻止查询栈接口返回参数值。

注: NoEcho属性设置暂不支持。

  - 可指定的最小长度为**6**，可指定的最大长度为**41**。
  - 允许大、小写字母字符和数字。

7.9.7.8.1.2 资源(Resources)

资源(Resources)：所需资源的详细定义，包括资源间的依赖关系、配置细节等。

- Resources可引用前述Parameters、Mappings、以及Functions的内容。
- Resources可被其他Resources和Outputs所引用。

语法

资源由资源逻辑UUID和资源描述组成。

- 资源描述用大括号{ }括起。
- 如果声明多个资源，用逗号,分隔开。

资源关键字列表：

关键字	描述	是否必需	举例
Type	资源类型，包括以下两种类型： • Resource类型 • Action类型	是	• "Type": "ZStack::Resource::VmInstance" • "Type": "ZStack::Action::AddIpRange" • 详情请参考**资源类型*(Type)***
Properties	资源属性，为资源指定创建参数	是	详情请参考**资源属性*(Properties)***

关键字	描述	是否必需	举例
DependsOn	资源依赖，定义资源所依赖的资源	否	• "DependsOn": [{"Ref": "WebServer1"}] • 详情请参考**资源依赖*(DependsOn)***
DeletionPolicy	删除策略 • 资源栈被删除时是否保留某个资源 • 若某个资源需要保留，则它所依赖的资源也要保留(系统自动为其保留) • 默认不保留	否	• "DeletionPolicy": "Retain" • 详情请参考**删除策略*(DeletionPolicy)***
Description	资源描述	否	• "Description" : "attach ip range to l3 network"

示例

代码段示例如下：

```
"Resources" : {
   "UUID-1" : {
      "Description" : "资源描述",
      "Type" : "资源类型",
      "Properties" : {
         资源属性描述
      }
   },
   "UUID-2" : {
      "Description" : "资源描述"
      "Type" : "资源类型",
      "Properties" : {
         资源属性描述
      } ,
      "DependsOn":"要依赖的资源，如UUID-1，注意上下文中必须包含此资源",
      "DeletionPolicy":"删除策略"
   }
}
```

本例中Parameters声明了两个资源，关键字说明如下：

- **输出UUID**

- UUID-1、UUID-2均为资源逻辑UUID，且均为变量。
- 在创建模板其它部分时，可以通过资源逻辑UUID引用该资源。
- 资源逻辑UUID在模板中具有唯一性。

- **资源类型(Type)**
  - 表示正在声明的资源的类型，包括：Resource类型、Action类型。
  - 例如，"Type": "ZStack::Resource::VmInstance"表示云主机实例，"Type": "ZStack::Action::AddIpRange"表示添加IP范围。
  - 关于资源编排支持的所有资源列表，详情请参考章节。
- **资源属性(Properties)**
  - 为资源指定创建参数。
  - 代码段示例如下：

```
"Resources" : {
   "InstanceOffering" : {
      "Type" : "ZStack::InstanceOffering",
      "Properties" : {
         "cpuNum" : "1",
         "cpuSpeed" : "1",
         "memorySize" : "1073741824",
         "name" : "instance-offering",
         "type" : "UserVm",
         "sortKey": 0,
         "allocatorStrategy": "LeastVmPreferredHostAllocatorStrategy"
      }
   }
}
```

  - 资源属性值定义规则：
    - 属性值可以是文本字符串、字符串列表、布尔值、引用参数、或者函数返回值。
    - 如果属性值为文本字符串或布尔值，该值会被双引号" "括起来。
    - 如果属性值为任一类型的字符串列表，该值会被中括号[ ]括起来。
    - 如果值为内部函数或引用的参数，该值会被大括号{ }括起来。
    - 将文字、列表、引用参数、和函数返回值合并起来取值时，上述规则适用。
    - 以下示例说明如何声明不同的属性值类型：

```
"Properties" : {
   "String" : "string",
   "LiteralList" : [ "value1", "value2" ],
   "Boolean" : "true"
   "ReferenceForOneValue" :  { "Ref" : "ResourceID" } ,
   "FunctionResultWithFunctionParams" : {
      "Fn::Join" : [ "%", [ "Key=", { "Ref" : "SomeParameter" } ] ] }
```

```
}
```

- 如果资源不需要声明任何属性，可以忽略该资源的属性部分。

- **资源依赖(DependsOn)**

  - 定义资源所依赖的资源。
  - 为某个资源添加DependsOn属性后，该资源仅在DependsOn属性中指定的资源之后创建。
  - 代码段示例如下：

```
{
   "ZStackTemplateFormatVersion" : "2018-06-18",
   "Resources" : {
      "WebServer": {
         "Type": "ZStack::Resource::VmInstance",
         "DependsOn": "DatabseServer"
      },
      "DatabseServer": {
         "Type": "ZStack::Resource::VmInstance",
         "Properties": {
            "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"},"VM"]]},
            "instanceOfferingUuid": {"Ref":"InstanceOfferingUuid"},
            "imageUuid":{"Ref":"ImageUuid"},
            "l3NetworkUuids":[{"Ref":"PrivateNetworkUuid"}],
            "dataDiskOfferingUuids":[{"Ref":"DiskOfferingUuid"}],
        "hostUuid":{"Ref":"HostUuid"}
         }
      }
   }
}
```

  本例表示WebServer将在DatabaseServer创建成功后才开始创建。

- **删除策略(DeletionPolicy)**

  - 在模板中，设置DeletionPolicy属性，可以声明资源栈被删除时是否保留资源。
  - DeletionPolicy有Retain和Delete两个选项。
    - 默认为Delete，表示删除资源栈默认会删除栈内编排创建的所有资源。
    - 若将DeletionPolicy设置为Retain，表示资源栈被删除时可保留资源。此时，该资源所依赖的资源也要保留（系统自动为其保留）。

      例如，模板对应的资源栈被删除时，保留栈内的云主机，代码段示例如下：

```
"Resources" : {
   "VMInstance" : {
      "Type" : "ZStack::Resource::VmInstance",
      "Properties": {
         "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"},"VM"]]},
         "instanceOfferingUuid": {"Ref":"InstanceOfferingUuid"},
         "imageUuid":{"Ref":"ImageUuid"},
         "l3NetworkUuids":[{"Ref":"PrivateNetworkUuid"}],
         "dataDiskOfferingUuids":[{"Ref":"DiskOfferingUuid"}],
     "hostUuid":{"Ref":"HostUuid"}
```

```
    },
    "DeletionPolicy" : "Retain"
  }
}
```

7.9.7.8.1.3 输出(Outputs)

输出(Outputs)：用于输出一些资源属性等有用信息，可以通过API获取输出的内容。

语法

输出由输出UUID和输出描述组成。

- 输出描述用大括号{ }括起。
- 如果声明多个输出项，用逗号,分隔开。

输出关键字列表：

关键字	描述	是否必需	举例
Description	输出描述	否	• "Description" : "print l3 network" • 详情请参考**输出描述(Description)**
Value	输出内容	是	• "Value" : {"Ref": "WebServer1"} • 详情请参考**输出内容(Value)**

示例

代码段示例如下：

```
"Outputs" : {
    "UUID-1" : {
        "Description" : "输出描述",
        "Value" : "输出内容"
    },
    "UUID-2" : {
        "Description" : "输出的描述",
        "Value" : "输出内容"
    }
}
```

本例中Output声明了两个输出项，关键字说明如下：

- **输出UUID**

- 输出UUID在模板中具有唯一性。

- **输出描述(Description)**
  - 用于描述输出值的String类型。
- **输出内容(Value)**
  - 在调用查询堆栈接口时，返回的属性值。
  - 代码段示例如下：

```
{
 "ZStackTemplateFormatVersion": "2018-06-18",
 "Description": "本示例将创建一个带云盘的云主机(基于本地存储), 创建示例前提环境：\n
计算规格，镜像，云盘规格，私有网络，可用物理机",
 "Parameters": {
    "InstanceOfferingUuid": {
       "Type": "String",
            "Label": "计算规格",
  "Description": "The instance offering uuid"
    },
    "ImageUuid": {
  "Type": "String",
            "Label": "镜像",
  "Description": "The Image uuid for creating VmInstance, Please choose an image not
iso"
    },
    "PrivateNetworkUuid": {
  "Type": "String",
            "Label": "私有网络",
  "Description" : "The private network uuid for creating VmInstance"
        },
    "DiskOfferingUuid": {
  "Type": "String",
            "Label": "云盘规格",
  "Description": "Volume size offering uuid"
    },
    "HostUuid": {
  "Type": "String",
            "Label": "物理机",
  "Description": "Host uuid, that vm will start on"
    }
},
"Resources": {
    "VmInstance": {
  "Type": "ZStack::Resource::VmInstance",
  "Properties": {
      "name": {"Fn::Join":["-",[{"Ref":"ZStack::StackName"},"VM"]]},
      "instanceOfferingUuid": {"Ref":"InstanceOfferingUuid"},
      "imageUuid":{"Ref":"ImageUuid"},
      "l3NetworkUuids":[{"Ref":"PrivateNetworkUuid"}],
      "dataDiskOfferingUuids":[{"Ref":"DiskOfferingUuid"}],
      "hostUuid":{"Ref":"HostUuid"}
  }
    }
},
"Outputs": {
    "VmInstance": {
```

```
        "Value": {
      "Ref": "VmInstance"
    }
     }
  }
}
```

本例中，输出部分有1个输出项，将输出VmInstance的属性值。

7.9.7.8.1.4 函数(Functions)

资源编排提供多个内置函数，用于管理资源栈。可在定义资源(Resources)、输出(Outputs)和映射(Mappings)时，使用内置函数。

提供的内置函数列表：

- Fn::Base64
- Fn::FindInMap
- Fn::GetAtt
- Fn::Join
- Fn::Split
- Fn::Select
- Ref

Fn::Base64

返回输入字符串的Base64编码结果。

- **声明**

```
"Fn::Base64" : stringToEncode
```

- **参数**
  - stringToEncode：转换成Base64的字符串。
- **示例**

```
"Fn::Base64" : "password"
```

- **返回值**

  用Base64表示的原始字符串。

  本例中，返回"cGFzc3dvcmQ="，即"password"的Base64编码结果。

Fn::FindInMap

返回与Mappings声明的双层映射中的键对应的值。

- **声明**

```
"Fn::FindInMap" : ["MapName", "TopLevelKey", "SecondLevelKey"]
```

- **参数**
  - MapName：Mappings 中所声明映射的 ID，包含键和值。
  - TopLevelKey：第一级键，其值是一个键/值对列表。
  - SecondLevelKey：第二级键，其值是一个字符串或者数字。
- **示例**

```
"Fn::FindInMap" : ["RegionMap", "cn-shanghai", "32"]
```

- **返回值**

  分配给SecondLevelKey的值。

  本例中，返回"RegionMap"中"cn-shanghai"对应的键/值对列表里，键为"32"对应的值。

- **支持的函数**

  可在Fn::FindInMap函数中嵌套使用以下函数：

  - Fn::FindInMap
  - Ref

Fn::GetAtt

返回模板中的资源的属性值。

- **声明**

```
"Fn::GetAtt": ["resourceUuid", "attributeName"]
```

- **参数**
  - resourceUuid：目标资源的逻辑UUID。
  - attributeName：目标资源的属性名称。
- **示例**

```
"Fn::GetAtt" : ["MyVMInstance", "ImageUuid"]
```

- **返回值**

属性值。

本例中，返回resourceUuid为"MyVMInstance"的"ImageUuid"属性。

Fn::Join

将一组值连接起来，用特定分隔符隔开。

- **声明**

```
"Fn::Join" : ["delimiter", ["string1", "string2", ...]]
```

- **参数**
  - delimiter：分隔符。分隔符可为空，可将所有的值直接连接起来。
  - ["string1", "string2", ...]：被连接起来的值列表示例。
- **示例**

```
"Fn::Join" : ["-", ["a", "b", "c"]]
```

- **返回值**

  被连接起来的字符串。

  本例中，返回"a-b-c"

- **支持的函数**

  可在Fn::Join函数中嵌套使用以下函数：

  - Fn::Base64
  - Fn::GetAtt
  - Fn::Join
  - Fn::Select
  - Ref

Fn::Split

通过指定分隔符对字符串进行切片，并返回所有切片组成的列表。

- **声明**

```
"Fn::Split" : ["delimiter", "original_string"]
```

- **参数**
  - delimiter：分隔符，例如：,，;，\n，\t 等。

- original_string：将要被切片的字符串。

- **示例**

```
"Fn::Split": [";", "foo; bar; achoo"]
```

- **返回值**

  切片后所有字符串组成的列表。

  本例中，返回["foo", " bar", "achoo"]

- **支持的函数**

  可在Fn::Split函数中嵌套使用以下函数：

  - Fn::Base64
  - Fn::FindInMap
  - Fn::GetAtt
  - Fn::Join
  - Fn::Select
  - Ref

Fn::Select

通过索引返回数据元列表中的单个数据元。

- **声明**

  - 数据元列表可为一个数组：

    ```
    "Fn::Select" : ["index", ["value1", "value2", ...]]
    ```

  - 数据元列表可为一个映射表：

    ```
    "Fn::Select" : ["index", {"key1": "value1", ...}]
    ```

- **参数**

  - index：待检索数据元的索引。

    - 如果数据元列表是一个数组，则索引是0到N-1之间的某个值，其中N代表阵列中元素的数量。
    - 如果数据元列表是一个映射表，则索引是映射表中的某个键。
    - 如果找不到索引对应的值，则返回空字符串。

- **示例**

- 示例一：数据元列表是一个数组

```
"Fn::Select" : ["2", ["foo", " bar", "achoo"]]
```

- 示例二：数据元列表是一个映射表

```
"Fn::Select" : ["shape", {"shape": "circle", "height": "80"}]
```

- 示例三：数据元列表是一个CommaDelimitedList

```
"Parameters" : {
 "userParam": {
          "Type": "CommaDelimitedList",
          "Default": "10.0.100.0/24, 10.0.101.0/24, 10.0.102.0/24"
      }
},
"Resources": {
 "resourceUuid": {
          "Properties": {
             "CidrBlock": {"Fn::Select" : ["0", {"Ref":"userParam"}]}
          }
      }
}
```

- **返回值**

  选定的数据元。

  - 示例一：返回"achoo"
  - 示例二：返回"circle"
  - 示例三：返回"10.0.100.0/24"

- **支持的函数**

  - 对于Fn::Select索引值，可在Fn::Select函数中嵌套使用Ref函数。
  - 对于对象的Fn::Select列表，可在Fn::Select函数中嵌套使用以下函数：
    - Fn::Base64
    - Fn::FindInMap
    - Fn::GetAtt
    - Fn::Join
    - Fn::Select
    - Ref

Ref

返回指定参数或资源的值。

- 如果指定参数是resourceUuid，则返回资源的值。
- 否则系统将认为指定参数是参数，将尝试返回参数的值。
- **声明**

```
"Ref":"logicalName"
```

- **参数**
  - logicalName：要引用的资源或参数的逻辑名称。
- **示例**

  若diskOfferingParam被定义为：

```
"diskOfferingParam": {
 "allocatorStrategy": "DefaultPrimaryStorageAllocationStrategy",
       "diskSize": "21474836480",
       "type": "DefaultDiskOfferingType",
       "sorkKey": "0"
}
```

```
"Ref":"diskOfferingParam"
```

- **返回值**

  资源的值或者参数的值。

  本例中，返回diskOfferingParam的值：

```
{
 "allocatorStrategy": "DefaultPrimaryStorageAllocationStrategy",
       "diskSize": "21474836480",
       "type": "DefaultDiskOfferingType",
       "sorkKey": "0"
}
```

- **支持的函数**

  不能在Ref函数中嵌套使用任何函数。必须指定为资源逻辑UUID的字符串。

7.9.7.8.1.5 映射(Mappings)

定义映射信息表，映射信息是一种多层的Map结构。

- 映射是一个Key-Value映射表。
- 在模板的Resources和Outputs中，可使用内置函数Fn::FindInMap，通过指定Key而获取映射表的Value。

语法

映射由Key-Value键值对组成。

- 其中Key和Value可以为字符串类型或者数字类型。
- 如果声明多个映射，用逗号,分隔开。
- 每个映射的名称不能重复。

示例

代码段示例如下：

```
"Mappings" : {
 "Mapping01" : {
        "Key01" : {
           "Name" : "Value01"
        },
        "Key02" : {
           "Name" : "Value02"
        },
        "Key03" : {
           "Name" : "Value03"
        }
    }
}
```

使用内置函数Fn::FindInMap返回对应的值示例：

```
{
 "ZStackTemplateFormatVersion": "2018-06-18",
    "Parameters": {
       "regionParam": {
          "Description": "选择创建云主机的区域",
          "Type": "String",
          "AllowedValues": ["cn-hangzhou", "cn-shanghai"]
       }
    },
    "Mappings" : {
       "ImageInRegions" : {
          "cn-hangzhou" : { "32" : "imageUuid-1", "64" : "imageUuid-2" },
          "cn-shanghai" : { "32" : "imageUuid-3", "64" : "imageUuid-4" }
       }
    },
    "Resources": {
       "WebServer": {
          "Type": "ZStack::Resource::VmInstance",
          "Properties": {
             "name" : "test-vm",
             "imageUuid" : {"Fn::FindInMap": ["ImageInRegions", {"Ref":"regionParam"}, "64"]},
             "instanceOfferingUuid": {"Ref":"instanceOfferingUuid"},
             "l3NetworkUuids": [{"Ref":"l3NetworkUuid"}]
          },
          "DeletionPolicy": "Retain"
       }
    }
```

```
}
```

7.9.7.8.2 资源索引

创建资源栈模板时，可根据**资源类型(Type)**和**资源属性(Properties)**信息，申明对所需资源的具体要求。

资源编排支持的**资源类型(Type)**包括以下两种：

- Resource类型
- Action类型

7.9.7.8.2.1 Resource类型

表 60: Resource类型资源索引表

Resouce类型	说明
ZStack::Resource::VmInstance	创建云主机*(CreateVmInstance)*
ZStack::Resource::DataVolume	创建云盘*(CreateDataVolume)*
ZStack::Resource::Image	添加镜像*(AddImage)*
ZStack::Resource::RootVolumeTemplate	***从根云盘创建根云盘镜像(CreateRootVolumeTemplateFromRootVolume)***
ZStack::Resource::DataVolumeTemplate	从云盘创建数据云盘镜像*(CreateDataVolumeTemplateFromVolume)*
ZStack::Resource::AffinityGroup	创建亲和组*(CreateAffinityGroup)*
ZStack::Resource::InstanceOffering	创建云主机规格*(CreateInstanceOffering)*
ZStack::Resource::DiskOffering	创建云盘规格*(CreateDiskOffering)*
ZStack::Resource::L2VxlanNetworkPool	创建*VXLAN*网络池*(CreateL2VxlanNetworkPool)*
ZStack::Resource::L2NoVlanNetwork	创建普通二层网络*(CreateL2NoVlanNetwork)*
ZStack::Resource::L2VlanNetwork	创建二层*VLAN*网络*(CreateL2VlanNetwork)*
ZStack::Resource::L2VxlanNetwork	创建*VXLAN*网络*(CreateL2VxlanNetwork)*
ZStack::Resource::L3Network	创建三层网络*(CreateL3Network)*
ZStack::Resource::VRouterRouteTable	创建云路由路由表*(CreateVRouterRouteTable)*
ZStack::Resource::VpcVRouter	创建*VPC*云路由*(CreateVpcVRouter)*

Resouce类型	说明
ZStack::Resource::SecurityGroup	创建安全组*(CreateSecurityGroup)*
ZStack::Resource::SecurityGroupRule	添加规则到安全组*(AddSecurityGroupRule)*
ZStack::Resource::Vip	创建虚拟*IP(CreateVip)*
ZStack::Resource::Eip	创建弹性*IP(CreateEip)*
ZStack::Resource::PortForwardingRule	创建端口转发规则*(CreatePortForwardingRule)*
ZStack::Resource::LoadBalancer	创建负载均衡器*(CreateLoadBalancer)*
ZStack::Resource::LoadBalancerListener	创建负载均衡监听器*(CreateLoadBalancerListener)*
ZStack::Resource::IPsecConnection	创建*IPsec*连接*(CreateIPsecConnection)*
ZStack::Resource::VirtualRouterOffering	创建云路由规格*(CreateVirtualRouterOffering)*
ZStack::Resource::VniRange	创建*Vni Range(CreateVniRange)*

7.9.7.8.2.2 Action类型

表 61: Action类型资源索引表

Action类型	说明
ZStack::Action::AddIpRange	添加*IP*地址范围*(AddIpRange)*
ZStack::Action::AddDnsToL3Network	向三层网络添加*DNS(AddDnsToL3Network)*
ZStack::Action::AddVmToAffinityGroup	添加云主机到亲和组*(AddVmToAffinityGroup)*
ZStack::Action::AddVRouterRouteEntry	添加云路由路由条目*(AddVRouterRouteEntry)*
ZStack::Action::AddCertificateToLoadBalancerListener	添加证书到负载均衡*(AddCertificateToLoadBalancerListener)*
ZStack::Action::AddIpRangeByNetworkCidr	通过网络*CIDR*添加*IP*地址范围*(AddIpRangeByNetworkCidr)*
ZStack::Action::AddVmNicToLoadBalancer	添加云主机网卡到负载均衡器*(AddVmNicToLoadBalancer)*
ZStack::Action::AddVmNicToSecurityGroup	添加虚拟机网卡到安全组*(AddVmNicToSecurityGroup)*
ZStack::Action::AddRemoteCidrsToIPsecConnection	添加远端*CIDR*到*IPsec*连接*(AddRemoteCidrsToIPsecConnection)*

Action类型	说明
ZStack::Action::AttachEip	绑定弹性IP(AttachEip)
ZStack::Action::AttachDataVolumeToVm	挂载云盘到云主机上(AttachDataVolumeToVm)
ZStack::Action::AttachPortForwardingRule	挂载规则到虚拟机网卡上(AttachPortForwardingRule)
ZStack::Action::AttachIsoToVmInstance	加载ISO到云主机(AttachIsoToVmInstance)
ZStack::Action::AttachPciDeviceToVm	绑定PCI设备到云主机(AttachPciDeviceToVm)
ZStack::Action::AttachUsbDeviceToVm	云主机挂载所在物理机USB设备(AttachUsbDeviceToVm)
ZStack::Action::AttachL2NetworkToCluster	挂载二层网络到集群(AttachL2NetworkToCluster)
ZStack::Action::AttachL3NetworkToVm	加载L3网络到云主机(AttachL3NetworkToVm)
ZStack::Action::AttachNetworkServiceToL3Network	挂载网络服务到三层网络(AttachNetworkServiceToL3Network)
ZStack::Action::AttachSecurityGroupToL3Network	挂载安全组到L3网络(AttachSecurityGroupToL3Network)
ZStack::Action::AttachL3NetworksToIPsecConnection	添加三层网络到IPsec连接(AttachL3NetworksToIPsecConnection)
ZStack::Action::AttachVRouterRouteTableToVRouter	绑定云路由路由表到云路由器(AttachVRouterRouteTableToVRouter)
ZStack::Action::AddCertificateToLoadBalancerListener	添加证书到负载均衡(AddCertificateToLoadBalancerListener)
ZStack::Action::AddHostRouteToL3Network	向三层网络添加主机路由(AddHostRouteToL3Network)

7.10 平台管理

平台管理主要涵盖：用户管理、计费管理、定时器、邮箱服务器、AD/LDAP、控制台代理。

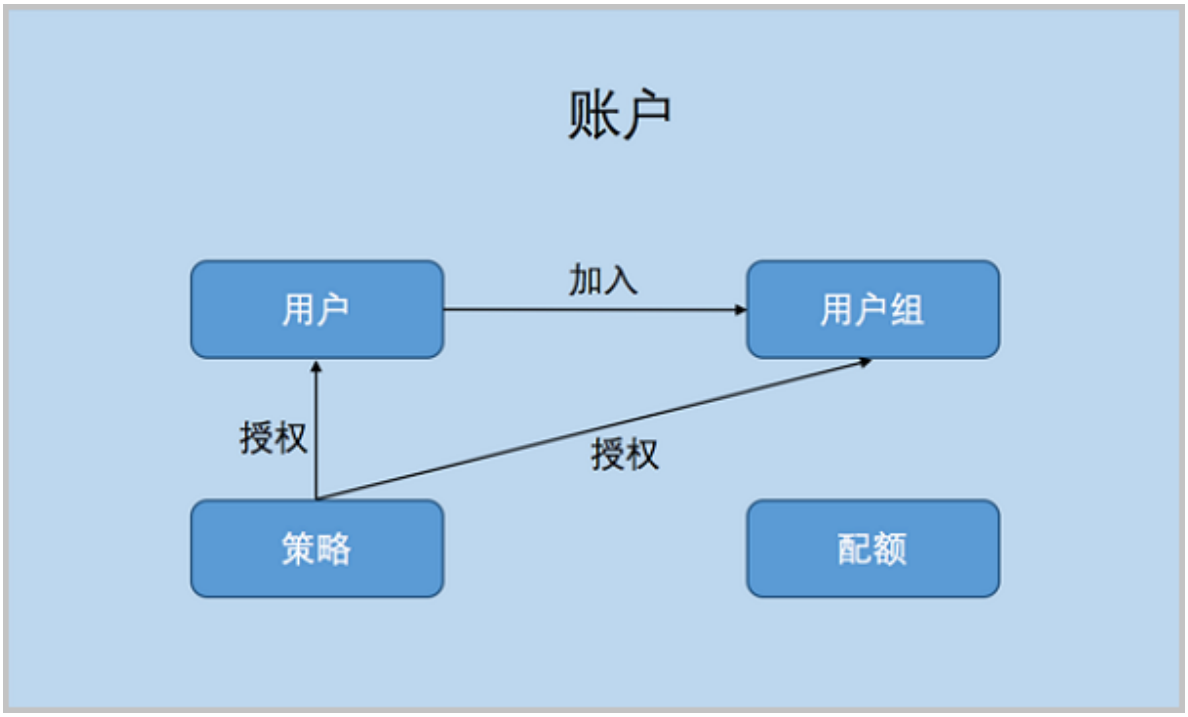
7.10.1 用户管理

用户管理主要提供了用户对系统资源的访问控制，可实现以细粒度对资源归属及权限控制的划分。

- 用户管理提供账户、用户组、用户的管理，同时涉及策略、配额等概念。

- 用户管理系统的整体结构如图 *707:* 用户管理系统所示：

  图 707: 用户管理系统



相关定义

- **账户**：

  作为资源拥有的基本单位，对作用域的资源可以进行创建、删除、分享、召回等操作。账户分为admin管理员账户和普通账户。

- **用户**：

  用户账户创建，用于实现更细粒度的权限控制。admin创建的用户，也称之为admin用户，拥有和admin账户相同的全部权限。

- **用户组**：

  普通账户可以通过创建用户组对一组用户进行批量的权限控制。

- **资源配额**：

  简称配额，是admin账户对普通账户的资源总量进行控制的衡量标准。

  - 主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。
  - admin账户可修改以上各参数对各个普通账户进行资源总额的控制。当资源删除后，但还未彻底删除时，会占用主存储资源和云盘数量。

相关约束

1. **admin管理员账户**：也称之为admin账户，不受权限控制，拥有超级权限，通常由IT系统管理员拥有。
   - admin账户可以共享计算规格、云盘规格、网络、镜像等其他资源给普通账户，而普通账户只能操作属于自己的资源。admin账户同时也可以对相关资源进行召回，不再共享。
   - admin账户可以通过修改配额对普通账户进行资源总量控制。
   - admin账户创建的admin用户，和admin账户一样，拥有全局的控制权限。
   - admin账户不能够修改别的账户的普通用户的权限。普通用户的权限应该由该用户所属的账户管理。
   - admin账户不支持创建用户组，也不支持对其他账户的用户和用户组进行跨越管理。但可以修改普通账户、普通用户的用户名、密码和简介。
   - admin账户创建VxlanNetworkPool后，普通账户可以基于VxlanNetworkPool创建VxlanNetwork。
   - 只支持删除admin用户，不支持删除admin账户。
   - 更改云主机所有者会更改云主机的EIP所有者属性。
2. **普通账户**：由admin管理员账户创建。
   - 普通账户拥有对自己创建的云主机、镜像、云盘、安全组、用户组和用户的管理权限。普通账户可以对admin账户共享的资源进行读操作，但不可以进行删除操作。
   - 普通账户可以通过权限控制来操控属于自己的用户或用户组。
   - 普通账户可以使用用户组对批量用户进行权限控制。
   - 删除普通账户会导致此账户下的所有资源被删除，例如，云主机、云盘、镜像、名下用户和用户组等信息。
   - 普通用户默认只拥有对普通账户资源的只读权限。
   - 普通用户不占有资源，经授权后，可共享并使用自己所属账户下的资源。
   - 删除普通用户只会删除普通用户的自身信息，其所创建的云主机、镜像、云盘均会保留在自己所属的账户名下。
   - 普通账户名称不可重复。同一账户下的用户和用户组名称不可重复。
   - 普通用户的名字、简介和密码可以通过admin账户修改，也可通过所属账户进行修改。
   - 同一用户可加入多个不同用户组。
   - 账户登录只需输入账户名和密码，用户登录需要输入账户名、用户名和密码。

- 普通账户首页看到的资源是admin账户分配的资源配额的上限。
- 普通账户创建云主机前，需要admin账户提前共享计算规格、网络和云盘规格等资源，否则不可创建云主机。
- 普通账户可以添加自有的镜像文件，也可由admin账户提前共享。
- 用户权限受到用户权限设置页以及该用户所属用户组权限设置页共同控制。只要用户权限设置页，或者该用户所属任意用户组权限设置页授予了某资源的权限，即代表该用户拥有该权限对应的操作。如果需要禁止该用户对某资源的操作权限，需要禁止该用户权限页，以及该用户所属所有用户组权限页相关资源的操作权限。

7.10.1.1 账户

在ZStack私有云主菜单，点击**平台管理** > **用户管理** > **账户**，进入**账户**管理界面，如图 *708:* 账户所示。

图 708: 账户

ZStack对账户操作的定义如下：

- **搜索**：在账户管理界面上支持三种搜索方式：名称、UUID和高级搜索。
- **创建账户**：在当前区域中创建一个新的账户，点击**创建账户**按钮，会打开**创建账户**界面，输入新的账户的名称、简介（选填）和密码然后点击**确定**按钮创建，如图 *709:* 创建账户所示。

图 709: 创建账户

- **修改密码**：admin账户和普通账户的密码都可以被修改。只支持单一操作。
  - 系统登录admin账户：可以修改admin账户和普通账户的密码。勾选要修改的账户，点击**更多操作** > **修改密码**按钮，在**修改密码**窗口中填写密码，然后确认。
  - admin账户也可以点击右上角的**个人设置** > **修改密码**来修改。

  注: 修改admin账户的密码后需退出admin账户后重新登录才可生效。
- **绑定AD/LDAP**：将AD/LDAP与账户名绑定，输入AD/LDAP服务器中已有的AD/LDAP用户ID进行相关绑定，可实现AD/LDAP账户登录ZStack界面进行云平台管理。只支持单一操作。
- **解绑AD/LDAP**：对于一个已经绑定AD/LDAP的账户，取消该账户与AD/LDAP用户的绑定。此账户将不再支持AD/LDAP登录。只支持单一操作。
- **删除**：删除账户会删除此账户下的所有资源，请谨慎操作。支持批量操作。

  注: admin账户不可删除。

admin账户和普通账户的详情界面不相同，这里重点介绍一下普通账户的详情界面：

- **普通账户的详情界面**：

在账户管理界面，点击普通账户名称可显示**账户详情**界面： 它包含：**基本属性**、**用户组**、**用户**、**云主机**、**路由器**、**云盘**和**AD/LDAP**，还有一个**账户操作**按钮可以对当前账户进行操作，它里面的操作菜单是账户管理界面上所有账户操作的合集。 如图 *710:* 普通账户详情所示。

图 710: 普通账户详情

- **基本属性**栏显示当前账户的基本信息，包括名称、简介、概览和更多信息。在此栏上可以修改账户的名称、简介和配额。
  - 修改配额：支持对普通账户名下云主机数量、运行中的云主机数量、CPU容量、内存容量、数据云盘数量、可用存储容量、镜像数量、所有镜像容量、VXLAN网络数量、三层网络数量、安全组数量、弹性IP数量、虚拟IP数量、快照数量、定时任务数量等进行相应的资源配额设置。设置后，普通账户对相关资源的配置不能超过配额控制。
- **用户组**栏显示了当前普通账户下所有的用户组列表及其基本信息但不能做任何操作，如图 *711:* 用户组所示。

图 711: 用户组

- **用户**栏显示了当前普通账户下所有用户的列表及其基本信息但不能做任何操作，如图 *712: 用户*所示。

图 712: 用户

- **云主机**栏显示了当前普通账户下所有的云主机列表及其基本信息。在此栏上可以对这些云主机正常做操作，如图 *713: 云主机*所示。

图 713: 云主机

- **云路由**栏显示当前普通账户下所有的云路由列表及其基本信息。在此栏上可以对这些云路由正常做操作，如图 *714: 云路由*所示：

图 714: 云路由

- **云盘**栏显示当前普通账户下所有的云盘列表及其基本信息。在此栏上可以对这些云盘正常做操作，如图 *715: 云盘*所示。

图 715: 云盘

- **AD/LDAP**栏显示当前普通账户下所有的AD/LDAP列表及其基本信息。在此栏上可以对这些AD/LDAP正常做操作，如图 *716: AD/LDAP*所示：

图 716: AD/LDAP

- **admin账户的用户组详情界面**：包含：基本属性、云主机、云路由、云盘和AD/LDAP。和基本账户相似。

注: admin账户的基本属性栏上比普通账户少了**配额**。

7.10.1.2 用户组

在ZStack私有云主菜单，点击**平台管理** > **用户管理** > **用户组**，进入**用户组**管理界面，如图 *717: admin账户用户组*和图 *718: 普通账户用户组*所示。

注: admin账户和**普通账户**登录后的用户组管理界面是不同的。

图 717: admin账户用户组

图 718: 普通账户用户组

- **admin账户**不支持创建用户组，也不支持用户组的操作。所以页面上没有任何操作按钮。
- **普通账户**可以创建和操作用户组。ZStack对普通账户的用户组操作的定义如下：
  - **搜索**：在用户组管理界面上支持三种搜索方式：名称、UUID和高级搜索。

- **创建用户组**：点击**创建用户组**按钮，在**创建用户组**界面，输入相应的用户组名称和简介，点击**确定**按钮即可创建用户组，如图 *719:* 创建用户组所示。

  图 719: 创建用户组

- **添加用户**：添加用户到当前的用户组中。只支持单一操作。
- **删除**：删除的用户组。支持批量操作。

admin账户和普通账户的用户组详情界面不相同，这里重点介绍一下普通账户的用户组详情界面：

- **普通账户的用户组详情界面**：

  用普通账户登录ZStack后，在用户组管理界面，点击用户组的名字，可以展开**用户组详情**界面，它包含三栏：**基本属性**、**用户**和**权限设置**。还有一个**用户组操作**按钮可以对当前用户组进行操作，它里面的操作菜单是用户组管理界面上所有用户组操作的合集。点击左上角**X**按钮可以关闭用户组详情界面，如图 *720:* 普通账户用户组详情所示。

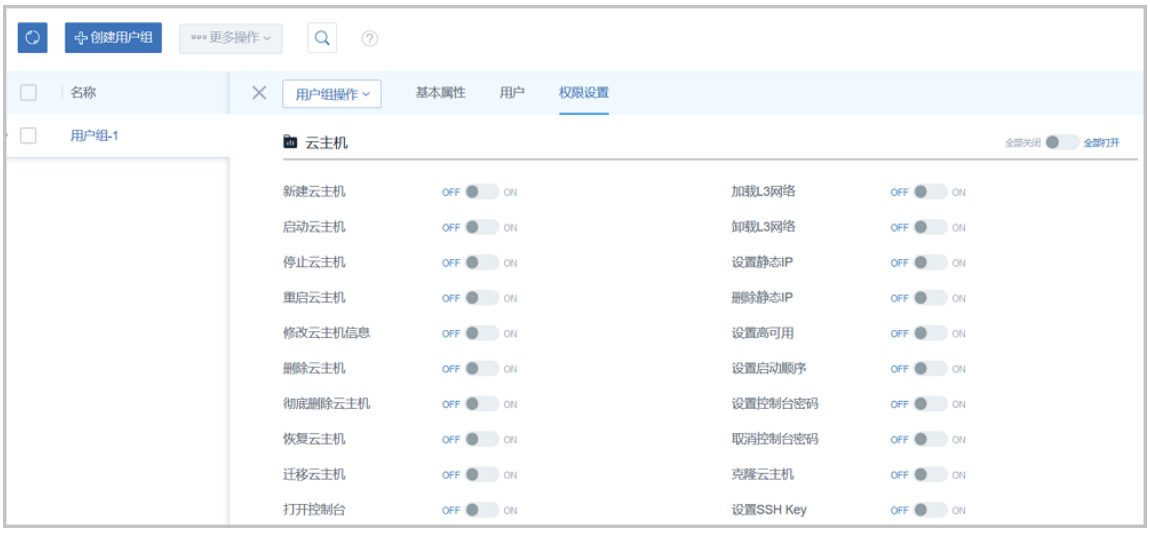
  图 720: 普通账户用户组详情

- **基本属性**栏显示当前用户组的基本信息，包括名称、简介和更多信息，如图 *720: 普通账户用户组详情*所示。在此栏上可以修改用户组的名称和简介。
- **用户**栏显示当前用户组下所有用户的列表及其基本信息，在此栏上可以对这些用户进行操作，如图 *721: 用户*所示。

图 721: 用户

- **权限设置**栏显示当前用户组对其下的用户权限有相同的权限控制条目，总共有八类资源：**云主机**、**定时任务**、**镜像**、**云盘**、**弹性IP**、**安全组**、**用户**和**标签**，如图 *722: 权限设置*所示。

图 722: 权限设置



- **总控开关**：八类资源都可通过总控的打开和关闭按钮进行统一控制。点击相应的**全部打开**和**全部关闭**按钮，可以对此八类资源进行批量控制。
- **条目开关**：此八类资源的权限还细分为更详细的权限控制条目。可以通过点击相应条目后面的on/off按钮进行开关的控制。

  注: 因为相应的权限条目之间存在相关的逻辑关系。在打开某个条目，可能导致其他权限条目也会打开，来保证相关业务流程正常运行。

  例如，打开冷迁移云主机权限，会需要卸载云盘，迁移云盘，加载云盘。所以打开冷迁移云主机权限，这几个权限也会打开。

- **admin账户的用户组详情界面**：包含两栏：基本属性栏和用户栏，和基本账户相似。

7.10.1.3 用户

在ZStack私有云主菜单，点击**平台管理** > **用户管理** > **用户**，进入**用户**管理界面，如图 *723: admin*账户用户管理和图 *724:* 普通账户用户管理所示。

图 723: admin账户用户管理

图 724: 普通账户用户管理

ZStack对用户的操作定义如下：

- **搜索**：在用户管理界面上支持三种搜索方式：名称、UUID和高级搜索。
- **创建用户**：点击**创建用户**按钮，打开**创建用户**界面，填入新用户的名称、简介（选填）和密码，然后点击**确定**按钮即可创建。如图 *725:* 创建用户所示。

  图 725: 创建用户

- **修改密码**：可以修改当前账户下的用户的密码。只支持单一操作。
- **删除**：删除当前账户下的用户。支持批量操作。

admin账户和普通账户的用户详情界面不相同，这里重点介绍一下普通账户的用户详情界面：

- **普通账户的用户详情界面**：

  用普通账户登录ZStack后，在用户管理界面，点击用户的名字可显示**用户**详情界面： 它包含：**基本属性**和**权限控制**。还有一个**用户操作**按钮可以对当前用户进行操作，它里面的操作菜单是用户管理界面上所有用户操作的合集。点击左上角**X**按钮可以关闭用户详情界面，如图 *726: 普通账户的用户详情*所示。

  图 726: 普通账户的用户详情

- **基本属性**栏显示当前用户的基本信息，包括名称、简介和更多信息，如图 *726:* 普通账户的用户详情所示。在此栏上可以修改用户的名称和简介。
- **权限设置**栏显示当前用户的权限控制条目。和用户组的权限设置栏相似。

  注: 对用户组的权限控制会对组内用户生效。对用户的权限控制只对本用户生效。如果用户组和用户的权限列表状态出现不一致的情况，用户组权限高于用户。例如其中某条目的权限在用户显示off，但是在用户组显示on，则此条目的权限为on状态。如果用户所在的任一用户组，打开了某权限，而尝试在用户界面进行关闭此权限会提示“不能关闭，所属用户组已打开权限”。需要将用户所在的所有打开此权限的用户组关闭掉，才可在用户界面关闭此权限。

- **admin账户的用户详情界面**：包含两栏：基本属性栏和用户组栏，和基本账户相似。

7.10.2 计费管理

7.10.2.1 账单

账单：按计费单价和使用时间来统计并显示所有项目或账户下各资源的资费信息。

在ZStack私有云主菜单，点击**平台管理** > **计费管理** > **账单**按钮，进入**账单**页面，如图 *727:* 账单所示：

图 727: 账单

- 账单页面分为项目和账户两个子页面，支持显示计费项目或计费账户、总额、根云盘、云主机、数据云盘和GPU设备的计费信息。

  注: 账单的**项目**子页面，需要安装企业管理模块许可证后才可见，否则只显示账户账单信息。

- 默认指定的时间段为当前时间过去的一个月，可根据实际需求选择不同的时间间隔来计算，精准至秒级。
- 账单详情页显示某账户在指定时间内的根云盘、数据云盘、云主机、GPU设备的基本属性及具体费用信息。
- 在计费单价变化的过程中，也会分阶段显示相关的费用信息。

7.10.2.2 计费设置

计费设置：计费信息的显示需提前对各资源创建计费单价。计费设置支持对处理器、内存、根云盘、数据云盘等基本计费资源进行计费单价设置。以各资源的规格大小和时间作为基本计费单位，并以时长作为服务使用记录，从而对不同账户使用的业务量进行统计计费。

在ZStack私有云主菜单，点击**平台管理** > **计费管理** > **计费设置**，进入**计费设置**管理界面，如图 *728:* 计费设置所示。

图 728: 计费设置

计费设置管理界面分为五栏：处理器、内存、根云盘、数据云盘和GPU设备。进入不同的栏可以对不同的计费类型进行操作。操作包括创建账单和删除账单。

- **创建账单**：在不同的栏可以对不同的计费类型创建计费。创建计费时包括下边几个选项：
  - **价格**：价格为单位时间内单位资源的费用，必须大于等于0，精确到5位小数；且不可修改。
  - **数量单位**：创建内存、根云盘和数据云盘计费时，数量单位默认为G, 可选值为 M、G、T。

    注: CPU的数量单位默认为**个**，没有单独列出。
  - **时间单位**：时间单位默认为小时，可选值为秒、分、小时、天、周、月（30天）。
  - **类型**：创建GPU设备账单需要选择GPU类型，可选项：桌面显卡、计算显卡
  - **型号**：创建GPU设备账单需要选择GPU型号

  创建计费单价后，在相关的资源管理界面，会显示相应的计费单价。在计费列表中，每个资源的首行代表该资源的当前使用价格，其他行代表该资源在特定时间段内的使用价格。价格列显示了资源的计费单价明细，例如**内存**栏的￥0.17/GB/小时，代表内存每小时每GB的价格为0.17元。开始时间列代表此价格的生效时间。

  - 例如May 26 2016 10:23:58 AM, 代表当前计费从2016年5月26日10点23分58秒开始计费。简介列详述了当前单价生效的时间段和单价的明细。

  如果相关资源成本发生变化时，也可以对资源的计费单价进行调整。例如，因市场发生变化，内存条价格下跌，相关的成本也开始下降，此时需要下调内存的计费单价，用户可以重新创建内存计费单价来进行计费。

  - 例如：如图 *729: 修改内存单价*所示，在￥0.17/GB/小时计费一段时间后，开始以￥0.15/GB/小时开始对内存进行计费。针对正在使用中的资源，计费单价会从新创建计费的时间点切入进行计费。图示的￥0.17/GB/小时的有效时间为2017年6月12日23点19分39秒

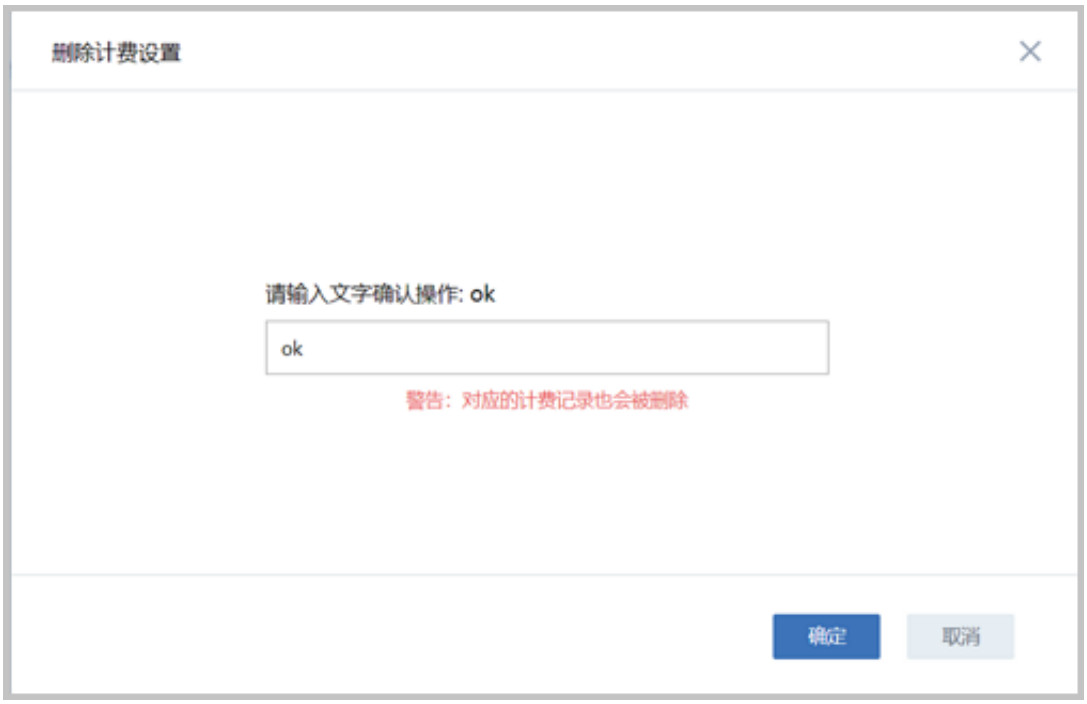
到2017年6月12日23点21分4秒，此时间段内的费用按照￥0.17/GB/小时的单价计费。从2017年6月12日23点21分4秒后，开始按照￥0.15/GB/小时进行内存计费。

图 729: 修改内存单价

- **删除**：如果想删除计费规则，则去对应的栏进行删除。勾选需要删除的计费规则，点击**删除**按钮，输入**ok**后，点击**确定**按钮即可删除相应的计费规则。删除内存计费规则如图 *730:* 删除计费所示。

  注: 如果删除所有计费规则，则账户计费清零。

图 730: 删除计费



7.10.3 定时

ZStack 定时器和定时任务完全解耦，用户可按需创建不同规则的定时器、以及不同的定时任务，并将定时任务灵活加载到定时器或从定时器上卸载。删除定时器后，该定时器上的定时任务将被卸载，定时任务可重新加载到其它定时器上。

7.10.3.1 定时器

定时器是承载定时任务的容器。该功能非常适用于长时间运行的操作，例如，为某个云主机定时创建快照。定时器和定时任务完全解耦，用户可按需创建不同规则的定时器、以及不同的定时任务，并将定时任务灵活加载到定时器或从定时器上卸载。定时器的操作会完整的进入审计中。

在ZStack私有云主菜单，点击 **平台管理** > **定时** > **定时器**，进入**定时器**页面，如图 *731:* 定时器所示：

图 731: 定时器

定时器页面显示了定时器的名称、执行策略、开始时间、周期、定时器状态和创建日期等信息。

创建定时器

在ZStack私有云主菜单，点击 **平台管理** > **定时** > **定时器**，点击 **创建定时器**按钮，弹出**创建定时器**界面，可参考以下示例输入相应内容：

- **名称**：自定义定时器名称
- **简介**：可选项，可留空不填
- **执行策略**：选择合适的执行策略，包括重复执行和按次数执行
  - 选择**重复执行**：定时任务按周期无限重复执行
  - 选择**选择次数**：定时任务按周期有限次执行，需设置执行次数

  注: 对于周期内有限次执行的定时器，当定时任务执行完后，定时器状态将显示为**已完成**。
- **开始日期**：默认当前时间，可按需更改

- **周期**：设置定时器执行周期，单位包括：分、小时、天

如图 *732: 创建定时器*所示：

图 732: 创建定时器

定时器详情页

定时器详情页包括基本属性、定时任务和审计三个子页面。

- **基本属性**

  基本属性子页面显示了定时器的基本信息，包括：定时器状态、定时器名称和简介、任务数量、执行策略、执行周期、开始时间及到期时间等。其中**执行策略**和**周期**支持在该页面上修改。如图 *733: 基本属性*所示：

  图 733: 基本属性

- **定时任务**

定时任务子页面不仅可查看该定时器上加载的定时任务信息，还可对定时任务进行相关操作，包括：创建定时任务、启用定时任务、停用定时任务、加载定时任务到定时器、将定时任务从定时器卸载、删除定时任务。如图 *734:* 定时任务所示：

图 734: 定时任务

- **审计**

审计子页面针对定时器调用API操作提供审计，可查看该调用API名称、消耗时间、任务结果、操作员，任务创建/完成时间，以及API行为的消息详情。

- 支持设置时间段，可查看所设时间段内调用API的审计信息。

注: 界面最多显示300条审计信息，请调整合适的时间段进行搜索。

- 支持通过输入资源类型/资源UUID/API名称/操作员，搜索调用API的审计信息。
- 支持调整每页显示的审计消息数量，可选值为：10、20、50、100；且支持翻页操作。

定时器支持的操作

- 创建定时器：创建一个新的定时器
- 创建定时任务：创建一个定时任务并加载到该定时器
- 删除：删除定时器。删除定时器后，该定时器上的定时任务将被卸载，定时任务可重新加载到其它运行的定时器上

7.10.3.2 定时任务

定时任务是加载到定时器上的任务条目。定时器和定时任务完全解耦，用户可按需创建不同规则的定时器、以及不同的定时任务，并将定时任务灵活加载到定时器或从定时器上卸载。此外，定时任务支持选择性停用/启用/加载/卸载，可灵活处理生产环境中的特殊情况。定时任务的操作也会完整的进入审计中。

在ZStack私有云主菜单，点击 **平台管理** > **定时** > **定时任务**，进入**定时任务**页面，如图 *735:* 定时任务所示：

图 735: 定时任务

定时任务页面显示了定时任务的名称、任务类型、资源名称、开始日期、任务策略、启用状态、定时器状态、定时器和创建日期等信息。

创建定时任务

在ZStack私有云主菜单，点击 **平台管理** > **定时** > **定时任务**，在**定时任务**页面点击**创建定时任务**按钮，可参考以下示例输入相应内容：

- **名称**：自定义定时任务名称

- **任务**：选择任务类型。目前支持任务类型包括：启动云主机、停止云主机、重启云主机、创建云主机快照、创建云盘快照
- **云主机**：选择执行任务的云主机，可多选
- **定时器**：可选项，可将定时任务加载到合适的定时器上

如图 *736:* 创建定时任务所示：

图 736: 创建定时任务

定时任务详情页

- **基本属性**

  定时任务子页面显示了该定时任务的基本信息，包括：任务类型、资源名称、开始执行的日期、挂载的定时器、任务策略等。如图 *737:* 基本属性所示：

  图 737: 基本属性

- **审计**

  审计子页面针对定时任务调用API操作提供审计，可查看该调用API名称、消耗时间、任务结果、操作员，任务创建/完成时间，以及API行为的消息详情。

  - 支持设置时间段，可查看所设时间段内调用API的审计信息。

    注: 界面最多显示300条审计信息，请调整合适的时间段进行搜索。

  - 支持通过输入资源类型/资源UUID/API名称/操作员，搜索调用API的审计信息。
  - 支持调整每页显示的审计消息数量，可选值为：10、20、50、100；且支持翻页操作。

定时任务支持的操作

- 创建定时任务：创建一个新的定时任务
- 启用：启用定时任务，启动后该定时任务生效，支持批量操作
- 停用：停用定时任务，停用后该定时任务不生效，支持批量操作
- 加载：将定时任务加载到运行的定时器上，支持批量操作
- 卸载：将定时任务从定时器上卸载，支持批量操作
- 删除：删除该定时任务，不可恢复，支持批量操作

7.10.4 应用中心

应用中心提供增强功能以及各类第三方应用快速访问。支持添加各类第三方应用入口URL，便于用户集中管理以及快速打开应用。

添加应用

在ZStack私有云主菜单，点击**平台管理** > **应用中心**按钮，在**应用中心**页面，点击**添加应用**按钮，可参考以下示例输入相应内容：

- **应用类型**：选择添加应用的类型，不同的类型在主界面可显示不同的图标。可选项：存储、数据库、安全、IaaS、PaaS、SaaS
- **应用**：选择应用，可选项：推荐（例如RANCHER）、其它
- **名称**：输入应用名称
- **简介**：可选项，可留空不填
- **URL**：输入应用的URL地址
- **共享权限**：设置共享权限，可选项：仅管理员可见、所有人可见

如图 *738:* 添加应用所示，点击**确定**按钮，完成应用添加。

图 738: 添加应用

添加完成后如图 *739: 添加完成*所示（已安装企业管理模块许可证）：

图 739: 添加完成

- 将鼠标移动至卡片，点击**进入应用**按钮，可直接跳转至目标路径。
- 点击卡片右上角的应用操作按钮中的**修改应用**，可对卡片的名称、简介、类型、URL、共享权限进行修改。
- 点击卡片右上角的应用操作按钮中的**删除应用**，可删除卡片。

7.10.5 邮箱服务器

ZStack支持ZWatch监控报警功能，若接收端选择邮件类型，需设置邮件服务器，用来接收报警邮件。

添加邮箱服务器

在ZStack私有云主菜单，点击**平台管理 > 邮箱服务器**，进入**邮箱服务器**界面，点击**添加邮箱服务器**按钮，在弹出的**添加邮箱服务器**界面，可参考以下示例输入相应内容：

- **名称**：设置邮箱服务器名称
- **简介**：可选项，可留空不填
- **用户名**：输入用户名
- **密码**：输入用户名对应的密码
- **邮箱服务器类型**：系统默认为smtp
- **邮箱服务器**：输入邮箱服务器地址
- **邮箱服务器端口**：输入邮箱服务器端口，默认为25

- **加密类型**：可选项，支持对邮箱服务器端口设置加密连接，加密类型有：STARTTLS、SSL/TLS、NONE

  注:

  - 默认选择STARTTLS加密类型，端口25；
  - 选择SSL/TLS加密类型时，端口默认465；
  - 若SMTP服务器不使用加密连接，可选择NONE。

如图 *740:* 添加邮箱服务器所示：

图 740: 添加邮箱服务器

注:

请按实际情况填写相关信息，如有疑问请联系相关邮箱服务器提供商。

7.10.6 AD/LDAP

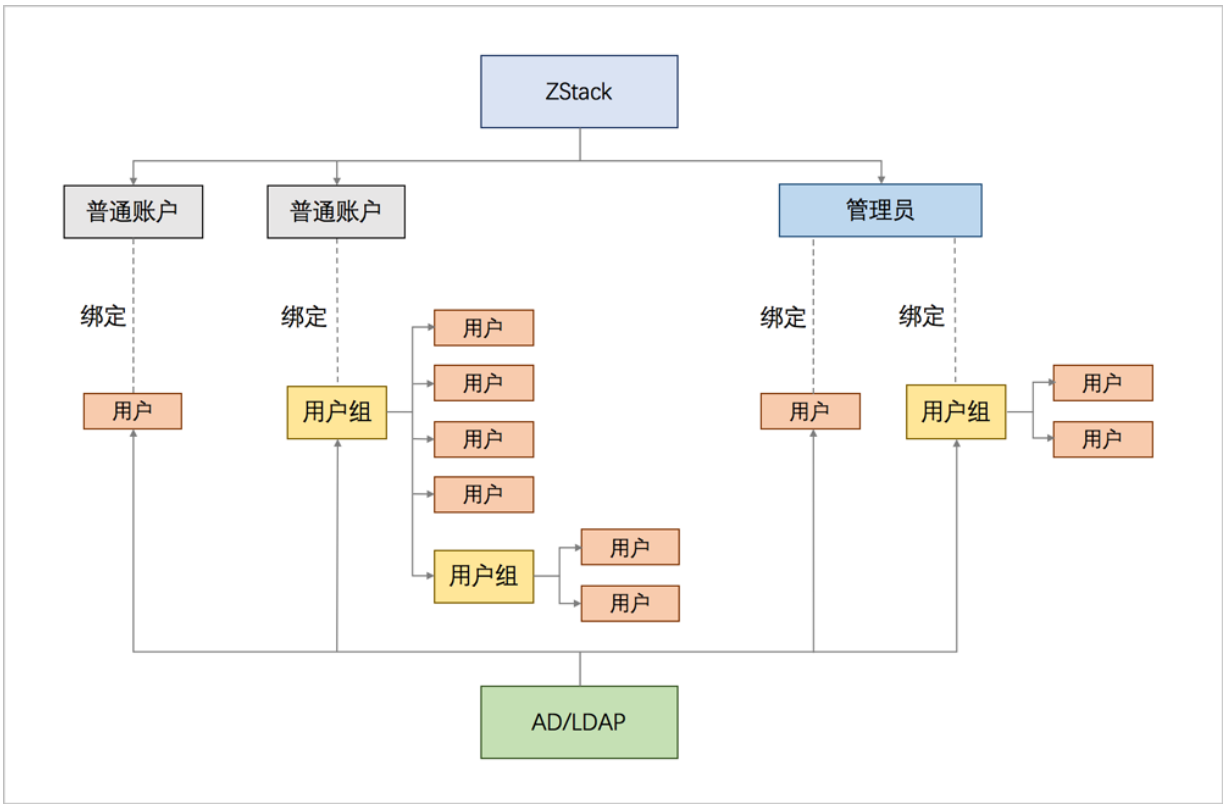
7.10.6.1 介绍

LDAP（Lightweight Directory Access Protocol）作为轻量级目录访问协议，可提供标准的目录服务。微软的WindowsAD软件（以下简称AD），以及众多流行的Linux发行版中提供的OpenLDAP软件（以下简称LDAP），均是基于LDAP协议的实现，它们为日益多样化的企业办公应用提供了一套独立、标准的登录认证系统。

ZStack支持无缝接入AD/LDAP统一认证服务，基于自定义规则添加AD/LDAP服务器，并获取成员列表；当AD/LDAP成员（用户/用户组）成功绑定ZStack账户（普通账户/管理员），就可使用成员登录属性直接登录ZStack云平台。

ZStack账户（普通账户/管理员）与AD/LDAP成员（用户/用户组）的绑定关系如图 *741: ZStack-AD/LDAP绑定关系*所示：

图 741: ZStack-AD/LDAP绑定关系



本教程将详细介绍ZStack接入AD/LDAP的配置方法。

注: 目前，仅支持接入一套AD/LDAP登录认证系统。

7.10.6.2 前提

在此教程中，假定已安装最新版本ZStack，具体方式请参考用户手册安装部署章节。

7.10.6.3 添加AD/LDAP

背景信息

ZStack支持基于自定义规则添加AD/LDAP服务器。

操作步骤

1. 登录ZStack

   使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*http://your_machine_ip:5000/*），默认用户名和密码为：*admin/password*。

   如图 *742: ZStack登录界面*所示：

   图 742: ZStack登录界面

2. 进入**AD/LDAP**管理界面。

   在ZStack私有云主菜单，点击**平台管理** > **AD/LDAP**，进入**AD/LDAP**管理界面。

   如图 *743: AD/LDAP管理界面*所示：

   图 743: AD/LDAP管理界面

3. 添加AD/LDAP。

   点击**添加AD/LDAP**，弹出**添加AD/LDAP**界面。

   如图 *744: AD/LDAP设置界面*所示：

   图 744: AD/LDAP设置界面

注: 由于AD/LDAP统一认证服务是基于LDAP协议的不同实现，添加AD/LDAP的方法基本一致，以下将以添加AD服务器为例进行介绍。

a) 在**AD/LDAP**设置界面，可参考以下示例输入相应内容：

- 选择添加的服务器类型：
  - **AD**：将添加WindowsAD类型的服务器
  - **LDAP**：将添加OpenLDAP类型的服务器

- **服务器**：填写AD/LDAP服务器的域名或IP地址

  以AD为例：*adtest.com*或*172.20.12.180*

- **端口**：填写访问AD/LDAP服务器所使用的端口，默认使用389端口
- **基准检索DN**：填写用于检索已绑定AD/LDAP成员的基准DN（Distinguished Name）

  注: 基准检索DN的设置会限制查询结果

  - 希望查询当前AD/LDAP域的所有成员，请设置基准检索DN为：域节点

    以AD为例：*DC=adtest,DC=com*

  - 希望查询当前AD/LDAP域中隶属某一组织的成员，请设置基准检索DN为：目标组织节点

    以AD为例：*OU=people,DC=adtest,DC=com*

- **登录属性**：设置AD/LDAP服务器的登录属性，登录属性决定了已绑定AD/LDAP成员的登录名

  以AD为例：

  - *distinguishedName*：表示已绑定AD成员可用*distinguishedName*相应的value（例如：*CN=xiaoming,OU=people,DC=adtest,DC=com*）作为ZStack登录名
  - *userPrincipalName*：表示已绑定AD成员可用*userPrincipalName*相应的value（例如：邮箱地址 *xiaoming@adtest.com*）作为ZStack登录名
  - *cn*：已绑定AD成员可用*cn*相应的value（例如：名称*xiaoming*）作为ZStack登录名

  注:

  - 支持自定义设置登录属性；默认情况下，设置AD服务器的登录属性为*cn*，LDAP服务器的登录属性为*uid*
  - 为确保成功登录，所指定的登录属性在AD/LDAP域中相应的value（作为登录名）必须全局唯一

- **用户DN**：填写用于AD/LDAP服务器认证的AD/LDAP成员的DN，需确保填写完整

  以AD为例：*CN=xiaoming,OU=people,DC=adtest,DC=com*

  注:

  所填写的用户DN，必须有权访问基准检索DN中的所有用户，因此是与基准检索DN相对应的或域级、或组织级、或用户组级的管理员DN

- **密码**：填写与用户DN相应的密码
- **清除规则**：可选项，自定义清除规则，系统将清理满足条件的绑定关系

  以AD为例：希望清除所有已离职员工的账号绑定关系，可设置清除规则*(description*=已离职*)*

如图 *745: 添加AD*所示：

图 745: 添加AD

b) 点击**确定**，将保存所填写配置信息。

4. 管理AD/LDAP服务器。

   在**AD/LDAP**管理界面，可对已添加的AD/LDAP进行管理，支持以下操作：

   - 查看：

     点击已添加的AD/LDAP，展开详情页，可查看名称、端口号、基准检索DN、登录属性、用户DN、清除规则等基本属性。

   - 测试：

     选中已添加的AD/LDAP服务器，点击**更多操作** > **测试**，会基于所填写配置信息尝试连接AD/LDAP。

   - 同步：

     当AD/LDAP的配置信息发生变化，例如，设置新的清除规则，选中已更新配置信息的AD/LDAP，点击**更多操作** > **同步**，将清除ZStack中无效的绑定信息。

   - 删除：

     目前仅支持添加一个AD/LDAP，如需添加其它AD/LDAP，或对已添加的AD/LDAP更新配置信息，需删除当前AD/LDAP，进行重新添加。

后续操作

至此，ZStack成功添加AD/LDAP，将获取AD/LDAP成员列表。接下来，ZStack需要绑定AD/LDAP成员。

7.10.6.4 绑定AD/LDAP成员

前提条件

ZStack账户（普通账户/管理员）与AD/LDAP成员（用户/用户组）的绑定关系如下：

- 普通账户：

  一套ZStack支持创建多个普通账户。

  - 一个普通账户可直接绑定一个或多个AD/LDAP成员（用户/用户组）
  - 普通账户绑定AD/LDAP用户组时，支持用户组中嵌套用户组
  - 一个AD/LDAP成员（用户/用户组）不可绑定多个普通账户
  - 一个AD/LDAP成员（用户/用户组）绑定一个普通账户后，不可再绑定管理员
  - 绑定普通账户的AD/LDAP成员登录ZStack后，所属资源、权限与当前所绑定的普通账户一致

- 管理员：

  一套ZStack仅支持创建一个管理员。

  - 管理员可直接绑定一个或多个AD/LDAP成员（用户/用户组）
  - 管理员绑定AD/LDAP用户组时，支持用户组中嵌套用户组
  - 一个AD/LDAP成员（用户/用户组）绑定管理员后，不可再绑定普通账户。
  - 绑定管理员的AD/LDAP成员登录ZStack后，所属资源、权限与当前所绑定的管理员一致

背景信息

普通账户绑定AD/LDAP成员，与管理员绑定AD/LDAP成员，操作方法完全一致，以下将以普通账户绑定AD/LDAP成员为例进行介绍。

操作步骤

1. 进入普通账户绑定AD/LDAP成员界面。

   在ZStack私有云主菜单，点击**平台管理** > **用户管理** > **账户**，进入**账户**界面，选择某一普通账户，进入其详情页。点击**AD/LDAP**，进入**AD/LDAP**界面。

   如图 *746: AD/LDAP界面*所示：

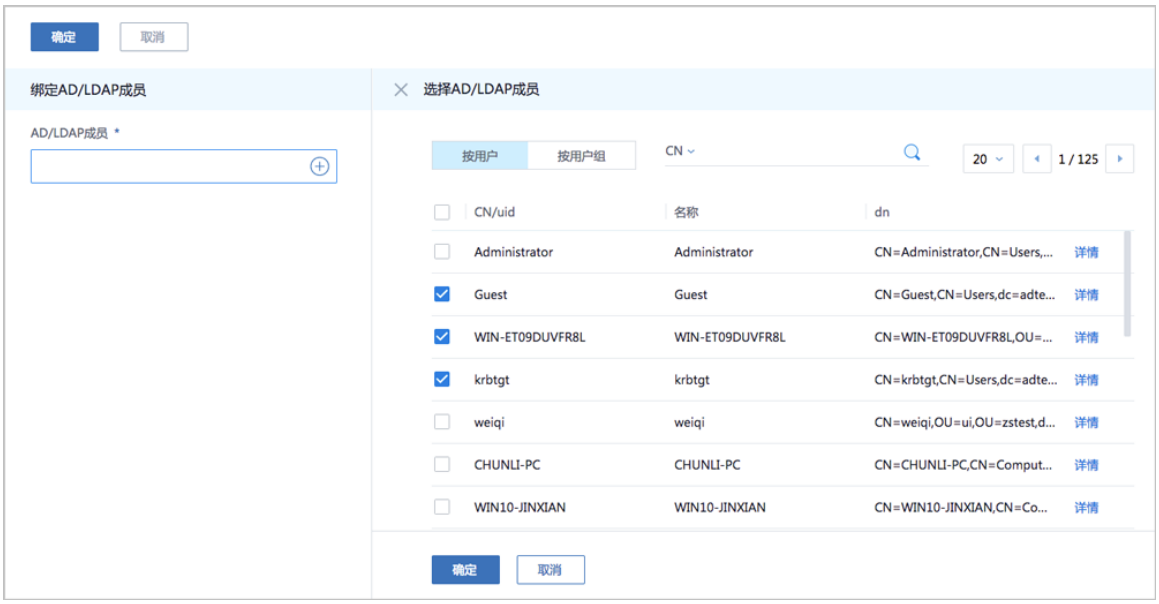
   图 746: AD/LDAP界面

2. 勾选绑定到普通账户的AD/LDAP成员。

   点击**操作** > **绑定AD/LDAP成员**，弹出**绑定AD/LDAP成员**界面，点击**+**，展开**选择AD/LDAP成员**列表页，分别提供**按用户**和**按用户组**两个分栏，可按需勾选绑定到该普通账户的AD/LDAP成员。

   如图 *747: 选择AD/LDAP成员*所示：

   图 747: 选择AD/LDAP成员

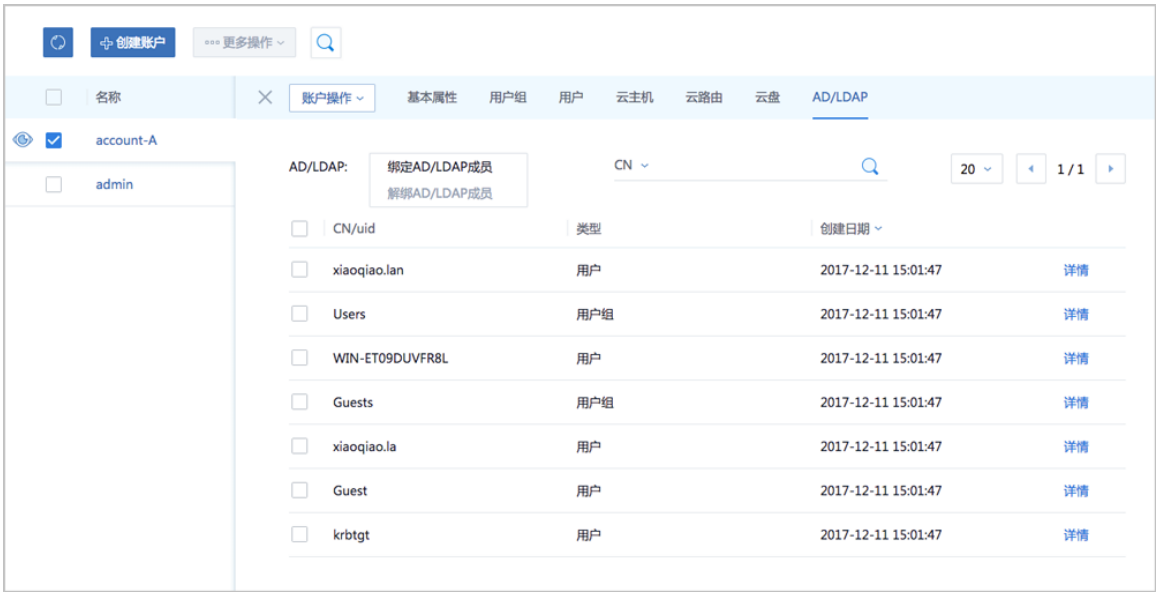


- 目前支持按*CN*、*uid*、高级搜索等条件快速搜索
- 可点击每个AD/LDAP成员的**详情**，查看更多属性

3. 依次点击**确定**按钮，所勾选AD/LDAP成员成功绑定到普通账户。

如图 *748: 普通账户绑定AD/LDAP成员*所示：

图 748: 普通账户绑定AD/LDAP成员



- 目前支持按*CN*、*uid*、高级搜索等条件快速搜索
- 可点击每个AD/LDAP成员的**详情**，查看更多属性
- 如需绑定更多AD/LDAP成员到普通账户，点击**操作** > **绑定AD/LDAP成员**即可。

- 如需将某一AD/LDAP成员从普通账户解绑，勾选该AD/LDAP成员，点击**操作 > 解绑AD/LDAP成员**即可，支持批量操作。

后续操作

至此，ZStack成功绑定AD/LDAP成员。接下来，可使用AD/LDAP成员登录属性直接登录ZStack云平台。

7.10.6.5 AD/LDAP登录

操作步骤

1. 打开AD/LDAP登录界面。

   如图 *749: AD/LDAP登录界面*所示：

   图 749: AD/LDAP登录界面

2. 使用已设置的AD/LDAP成员登录属性直接登录ZStack云平台。

   以AD为例：

   - 若已设置登录属性为*cn*，某一已绑定的AD成员可用*cn*相应的value（例如：名称*xiaoqiao.la*）作为ZStack登录名；
   - 该AD成员在AD域中使用的密码作为ZStack登录密码。

如图 *750: 基于登录属性登录ZStack*所示：

图 750: 基于登录属性登录ZStack

3. AD/LDAP成员成功登录ZStack，所属资源、权限与当前所绑定的ZStack账户一致。

如图 *751: AD/LDAP登录成功*所示：

图 751: AD/LDAP登录成功

至此，ZStack接入AD/LDAP的配置方法介绍完毕。

7.10.7 控制台代理

在ZStack私有云主菜单，点击**平台管理** > **控制台代理**，进入**控制台代理**界面，显示了当前控制台代理的信息，即打开云主机的控制台时使用的代理信息，如图 752: 控制台服务界面所示:

图 752: 控制台服务界面

- 控制台代理地址只需要在管理节点修改。
- 默认代理显示的地址为管理节点的IP地址。
- 显示类型为ManagementServerConsoleProxy。
- 只有当状态为**启用**和**已连接**时，才可正常打开控制台访问云主机。

控制台代理支持的操作：

- **重连**：一般发生在云主机控制台打开失败时，进行重连操作。重连后状态显示为启用和已连接时，代表控制台可以正常打开。
- **设置控制台代理地址**：ZStack支持在UI界面上设置控制台代理地址，无需重启管理节点，直接生效。

7.10.8 证书

目前证书仅用于负载均衡服务，当负载均衡监听器使用HTTPS协议，需绑定证书使用。

- 需提前准备好证书，可使用相关工具生成自签证书，也可购买正规CA签发证书。
- 将准备好的证书上传到云平台，支持上传证书和证书链。
- 负载均衡只支持PEM格式的证书。在上传前，确保证书、私有密钥和证书链符合格式要求。

创建证书

在**私有云**界面，点击**平台管理** > **证书**，进入**证书**管理界面，点击**创建证书**，在弹出的**创建证书**界面，可参考以下示例输入相应内容：

- **名称**：设置证书名称
- **简介**：可选项，可留空不填
- **证书正文**：将准备好的证书内容传入
  - 以-----BEGIN CERTIFICATE-----, -----END CERTIFICATE-----作为开头和结尾
  - 证书内容不能包含空格
  - 证书正文示例：

```
-----BEGIN CERTIFICATE-----
#end-user证书#
-----END CERTIFICATE-----
```

- **私有密钥**：将准备好的私有密钥传入
  - 以-----BEGIN PRIVATE KEY-----, -----END PRIVATE KEY-----作为开头和结尾
  - 私有密钥内容不能包含空格
  - 私有密钥示例：

```
-----BEGIN PRIVATE KEY-----
#私有密钥#
-----END PRIVATE KEY-----
```

- **证书链**：可选项，若有多份证书需要上传，需将root证书、intermediates证书合并在一起上传
  - root证书放在第一位，intermediates证书从第二位开始依次排列，证书之间不能有空行
  - 证书内容不能包含空格
  - 证书链示例：

```
-----BEGIN CERTIFICATE-----
#root证书#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#intermediates证书#
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
#intermediates证书#
-----END CERTIFICATE-----
```

如图 *753:* 创建证书所示：

图 753: 创建证书

证书支持的操作

- 修改名称和简介：修改证书的名称和简介
- 删除：删除证书，若该证书绑定一个或多个监听器，该证书与监听器的绑定关系将一并删除。
- 解绑证书：将已绑定该证书的监听器解绑。

7.11 设置

在ZStack的设置中，主要涉及到以下内容：

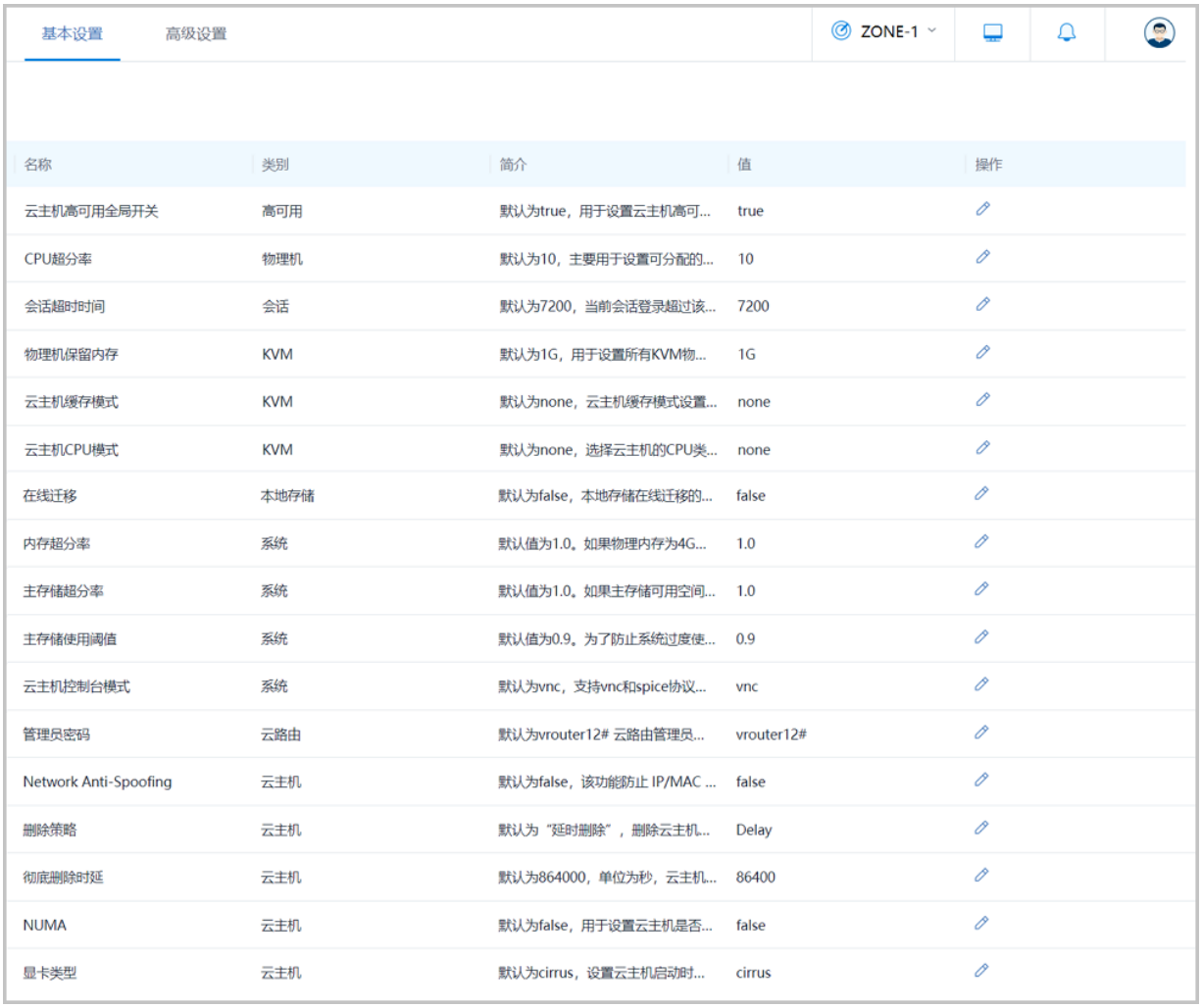
- **全局设置**：管理员可以使用全局配置对很多特性进行配置；所有的全局配置都有一个默认值；更新全局配置并不需要重启管理节点。

- **自定义UI**：用户可以根据自己的需求，自定义UI界面的浏览器标题、首页标题栏、登录页标题、大屏标题、浏览器图标、首页logo和登录页logo等信息。设置或重置成功后，需要手动刷新页面。

7.11.1 全局设置

在ZStack私有云主菜单，点击**设置** > **全局设置**，进入**全局设置**管理界面，如图 *754:* 全局设置所示：

图 754: 全局设置



全局设置包括**基础设置**与**高级设置**。ZStack支持上百种高级设置，用户可根据自身需求搜索并且修改对应的设置。

目前基础设置支持以下选项， 具体介绍如下：

- **云主机高可用全局开关**：

- 可以打开或者关闭云主机高可用功能。默认为：**ture**。
- 如果关闭此选项， 则云主机不支持设置高可用，云主机详情也不会显示高可用信息。
- 如果关闭此选项，将全局禁用高可用功能，请谨慎操作！

- **物理机CPU超分率**：
  - 主要用于设置可分配的虚拟CPU个数。默认为：**10**。
  - 如果物理机的CPU为四核八线程， ZStack会将物理机CPU的总线程（8）乘以处理器超分率的倍数（10）计算可分配的虚拟CPU的个数，即总量为80。
  - 虚拟CPU的总数可以在首页的处理器的总量查看。
- **会话超时时间**：
  - 设定ZStack图形界面登录后会话多长时间失效。默认为：**7200秒**，即2小时。
  - 当登录会话失效后，需要重新登录。
- **KVM物理机保留内存**：
  - 所有KVM主机上保留的内存容量。建议可用单位：T/G/M。默认为：**1G**。
  - 例如：512M表示为系统预留512M内存，当系统剩下700M的内存时，用户又希望启动一个内存为512M的云主机是无法启动的。
- **KVM云主机缓存模式**：
  - 云主机缓存模式设置。可选模式为：writethrough、none,、writeback。默认为：**none**。
    - **writethrough**：物理机的页面缓存工作在透写模式，数据完全写入云主机存储设备后，才返回成功。
    - **none**：云主机不使用物理机的页面缓存，直接访问存储，不带cache。
    - **writeback**：云主机使用了物理机的页面缓存机制，数据写入物理机页面缓存即报告给云主机返回成功。
- **KVM云主机CPU模式**：
  - 选择云主机的CPU类型是否与物理机的CPU类型一致。可选模式为：host-model、none、host-passthrough。默认为：**none**。
    - **host-model**：云主机的CPU类型将与物理机的CPU类型相符，例如都显示为Haswell的Intel CPU。
    - **host-passthrough**：云主机的CPU类型将与物理机的CPU完全一致。

注:

当选择**host-model**或者**host-passthrough**类型时，云主机可以支持嵌套虚拟化，但可能导致云主机在不同型号CPU的物理机之间迁移失败。

- **本地存储在线迁移**：
  - 本地存储在线迁移的全局设置打开或关闭。默认为：**false**。
  - 打开此开关，则支持本地热迁移。
  - 本地存储上Windows的云主机不支持热迁移。
- **系统内存超分率**：
  - 内存超分率允许的范围: [1.00, 1000.00]（1到1000之间的数，如果是小数，最多两位）。默认值为：**1.0**。
  - 如果物理内存为4G，设置为**2.0**，那么ZStack会认为系统可以分配8G内存给云主机使用。
  - 该数值为经验数值，需要根据不同系统和应用的需求进行配置。通常不应设置得过大，否则会影响云主机性能。
  - 在生产环境中，如果用户打算采用物理内存超分，建议在安装系统时，配置相应的swap分区。
    - 例如，如果物理机内存为100G，并打算设置物理内存超分为2，建议设置swap分区也为100G，这样的配置在实际使用中，有足够的swap空间供内存超分使用。
- **系统主存储超分率**：
  - 主存储超分率允许的范围: [1.00, 1000.00]（1到1000之间数，如果是小数，最多两位）。默认值为：**1.0**。
  - 如果主存储可用空间为2T，设置为**2.0**，那么ZStack会认为系统可以分配4T主存储空间给云主机使用。
  - 该数值不应设置得过大，用户需完全理解该设置的含义并设置正确的主存储使用阈值后，才能进行相应的设置。否则会有严重的数据丢失风险！
- **系统主存储使用阈值**：
  - 为了防止系统过度使用主存储空间（尤其是当设置了主存储的超分比例后，过度分配云盘有可能使存储溢出，从而导致云主机存储失效崩溃），需要设置主存储阈值。
  - 主存储使用阈值: (0, 1] 之间的小数，最多四位。默认值为：**0.9**。

    - 例如，阈值为0.9， 如果当前主存储空间实际使用率到达总容量的90%，整个系统将不能新建云主机或者云盘。
    - 此时用户需添加更多的云盘给主存储，并手动重新连接计算节点后，即可进行新建云盘操作。
  - 当使用大于1的主存储超分率后，该阈值应设定为0.6或更小，以确保可及时添加主存储。
  - 用户需完全理解该设置的含义，才能进行相应的设置。否则会有严重的数据丢失风险！
- **系统云主机控制台模式**：
  - 用于设置控制台链接的协议类型。支持vnc和spice协议。默认为：**vnc**。
- **云路由管理员密码**：
  - 登录云路由器的密码。
  - 默认为**vrouter12#**，云路由器管理员账户是：**vyos**。
  - 管理员可以直接在此处设置任意长度字符串，以字母/数字开头, 只能包含数字、字母、 '-'、'_'、'#'。
  - 设定密码后需要通过UI重启云路由器，该密码才会生效。
  - 该操作对所有云路由器生效。
- **云主机Network Anti-Spoofing**：
  - 防**IP/MAC**伪造和ARP欺骗。
  - 默认为：**false**。
- **云主机删除策略**：
  - 该策略设置会设定用户在删除云主机，云盘以及镜像相关内容的删除规则。
  - 可以选择三种策略，立刻删除（Direct），延时删除（Delay）和永不删除（Never）。默认为：**Delay**。
    - **立刻删除**（Direct）：当设置为立刻删除时，如果用户删除云主机或者其他资源，这些相关资源会被立刻删除。
    - **延时删除**（Delay）：当设置为延时删除（默认）时，如果用户删除云主机或者其他资源，这些资源会被标记为**已删除**，显示在对应资源的**已删除**栏，等彻底延时删除时延（默认时延24小时，也就是86400秒）超时后或用户手动强制删除时，才会彻底删除相关资源。
    - **永不删除**（Never）：当设置为永不删除时，当用户删除云主机或者其他资源，这些资源永远不会被系统自动删除。

- **云主机彻底删除时延**：
  - 当删除策略为延时删除时，可以选择延时多久彻底删除资源。
  - ZStack默认时延为**86400秒**，即24小时。
- **云主机NUMA**：
  - 打开NUMA选项可支持在线修改CPU内存。默认为：**false**。
  - 此操作支持CentOS7.2、CentOS6.6、Ubuntu14.04、Ubuntu16.04等云主机操作系统
  - 不建议在生产环境中对Windows云主机执行在线修改CPU、内存的操作。
  - 建议对Windows云主机关机后再修改配置。
- **云主机显卡类型**：
  - 管理员可以进入基础设置页面更改云主机启动时默认的显卡类型。默认为：**cirrus**。
  - 更改后可通过`ps -ef | grep qemu`命令查看`-device`后的显示类型，检查qemu终端设置是否与对应的VM一致。
  - ZStack提供更改以下三种显卡类型：
    - **cirrus**：提供一种简单的显卡类型，但对某些操作系统，无法提供更好的显示支持；`-device cirrus-vga`）
    - **vga**：提供一种更好分辨率的显卡类型；`-device VGA`
    - **qxl**：该显卡类型在SPICE协议下能够表现出更好的性能；`-device qxl-vga`或`virsh dumpxml $domainID`指令查看是否对应，其中`$domainID`指云主机UUID。

注: 该选项改变后， 只针对新创建的云主机和停止后再启动的云主机生效。

7.11.2 自定义UI

背景信息

本章描述了安装ZStack后如何定制化Logo及发行信息。

操作步骤

1. 登录ZStack

   使用Chrome浏览器或FireFox浏览器进入ZStack管理界面（*http://your_machine_ip:5000/*），默认用户名和密码为：*admin/password*。

如图 *755: ZStack*登录界面所示：

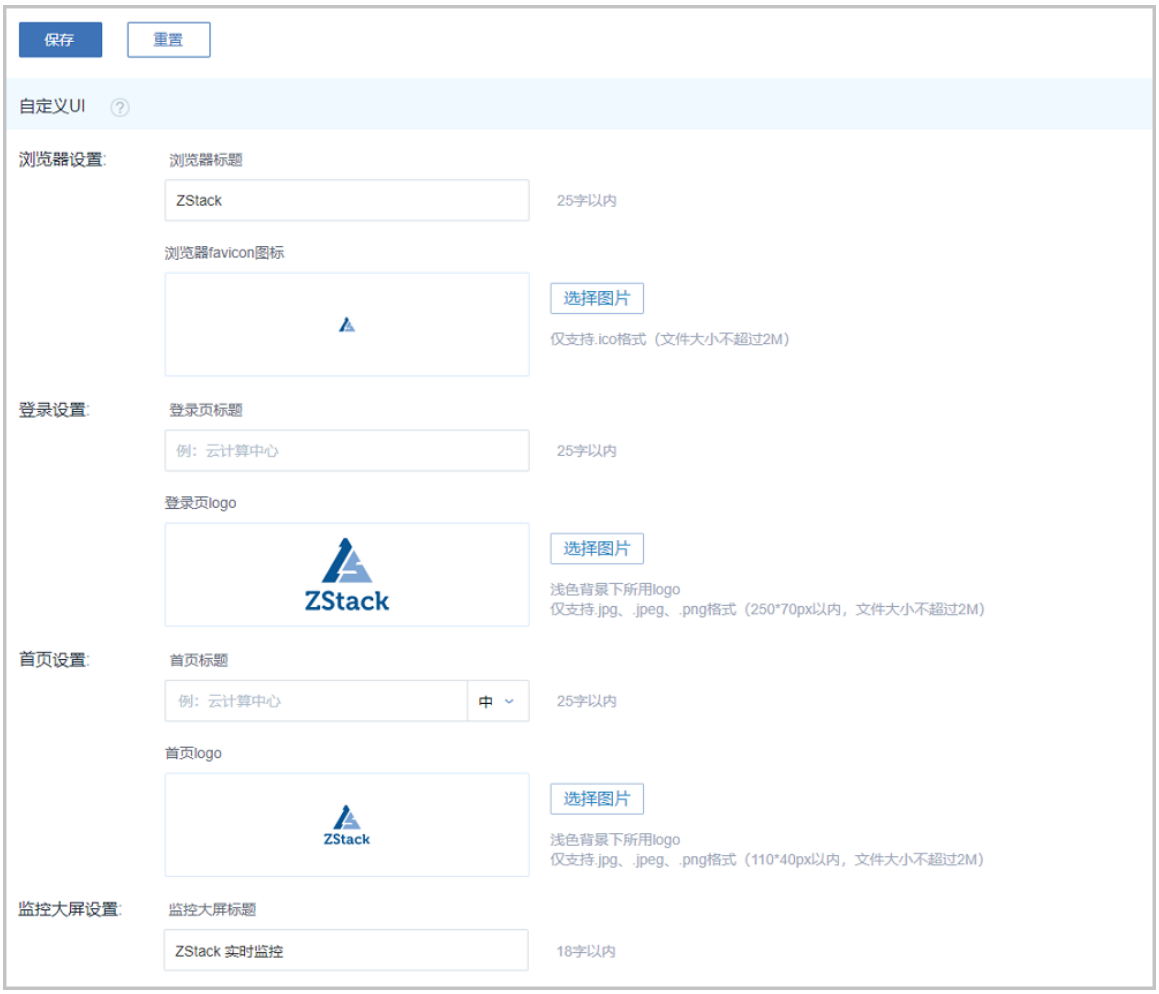
图 755: ZStack登录界面

2. 进入**自定义UI**设置界面。

   在ZStack私有云主菜单，点击**设置** > **自定义UI**，进入**自定义UI**设置界面。

   如图 *756:* 自定义*UI*设置界面所示：

   图 756: 自定义UI设置界面



3. 在**自定义UI**设置界面，可参考以下示例输入相应内容：

- **浏览器设置**：
  - **浏览器标题**：自定义浏览器标题，25字以内。例如：ZStack
  - **浏览器favicon图标**：点击右侧**选择图片**按钮，本地上传即可

    注: 自定义浏览器favicon图标需满足以下要求：
    - 仅支持ico格式
    - 文件大小不超过2M
- **登录设置**：
  - **登录页标题**：自定义登录页标题，25字以内。例如：云计算中心
  - **登录页logo**：点击右侧**选择图片**按钮，本地上传即可

    注: 自定义登录页logo图片需满足以下要求：
    - 浅色背景下所用logo

- 仅支持JPG、JPEG、PNG格式
- 像素在250*70px以内，文件大小不超过2M

- **首页设置**：
  - **首页标题**：自定义首页标题，25字以内。例如：云计算中心
  - **首页logo**：点击右侧**选择图片**按钮，本地上传即可

注: 自定义首页logo图片需满足以下要求：

- 深色背景下所用logo
- 仅支持JPG、JPEG、PNG格式
- 像素在110*40px以内，文件大小不超过2M

- **监控大屏设置**：
  - **监控大屏标题**：自定义监控大屏标题，18字以内。例如：ZStack 实时监控

4. 点击**保存**按钮，手动刷新页面，UI界面的相关logo及发行信息将更换为定制化版本。

注:

- 点击**保存**按钮后，必须手动刷新页面才显示更换效果。
- 已上传的定制化logo图片及发行信息存储在*/var/lib/zstack/static*路径下，其中发行信息以json文件形式保存。

5. 点击**重置**按钮，可一键清除当前定制化设置，重新恢复为默认设置。

注:

- 点击**重置**按钮后，必须手动刷新页面才显示还原效果。
- 点击**重置**后，存储在*/var/lib/zstack/static*路径下的定制化logo图片及发行信息将被删除。

至此，定制化logo及发行信息方法介绍完毕。

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。