运维手册

产品版本：ZStack 3.1.1

文档版本：V3.1.1

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 10
3 系统架构 30
3.1 ZStack功能架构 30
3.2 ZStack资源结构 32
4 网络配置 36
5 安装部署 40
5.1 环境准备 40
5.1.1 网卡归一化(可选) 53
5.2 安装ZStack 64
5.2.1 ZStack管理节点模式(企业版/社区版) 66
5.2.2 ZStack计算节点模式 101
5.2.3 ZStack专家模式 102
5.3 管理ZStack 103
5.4 升级ZStack 104
5.4.1 c72版 升级 107
5.4.2 c74版 升级 111
6 系统登录 116
6.1 HTTPS方式登录UI 116
7 Wizard引导设置 119
8 首页 124
8.1 大屏监控 124
8.2 关于 126
9 云资源池 133
9.1 云主机 133
9.2 云盘 145
9.3 镜像 149
9.4 亲和组 153
9.5 计算规格 156
9.6 云盘规格 158
9.7 弹性伸缩组 158
10 硬件资源 163
10.1 区域 163
10.2 集群 164
10.3 物理机 168
10.3.1 GPU设备透传 171
10.3.2 USB设备透传 172
10.4 主存储 173
10.4.1 本地存储 175
10.4.2 NFS 176
10.4.3 Shared Mount Point 177
10.4.4 Ceph 178

10.4.5 Shared Block....179
10.5 镜像服务器....179
10.6 SAN存储....182
11 网络资源....184
11.1 网络拓扑....184
11.2 二层网络资源....186
11.2.1 VXLAN Pool....186
11.2.2 二层网络....187
11.3 三层网络....189
11.4 扁平网络....190
11.5 云路由网络....192
11.6 VPC....196
11.6.1 VPC路由器....198
11.6.2 VPC网络....199
12 网络服务....202
12.1 安全组....204
12.2 虚拟IP....206
12.3 弹性IP....209
12.4 端口转发....210
12.5 负载均衡....212
12.6 IPsec隧道....214
13 vCenter....217
13.1 基础资源....217
13.2 云主机....218
13.3 网络....220
13.4 网络服务....221
13.4.1 虚拟IP(ESX类型)....222
13.4.2 弹性IP....223
13.4.3 端口转发....224
13.4.4 负载均衡....224
13.4.5 IPsec隧道....226
13.5 云盘....226
13.6 镜像....227
14 平台运维....229
14.1 性能TOP5....229
14.2 性能分析....230
14.3 ZWatch....230
14.4 通知服务....232
14.5 消息中心....233
14.6 操作日志....233
14.7 资源编排....234
14.7.1 资源栈....235
14.7.2 资源栈模板....236
14.7.3 资源栈示例模板....236
15 平台管理....237
15.1 用户管理....237
15.2 计费管理....239
15.3 定时....239
15.3.1 定时器....239

15.3.2 定时任务 240
15.4 应用中心 240
15.5 邮箱服务器 240
15.6 AD/LDAP 241
15.7 控制台代理 242
15.8 证书 243
16 高级功能(Plus) 244
16.1 企业管理 244
16.1.1 平台管理员 249
16.1.2 组织架构 249
16.1.3 项目管理 252
16.1.4 工单管理 254
16.2 裸金属管理 255
16.2.1 裸金属集群 256
16.2.2 部署服务器 257
16.2.3 裸金属设备 258
16.2.4 裸金属主机 259
16.3 灾备服务 260
16.3.1 备份任务 265
16.3.2 本地备份数据 266
16.3.3 本地备份服务器 266
16.3.4 远端备份服务器 268
16.4 迁移服务 269
16.4.1 V2V迁移 269
16.4.2 迁移服务器 271
17 设置 272
17.1 全局设置 272
17.1.1 基础设置 272
17.1.2 高级设置 276
18 管理节点高可用 292
18.1 管理节点云主机高可用 292
18.2 多管理节点物理机高可用 292
19 基本运维 295
19.1 安装部署 295
19.2 启动服务 297
19.3 zstack-ctl命令 298
19.4 zstack-cli命令 299
19.5 重连物理主机 300
19.6 重连主存储 300
19.7 重连镜像服务器 301
19.8 云主机异常 301
19.9 日志分析 308
19.10 端口占用 309
19.11 网络脚本 311
19.12 机房维护步骤 314
20 其他配置运维 316
20.1 安装多个管理节点 316
20.2 配置独立的MySQL服务器 317
20.3 zstack.properties核心配置文件 318

20.4 zstack.ui.properties核心配置文件 320
20.5 云平台硬件资源密码变更 321
20.6 管理节点更改物理环境 322
20.7 数据库备份与恢复 322
20.8 管理节点灾难恢复 322
20.8.1 准备工作 323
20.8.2 管理节点灾难恢复 323
20.9 本地存储空间扩容 325
20.10 云主机根云盘扩容 325
21 常见问题 332
21.1 快速入门 332
21.2 安装部署 334
21.3 系统登录 342
21.4 云资源池 345
21.5 硬件设施 365
21.6 网络 376
21.7 vCenter 380
21.8 平台管理运维 382
21.9 高级功能 383
术语表 384

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 3.1.0

读者对象

本文档详述了ZStack企业版 3.1.0在安装部署使用过程中需要注意的事项，以及管理运维过程中的常见问题解决方案。本文档主要适用于以下读者：

- 部署运维工程师
- 技术支持工程师
- 对ZStack有兴趣研究的相关人员

版本更新

3.1.1

2018/11/23主要更新：

1. 裸金属服务增强：独立部署PXE服务器
2. 更细粒度展示Ceph存储容量
3. 修复已知问题，提升系统稳定性

3.1.0

2018/11/15主要更新：

1. 扁平网络新增支持IPv6/双栈协议
2. V2V迁移服务增强
   - 主流Linux/Windows操作系统全覆盖
   - UEFI云主机迁移
3. 云主机弹性伸缩
4. FC-SAN透传
5. Shared Block主存储增强：支持精简置备
6. 裸金属服务增强：UI批量添加裸金属设备
7. 大屏展示VMware资源
8. ZWatch监控报警增强

- 单个报警器批量添加资源
- 提供多种系统默认报警模板

9. 灾备服务增强

- 备份任务支持网络QoS和磁盘QoS
- 本地备份服务器指定数据网络

10.云盘QoS增强：对云盘读和写分别设置QoS

11.UI批量添加计算节点

12.一键恢复默认全局设置

13.单个云主机启用/停用防欺诈模式

14.自定义启用/停用安全组

15.优化许可证上传用户体验

- 许可证合并上传
- 多管理节点物理机高可用支持UI上传许可证

16.其它功能和优化

- 基于快照恢复的云主机支持自动启动
- SSH密码登录路由器支持全局启用/禁用
- 物理机密码在数据库中加密存储支持全局启用/禁用
- 普通账户/企业管理账号体系不允许自由修改云盘/网卡QoS
- 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：功能模块菜单合并等
- 优化部分业务逻辑

3.0.1

2018/09/30主要更新：

1. V2V迁移服务

2. 修复已知问题，提升系统稳定性

3.0.0

2018/09/17主要更新：

1. 整机备份/还原
2. VMware多租户管理增强
3. 云平台数据库可视化灾备
4. 工单自定义流程审批
5. 虚拟CPU与物理CPU绑定
6. Shared Block主存储支持iSCSI自动登录
7. 负载均衡监听器新增支持UDP协议
8. 镜像仓库垃圾文件清理
9. VM高可用恢复过程UI界面展示
10. 其它功能和优化

2.6.2

2018/08/27主要更新：

1. 登录验证码支持开启/关闭
2. 修复已知问题，提升系统稳定性

2.6.0

2018/08/09主要更新：

1. 云灾备
2. 可视化资源编排
3. VMware多租户管理和工单审批
4. 裸金属服务
5. 主存储支持阿里云盘古NAS
6. 全新双管理节点高可用功能
7. 双因子认证
8. 定时创建快照指定最大数量
9. Shared Block主存储功能增强
10. 其它功能和优化

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

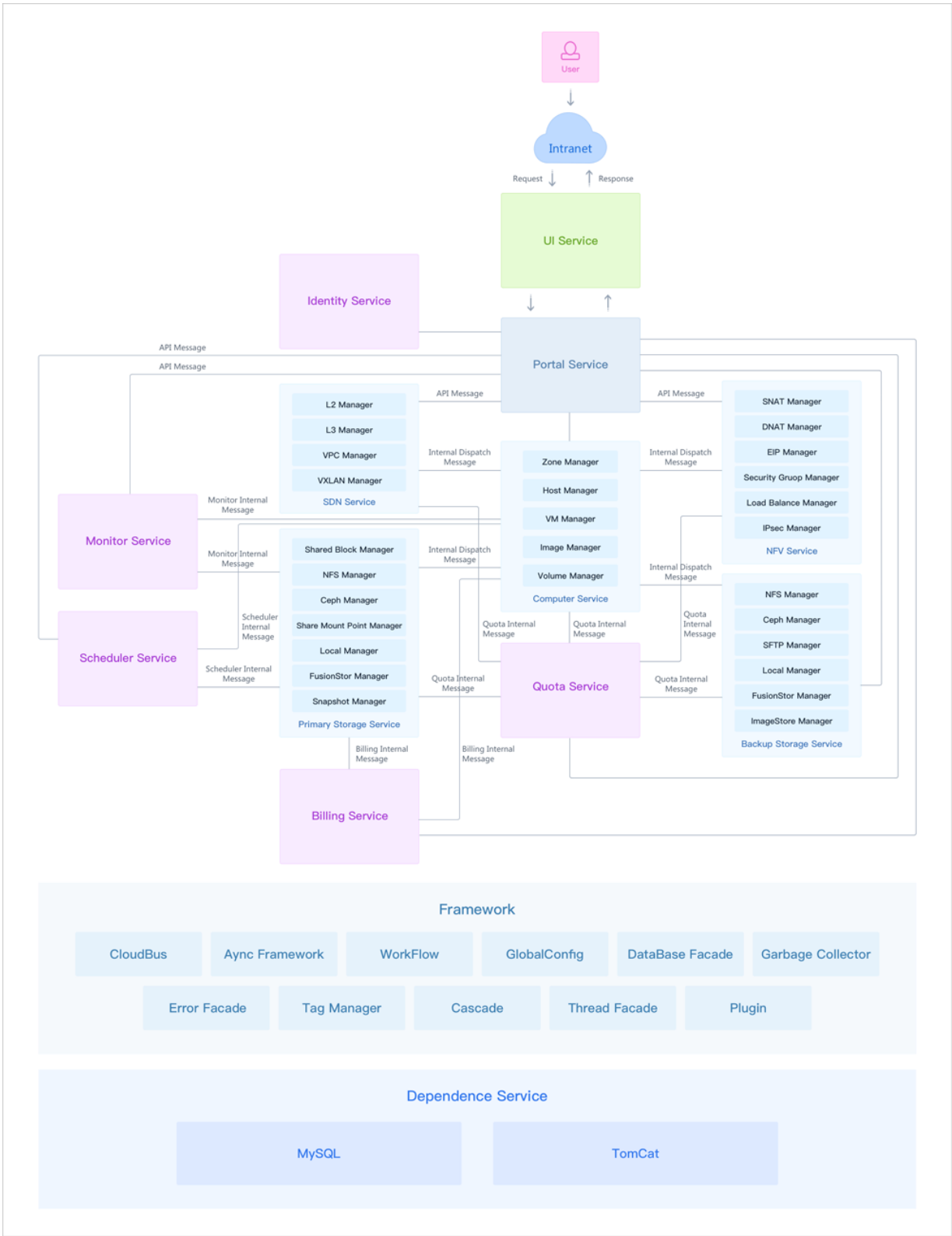
11.优化部分业务逻辑

2 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（软件即服务）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
	vCenter多租户管理	• 普通账户/项目负责人/项目管理员/项目成员可对vCenter云主机或云盘进行相关操作 • 普通账户/项目负责人/项目管理员/项目成员可使用admin共享的vCenter网络或镜像 • 支持在普通账户/项目负责人/项目管理员/项目成员视角的首页分别展示KVM和vCenter云主机的使用量 • 支持在普通账户/项目负责人/项目管理员/项目成员视角分别展示KVM和vCenter账单详情 • 普通账户/项目负责人/项目管理员/项目成员支持使用虚拟IP、弹性IP、端口转发和负载均衡 • 工单审批支持申请vCenter云主机
	ESX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

类别	特性	ZStack企业版
	云盘	支持云盘的创建、删除、加载、卸载
	实时性能监控	采集ESX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
	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，提升平台稳定性 • 支持灾备模块，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）
	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

类别	特性	ZStack企业版
	密码加密存放	支持物理机密码加密存放
	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
	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类型的镜像服务器） • 关机快照（支持ImageStore/Sftp/Ceph类型的镜像服务器） • 支持恢复快照后自动启动云主机
	云盘在线快照	在使用云盘的过程中进行快照
	CPU绑定	将云主机的逻辑CPU与计算节点的物理CPU绑定
	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）

类别	特性	ZStack企业版
	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
	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
	BIOS模式	• 创建云主机会继承所选镜像的BIOS模式，包括Legacy和UEFI • 创建云主机镜像、克隆云主机操作，将继承原镜像BIOS模式 • 云主机详情页支持动态修改BIOS模式
	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

类别	特性	ZStack企业版
	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，支持UI上展示恢复过程
	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
	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 • 默认禁用vyos ssh认证方式登录，提升安全性
	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
	防欺诈模式	• 全局设置云主机防欺诈模式，提升安全性 • 为单个云主机单独设置防欺诈模式开关，提升灵活度
弹性伸缩组	生命周期	支持弹性伸缩组的创建、启动、停止、删除

类别	特性	ZStack企业版
	健康检查	支持自定义健康检查方式、健康检查时间、健康检查宽限时间
	弹性伸缩策略	• 支持自定义触发条目、触发条件、持续时间、冷却时间、每次增加数量的扩容策略 • 支持自定义触发条目、触发条件、持续时间、冷却时间、云主机移除策略、每次减少数量的缩容策略 • 触发伸缩条件后，根据所设定的策略自动增加或减少云主机数量 • 支持对CPU使用率、内存使用率进行监控
	消息通知	• 支持查看伸缩记录 • 支持选择是否接收弹性伸缩活动的消息通知 • 支持通过ZWatch和站内信的形式发送消息通知
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
	设置QoS	创建云盘规格时，通过设置总带宽或读写带宽的方式，为云盘设置QoS
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
	BIOS模式	• 添加镜像支持Legacy、UEFI两种BIOS模式 • 创建云主机、创建云主机镜像、克隆云主机操作，将继承原镜像BIOS模式
	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
	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

类别	特性	ZStack企业版
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
	获取已有镜像	添加ImageStore类型的镜像服务器时，可获取该镜像服务器中URL路径下的已有镜像文件
	镜像同步	支持镜像仓库间的镜像互传，可以跨区域使用
	镜像仓库清理	支持清理镜像服务器中已被彻底删除的无效数据，释放存储空间
	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、阿里云NAS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

类别	特性	ZStack企业版
		• 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
	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iSCSI服务器，支持自动在线扫描并发现磁盘和自动配置iSCSI发起等操作 • 支持共享云盘 • 支持添加多个LUN • 添加Shared Block主存储时，支持显示共享块设备候选列表 • 使用Shared Block主存储创建云主机或云盘，支持设置置备方式，包括精简置备或厚置备 • 支持FC-SAN透传，直观的展示透传的FC存储，并可将透传的块设备加载到云主机 • 添加Shared Block主存储时，支持清理VG数据 • 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
	NAS存储	• 支持云盘存放到POSIX兼容的分布式网络文件存储 • 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 • 支持清理块设备，可强制清理块设备中的文件系统、RAID或分区表中的签名 • 支持实时查看主存储已用容量百分比趋势图

类别	特性	ZStack企业版
	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 • 支持添加IPv4、IPv6类型的网络
	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
	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、加载/卸载VPC路由器、删除 • VPC网络支持以下网络服务：安全组、虚拟IP、弹性IP、端口转发、负载均衡 • 负载均衡支持TCP/HTTP/HTTPS/UDP协议
	公有网络	• 支持创建云主机 • 支持为网络服务提供虚拟IP • 支持添加IPv4、IPv6类型的网络
	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	• 云路由支持以下网络服务：安全组、虚拟IP、弹性IP、端口转发、负载均衡 • 负载均衡支持TCP/HTTP/HTTPS/UDP协议 • 支持基于云路由的IPsec隧道服务

类别	特性	ZStack企业版
		• 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 • 创建云主机/云盘快照定时任务时，如果选择的所有云主机/云盘都使用Ceph主存储，支持设置保留快照数量
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
	可视化资源编排	• 支持可视化拖拽资源方式创建资源栈模板 • 支持预览模板、生成资源栈、另存为资源栈模板 • 支持撤销、恢复、删除、清空画布操作
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 • 支持启用、停用安全组
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

类别	特性	ZStack企业版
		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 • 提供常用默认报警器，实时监控基础资源状态 • 按需选择监控范围，支持对监控对象的单个资源或全部资源进行监控
	多接收端	支持邮件/钉钉/HTTP应用等多种接收端
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

类别	特性	ZStack企业版
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，支持一键恢复默认配置 • 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
	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

类别	特性	ZStack企业版
	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 • 支持动态验证码验证。多次登陆（6次）失败触发验证码验证，防止恶意登陆 • 支持双因子认证。额外增加安全码身份验证，进一步增强账号安全
	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	• 华丽大屏展示平台资源情况 • 支持切换虚拟化，分别展示KVM或vCenter大屏 • 支持切换区域，展示全部区域或某个区域的大屏
	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

类别	特性	ZStack企业版
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 • 支持本地浏览器上传License • 支持License到期提醒 • 企业单机无限期试用版支持所有功能
	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、裸金属管理模块、灾备服务模块 • 支持本地浏览器上传License • License到期提醒
	上传许可证	根据需求自由打包许可证，统一上传
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
	双物理机管理节点高可用	• 支持双物理机管理节点高可用。采用主备方案，某个管理节点故障后能迅速切换到另一个管理节点，保证业务正常运行 • 通过VIP登录管理节点，支持分别为两个管理节点添加许可证
计算节点	批量添加物理机	• 可根据填写的网络段批量添加物理机 • 支持通过模板导入方式批量添加物理机
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

类别	特性	企业管理模块
		• 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 • 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
	设置QoS	• admin/平台管理员可以对云主机、云盘、网卡设置QoS • 磁盘QoS可通过设置总带宽或读写带宽的方式进行设置

类别	特性	企业管理模块
		• 控制QoS设置范围，普通账户/项目负责人/项目管理员/项目成员修改QoS上限不能超过admin/平台管理员设置的值
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	• 支持默认流程审批和自定义流程审批 • 默认流程审批：项目成员提交工单申请，admin可进行一键审批，审批通过后，资源可自动部署成功并分发到项目中 • 自定义流程审批：项目成员提交工单申请，按自定义工单流程经由各级审批人进行审批，最终由admin进行一键审批，审批通过后，资源可自动部署成功并分发到项目中 • 支持admin通过并部署工单以及驳回工单 • 支持项目负责人/项目管理员通过工单、驳回工单
	自定义流程管理	• 支持admin对不同项目设置各自的自定义工单流程 • admin创建自定义工单流程过程中，支持将项目成员/项目管理员/项目负责人添加到各审批环节 • 支持admin启用、停用、修改、删除自定义工单流程
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

ZStack裸金属管理模块功能列表：

类别	特性	裸金属管理模块
裸金属管理	裸金属集群	• 通过创建裸金属集群，管理物理裸机 • 支持为裸金属集群加载二层网络
	部署服务器	• 通过部署服务器自动化对新上线裸金属设备进行系统安装部署

类别	特性	裸金属管理模块
		• 支持独立部署PXE服务器
	裸金属设备	• 通过IPMI网络批量部署裸金属设备 • 支持对裸机进行远程电源管理 • 支持VNC无人值守模式 • 可根据填写的网络段批量添加裸金属设备 • 支持通过模板导入方式批量添加裸金属设备
	裸金属主机	• 支持使用ISO类型镜像为裸金属设备安装Linux操作系统 • 支持为裸金属主机添加网络配置

ZStack灾备服务模块功能列表：

类别	特性	灾备服务模块
灾备服务	备份	• 支持为云主机、云盘和管理节点数据库创建备份任务 • 支持云主机的整机备份 • 支持用户按周/天/小时为任务设置备份策略 • 支持将数据备份在本地备份服务器并同步到远端备份服务器 • 支持查看云主机、云盘和数据库的本地备份数据/远端备份数据 • 支持删除本地备份数据/远端备份数据 • 可直接使用本地数据中心已部署的镜像仓库作为本地备份服务器，也可部署新的本地备份服务器 • 当备份任务指定多个本地备份服务器时，支持主备无缝切 • 仅允许添加一个远端备份服务器，包括异地和阿里云两种类型 • 备份数据仅可从本地备份服务器同步至远端备份服务器 • 清理本地备份服务器/远端备份服务器中已被彻底删除的无效备份数据，释放存储空间 • 备份任务支持设置磁盘QoS和网络QoS
	还原	• 从本地云主机/云盘的本地/远端备份数据还原资源时，支持新建资源以及覆盖原始资源 • 支持云主机的整机还原 • 本地云主机/云盘的远端备份数据需先同步至本地备份服务器，才可还原至本地，数据库的远端备份数据直接还原至本地

类别	特性	灾备服务模块
		• 在本地有数据的情况下（Zone存在），可通过数据库的本地/远端备份数据一键还原数据中心 • 在本地无数据的情况下（Zone不存在），可通过数据库的本地/远端备份数据以Wizard引导界面的方式还原数据中心 • 支持将数据库的本地/远端备份数据导出进行手动还原

ZStack迁移服务模块功能列表：

类别	特性	迁移服务模块
迁移服务	V2V迁移	• 将已接管的vCenter云主机迁移至ZStack云平台 • 支持对云主机进行一键式批量的V2V迁移 • 创建迁移任务过程中，支持对目标云主机进行自定义配置 • 支持设置迁移网络，并设置QoS • 支持取消、重新启动迁移任务 • 支持迁移的源vCenter平台版本包括：5.5、6.0、6.5、6.7 • 支持多种操作系统的云主机进行V2V迁移，包括：RHEL/CentOS 5.x/6.x/7.x、Windows 7/2003/2008/2012/2016

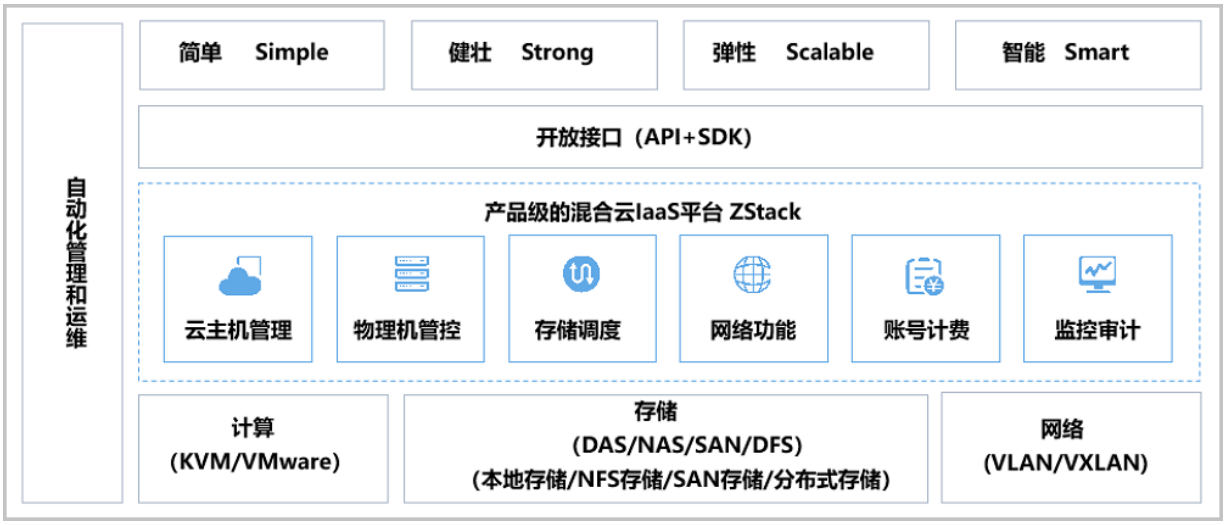
3 系统架构

ZStack作为新一代产品级私有云管理平台，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各种资源。

3.1 ZStack功能架构

ZStack功能架构如图 2: ZStack功能架构所示：

图 2: ZStack功能架构



ZStack提供了对企业数据中心基础设施的计算、存储、网络等资源的管理，底层支持KVM和VMware虚拟化技术，支持DAS/NAS/SAN/DFS等存储类型，支持本地存储、NFS存储、SAN存储、分布式块存储，支持VLAN/VXLAN等网络模型。

ZStack的核心云引擎，使用消息总线同数据库MariaDB及各服务模块进行通信，提供了云主机管理、物理主机管控、存储调度、网络功能、账号计费、实时监控等功能。ZStack还提供了Java和Python的SDK，且支持RESTful APIs进行资源调度管理。基于ZStack打造的专有云管理平台充分体现专有云的4S优势，即：简单Simple、健壮Strong、弹性Scalable、智能Smart。

ZStack核心架构设计特点：

1. **全异步架构**：异步消息、异步方法、异步HTTP调用。
   - ZStack使用消息总线进行各服务的通信连接，在调用服务时，源服务发消息给目的服务，并注册一个回调函数，然后立即返回；一旦目的服务完成任务，就会触发回调函数回复任务结果。异步消息可以并行处理。

- ZStack服务之间采用异步消息进行通信，对于服务内部，一系列相关组件或插件，也是通过异步方法来调用，调用方法与异步消息一致。
- ZStack采用的插件机制，给每个插件设置相应的代理程序。ZStack为每个请求设置了回调URL在HTTP的包头，任务结束后，代理程序会发送应答给调用者的URL。
- 基于异步消息、异步方法、异步HTTP调用这三种方式，ZStack构建了一个分层架构，保证了所有组件均能实现异步操作。
- 基于全异步架构机制，单管理节点的ZStack每秒可并发处理上万条API请求，还可同时管理上万台服务器和数十万台云主机。

2. **无状态服务**：单次请求不依赖其他请求。

- ZStack的计算节点代理、存储代理、网络服务、控制台代理服务、配置服务等，均不依赖其他请求，一次请求可包含所有信息，相关节点无须维护存储任何信息。
- ZStack使用一致性哈希环对管理节点、计算节点或者其他资源以UUID为唯一ID进行认证的哈希环处理，消息发送者无需知道待处理消息的服务实例，服务也无须维护、交换相关的资源信息，服务只需单纯的处理消息即可。
- ZStack管理节点间共享的信息非常少，两个管理节点即可满足高可用性和可扩展性需求。
- 无状态服务机制让系统更为健壮，重启服务器不会丢失任何状态信息，数据中心的弹性扩展和伸缩性维护更为简单。

3. **无锁架构**：一致性哈希算法。

- 一致性哈希算法保证了同一资源的所有消息均被同一个服务实例来处理。这种聚合消息到特定节点的方法，降低了同步与并行的复杂度。
- ZStack使用工作队列来避免竞争锁的问题，串行任务以工作队列的方式保存在内存中，工作队列可对任意资源的任意操作进行并行处理来提高系统并行度。
- ZStack基于队列的无锁架构，使得任务可以简单地控制并行度，从而提升系统性能。

4. **进程内微服务**：微服务解耦。

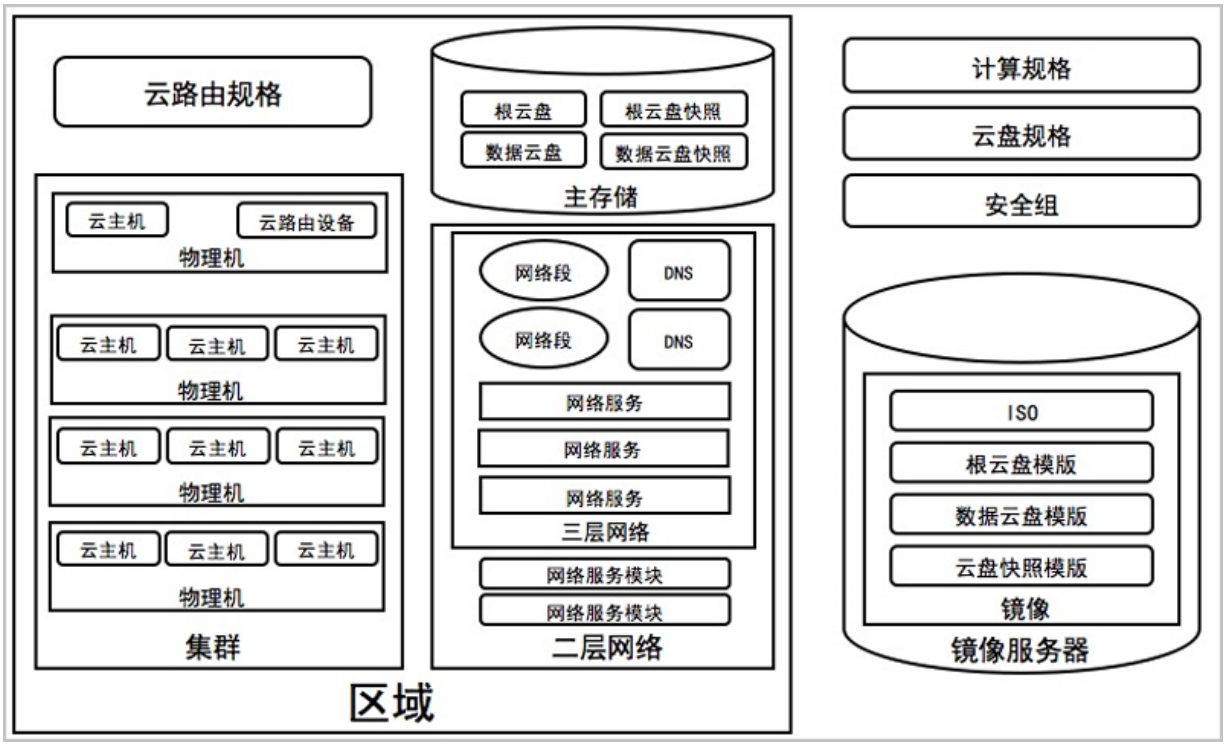
- ZStack使用消息总线对各服务进行隔离控制，例如，云主机服务、身份认证服务、快照服务、云盘服务、网络服务、存储服务等。所有的微服务都集合在管理节点的进程内，各服务之间利用消息总线进行交互，所有消息发送到消息总线后，再通过一致性哈希环选择目的服务进行转发处理。
- 进程内微服务，以星状架构实现各服务独立运行，将高度集中的控制业务进行解耦，实现了系统的高度自治和高度隔离，任何服务出现故障并不影响其他组件。可靠性与稳定性得到有效保障。

5. **全插件结构**：插件支持横向扩展。
   - ZStack使用中任何新加入的插件对目前其他的插件没有任何影响， 均是独立自主提供服务。
   - ZStack支持策略模式和观察者模式进行插件设计。策略插件会继承父类的接口然后执行具体实现；观察者插件，会注册listener进行监控内部的业务逻辑的事件变化，当应用内部发现事件时，插件会对此事件做出自响应，在插件自身的代码里执行相应的业务流。
   - ZStack支持插件的横向扩展，云平台可以快速更迭，而整体系统架构依然健壮。
6. **工作流引擎**：顺序管理，出错回滚。
   - ZStack工作流基于XML对每个工作流程进行清晰定义，在任何步骤出现错误均可按照原本执行路径进行回滚，清理掉执行过程的垃圾资源。
   - 每个工作流还可以包含子工作流用于扩展业务逻辑。
7. **标签系统**：支持业务逻辑变更，增加资源属性。
   - ZStack支持利用系统标签和插件机制对原本的业务逻辑进行扩展变更。
   - 使用标签机制，可对资源进行分组划分，支持对指定标签进行资源搜索。
8. **瀑布流架构**：支持资源的级联操作。
   - ZStack使用Cascade Framework对资源管理进行瀑布状的级联操作，对资源进行卸载或者删除时，会对相关的资源进行级联操作。
   - 资源也可以通过插件形式加入到瀑布框架中，加入或者退出瀑布框架，并不影响其他资源。
   - 级联机制使得ZStack的配置灵活轻便，快速满足客户资源配置的变更。
9. **全自动化Ansible部署**：Ansible无代理自动部署。
   - ZStack使用Ansible进行无代理的全自动化安装依赖、配置物理资源，部署代理程序，全过程对用户透明，无须额外干预，可透过重连代理程序对代理进行升级。
10. **全API查询**：任意资源的任意属性均可查询。
   - ZStack支持数百万个条件的资源查询，支持全API查询，支持任意组合。

3.2 ZStack资源结构

ZStack在本质上是云资源的配置管理系统。ZStack管理的相关资源在结构上如*图 3: ZStack资源结构*所示：

图 3: ZStack资源结构



ZStack主要包括以下资源：

- 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。
- 集群：一组物理主机（计算节点）的逻辑集合。
- 物理主机：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。
- 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。支持本地存储、NFS、Shared Mount Point、Shared Block、Ceph类型。
- 镜像服务器：用于保存镜像模板的存储服务器，支持镜像仓库、Sftp、Ceph类型。
- VXLAN Pool：VXLAN网络中的Underlay网络，一个 VXLAN Pool可以创建多个VXLAN Overlay网络，这些Overlay网络运行在同一组Underlay网络设施上。
- 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。支持 L2NoVLANNetwork、L2VLANNetwork、VXLANNetwork类型。
- 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。
- 计算规格：云主机的CPU、内存、磁盘带宽、网络带宽的数量或大小规格定义。
- 云盘规格：云主机使用的云盘的大小规格定义。
- 云主机：运行在物理主机上的虚拟机实例，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。

- 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，其中系统云盘镜像支持ISO和Image类型， 数据云盘镜像支持Image类型。
- 根云盘：安装云主机操作系统的磁盘，用于支撑云主机的系统运行。
- 数据云盘：为云主机提供了额外的存储空间，用于云主机的存储扩展。
- 快照：采用增量机制对云盘在特定时间点上的数据进行备份。
- 网络服务模块：用于提供网络服务的模块。在UI界面已隐藏。
- 网络服务：给云主机提供的各种网络服务，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。
- 安全组：给云主机提供三层网络防火墙控制。
- 云路由规格：指定云路由器使用的CPU、内存、云路由镜像、管理网络、公有网络等资源定义。
- 云路由器：为云主机提供分布式DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等各种网络服务的定制云主机。
- VPC路由器：基于云路由规格直接创建的路由器，拥有公有网络和管理网络，是VPC的核心。公有网络作为默认网络，用于提供各种网络服务，包括：DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等。

ZStack资源间存在以下关系：

- 父子关系：一个资源可以是另一个资源的父亲或孩子。例如集群和物理主机，物理主机和云主机。
- 兄弟关系：拥有同样父资源的资源为兄弟关系。例如集群和二层网络，集群和主存储。
- 祖先和后裔关系：一个资源可以是另一个资源的直系祖先或者直系后裔。例如集群和云主机，区域和物理主机。
- 朋友关系：一些资源与资源之间没有以上三种关系，但是这些资源在某些情境下需要分工合作，这时它们是朋友关系。例如主存储和镜像服务器，区域和镜像服务器。

注: 主存储和镜像服务器的关系为：

- 创建VM时，主存储会从镜像服务器下载复制云主机的镜像模板文件作为缓存 。
- 创建镜像时，主存储会将根云盘拷贝到镜像服务器保存为模板 。

ZStack资源均含有以下基本属性：

- UUID：通用唯一识别码UUIDv4（Universally Unique Identifier）来唯一标识一个资源。
- 名称：用于标记资源的可读字符串，名称可以重复，一般为必选项。
- 描述：也称之为简介，用于概述资源，可选项。

- 创建日期：资源创建的日期。
- 上次操作日期：资源上次被更新的时间。

ZStack资源一般都支持CRUD操作：

- 创建：创建或者添加新的资源。
- 查询：读取查询资源信息。
- 更新：更新资源信息。
- 删除：删除资源，ZStack使用的瀑布框架级联机制，使得父资源被删除后，相关子资源和后裔资源均会被删除。

4 网络配置

ZStack支持复杂的网络场景，根据业务需求和实际环境，下面列出了几种常见的网络架构：

1. 本地存储+扁平网络架构

其架构如图 *4: 本地存储 +扁平网络*所示，此架构支持以下特性：

- 物理主机使用本地存储来存储云主机的系统盘和数据盘。
- 云主机数据保护需要依赖物理主机的RAID阵列技术。
- 物理主机和云主机在同一个二层网络，云主机IP可与物理主机IP互通。
- 支持分布式DHCP、分布式弹性IP、Userdata服务。
- 云主机在线迁移受限。
- 成本低廉，并发性能高，适用于软件开发测试环境、应用层可提供高可用的场景。

图 4: 本地存储 +扁平网络

管理网络：

- 负责管理各计算节点及存储节点资源的网络。
- 图示的em01即为管理节点使用的网卡，是管理节点用于和计算节点及镜像服务器通信的网络。

数据网络：

- 给云主机使用的网络。
- 图示的em02即为创建云主机使用的网络，云主机的网络如果设置与物理主机同一网段，就可以与物理主机互通，IP互通时，注意IP段不可重叠。
- 可以设置VLAN或VXLAN进行二层隔离，网络隔离后，云主机只能在私网内使用，无法直接访问外部网络，需要使用弹性IP机制来实现网络互通。

镜像服务器：

- 镜像服务器可以使用单独的服务器提供服务。
- 在小型的数据中心，也可与管理节点使用同一台机器。

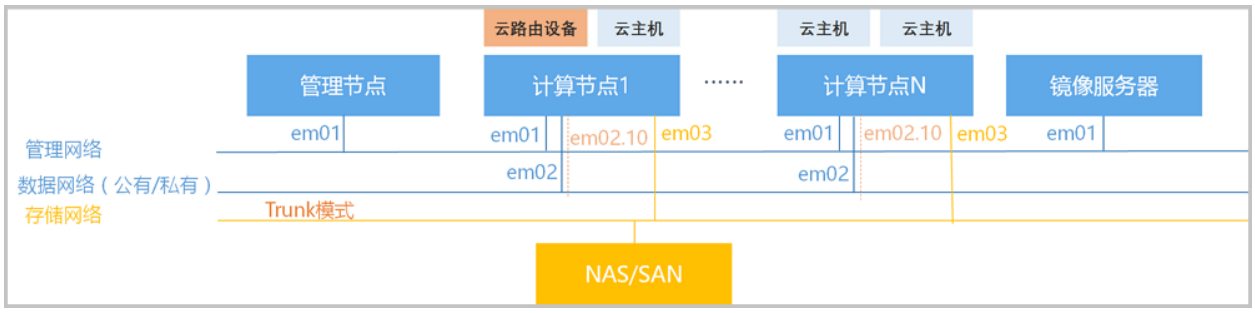
2. NAS/SAN +云路由网络架构

其架构如图 *5: NAS/SAN +云路由网络*所示，此架构支持以下特性：

- 云主机数据存放在集中存储，云盘数据通过存储双控和RAID技术提供保护。
- 需要准备存储网络，准备集中存储，建议万兆以上网络，云主机受高可用保护。
- 添加到ZStack时，可添加为NFS或Shared Mount Point主存储。
- 构建了存储网，云主机支持高可用，数据支持安全保护，IO性能有瓶颈，建议8～10计算节点共用一个存储。
- 使用云路由器提供DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec、安全组等网络服务。
- 支持分布式DHCP网络。

- 需要一定的投资，适用于传统应用、应用数据紧密、SLA高可用保证、数据安全场景。

图 5: NAS/SAN +云路由网络



管理网络：

- 负责管理各计算节点及存储节点资源的网络。
- 图示的em01即为管理节点使用的网卡，是管理节点用于和计算节点及镜像服务器通信的网络。

数据网络：

- 同一个物理接线通过VLAN设置为公有网络和私有网络。
- 其中公有网络为不带VLAN的em02，可以访问互联网，私有网络为VLAN编号为10的em02，交换机端需设置Trunk模式，云主机可以通过云路由器访问互联网，云路由网络使用云路由器来提供各种网络服务，云路由器的网络默认IP为公有网络的IP地址。

注:

如果物理主机网卡较少，管理网络和数据网络可以合并为同一个网络。

存储网络：

- 用于提供NAS/SAN存储的网络。
- 建议使用万兆以太网或FC，加速存储访问。图示使用的是em03来专门提供存储网络流量的访问。

镜像服务器：

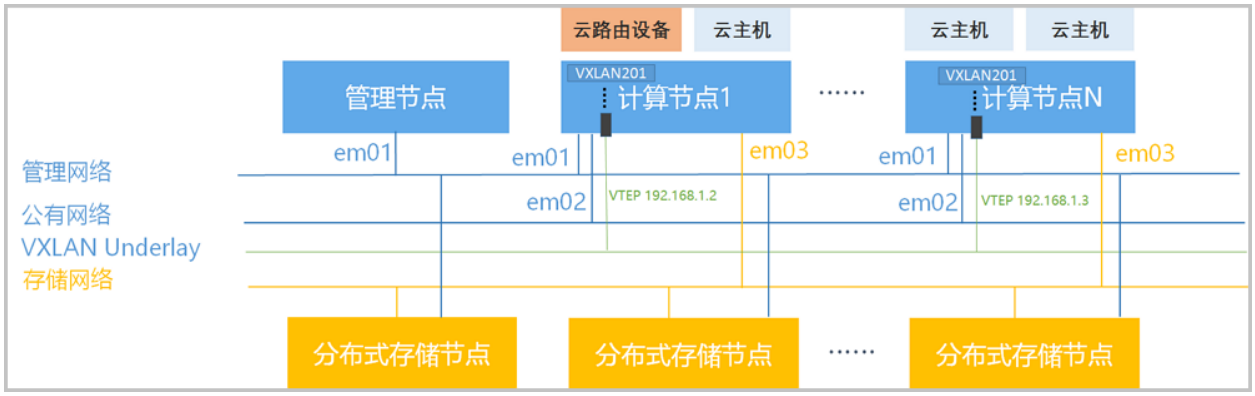
- 镜像服务器可以使用单独的服务器提供服务。
- 在小型的数据中心，也可与管理节点使用同一台机器。

3. **Ceph+VXLAN云路由网络架构**

其架构如*图 6: Ceph + VXLAN云路由网络*所示，此架构支持以下特性：

- 云主机数据存放在分布式存储，数据通过多副本和纠删码机制提供保护。
- 需要准备存储网络，云主机受高可用保护。
- Ceph主存储和Ceph镜像服务器使用同一套分布式存储。
- 构建了存储网，云主机支持高可用，数据支持多副本，计算和存储都可以横向扩展。
- 使用VXLAN的VTEP提供二层逻辑子网，VXLAN Underlay网络供云主机访问。
- 使用云路由器提供DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec、安全组等网络服务。
- 支持分布式DHCP网络。
- 适用于租用平台、通用型应用、应用数据紧密、SLA高可用保证、大规模环境。

图 6: Ceph + VXLAN云路由网络



管理网络：

- 负责管理各计算节点及存储节点资源的网络。
- 图示的em01即为管理节点使用的网卡，是与计算节点和分布式存储通信的网络。

公有网络：

- 可以访问外部互联网的网络。
- 云主机可以通过云路由器访问互联网，云路由网络使用云路由器来提供各种网络服务，云路由器的网络默认IP为公有网络的IP地址。
- 图示使用的em02来提供公有网络服务。如果网卡不足，也可将管理网络和公有网络合并为一个网络使用。

VXLAN Underlay网络：

- 给云主机使用的VXLAN Underlay私有网络。
- 基于三层IP地址的二层逻辑网络，例如图示采用的是*192.168.1.x/24*的VTEP来提供VNI为201的私有网络。

存储网络：

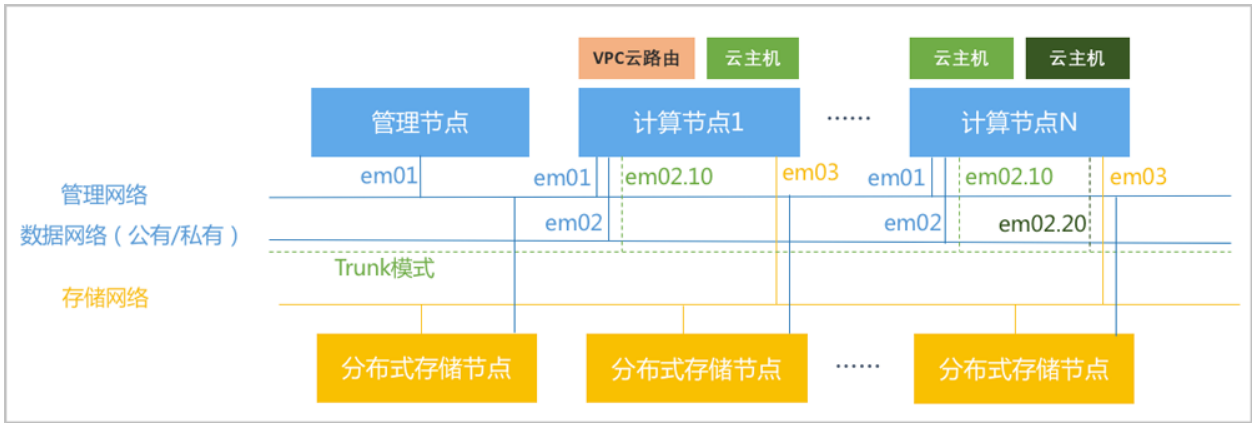
- 用于提供分布式块存储的网络。
- 用于提供分布式块存储的网络，建议使用万兆以太网或FC，加速存储访问。
- 例如图示的em03的存储网络。Ceph分布式存储至少需要有一个Mon IP可与管理网络互通。

4. Ceph+VPC网络架构

其架构如图 *7: Ceph + VPC网络*所示，此架构支持以下特性：

- 云主机数据存放在分布式存储，数据通过多副本和纠删码机制提供保护。
- 需要准备存储网络，云主机受高可用保护。
- Ceph主存储和Ceph镜像服务器使用同一套分布式存储。
- 构建了存储网，云主机支持高可用，数据支持多副本，计算和存储都可以横向扩展。
- 使用VPC路由器提供DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec、安全组等网络服务。
- 支持分布式DHCP网络。
- 适用于租用平台、通用型应用、应用数据紧密、SLA高可用保证、大规模环境。

图 7: Ceph + VPC网络



管理网络：

- 负责管理各计算节点及存储节点资源的网络。
- 图示的em01即为管理节点使用的网卡，是管理节点用于和计算节点及镜像服务器通信的网络。

数据网络：

- 同一个物理接线通过VLAN设置为公有网络和私有网络。
- 其中公有网络为不带VLAN的em02，可以访问互联网，私有网络（VPC网络）包括：VLAN编号为10的em02、以及VLAN编号为20的em02，交换机端需设置Trunk模式，云主机可以通过VPC路由器公有网络访问互联网，VPC网络使用VPC路由器来提供各种网络服务，VPC路由器的网络默认IP为公有网络的IP地址。

注:

如果物理主机网卡较少，管理网络和数据网络可以合并为同一个网络。

存储网络：

- 用于提供分布式块存储的网络。
- 用于提供分布式块存储的网络，建议使用万兆以太网或FC，加速存储访问。
- 例如图示的em03的存储网络。Ceph分布式存储至少需要有一个Mon IP可与管理网络互通。

5 安装部署

本章主要介绍ZStack企业版 3.1.1的安装/升级过程。

5.1 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：
   - c74版：ZStack-x86_64-DVD-3.1.1-c74.iso
   - c72版：ZStack-x86_64-DVD-3.1.1-c72.iso

   注:

   - 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，详情请参考官网《升级教程》。
   - 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，详情请参考官网《升级教程》。
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c74 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-3.1.1-c74.iso

  - 下载地址：点击这里
- ZStack安装包
  - 文件名称：ZStack-installer-3.1.1.bin
  - 下载地址：点击这里

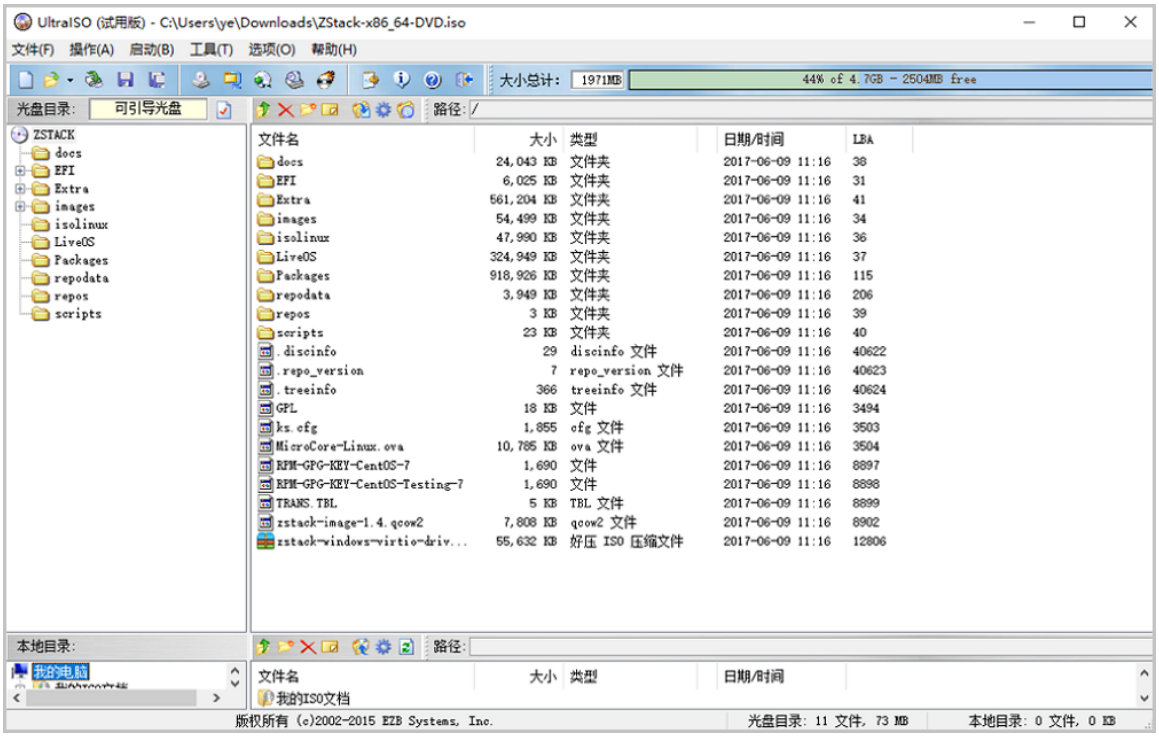
注: 软件下载后，需通过MD5校验工具核对校验码，以确保软件完整无损。

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 *8: 在UltraISO打开ISO镜像*所示：

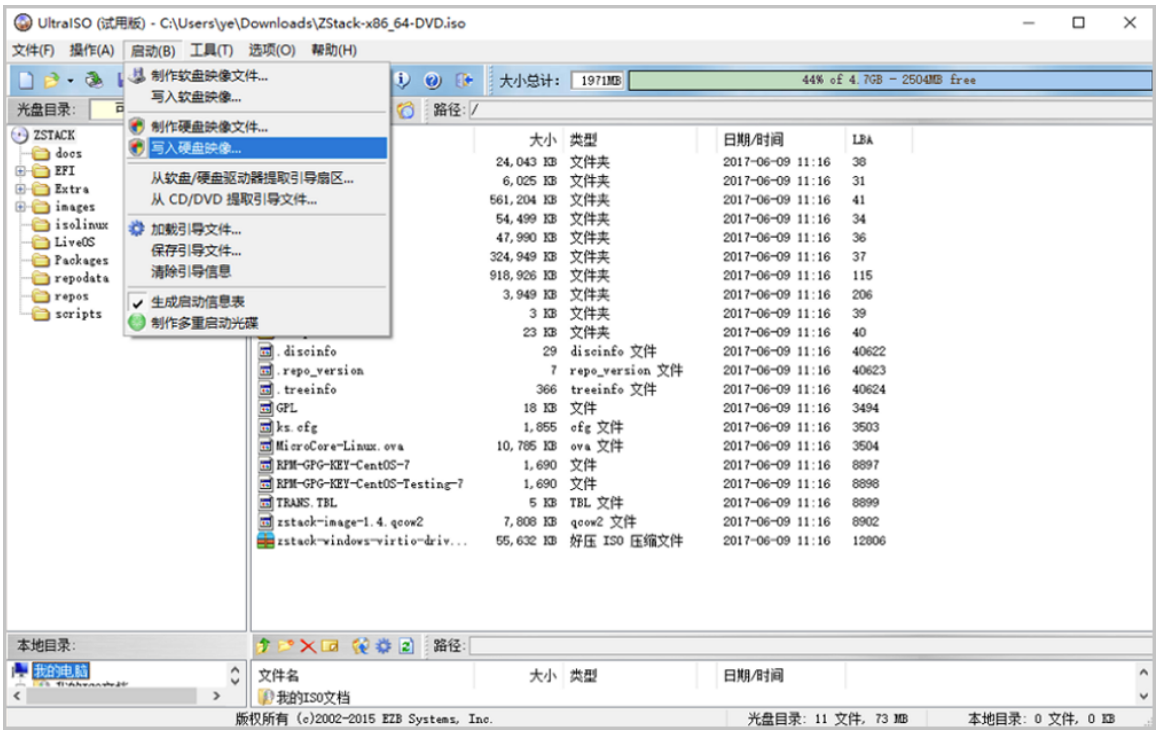
图 8: 在UltraISO打开ISO镜像



b) 写入硬盘镜像。

在UltraISO，点击**启动** > **写入硬盘映像**，如图 *9: 在UltraISO写入硬盘映像*所示：

图 9: 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 *10: 在UltraISO确认写入ISO镜像*所示：

图 10: 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。

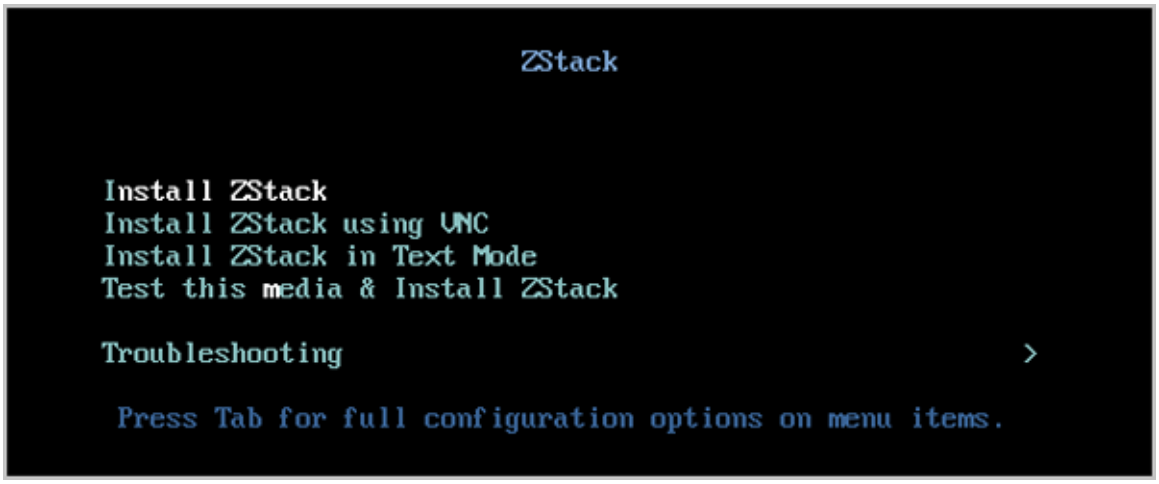
a) 管理员需要预先在服务器进行以下配置：

- 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 *11: 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 11: U盘引导界面



注:

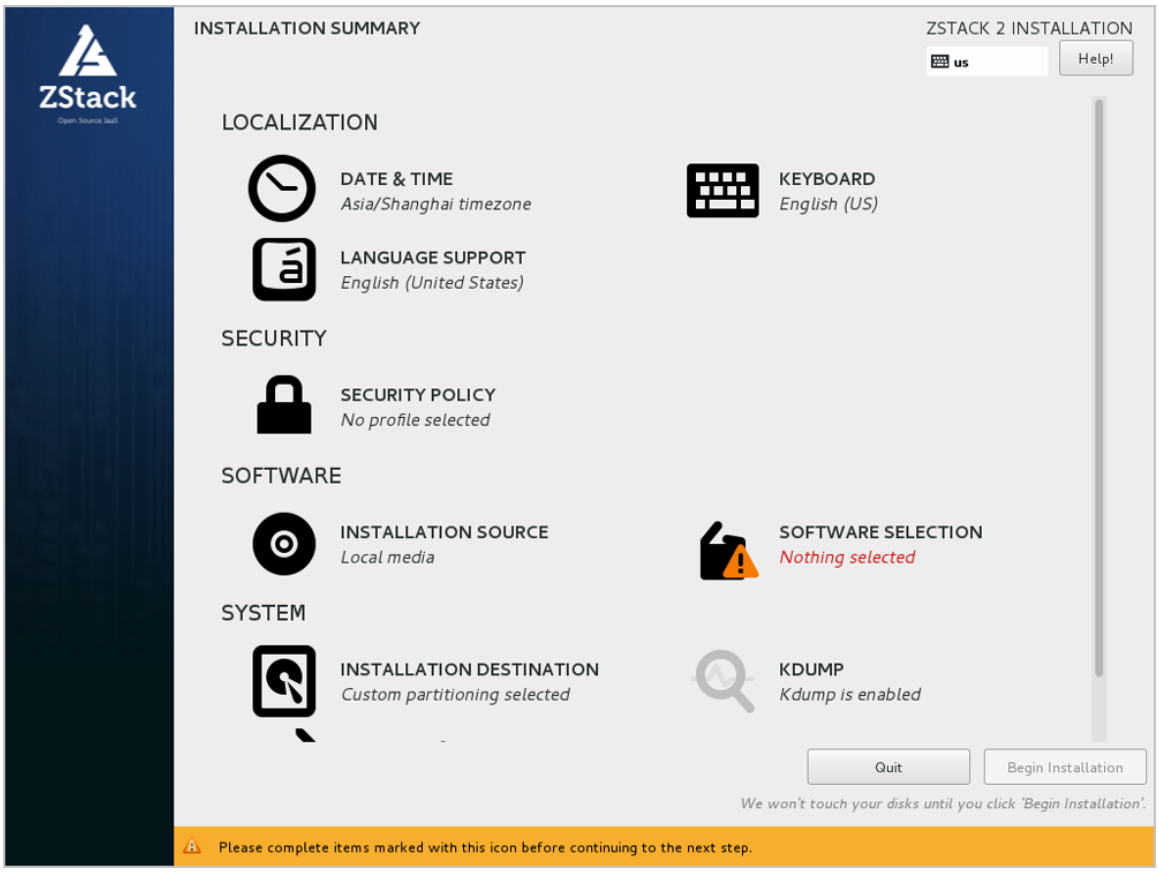
- ZStack提供了三种安装方式：图形界面安装、通过VNC安装和字符界面安装，用户可根据实际情况选择。
- ZStack建议图形界面安装是最好的选择。
- 考虑到某些服务器是不带VGA接口的，只能通过串口连接，这时用户可以选择VNC或者Text Mode。

c) 进入系统安装界面后，已经预先配置如下默认选项，管理员可按实际情况更改配置。

- **DATE&TIME**：默认亚洲东八区，建议管理员提前检测物理机时间，配置为当前时间和时区
- **LANGUAGE**：默认English(United States)
- **KEYBOARD**：默认English(US)

如图 *12: 系统安装界面*所示：

图 12: 系统安装界面



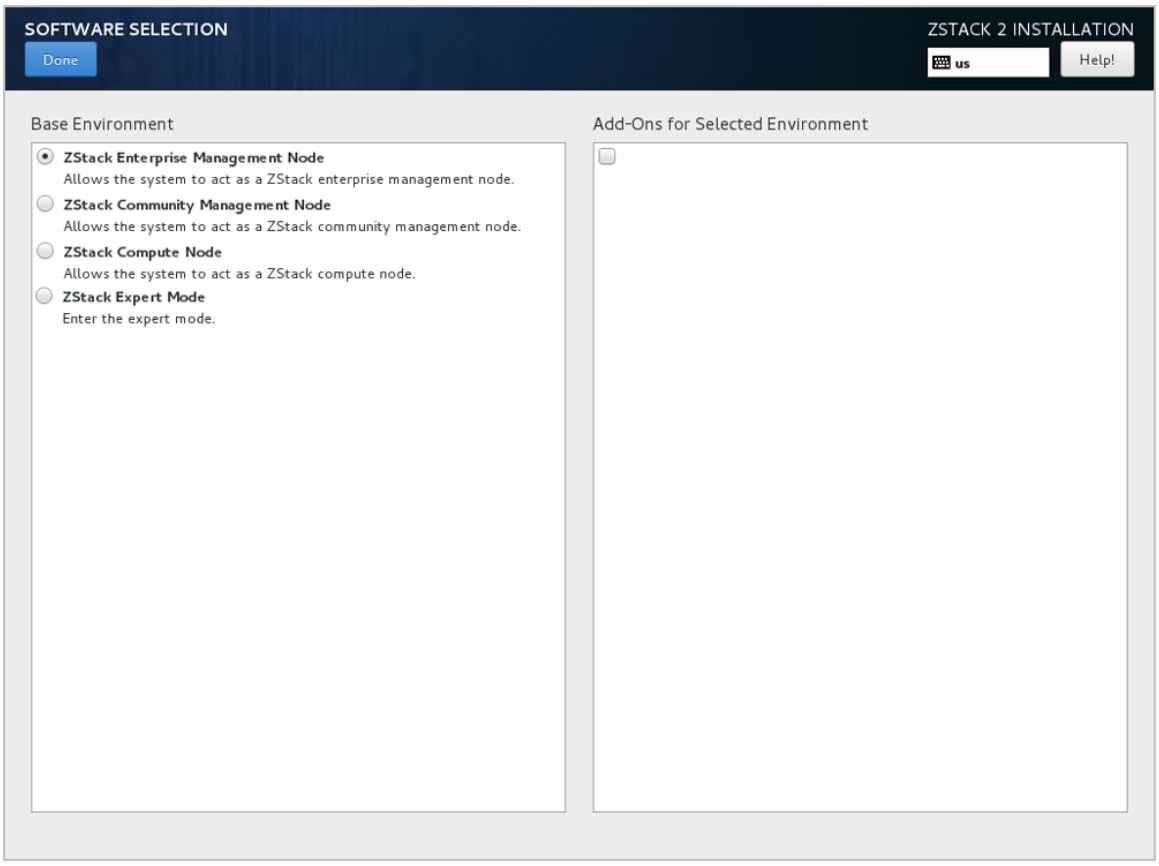
d) 选择安装模式。

在系统安装界面，点击**SOFTWARE SELECTION**进入服务器安装模式候选，如图 *13:* 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**。

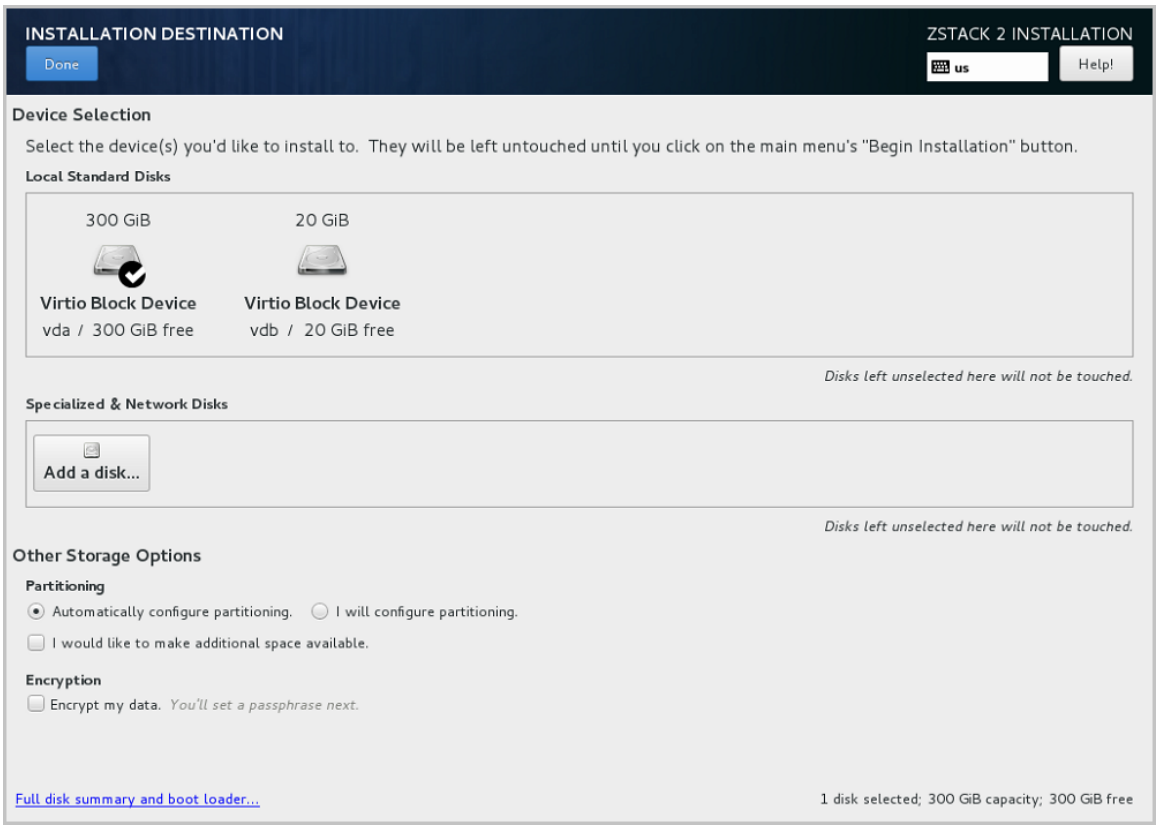
图 13: 选择安装模式



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 *14: 系统预先默认设置 - 自动硬盘分区*所示：

图 14: 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。

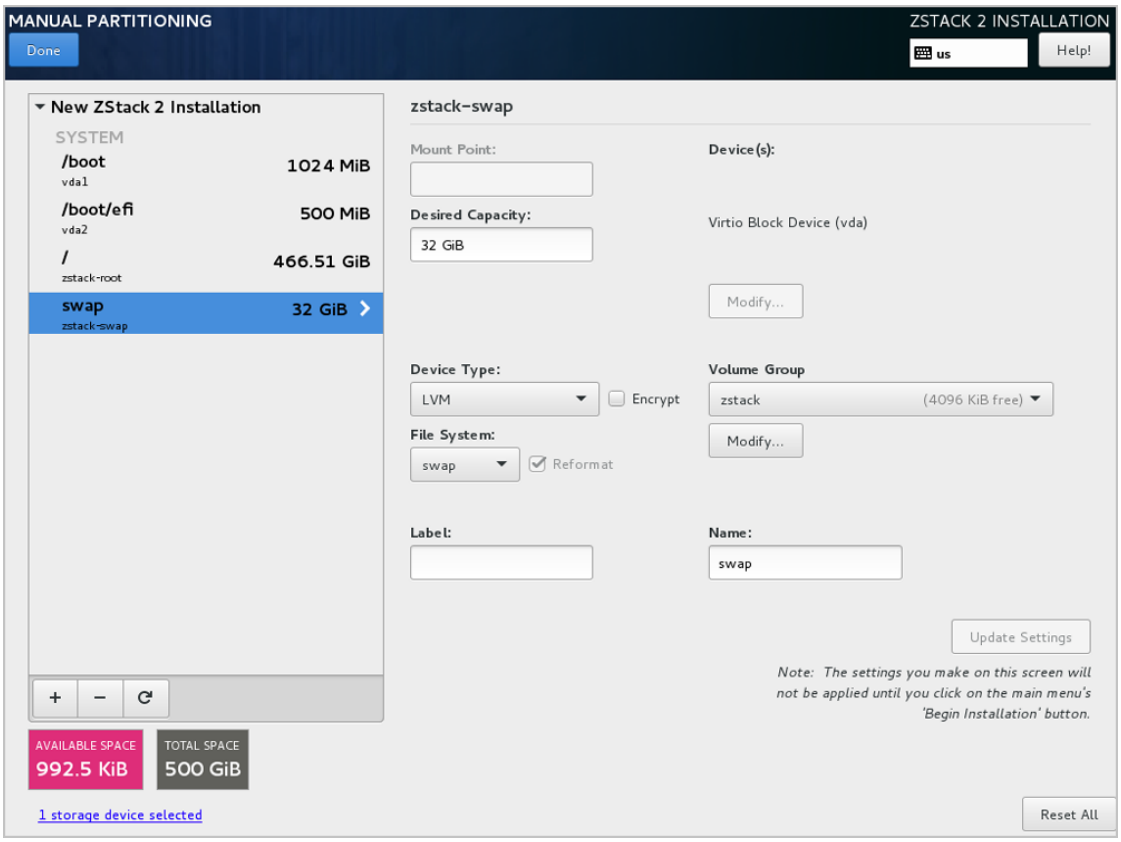
系统预先默认设置：**Automatically configure partitioning**，ZStack建议遵循默认设置，执行自动硬盘分区。

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 *15: 手动分区推荐UEFI模式*所示：

图 15: 手动分区推荐UEFI模式



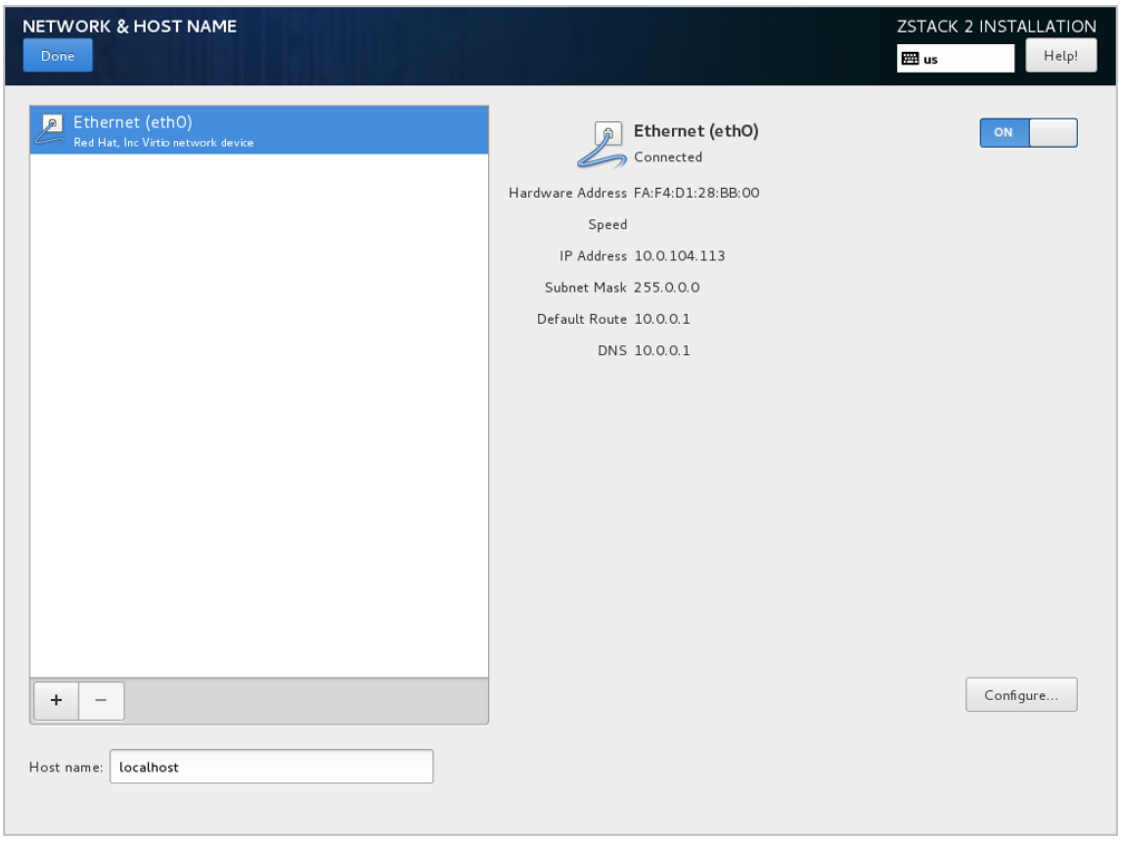
f) 配置网络。

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 *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. 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 *16:* 网卡配置主界面，选中**Ethernet**（eth0），点击**Configure...**，打开**eth0**配置界面，如图 *17:* 配置*eth0*静态*IP*所示。

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

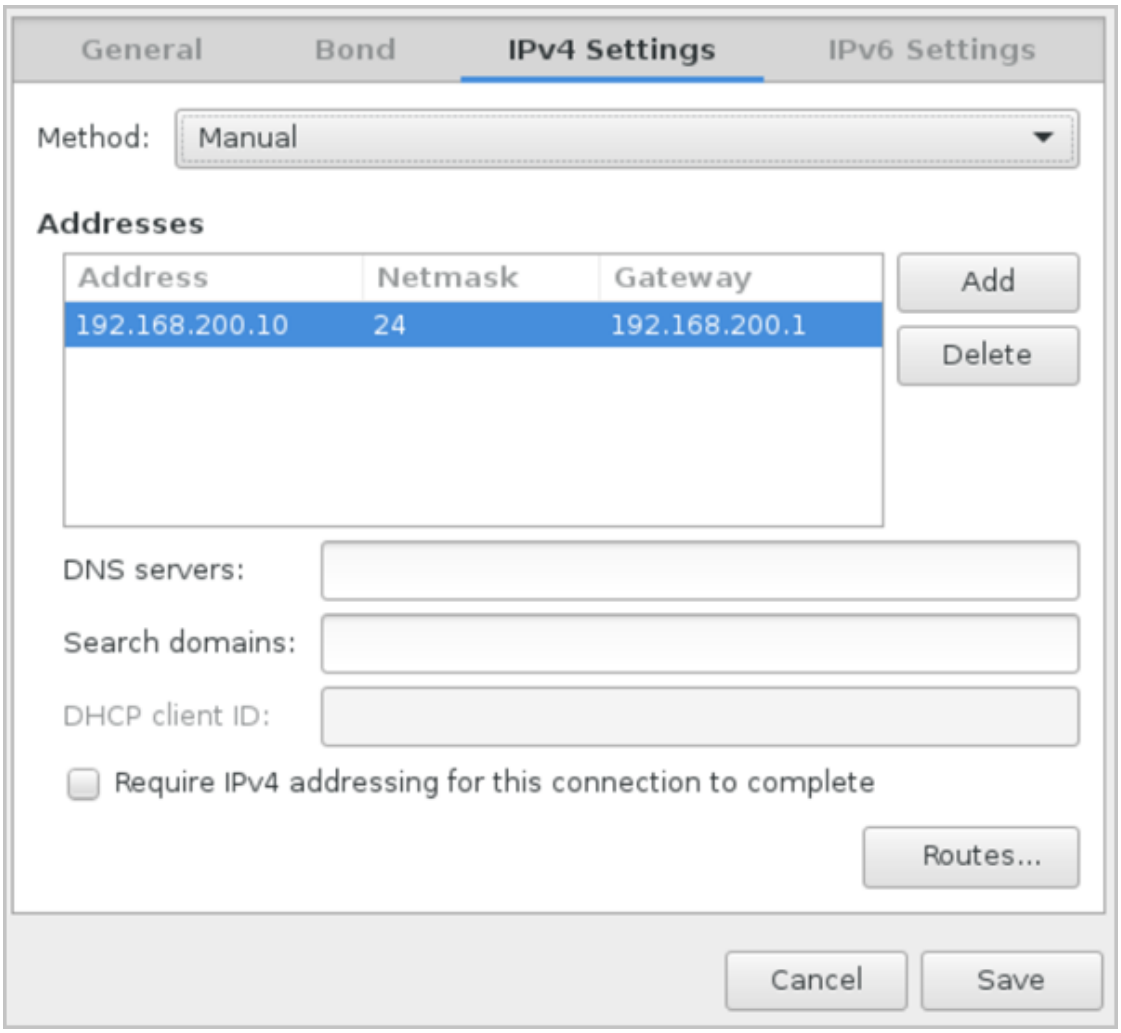
   c. 在**Method**列表选择**Manual**以进行手动配置。

   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 17: 配置eth0静态IP



4. 设置eth0自动连接。

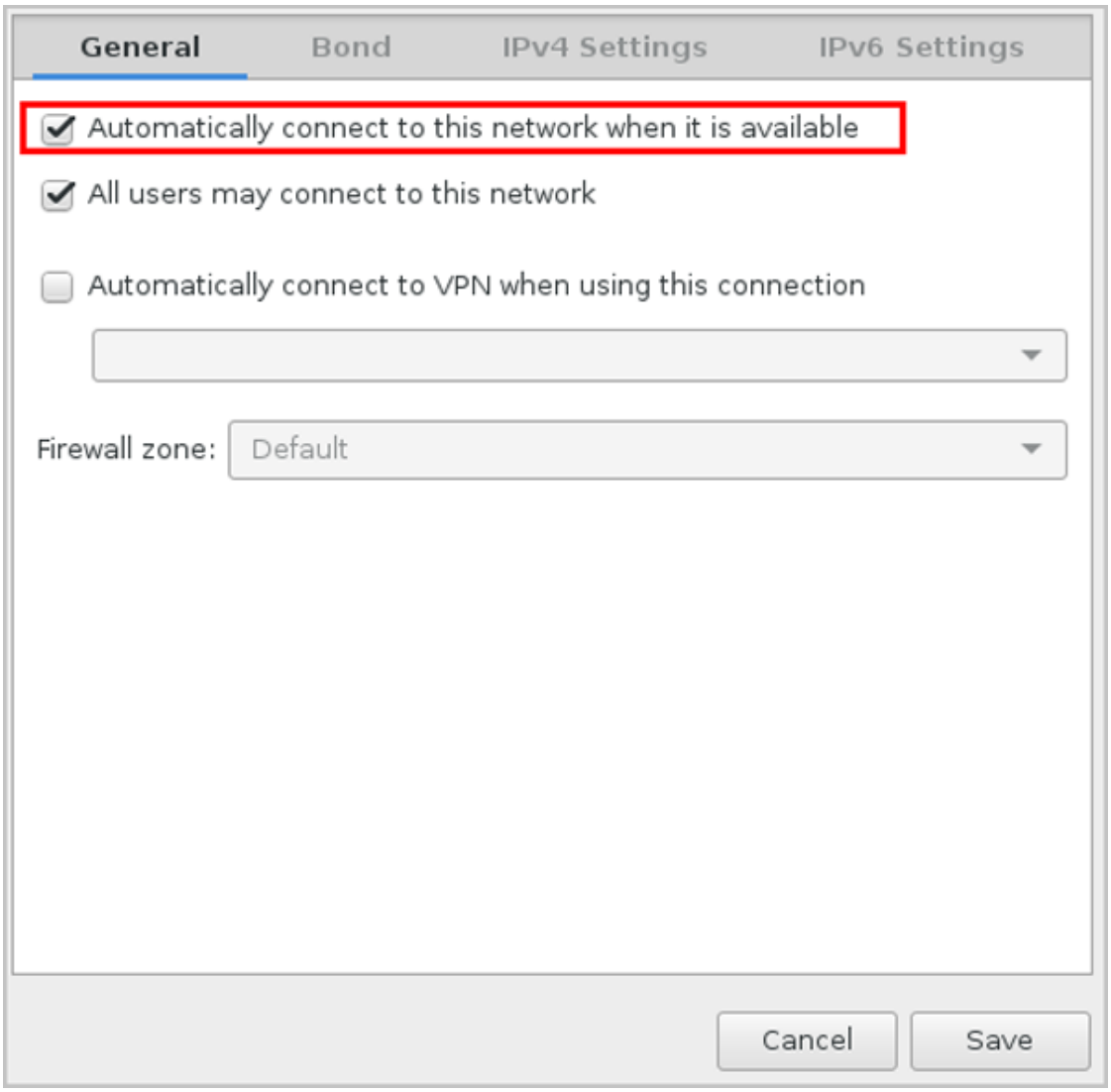
   a. 在图 *16: 网卡配置主界面*，选中**Ethernet**（eth0），点击**Configure...**，打开**eth0**配置界面，如图 *18: 设置eth0自动连接*所示。

   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。

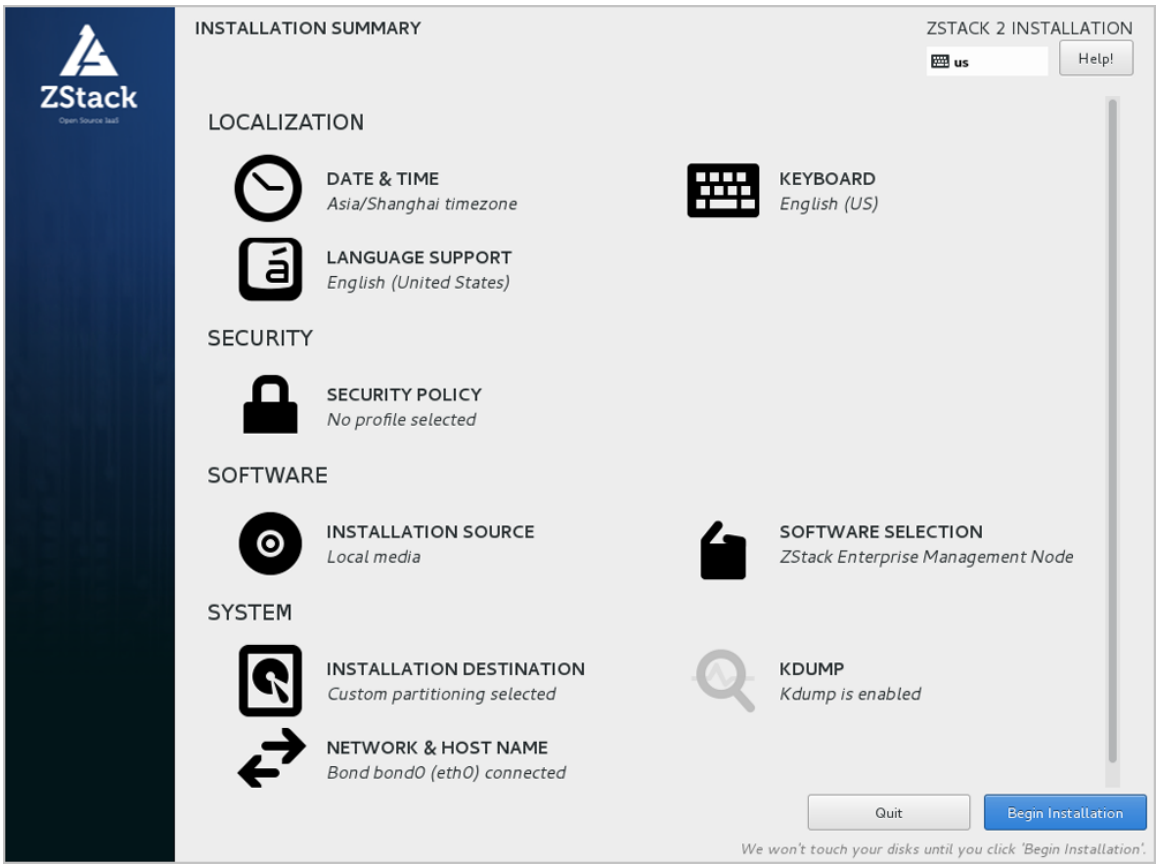
图 18: 设置eth0自动连接



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 *19: 点击Begin Installation*所示：

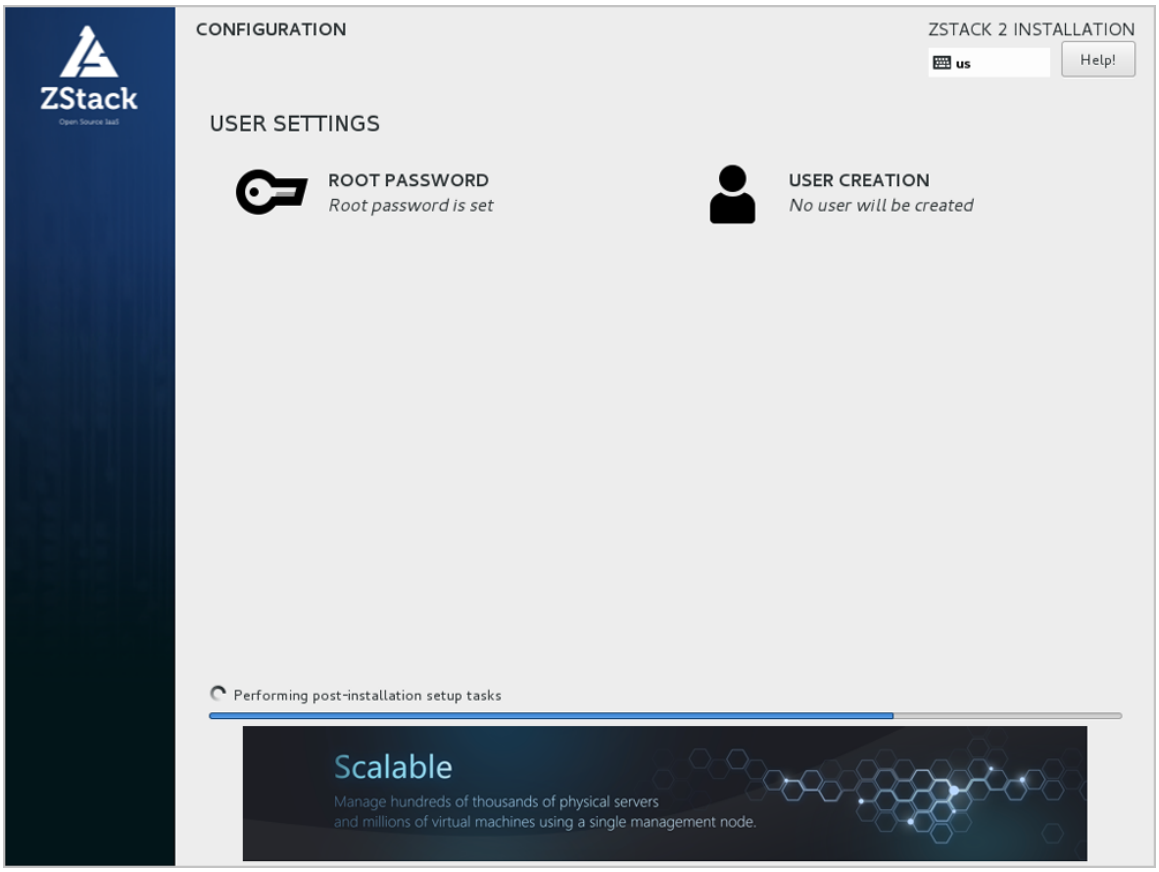
图 19: 点击Begin Installation



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

如图 *20: 系统安装过程界面*所示：

图 20: 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c74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。

5.1.1 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：

```
# 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 eth0

# 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
```

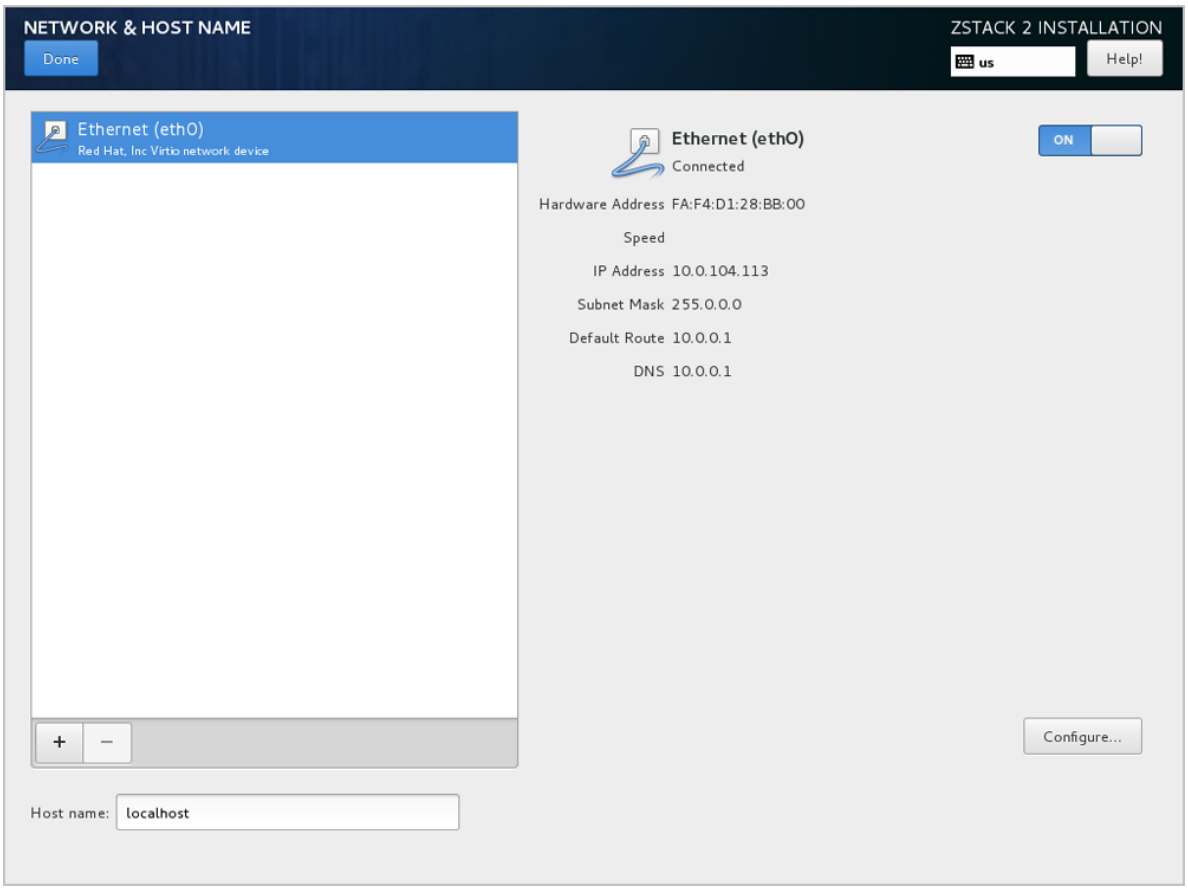
图形界面方式

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 21: 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

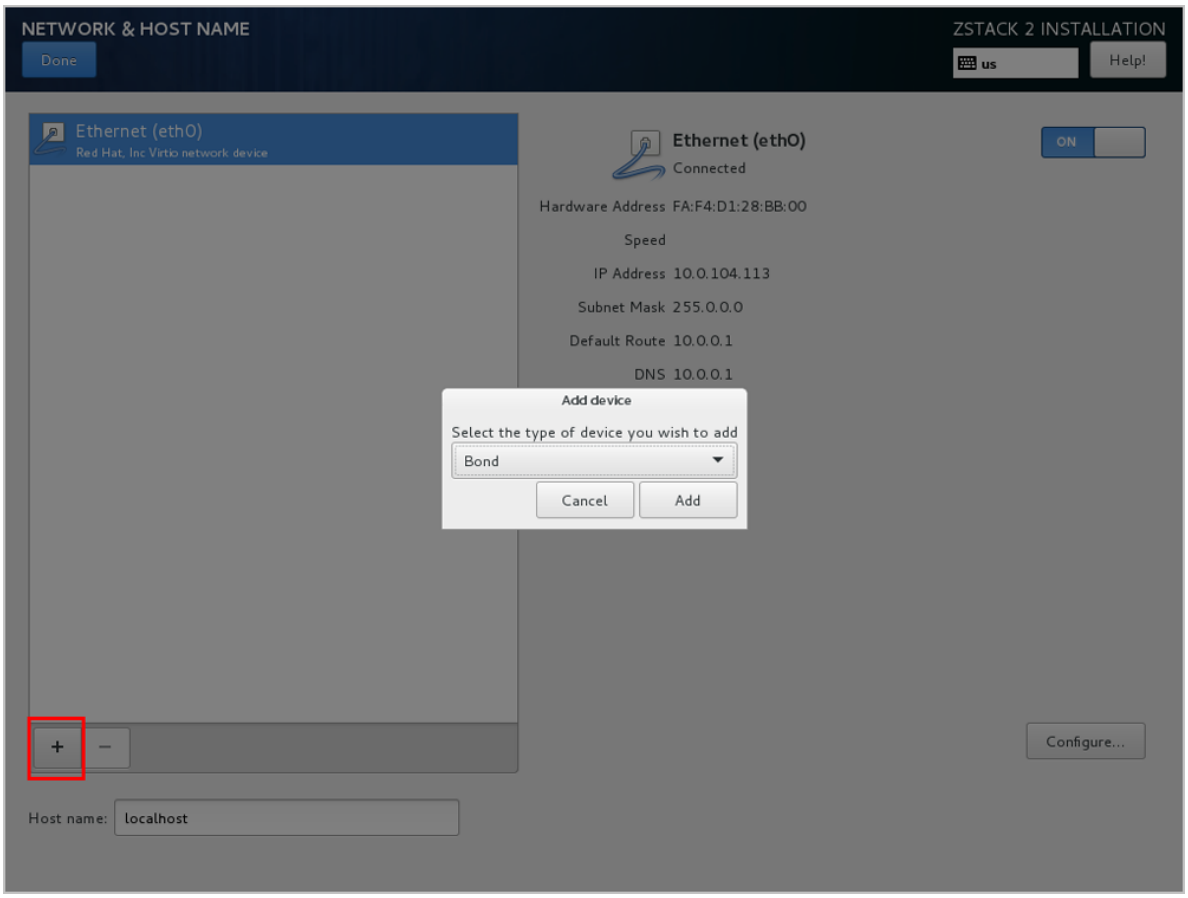
   图 21: 网卡配置主界面



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 *22: 添加一个Bond设备*所示：

   图 22: 添加一个Bond设备



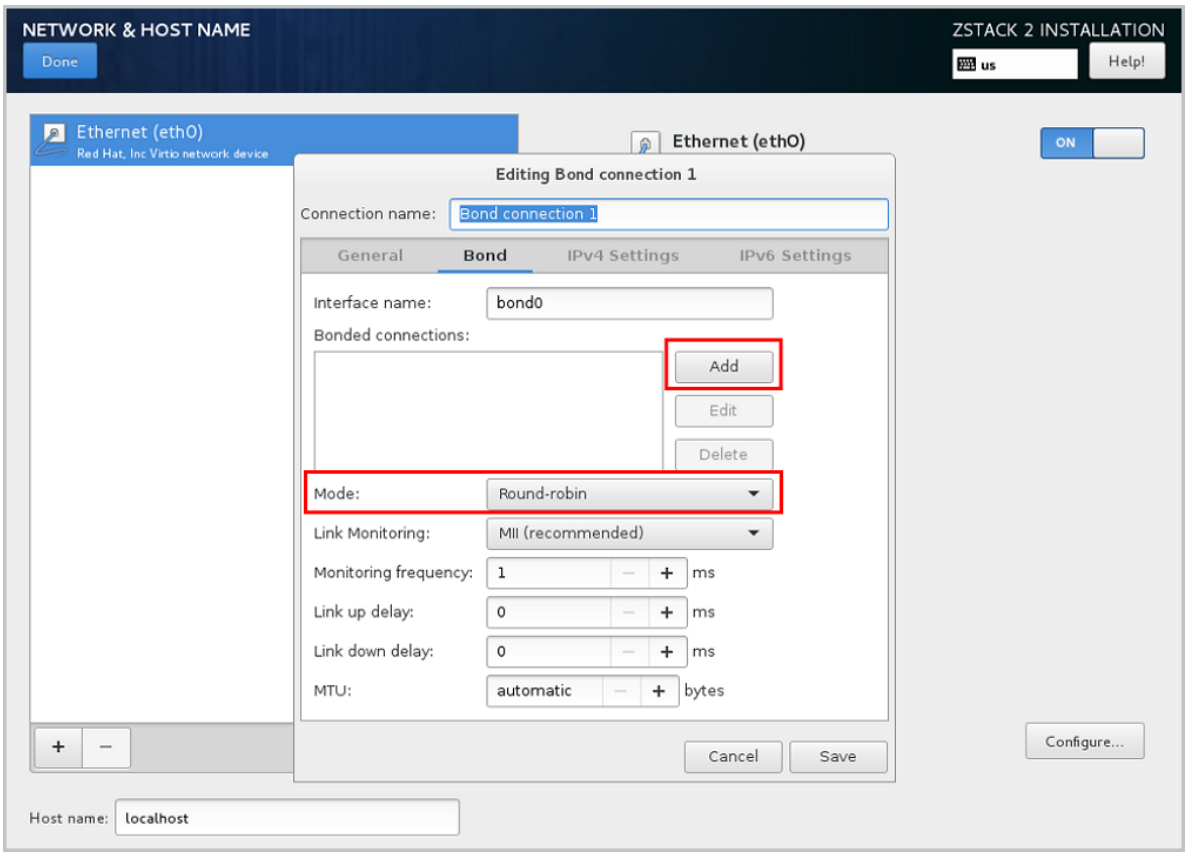
3. 配置Bond。

弹出**Editing Bond connection 1**界面的**Bond**子页面，如图 *23: 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。

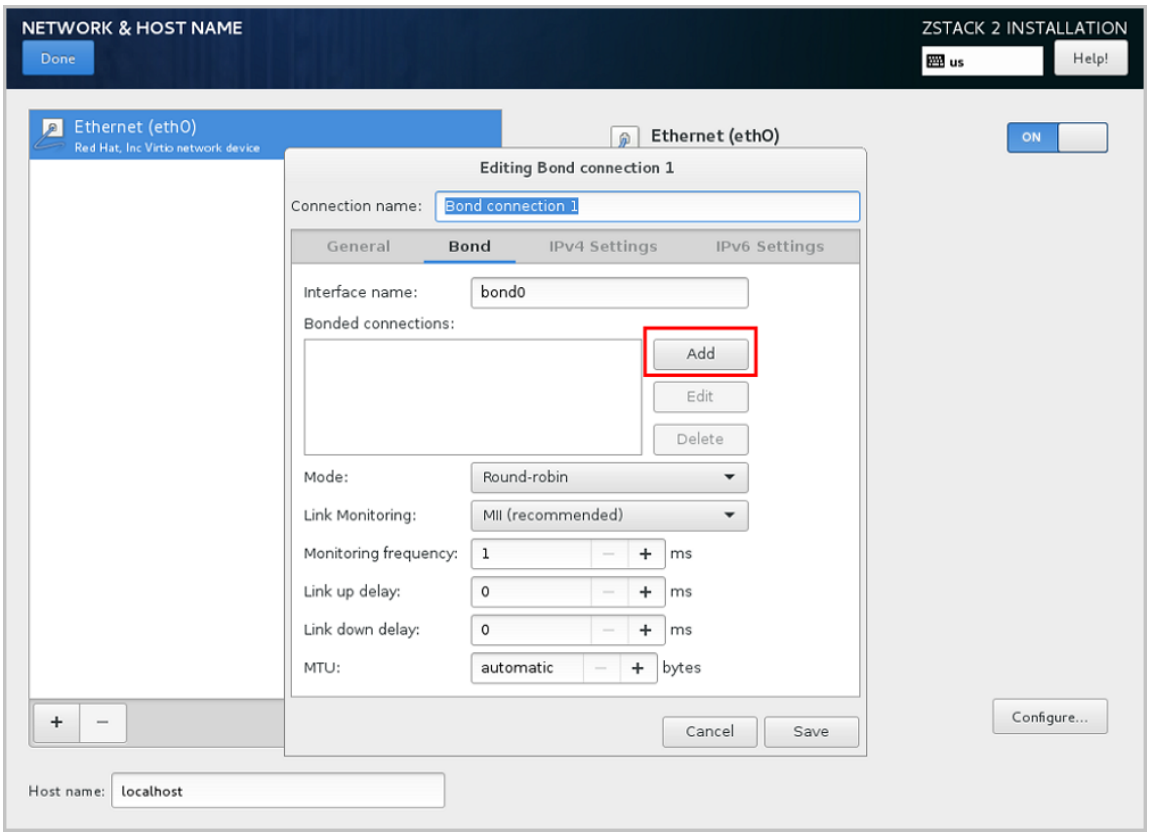
图 23: 配置Bond



4. 添加Bond Slave。

- 在Bond配置界面，点击**Add**，添加Bond Slave，如*图 24: 添加Bond Slave*所示：

图 24: 添加Bond Slave

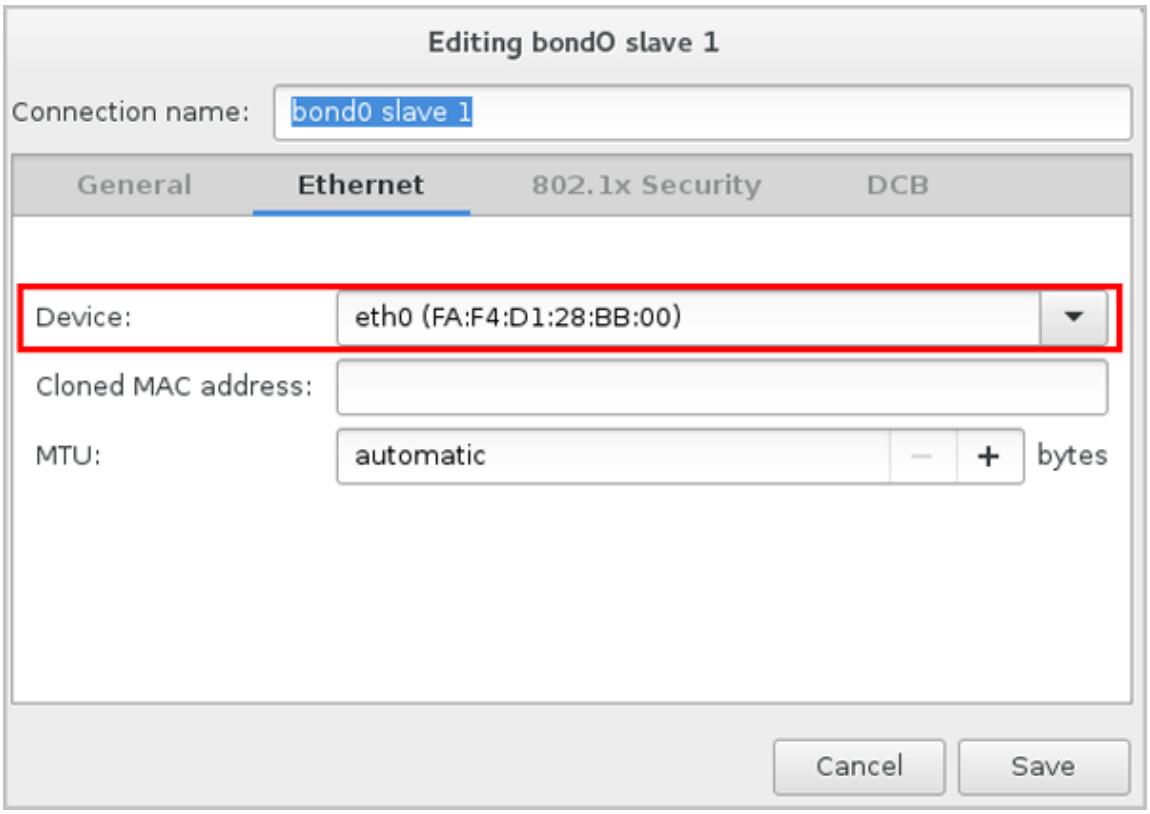


- 弹出**Chooes a Connection Type**界面，在下拉菜单中选择Bond Slave连接类型，如**Ethernet**，点击**Create...**，如图 *25: 选择Bond Slave连接类型*所示：

图 25: 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 *26: 选择Bond Slave设备*所示：

图 26: 选择Bond Slave设备

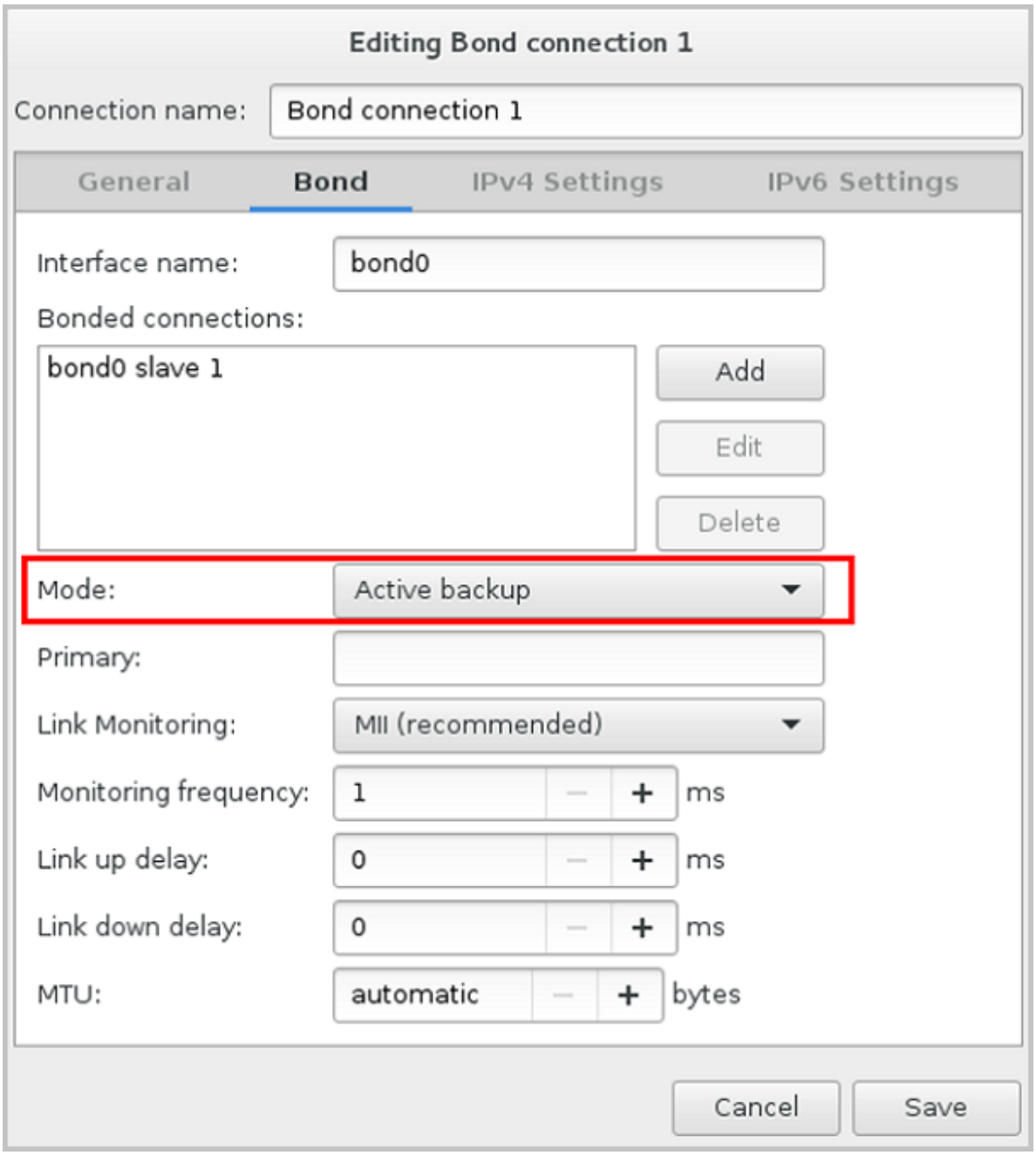


- 至此，Bond Slave已成功添加。

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 *27: 选择Bond模式*所示：

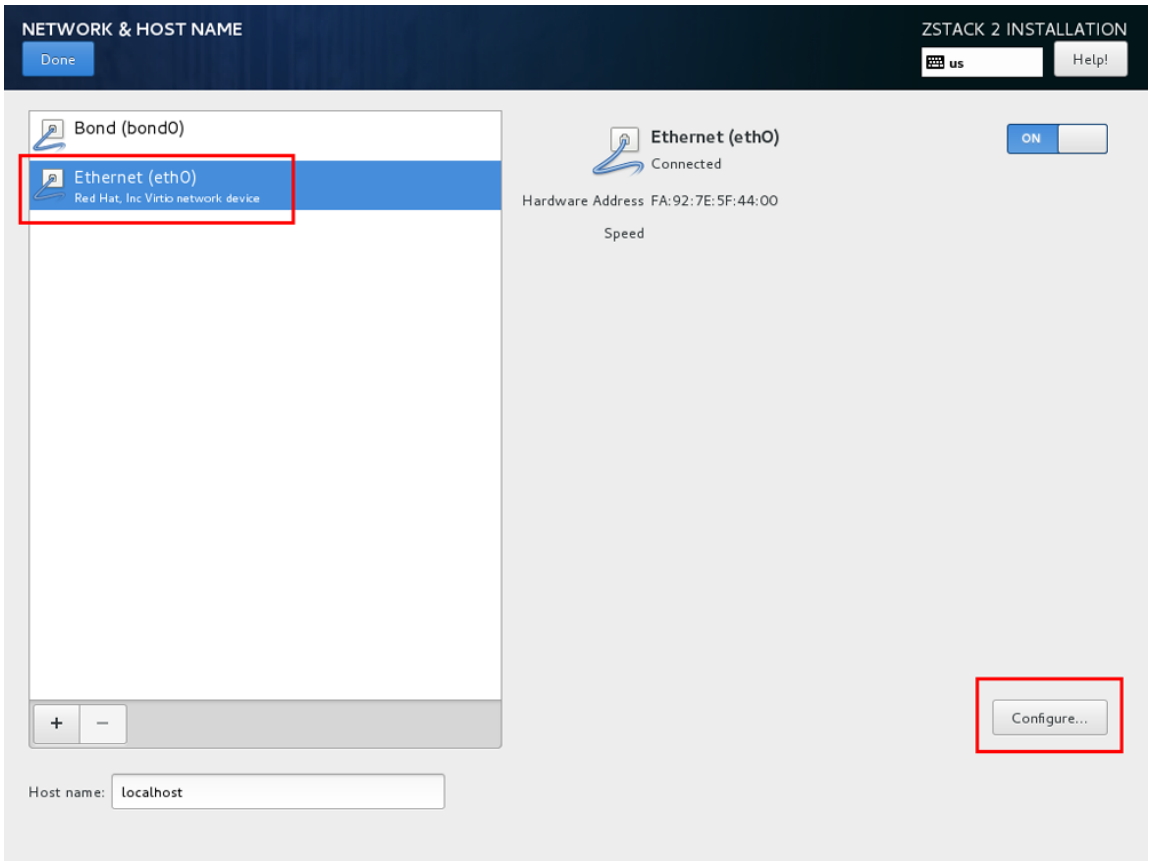
图 27: 选择Bond模式



6. Bond Slave的IPv4设置为禁用。

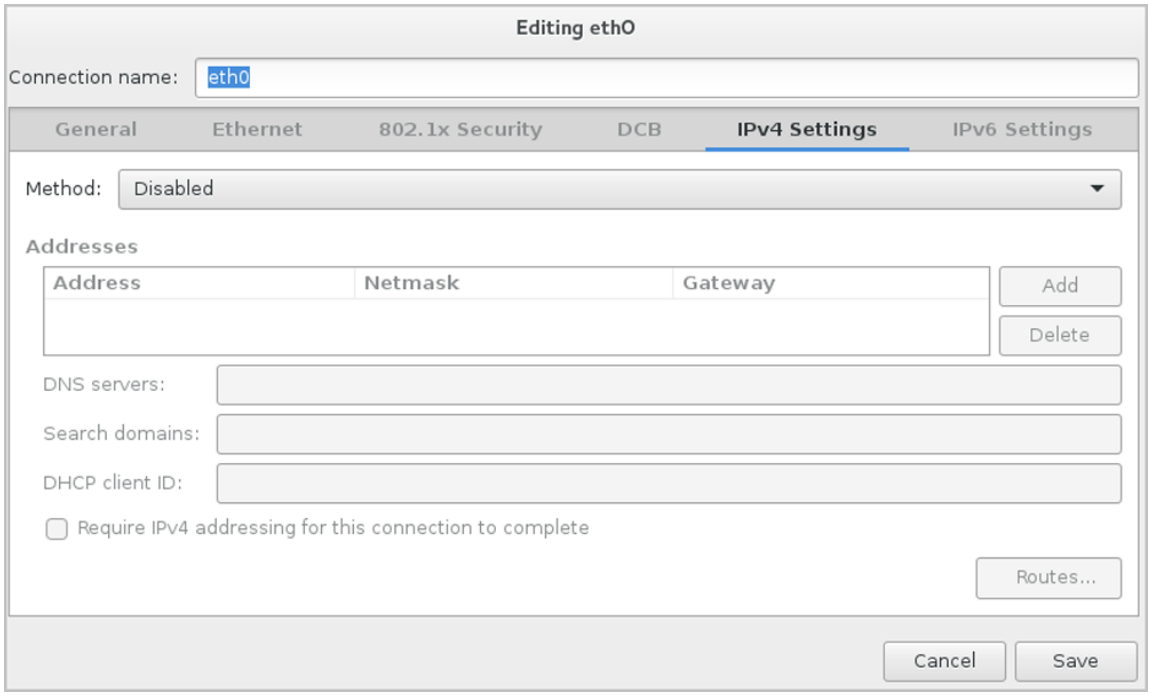
- 回到网卡配置主界面，选中Bond Slave（如eth0），点击**Configure...**，如*图 28: 打开Bond Slave配置界面*所示：

图 28: 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 29: Bond Slave的IPv4设置为禁用*所示：

图 29: Bond Slave的IPv4设置为禁用



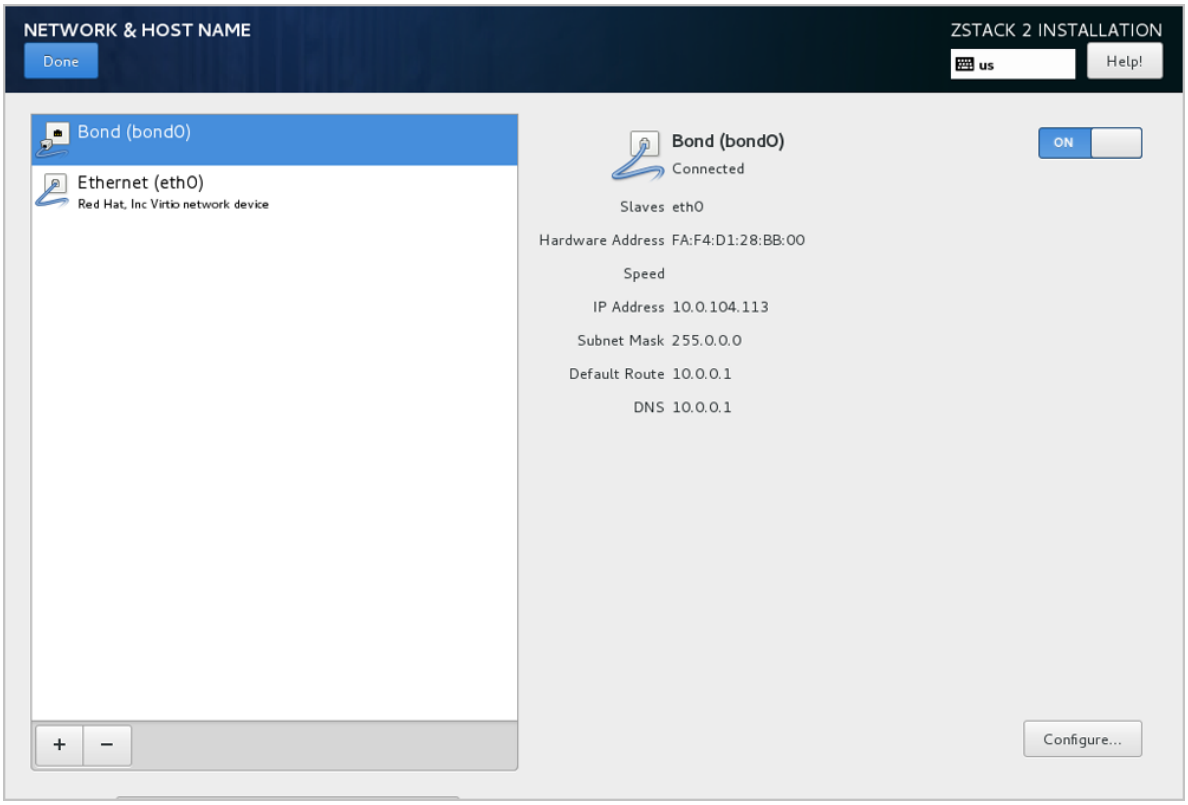
7. 网卡归一化完成。

如图 *30: 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 30: 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 *21: 网卡配置主界面*，选中**Bond**（bond0），点击**Configure...**，打开Bond配置界面，如图 *31: 配置Bond静态IP*所示。

   b. 进入Bond的**IPv4 Settings**选项页。

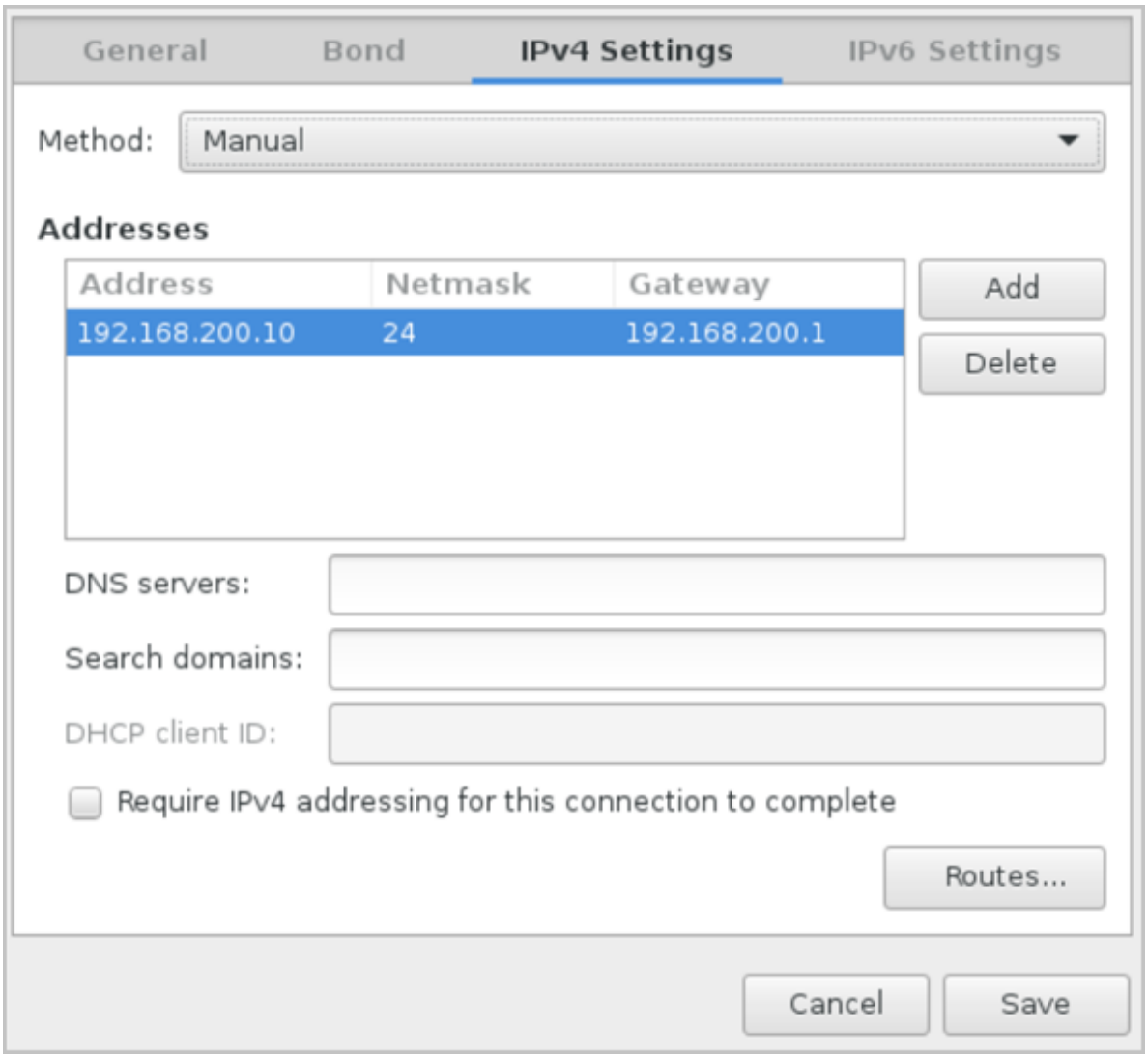
   c. 在**Method**列表选择**Manual**以进行手动配置。

   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 31: 配置Bond静态IP



9. 设置Bond自动连接。

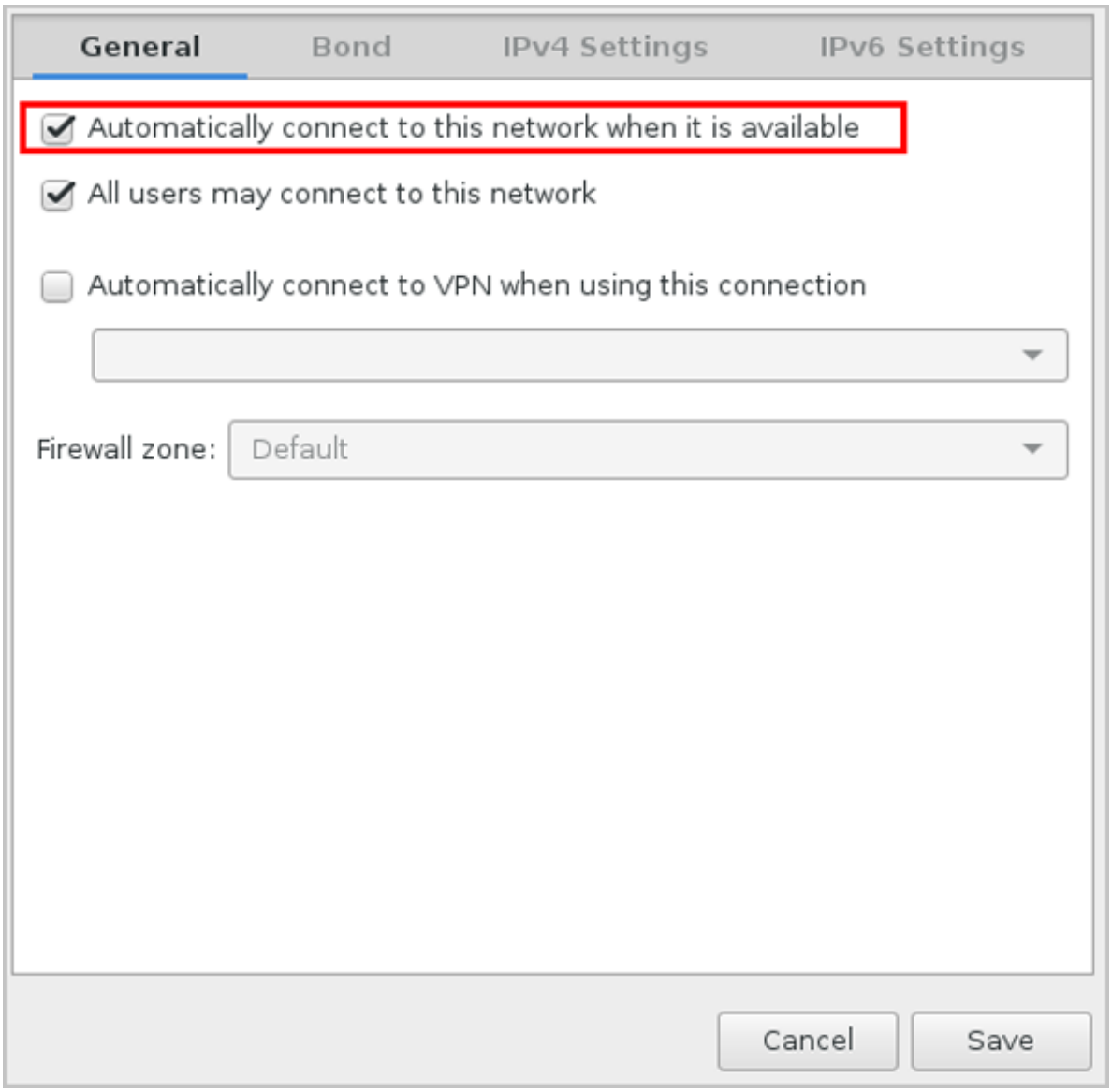
   a. 在图 *21: 网卡配置主界面*，选中**Bond**（bond0），点击**Configure...**，打开Bond配置界面，如图 *32: 设置Bond自动连接*所示。

   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 32: 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。

5.2 安装ZStack

本节主要介绍ZStack企业版 3.1.1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、消息总线等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、消息总线等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**

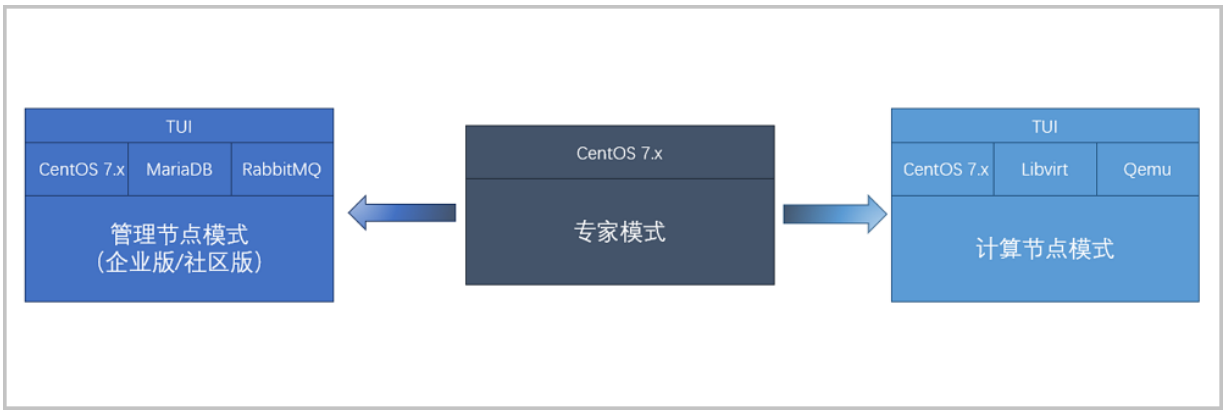
- 安装基础系统

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 *33:* 四种安装模式示意图所示：

图 33: 四种安装模式示意图



5.2.1 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

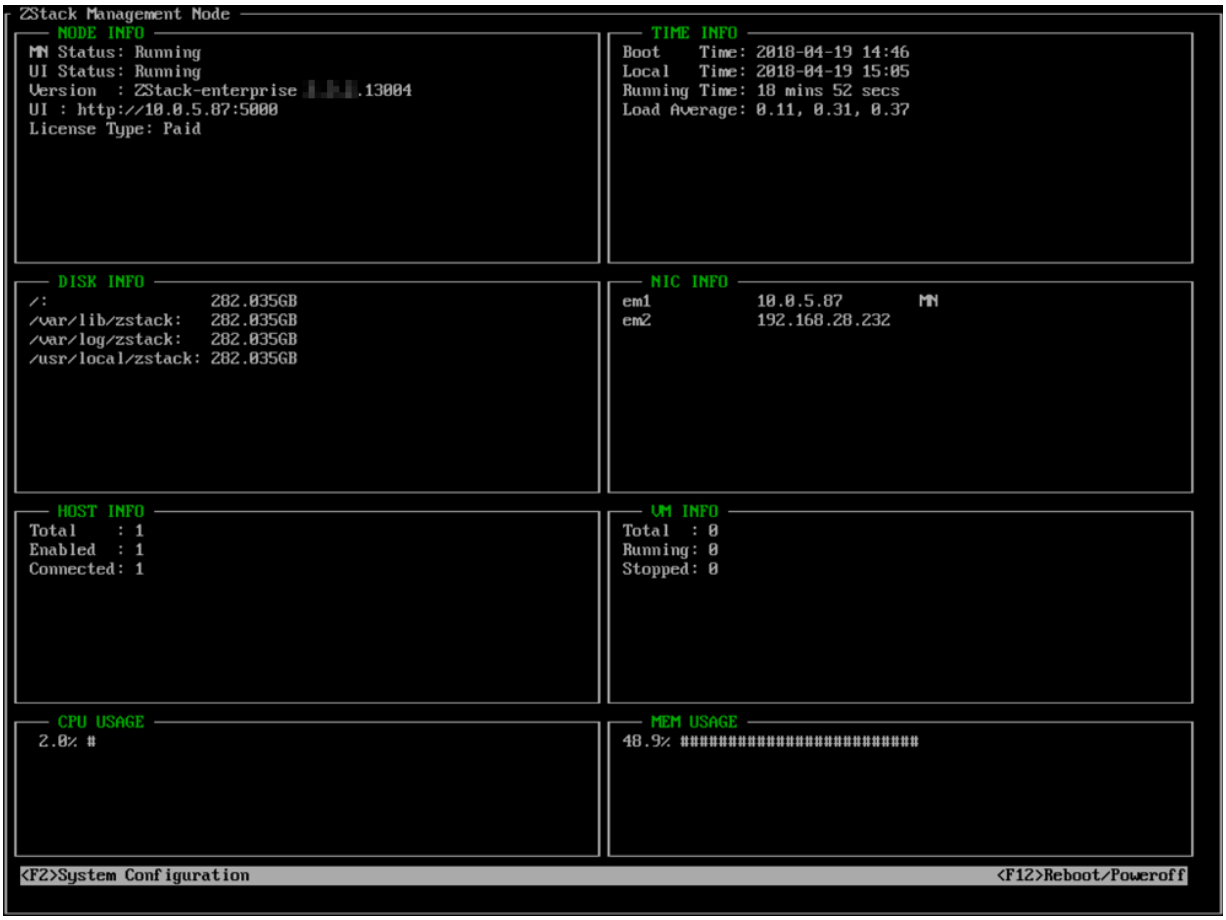
如果选择企业版/社区版管理节点模式，重启后会自动安装ZStack管理节点，安装完成后将自动进入TUI，如图 *34:* 自动安装管理节点所示：

图 34: 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 *35: 管理节点TUI主界面*所示:

图 35: 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。

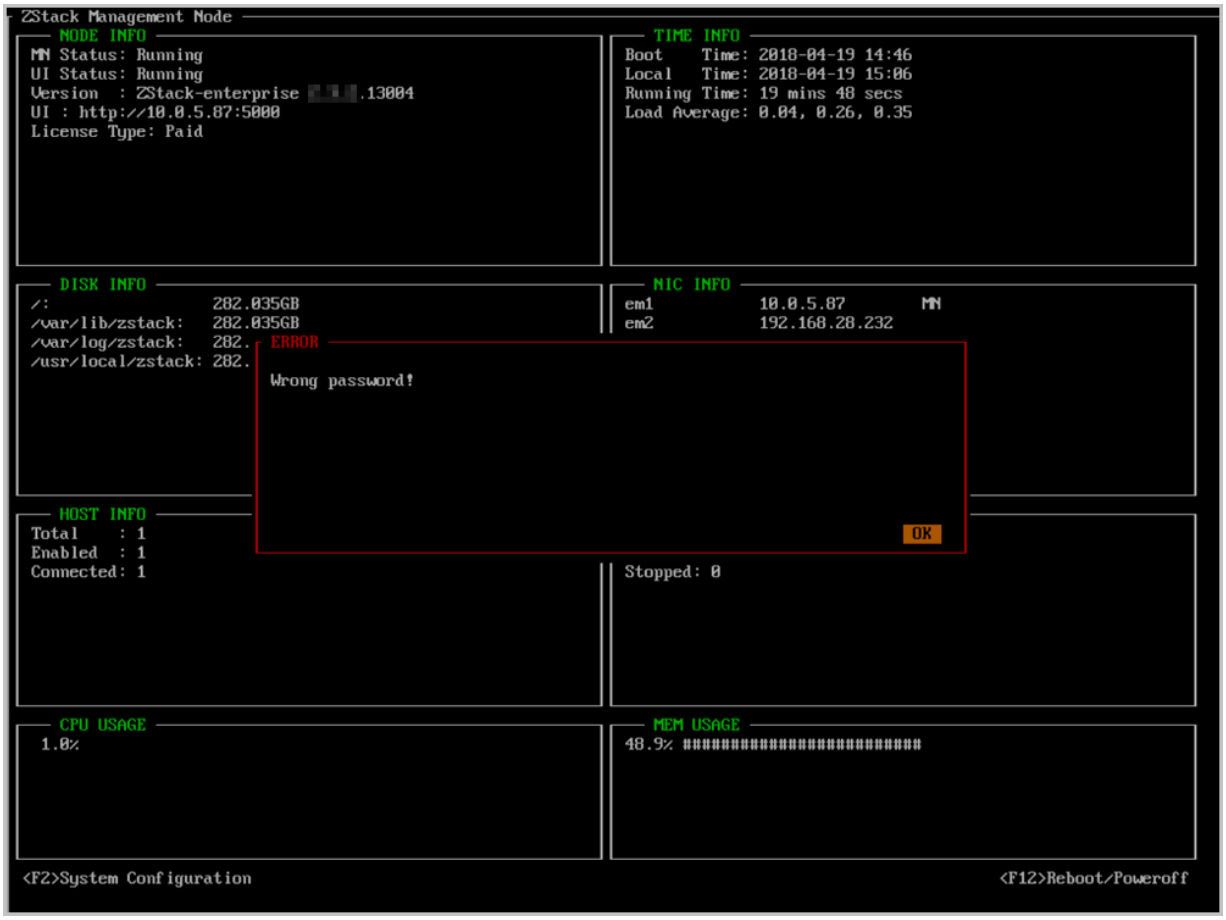
下图中显示了输入系统密码的窗口，**根据提示输入ROOT密码**，**回车即可**。

图 36: 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 37: 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 *38: 系统配置*所示：

图 38: 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账号的消息总线密码

如图 *39: 四种密码修改动作*所示：

图 39: 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 *40: 修改系统root密码*所示：

   图 40: 修改系统root密码

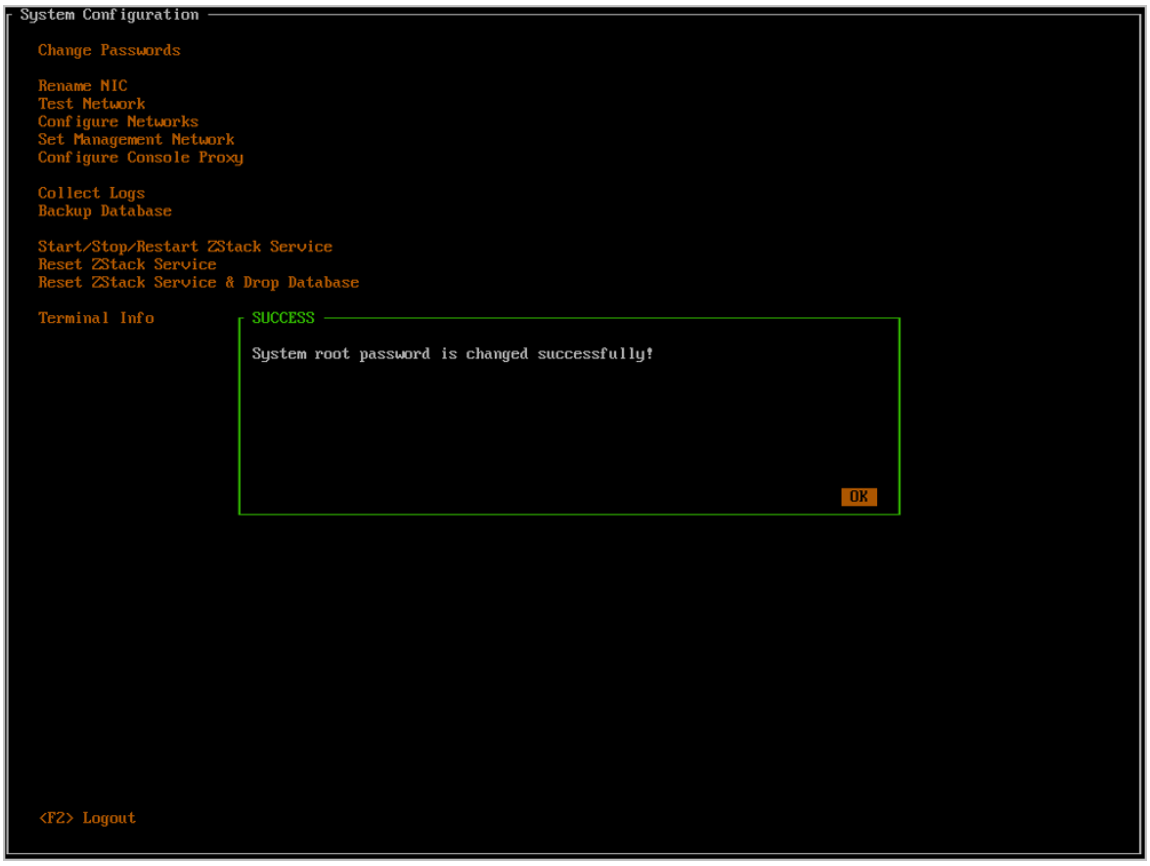
如果旧系统密码不正确、或者密码确认不一致，都会弹出错误窗口，如图 *41:* 错误窗口所示：

图 41: 错误窗口

需要根据提示，按**Y**键以确认，如图 *42: 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 *43: 修改系统root密码成功*所示。

图 42: 修改系统root密码的确认界面

图 43: 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 44: 修改root账号/ZStack账号的MySQL密码*所示：

图 44: 修改root账号/ZStack账号的MySQL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 45: 重命名网卡*所示：

图 45: 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 *46:* 测试网络所示：

图 46: 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 *47:* 配置网络所示：

图 47: 配置网络

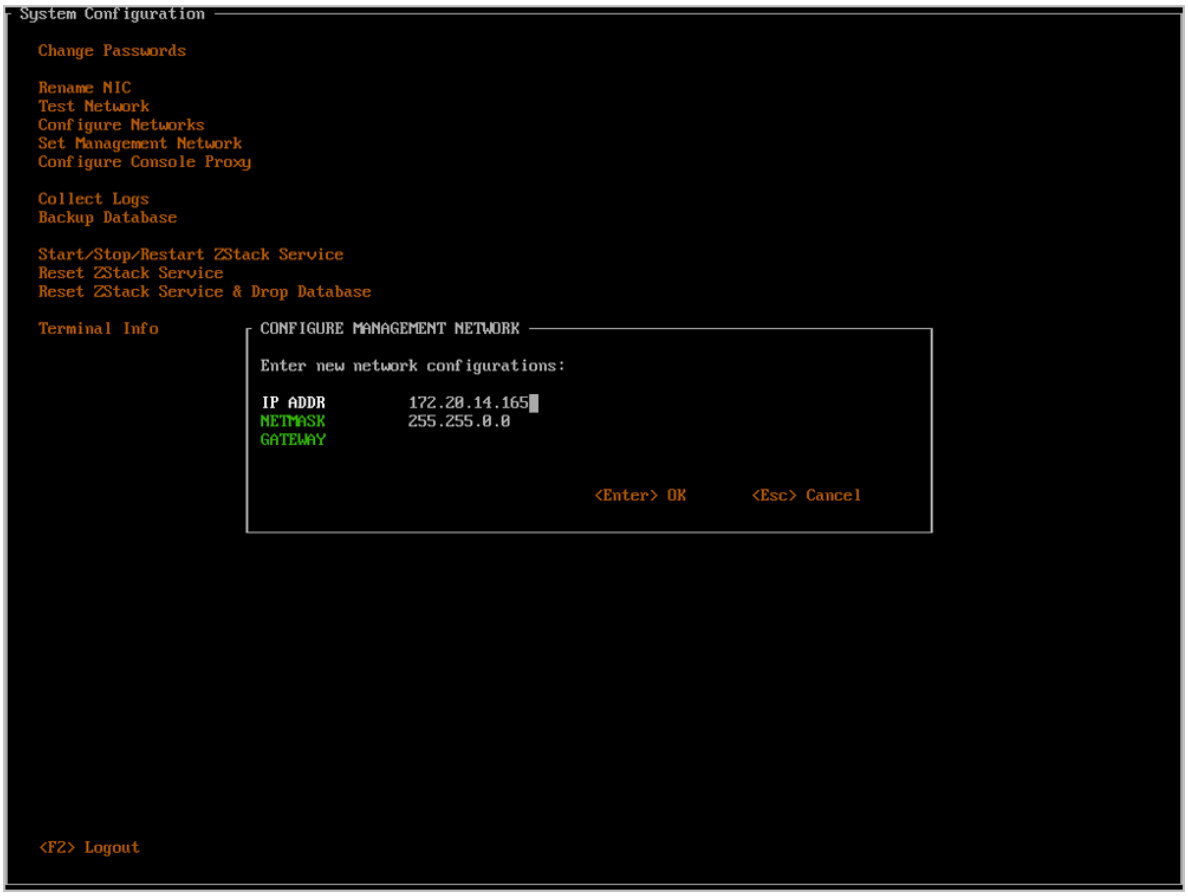
这里罗列了管理节点中所有处于启动状态的网卡，包括物理网卡和逻辑网卡。由于前文已做网卡归一化，这里仅需关心Bond的配置即可。

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 *48:* 填写信息所示：

图 48: 填写信息



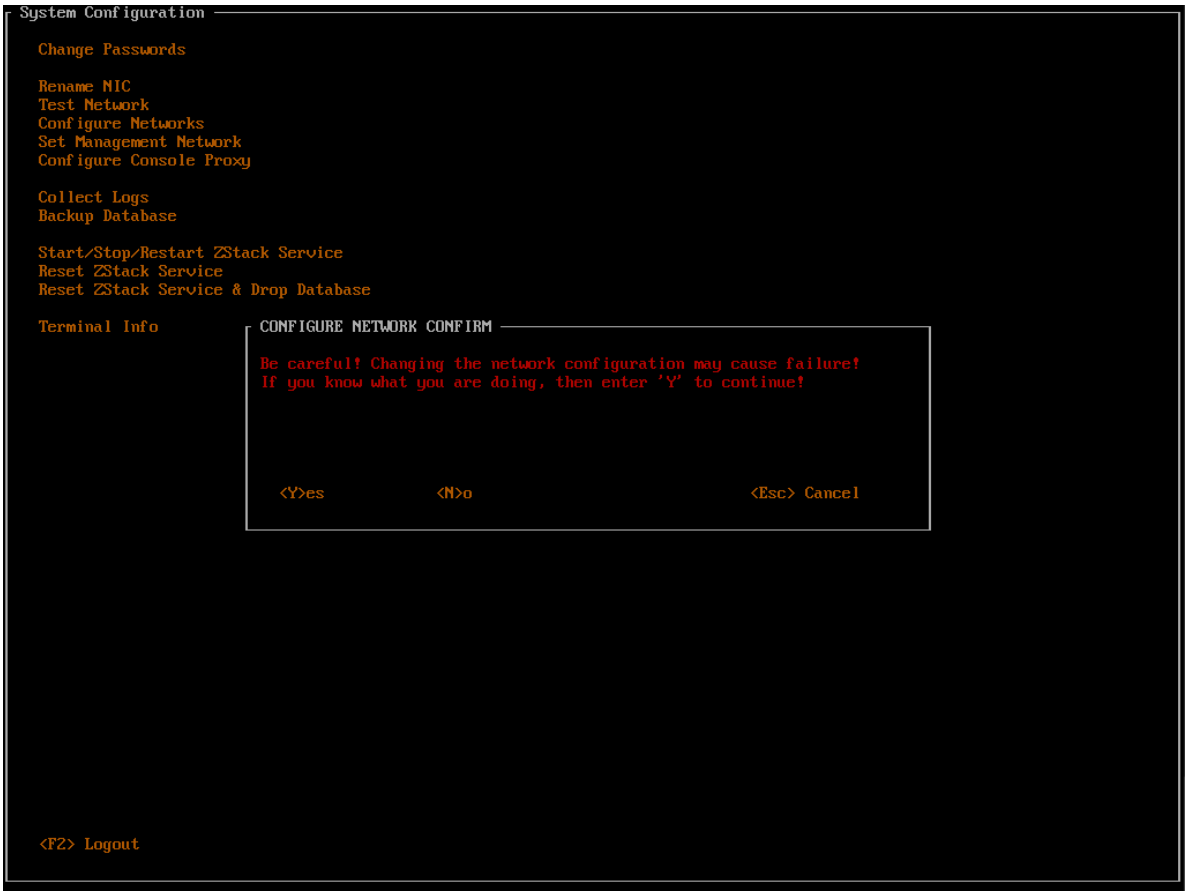
所选Bond设备的已有配置会默认显示在输入框中（网关除外），用户可根据实际情况修改。

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 *49: 确认界面*所示：

图 49: 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。

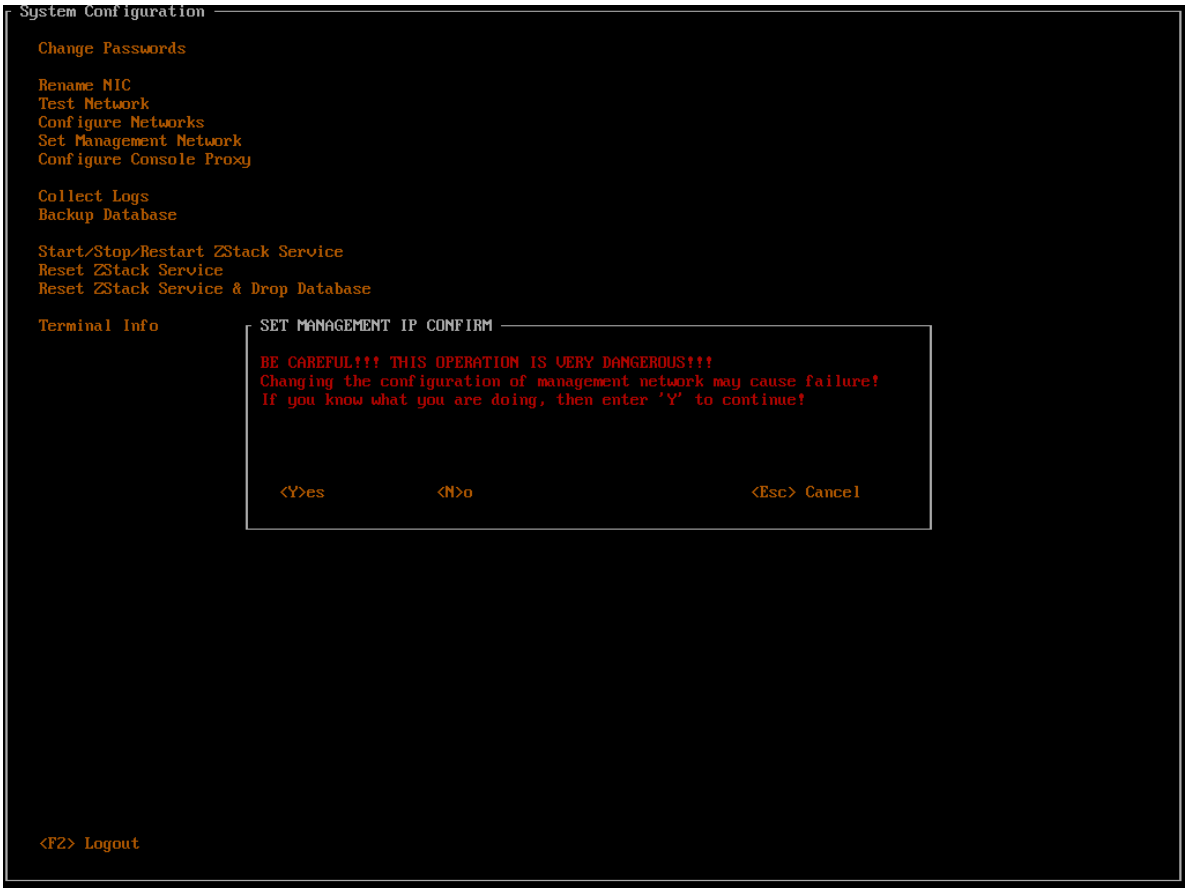
注: 配置管理网络耗时较长，请谨慎操作。

如图 *50:* 配置管理网络所示：

图 50: 配置管理网络

确认界面如图 *51:* 确认界面所示：

图 51: 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；
- 需要用户按**Y**键确认；
- 不支持设置域名。

如图 52: 配置控制台代理所示：

图 52: 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。

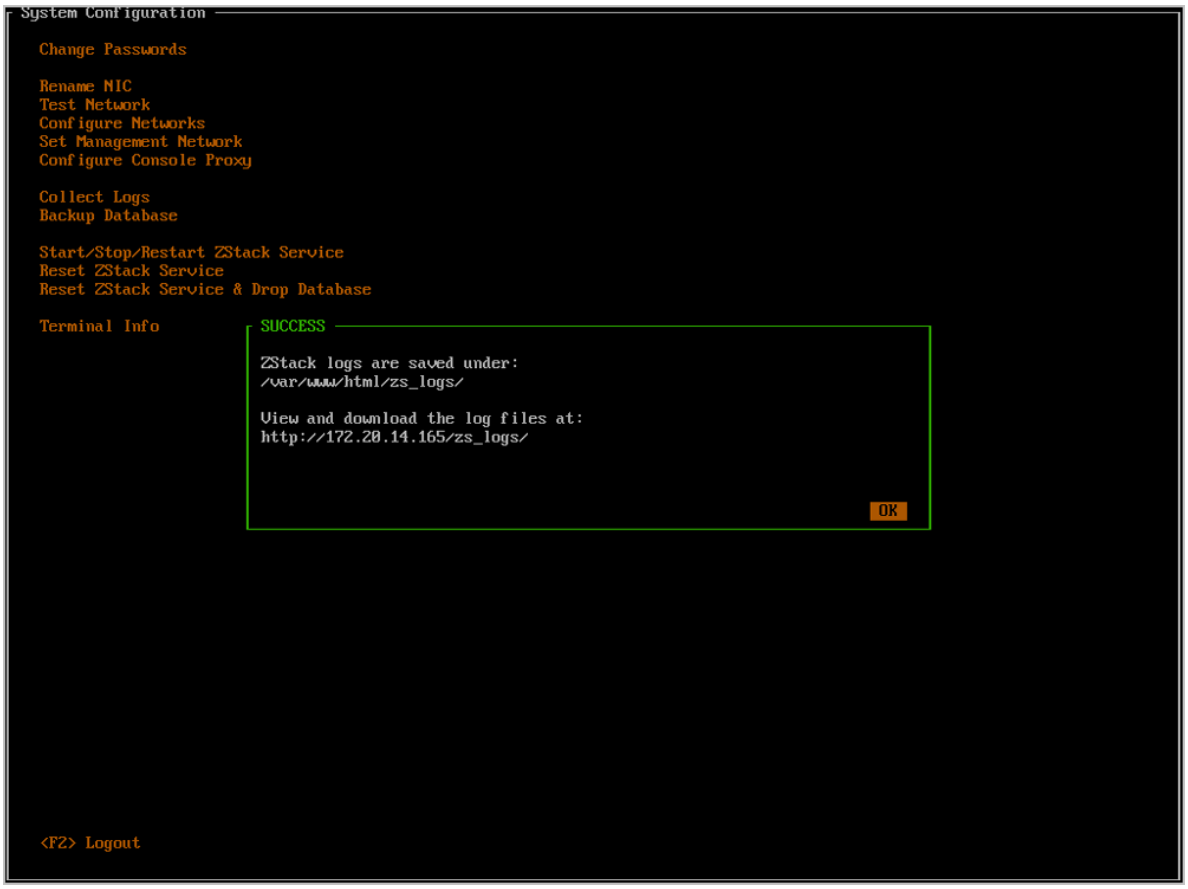
如图 53: 收集日志所示：

图 53: 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 *54:* 日志导出成功所示：

图 54: 日志导出成功

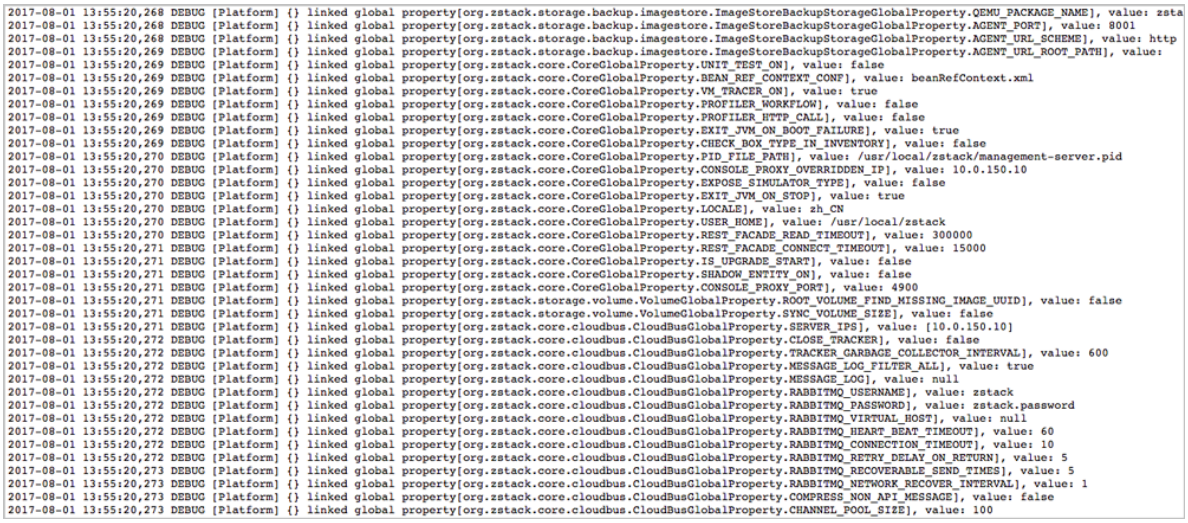


根据提示，用户可以通过浏览器直接访问所有日志内容，支持下载/在线浏览日志。

如图 *55: 导出日志至HTTP服务器中*所示，

图 55: 导出日志至HTTP服务器中

图 56: 在线浏览日志



```
2017-08-01 13:55:20,268 DEBUG [Platform] {} linked global property[org.zstack.storage.backup.imagestore.ImageStoreBackupStorageGlobalProperty.QEMU_PACKAGE_NAME], value: zsta
2017-08-01 13:55:20,268 DEBUG [Platform] {} linked global property[org.zstack.storage.backup.imagestore.ImageStoreBackupStorageGlobalProperty.AGENT_PORT], value: 8001
2017-08-01 13:55:20,268 DEBUG [Platform] {} linked global property[org.zstack.storage.backup.imagestore.ImageStoreBackupStorageGlobalProperty.AGENT_URL_SCHEME], value: http
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.storage.backup.imagestore.ImageStoreBackupStorageGlobalProperty.AGENT_URL_ROOT_PATH], value:
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.UNIT_TEST_ON], value: false
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.BEAN_REF_CONTEXT_CONF], value: beanRefContext.xml
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.VM_TRACER_ON], value: true
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.PROFILER_WORKFLOW], value: false
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.PROFILER_HTTP_CALL], value: false
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.EXIT_JVM_ON_BOOT_FAILURE], value: true
2017-08-01 13:55:20,269 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.CHECK_BOX_TYPE_IN_INVENTORY], value: false
2017-08-01 13:55:20,270 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.PID_FILE_PATH], value: /usr/local/zstack/management-server.pid
2017-08-01 13:55:20,270 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.CONSOLE_PROXY_OVERRIDDEN_IP], value: 10.0.150.10
2017-08-01 13:55:20,270 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.EXPOSE_SIMULATOR_TYPE], value: false
2017-08-01 13:55:20,270 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.EXIT_JVM_ON_STOP], value: true
2017-08-01 13:55:20,270 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.LOCALE], value: zh_CN
2017-08-01 13:55:20,270 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.USER_HOME], value: /usr/local/zstack
2017-08-01 13:55:20,270 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.REST_FACADE_READ_TIMEOUT], value: 300000
2017-08-01 13:55:20,271 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.REST_FACADE_CONNECT_TIMEOUT], value: 15000
2017-08-01 13:55:20,271 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.IS_UPGRADE_START], value: false
2017-08-01 13:55:20,271 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.SHADOW_ENTITY_ON], value: false
2017-08-01 13:55:20,271 DEBUG [Platform] {} linked global property[org.zstack.core.CoreGlobalProperty.CONSOLE_PROXY_PORT], value: 4900
2017-08-01 13:55:20,271 DEBUG [Platform] {} linked global property[org.zstack.storage.volume.VolumeGlobalProperty.ROOT_VOLUME_FIND_MISSING_IMAGE_UUID], value: false
2017-08-01 13:55:20,271 DEBUG [Platform] {} linked global property[org.zstack.storage.volume.VolumeGlobalProperty.SYNC_VOLUME_SIZE], value: false
2017-08-01 13:55:20,271 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.SERVER_IPS], value: [10.0.150.10]
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.CLOSE_TRACKER], value: false
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.TRACKER_GARBAGE_COLLECTOR_INTERVAL], value: 600
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.MESSAGE_LOG_FILTER_ALL], value: true
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.MESSAGE_LOG], value: null
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_USERNAME], value: zstack
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_PASSWORD], value: zstack.password
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_VIRTUAL_HOST], value: null
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_HEART_BEAT_TIMEOUT], value: 60
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_CONNECTION_TIMEOUT], value: 10
2017-08-01 13:55:20,272 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_RETRY_DELAY_ON_RETURN], value: 5
2017-08-01 13:55:20,273 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_RECOVERABLE_SEND_TIMES], value: 5
2017-08-01 13:55:20,273 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.RABBITMQ_NETWORK_RECOVER_INTERVAL], value: 1
2017-08-01 13:55:20,273 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.COMPRESS_NON_API_MESSAGE], value: false
2017-08-01 13:55:20,273 DEBUG [Platform] {} linked global property[org.zstack.core.cloudbus.CloudBusGlobalProperty.CHANNEL_POOL_SIZE], value: 100
```

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。

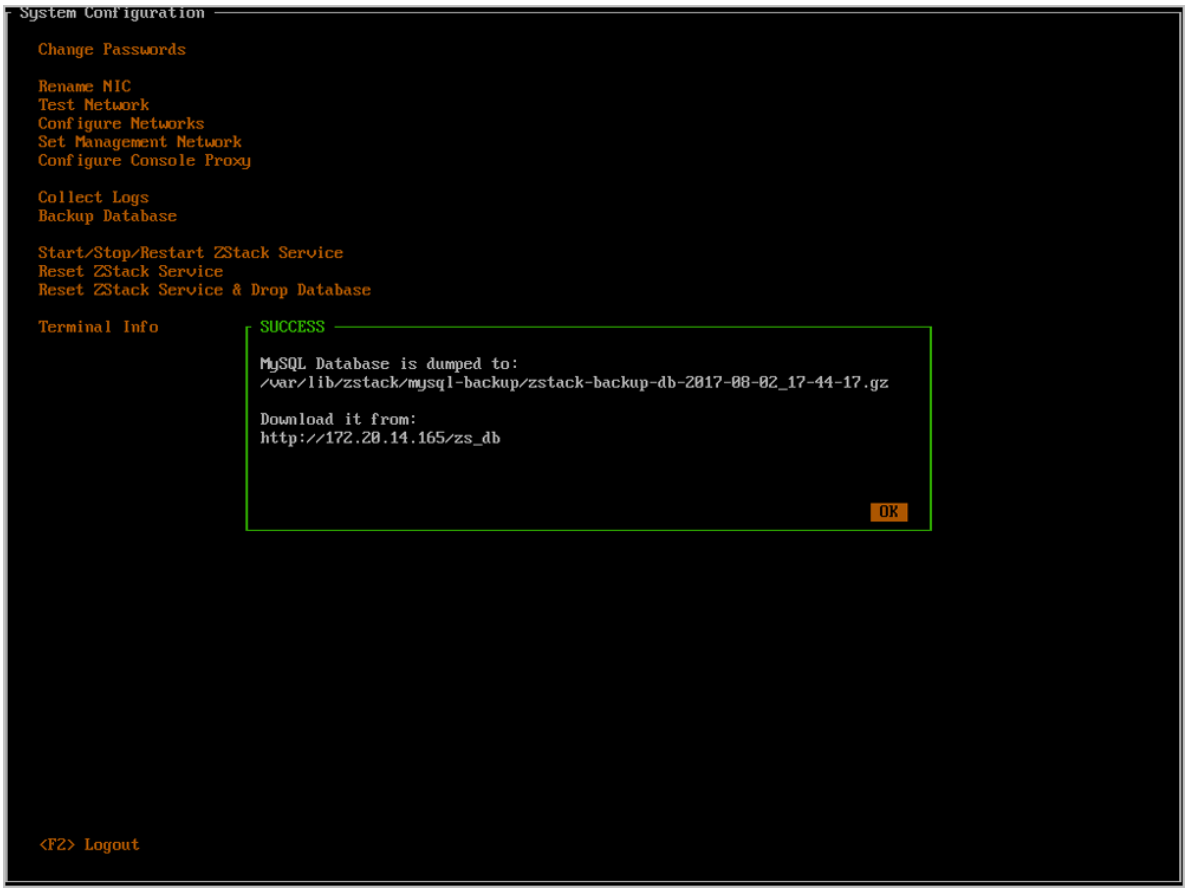
回车即可导出数据库至HTTP服务器中，以供下载。

如图 *57:* 备份数据库和图 *58:* 备份数据库成功所示：

图 57: 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 58: 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 59: 启动/关闭/重启ZStack服务*所示：

图 59: 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 60: 启动ZStack服务*所示：

图 60: 启动ZStack服务

如图 *61: 关闭ZStack服务*所示：

图 61: 关闭ZStack服务

如图 *62: 重启ZStack服务*所示：

图 62: 重启ZStack服务

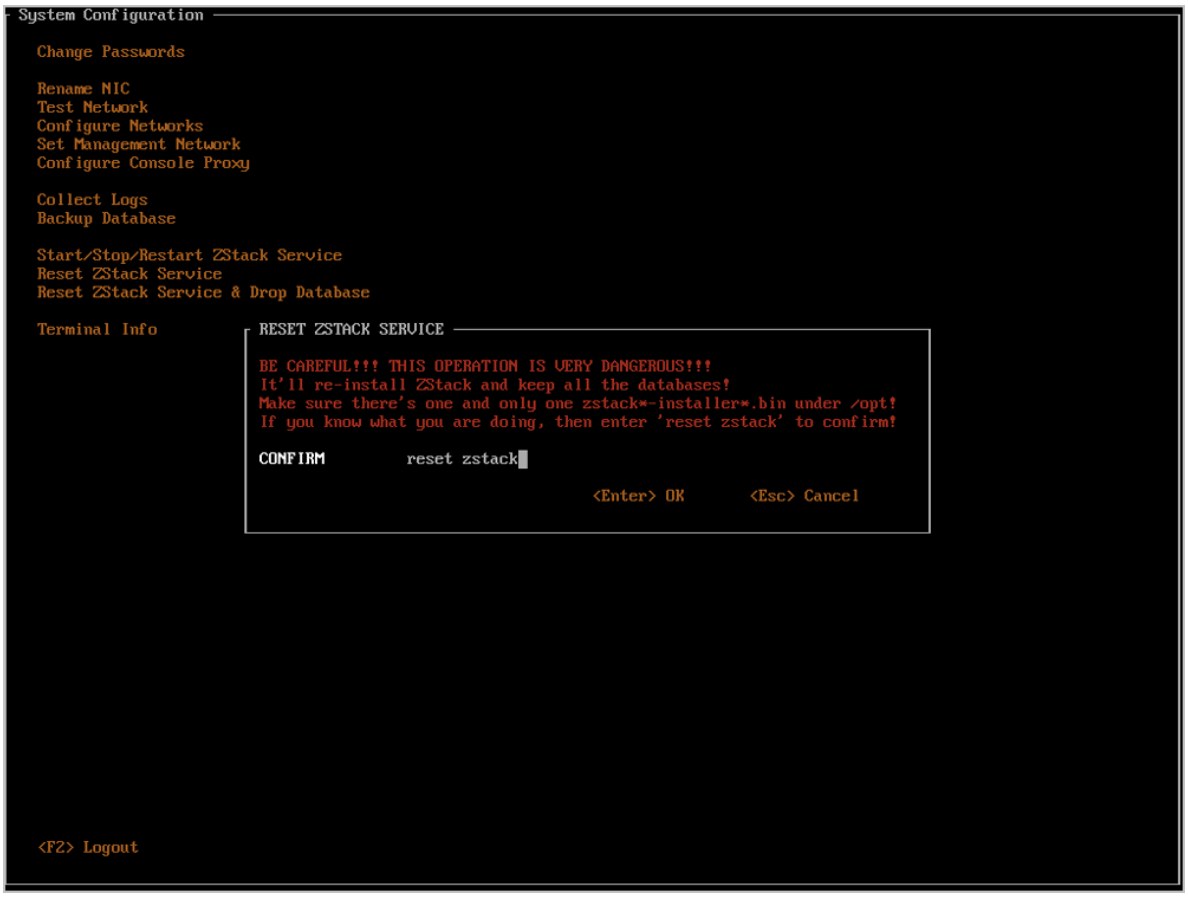
10.重装ZStack服务

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 *63: 重装ZStack服务*所示：

图 63: 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 *64: 重装ZStack服务并删除数据库*所示

图 64: 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 *65:* 进入终端提示所示

图 65: 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 *66:* 重启/关机所示：

图 66: 重启/关机

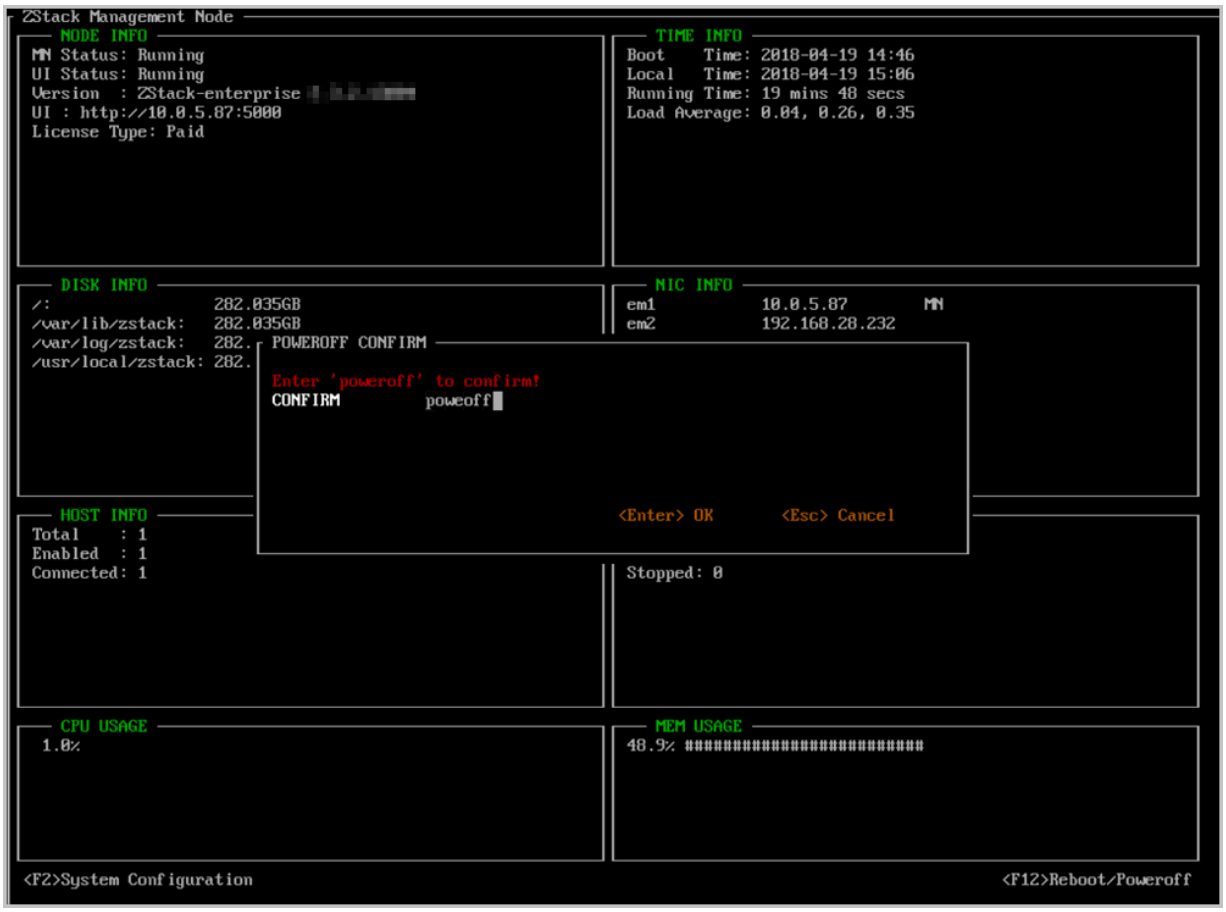
两种操作都需要用户根据提示输入**REBOOT**或**POWEROFF**才可以回车确认，以免误操作。

如图 *67:* 重启确认所示：

图 67: 重启确认

如图 *68: 关机确认*所示：

图 68: 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 *69:* 网卡异常情况处理所示：

图 69: 网卡异常情况处理

```
Try the following steps to install ZStack:
- Make sure at least one NIC is up and have IP
- Check /tmp/zstack_installation.log if it exists
- Run command 'bash /opt/zstack-*installer.bin -E -I NIC_NAME' to install ZStack Enterprise
- Or run command 'bash /opt/zstack-*installer.bin -I NIC_NAME' to install ZStack Community

localhost login:
```

5.2.2 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 *70: 计算节点TUI主界面*所示：

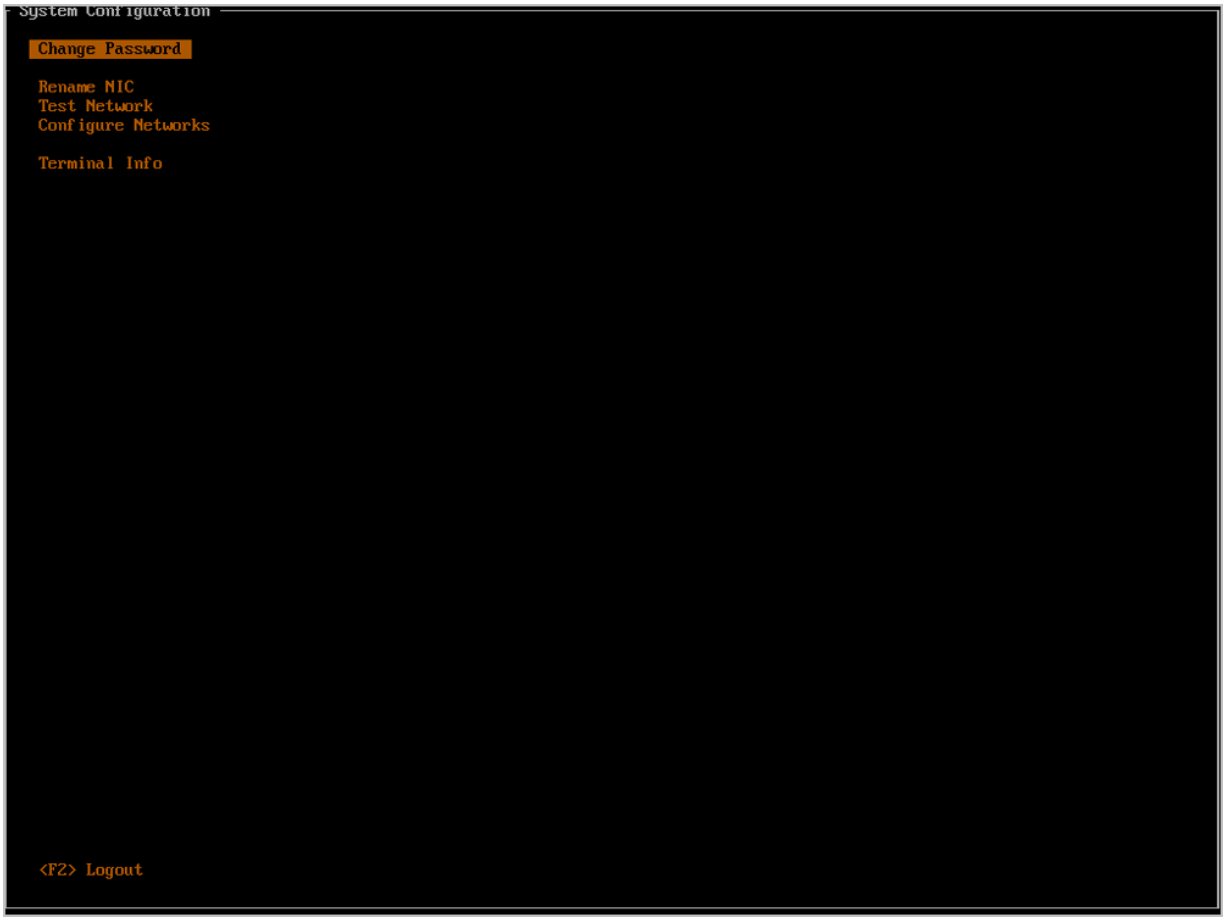
图 70: 计算节点TUI主界面

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 *71: 系统配置*所示：

图 71: 系统配置



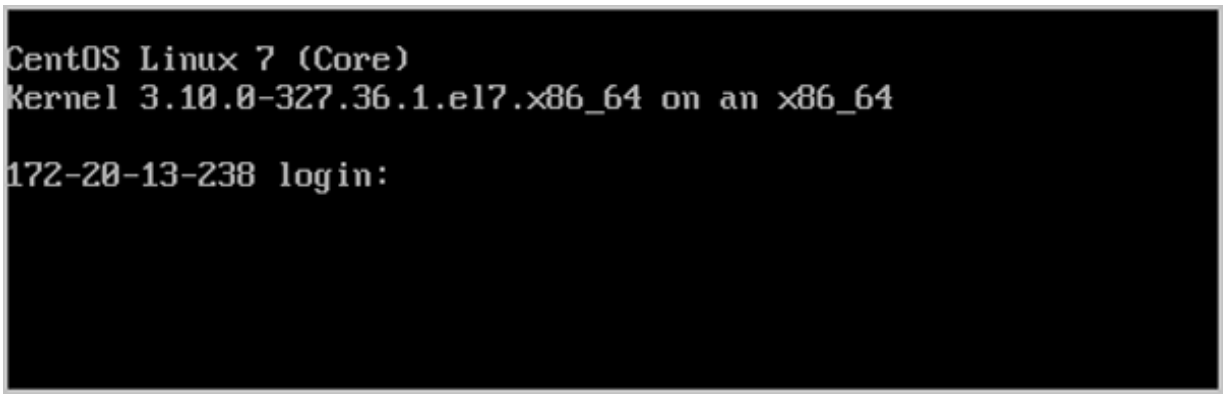
补充说明：管理节点可以添加计算节点的个数在技术上无限制，跟License有关。程序模拟过100万个计算节点。

5.2.3 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 *72: 终端界面*所示：

图 72: 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。

5.3 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
```

5.4 升级ZStack

由于c72 ISO与c74 ISO的升级步骤基本相同，因此以c74版的升级场景为例进行介绍。

- 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-3.1.1.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-3.1.1.bin -u
```

注:

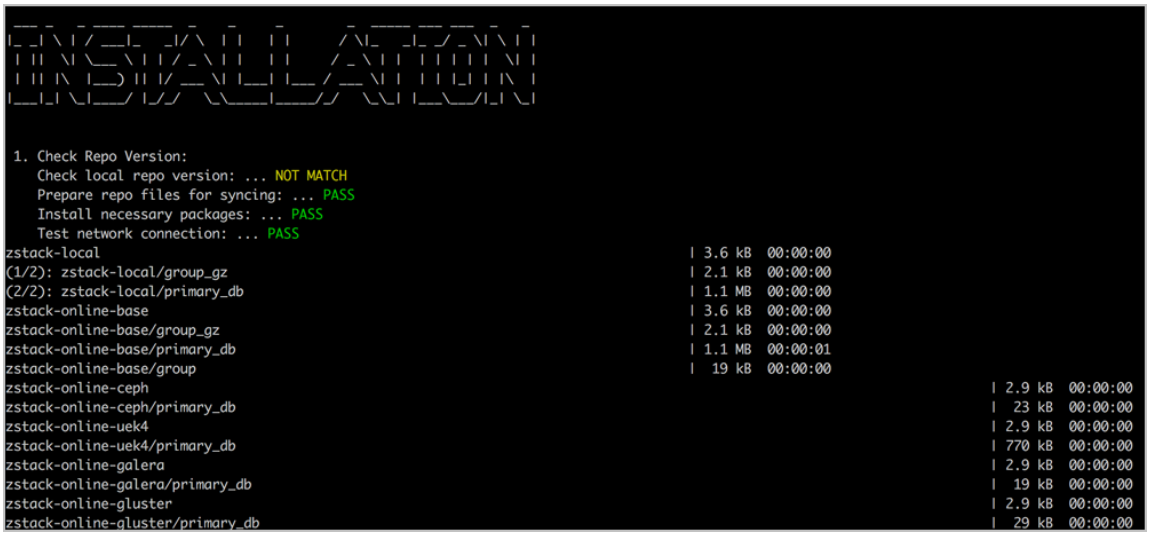
- 若数据库root密码采用系统默认的**zstack.mysql.password**，执行上述命令进行升级即可。
- 若数据库root密码采用自定义非空密码，需执行以下命令进行升级：

```
[root@zstack-1 opt]# bash ZStack-installer-3.1.1.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：

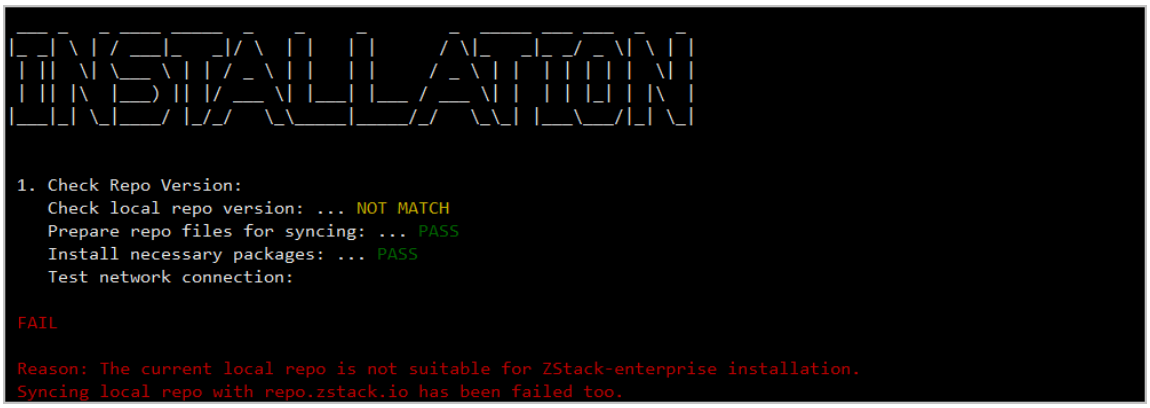
- 如果检测到ISO版本过低，会自动将本地源同步到最新，然后开始ZStack的安装，如*图 73: 自动将本地源同步到最新*所示。

图 73: 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 74: 同步本地源过程中报错*所示。

图 74: 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-3.1.1-c74.iso
     - 下载地址：点击这里
   - ZStack安装包
     - 文件名称：ZStack-installer-3.1.1.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-3.1.1-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-3.1.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-3.1.1.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-3.1.1-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-3.1.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-3.1.1.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 *75: 升级成功*所示：

图 75: 升级成功

5.4.1 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-3.1.1.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-3.1.1.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-3.1.1.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 76: 自动将本地源同步到最新*所示。

图 76: 自动将本地源同步到最新

```
 1. Check Repo Version:
    Check local repo version: ... NOT MATCH
    Prepare repo files for syncing: ... PASS
    Install necessary packages: ... PASS
    Test network connection: ... PASS
zstack-local                                                     | 3.6 kB  00:00:00
(1/2): zstack-local/group_gz                                     | 2.1 kB  00:00:00
(2/2): zstack-local/primary_db                                   | 1.1 MB  00:00:00
zstack-online-base                                               | 3.6 kB  00:00:00
zstack-online-base/group_gz                                      | 2.1 kB  00:00:00
zstack-online-base/primary_db                                    | 1.1 MB  00:00:01
zstack-online-base/group                                         |  19 kB  00:00:00
zstack-online-ceph                                                                   | 2.9 kB  00:00:00
zstack-online-ceph/primary_db                                                        |  23 kB  00:00:00
zstack-online-uek4                                                                   | 2.9 kB  00:00:00
zstack-online-uek4/primary_db                                                        | 770 kB  00:00:00
zstack-online-galera                                                                 | 2.9 kB  00:00:00
zstack-online-galera/primary_db                                                      |  19 kB  00:00:00
zstack-online-gluster                                                                | 2.9 kB  00:00:00
zstack-online-gluster/primary_db                                                     |  29 kB  00:00:00
```

- 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 *77: 同步本地源过程中报错*所示。

图 77: 同步本地源过程中报错

```
 1. Check Repo Version:
    Check local repo version: ... NOT MATCH
    Prepare repo files for syncing: ... PASS
    Install necessary packages: ... PASS
    Test network connection:

 FAIL

 Reason: The current local repo is not suitable for ZStack-enterprise installation.
 Syncing local repo with repo.zstack.io has been failed too.
```

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-3.1.1-c74.iso
  - 下载地址：点击这里
- ZStack安装包

  - 文件名称：ZStack-installer-3.1.1.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-3.1.1-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-3.1.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-3.1.1.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-3.1.1-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-3.1.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-3.1.1.bin -u -P
 MYSQL_ROOT_PASSWORD
```

4. 升级成功界面如图 *78: 升级成功*所示：

图 78: 升级成功

```
 1. Check Repo Version:
    Check local repo version: ... PASS

 2. Check System:
    Pre-Checking: ... PASS
    Check System: ... PASS
    Update Package Repository: ... PASS

 3. Get ZStack-enterprise:
    Download ZStack-enterprise package: ... PASS
    Unpack ZStack-enterprise package: ... PASS

 4. Upgrade ZStack-enterprise:
    Upgrade apache-tomcat: ... PASS
    Upgrade zstack-ctl: ... PASS
    Install General Libraries (takes a couple of minutes): ... PASS
    Stop ZStack-enterprise: ... PASS
    Stop ZStack-enterprise UI: ... PASS
    Upgrade ZStack-enterprise: ... PASS
    Deploy yum repo for ZStack-enterprise: ... PASS
    Add cronjob to clean logs: ... PASS
    Install ZStack-enterprise management node: ... PASS
    Enable ZStack-enterprise bootstrap service: ... PASS
    Enable chronyd: ... PASS
    Config zstack.properties: ... PASS
    Append iptables: ... PASS
    Install ZStack-enterprise management node: ... PASS
    Enable ZStack-enterprise bootstrap service: ... PASS
    Enable chronyd: ... PASS
    Config zstack.properties: ... PASS
    Append iptables: ... PASS
    Install ZStack-enterprise Web UI (takes a couple of minutes): ... PASS
    Upgrade ZStack-enterprise UI Database: ... PASS
    Start ZStack-enterprise management node (takes a couple of minutes): ... PASS
    Start ZStack-enterprise Web UI: ... PASS

ZStack-enterprise in /usr/local/zstack has been successfully upgraded to version: 2.6.0.15142

 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.

 - chrony server sources is set to management node by default.

 Your old zstack was saved in /usr/local/zstack/upgrade/2018-07-30-16-23-54
```

5.4.2 c74版 升级

由于c72 ISO与c74 ISO的升级步骤基本相同，因此以c74版的升级场景为例进行介绍。

- 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-3.1.1.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-3.1.1.bin -u
```

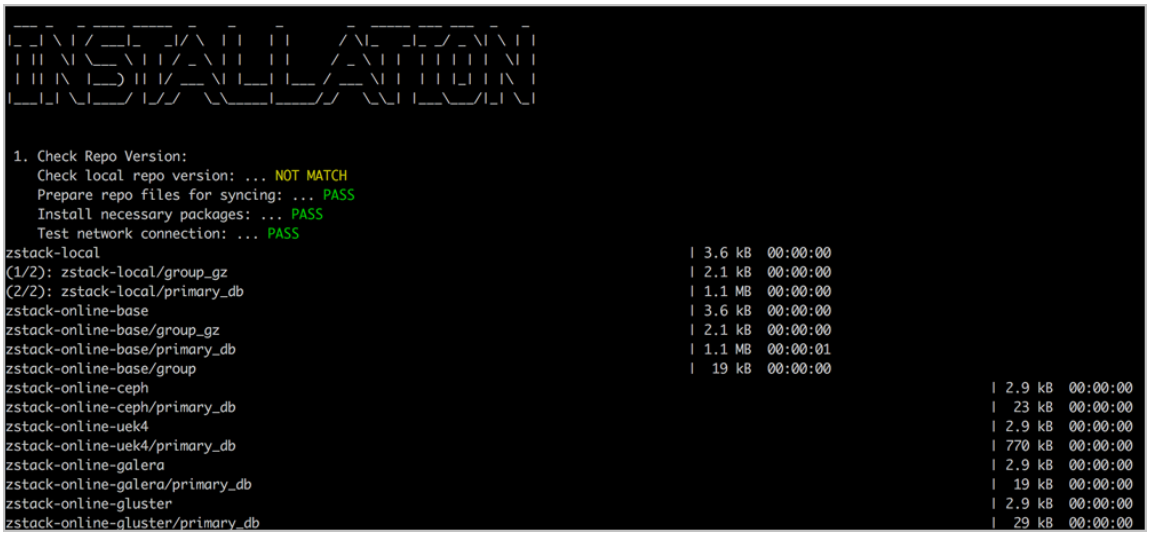
注:

- 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-3.1.1.bin -u -P
 MYSQL_ROOT_PASSWORD
```

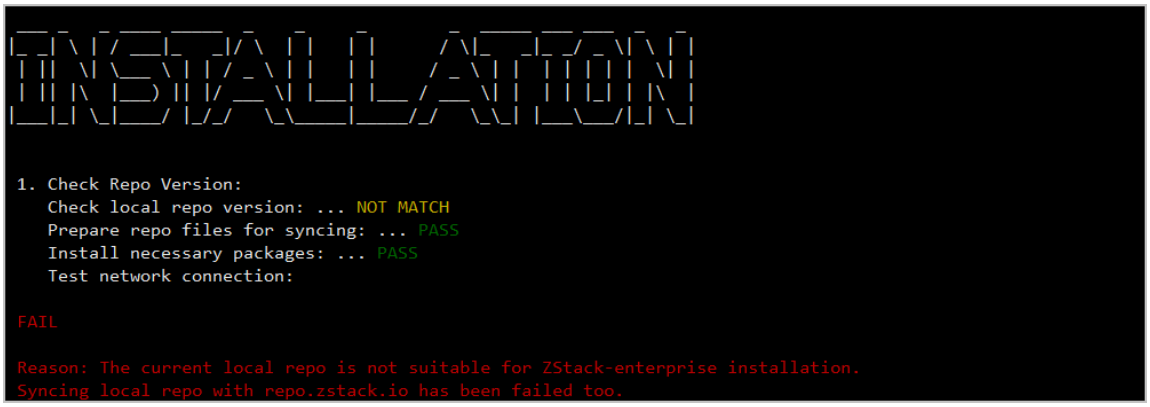
4. 执行升级安装，该安装包会自动检测ISO版本：
   - 如果检测到ISO版本过低，会自动将本地源同步到最新，然后开始ZStack的安装，如图 *79: 自动将本地源同步到最新*所示。

图 79: 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 *80: 同步本地源过程中报错*所示。

图 80: 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-3.1.1-c74.iso
     - 下载地址：点击这里
   - ZStack安装包
     - 文件名称：ZStack-installer-3.1.1.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-3.1.1-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-3.1.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-3.1.1.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-3.1.1-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-3.1.1-c74.iso
[root@zstack-1 opt]# bash ZStack-installer-3.1.1.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 *81:* 升级成功所示：

图 81: 升级成功

```
 1. Check Repo Version:
    Check local repo version: ... PASS

 2. Check System:
    Pre-Checking: ... PASS
    Check System: ... PASS
    Update Package Repository: ... PASS

 3. Get ZStack-enterprise:
    Download ZStack-enterprise package: ... PASS
    Unpack ZStack-enterprise package: ... PASS

 4. Upgrade ZStack-enterprise:
    Upgrade apache-tomcat: ... PASS
    Upgrade zstack-ctl: ... PASS
    Install General Libraries (takes a couple of minutes): ... PASS
    Stop ZStack-enterprise: ... PASS
    Stop ZStack-enterprise UI: ... PASS
    Upgrade ZStack-enterprise: ... PASS
    Deploy yum repo for ZStack-enterprise: ... PASS
    Add cronjob to clean logs: ... PASS
    Install ZStack-enterprise management node: ... PASS
    Enable ZStack-enterprise bootstrap service: ... PASS
    Enable chronyd: ... PASS
    Config zstack.properties: ... PASS
    Append iptables: ... PASS
    Install ZStack-enterprise management node: ... PASS
    Enable ZStack-enterprise bootstrap service: ... PASS
    Enable chronyd: ... PASS
    Config zstack.properties: ... PASS
    Append iptables: ... PASS
    Install ZStack-enterprise Web UI (takes a couple of minutes): ... PASS
    Upgrade ZStack-enterprise UI Database: ... PASS
    Start ZStack-enterprise management node (takes a couple of minutes): ... PASS
    Start ZStack-enterprise Web UI: ... PASS

ZStack-enterprise in /usr/local/zstack has been successfully upgraded to version: 2.6.0.15142

 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.

 - chrony server sources is set to management node by default.

 Your old zstack was saved in /usr/local/zstack/upgrade/2018-07-30-16-23-54
```

6 系统登录

1. ZStack安装部署完毕后，支持HTTP与HTTPS两种方式登录UI管理界面。
2. HTTP方式默认支持5000端口。假定管理节点IP地址为*172.20.1.20*，那么使用UI进行控制的URL需要输入*http://172.20.1.20:5000*
3. HTTPS方式默认不启用。如需启用，详情可参考*HTTPS方式登录UI*章节。
4. 建议使用Chrome或Firefox打开浏览器。
5. 系统首次登录时，默认账户名：admin ，默认初始密码：password。
6. 默认登录时效为2小时，超时需重新登录。超时时间可以在全局设置界面进行配置。
7. ZStack登录方式支持：
   - 账户登录：需输入账户名和账户密码。
   - 用户登录：需输入用户名和用户密码。
   - AD/LDAP登录：需输入登录属性名和AD/LDAP密码。AD/LDAP需提前设置AD/LADP服务器和AD/LDAP账户绑定。

   注: 登录失败需检查管理节点服务，确保管理服务和UI服务均正常运行。

6.1 HTTPS方式登录UI

默认HTTPS方式

以下介绍使用系统默认证书以HTTPS方式登录UI的方法：

1. 在管理节点停止管理节点服务，执行：

```
zstack-ctl stop
```

2. 在管理节点配置证书，执行：

```
openssl pkcs12 -in /usr/local/zstack/zstack-ui/ui.keystore.p12 -out /usr/local/zstack/zstack-ui/ui.keystore.pem -nodes
```

   注: 执行过程中要求输入默认密码：**password**

3. 修改**zstack.properties**配置文件，将证书路径设置为绝对路径：

进入/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties修改**zstack.properties**配置文件，将证书路径设置为绝对路径（绝对路径指向证书私钥密码文件）

```
consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem
```

4. 配置HTTPS UI登录模式：

```
zstack-ctl config_ui --enable-ssl True
```

5. 启动管理节点管理服务，执行：

```
zstack-ctl start
```

自定义HTTPS方式

以下介绍使用自定义证书以HTTPS方式登录UI的方法：

1. 准备好自定义证书，可使用相关工具生成自签证书，也可购买正规CA签发证书。例如使用Keytool（Java数据证书管理工具）生成自签证书，执行：

```
mkdir certs

keytool -genkey -alias tomcat  -storetype PKCS12 -keyalg RSA -keysize 2048 -keystore ./
certs/keystore.p12 -validity 365
```

2. 在管理节点停止管理节点服务，执行：

```
zstack-ctl stop
```

3. 在管理节点配置证书，执行：

```
openssl pkcs12 -in /root/certs/keystore.p12 -out ui.keystore.pem -nodes
```

注: 执行过程中要求输入密码。

4. 修改**zstack.properties**配置文件，将证书路径设置为绝对路径：

进入/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties修改**zstack.properties**配置文件，将证书路径设置为绝对路径（绝对路径指向证书私钥密码文件）

```
consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem
```

5. 配置HTTPS UI登录模式：

```
zstack-ctl config_ui --enable-ssl True \
--ssl-keyalias=tomcat --ssl-keystore=/root/certs/keystore.p12 --ssl-keystore-type=PKCS12 \
```

```
--ssl-keystore-password=password --server-port=8888
```

6. 启动管理节点管理服务，执行：

```
zstack-ctl start
```

恢复HTTP方式

如需取消HTTPS方式，恢复HTTP方式登录UI：

1. 关闭HTTPS UI登录，执行：

```
zstack-ctl config_ui --enable-ssl False
```

2. 重启管理节点服务，执行：

```
zstack-ctl stop_ui
zstack-ctl start_ui
```

7 Wizard引导设置

首次登录ZStack，系统界面将引导进行基本的初始化环境配置。

1. **区域**

   一般对应了数据中心的一个机房。包含集群、二层网络、主存储等资源。

   规划区域时，需注意：

   - 同一个物理二层广播域中的物理主机应该在同一个区域，可被划分为一个或多个集群；
   - 物理二层广播域不应跨域多个区域，应规划为单个区域的二层网络；
   - 同一个主存储不应跨越多个区域。
2. **集群**

   一组物理主机的逻辑集合，一个集群一般对应了一个机架。

   规划集群时，需注意：

   - 本集群内所有的物理主机必须拥有相同的操作系统；
   - 本集群内所有的物理主机必须拥有相同的网络配置；
   - 本集群内所有的物理主机必须能够访问相同的主存储。
3. **物理机**

   为云主机实例提供计算、网络或存储的物理主机。添加物理主机需要输入物理主机的IP、SSH端口、用户名和用户密码。

   添加物理主机时，需注意：

   - 需使用ZStack定制版ISO安装CentOS 7.2或CentOS 7.4系统；
   - BISO需打开Intel VMX或AMD SVM的硬件虚拟化功能；
   - 需确保IP地址、用户名、密码正确；
   - 输入的用户名须拥有sudo权限；
   - SSH端口需开启iptables允许；
   - 管理节点的管理IP需正常访问物理主机的SSH端口以部署软件和代理程序；
   - 物理主机的IP地址需可以访问管理节点的8080端口。
4. **镜像服务器**

   用于保存镜像模板的存储服务器。首次创建云主机/云盘时，镜像模板会下载到主存储的镜像缓存中。

   镜像服务器支持以下类型：

   1. **ImageStore**

      - ImageStore镜像仓库采用内容相联存储的方式，支持在线快照、在线创建镜像、在线克隆等功能。
      - 添加镜像仓库服务器需输入镜像服务器的IP、URL、SSH端口、用户名和用户密码。

        例如：IP为*192.168.0.1*，URL为*/zstack_bs*，SSH端口为22，用户名为root，密码为password。

        表示使用*192.168.0.1*此机器的*/zstack_bs*目录来存储镜像文件。
   2. **Sftp（仅ZStack社区版支持）**

      - Sftp镜像服务器采用文件方式存储镜像文件，支持关机创建快照、支持关机创建镜像等功能。
      - 添加Sftp镜像服务器需输入镜像服务器的IP、URL、SSH端口、用户名和用户密码。

例如：输入IP为*192.168.0.1*，URL为*/zstack_bs*，SSH 端口为22，用户名为root，密码为password

表示使用*192.168.0.1*此机器的*/zstack_bs*目录来存储镜像文件。

3. **Ceph**

- Ceph镜像服务器采用了Ceph集群提供的分布式块存储作为镜像存储。
- 添加Ceph镜像服务器需输入Ceph存储集群的监控节点Mon IP、SSH端口、用户名和用户密码。

  Ceph 存储池名，为可选项，默认会自动创建。如果指定，则需提前在Ceph存储集群自行创建此存储池。

  例如：输入Mon IP为*192.168.0.1*，SSH 端口为22，用户名为root，密码为password。

  表示使用Mon IP为*192.168.0.1*所在的Ceph存储集群来存储镜像文件。

添加镜像服务器，需注意：

- 需确保IP地址、用户名、密码正确；
- 输入的用户名须拥有sudo权限；
- SSH端口需开启iptables允许；
- 针对Sftp或镜像仓库类型，输入的URL对应的目录需提前挂载大容量存储。
- 管理节点的管理IP需正常访问镜像服务器的SSH端口以部署软件和代理程序。
- 镜像服务器的IP地址需可以访问管理节点的8080端口。
- UI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。
- 添加镜像服务器时，默认挂载到了当前区域。
- 在删除区域的同时会直接删除挂载此区域的镜像服务器。

5. **主存储**

用于存储云主机的磁盘文件（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。

主存储支持以下类型：

1. **本地存储**

- 使用各物理主机的本地硬盘上指定的目录作为主存储。
- 所有的物理主机都会使用此目录来存放云主机的磁盘文件。
- 本地主存储容量由各物理主机的主存储目录的容量累加。
- 建议提前对每个物理主机的此目录提前挂载大容量存储。
- 添加本地存储，需输入URL，例如*/zstack_ps*

2. **NFS**

- 使用网络文件系统作为主存储，需提供NFS的共享文件目录。
- ZStack会在所有的物理主机上自动挂载此目录作为主存储。
- 添加NFS主存储的URL格式为*192.168.0.1:/nfs_root*
- 其中*192.168.0.1*为NFS 服务器的IP地址，*/nfs_root*是NFS服务器上可被挂载的目录。
- NFS的挂载目录需提供读写权限。
- NFS的挂载参数，为可选项，需NFS Server端支持，每个参数以逗号隔开。

  例如，输入**nfsvers=3,sec=sys,tcp,intr,timeo=5,**

  表示NFS Server端的版本为3，采用标准的unix验证机制，采用tcp作为传输协议，允许通知中断一个nfs调用，设置超时时间为0.5秒（5/10）。

3. **Shared Mount Point**
   - 采用共享文件系统存储为主存储，支持SAN存储，格式化为MooseFS，GlusterFS，OCFS2，GFS2等文件系统。
   - 需在各物理主机提前挂载各挂载点，挂载到相同目录。
   - 添加Shared Mount Point主存储时，需输入共享文件系统存储挂载到物理主机的本地目录，例如*/mnt/nfs*
4. **Ceph**
   - 使用Ceph集群提供的分布式块存储作为主存储。
   - 关闭CEPHX，可选项代表关闭Ceph密钥认证，如果存储节点和计算节点的网络较安全，可关闭此项，以避免Ceph使用时的认证失败错误。
   - 如果指定了镜像缓存、根云盘、数据云盘的Ceph存储池名，则这些存储池需提前在Ceph集群自行创建。
   - 镜像缓存、根云盘、数据云盘的Ceph存储池名，为可选项，默认会自动创建。如果指定，则需提前在Ceph存储集群自行创建此存储池。
   - 添加Ceph主存储需输入与Ceph镜像服务器同一存储集群的监控节点Mon IP、SSH端口、用户名和用户密码。

     例如：输入Mon IP为*192.168.0.1*，SSH端口为22，用户名为root，密码为password

     表示使用Mon IP为*192.168.0.1*所在的Ceph存储集群来存储镜像文件。
5. **Shared Block**
   - 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。
   - 勾选清理块设备后将强制清理块设备中的文件系统、RAID或分区表中的签名，请谨慎选择。
   - 支持添加一个或多个共享块设备，支持追加共享块设备，但目前不支持删除共享块设备。

添加主存储，需注意：

- 主存储与镜像服务器的依赖关系：
  - 如果镜像服务器使用了ImageStore镜像仓库类型，那么主存储可以使用本地存储、NFS、Shared Mount Point、Ceph、Shared Block类型。
  - 如果镜像服务器使用了Sftp类型，那么主存储可以使用本地存储、NFS、Shared Mount Point类型。
  - 如果镜像服务器采用了Ceph，那么主存储也需使用同一个Ceph集群做镜像存储。
  - 如果类型不匹配，系统会提示当前选择的主存储与镜像服务器不匹配。
- 需确保相应的URL、IP地址、用户名、密码正确；
- 输入的用户名须拥有sudo权限；
- 相应的端口需开启iptables允许；
- 针对本地存储或Shared Mount Point存储，输入的URL对应的目录需提前挂载大容量存储。
- NFS或者Shared Mount Point提供的目录需提供读写权限。
- 管理节点的管理IP需正常访问Ceph Mon IP的SSH端口以部署软件和代理程序。
- Ceph Mon IP的IP地址需可以访问管理节点的8080端口。

6. **计算规格**

   用于定义云主机的CPU、内存、磁盘带宽、网络带宽的数量或大小规格。

   使用计算规格，需注意：

   - 当创建虚拟机时，ZStack会根据选择的计算规格，来指定此云主机的CPU数量、内存大小、磁盘或网络带宽的规格定义。

- 内存大小不能小于16M，否则计算规格会添加失败。因为主流操作系统（例如Linux）需要的最小内存为16M。
- 磁盘带宽、网络上下行带宽均为可选项，代表不做限制，如果限制带宽，则需注意不可过低，否则会导致云主机不能正常工作。
- 首次创建，可按照默认的1CPU、1G内存来配置。

7. **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，在首次创建云主机/云盘时下载到主存储上作为镜像缓存使用。

- 平台类型（Platform）：

  决定创建虚拟机时是否使用KVM virtio驱动（包括磁盘驱动和网卡驱动）。

  - Linux：使用virtio驱动。
  - WindowsVirtio：使用virtio驱动。请确保镜像的Windows操作系统里已安装了virio-disk和virtio-network驱动。
  - Paravirtualization：使用virtio驱动。镜像的操作系统可以是安装了virtio驱动的任何操作系统。
  - Windows：不使用virtio驱动。镜像操作系统是未安装virtio的Windows。
  - Other：不使用virtio驱动。镜像操作系统可以是任何操作系统。
- URL：

  URL支持以下两种格式：

  1. HTTP/HTTPS URL，ZStack会使用wget下载该镜像。

     例如：*http://cdn.zstack.io/product_downloads/images/zstack-image.qcow2*
  2. 镜像服务器的绝对路径。可以先手动将镜像放到镜像服务器的某个目录，再指定添加。

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

添加镜像，需注意：

- 输入的URL需可被镜像服务器访问，且存在此镜像文件。
- 如果镜像文件比较大，下载的时间会比较长，请耐心等待。
- 建议在本地数据中心搭建一个HTTP服务器保存常用的镜像，可获得较快的镜像下载速度。
- 使用file格式添加镜像，暂不支持Ceph镜像服务器。
- 已安装Qemu guest agent选项，勾选表示待添加的镜像已安装了Qemu guest agent，创建出的云主机默认支持在线修改密码功能。

8. **二层网络**

二层网络对应了二层广播域，进行二层相关的隔离，一般以设备编号进行识别。

在初始化引导时，支持选择以下类型 ：

- **L2NoVlanNetwork**
  - L2NoVlanNetwork类型表示相关的物理主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。
  - 创建二层网络，会根据输入的网络设备号创建网桥设备。
- **L2VlanNetwork**
  - L2VlanNetwork类型表示相关的物理主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。

  - 此类型需在物理主机接入的交换机端进行Trunk设置。
  - 创建二层网络，会根据输入的网络设备号创建VLAN设备，并基于此VLAN设备创建网桥。
  - 例如输入eth0， VLAN 10会创建eth0.10设备，并基于此设备创建网桥。

添加二层网络，需注意：

- NovlanNetWork和VlanNetwork作为一组物理定义的二层网络，主要差异在于是否支持VLAN，在添加时，指定的是网卡设备编号，与物理主机网卡端口在交换机端的设置应相同。
- 添加二层网络 会检查集群内的物理主机是否存在此网络设备，如果不存在将会添加失败。

9. 三层网络

定义了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。

- 三层网络属于二层网络的子资源，创建时默认选择了已创建的二层网络。
- 初始化界面的网络配置默认采用扁平网络，可实现云主机和物理主机直接互通。
- 网络服务会根据选择的扁平网络，配置DHCP、弹性IP、安全组、UserData等网络服务。
- 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。
- 添加三层网络的网络段可使用IP范围和CIDR（无域间路由）两种方式：
  - IP范围的添加可指定*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*。
  - CIDR无域间路由可以使用，例如*192.168.1.0/24*。
- DNS用于设置云主机网络的DNS解析服务，例如指定*114.114.114.114*。

8 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。
- **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。
- **计算、存储、网络、平台的资源可用性统计**

  通过对当前区域（或所有区域）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。

首页右上方从左到右的功能按钮依次为：产品与服务快速入口、区域切换、大屏监控入口、报警消息、操作日志、帮助信息、个人中心。

- **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。
- **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界面，对所有区域的数据中心实时资源状态进行统一直观展示。
- **报警消息**：可查看最新报警消息。
- **操作日志**：可查看最近的进行中操作日志和已完成操作日志。
- **帮助信息**：可选择进入**常见问题解答**界面或**关于**界面。
  - **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，详情可参考关于章节。
- **个人中心**：支持对当前账户进行修改密码、UI界面语言切换和登出操作。

8.1 大屏监控

ZStack支持数据中心大屏监控特性。大屏监控主要分为四大部分：

- 左侧：Top5云主机CPU负载、Top5云主机内存负载、Top5物理主机CPU负载、Top5物理主机内存负载

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。

- 中间上侧：总物理主机的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。

- 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。

- 下侧：云主机、物理主机、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。

- 右上侧：大屏切换

  ZStack大屏支持根据不同的虚拟化和区域显示，通过右上角下拉框进行选择切换虚拟化或区域，分别展示不同的大屏监控。

  - 支持切换KVM或vCenter虚拟化
  - 支持切换所有区域或某个区域

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。

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。

8.2 关于

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 *82: 个人中心*所示，在UI界面右上角点击**个人中心** > **关于**，展开**关于**界面，如图 *83: 关于界面*所示：

图 82: 个人中心

图 83: 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：VMware管理模块、迁移服务模块、企业管理模块、灾备服务模块、裸金属管理模块许可证。

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。

基本类型	授权协议	授权协议说明
	混合云版	• ZStack和阿里云联合推出的ZStack for Alibaba Cloud，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**）	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。
	迁移服务	• 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提供V2V迁移功能，将其他虚拟环境的云主机系统及数据完整迁移至当前云平台； • 在售后服务期内可获得官方售后技术支持服务。
	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。
	灾备服务	• 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；

基本类型	授权协议	授权协议说明
		• 在许可证授权期限内提供云主机数据在线备份到备份服务器。支持本地备份、异地备份和混合云备份多种场景，数据更可靠 。 • 在售后服务期内可获得官方售后技术支持服务。
	裸金属管理	• 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提供指定数量的专属物理服务器，保证核心应用的高性能和稳定性。 • 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。

加载许可

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 *84:* 本地上传许可证所示：

图 84: 本地上传许可证

注:

- 支持统一/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 *85:* 许可证即将过期所示：

  图 85: 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 *86:* 许可证已过期所示：

图 86: 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。

9 云资源池

9.1 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。

创建云主机最重要的三个输入

1. **计算规格**：

   用于确定云主机的CPU、内存大小，在分配资源前，ZStack会筛选拥有这些资源的物理主机作为候选来创建云主机。

2. **镜像**：

   用于确定使用哪个镜像来创建云主机。

   选择镜像时：

   - 假如此镜像对应的镜像服务器为ImageStore镜像服务器，则ZStack会自动选择那些挂载了本地存储、NFS、SharedMountPoint、Ceph、Shared Block主存储的集群作为备选集群。
   - 假如此镜像对应的镜像服务器为Sftp镜像服务器（仅社区版支持），则ZStack会自动选择那些挂载了本地存储、NFS、SharedMountPoint主存储的集群作为备选集群。
   - 假如此镜像对应的镜像服务器为Ceph镜像服务器，则ZStack会自动选择挂载了此Ceph镜像服务器对应的Ceph主存储的集群。

3. **网络**：

   用于指定云主机的网络。在选择镜像后，待创建的云主机的可用集群已经确定下来，ZStack会根据此集群挂载的网络来提供可选网络。

注:

- 在确定完毕以上输入后，创建此云主机需要的各种资源已经确定，此时可选的资源被筛选为：使用此镜像对应的镜像服务器，接着根据此镜像服务器可选择的集群，根据此集群确定的相关网络。
- 如果有满足条件的多个集群挂载已选择的网络，那么高级选项还可以继续筛选相应的集群、主存储、物理主机等资源。

创建云主机的多主存储分配策略

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。

云主机相关操作定义

- 启动：

  启动云主机，将停止状态的云主机启动起来，使其正常运行。云主机启动默认会使用上次所在的物理主机启动。

  注意以下几种场景：

场景	云主机启动
此云主机所在集群只挂载了本地存储（一个或多个）	此云主机只能在上次所在的物理主机上启动
此云主机所在集群只挂载了共享存储（一个或多个，目前支持多个NFS主存储或多个Shared Block）	此云主机可在使用此主存储的可用物理主机上启动
此云主机所在集群挂载了不同类型的主存储（目前支持1个LocalStorage + 1个NFS、1个LocalStorage + 1个SMP、1个LocalStorage + 1个Shared Block）	**1.** 如果此云主机使用了本地存储的根云盘或数据盘，则此云主机只能在上次所在的物理主机启动 **2.** 如果此云主机只使用了共享存储（也可带数据云盘），则此云主机可在使用此主存储的可用物理主机上启动

启动云主机失败，需检查以下资源：

- 其所在集群内是否有物理主机连接并启用，如果没有可用连接的物理主机，会提示找不到可用物理主机；
- 其所在集群内物理主机的资源（CPU、内存）是否充足，如果所有的物理主机各自可用的CPU、内存资源不足以支持此云主机的CPU 内存大小，则会提示找不到可用物理主机；
- 其所在集群是否挂载了二层网络，如果集群未挂载二层网络，则此云主机上也不会存在三层网络，则会提示此云主机无网络，无法启动；
- 其所在集群对应的二层网络是否存在三层网络，如果此集群挂载的二层网络均无三层网络，则此云主机上也不会存在三层网络，则会提示此云主机无网络，无法启动；
- 其所在集群是否挂载了主存储，如果集群未挂载主存储（一般发生在卸载主存储后），则会提示此云主机的根云盘文件找不到，需挂载回原本的主存储才可正常启动；
- 其所在集群的主存储可用容量是否充足（创建云主机时判断），如果主存储无法提供云主机需要的容量，则会提示容量不足。

- 停止：

  停止云主机，将运行状态的云主机停止起来，使其正常关机。

- 重启：

  重启云主机，将运行状态的云主机重新启动，重启过程中会更新其全部配置（包括启动顺序、控制台密码、控制台模式、USB设备重定向、屏幕数量控制）。

- 关闭电源：

  关闭电源，将运行状态的云主机直接断电，强制关闭，此操作存在丢失数据的风险，需谨慎操作。

- 暂停：

  暂停云主机，云主机继续消耗内存或资源，但是暂时不调度hypervisor，可以恢复到运行状态，也可删除。

- 恢复（Resume）：

  从暂停状态恢复正常运行，云主机内可继续运行。

- 删除（destroy）：

  如果云主机运行状态，则将其关闭电源并置为已删除状态；如果云主机处于其他状态，则将其直接置为已删除状态。

- 恢复（Recover）：

  将VM从已删除状态恢复为停止状态。

- 彻底删除：

  彻底删除，会将云主机从ZStack彻底移除，并且移除根云盘真实占用的存储空间。

- 打开控制台：

  通过VNC方式访问云主机，要求浏览器所在电脑可以访问控制台代理IP。如果打开控制台返回成功，但是无内容，需确保控制台代理指定的IP地址可以被用户的客户机（笔记本电脑）正常访问，如有必要，需修改控制台代理IP，并重启MN服务 。

  注:

  修改步骤如下：

  - **命令行方式**：

    1. 修改*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties*中的**consoleProxyOverriddenIp**为外部可访问的IP地址。
    2. 重启管理节点服务：`zstack-ctl restart_node`

  - **UI方式**：

    1. 在**平台管理** > **控制台代理**页面手动修改。

- 本地存储迁移：

  主要是指冷迁移，主要迁移根云盘或数据云盘，冷迁移前需卸载相关的数据云盘。

  本地存储也支持热迁移，需全局打开支持，且Windows云主机不支持，本地存储在热迁移前也需要先卸载数据云盘。

- 网络共享存储迁移：

  为在线实时迁移，主要拷贝内存及CPU相关寄存器状态，支持跨集群迁移，只需目的集群与原本集群均挂载云主机使用的网络和主存储，多个不同主存储的情况下，加载了不同类型存储后，需要卸载云盘后才可迁移。

- 创建镜像：

  将云主机封装成镜像，可以使用此镜像再创建更多云主机。

  - 在线创建：云主机运行时，镜像仓库和Ceph镜像服务器支持在线创建镜像。
  - 关机创建：云主机关机后，各种镜像服务器均支持创建镜像。

- 创建快照：

  针对根云盘或数据云盘在指定的时间点创建的数据映像，可以在数据丢失时，有效恢复数据。

  - 在线快照：云主机运行时，镜像仓库和Ceph镜像服务器支持增量快照备份。
  - 关机快照：云主机关机后，各种镜像服务器均支持创建快照。
- 恢复快照：

  将云主机恢复至当前快照点，云盘内相关的数据会恢复至快照点。恢复快照前，需提前备份云盘数据。
- 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。

  - 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。但在线克隆不保证时序一致性，推荐暂停/关机克隆。
    - Shared Block类型的主存储，支持暂停/关机克隆。
- 创建灾备数据：将本地云主机备份到异地或公有云的灾备服务器中，云主机备份为镜像。
- 创建云盘：

  从云主机所属集群已挂载的主存储创建数据云盘。

  在多主存储的情况下，可指定主存储来创建云盘。

  - 针对多个本地主存储，默认会选择可用容量大的存储来创建；
  - 针对多个NFS主存储或多个Shared Block主存储，默认会随机选择主存储来创建；
  - 针对本地主存储+NFS/Shared Mount Point/Shared Block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。

  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/卸载云盘：

  - 加载云盘：可选择云主机所属集群已挂载的主存储上可用云盘来加载。

  - 卸载云盘：将云盘从云主机卸载，本地存储冷迁移和存储迁移，需要先卸载相关数据云盘。
- 云盘扩容：

  云主机停止后可按需进行数据云盘扩容，更改容量将在启动云主机后生效。数据云盘扩容容量只增不减。
- 创建云盘镜像：

  将云盘封装成镜像，可以使用此镜像再创建更多云盘，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。
- 加载ISO/卸载ISO：
  - 加载或卸载ISO，需要提前添加ISO镜像，加载ISO镜像后，可在云主机内识别并加载。
  - 如果打算进行系统修复或系统重新安装，可以加载ISO，调整启动顺序以ISO优先，并重启云主机，用ISO引导系统。
  - 支持加载多个ISO，最多支持加载3个，不支持批量加载。
- 加载SSH Key/删除SSH Key：

  SSH Key注入需注意：

  - SSH Key注入需要云主机提前安装cloud-init，CentOS可执行yum install cloud-init来安装Cloud-init，输入指定主机的对应用户的公钥，公钥由ssh-keygen生成，存放在*~/.ssh/id_rsa.pub*。
  - 安装cloud-init后，ssh密码认证默认关闭，需将*/etc/cloud/cloud.cfg*的ssh_pwauth选项设置为**1**才能开启。
  - 添加SSH Key时，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， 以清理先前配置并重启云主机。
  - 删除SSH Key只删除系统中记录的SSH Key信息，并不从云主机中删除相关的Key信息，并不移除已经生效的Key，如果需要再次注入，需手动清理*/var/lib/cloud/instances*里面的信息，如果需要删除已经生效的Key，则需手动清理云主机里*~/.ssh/authorized_keys*的Key。
- 设置高可用：

  设置为NeverStop的云主机在资源允许的条件下永不停机。

  - 如果云主机的云盘使用了本地存储，在其物理主机异常关机后，此云主机不能再次启动，直到物理主机恢复可用连接状态。

  - 如果云主机的云盘使用了共享存储，则在资源可用的情况下，云主机会始终保持开机，即使停止也会再次启动，假定其所在物理主机异常断电关机，此云主机也会在其他可用物理主机再次启动。
  - NeverStop云主机可设置本次关机不自动启动。
  - NeverStop云主机恢复过程在UI界面上支持展示。
- 修改计算规格/修改CPU、内存：

  修改云主机的CPU、内存、磁盘QoS、网络QoS等。

  - 在线修改：需全局开启NUMA模式，再重启或者新建的云主机才能生效。不支持在线修改Windows云主机的计算规格。在线修改计算规格，只能增加CPU、内存的配置，不能降低配置。
  - 关机修改：云主机关机后，可修改云主机的配置信息。
- 设置启动顺序：

  在加载ISO后，修改云主机的启动顺序，可用于系统修复或系统重新安装，设置启动顺序以CdRom优先，需重启云主机生效，只生效一次，下次再重启后会默认再从硬盘引导。用户在第一次创建云主机选择ISO进行安装时，无需选择启动顺序，系统会自行从ISO引导。
- 启动（指定物理主机）：

  从可用的物理主机列表选择指定的物理主机来启动云主机，适用于共享存储。使用本地存储的云主机，只能使用根云盘所在的物理主机启动。
- 设置控制台密码/取消控制台密码：

  设置控制台密码后，打开VNC控制台则需要正确输入控制台密码后才可访问控制台。取消控制台密码后，访问此云主机的控制台则无须输入密码。设置和取消控制台密码需要云主机重启（靠ZStack重启）才会生效。
- 重置云主机：

  将停止状态的云主机恢复到镜像模板的初始状态，云主机内目前已修改的数据会被擦除。重置云主机前，需提前备份云盘数据。
- 更改所有者：

  变更云主机的所有者给其他普通账户。
- 设置RDP模式：

  设置VDI场景下的RDP模式，默认以RDP模式打开控制台，设置后立刻生效。

- USB重定向

  USB重定向主要用于VDI，将客户端插入的USB设备重定向至云主机，修改后，需重启生效。
- QGA选项：

  开启前需确保云主机已安装并运行qemu-guest-agent；开启后云主机默认支持在线修改密码。
- 在线修改密码：

  需要打开QGA选项，且云主机需安装并运行qemu guest agent，支持Linux和Windows云主机，需确保输入的用户名已存在。
- 系统扩容：

  将云主机的根云盘容量扩容增加。

  - 使用LVM分区的Linux云主机可使用lvextend直接扩容系统分区。
  - Windows云主机也可以右击磁盘管理进行系统扩容。
- 切换控制台模式：

  控制台模式支持VNC和SPICE，VNC可以直接在浏览器上打开控制台，SPICE协议需SPICE客户端打开，支持两种模式切换，重启后生效。
- 存储迁移：

  云主机支持关机状态下跨网络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/解绑亲和组：绑定云主机到亲和组，或从亲和组解绑云主机。

  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。

- 更换系统：

  将云主机停止后，可指定目标镜像更换系统，目标镜像需为Image类型。更换系统后，云主机保持关机状态。

  - 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。

- QoS设置：

  限制云主机云盘、网络上下行带宽的设置，无须重启立刻生效，过低的QoS可能导致云主机工作异常。

- User Data注入：

  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。

- 修改平台：

修改云主机的平台，可选择Linux、Windows、WindowsVirtio、Other、Paravirtualization模式，其中Linux、WindowsVirtio、Paravirtualization支持Virtio类型的设备驱动，Windows、Other使用Qemu模拟的设备。需重启后生效。

- 修改屏幕数量：

  VDI场景下云主机可接入的最多屏幕数量，默认为1 ，修改后，需重启生效。支持SPICE模式。

- 加载网卡：

  从可用的三层网络列表，选择可用网络加载至云主机。

- 卸载网卡：

  将云主机的网卡卸载，如果云主机没有任何网卡，停止后，将无法启动，需至少加载一个网卡。

- 更改默认网络：

  支持更改云主机的默认网络，需要在云主机内部重启网络服务后生效。

- 设置MAC：

  创建云主机时可以指定MAC地址，停止云主机后，可设置或更改MAC地址，从可用的IP地址段选择可用IP指定给云主机使用，需避免IP冲突。

- 设置静态IP：

  设置云主机的静态IP，从可用的IP地址段选择可用IP指定给云主机使用，需避免IP冲突。

- 加载GPU设备：

  将物理主机的GPU设备加载给云主机使用，使得云主机独占使用GPU设备，拥有GPU设备的云主机不支持在线迁移。

- 卸载GPU设备：

  将云主机上已独占的GPU设备卸载。

- 加载USB设备：

  开启USB透传功能，云主机可加载USB设备。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。一台云主机加载的所有USB设备只能处于同一台物理主机上。

- 卸载USB设备：

  云主机卸载USB设备。

- 加载其它外接设备：

  开启其他外接设备透传功能，云主机可加载其他外接设备。

- 卸载其它外接设备：

  云主机卸载其他外接设备。

- 定时任务：

  基于定时器，创建定时任务，支持定时关机、定时开机、定时重启、定时快照等任务。

- 报警：

  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。

- 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。

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：

需要重启云主机才可以生效	需要关机才可以执行	云主机运行中即刻生效
• 设置NUMA结构 • 修改显卡类型 • 修改云主机CPU模式 • 修改云主机缓存模式 • 修改云主机控制台模式 • 设置、取消控制台密码 • 设置USB重定向 • 设置平台类型 • 设置启动顺序	• 启动云主机 • 存储迁移 • 更换系统 • 恢复快照 • 启动指定物理主机 • 设置MAC • 重置云主机 • 设置、取消静态IP	• 克隆云主机 • Network Anti-Spoofing • 绑定、解绑亲和组 • 创建、删除快照 • 创建、删除、加载、卸载云盘 • 创建云盘镜像 • 创建云主机镜像 • 创建灾备数据（混合云版支持） • 定时任务 • 更改所有者 • 在线修改密码 • 加载、卸载网卡 • 加载、卸载GPU设备 • 加载、卸载ISO • 加载、卸载USB设备 • 设置、取消网卡QoS • 设置、取消网盘QoS • 设置QGA状态 • 设置RDP模式

需要重启云主机才可以生效	需要关机才可以执行	云主机运行中即刻生效
		• 设置VDI设备最多支持的屏幕数量 • 设置高可用 • 云盘扩容 • 云主机高可用全局开关 • 在线迁移（共享存储） • 主存储超分率 • 主存储使用阈值 • 在线修改内存 • 修改彻底删除时延 • 修改计算规格 • 系统扩容

注意事项

使用云主机需注意：

- 云主机的快照链如果过长，可能会导致云主机IO性能下降。
- 如果SSH Key注入和User Data同时注入，User Data生效，而注入的SSH Key不生效。
- 云主机导入User Data需注意：
  - 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云主机镜像需提前安装Cloud-Init；Windows云主机镜像需提前安装Cloudbase-Init。
  - 进入云主机的*/var/lib/cloud/instance/user-data.txt*，看数据是否已成功导入，若没有，请登录云主机所在物理机执行以下命令进行检查：
    - 执行`ps -ef|grep http`，查看是否有User Data
    - 执行`ip netns`，获取namespace
    - 执行`ip netns exec namespace ip a`，查看namespace里是否有目标ip

      例如：

```
# 获取namespace为br_eth0_1101_f8e41fc3a3b9431d9ea5f2bf090e085e
[root@localhost ~]# ip netns
br_eth0_1101_f8e41fc3a3b9431d9ea5f2bf090e085e (id: 0)
# 查看namespace里是否有目标ip：169.254.169.254
[root@localhost ~]# ip netns exec
 br_eth0_1101_f8e41fc3a3b9431d9ea5f2bf090e085e ip a
1: lo: <LOOPBACK> mtu 65536 qdisc noop state DOWN
```

```
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
10: inner0@if11: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
 pfifo_fast state UP qlen 1000
    link/ether 2e:6d:a4:6c:ab:79 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.164.230/24 scope global inner0
       valid_lft forever preferred_lft forever
    inet 169.254.169.254/32 scope global inner0
       valid_lft forever preferred_lft forever
    inet6 fe80::2c6d:a4ff:fe6c:ab79/64 scope link
       valid_lft forever preferred_lft forever
```

- 数据云盘默认采用Virtio设备，需安装相应驱动才可识别使用，Linux各发行版默认已集成Virtio驱动，无须额外安装，Windows需额外安装驱动。
- 共享云盘需要使用Virtio SCSI类型云盘，各挂载的云主机可同时进行读写。Ceph存储支持共享云盘。
- GPU透传功能需要物理主机支持IOMMU及BIOS打开VT-d选项。
- 云主机多网卡的情况下，修改默认网卡，需要在云主机内部重启网络服务后生效。
- 云主机加载/卸载云盘是动态操作，而云主机的*/etc/fstab*是静态配置文件。如果加载云盘后修改云主机fstab文件，对该云主机在线创建镜像，使用该镜像创建其它云主机时，由于fstab文件没有相应的挂载信息，再创建的云主机会hang住无法启动。
  - Linux云主机加载云盘后不能修改*/etc/fstab*文件。
  - 正确的做法：

    进入*/etc/rc.local*执行*mount*命令来挂载云盘：

    ```
    # chmod +x /etc/rc.local
    # mount -t 云盘UUID 目标挂载路径
    ```

    注： 建议使用云盘的ID来挂载而非*/dev/vdb*类似的盘符来挂载。

9.2 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。

云盘相关操作定义

- 启用：

将停用的云盘启用，启用后，可以加载到云主机。针对已经加载的云盘，停用不影响其正常工作，在其卸载后就不可再加载。

- 停用：

  将启用的云盘停用，停用后，此云盘不可作为候选加载到其他云主机。

- 加载：

  将云盘加载到云主机，云主机运行或关机状态均可加载。

- 卸载：

  从云主机将云盘卸载，卸载后可加载到其他云主机。

- 迁移：

  本地存储的云盘可以在卸载后，迁移至其他物理主机，迁移后，可以加载到目的物理主机的其他云主机上。

- 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：

  将云盘封装成镜像，可以使用此镜像再创建更多云盘，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。

- 云盘扩容：

  支持在线扩容功能，按需求进行数据云盘扩容，数据云盘扩容后容量实时生效，扩容容量只增不减且增量不得小于4MB。

- 创建快照：

  针对云盘在指定的时间点创建数据映像，可以在数据丢失时，有效恢复数据。与云主机根云盘创建快照类似。卸载后，均可创建快照。针对已加载到运行状态的云主机的云盘。

- 恢复快照：

  把云盘还原到当前快照状态。只能操作一个已卸载或已停止的云主机上的云盘。

- 删除快照：

  删除当前快照。

- 更改所有者：

变更云盘的所有者给其他普通账户。

- 存储迁移：

  云盘支持跨网络共享存储的迁移，目前支持跨Ceph存储迁移以及跨NFS存储迁移。

  - 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：

  将已挂载、未挂载或未实例化的云盘删除掉，未实例化云盘删除操作为立即删除，删除后系统不再记录此云盘。

- 恢复：

  将已删除的云盘恢复到就绪状态。

- 彻底删除：

  将已删除的云盘彻底删除，系统将不再记录此云盘，并删除真实的数据。

- 定时任务：

  基于定时器，创建定时任务，目前云盘定时任务只支持数据云盘快照任务，支持创建、启用、停用、删除定时任务。

注意事项

使用云盘需注意：

- 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。
- 云盘存储在主存储中，需确保主存储可用，为可连接状态，云盘才可正常工作。
- 创建云盘时，需要指定云盘规格。
- 创建云盘时，如果未指定主存储，则创建出的云盘为未实例化云盘。
- 未实例化云盘不占用存储空间，只有挂载到云主机，实例化后会占用真实存储空间。
- 指定主存储后，如果选定的云盘规格超过目前主存储的可用虚拟容量，创建云盘会失败，提示主存储可用容量不足。
- 指定的主存储如果是本地存储，则同时需选择挂载此主存储的集群下可用的物理主机。
- VirtioSCSI类型的云盘表示采用VirtioSCSI总线，云盘属于SCSI类型，支持IO多队列，可以通过唯一识别ID（WWN）识别。
- 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。
- 本地存储的云盘在卸载后，支持迁移到其他物理主机上，迁移后，可加载到新物理主机上的云主机。
- 可对云盘创建快照，表示在特定时间点上的数据进行备份。可在数据丢失时，有效恢复数据。本地存储、NFS和SMP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。
- 云盘快照均增量快照，恢复后，快照点当时的数据会恢复并覆盖云盘内所有数据，需谨慎操作。

- 多主存储时创建云盘策略：
  - 存在多个主存储时，可以指定主存储来创建云盘。
  - 如果未指定主存储：
    - 存在多个本地主存储时，创建云主机会优先选择可用容量大的存储来创建云盘。
    - 存在多个NFS主存储时或多个Shared Block主存储，创建云主机会随机选择主存储来创建云盘。
    - 针对本地主存储+NFS/Shared Mount Point/Shared Block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。
- 针对云盘，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。
- 加载/卸载云盘是动态操作，而云主机的*/etc/fstab*是静态配置文件。如果加载云盘后修改云主机fstab文件，再卸载云盘，此时一旦重启云主机，云主机将无法启动，因为fstab文件没有相应挂载信息，云主机会hang住无法启动。

  正确的做法：

  - 进入*/etc/rc.local*执行*mount*命令来挂载云盘：

    ```
    # chmod +x /etc/rc.local
    # mount -t 云盘UUID 目标挂载路径
    ```

    注: 建议使用云盘的ID来挂载而非*/dev/vdb*类似的盘符来挂载。

9.3 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。

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。

镜像相关操作定义

- 启用：

  将停用的镜像启用，可作为候选来创建云主机。

- 停用：

  将镜像停用，此镜像不可作为候选使用来创建云主机。

- 导出：

  将镜像仓库的镜像导出，可直接下载，导出的镜像默认存放在镜像仓库目录下的*export*子目录下。

  针对Sftp镜像服务器，可以直接拷贝镜像所在的地址，进行拷贝导出。

  针对Ceph镜像服务器，可参考镜像所在的Pool信息使用rbd export进行手动导出。

- 全局共享：

  将镜像共享给所有账户，使得所有普通账户均可使用。

- 共享：

  将镜像共享给指定的一个或多个账户。

- 全局召回：

  将共享的镜像全部召回，不再共享。全局召回不影响单独共享，单独指定共享的镜像，普通账户依然可以使用。

- 召回：

  将镜像从指定的用户召回，不再共享。

- 更改所有者：

  变更镜像的所有者给其他普通账户。

- 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。

  将Ceph存储里面的镜像跨存储迁移至其他Ceph存储。迁移后，新的Ceph存储可使用此镜像，原本的Ceph存储则不再保留原本镜像。进行存储迁移前，需确保目的Ceph存储容量充足。

- 删除：

  将镜像删除，删除后可进行彻底删除或恢复。

- 恢复：

  将已删除的镜像恢复为就绪状态。

- 彻底删除：

  将已删除的镜像彻底删除，并删除镜像服务器上的真实数据。

- 下载已导出镜像：

  将已导出的镜像下载到浏览器对应本地硬盘中。

- 复制URL：

  将已导出的镜像的URL拷贝出来，可以添加到其他云平台，也可直接使用wget下载此URL。

- 删除已导出镜像：

  将已导出的镜像从镜像从镜像仓库删除，不再占用存储容量。

- 修改平台：

  修改镜像的平台类型，修改后新建的云主机会以新的类型来决定云主机的设备驱动，Linux、Windows virtio、Paravirtualization采用了virtio的驱动，Windows和Other采用了Qemu模拟设备。

- 修改QGA选项：

  打开QGA选项，表示镜像里面已经预装并开机运行qemu-guest-agent，使用此镜像创建的云主机，支持在线修改密码。

- 刷新容量：

刷新镜像所在镜像服务器的真实容量。

注意事项

使用镜像需注意：

- 使用*file*格式添加镜像，暂不支持Ceph镜像服务器。
- 输入的URL需可被镜像服务器访问，且存在此镜像文件，如果镜像服务器无法访问输入的URL，则会提示下载镜像失败。
- 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，添加ISO镜像时，此选项禁用。
- admin可共享镜像给普通账户，分享后，普通账户可使用此镜像创建云主机。
- 普通账户可添加镜像创建云主机，也可使用admin共享的镜像资源，普通账户可以删除自身添加的镜像，不可删除其他镜像。
- 镜像停用后，此镜像不可作为候选来创建云主机。
- 镜像容量为虚拟容量，表示此镜像的虚拟大小，镜像真实容量为镜像占用的镜像服务器的空间，类似du -sm读取的文件大小。
- 镜像仓库类型的镜像支持导出功能，导出后，可使用提供的URL下载镜像。
- 添加镜像支持Legacy和UEFI两种BIOS模式，创建云主机时，镜像中的BIOS模式会继承给云主机，BIOS模式不匹配可能导致云主机无法正常工作，请谨慎选择
  - 对于qcow2或raw格式的镜像，请选择与封装时一致的BIOS模式
  - 对于iso格式的镜像，可自行选择BIOS模式，系统将基于所选模式引导安装
  - 对于Windows类型的镜像，建议选择Legacy引导模式
  - 对于使用UEFI引导模式的CentOS 7.4及以上版本Linux类型镜像，创建的云主机启动后进入UEFI Shell，需执行以下命令，才能成功启动进入操作系统：

```
Shell> fs0:
FS0:\> cd EFI
FS0:\EFI\> cd centos
FS0:\EFI\centos\> shimx64-centos.efi
```

9.4 亲和组

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)：

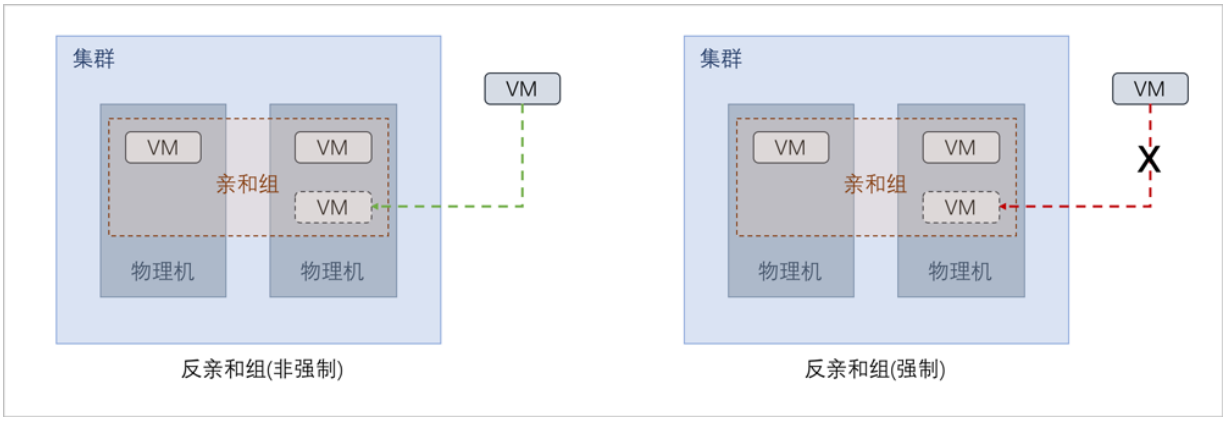
  将亲和组内的云主机尽量分配到不同物理机上，当没有更多物理机可分配时，回归普通分配策略。

- 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 *87: 反亲和组(非强制)与反亲和组(强制)*所示：

图 87: 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。

亲和组相关操作定义

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。

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。

注意事项

- 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。
- 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。

9.5 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。

物理主机分配策略

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

计算规格相关操作定义

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。

注意事项

使用计算规格需注意：

- 计算规格的内存需大于16M，过低的规格会无法启动云主机。
- 磁盘网络带宽均为可选项，限制了过低的带宽，可能导致云主机工作异常。
- 首次创建，可按照默认的1CPU-1G内存来配置。
- 计算规格支持在线修改，需要全局配置打开NUMA支持。不支持在线修改Windows云主机。
- 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。
- 创建云主机时，如果同时指定了亲和组策略和物理主机分配策略：
  - 指定亲和组策略为反亲和组(非强制)：物理主机分配策略优先
  - 指定亲和组策略为反亲和组(强制)：亲和组策略优先

9.6 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。

云盘规格支持启用、停用、共享、召回等操作。 使用ISO安装云主机时，需指定云盘规格来指定根云盘大小。

云盘规格相关操作定义

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。

9.7 弹性伸缩组

ZStack提供基于负载均衡的云主机弹性伸缩，可根据用户业务的负载变化，按照预定义的策略，自动调整伸缩组内云主机的数量，提高云平台资源的使用效率，降低运维成本，保证业务平稳运行。

伸缩模式

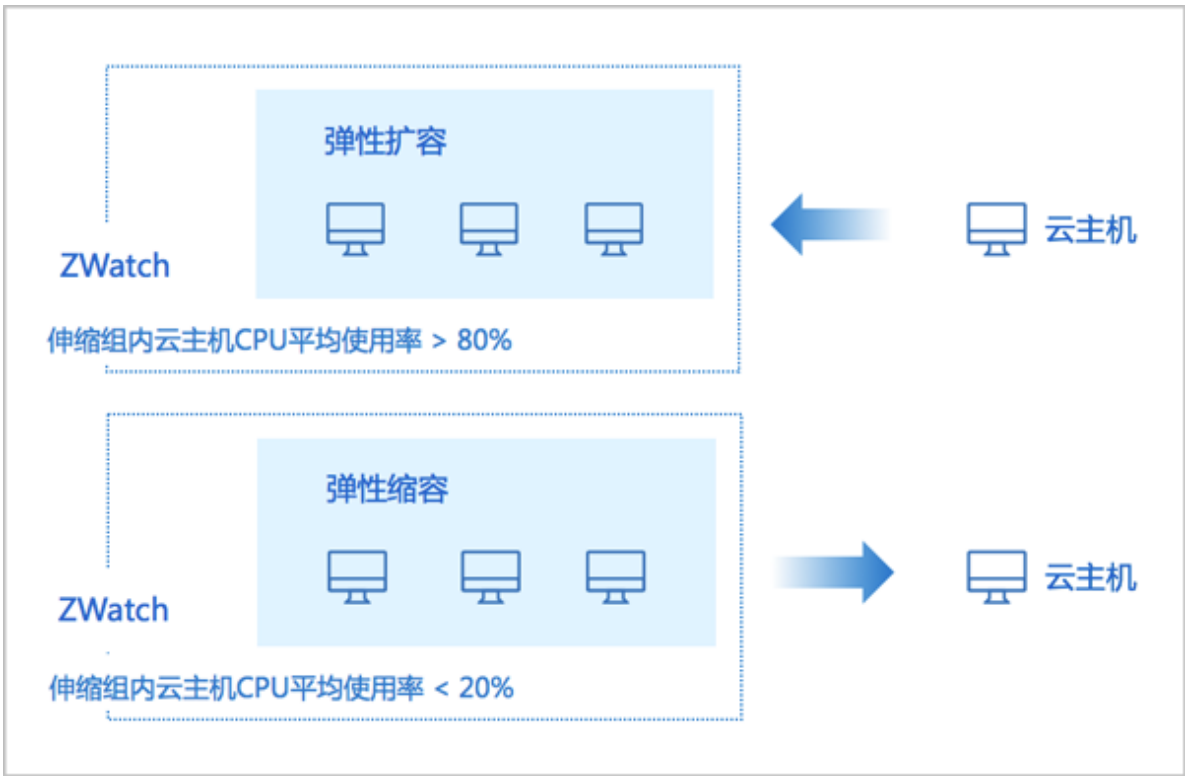
支持以下两种伸缩模式：

1. **弹性伸缩**

   - 弹性伸缩包括：弹性扩容、弹性缩容，前者在业务增长时自动增加云主机，后者在业务下降时自动减少云主机；
   - 提供ZWatch监控报警触发弹性伸缩，可自定义接收端类型，包括：邮箱、钉钉、HTTP应用。

   如*图 88: 弹性伸缩*所示：

   图 88: 弹性伸缩

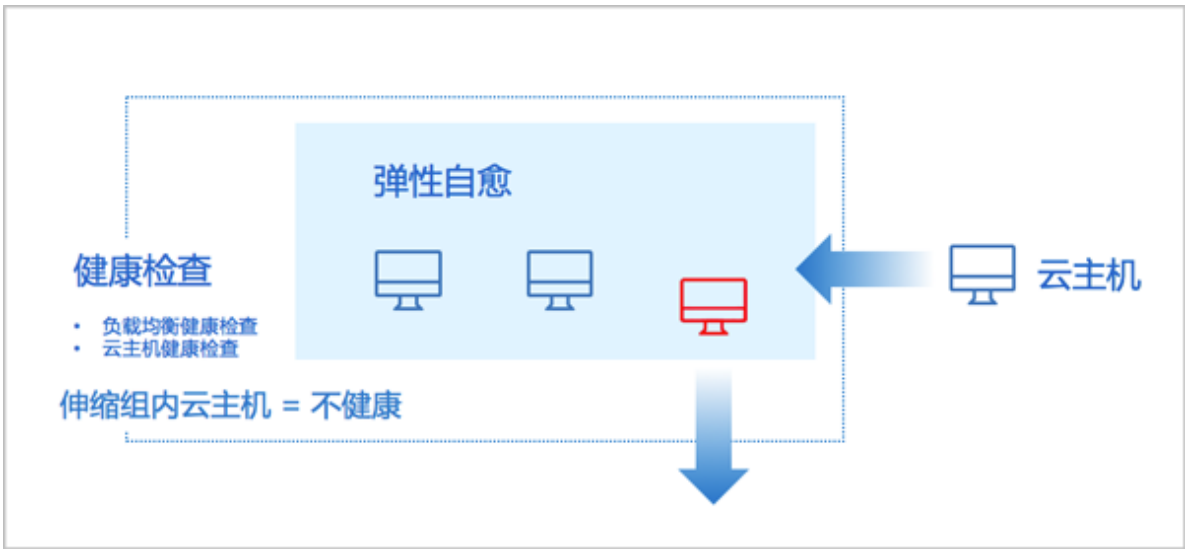


2. 弹性自愈

- 弹性自愈：通过监控伸缩组内云主机的健康状态，自动移除不健康云主机并创建新的云主机，确保组内健康云主机数不低于设置的最小值；
- 提供两种健康检查机制触发弹性自愈：负载均衡健康检查、云主机健康检查，若伸缩组配置了负载均衡功能，建议选择负载均衡器自带的健康检查机制。

如图 *89:* 弹性自愈所示：

图 89: 弹性自愈



伸缩策略

扩容策略

- 在业务增长时，伸缩组自动增加云主机进行扩容，避免访问延时和资源超负荷运行
- 通过设置ZWatch监控报警机制触发弹性扩容，例如，当监测到伸缩组内全部云主机的平均内存使用率在一段时间内持续突破80%，将自动创建合适数量的云主机，使伸缩组重新达到合理的负载均衡
- 需设置冷却时间（伸缩组执行完成一次伸缩活动后的一段时间），在该时间内，伸缩组处于锁定状态，不执行其它伸缩活动
- 伸缩组每次扩容最小允许增加1台云主机，该数值设置过大可能导致扩容活动失败

缩容策略

- 在业务下降时，伸缩组自动减少云主机进行缩容，避免资源浪费
- 设置缩容策略时，触发条目不可选择，与扩容时触发条目保持一致
- 通过设置ZWatch监控报警机制触发弹性缩容，例如，当监测到伸缩组内全部云主机的平均内存使用率在一段时间内持续低于20%，将自动移除合适数量的云主机，使伸缩组重新达到合理的负载均衡
- 支持以下四种移除策略：
  - 最早创建的云主机：当伸缩组开始执行缩容活动时，将从最早创建的云主机开始逐台移除
  - 最新创建的云主机：当伸缩组开始执行缩容活动时，将从最新一次创建的云主机开始逐台移除

  - CPU利用率最低的云主机：当伸缩组开始执行缩容活动时，将从CPU利用率最低的云主机开始逐台移除
  - 内存利用率最低的云主机：当伸缩组开始执行缩容活动时，将从内存利用率最低的云主机开始逐台移除
- 伸缩组每次缩容最小允许减少1台云主机，该数值设置过大可能导致缩容活动失败

注意事项

- 弹性扩容时组内云主机数不能高于设置的最大值，弹性缩容时不能低于设置的最小值，初次创建伸缩组时组内云主机数为设置的初始值
- 伸缩组每次扩容最小允许增加1台云主机，该数值设置过大可能导致扩容活动失败；伸缩组每次缩容最小允许减少1台云主机，该数值设置过大可能导致缩容活动失败
- 可为伸缩组配置负载均衡功能，实现基于负载均衡的云主机弹性伸缩，此时建议选择负载均衡器自带的健康检查机制
- 选择负载均衡器后，必须选择监听器，若选多个监听器，将分别通过不同端口或端口组对同一组云主机进行监听
- 目前支持云路由网络/VPC网络场景的云主机弹性伸缩
- 伸缩组支持配置ZWatch监控报警机制触发弹性伸缩，可自定义接收端类型，包括：邮箱、钉钉、HTTP应用
- 云主机镜像目前支持添加qcow2格式和raw格式
- 若将模板配置中的资源删除（例如计算规格、镜像、网络等），将导致伸缩组创建失败，请谨慎操作
- 若伸缩组已触发伸缩活动，停用伸缩组，正在执行的伸缩活动不受影响，该伸缩活动执行完成后，将停止触发新的伸缩活动；
- 若伸缩组处于检测中，停用伸缩组，ZWatch/健康检查机制将立即停止检测伸缩组，并停止触发新的伸缩活动。

补充说明

- 弹性伸缩组内云主机上运行的业务应用必须无状态并且可横向扩展。
- 弹性伸缩组无法纵向扩展，即：无法自动扩缩云主机的计算规格、网络带宽等配置。
- 关于弹性伸缩服务，提供以下全局设置：
  - 当伸缩组使用负载均衡健康检查机制时，可设置云主机在负载均衡中健康状态检查的时间间隔。

设置方法：进入**设置** > **全局设置** > **高级设置**，设置**负载均衡云主机健康检查间隔**即可，默认为10，单位为秒，最小值不能低于10秒，最大值不能高于1000秒。

- 当伸缩组使用负载均衡健康检查机制时，可设置云主机在负载均衡中健康状态检查的线程数。

  设置方法：进入**设置** > **全局设置** > **高级设置**，设置**负载均衡云主机健康检查线程数**即可，默认为10，最小值不能低于10线程，最大值不能高于1000线程。

- 当伸缩组使用云主机健康检查机制时，可设置删除组内不健康云主机的时间间隔。

  设置方法：进入**设置** > **全局设置** > **高级设置**，设置**组内不健康实例删除间隔**即可，默认为30，单位为秒，最小值不能低于10秒，最大值不能高于1000秒。

- 当伸缩组使用云主机健康检查机制时，可设置删除组内不健康云主机的线程数。

  设置方法：进入**设置** > **全局设置** > **高级设置**，设置**组内不健康实例删除线程数**即可，默认为10，最小值不能低于10线程，最大值不能高于1000线程。

- 可设置伸缩组内云主机数量检查的时间间隔。

  设置方法：进入**设置** > **全局设置** > **高级设置**，设置**组内实例数量检查间隔**即可，默认为20，单位为秒，最小值不能低于10秒，最大值不能高于1000秒。

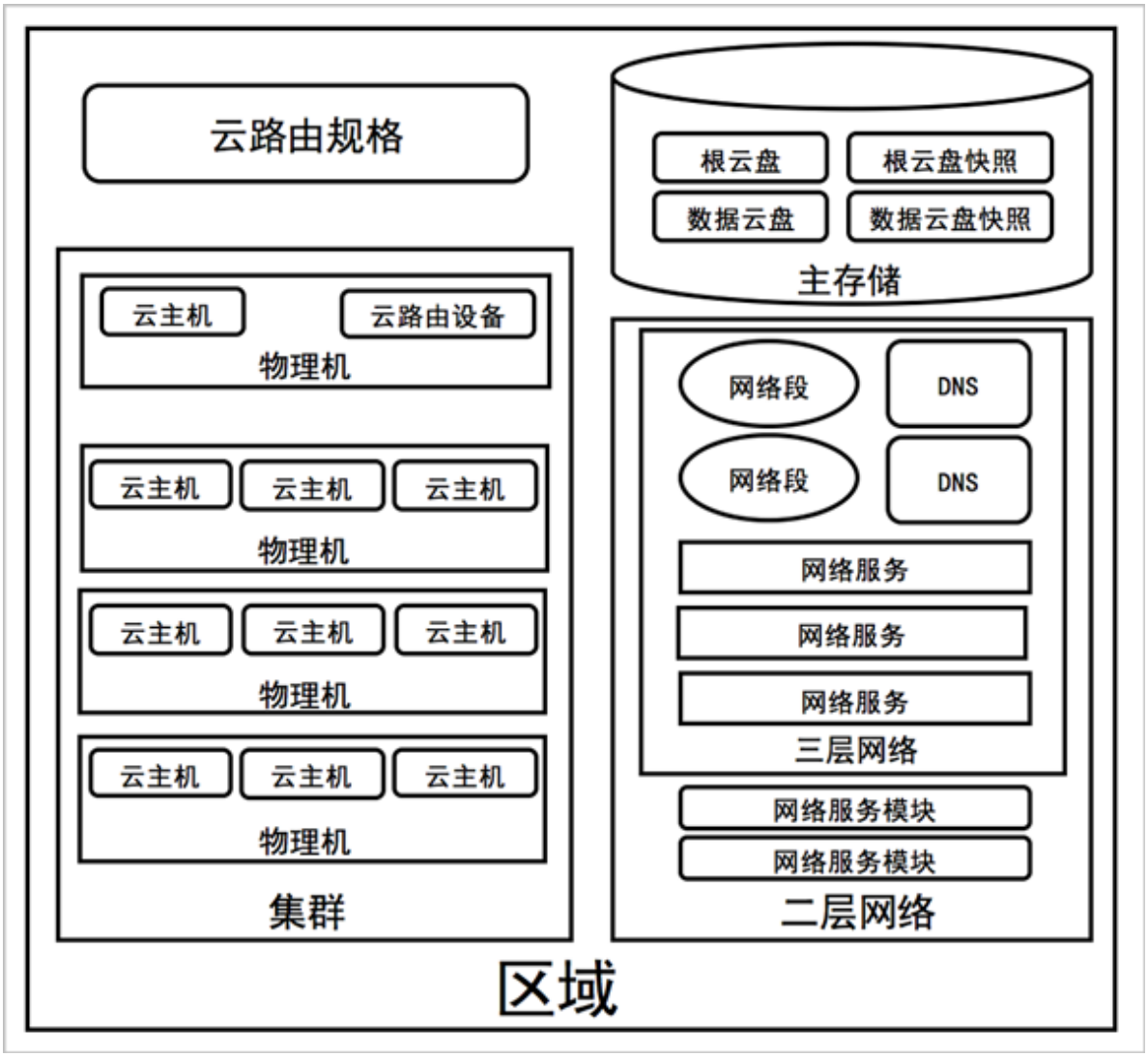
10 硬件资源

10.1 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 *90:* 区域资源结构所示，区域中的资源以如下形式组织：

图 90: 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。

注意事项

使用区域需注意：

- 禁用区域：禁用区域会导致此区域下的所有集群及集群内所有物理主机均被禁用，此时本区域的所有集群内均不可再申请新资源，需再次启用才可申请。
- 启用区域：启用区域会导致此区域下的所有集群及集群内所有物理主机均会被启用。
- 删除区域：删除区域会删除此区域下所有资源包括其子资源，包括集群、二层网络、主存储及其子资源物理主机、云主机、云盘、快照、三层网络、各网络服务等，此操作非常危险，请极其慎重操作！这里的删除所有资源，只是移除所有资源在ZStack中的记录，并不删除真实的数据。
- UI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。在删除区域的同时会直接删除与挂载此区域的镜像服务器。

10.2 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。

集群的目的：

- 用于提高整体系统的计算能力、IO能力；
- 提高服务的可靠性；
- 提升系统的规模扩展能力，降低系统的运维成本。

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。

集群相关约束条件

1. 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。

2. 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。

     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
Shared Block	支持挂载一个或多个Shared Block

主存储	集群
Share Mount Point	支持挂载一个SMP
Ceph	为挂载到集群的Ceph，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。
- 删除使用本地存储的集群，会删除集群内所有的物理主机，也会删除所有的云主机 ，但不删除物理主机内所有的云盘和快照真实数据。
- 删除使用共享存储的集群，相关的云主机会被停止，如果这些已停止的云主机设置了高可用标签，那么可以在其他可用的集群上的物理主机再次启动。
- 如果不同集群挂载了相同网络和相同主存储，则支持云主机跨集群迁移 。
- 从集群卸载主存储，ZStack会停止集群内所有的云主机，只有再次加入挂载此主存储，这些云主机才可正常启动。
- 云主机不支持在多个不同类型主存储之间进行迁移。
- 云主机的数据盘所在的主存储进入维护模式，云主机会停止且无法启动。

3. 集群支持定义集群的CPU模式

- 此设置生效前提：在**设置** > **全局设置** > **高级设置**中将**物理主机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类型的物理主机。
- 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。

4. 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。
- 此外，从集群卸载网络， ZStack会卸载掉集群内所有云主机的网卡 ，此时云主机没有网卡，运行中的云主机一旦停止，将无法再次开机，需要再次给集群加载网络后，再给云主机添加网卡，才可正常开机。
- 集群支持添加迁移网络，可用于迁移操作。如果不设置该网络，迁移默认使用管理网络。

5. 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
LocalStorage	○	○	×
NFS	○	○	×
Shared Mount Point	○	○	×
Ceph	○	×	○
Shared Block	○	×	×

6. 集群 | 物理主机

- 停用集群后，会停用此集群下所有的物理主机，停用后，此集群就不能作为候选用于申请新资源，原本运行的云主机不受影响，但这些运行的云主机停止后就不能再次在此集群启动。
- 启用集群后，会同时启用此集群下所有的物理主机。

7. 集群 | VDI网络

- 在VDI场景，创建集群时，如果已经部署了VDI单独使用的网络，可以指定VDI网络的CDIR，此网络用于VDI连接的协议流量，例如输入*172.20.0.0/16*，则在物理主机上以此网络进行VDI协议流量的传输。
- 如果输入错误或不存在的网络CIDR，则会默认使用管理节点添加物理主机时的管理网络。

10.3 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 *91:* 物理机所示：

图 91: 物理机

添加物理机注意事项

添加物理主机需注意：

- 管理节点的管理IP需正常访问物理主机的SSH端口以部署代理程序。
- 物理主机的用户名须拥有sudo权限。
- SSH端口需开启防火墙或iptables允许。
- 需支持Intel VMX|AMD SVM的硬件虚拟化特性。

- 添加或更改物理主机的信息，需与实际环境相匹配 。
- 物理主机有一个字段managementIp，用于表示如果此物理主机有多个IP的情况下，添加的IP地址用于管理节点对此物理主机进行连接部署代理程序的IP。
- 管理节点会周期性的向物理主机发送*ping*命令以检查通道的健康状态; 一旦某个物理主机响应失败，或者*ping*命令超时，此物理主机就会变为失联状态，失联后物理主机上运行的云主机会变成unknown状态，待物理主机恢复连接后，会再次同步其上云主机的状态。
- 管理节点会提供ntpdate时间服务器对各物理主机进行时间同步。

物理机使用注意事项

使用物理主机需注意：

- 物理主机维护模式 ，主要用于管理员对物理主机打算进行关机实施维护操作，例如添加硬盘，更换网卡等。
- 物理主机维护模式，若主存储为本地存储，则会停止此物理主机上所有云主机，若主存储为共享存储，则会自动迁移其上云主机到可用物理主机上，如果其他物理主机资源不足，则会停止这些云主机。
- 物理主机停用后，原本运行的云主机依然保持运行状态，如果停止后将不能使用此物理主机启动。
- 物理主机停用或维护后，此物理主机不能再作为候选用于申请新资源，只有再次启用后，才可正常使用 。
- 物理主机失联或者进入维护模式后，才可删除物理主机 。
- 删除本地存储上的物理主机会直接彻底删除此物理主机上所有的云主机或云盘 。这里的删除，只是移除物理主机、云主机、云盘等信息在ZStack中的记录，并不删除真实的数据。
- 删除共享存储上的物理主机，不会直接删除其上的云主机或云盘，这些资源可在其他物理主机上重新启用或使用。
- 删除物理主机后，即使再次添加回来，系统也将无法识别删除的云主机，需慎重删除 。
- 如果打算使用GPU透传功能，物理主机的BIOS需开启VT-d功能，添加物理主机时，需勾选IOMMU选项，以扫描IOMMU设备。IOMMU启用状态为启用， IOMMU就绪状态为可用时，才可使用GPU设备透传功能。

物理主机运维异常检查事项

物理主机运维出现异常需检查：

- **管理节点日志**：

在管理节点检查*/usr/local/zstack/apache-tomcat/logs/management-server.log*是否存在异常。

- **物理主机agent进程**：

  在物理主机检查`ps -ef|grep kvmagent`，检查kvmagnet代理进程是否存在异常。

- **物理主机日志**：

  在物理主机检查*/var/log/zstack/zstack-kvmagent.log*是否存在异常。

- **物理主机libvirt状态**：

  在物理主机检查`service libvirtd status`状态是否存在异常。

- **物理主机系统日志**：

  在物理主机检查*/var/log/messages*是否存在异常。

- **物理主机与主存储连接**：

  检查物理主机是否与主存储连接是否出现异常。

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**：停用选中的物理机，**支持批量操作**。停用后，该物理机上原有资源不受影响，但不可作为候选物理机再申请新资源。
- **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**：删除选中的物理机，**支持批量操作**。

  注:

  - 若主存储为本地存储
    - 删除物理机将同时删除该物理机上的云主机和云盘。
    - 即使重新添加此物理机，系统也将重新部署物理机，若之前的数据库资源未备份，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**，删除云主机所在的物理机后，相应的云主机会停止。
- 若云主机的**高可用级别**为**NeverStop**，删除云主机所在的物理机后，如果物理机资源允许，相应的云主机会在线迁移至其他可用的物理机且不会影响数据安全性；如果物理机资源不足，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它物理机资源满足条件已迁移，另一部分云主机因资源不足而停止。
- 删除物理机对共享存储上的数据云盘无影响。

10.3.1 GPU设备透传

GPU设备透传：将物理主机的GPU显卡设备，直接透传给云主机使用，云主机独占显卡设备，适用于视频渲染、游戏、人工智能等场景。

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。

注意事项

使用GPU设备透传需注意：

- 需在物理主机上准备GPU设备，支持AMD全系列显卡，支持NVIDIA计算卡。
- 在BIOS开启VT-d或IOMMU支持。
- 添加物理主机时，需勾选扫描物理主机的IOMMU设备，以支持GPU设备透传， 勾选此项后，会遍历物理主机可用的GPU设备，扫描后，需重启物理主机以使得IOMMU配置在内核生效。
- IOMMU启用状态：表示IOMMU设备直通的状态，勾选表示已在内核启用IOMMU配置，需系统重启后生效。

- IOMMU就绪状态：确保物理主机IOMMU为就绪状态才可正常使用GPU设备透传。如果不就绪，表示物理主机BIOS或者内核的IOMMU选项未打开。
- 使用GPU透传后物理主机的GPU设备透传给云主机后，接入的显示器只显示云主机的界面，物理主机的界面将不再显示。
- GPU设备透传需先建立云主机后，再动态加载GPU设备到相应的云主机上，加载后，需安装相应的显卡驱动，才可正常显示。
- 拥有GPU透传设备的云主机不支持迁移功能，需卸载后迁移。
- 拥有GPU透传设备的云主机关机后，只能从原本拥有GPU设备的物理主机启动，不支持跨物理主机启动。
- 共享存储上的云主机，在关机情况下加载GPU设备时，可以选择任意物理主机，但启动时会从选定的物理主机启动，如果此物理主机资源不足，会启动失败。
- 单个云主机可以挂载多个GPU设备，但是这些GPU设备只能来源于同一个物理主机。

10.3.2 USB设备透传

USB设备透传：物理主机USB设备可直接透传至该物理主机上所运行的云主机，从而让云主机能够直接使用物理主机上的USB设备。

注意事项

使用USB设备透传需注意：

- 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。
- 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。
- 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！

Windows XP、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。

参考路径：

http://cdn.zstack.io/tools/renesas_usb30_21390.exe

双击文件完成安装。

注:

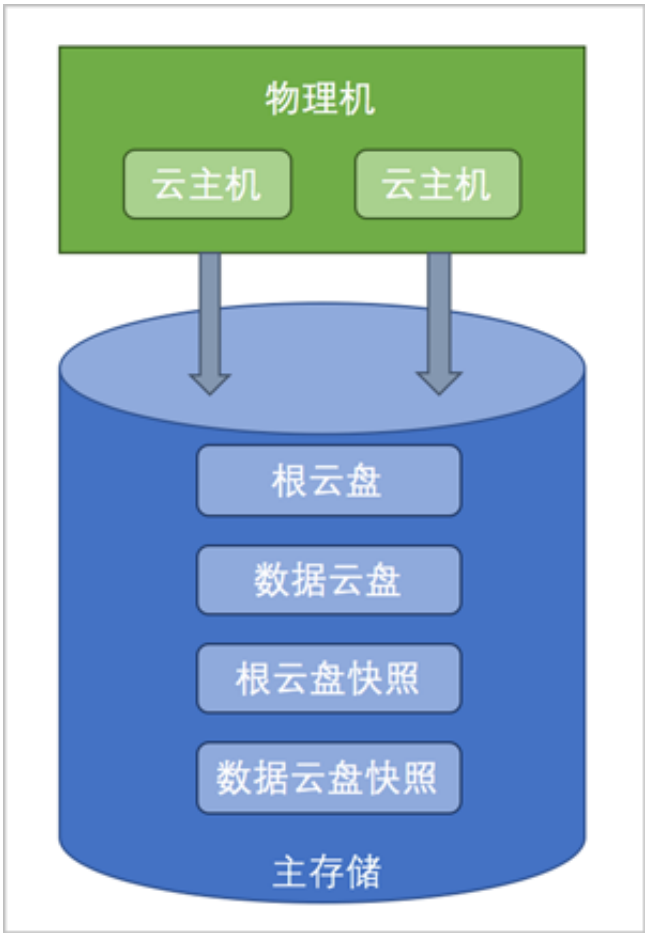
- 对于USB2.0设备，Linux和Windows云主机均可加载并识别；
- 对于USB3.0设备，Linux云主机可加载并识别；Windows云主机中，Windows XP、Windows 2003、Windows 2008和Windows 7系统需要手动安装，或将USB3.0设备插在USB2.0口中，以提高识别率。
- 云主机加载USB设备的数量有上限限制：
  - USB1.0设备：最多支持加载1个
  - USB2.0设备：最多支持加载6个
  - USB3.0设备：最多支持加载4个

10.4 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 *92:* 主存储所示：

图 92: 主存储



主存储支持类型可分为以下两大类：

- **本地存储**（Local Storage）：使用物理机的硬盘进行存储。
- **网络共享存储**：支持NFS、Shared Mount Point、Ceph、Shared Block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。

集群挂载主存储场景

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。

注意事项

使用主存储需注意：

- 本地存储、NFS、Shared Mount Point主存储基于qcow2。
- Ceph存储使用的是分布式块存储。
- Shared Block存储使用的是共享块存储。
- 以虚拟容量来计算云主机的根云盘和数据云盘消耗。
- 主存储停用后，将不能使用此主存储申请新资源，但不影响当前运行中的云主机，只是不能新建云主机和新建数据盘。
- 主存储维护后，将不能使用此主存储申请新资源，原本运行中的云主机也会被停止。
- 主存储 | 镜像服务器之间的约束关系：
  - 本地存储、NFS、Shared Mount Point、Ceph、Shared Block主存储支持匹配镜像仓库类型镜像服务器使用。
  - 本地存储、NFS、Shared Mount Point主存储支持匹配Sftp类型镜像服务器使用。
  - Ceph主存储支持匹配镜像仓库类型镜像服务器使用，以及匹配同一Ceph镜像服务器使用。
- 主存储的使用基于瘦身模式，支持超分，超分比例设置过大时，需留意真实物理容量的使用。
- ZStack创建云盘时使用的是虚拟大小，如果虚拟大小不足以提供需要的容量，此时创建云盘会提示失败。
- 删除主存储会删除主存储所有的云主机、云盘和快照。需谨慎操作！这里的删除，只是移除主存储、云主机、云盘和快照等信息在ZStack中的记录，并不删除真实的数据。
- 共享存储可以设置独立的存储网络与管理网络隔离，管理节点依据此存储网络来判断云主机健康状态，如果不存在独立的存储网络，可以留空不填，表示采用管理网络来判断云主机健康状态。

10.4.1 本地存储

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。

本地存储特性

- 使用物理主机的本地存储空间，存放云盘数据。
- 云主机数据保护需依赖节点RAID阵列技术。
- 投资低、性能高、大规模，但云主机热迁移存在问题，需要业务层高可靠。
- 适用于软件开发测试环境、分布式应用、应用与数据分离的场景。

注意事项

使用本地主存储需注意：

- 不能使用以下：/、 */dev/*、*/proc/*、*/sys/*、*/usr/bin*、*/bin*等系统目录，使用这些目录可能会导致物理主机异常。
- 本地主存储的状态一般为Connected。
- 本地主存储容量由各物理主机的主存储目录的容量累加。
- 镜像缓存在添加镜像后，会自动分发到各物理主机的主存储目录进行缓存，使用此镜像的不同云主机共享使用此镜像缓存作为base。
- 因为存储的隔离性，使用本地存储的云主机，不支持高可用，不支持指定物理主机启动。
- 使用本地存储的云主机默认支持冷迁移。
- 使用本地存储的云主机支持在线热迁移，默认关闭，需要在全局设置打开，本地存储的云主机不支持带数据盘的热迁移，Windows操作系统的云主机不支持热迁移。
- 本地存储的镜像缓存在删除镜像后，如果没有任何云主机使用，此镜像缓存会自动删除。
- 本地存储一般都处于可连接状态，若某物理主机失联，则此物理主机上的本地存储容量将被扣除，一旦物理主机再次连接，容量会被再次计算进来。
- 一个集群支持挂载多个本地主存储，创建云主机时，可指定任意主存储；若未指定，系统自动选择可用容量最充足的本地主存储。

10.4.2 NFS

NFS主存储：使用网络文件系统作为主存储，需提供NFS的共享文件目录。

NFS主存储特性

- 云盘存放在集中存储，数据需通过存储双控和RAID技术保护。
- 需要构建万兆存储网络，购买集中存储，云主机受高可用保护。
- 特点：构建了存储网、云主机支持高可用、数据支持安全保护、IO性能有瓶颈（8～10节点/一个存储）。

- 场景：适用于传统应用、应用数据紧密、SLA高可用保证、数据安全场景。

注意事项

使用NFS主存储需注意：

- NFS使用时添加的URL格式参考如下：*192.168.0.1:/nfs_root*
- NFS的挂载目录需提供读写权限，NFS的挂载参数需NFS Server端支持。
- ZStack会在所有的物理主机上自动挂载此目录作为主存储。
- 只要集群内任一物理主机可访问NFS主存储，则主存储就处于可连接状态。
- NFS属于共享存储，支持云主机在线迁移。
- NFS主存储是所有物理主机共享带宽访问同一目录，效率和性能具有瓶颈 。
- NFS主存储只会拷贝一份镜像缓存到主存储的共享目录。
- NFS存储支持输入存储网络CIDR，表示基于此存储网络来判断云主机的健康状态。
- 一个集群支持挂载多个NFS主存储，创建云主机时，可指定任意主存储，若未指定，系统随机分配可用主存储。
- 一个集群支持挂载一个NFS主存储和一个本地主存储，在创建云主机时，可指定任意主存储，如果带数据云盘，则需指定数据云盘所使用的主存储；如果不指定主存储，则使用本地主存储来创建云主机。
- 使用NFS+本地主存储的云主机，进行迁移前，需卸载其本地主存储上的云盘。这里的迁移仅限于同一主存储内部，不可跨主存储迁移。

10.4.3 Shared Mount Point

Shared Mount Point主存储：采用共享文件系统存储为主存储，支持SAN存储，格式化为MooseFS，GlusterFS，OCFS2，GFS2等文件系统。

Shared Mount Point主存储特性

- 云盘存放在集中存储，数据需通过存储双控和RAID技术保护。
- 需要构建万兆存储网络，购买集中存储，云主机受高可用保护。
- 特点：构建了存储网、云主机支持高可用、数据支持安全保护，IO性能有瓶颈（8 ~ 10节点/一个存储）。
- 场景：适用于传统应用、应用数据紧密、SLA高可用保证、数据安全场景。

注意事项

使用Shared Mount Point主存储需注意：

- 需在各物理主机提前挂载各挂载点，挂载到相同目录。
- 在添加到ZStack时，需提供挂载到物理主机的本地目录。
- 支持在线迁移，对应挂载目录需提供读写权限。
- Shared Mount Point存储支持输入存储网络CIDR，表示基于此存储网络来判断云主机的健康状态。
- 一个集群支持挂载一个Shared Mount Point和本地主存储，创建云主机时，可指定任意主存储，如果带数据云盘，则需指定数据云盘所使用的主存储；如果不指定主存储，则使用本地主存储来创建云主机。
- 使用Shared Mount Point+本地主存储的云主机，进行迁移前，需卸载其本地主存储上的云盘。这里的迁移仅限于同一主存储内部，不可跨主存储迁移。

10.4.4 Ceph

Ceph主存储：Ceph集群提供的分布式块存储作为主存储。

Ceph分布式存储特性

- 云盘存放在分布式存储，数据通过多副本和纠删码机制提供保护。
- 需要构建存储网络，基于x86通用服务器提供存储服务，云主机受高可用保护。
- 特点：构建了存储网，云主机支持高可用，数据支持多副本，计算和存储都可以横向扩展。
- 适用场景：租用平台、通用型应用、应用数据紧密、SLA高可用保证、大规模环境。
- 支持以Pool为单位显示其容量。

注意事项

使用Ceph主存储需注意：

- 需输入Mon IP节点信息以部署相关的代理程序。
- 如果指定了镜像缓存、根云盘、数据云盘的Ceph存储池名，则这些存储池需提前在Ceph集群自行创建。
- 存储池名为可选项，如果不指定，则ZStack会自动创建以uuid相关命名的存储池，如果指定了存储池名，但是实际不存在，添加Ceph主存储会提示失败。
- 添加Ceph主存储，可添加镜像仓库类型的镜像服务器，或者添加同一Ceph集群存储作为镜像服务器。
- Ceph主存储可指定多个Mon IP，需至少一个Mon处于连接状态。
- Ceph存储支持共享云盘，要求使用VirtioSCSI类型作为前提。

- Ceph集群工作异常时，主存储会失联，可通过`ceph -s`检查状态。
- Ceph存储支持输入存储网络CIDR，表示基于此存储网络来判断云主机的健康状态。
- Ceph存储支持添加扩展池，用于存储数据云盘，可表示不同性能的云盘。可添加或创建Ceph存储池，添加表示使用Ceph集群中已经存在的Pool，如果Ceph存储池已经存在，需进行添加，如果不存在，可指定存储池名来创建，创建时，会采用默认的CRUSH Map。
- 删除扩展池，会删除Pool下所有的数据盘。这里的删除只移除Ceph Pool在ZStack的记录，并不删除真实数据，Ceph存储集群依然可看到此Pool及其上数据。
- 拥有独立存储网络的Ceph存储，节点管理IP表示管理节点连接存储节点的IP，Mon IP表示存储网络的监控节点IP，可以通过`ceph -s`读取。

10.4.5 Shared Block

如果主存储类型采用Shared Block（共享块存储），则可将用户在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SMP类型的主存储相比，Shared Block主存储具备便捷部署、灵活扩展、性能优异等优势。

- Shared Block主存储采用了共享块存储方式，匹配镜像仓库。
- 支持在线添加共享块设备（即LUN设备）
- 支持一个集群添加多个Shared Block主存储；
- 支持一个集群添加1个LocalStorage+1个Shared Block主存储；
- 支持云主机关机状态下带云盘（除共享云盘外）存储迁移；
- 支持精简置备和厚置备两种置备方式：
  - 精简置备：按实际使用情况分配存储空间，实现更高的存储利用率
  - 厚置备：预先分配需要的存储空间，提供充足的存储容量，保证存储性能

注意事项

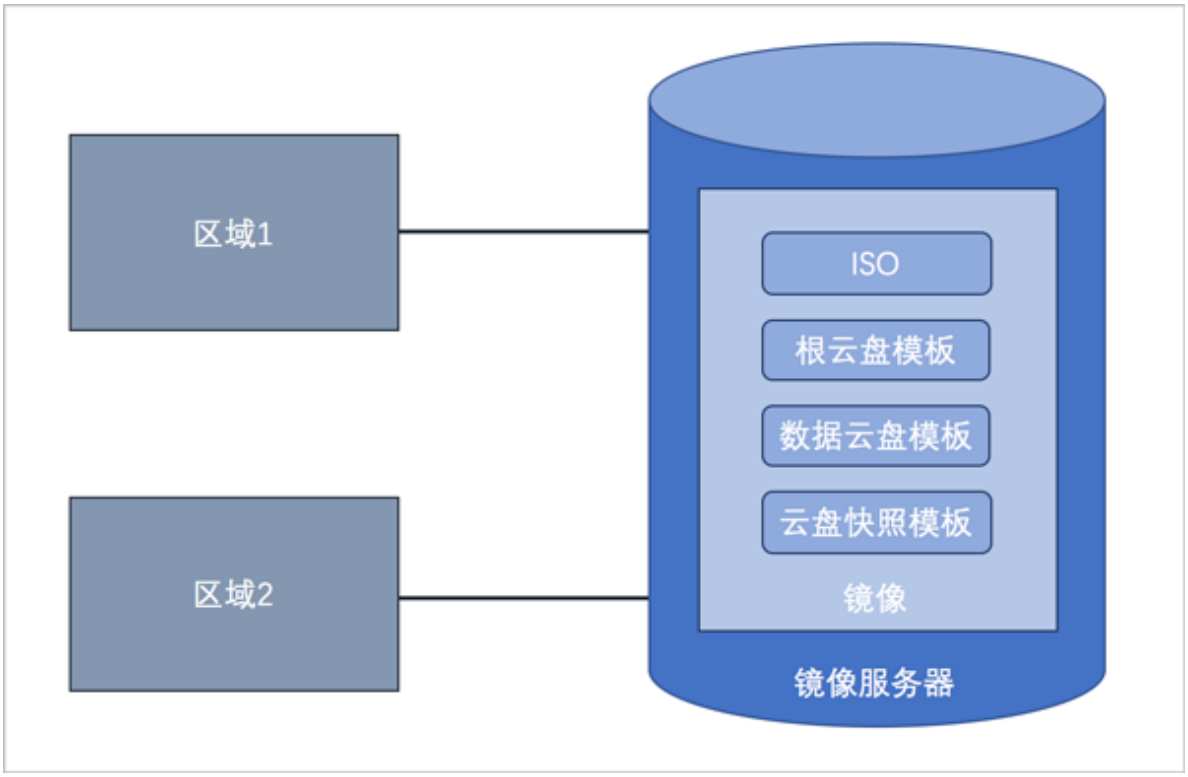
- 添加Shared Block主存储时，清理块设备按钮默认不勾选。
  - 勾选后，将强制清理块设备中的数据，如文件系统、RAID或分区表中的签名等
  - 若块设备中存有数据，不清理块设备，将导致添加共享块或挂载主存储失败
  - 添加的块设备中不能有分区，否则会添加失败

10.5 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 93: 镜像服务器所示：

图 93: 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 | 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
LocalStorage	○	○	×
NFS	○	○	×
Shared Mount Point	○	○	×

Ceph	○	×	○
Shared Block	○	×	×

- 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/混合云版）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。

注意事项

使用镜像服务器需注意：

- 四种镜像服务器类型：

  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。
     - 支持获取已有镜像，可获取该镜像服务器中URL路径下的已有镜像文件。
  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 61ece0adc7244b0cbd12dafbc5494f0c /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
```

注:

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

- 删除镜像服务器会删除所有镜像文件，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。
- 关于镜像服务器支持克隆和快照的关系：
  - 在线克隆：镜像仓库支持不带云盘克隆和整机克隆、Ceph支持不带云盘克隆；
  - 关机克隆：镜像仓库支持不带云盘克隆和整机克隆、Ceph支持不带云盘克隆；
  - 在线快照：镜像仓库、Ceph支持；
  - 关机快照：镜像仓库、Sftp、Ceph均支持；
  - 在线创建镜像：镜像仓库和Ceph支持；
  - 关机创建镜像：镜像仓库、Sftp、Ceph均支持。
- 支持数据清理功能，清理镜像服务器中已被彻底删除的无效数据，释放存储空间。

注:

- 例如，将某镜像文件彻底删除，并将使用该镜像创建的云主机彻底删除，这时执行数据清理操作，就可释放镜像服务器的存储空间；
- 仅ImageStore类型的镜像服务器支持该操作。

10.6 SAN存储

ZStack支持的SAN存储，目前支持添加iSCSI服务器。

iSCSI服务器

ZStack支持添加iSCSI服务器，无需进入每个物理机进行配置，即可自动登录iSCSI。支持自动在线扫描并发现磁盘和自动配置iSCSI发起等操作，方便快捷。

FC存储

ZStack支持FC存储透传，直观的展示透传后的FC存储详情，并且透传后的块设备可直接加载到云主机使用。

11 网络资源

11.1 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。

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

路由器/云主机状态	右上角圆点颜色
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

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*Table 1*。

11.2 二层网络资源

11.2.1 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。

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。

注意事项

- VXLAN Pool和VxlanNetwork作为一组基于三层网络上叠加的逻辑定义的二层网络，是专门提供VxlanNetwork使用，在使用VxlanNetwork前，需要先建立VXLAN Pool。与集群发生关系的是三层VTEP，基于VTEP进行VXLAN报文的封装和解封装。创建完毕VXLAN Pool后，可指定或随机选择Vni来创建VxlanNetwork。最后基于VxlanNetwork来创建三层网络，再创建云主机。
- VXLAN Pool挂载集群时，需检查集群内所有的物理主机在对应网段是否存在可用IP来匹配VTEP，如果不存在，则此VXLAN Pool不能正确挂载集群。
- 只有VXLAN Pool可以挂载集群和卸载集群的操作，VxlanNetwork作为VXLAN Pool的子资源，不可进行挂载集群和卸载集群的操作。

11.2.2 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。

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。

注意事项

使用二层网络需注意：

- NovlanNetWork和VlanNetwork作为一组物理定义的二层网络，主要差异在于是否支持Vlan，在添加时，指定的是网卡设备号，与物理主机网卡端口在交换机端的设置应相同。
- NoVlanNetWork、VlanNetwork、以及VXLAN Pool均可挂载集群，VxlanNetwork只是Vni Range的子集，不能挂载集群。
- 当使用Vlan设备时，无需在物理主机上创建带有Vlan号的网卡，例如eth0.2016，用户只需要输入设备名为eth0，Vlan号为2016，ZStack就会自动创建eth0.2016。如果已经存在eth0.2016网络设备时，用户又输入了Vlan号为2016，ZStack会创建一个新的名为eth0.2016.2016的网络设备。

11.3 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。
- 存储心跳网络

  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CIDR，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。

11.4 扁平网络

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：

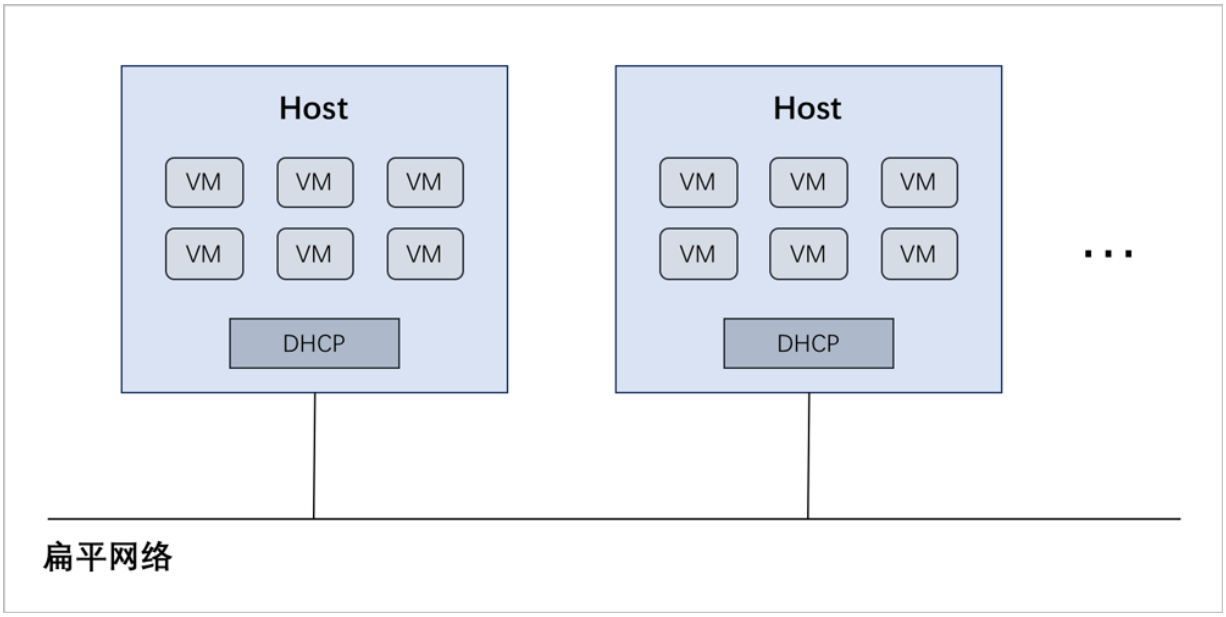
- User Data：使用cloud-init进行云主机开机加载并执行特定的用户数据，例如ssh-key注入。
- 弹性IP：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
- DHCP：分布式DHCP实现动态获取IP地址。

  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 *94:* 扁平网络架构图所示：

图 94: 扁平网络架构图



注意事项

使用扁平网络需注意：

- 扁平网络在每台物理主机上均独立运行DHCP服务器进行云主机IP地址的分配。
- 扁平网络使用dnsmasq来提供DHCP服务。
- 如果某物理主机上所有的云主机都无法获取IP，此时需要在物理主机上检查dnsmasq进程及*/var/lib/zstack/dnsmasq/*对应二层网卡目录下的dnsmasq.log日志。
- 扁平网络使用Linux的namespace和iptables来实现弹性IP的转发。
- 扁平网络的弹性IP需要云主机存在通向私网网关的默认路由。

- 添加IPv4类型网络段时，需要注意以下情况：
  - 不可将网关、广播地址和网络地址包含在添加的IP段中
  - 私有网络网络段，不可与云路由规格里的公有网络或管理网络重叠
- 添加IPv6类型网络段时，需要注意以下情况：
  - 采用Stateless-DHCP或SLAAC分配方式时，用户需手动修改云主机的IP地址生成方式为EUI64
  - 前缀长度范围为64~126，若设置值小于64，将导致云主机创建失败
  - 不可将网关包含在添加的IP段中

11.5 云路由网络

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：

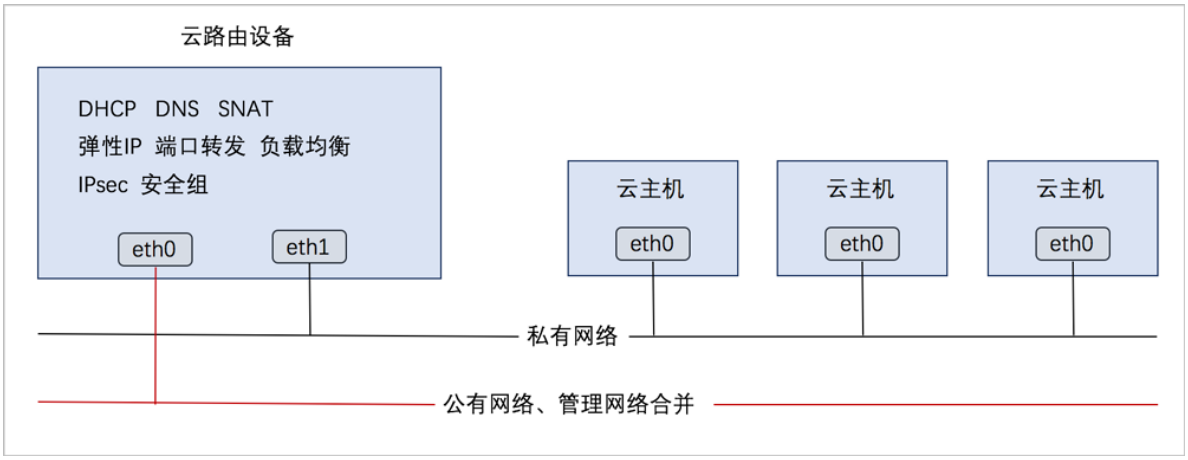
  也称之为业务网络或接入网络，是云主机使用的内部网络。

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 95: 部署方式-1所示：

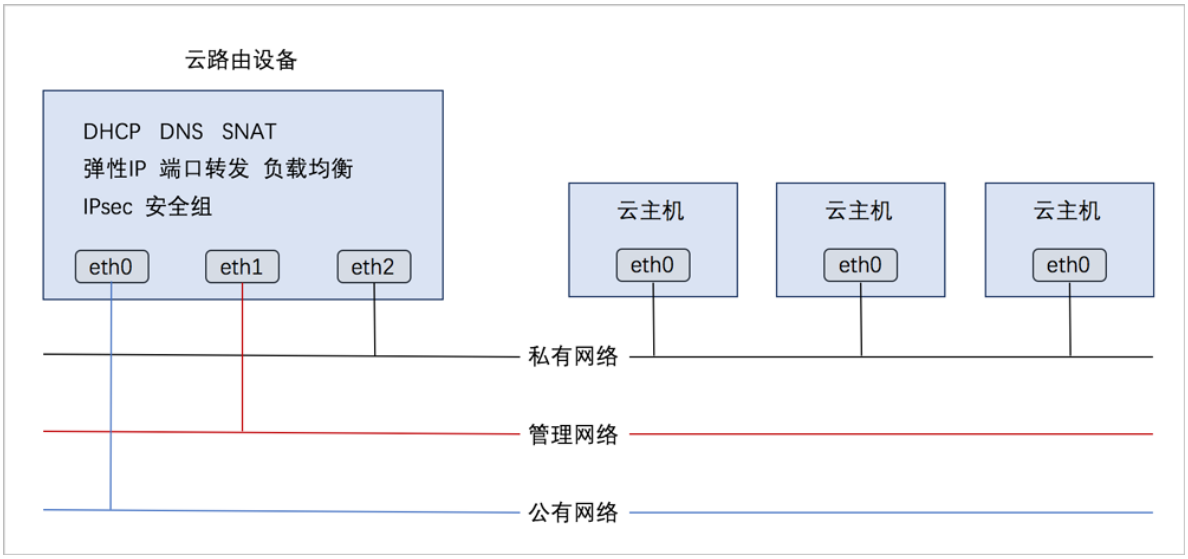
图 95: 部署方式-1



- 公有网络、管理网络、私有网络均独立部署

如图 96: 部署方式-2所示：

图 96: 部署方式-2



云路由网络服务

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

- DHCP：
  - 在云路由器中，默认由扁平网络服务模块提供分布式DHCP服务；

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

云路由网络使用注意事项

使用云路由网络需注意：

- 需先建立公有网络、再建立管理网络，再建立云路由规格，再创建云路由私有网络，在创建云主机时，会自动创建云路由器。
- 创建云路由器至少需要一个集群，同时挂载了管理网络、公有网络、私有网络，而且此集群要求有可用物理主机来创建云路由器。
- 创建云路由规格时，管理网络可从系统网络和公有网络里选择，如果公有网络和管理网络合一，需选择公有网络作为管理网络；如果存在独立的管理网络，则需在系统网络选择。

  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。
- 云路由器的默认IP为公有网络的IP，会从公有网络的网络段中选择IP地址，提供各种网络服务。

- 云路由器的私有网络段地址如果是类似*192.168.0.0/24*，那么云路由器的私网IP默认为*192.168.0.1*，并以此作为使用此云路由网络的普通云主机的默认网关。普通云主机使用此网关，在云路由器里，进行路由转发以访问互联网。
- 云路由器中公有网络、管理网络、私有网络或其他网络的网络段之间，其CIDR不可重叠。

  例如，假定私有网络网络段为*10.0.0.0/8*，云路由器加载网络时，新的网络段就不可为*10.20.0.0/16*，后者作为前者的子集，存在IP地址冲突的风险。
- 在云路由网路场景下，可通过设置私有网络接口IP为云路由器配置双网关，从而实现更好的分布流量，提高网络灵活性和稳定性；该私有网络接口IP不能与基本设置中的IP范围有重叠，但要与基本设置中的网关能互通；设置私有网络接口IP后，还需在交换机上配置相应的策略路由，该场景才可正常工作。

路由表和路由条目使用注意事项

云路由器支持加载多网卡，并支持路由表和路由条目，使用时需注意：

- 加载多网卡一般用于多网互联的场景，例如混合云互通。
- 云路由器支持加载路由表，加载后，路由表内的路由条目会添加至云路由器，对使用云路由的私有网络进行相应的路由功能。
- 添加路由条目时，需指定目标网段，并输入下一跳的地址，需确保下一跳可达。 路由类型一般设置静态路由。为防止环路，也可设置黑洞路由，表示丢弃匹配的数据包。路由优先级的数字越大，表示优先级越低。

如果打算两个云路由器的私有网络互通，需设置以下路由：

前提：

1. 云路由器1

   公网IP *10.58.22.144*
   私有网络段 *172.24.0.0/24*
2. 云路由器2

   公网IP *10.58.23.84*
   私有网络段 *192.168.1.0/24*

执行以下步骤进行互通：

1. 创建路由表1，挂载到云路由器1，添加路由条目下一跳为云路由器2的公网IP *10.58.23.84*，目标网络段为*192.168.1.0/24*
2. 创建路由表1，挂载到云路由器2，添加路由条目下一跳为云路由器1的公网IP *10.58.22.144*，目标网络段为*172.24.0.0/24*

云路由器创建失败检查事项

云路由器创建失败需检查：

- 云路由规格定义的镜像：
  - 如果存放在ImageStore镜像服务器，则应存在挂载了本地存储、NFS、SharedMountPoint、或者Ceph主存储的集群；
  - 如果存放在Sftp镜像服务器，则应存在挂载了本地存储、NFS或者SharedMountPoint主存储的集群；
  - 如果存放在Ceph镜像服务器，则应存在挂载了此Ceph镜像服务器对应的Ceph主存储的集群；
- 需存在可用集群同时加载了公有网络、管理网络和私有网络，此集群内有可用的物理主机满足云路由规格定义的CPU、内存大小。
- 为了防止恶意攻击，云路由器默认禁止ssh密码登录。可在全局配置中打开。

11.6 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

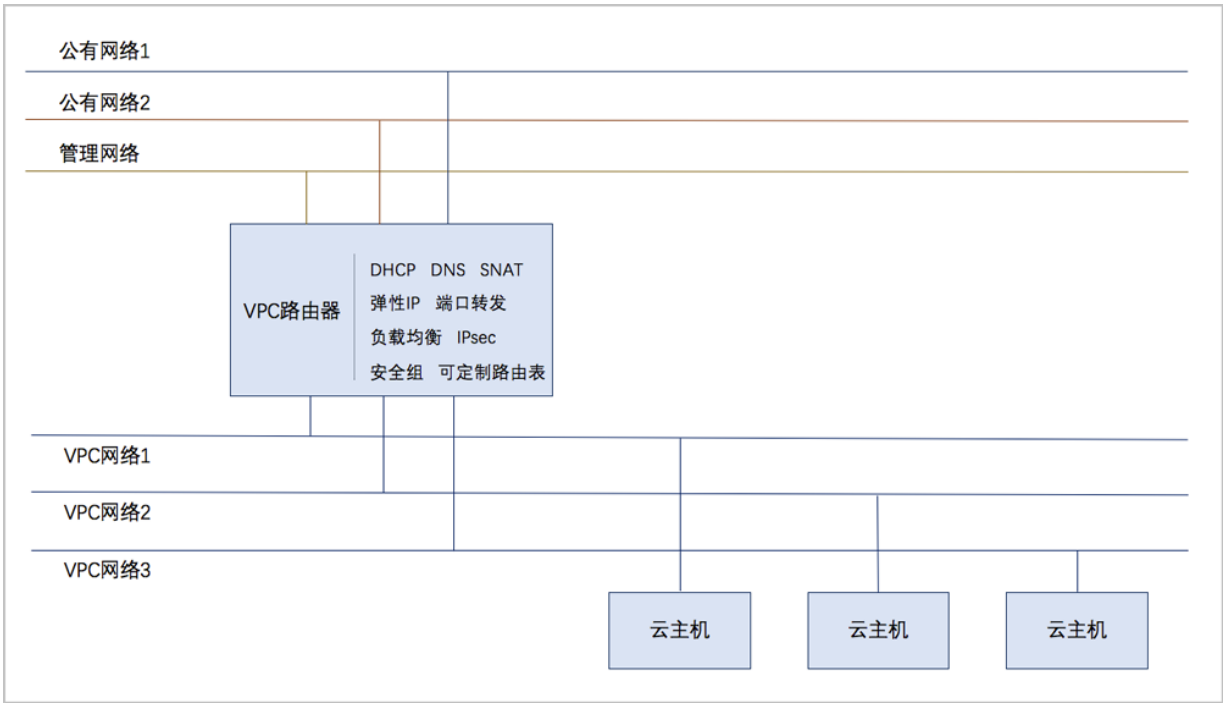
VPC由VPC路由器和VPC网络组成。

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

- 新建的网络段不可与VPC路由器内任一网络的网络段重叠。

VPC网络拓扑如图 *97: VPC网络拓扑示意图*所示：

图 97: VPC网络拓扑示意图



VPC特点

VPC具有以下特点：

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

VPC网络服务

VPC网络作为VPC的私有网络，使用VPC路由器提供各种网络服务。

- DHCP：默认采用扁平网络服务模块提供分布式DHCP服务。
- DNS：VPC路由器作为DNS服务器提供DNS服务。在云主机中看到的DNS地址默认为VPC路由器的IP地址，用户设置的DNS地址由VPC路由器负责转发配置。

- SNAT：VPC路由器向云主机提供原网络地址转换，云主机使用SNAT可直接访问外部互联网。
- 安全组：由安全组网络服务模块提供安全组服务，使用iptables进行云主机防火墙的安全控制。
- 弹性IP：可绑定弹性IP到VPC网络，实现公有网络到云主机私有网络的互联互通。
- 端口转发：提供公网IP到云主机私有网络IP的端口到端口的相关网络协议的互通。
- 负载均衡：将公网地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的互联互通。

11.6.1 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。

VPC路由器 | 普通云路由器 对比

VPC路由器 | 普通云路由器 相同点	VPC路由器 | 普通云路由器 不同点
• 实质相同，均采用vyos实现的Linux云主机作为路由设备； • 均需创建云路由规格定义的公有网络和管理网络、云路由镜像资源； • 均支持DHCP、DNS、SNAT、安全组、弹性IP、端口转发、负载均衡、IPsec隧道等网络服务； • 均不可卸载云路由规格里定义的公有网络和管理网络； • 均支持路由表和路由条目的配置； • 均支持高可用，共享存储下，资源充足的条件下永不停机； • 均支持加载和卸载新的公有网络；	• VPC路由器，可由用户手动创建，普通云路由器目前仅支持随着使用此云路由的私网的云主机一同创建，不支持手动创建； • 手动创建的VPC路由器运行状态可以只有公有网络和管理网络，但普通的云路由器必须存在公有网络、管理网络和私有网络； • VPC路由器，支持加载和卸载VPC网络，普通的云路由器不支持加载和卸载私有网络。

VPC路由器 | 普通云路由器 相同点	VPC路由器 | 普通云路由器 不同点
• 普通的云路由网络可以看做VPC下的一个特例，即只有一个不可卸载的私有网络下的VPC。	

注意事项

使用VPC路由器需注意：

- 需先建立云路由规格里的二层公有网络、三层公有网络、二层管理网络和三层管理网络；
- 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；
- 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。
- 为了防止恶意攻击，VPC路由器默认禁止ssh密码登录。可在全局配置中打开。

11.6.2 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。

VPC网络 | 普通私有网络 对比

VPC网络 | 普通私有网络 相同点	VPC网络 | 普通私有网络 不同点
• VPC路由器/云路由器均支持灵活挂载多公网，云路由规格定义的公有网络不可卸载。VPC路由器/云路由器的默认IP均为云路由规格定义的公有网络的IP，从该公有网络的网络段中选择IP地址，提供各种网络服务。 • 在创建云路由规格时，管理网络可从系统网络和公有网络里面选择，如果公有网络和管理网络合一，需选择公有网络作为管理网	• VPC网络作为VPC的私有网络，使用了VPC路由器提供的各种网络服务，普通私有网络支持扁平网络和云路由两种结构； • VPC路由器支持灵活挂载多个VPC网络。 如果VPC路由器下挂载的某一VPC网络段地址是类似*192.168.0.0/24*，那么VPC路由器对应此VPC网络的私网IP默认为*192.168.0.1*，并以此作为使用此VPC网络的普通云主机的默认网关。

VPC网络 | 普通私有网络 相同点	VPC网络 | 普通私有网络 不同点
络；如果存在独立的管理网络，则需在系统网络选择。 **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。 • 云路由器中公有网络、管理网络、私有网络或其他网络的网络段之间，其CIDR不可重叠。 例如，假定私有网络网络段为*10.0.0.0/8*，云路由器加载网络时，新的网络段就不可为*10.20.0.0/16*，后者作为前者的子集，存在IP地址冲突的风险。 同样地，VPC路由器内任一网络的网络段不可重叠，且新建的VPC网络段不可与VPC路由器内任一网络的网络段重叠。	普通云主机使用此网关，在VPC路由器里，进行路由转发以访问互联网。 • 云路由器允许挂载的普通私有网络有且仅有一个。 如果云路由器的私有网络段地址是类似*192.168.0.0/24*，那么云路由器的私网IP默认为*192.168.0.1*，并以此作为使用此云路由网络的普通云主机的默认网关。 普通云主机使用此网关，在云路由器里，进行路由转发以访问互联网。

路由表和路由条目使用注意事项

VPC路由器支持加载多网卡，并支持路由表和路由条目，使用时需注意：

- 加载多网卡一般用于多网互联的场景，例如混合云互通。
- VPC路由器支持加载路由表，加载后，路由表内的路由条目会添加至VPC路由器，对使用VPC路由器的VPC网络进行相应的路由功能。
- 添加路由条目时，需指定目标网段，并输入下一跳的地址，需确保下一跳可达。 路由类型一般设置静态路由。为防止环路，也可设置黑洞路由，表示丢弃匹配的数据包。路由优先级的数字越大，表示优先级越低。

VPC路由器创建失败检查事项

VPC路由器创建失败需检查：

- 云路由规格定义的镜像：
  - 如果存放在ImageStore镜像服务器，则应存在挂载了本地存储、NFS、SharedMountPoint、或者Ceph主存储的集群；

  - 如果存放在Sftp镜像服务器，则应存在挂载了本地存储、NFS或者SharedMountPoint主存储的集群；
  - 如果存放在Ceph镜像服务器，则应存在挂载了此Ceph镜像服务器对应的Ceph主存储的集群；
- 需存在可用集群同时加载了公有网络、管理网络和私有网络，此集群内有可用的物理主机满足云路由规格定义的CPU、内存大小。

12 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。

12.1 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。

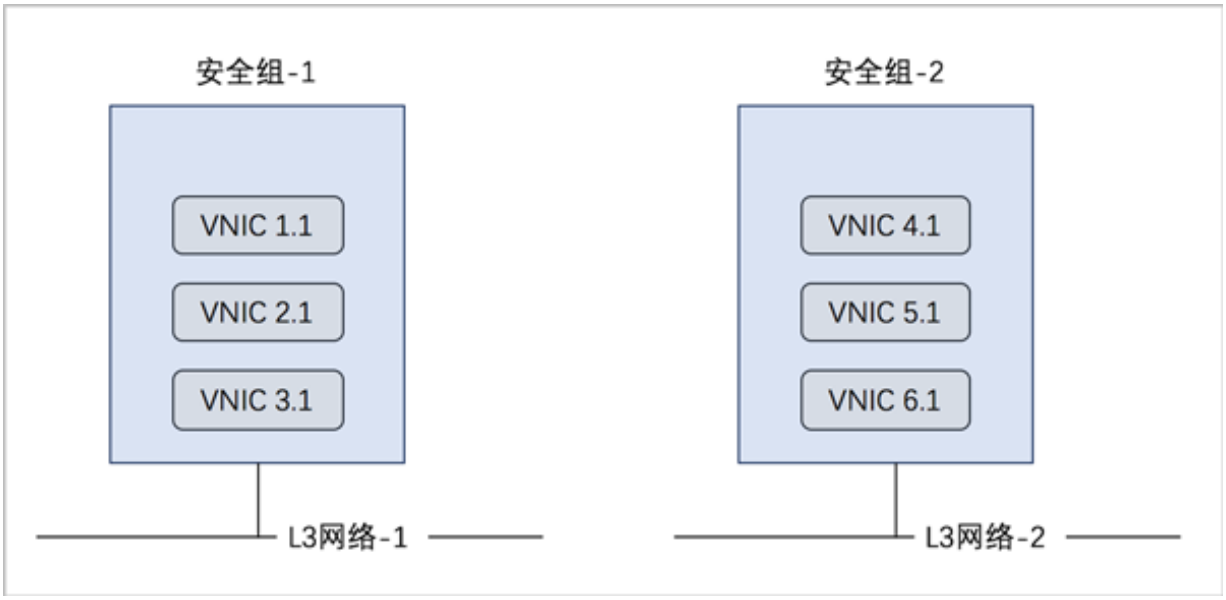
安全组规则：

- 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 *98:* 安全组所示：

图 98: 安全组



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。

12.2 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。

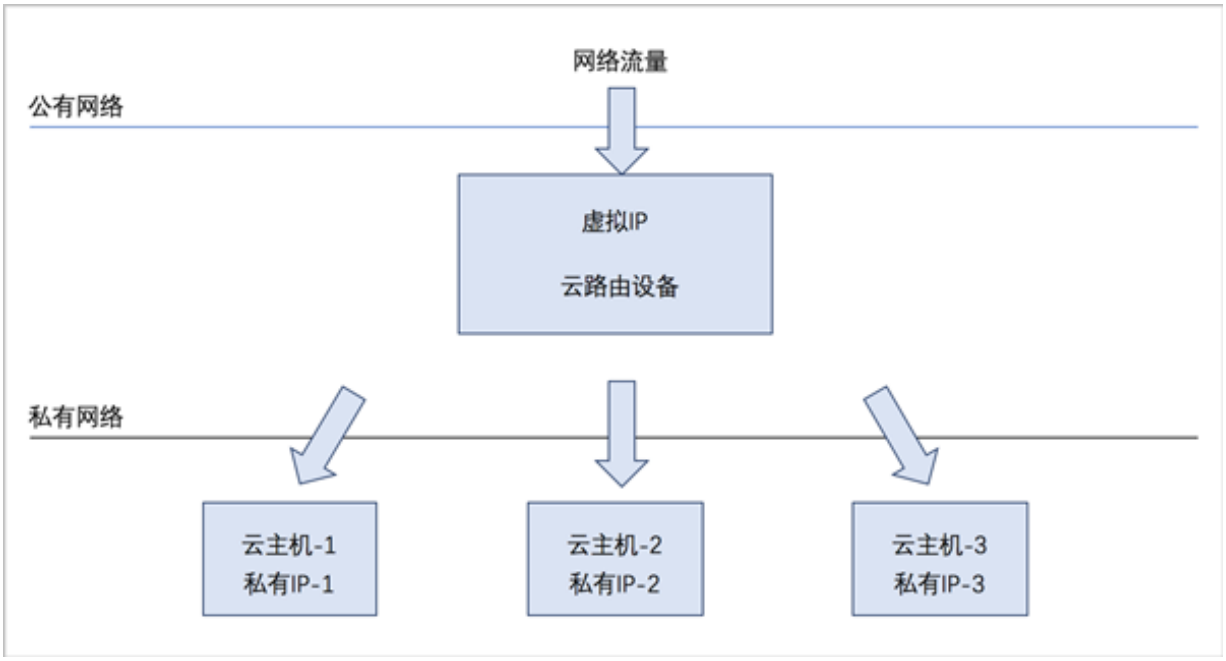
    注: 不同类型服务不能使用相同的端口号。

  - 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 *99: 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 99: 虚拟IP-负载均衡



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。

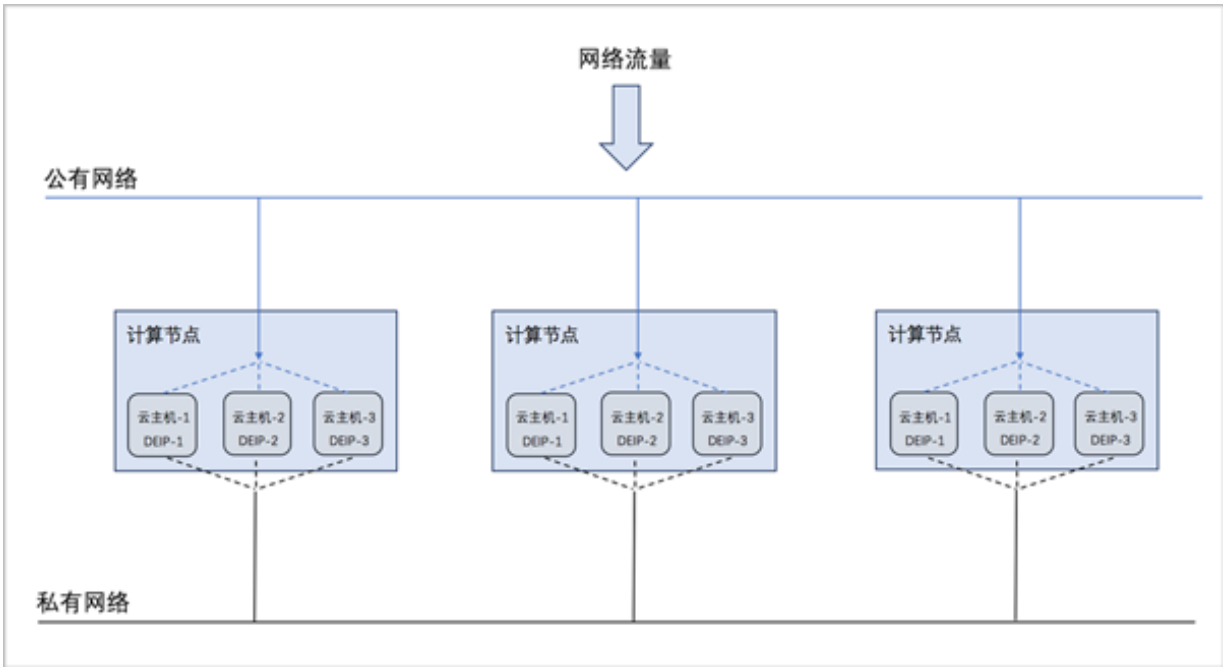
12.3 弹性IP

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 *100: 扁平网络下弹性IP的应用场景*所示：

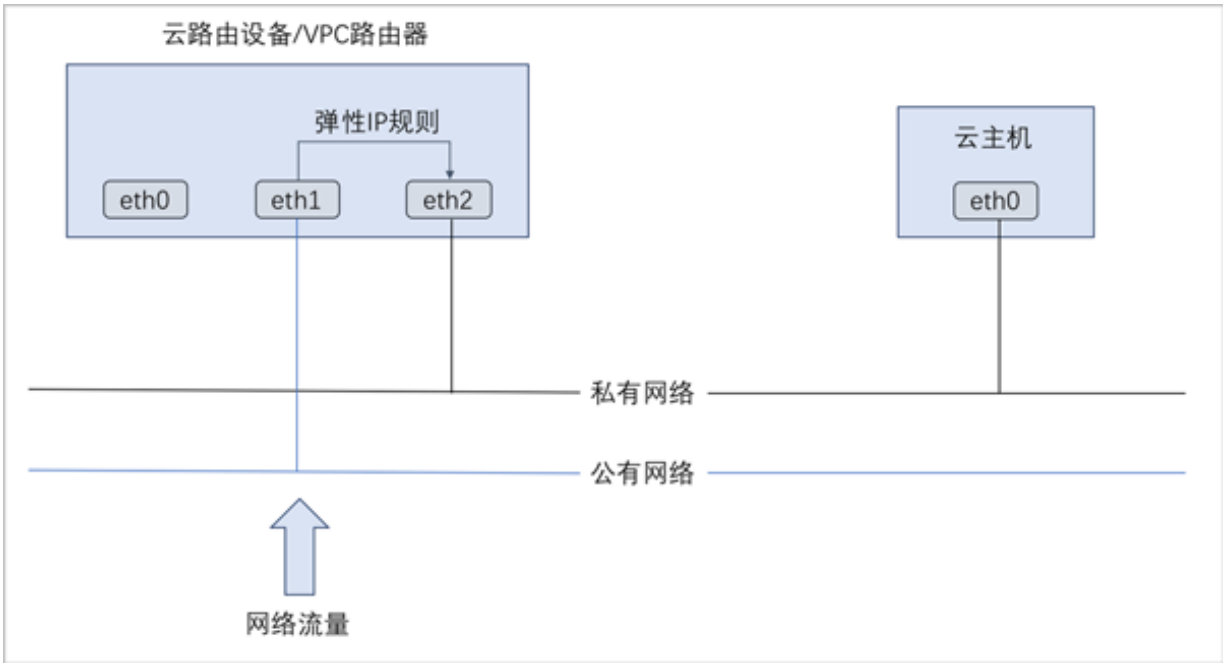
图 100: 扁平网络下弹性IP的应用场景



- 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 *101: 云路由网络/VPC下弹性IP的应用场景*所示：

图 101: 云路由网络/VPC下弹性IP的应用场景



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。

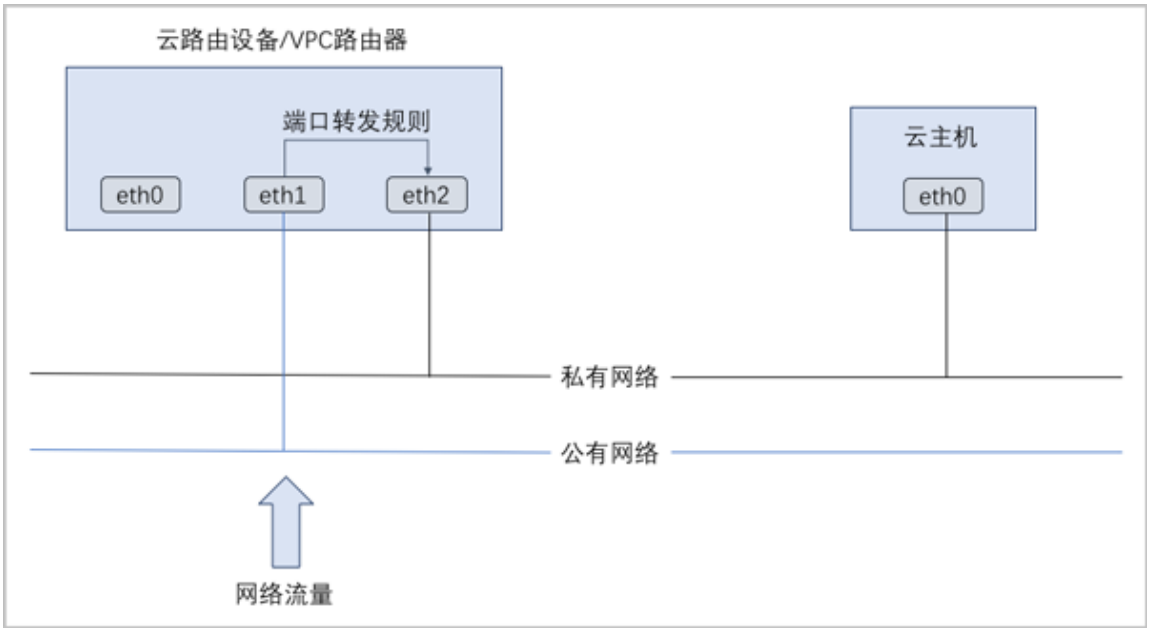
12.4 端口转发

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。

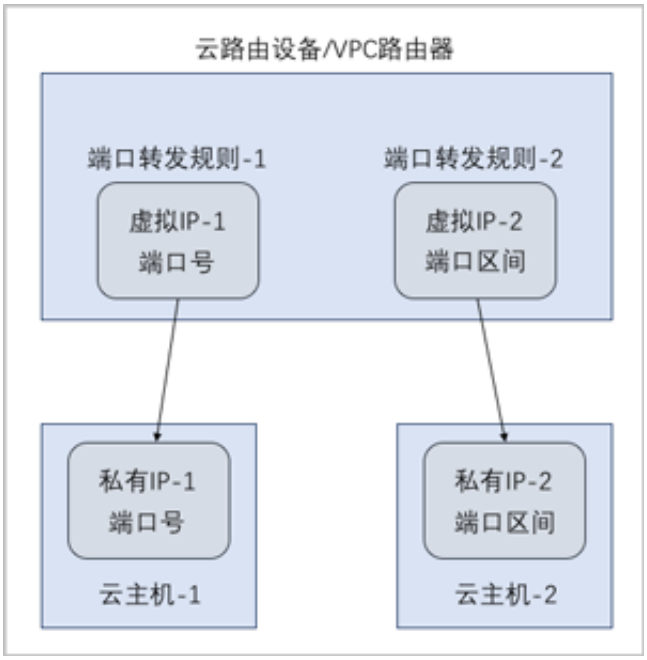
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *102:* 端口转发所示：

图 102: 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 *103:* 虚拟*IP*-端口转发所示：

图 103: 虚拟IP-端口转发



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。

12.5 负载均衡

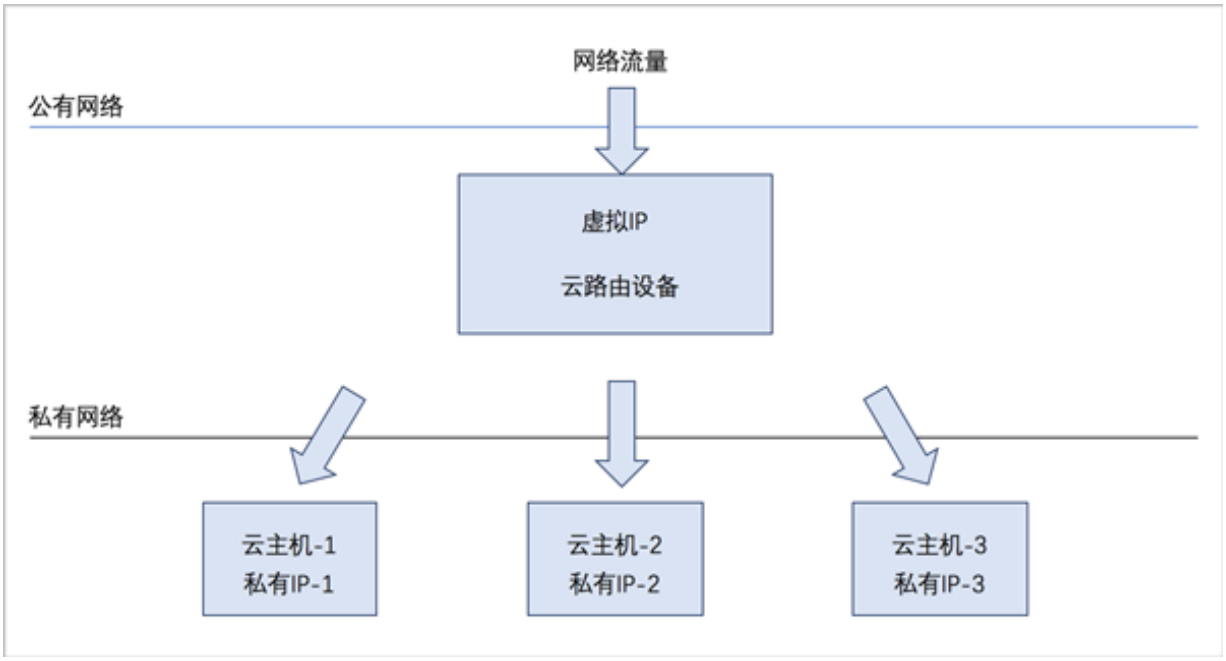
负载均衡（LB）：将公网地址的访问流量分发到一组后端的云主机， 并支持自动检测并隔离不可用的云主机，从而提高业务的服务能力和可用性。

- 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/UDP四种协议。
- 当监听协议为HTTPS，需绑定证书使用，支持上传证书和证书链。
- 负载均衡器支持灵活配置多种转发策略，实现高级转发控制功能。

如图 *104: 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 104: 虚拟IP-负载均衡



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/UDP，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/UDP，该按钮禁用。
- 显示健康数量：监听器页面，支持显示绑定云主机的健康数量，如：健康后端数/后端总数
- 监控数据：支持显示监听器的会话数、监听器进出流量的监控数据
- 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。

注意事项

- 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。
- 负载均衡监听器支持HTTPS协议，需绑定证书使用，支持上传证书和证书链。

12.6 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**

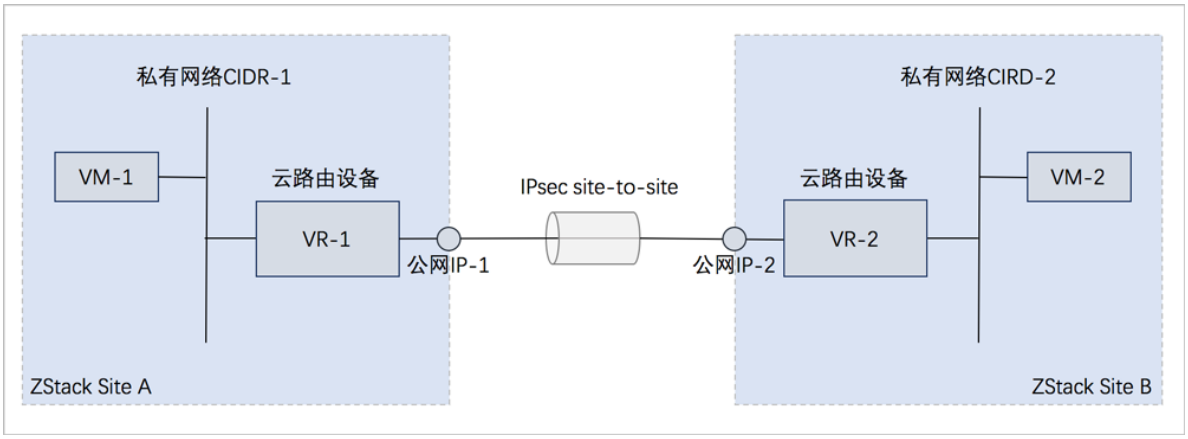
  仅支持基于对端网段配对模型，仅支持路由配对模式，不支持路由转发模式（不支持OSPF或BGP等动态路由协议）。

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 *105: 云路由网络下IPsec隧道应用场景*所示：

  图 105: 云路由网络下IPsec隧道应用场景



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。

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。

13 vCenter

13.1 基础资源

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。

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。

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。

注: 远端vCenter上已部署的vCSA（vCenter Server Appliance）不会同步至本地，避免误操作。

- 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。

13.2 云主机

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。

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。
- 更改所有者：将云主机的所有者更改。

注:

ZStack对接管的vCenter支持多租户管理，普通账户/项目负责人/项目管理员/项目成员可对vCenter云主机进行相关操作。

- 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：打开云主机的控制台，可以登录控制云主机。

注:

ZStack接管vCenter后，原本运行的vCenter云主机不能直接打开控制台；

只有满足以下任一条件的vCenter云主机，才能直接打开控制台：

- 通过ZStack创建的vCenter云主机
- 通过ZStack重启的vCenter云主机
- 通过ZStack进行动态迁移的vCenter云主机（基于共享存储）

- 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。
- 加载网卡：将一个可用的网卡加载到当前云主机，支持加载公有网络、私有网络。
- 卸载网卡：之前添加的网卡从云主机卸载。
- 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。

13.3 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。

云路由网络

vCenter云路由网络搭建流程：

1. 在vCenter的网络界面创建公有网络（包括二层公有网络和三层公有网络）。
2. 在创建vCenter云路由网络前，需提前在云路由界面添加云路由镜像和云路由规格。
3. 创建vCenter云路由网络。

注意事项：

- 搭建vCenter云路由网络，需提前确认ZStack管理节点与vCenter物理主机能互相访问。
- 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。
- 支持L2NoVlanNetwork、L2VlanNetwork两种类型，如选择L2VlanNetwork，需输入Vlan ID

扁平网络

vCenter扁平网络搭建流程：

- 在vCenter的网络界面创建扁平网络对应的二层网络和三层网络。

注意事项：

- 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
- 支持L2NoVlanNetwork、L2VlanNetwork两种类型，如选择L2VlanNetwork，需输入Vlan ID

vCenter网络支持的操作

- vCenter公有网络：添加网络段、添加DNS、全局共享、全局召回、删除、修改名称和简介、加载集群、删除网络段、删除DNS、共享给指定账户/项目、从指定账户/项目召回
- vCenter扁平网络：添加网络段、添加DNS、全局共享、全局召回、删除、修改名称和简介、加载集群、删除网络段、删除DNS、共享给指定账户/项目、从指定账户/项目召回
- vCenter云路由网络：添加网络段、添加DNS、加载云路由规格、卸载云路由规格、全局共享、全局召回、删除、改名称和简介、加载集群、删除网络段、删除DNS、共享给指定账户/项目、从指定账户/项目召回

注:

- ZStack对接管的vCenter支持多租户管理，普通账户/项目负责人/项目管理员/项目成员可使用admin共享的vCenter网络。
- 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。）

13.4 网络服务

vCenter支持的网络服务

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。

13.4.1 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)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。

13.4.2 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。

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。

13.4.3 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。

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。

13.4.4 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/UDP，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/UDP，该按钮禁用。
- 显示健康数量：监听器页面，支持显示绑定云主机的健康数量，如：健康后端数/后端总数
- 监控数据：支持显示监听器的会话数、监听器进出流量的监控数据
- 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。

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。

13.4.5 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。

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。

13.5 云盘

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。

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。
- 更改所有者：将云盘的所有者更改。

注:

ZStack对接管的vCenter支持多租户管理，普通账户/项目负责人/项目管理员/项目成员可对vCenter云盘进行相关操作。

- 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。

13.6 镜像

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。

vCenter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。

- 全局共享：将镜像进行全局共享，所有普通账户/项目均可使用此镜像。
- 全局召回：将已全局共享的镜像进行全局召回，其它账户/项目均看不见此镜像。
- 共享：将镜像共享给指定账户/项目。
- 召回：将已共享的镜像从指定账户/项目召回。
- 更改所有者：将镜像的所有者更改。
- 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。

14 平台运维

14.1 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。

- 物理主机页面：

  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。

- 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。

- 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。

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。

14.2 性能分析

ZStack平台管理提供对已运行云主机、云路由、物理主机的实时性能分析。其中：

- **云主机、路由器、物理主机**：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
- **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
- **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
- **镜像服务器**：显示了名称、镜像存储可用容量百分比信息
- **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%

14.3 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。

- 监控数据默认保存6个月，在高级设置中可自定义设置监控数据保留周期，设置方法如下：在**设置** > **高级设置**页面，可设置**监控数据保留周期**，默认为6，单位为月，可设置1到12之间的整数。

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。

- 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。
- 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。

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

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

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。

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

14.4 通知服务

用户可以用不同的接收端订阅主题，接收端类型包括：系统、邮箱、钉钉、HTTP应用。

- 系统默认提供一个系统类型接收端，若报警器绑定系统类型接收端，UI界面右上角的最近消息按钮处会出现弹窗提醒。
- 用户也可自行创建邮箱/钉钉/HTTP应用类型接收端。

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。

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。

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。

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

14.5 消息中心

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。

14.6 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。

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。

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。

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。

14.7 资源编排

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 *106:* 资源编排所示：

图 106: 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. 云平台提供示例模板，也可使用可视化编辑器，快速创建资源栈模板；
3. 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；
4. 如果不再需要某资源栈，可一键删除该栈及栈内所有资源；
5. 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；
6. 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。

14.7.1 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

14.7.2 资源栈模板

用于创建资源栈的模板，创建资源栈模板需遵循模板编辑语法。

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

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

14.7.3 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

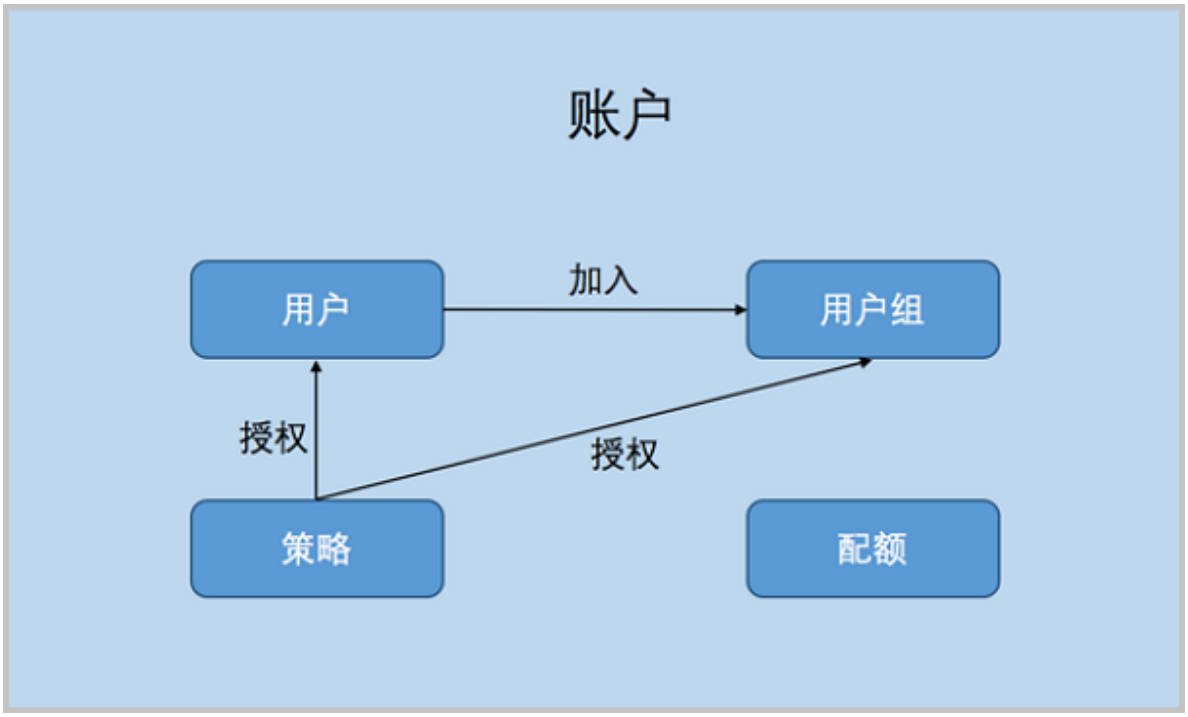
15 平台管理

15.1 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 *107:* 用户管理系统所示：

图 107: 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。

15.2 计费管理

计费管理包括账单和计费设置

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。

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。

15.3 定时

15.3.1 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。

定时器执行策略：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。**

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

15.3.2 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。

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

15.4 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。

15.5 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。

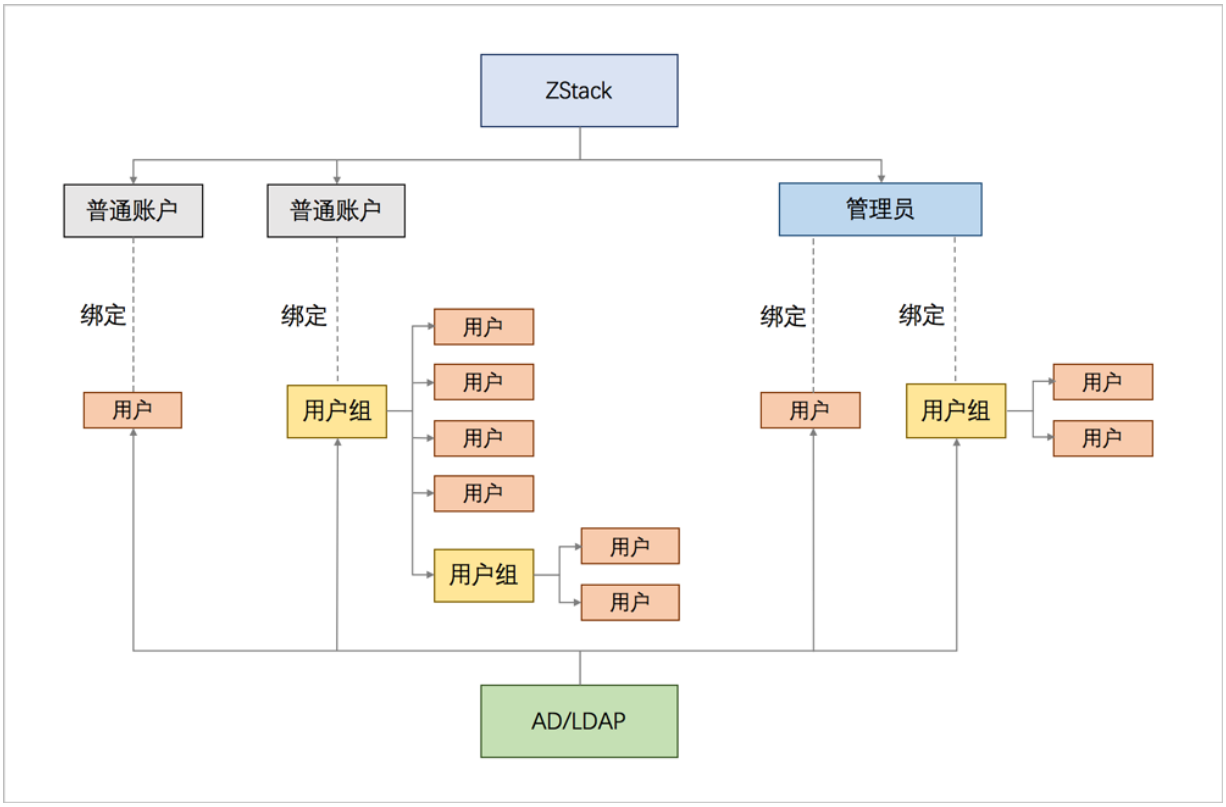
15.6 AD/LDAP

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 108: ZStack-AD/LDAP绑定关系*所示：

图 108: ZStack-AD/LDAP绑定关系



添加AD/LDAP

ZStack支持基于自定义规则添加AD/LDAP服务器。

绑定AD/LDAP成员

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

AD/LDAP登录

使用已设置的AD/LDAP成员登录属性直接登录ZStack云平台。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。

15.7 控制台代理

ZStack平台管理支持显示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。

- 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。
  - 控制台代理地址可填写：管理节点公网IP地址、NAT地址、域名，不支持设置端口；
  - 无需重启管理节点，直接生效。

15.8 证书

遵守数字证书协议，受信任的数字证书颁发机构CA，在验证服务器身份后颁发，具有服务器身份验证和数据传输加密功能。

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。

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。

16 高级功能(Plus)

ZStack提供以下高级功能：

- 企业管理
- 裸金属管理
- 灾备服务
- 迁移服务

高级功能以单独的功能模块形式提供，需提前购买相应的模块许可证（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。

16.1 企业管理

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、工单管理、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。

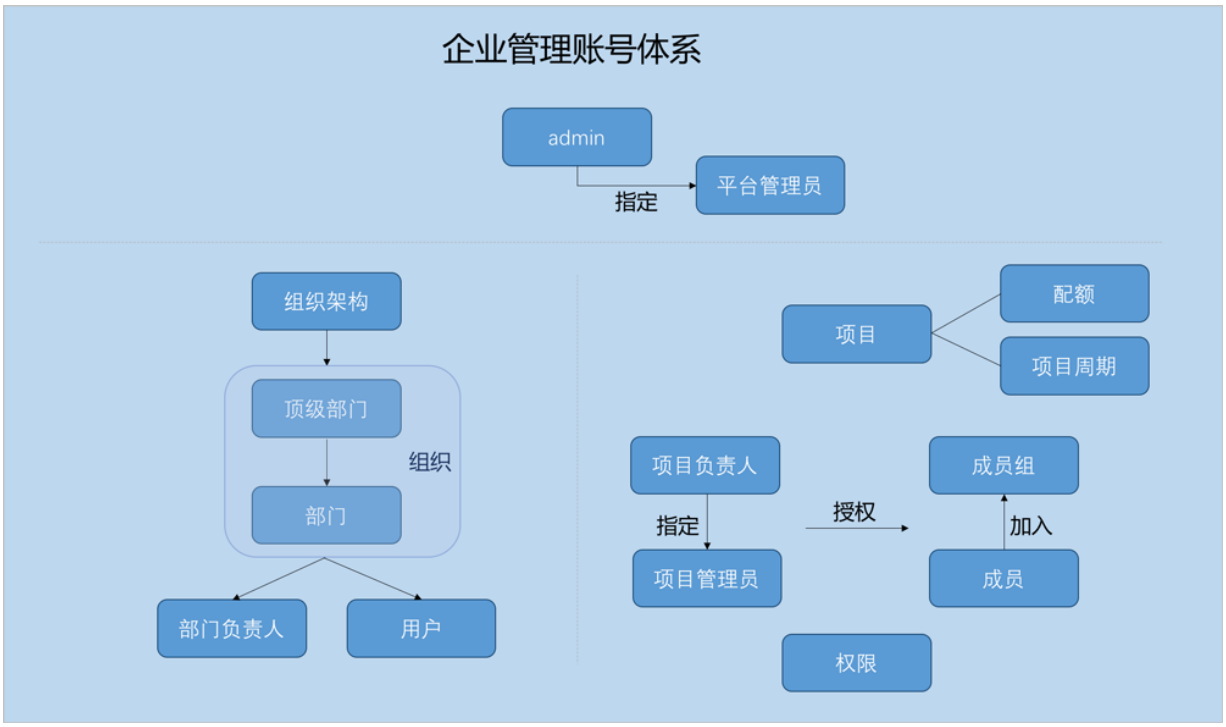
企业管理账号体系

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 *109:* 企业管理账号体系所示：

图 109: 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：
    - 项目有效期限不足7天时，项目负责人/项目管理员/项目成员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。
    - 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 *110:* 主登录界面所示：

图 110: 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 *111:* 项目登录界面所示：

  图 111: 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**、**工单管理**、**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。

  详情可参考项目管理详解章节。

- **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，通过admin为每个项目创建的自定义工单审批流程，对工单进行审批，最终由admin进行一键审批部署，资源将自动部署成功并分发到项目中。

  详情可参考工单管理详解章节。

- **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。

详情可参考独立区域管理详解章节。

16.1.1 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。

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

16.1.2 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**：

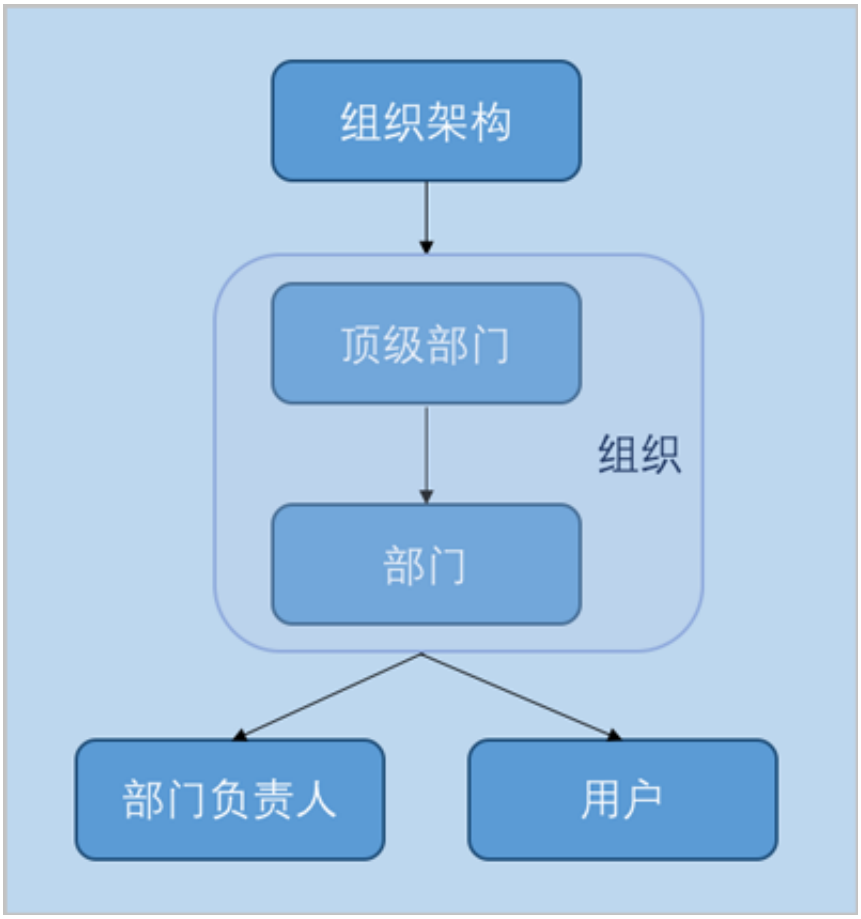
组织是企业管理中组织架构的基本单位，admin/平台管理员可基于用户建立相应的组织架构，组织可分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门。

- **部门负责人**：

  创建组织，需指定相应的用户作为部门负责人。

组织架构相关概念如图 *112: 组织架构相关概念*所示：

图 112: 组织架构相关概念



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

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

16.1.3 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。

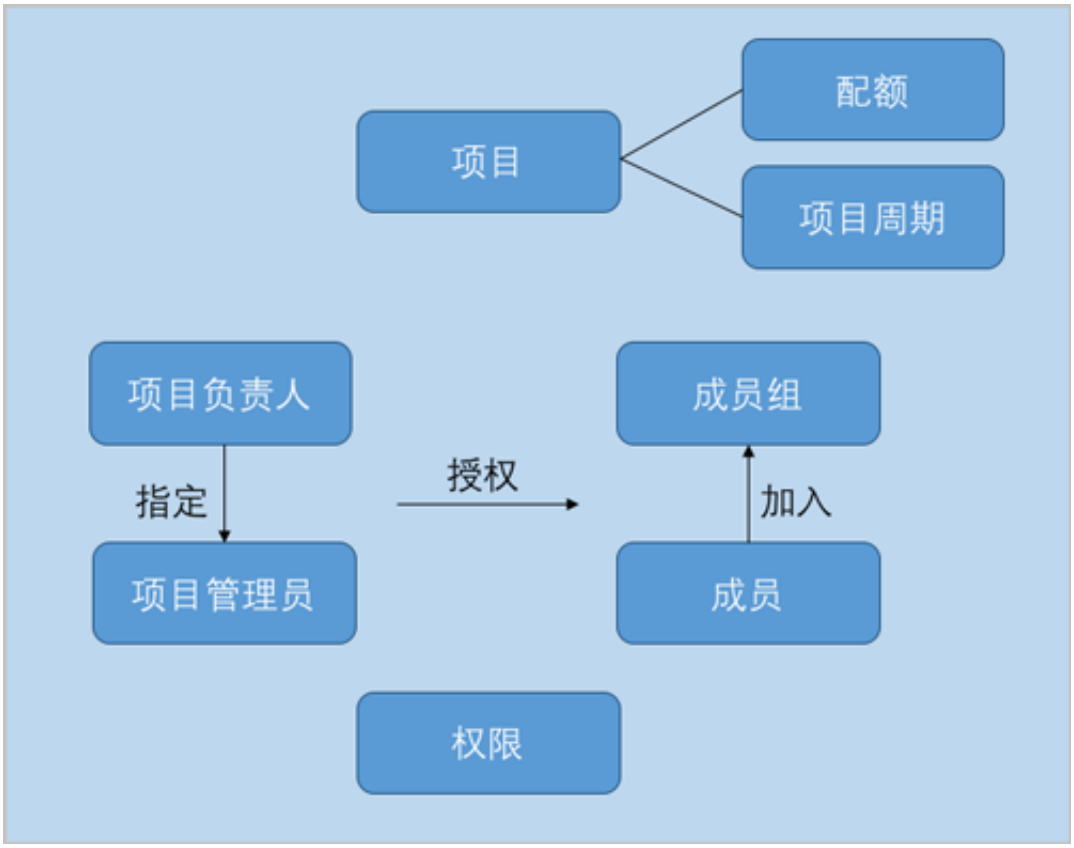
- **项目周期**：

  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：
  - 项目有效期限不足7天时，项目负责人/项目管理员/项目成员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。
  - 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。

项目管理相关概念如图 *113:* 项目管理相关概念所示：

图 113: 项目管理相关概念



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：将成员从项目移除，不允许将项目负责人/项目管理员从项目移除
- 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

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，可参考项目管理详解章节。

16.1.4 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，通过admin为每个项目创建的自定义工单审批流程，对工单进行审批，最终由admin进行一键审批部署，资源将自动部署成功并分发到项目中。

16.2 裸金属管理

ZStack提供裸金属管理服务，可为应用提供专属的物理服务器，保障核心应用的高性能和稳定性。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UI界面批量部署裸金属设备，部署完成后可使用裸金属设备创建裸金属主机，支持自定义安装操作系统，并对裸金属主机进行全生命周期管理。

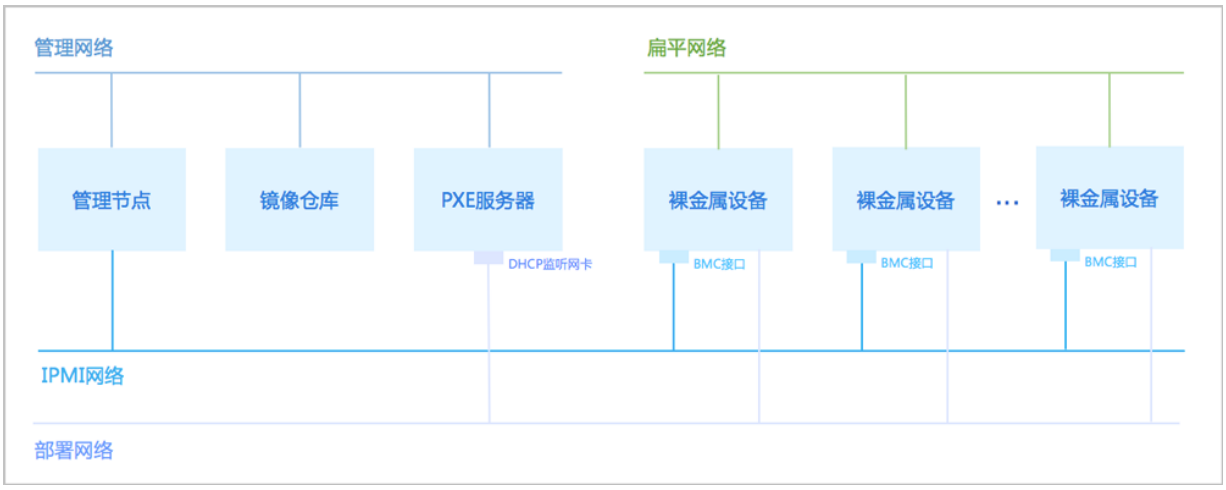
裸金属管理服务以单独的功能模块形式提供，需提前购买裸金属管理模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

基本原理

裸金属管理服务的基本原理是：PXE服务器提供DHCP服务和FTP服务，指示多台裸金属设备由PXE网卡启动并分配动态IP，裸金属设备从PXE服务器中下载相关软件包，用于裸金属主机的系统安装。

网络拓扑如图 *114:* 裸金属管理网络拓扑所示：

图 114: 裸金属管理网络拓扑



功能优势

裸金属管理服务具有以下功能优势：

- 为应用提供专属的物理服务器，保障核心应用的高性能和稳定性；
- 推荐独立部署PXE服务器，可满足多管理节点物理机高可用场景需求，而且网络环境更加简单，一定程度避免DHCP冲突，由于每个裸金属集群均可挂载独立的PXE服务器，避免单点故障，大幅提升部署效率；

- 管理员可在UI界面上批量添加裸金属设备，包括：手动添加和模板文件导入两种方式，支持批量添加IPMI地址，高效部署裸金属集群，提升运维效率；
- 支持自定义安装操作系统，目前支持的操作系统版本包括：RHEL/CentOS系列 6.X和7.X 版本ISO（非LiveCD）；
- 支持扁平网络场景，同一个二层网络上的裸金属主机和云主机之间可互相访问，无需通过网关进行路由。

典型应用场景

裸金属管理服务适用于以下典型应用场景：

- 高安全严监管场景

  例如金融、证券行业对业务部署的合规性、数据安全有苛刻要求，采用裸金属管理服务，可确保资源独享、数据隔离、可监管可追溯。

- 高性能计算场景

  例如超算中心、基因测序等高性能计算场景，对服务器的计算性能、稳定性和实时性要求很高。虚拟化带来的性能损耗和超线程对裸金属服务器影响不大，部署一定规模的裸金属集群可满足高性能计算的需求。

- 核心数据库场景

  由于客户业务需要，某些核心数据库业务不能部署在虚拟机上，必须通过资源专享、网络隔离、性能有保障的物理服务器承载。采用裸金属管理服务，可为应用提供专属的高性能物理服务器，可满足该场景下的业务需求。

16.2.1 裸金属集群

裸金属集群：为裸金属设备提供单独的集群管理。

- 裸金属集群必须挂载部署服务器，才能为集群中的裸金属主机提供PXE服务；
- 一个裸金属集群只允许挂载一个部署服务器，一个部署服务器可同时挂载到多个裸金属集群；
- 裸金属集群可挂载二层网络，为集群中裸金属主机提供网络服务；
- 支持扁平网络场景，同一个二层网络上的裸金属主机和云主机之间可互相访问，无需通过网关进行路由。

裸金属集群支持以下操作：

- 创建裸金属集群
- 查看裸金属集群详情

- 启用/停用裸金属集群
- 加载/卸载二层网络
- 加载/卸载部署服务器
- 删除裸金属集群

16.2.2 部署服务器

部署服务器：可单独指定服务器作为部署服务器（或称：PXE服务器），为裸金属设备提供PXE服务和控制台代理服务。

- 推荐独立部署PXE服务器，满足多管理节点物理机高可用场景需求，且避免单点故障，大幅提升部署效率；
- 要求部署服务器挂载到裸金属集群中；
- 一个裸金属集群只允许挂载一个部署服务器，一个部署服务器可同时挂载到多个裸金属集群；
- 要求部署服务器有足够的存储空间，保存用于PXE部署的镜像；
- 要求部署服务器连接到管理网络，与管理节点连通；
- 要求部署服务器连接到部署网络，与裸金属设备连通；
- 要求部署服务器上的DHCP监听网卡连接到部署网络，并保证该部署网络上不存在其他DHCP服务，以免冲突；
- 要求部署服务器安装最新版ZStack定制版ISO（推荐c74版），否则部署服务器无法通过FTP服务为裸金属设备提供软件包。

部署服务器支持以下操作：

- 创建部署服务器
- 查看部署服务器详情
- 启用/停用部署服务器
- 重连部署服务器
- 加载/卸载裸金属集群
- 删除部署服务器

注意事项

- 要求DHCP监听网卡连接到裸金属设备部署网络，且已配置IP地址
- 要求DHCP监听网卡是一个独立的、有IP地址的网卡，对外提供稳定的DHCP服务
- 要求DHCP监听网卡所在的部署网络内不能存在其它DHCP服务，以免冲突

- 要求部署服务器有足够的存储空间，保存用于PXE部署的镜像
- 停用部署服务器，相应集群内的裸金属设备将不能获取硬件信息，也不能用于创建裸金属主机
- 一个裸金属集群只允许挂载一个部署服务器，一个部署服务器可同时挂载到多个裸金属集群
- 卸载裸金属集群将导致部署中的裸金属主机彻底删除，已部署的裸金属主机无法打开控制台，请谨慎操作
- 删除部署服务器将导致部署中的裸金属主机彻底删除，已部署的裸金属主机无法打开控制台，请谨慎操作

16.2.3 裸金属设备

裸金属设备：待安装操作系统的裸金属服务器，通过BMC接口以及IPMI配置进行唯一识别。通过IPMI网络，管理节点可远程控制裸金属设备的开关机、网络启动、磁盘启动等行为。支持admin在UI界面上完成所有裸金属设备的批量部署。

- 要求管理节点连接到IPMI网络，通过IPMI远程控制裸金属设备；
- 要求裸金属设备配备BMC接口，配置IPMI地址、端口、用户名、密码，并连接至IPMI网络；
- 要求裸金属设备的PXE启动网卡连接至部署网络；
- 裸金属设备的其他网卡按需连接至相应的二层网络。

裸金属设备支持以下操作：

- 添加裸金属设备
- 查看裸金属设备详情
- 启用/停用裸金属设备
- 开机/关机/重启
- 获取硬件信息
- 删除裸金属设备

补充说明

裸金属设备的**部署状态**、**启用状态**、**电源状态**总结如下：

部署状态	备注
硬件信息未知	裸金属设备未能获取硬件信息 **注:** • 可能原因：添加裸金属设备时未勾选**重启裸金属设备**，添加完成后，裸

部署状态	备注
	金属设备的部署状态为：硬件信息未知； • 解决办法：手动**重启**裸金属设备，或手动**获取硬件信息**。
PXE启动中	PXE服务器远程指示裸金属设备由PXE网卡启动并分配动态IP
PXE启动失败	裸金属设备由PXE网卡启动失败 **注:** 请检查以下事项，是否满足要求： • 确保部署网络内除了部署服务器没有其它DHCP服务； • 确保裸金属设备连接部署网络的网卡在BIOS中开启PXE功能； **注:** • 对于部分机型，还需确保该PXE网卡为首张启动网卡，或确保（启动顺位）在PXE网卡之前的所有网卡均关闭PXE功能。 • 确保裸金属设备的启动模式为Legacy。
可用	裸金属设备可用于创建裸金属主机，支持自定义安装操作系统
被分配	裸金属设备已用于创建裸金属主机
重启中	裸金属设备处于重启中

启用状态	电源状态
• 启用 • 停用	• 已开机 • 重启中 • 已关机

16.2.4 裸金属主机

裸金属主机：已安装操作系统的裸金属服务器，裸金属设备部署完成后可用于创建裸金属主机。

- 支持自定义安装操作系统，目前支持的操作系统版本包括：RHEL/CentOS系列 6.X和7.X 版本ISO（非LiveCD）；
- 支持扁平网络场景，同一个二层网络上的裸金属主机和云主机之间可互相访问，无需通过网关进行路由。

裸金属主机支持以下操作：

- 创建裸金属主机
- 查看裸金属主机详情
- 启动/停止/重启裸金属主机
- 打开控制台
- 删除裸金属主机
- 恢复/彻底删除裸金属主机

注意事项

- 目前支持RHEL/CentOS系列 6.X和7.X 版本ISO（非LiveCD），安装系统过程需要手动执行
- 镜像服务器仅支持ImageStore类型
- 裸金属主机支持添加扁平网络，添加网络后，可与同二层网络下的裸金属主机或云主机进行通信
- 支持扁平网络场景，同一个二层网络上的裸金属主机和云主机之间可互相访问
- 添加网络配置时所选的网卡和网络必须匹配

16.3 灾备服务

灾备服务以业务为中心，融合定时增量备份等多种灾备技术到ZStack私有云平台中，支持本地灾备、异地灾备、公有云灾备多种灾备方案，用户可根据自身业务特点，灵活选择合适的灾备方式。灾备服务以单独的功能模块形式提供，需提前购买灾备服务模块许可证（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。

典型灾备场景

灾备服务模块提供本地灾备、异地灾备、公有云灾备三种典型灾备场景。

- **本地灾备**：

  支持将本地部署的镜像仓库作为**本地备份服务器**，用于存放本地云主机/云盘/管理节点数据库（以下简称数据库）的定时备份数据。同时本地备份服务器支持主备无缝切换，有效保障业务连续性。

当发生本地数据误删，或本地主存储中数据损坏等情况，可将本地备份服务器中的备份数据还原至本地；当本地数据中心发生灾难时，完全可依赖本地备份服务器重建数据中心并恢复业务。

更多详情可参考本地灾备实践章节。

本地灾备场景如图 *115:* 本地灾备场景*1*和图 *116:* 本地灾备场景*2*所示：

图 115: 本地灾备场景1

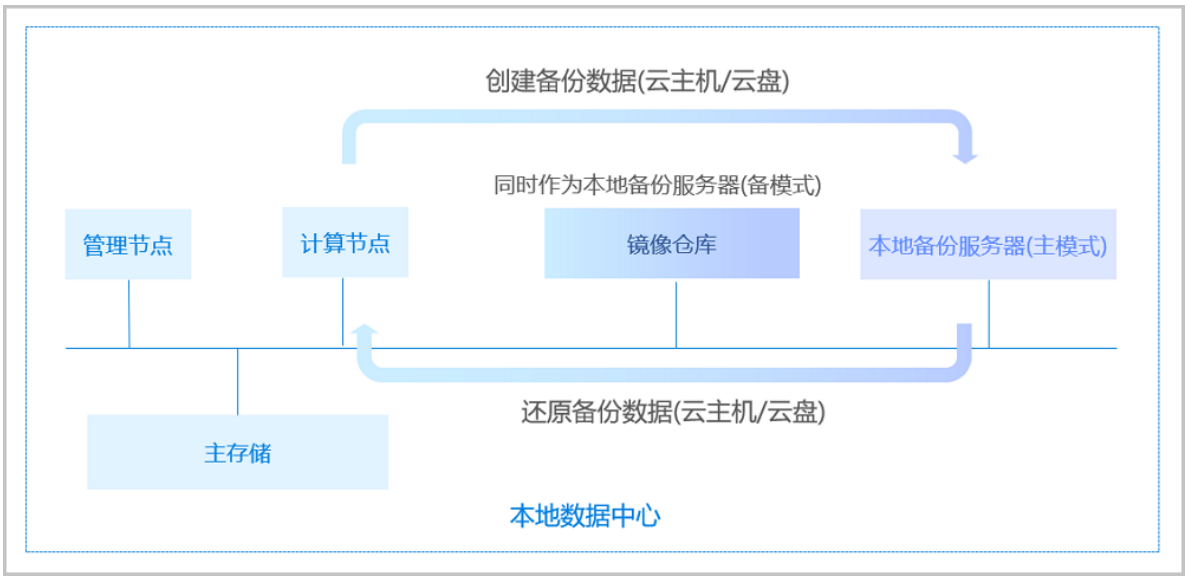
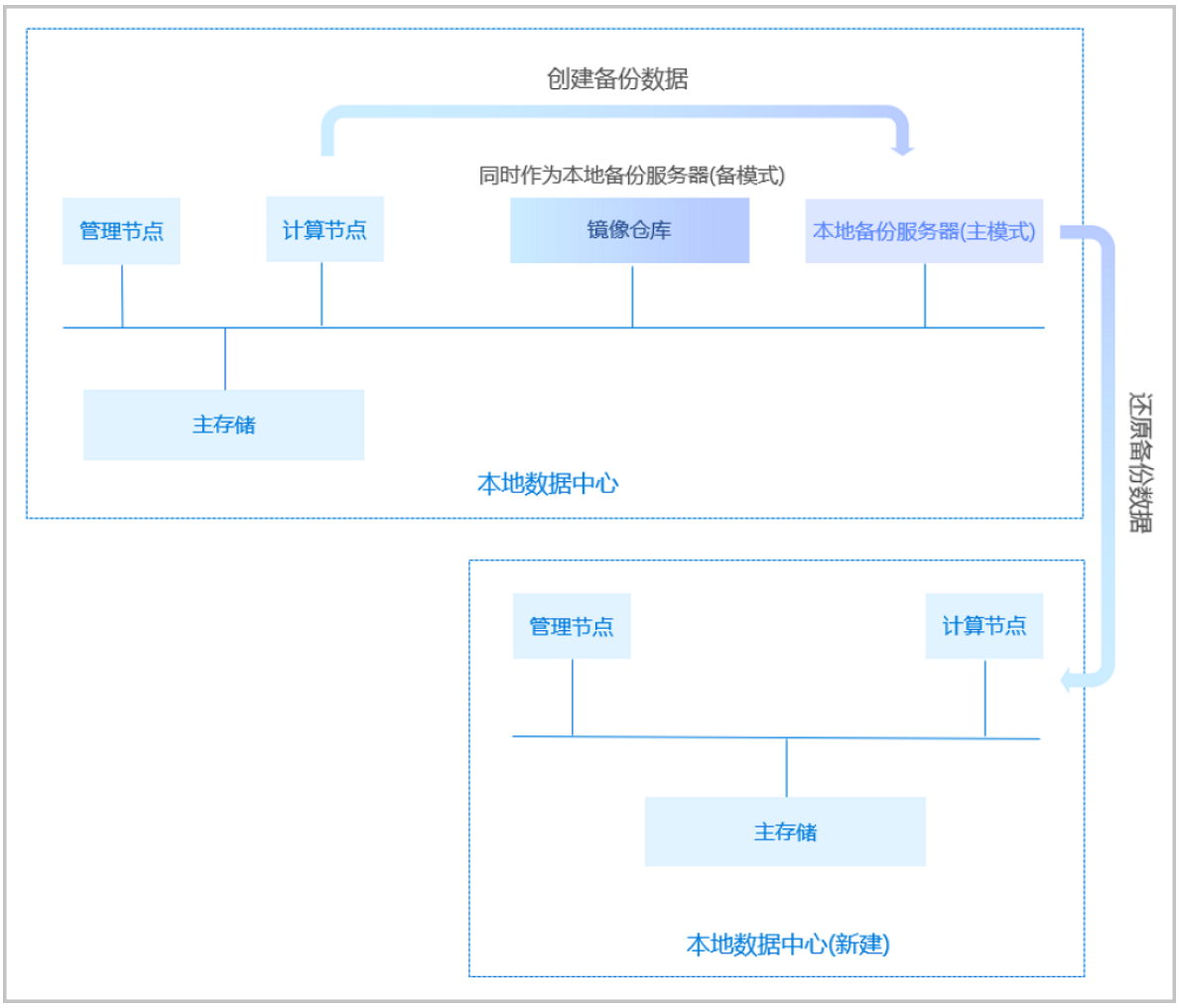


图 116: 本地灾备场景2



- **异地灾备**：

  支持将异地机房的存储服务器作为**异地备份服务器**，用于存放本地云主机/云盘/数据库的定时备份数据。备份数据需通过本地备份服务器同步至异地备份服务器。

  当发生本地数据误删，或本地主存储中数据损坏等情况，可将异地备份服务器中的备份数据还原至本地。当本地数据中心发生灾难时，完全可依赖异地备份服务器重建数据中心并恢复业务。

  更多详情可参考异地灾备实践章节。

  异地灾备场景如*图 117: 异地灾备场景1*和*图 118: 异地灾备场景2*所示：

  图 117: 异地灾备场景1

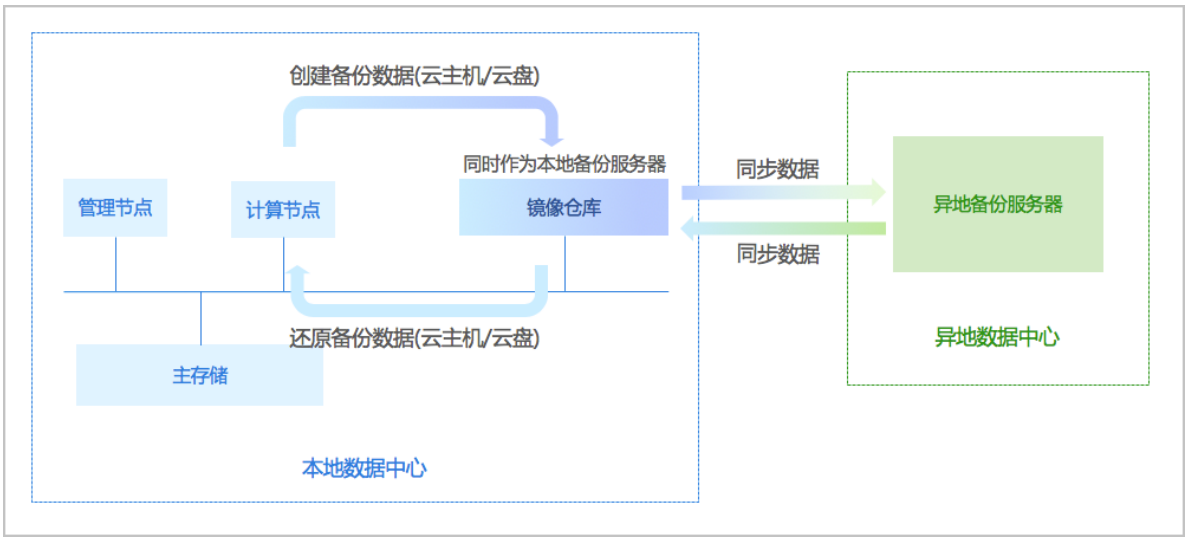
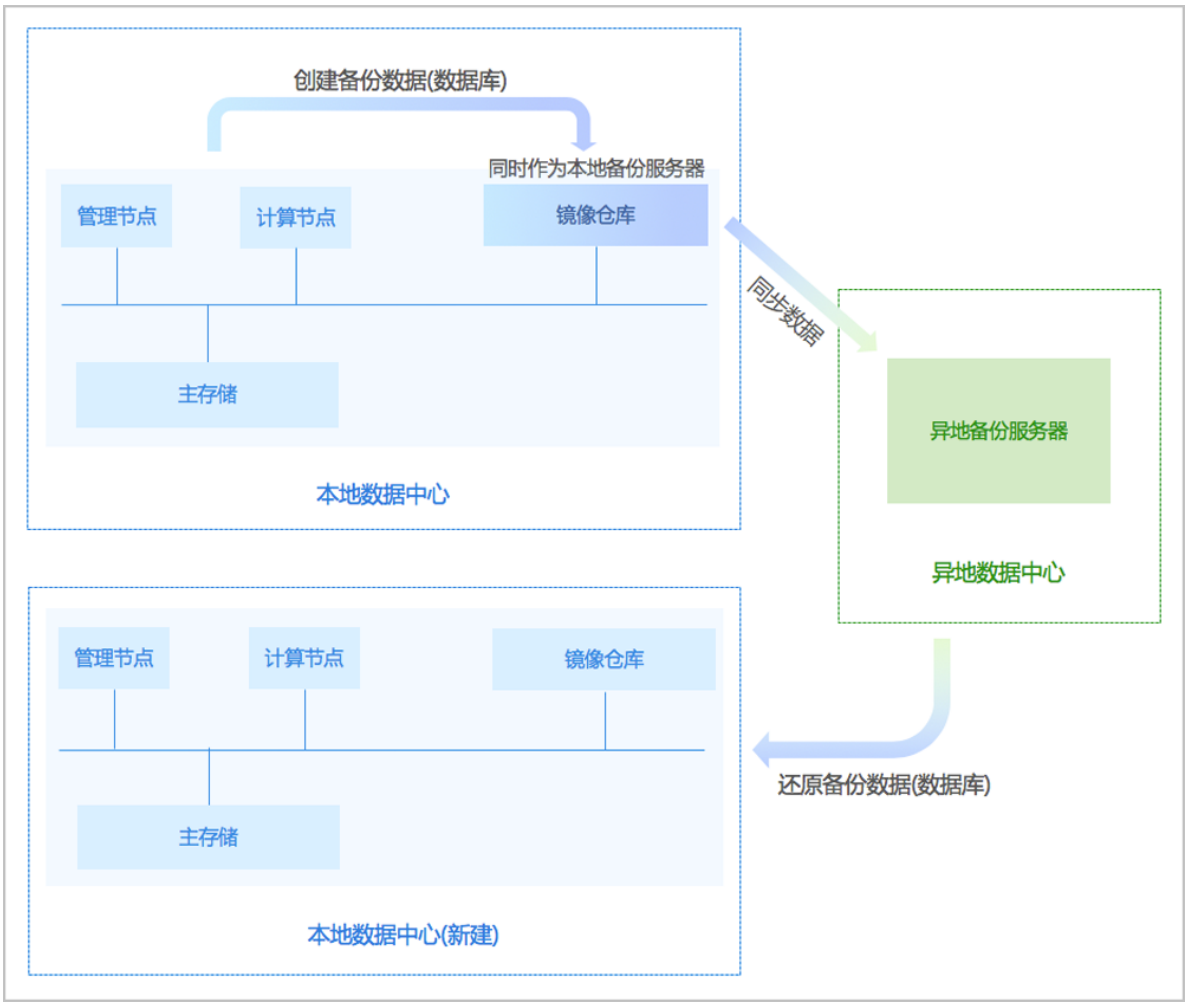


图 118: 异地灾备场景2



- **公有云灾备**：

支持将公有云上的存储服务器作为**公有云备份服务器**，用于存放本地云主机/云盘/数据库的定时备份数据。备份数据需通过本地备份服务器同步至公有云备份服务器。

当发生本地数据误删，或本地主存储中数据损坏等情况，可将公有云备份服务器中的备份数据还原至本地。当本地数据中心发生灾难时，完全可依赖公有云备份服务器重建数据中心并恢复业务。

更多详情可参考公有云灾备实践章节。

公有云灾备场景如图 *119:* 公有云灾备场景*1*和图 *120:* 公有云灾备场景*2*所示：

图 119: 公有云灾备场景1

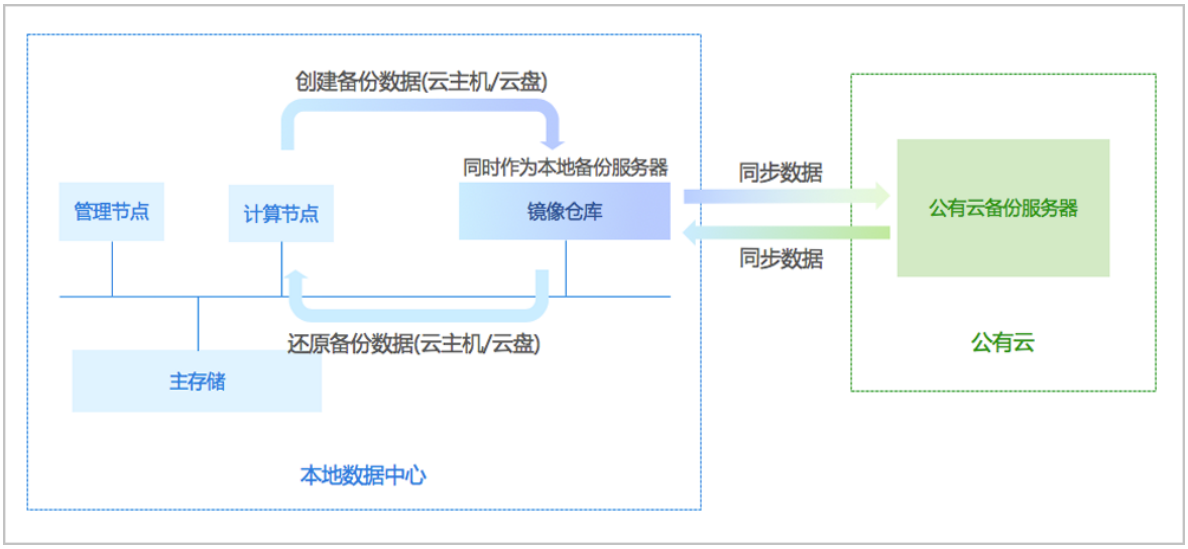
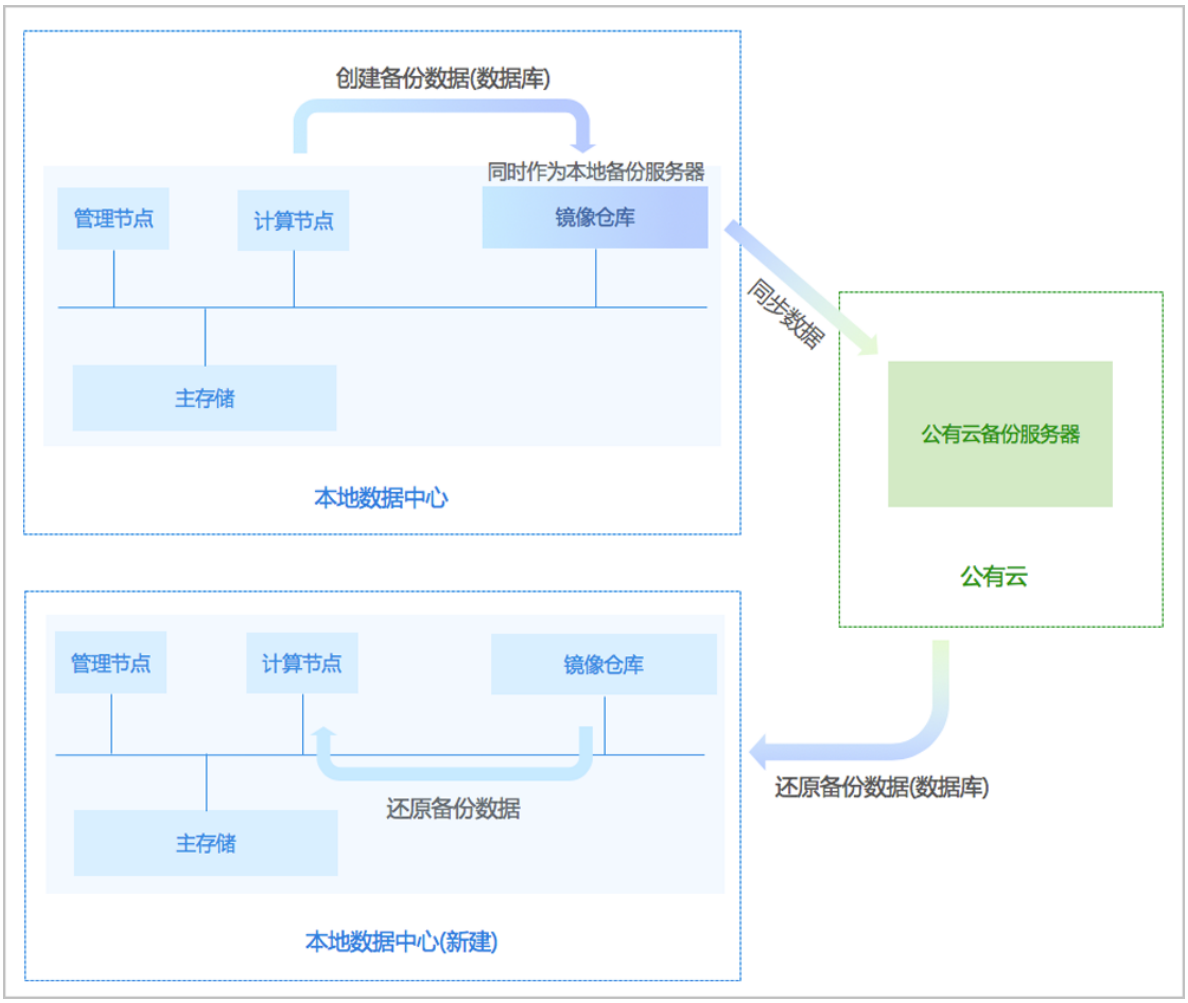


图 120: 公有云灾备场景2



16.3.1 备份任务

注意事项

通过备份任务，本地云主机/云盘/数据库可定时备份到指定的本地存储服务器，同时备份数据可同步到指定的远端备份服务器（异地备份服务器/公有云备份服务器）。

- 当指定多个本地备份服务器时，支持主备无缝切换；
- 支持定时增量备份；
- 支持备份任务设置磁盘/网络QoS；
- 暂不支持共享云盘做定时备份。
- 云主机需处于开机状态，才可对其创建备份任务。
- 云盘需挂载到开机状态的云主机，才可对其创建备份任务。
- 当指定多个本地备份服务器时，主备由添加次序决定，第一个添加的备份服务器系统默认为主，第二个开始均为备。

- 当本地备份服务器（主）发生故障，支持主备无缝切换。
  - 当备份服务器（主）正常工作时，备份任务直接在备份服务器（主）上做备份；
  - 当备份服务器（主）停用/删除/故障失联时，备份任务会自动切换到备份服务器（备）上做备份；
  - 当备份服务器（主）恢复正常时，备份任务会自动切回到备份服务器（主）上做备份。

16.3.2 本地备份数据

本地备份数据是备份在本地备份服务器中的本地云主机/云盘/数据库的备份数据。用户可在**本地备份数据**界面，对本地备份数据进行管理。

本地备份数据支持以下操作：

- 查看本地备份数据
- 还原本地备份数据
- 将本地备份数据同步到远端
- 删除本地备份数据
- 导出本地数据库备份数据

注意事项

- 覆盖原始资源时需提前确保云主机处于关机状态。
- 将本地备份数据同步到远端时需提前添加远端备份服务器到ZStack私有云平台，且只允许添加一个。
- 删除本地备份数据时默认只删除本地备份数据，如需同时删除远端备份服务器中的备份数据，请勾选**同步删除远端备份数据**。
- 若同步删除远端备份数据，将会删除远端备份数据的本地记录，真实数据不受影响。

16.3.3 本地备份服务器

本地备份服务器是位于本地数据中心的存储服务器，用于存放本地云主机/云盘/数据库的备份数据。

- 可直接使用本地数据中心已部署的镜像仓库作为本地备份服务器；
- 也可部署新的本地备份服务器；
- 允许添加多个本地备份服务器；
- 当备份任务指定多个本地备份服务器时，支持主备无缝切换；

- 支持定时增量备份；
- 支持清理已被彻底删除的无效备份数据，释放存储空间；
- 备份到本地备份服务器上的备份数据可在详情页中查看。

本地备份服务器支持以下操作：

- 添加本地备份服务器
- 启用本地备份服务器
- 停用本地备份服务器
- 重连本地备份服务器
- 本地备份服务器数据清理
- 删除本地备份服务器
- 修改本地备份服务器基本属性
- 管理本地备份数据

注意事项

- 添加已有镜像仓库，**名称**选项将自动识别已有镜像仓库名称。也可在添加完成后，进入本地备份服务器详情页修改名称。
- 若备份任务指定一个本地备份服务器，将本地备份服务器停用，备份任务会执行失败。
- 若备份任务指定多个本地备份服务器，将本地备份服务器（主）停用，备份任务会自动切换到本地备份服务器（备）上做备份。
- 若本地备份服务器为已有镜像仓库，删除本地备份服务器，并不会删除服务器上备份数据的本地记录以及真实数据，当重新添加本地备份服务器，备份数据的本地记录实时恢复。
- 若本地备份服务器为新添加的存储服务器，删除本地备份服务器，将会删除服务器上备份数据的本地记录，真实数据不受影响，当重新添加本地备份服务器，备份数据的本地记录无法自行恢复，需谨慎操作！
- 支持数据清理功能，清理本地备份服务器中已被彻底删除的无效备份数据，释放存储空间。

注:

例如，将某个云主机/云盘的本地备份数据彻底删除，并将基于该备份数据还原的云主机/云盘彻底删除，这时执行数据清理操作，就可释放本地备份服务器的存储空间。

16.3.4 远端备份服务器

远端备份服务器是位于异地数据中心/公有云上的存储服务器，用于存放本地云主机/云盘/数据库的备份数据。

- 备份数据仅可从本地备份服务器同步至远端备份服务器；
- 仅允许添加一个远端备份服务器；
- 备份到远端备份服务器上的备份数据可在详情页中查看；
- 本地云主机/云盘的远端备份数据需先同步至本地备份服务器，才可还原至本地；
- 数据库的远端备份数据直接还原至本地。

远端备份服务器支持以下操作：

- 添加远端备份服务器
- 启用远端备份服务器
- 停用远端备份服务器
- 重连远端备份服务器
- 远端备份服务器数据清理
- 删除远端备份服务器
- 修改远端备份服务器基本属性
- 加载/卸载区域
- 管理远端备份数据

注意事项

- 若备份任务指定远端备份服务器，将远端备份服务器停用，备份任务会继续在本地备份服务器做备份，但停止同步至远端备份服务器。
- 删除远端备份服务器，将会删除服务器上备份数据的本地记录，真实数据不受影响，当重新添加远端备份服务器，备份数据的本地记录无法自行恢复，需谨慎操作！
- 远端备份数据需先同步至本地备份服务器，才可还原至本地。
- 支持数据清理功能，清理本地备份服务器中已被彻底删除的无效备份数据，释放存储空间。

注:

例如，将某个云主机/云盘的本地备份数据彻底删除，并将基于该备份数据还原的云主机/云盘彻底删除，这时执行数据清理操作，就可释放本地备份服务器的存储空间。

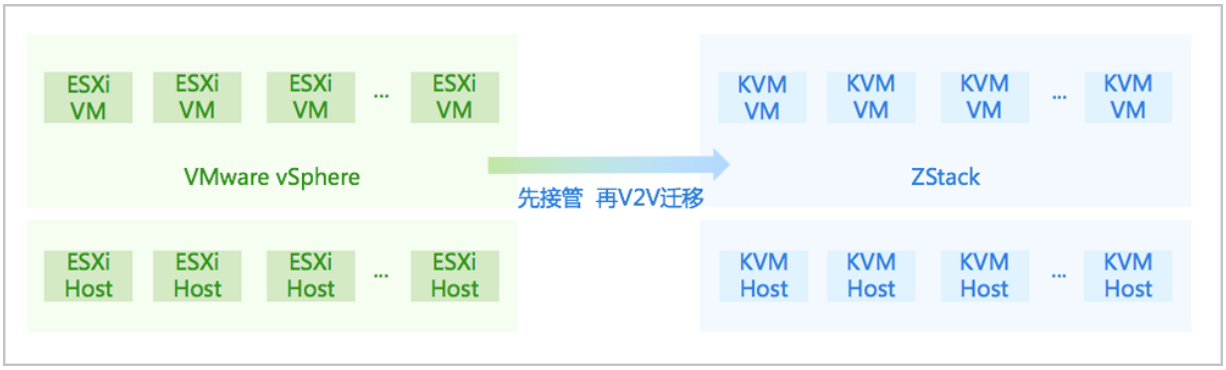
16.4 迁移服务

ZStack提供V2V迁移服务，可将其它虚拟化平台的云主机系统及数据完整迁移至当前云平台。目前支持将已接管的vCenter云主机迁移至当前云平台（支持迁移的源vCenter平台版本包括：5.5、6.0、6.5、6.7）。

V2V迁移服务以单独的功能模块形式提供，需提前购买迁移服务模块许可证（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。

V2V迁移服务如图 *121: V2V迁移*所示：

图 121: V2V迁移



V2V迁移服务具有以下功能优势：

- 支持对云主机进行一键式批量的V2V迁移；
- 用户只需添加迁移服务器并创建迁移任务，其余工作均交由云平台执行；
- 支持对迁移服务器设置网络QoS，控制传输瓶颈，提高迁移效率；
- 创建迁移任务过程中，支持对目标云主机进行自定义配置；
- 支持多种操作系统的云主机进行V2V迁移，包括：RHEL/CentOS 5.x/6.x/7.x、Windows 7/2003/2008/2012/2016；
- 对于Windows云主机，迁移过程中支持自动安装WindowsVirtIO驱动，提高网卡、磁盘工作效率；
- 整个迁移过程可通过直观可视化的UI界面进行监控和管理。

16.4.1 V2V迁移

通过创建迁移任务，可将已接管的vCenter云主机迁移至当前云平台。

- 用户可对云主机进行批量的V2V迁移，并对迁移的目标云主机进行自定义配置；
- 迁移的源vCenter平台版本支持：5.5、6.0、6.5、6.7；

- 迁移的源vCenter云主机系统支持：RHEL/CentOS 5.x/6.x/7.x、Windows 7/2003/2008/2012/2016；
- 云主机在V2V迁移过程中将强制关闭，注意业务影响；
- 迁移的目标主存储支持Shared Block类型以及Ceph类型；
- 从ZStack 3.1.0开始，支持UEFI引导的源云主机进行V2V迁移，迁移后仍使用UEFI引导启动。

注意事项

- V2V迁移过程中，不能将已停止的源vCenter云主机开机，否则会导致迁移任务失败；
- 对于Windows云主机，迁移过程中自动安装WindowsVirtIO驱动，迁移完成后需手动更新网卡驱动（WindowsVirtIO驱动已安装在本地目录，自动搜索更新即可）；
- 若已设置迁移完成后自动开启云主机，迁移后由于集群物理资源不足，目标云主机将启动失败而处于停止状态，此时迁移任务状态显示为成功；
- 对于带云盘的Windows云主机，迁移后云盘为脱机模式，需手动更改为联机模式；
- 对于带云盘的Linux/Windows云主机，迁移后云盘盘符可能会被修改；
- 对于Linux云主机，若迁移前使用图形化方式启动，迁移后第一次启动可能需要更新显示配置；
- 对于UEFI引导的Linux云主机，系统版本为RHEL/CentOS 5.x/6.x/7.x，迁移后需删除启动选项中的**rhgb**参数，才能成功启动；
- 对于UEFI引导的Linux云主机，系统版本为CentOS 7.4及以上，迁移后启动进入UEFI Shell，需执行以下命令，才能成功启动进入操作系统：

```
Shell> fs0:
FS0:\> cd EFI
FS0:\EFI\> cd centos
FS0:\EFI\centos\> shimx64-centos.efi
```

- 用户可自行设置同一时刻最多允许运行的V2V迁移任务。设置方法：

  进入**设置** > **全局设置** > **高级设置**，设置**V2V迁移任务并行度**即可，默认为10。

- 用户可自行设置迁移后的目标云主机选择物理机启动策略。设置方法：

  进入**设置** > **全局设置** > **高级设置**，设置**物理机分配策略**即可，默认选择运行云主机数量最少的物理机启动目标云主机。

- 若迁移数据缓存存在，重新启动迁移任务后，将大幅提高迁移效率。
- 用户可自行设置迁移数据缓存留存时限，设置方法：

  进入**设置** > **全局设置** > **高级设置**，设置**迁移数据缓存留存时限**即可，默认为86400秒（即1天）。

16.4.2 迁移服务器

V2V迁移需要指定目标集群内的物理机作为迁移服务器。

- 迁移服务器必须有足够的硬件资源，包括：网络带宽、磁盘空间等，建议的最低配置如下：

表 6: 迁移服务器最低配置建议

硬件资源	最低配置
CPU	不低于8核心
内存	不低于16GB
网络	至少需配置1块千兆网卡
存储	剩余存储空间不低于50GB **注:** 根据实际迁移云主机数量改变。

- 支持对迁移服务器设置网络QoS，控制传输瓶颈，提高迁移效率。

注意事项

- 需提前添加迁移服务器到云平台；
- 迁移服务器为指定目标集群内的一个物理机，且需有足够的硬件资源用于V2V迁移；
- 若已选择多台源云主机，则相应创建的多个迁移任务均使用这台迁移服务器。

17 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。

17.1 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。

在**全局设置**界面，点击右上角**恢复全局设置**按钮，全局设置将恢复至初始配置（社区版不支持该操作）。

17.1.1 基础设置

目前基础设置支持以下选项， 具体介绍如下：

- **保留容量**：
  - 用于设置镜像服务器在使用是的保留使用容量。默认为：**1G**。
  - 镜像服务器保留容量在 0 到 1T 之间，输入形如 （ 1-1023 ） G/M/K/B g/m/k/b 或（ 0,1 ）T/t 。
- **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！
- **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。

- **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。
- **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。
- **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：none、host-model、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特性将与物理机的CPU特性完全一致，例如都支持扩展页表，大页内存以及虚拟化等。

      注:

      - host-passthrough模式支持云主机的嵌套虚拟化，但该模式可能导致云主机在不同型号CPU的物理机之间迁移失败。
      - 选择host-model模式可能会缺失诸多CPU扩展功能，例如扩展页表，大页内存以及虚拟化等。
- **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。
- **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。

- **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！
- **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！
- **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**。
- **保留容量**：
  - 用于设置主存储的保留容量。默认为：**1G**。

- 主存储保留容量在 0 到 1T 之间，输入形如 (1-1023) G/M/K/B g/m/k/b 或（ 0,1 ）T/t。

- **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。
- **防欺诈**：
  - 防**IP/MAC**伪造和ARP欺骗。
  - 默认为：**false**。
- **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。
- **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。
- **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。

- **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。

17.1.2 高级设置

ZStack支持上百种高级设置，用户可根据自身的需求搜索并且修改对应的设置。

目前高级设置支持以下选项， 具体介绍如下：

- **agent自动启动**：

  默认为false。

  - 默认情况下，云路由器已集成了agent程序，支持开机自动启动，如果设置并部署新的agent，并打算使其生效，此选项需设置为true。
  - 设置为true后，在云路由器在每次创建、启动或重启时，管理节点均会部署新的agent程序。

- **连接超时时间**：

  默认为300，单位为秒，用于设置管理节点与云路由器上运行的agent程序的连接超时上限，如果管理节点在指定时间内没有连接成功agent程序，则云路由器会启动失败并被删除。

- **SSH超时时间**：

  默认为300，单位为秒，用于设置管理节点与云路由器进行SSH连接的超时上限，如果管理节点在指定时间内没有SSH成功云路由器，则云路由器会启动失败并被删除。

- **组内实例数量检查间隔**：

默认为20，单位为秒，用于设置检查弹性伸缩组内实例数量的时间间隔，最小值不能低于10秒，最大值不能高于1000秒。

- **组内不健康实例删除间隔**：

  默认为30，单位为秒，用于设置删除弹性伸缩组内不健康实例的时间间隔，最小值不能低于10秒，最大值不能高于1000秒。

- **组内不健康实例删除线程数**：

  默认为10，用于设置删除弹性伸缩组内不健康实例的线程数，最小值不能低于10线程，最大值不能高于1000线程。

- **负载均衡云主机健康检查间隔**：

  默认为10，单位为秒，用于设置云主机在负载均衡中健康状态检查的时间间隔，最小值不能低于10秒，最大值不能高于1000秒。

- **负载均衡云主机健康检查线程数**：

  默认为10，用于设置云主机在负载均衡中健康状态检查的线程数，最小值不能低于10线程，最大值不能高于1000线程。

- **Ping间隔**：

  默认为60，单位为秒，用于设置管理节点在指定的时间间隔去检查镜像服务器，如果检查成功，表示镜像服务器是连接状态。

- **Ping最大并发度**：

  默认为50，用于设置管理节点同时检查多个镜像服务器时，最大的并发度。

- **保留容量**：

  默认为1G，用于设置镜像服务器在使用时保留使用的容量。

- **删除策略**：

  删除裸金属主机的策略，默认为“延时删除”。可选策略为：立刻删除，延时删除，永不删除。

  - 立刻删除（Direct）：当设置为立刻删除时，如果用户删除裸金属主机，这些裸金属主机会被立刻删除。
  - 延时删除（Delay）：当设置为延时删除（默认）时，如果用户删除裸金属主机，这些裸金属主机会被标记为已删除，显示在对应裸金属主机的已删除栏，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，才会彻底删除裸金属主机。

  - 永不删除（Never）：当设置为永不删除时，当用户删除裸金属主机时，这些裸金属主机永远不会被系统自动删除。
- **镜像下载超时时间**：

  默认为3600，单位为秒，用于设置Ceph镜像服务器下载镜像时的超时时间，如果超过此时间，镜像还未下载完成，此镜像会添加失败。
- **镜像服务器Mon自动重连**：

  默认为true，用于设置Ceph镜像服务器的Mon IP在检查失败时，是否开启自动重连。
- **镜像服务器Mon重连延迟**：

  默认为30，单位为秒，用于设置Ceph镜像服务器的Mon IP在一次检查失败后，再次重连的延迟间隔。
- **GC清理时间间隔**：

  默认为3600，单位为秒，用于设置Ceph主存储回收清理云盘垃圾数据的时间间隔。
- **镜像缓存清理间隔**：

  默认为43200，单位为秒，用于设置Ceph镜像已删除后，也无云主机使用的前提下，Ceph主存储里面不再使用的镜像缓存被执行清理的时间间隔。
- **主存储删除Pool选项**：

  默认为false，在删除Ceph主存储时，是否删除所有的ceph存储池，默认关闭，打开此选项，非常危险，可能导致数据丢失，需谨慎操作。
- **主存储Mon自动重连**：

  默认为true，用于设置Ceph主存储的Mon IP在检查失败时，是否开启自动重连。
- **主存储Mon重连延迟**：

  默认为30，单位为秒，用于设置Ceph主存储的Mon IP在一次检查失败后，再次重连的延迟间隔。
- **集群升级并行度**：

  默认为2，用于设置同一时刻最多可执行并行系统升级的集群个数。
- **AgentPing间隔**：

  默认为60，单位为秒，用于设置检查控制台agent程序的时间间隔。
- **Agent空闲超时**：

默认为60，单位为秒，用于设置空闲的控制台agent等待的最大时间 。

- **vnc会话超时**：

  默认为1800，单位为秒，用于设置VNC会话的超时时间。

- **从备份数据恢复数据库**：

  默认为true，是否允许在有数据的情况下从备份数据中恢复数据库。

- **物理机密码加密存储开关**：

  默认为false，用于设置物理机密码在数据库中是否启用加密存储。若为true，物理机密码将在数据库中加密存储。

- **向云主机注入DNS**：

  默认为false，向云主机注入DNS服务器地址，如果设置为True，云主机间可通过HostNmae互相访问。

- **孤儿GC清理间隔**：

  默认为60，单位为秒，在管理节点以指定时间间隔扫描孤儿GC，若有则进行接管。

- **异常物理机检查间隔**：

  默认为5，单位为秒，用于设置在指定的时间间隔去检查一个异常的物理机。

- **判定物理机失联尝试次数**：

  默认为12，用于设置在指定的最大次数去重连物理机，如果在指定最大次数内连接此物理机均失败，则判定物理机失联。

- **判定物理机成功间隔**：

  默认为5，用于判定物理机成功连接的时间间隔，如果物理机在此间隔内成功返回，则表示连接成功。

- **判定物理机成功尝试几率**：

  小数，默认为0.5，用于设置在指定连接次数的既有成功又有失败的情况下，以多大几率来判定物理机连接成功。

- **物理机成功次数**：

  默认为5，用于设置在物理机连接成功的判定时，需要至少建立几次成功的连接。

- **物理机自检间隔**：

  默认为5，设置物理机状态自检的间隔。

- **物理机自检最大尝试次数**：

  默认为6，用于设置在指定的最大次数去自检物理机，在最大的尝试测试次数均失败时，会判定物理机网络异常。

- **物理机自检主存储检查超时时间**：

  默认为15，单位为秒，用于设置在物理机自检连接主存储的超时时间。

- **永不停止云主机GC最大重试间隔时间**：

  默认为300，单位为秒，针对永不停止的云主机，如果异常停止，用于执行GC任务尝试重试启动的最大时间间隔。

- **永不停止云主机尝试的延迟时间**：

  默认为60，单位为秒，针对永不停止的云主机 ，如果上一次尝试启动失败，到下一次尝试时中间的延迟时间。

- **永不停止云主机扫描间隔**：

  默认为60，单位为秒，针对永不停止的云主机 ，如果启动失败，下次扫描的时间间隔。

- **物理机分配器并发度**：

  默认为2，用于设置分配物理机时的分配器并发度。

- **Ping不通时自动重连**：

  默认为true，管理节点连不通物理机时，会自动重连。

- **自动重连**：

  默认为true，管理节点在启动服务过程中，是否全部重连物理机。

- **重连并发度**：

  默认为100，管理节点在重连物理机过程中，全部重连物理机时的最大并发度。

- **维护模式忽略错误**：

  默认为false，物理机维护模式，忽略相关错误，会返回成功。

- **Ping间隔**：

  默认为60，单位为秒，管理节点在指定间隔对物理机进行检查，来物理机是否连接。

- **检查计算节点失败阈值**：

  默认为3，单位为次，管理节点在检查计算节点时，尝试检查时允许的最大失败次数。

- **Ping并发度**：

默认为100，管理节点在检查物理机是否连接时，支持的最大并发度。

- **物理机自动重连**：

  默认为true，管理节点在启动服务过程中，是否全部重连物理机。

- **物理机升级并行度**：

  默认为2，用于设置一个集群内同一时刻最多可执行并行系统升级的物理机个数。

- **彻底删除间隔**：

  默认为3600，单位为秒，执行彻底删除项目任务运行的时间间隔。

- **彻底删除时延**：

  默认为86400，单位为秒，项目删除策略为延迟删除时，针对已删除的项目，选择延时多久彻底删除项目。

- **清理间隔**：

  默认为3600，用于设置在指定的时间间隔清理哪些已经超时的会话。

- **最大会话数**：

  默认为500，用于设置管理节点可接受的最大会话数量，超过此数值，将不能建立新的会话。

- **删除策略**：

  可选类型为直接删除、延迟删除、永不删除，用于在删除镜像时，管理节点设置的删除策略：

  1. 直接删除：直接从数据库删除和文件级别删除镜像；
  2. 延迟删除：将此镜像的状态变为已删除，在镜像彻底删除到期后，会从数据库删除和文件级别删除镜像；
  3. 永不删除：从数据库删除镜像，但是永不删除其文件。

- **启用重置密码**：

  默认为true，用于设置镜像是否启用重置密码。

- **彻底删除间隔**：

  默认为3600，单位为秒，用于设置执行彻底删除镜像任务的时间间隔。

  彻底删除周期：

  默认为86400，单位为秒，用于设置将一个已删除的镜像从数据库移除，并从镜像服务器移除的执行周期。

- **物理机CPU型号检测**：

默认为false，用于迁移和添加物理机时是否检测物理机CPU型号的一致性。

- **云主机云盘的最大数量**：

  默认为24，用于设置一个云主机可支持的最大数据盘数量。

- **物理机并发级别**：

  默认为10，用于设置在物理机执行命令的并发数量，如果设置的并发数量过大，可能导致物理机负载过高。

- **ignore_msrs参数开关**：

  默认关闭，控制物理机的KVM内核模块是否打开ignore_msrs参数。

- **auto-converge功能开关**：

  默认为false，用于设置auto-converge功能是否启用。若为true，KVM云主机热迁移时将启用auto-converge功能。启用auto-converge前，请确保应用能够容忍系统变慢，注意auto-converge不能确保热迁移一定成功。

- **云主机并发迁移数量**：

  默认为2，用于设置物理机维护模式时，同时迁移云主机的数量。

- **物理机Ping时云主机状态同步**：

  默认为true，用于设置物理机在连接时，是否同步云主机的状态。

- **返回结果**：

  默认为**member,uniqueMember,memberOf**，默认返回结果分隔符应为**","**。配置AD/LDAP返回结果，可以是多条，用AD/LDAP返回结果分隔符分割开。

- **默认算法**：

  默认为roundrobin，即：轮询法，可选方法包括轮询法（roundrobin）、最少连接法（leastconn）和源地址法（source），用于设置负载均衡时，采用哪种算法。

- **空闲连接超时时间**：

  默认为60，单位为秒，在没有数据传输时，设置触发负载均衡器终止服务器和客户端连接的超时时间。

- **健康检查间隔**：

  默认为5，单位为秒，用于设置对负载均衡器内的云主机进行健康检查的时间间隔。

- **健康检查超时时间**：

默认为2，单位为秒，用于设置在指定时间内如果负载均衡检查没有相应则判定检查失败。

- **健康阈值**：

  默认为2，在执行多少次成功检查后，将云主机移至健康状态。

- **最大连接**：

  默认为5000，用于设置负载均衡器同时建立的最大连接数。

- **不健康阈值**：

  默认为2，在执行多少次失败检查后，将云主机移至不健康状态。

- **语言**：

  默认为zh_CN，设置记录相关日志的地域，此设置影响相关的日志记录的地域时间。

- **登录失败最大次数**：

  默认为6，用于设置连续登录失败的次数上限。

- **登录验证码开关**：

  默认为false，是否启用登录控制中的验证码功能。开启后连续登录失败次数超过上限将触发验证码保护机制，要求输入正确的账户名、密码以及验证码才能成功登录云平台。

- **心跳检测间隔**：

  默认为5，单位为秒，用于设置管理节点将心跳写入数据库的时间间隔。

- **支持内核aio**：

  默认为false，在QEMU存储驱动中使用内核异步IO。

- **分发镜像**：

  默认为true，在添加镜像后，设置是否分发镜像到本地存储。

- **分发镜像并发度**：

  默认为2，在添加镜像后，同时分发镜像到本地存储的并发度。

- **触发器恢复检查间隔**：

  默认为10，单位为秒，设置时间间隔周期性的检查触发器是否已恢复。

- **虚拟网络DHCP**：

  默认为1500，用于设置虚拟网络的默认最大传输单元的字节数。

- **NoVlan网络DHCP**：

  默认为1500，用于设置L2NoVlan网络的最大传输单元的字节数。

- **Vlan网络DHCP**：

  默认为1500，用于设置L2Vlan网络的最大传输单元的字节数。

- **VXLAN网络DHCP**：

  默认为1450，用于设置VXLAN网络的最大传输单元的字节数。

- **GC清理时间间隔**：

  默认为3600，单位为秒，用于设置NFS主存储GC清理云盘和快照的时间间隔。

- **PCI设备IOMMU开关**：

  默认为false，控制连接物理机时，用于设置是否开启IOMMU。

- **物理机CPU使用率最低采集间隔**：

  默认为600，单位为秒，用于设置物理机CPU使用率的采集时间间隔，挑选出CPU使用率最低的物理机来创建云主机。

- **物理机内存使用率最低采集间隔**：

  默认为600，单位为秒，用于设置物理机内存使用率的采集时间间隔，挑选出内存使用率最低的物理机来创建云主机。

- **镜像缓存的GC时间间隔**：

  默认为86400，单位为秒，用于设置主存储定期扫描那些孤儿的需要被清理的镜像缓存的时间间隔。

- **Ping间隔**：

  默认为60，单位为秒，管理节点在指定间隔对主存储进行检查是否连接。

- **Ping并发度**：

  默认为50，管理节点在检查多个主存储时，支持的最大并发度。

- **主存储开启垃圾回收**：

  默认为true，创建云主机/云盘失败后，用于设置是否开启清理主存储上垃圾数据的功能。

- **主存储垃圾回收的时间间隔**：

  默认为600，单位为秒，用于设置主存储上垃圾回收的时间间隔。

- **主存储垃圾回收的重复次数**：

  默认为50， 用于设置主存储上垃圾回收重复执行的次数。

- **保留容量**：

默认为1G，用于设置主存储的保留容量。

- **清理线程间隔**：

  默认为300，单位为秒，用于设置清理过期的进度条记录的时间间隔。

- **开启**：

  默认true，用于设置是否开启进度条功能。

- **记录保存时间**：

  默认为86400，单位为秒，用于设置进度条数据在数据库中进保留的最长时间。

- **监控数据保留周期**：

  默认为6，单位为月，监控数据在本地保留的周期，可设置1到12之间的整数。

- **亲和组数量配额**：

  默认为20，设置账户的亲和组数量默认配额。

- **弹性IP数量配额**：

  默认为20，设置账户的弹性IP数量默认配额。

- **镜像数量配额**：

  默认为20，设置账户的镜像IP数量默认配额。

- **镜像容量配额**：

  默认为10T，设置账户的镜像容量默认配额。

- **三层网络数量配额**：

  默认为20，设置账户的三层网络数量默认配额。

- **负载均衡器数量配额**：

  默认为20，设置账户的负载均衡器配额。

- **端口转发数量配额**：

  默认为20，设置账户的端口转发数量默认配额。

- **定时任务数量配额**：

  默认为80，设置账户的定时任务数量默认配额。

- **定时器数量配额**：

  默认为80，设置账户的定时器数量默认配额。

- **安全组数量配额**：

  默认为20，设置账户的安全组数量默认配额。

- **云盘快照数量配额**：

  默认为200，设置账户的云盘快照配额。

- **虚拟IP数量配额**：

  默认为20，设置账户的虚拟IP数量默认配额。

- **CPU数量配额**：

  默认为60，设置账户的CPU数量默认配额。

- **内存大小配额**：

  默认为80G，设置账户的内存大小默认配额。

- **运行中的云主机数量配额**：

  默认为20，设置账户的运行中的云主机数量默认配额。

- **云主机数量配额**：

  默认为20，设置账户的云主机数量默认配额。

- **可用存储容量配额**：

  默认为10T，设置账户的可用存储容量默认配额。

- **数据云盘数量配额**：

  默认为40，设置账户的数据云盘数量默认配额。

- **VXLAN网络数量配额**：

  默认为8，设置账户的VXLAN网络数量默认配额。

- **出口策略**：

  默认为允许（accept），没有安全组规则时，默认的出口规则是允许（accept）。

  - 设置为accept：
    - 没有安全组规则时，只有一个accept规则，即允许所有流量；
    - 有安全组规则时，则最后的默认规则为accept。
  - 设置为deny：
    - 没有安全组规则时，只有一个deny规则，即拒绝所有流量；
    - 有安全组规则时，则最后的默认规则为deny。

- **进入策略**：

  默认为丢包（drop），没有安全组规则时，默认的进入规则是丢包（drop）。

  - 设置为drop：
    - 没有安全组规则时，只有一个drop规则，即丢掉所有流量；
    - 有安全组规则时，则最后的默认规则为drop。
  - 设置为accept：
    - 没有安全组规则时，只有一个accept规则，即允许所有流量；
    - 有安全组规则时，则最后的默认规则为drop。
  - 设置为deny：
    - 没有安全组规则时，只有一个deny规则，即拒绝所有流量；
    - 有安全组规则时，则最后的默认规则为deny。
- **失效云盘清理间隔**：

  默认为3600，单位为秒，用于设置共享块存储GC清理云盘和快照的时间间隔。
- **关闭多路径queue_if_no_path设置**：

  默认为true，当Shared Block主存储所使用的多路径设备全部路径失效时，返回IO失败；若修改为false，可能导致ZStack心跳探测与故障恢复无法正常运行，请谨慎修改。
- **云盘预分配策略**：

  默认为full，配置共享块存储下QCOW2文件的预分配策略，可选none, metadata, falloc, full。
- **QCOW2 Cluster大小**：

  配置共享块存储下QCOW2文件的cluster大小，可填值为2的次方，介于512K到2M之间，单位为字节。
- **精简置备磁盘初始磁盘大小**：

  默认为5G，单位为字节，用于设置精简置备磁盘的初始磁盘大小，最小值不能低于1073741824字节。
- **精简置备磁盘最小剩余空间**：

  默认为2G，单位为字节，用于设置精简置备磁盘的最小剩余空间，当精简置备磁盘实际大小减去实际写入所剩余的空间小于最小剩余空间时，磁盘将基于预设大小自动扩容一次。
- **精简置备磁盘自动扩容大小**：

默认为2G，单位为字节，用于设置精简置备磁盘的自动扩容大小，当精简置备磁盘触发自动扩容时，将自动扩容该值大小的空间。

- **精简置备磁盘最大磁盘使用率**：

  默认为85，单位为百分比，用于设置精简置备磁盘的最大磁盘使用率，当磁盘实际写入占磁盘实际大小的百分比大于最大磁盘使用率时，磁盘将基于预设大小自动扩容一次。

- **双因子认证开关**：

  默认为false，登录云平台时，是否开启双因子认证。

- **迁移数据缓存留存时限**：

  默认为86400，单位为秒，用于设置V2V迁移任务失败后，迁移数据缓存允许留存的最大时限。

- **物理机分配策略**：

  云主机从VMware平台迁移到KVM平台，基于物理机分配策略选择物理机启动，默认选择运行云主机数量最少的物理机启动云主机。

- **V2V迁移任务并行度**：

  默认为10，用于设置同一时刻最多可运行的V2V迁移任务数量。

- **命令并发度**：

  默认为100，用于设置云路由可以执行命令的最大并发度。

- **重启DNSMASQ边界**：

  默认为500，在发送多少次SIGUSER1后重启DNSMASQ，因为如果有非常多的SIGUSER1的话DNSMASQ会在重新加载配置文件的时候卡住。

- **Ping间隔**：

  默认为60，单位为秒，用于设置管理节点在指定的时间间隔去检查云路由器，如果检查成功，表示云路由器是连接状态。

- **Ping最大并发度**：

  默认为500，单位为个，用于设置管理节点在同时去检查多个云路由器时，最大的并发度。

- **SSH密码登录路由器开关**：

  默认为false，用于设置路由器登录时是否启用SSH密码登录。若为true，允许通过SSH密码登录路由器，SSH KEY存放路径：$ZSTACK_HOME/WEB-INF/classes/ansible/rsaKeys/id_rsa。

- **SSH端口**：

默认为22，云路由的SSH登录端口。

- **用户名**：

  默认为vyos，登录云路由器的用户名。

- **路由器启动超时时间**：

  默认为60，单位为秒，云路由配置agent程序的echo超时上限。如果云路由在指定时间内没有配置成功agent程序，则云路由器会启动失败并被删除。

- **云主机引导菜单**：

  默认为true，用于设置云主机启动时是否启用引导菜单，少数不支持虚拟机引导菜单的服务器可以设置为false。

- **云主机Hyper-V开关**：

  默认为false，云主机Hyper-V模拟的开启或关闭。

- **云主机彻底删除间隔**：

  默认为3600，单位为秒，执行彻底删除云主机任务运行的时间间隔。

- **计算规格删除后设置为空**：

  默认为true，用于设置在删除计算规格时，是否更新云主机的计算规格列表为NULL。

- **隐藏KVM虚拟化标记**：

  默认为false，如果设置为true，则会在新启动虚拟机定义XML中对<kvm>插入<hidden state='on'>，如果为false则不会。

- **VDI Spice Streaming**：

  默认为off。

  1. all：表示对传输的所有视频帧做编码压缩并传输。带宽要求会降低，流畅度会提高，瘦客户端CPU压力会增大。
  2. filter：表示对增量视频帧做编码压缩并传输。带宽要求会更低，流畅度更高，瘦客户端CPU压力较低，但瘦客户端的chrome播放flash会有拖影问题。
  3. off：表示视频帧不做编码压缩，清晰度最高，带宽要求最高，瘦客户端CPU压力最小。

- **禁用vmwareIO端口模拟**：

  默认为false，用于设置是否关闭vmwareIO端口模拟。

- **快照增量的最大数目**：

默认为128，一个云盘快照链的最大长度。当一个云盘的快照链的长度达到这个数字时，下一个云盘快照会是一个完整的快照。

- **删除策略**：

  删除数据云盘有三种策略：立刻删除，延时删除，永不删除。

  1. 立刻删除：被删除的云盘会从数据库和主存储中删除；
  2. 延时删除：被删除的云盘会在数据库中被标记为已删除，等彻底延时删除时延超时后，才会彻底从数据库与主存储中删除云盘；
  3. 永不删除：当设置为永不删除时，当用户删除云盘时，这些资源永远不会被系统自动删除。

- **云盘规格删除时设置为空**：

  默认为true，删除磁盘规格时，是否更新磁盘的磁盘规格列表为NULL。

- **云盘彻底删除间隔**：

  默认为3600，单位为秒，执行彻底删除云盘的任务运行的时间间隔。

- **云盘彻底删除时延**：

  默认为864000，单位为秒，云盘删除策略为延迟删除时，针对已删除的云盘，选择延时多久彻底删除云盘。

- **云盘容量刷新间隔**：

  默认为3600，单位为秒，当创建云盘容量报警器后，用于设置云盘容量刷新的时间间隔，最小间隔不能低于600秒。

- **zsnp协议的老化时间**：

  默认为 960，单位为秒，越小表示zsnp老化时间越短，刷新越快。

- **三层网络安全默认规则**：

  内部用户通过虚拟IP访问负载均衡。默认为reject，表示不允许。accept表示允许，可能会影响其他安全规则。修改后重连云路由器生效。

- **报警器不重复报警时间间隔**：

  默认为1800，单位为秒，用于设置报警器不重复报警时间间隔。

- **报警器报警检测周期**：

  默认为10，单位为秒，用于设置报警器报警检测周期，最小值为10秒。

- **报警检测线程数**：

默认为5，用于设置报警检测线程数。

- **系统报警器检测的管理节点目录**：

  默认为*/var/lib/zstack/,/usr/local/zstack/*，用户也可自行设置系统报警器检测的管理节点目录。

- **监控数据采样时间间隔**：

  默认为10，单位为秒。用于监控数据采样时间间隔，最小间隔不能低于10秒。

18 管理节点高可用

18.1 管理节点云主机高可用

管理节点云主机高可用方案采用共享存储，使用云主机作为管理节点来管理云平台。

分为两种类型：

- 超融合基础架构：基于Ceph分布式块存储，存储与计算融合部署，管理节点以云主机方式运行，管理融合节点的计算、存储、网络资源。
- 共享文件系统高可用：基于NFS或Shared Mount Point共享文件系统存储，独立共享存储，管理节点以云主机方式运行，管理计算节点的计算、存储、网络资源。

管理节点云主机高可用方案支持以下三个层级的高可用：

1. 管理节点的高可用：由zsha和consul守护进程来提供管理节点高可用，保证管理节点云主机的高可用运行状态。
2. 业务云主机的高可用：通过对云主机所在的物理网络或节点进行检测，在失效时，会自动切换云主机到其他健康节点，以提供业务的可用性。
3. 存储的高可用：分布式块存储的提供的多副本机制和故障域隔离机制；共享文件系统存储由底层存储提供的高可用保障机制，例如，Raid、主备等机制。

存储可支持Ceph分布式块存储，也支持NFS存储、Shared Mount Point存储、以及使用NAS转化为Shared Mount Point存储。

管理节点云主机高可用方案在部署时，需提前规划网络，支持管理网络和存储网络合并，也支持管理网络和存储网络分离，使用独立的存储网络，ZStack使用存储网络作为基准来判定管理节点云主机状态。

18.2 多管理节点物理机高可用

概述

ZStack以单独的高可用套件形式，提供多管理节点物理机高可用功能。当其中任何一个管理节点失联，秒级触发高可用切换，从而保障管理节点持续提供服务。

高可用原理：每个管理节点均运行**zsha2**高可用进程，负责实时监控管理节点上的关键服务（包括：管理节点服务、UI服务、数据库服务），当任何一个关键服务出现宕机，立即通过Keep Alived触发VIP（Virtual IP）迁移，然后尝试恢复宕机服务。

本章节以部署双管理节点物理机高可用为例进行介绍。

安装部署

- 已有单管理节点环境，部署为双管理节点物理机高可用环境

  1. 下载官方发布的最新版ZStack定制版ISO、bin包和多管理节点高可用套件。
  2. 将已有管理节点升级到最新版ZStack。
  3. 对新增管理节点安装最新版ZStack。
  4. 对新增管理节点安装许可证，要求两个管理节点安装的许可证类型要求完全一致。
  5. 将高可用套件导入老管理节点，并解压安装。

- 新装双管理节点环境，部署为双管理节点物理机高可用环境

  1. 下载官方发布的最新版ZStack定制版ISO、bin包和多管理节点高可用套件。
  2. 对两个新管理节点安装最新版ZStack。
  3. 对两个新管理节点安装许可证，要求两个管理节点安装的许可证类型要求完全一致。
  4. 将高可用套件导入其中一个管理节点，并解压安装。

升级

- 高可用套件升级：管理员获得新版高可用套件后，可用于升级当前的*zsha2*服务。

  当主备管理节点的数据库完成自动同步后，请将新版高可用套件导入主管理节点并解压，在主管理节点中安装新版高可用套件。

- 管理节点升级

  管理员只需在一个管理节点中执行*upgrade-mn*命令，就可对两个管理节点进行升级。

注意事项

- 管理节点物理机配置需在8CPU+12G内存及以上。
- 管理网络建议采用万兆以上带宽，若独立部署，允许千兆带宽。
- 推荐使用*zs-network-setting*创建静态网桥。
- 多管理节点高可用套件需依赖ZStack 2.6.0及以上版本。且两者必须配套使用，即：2.6.0版高可用套件必须与2.6.0版ZStack配套使用。
- 两个管理节点安装的ZStack版本必须一致，且两个管理节点安装的许可证类型必须一致。
- 安装高可用套件，需将**zsha2**和**zstack-hamon**放在一个目录，安装过程中，**zsha2**会自动部署**zstack-hamon**以及相关配置文件。
- 安装过程中，备管理节点的数据库会被主管理节点的数据库覆盖，请谨慎配置。

- 为确保双管理节点间的监控数据实时同步，建议在两个管理节点之间做SSH免密登录。
- 用于访问管理节点的Chrom浏览器要求在49版本以上。

19 基本运维

本章主要针对ZStack基本操作异常给出处理办法。

19.1 安装部署

安装部署以及升级ZStack失败需检查的因素：

1. 假定安装操作系统时选择了管理节点模式，但是安装系统后，没有安装ZStack。

   原因：

   安装操作系统时，没有设置合适的IP地址，ZStack管理节点必须要求有可用IP。

   解决方案：

   - 此时需执行`bash /opt/zstack*installer.bin -E` 安装ZStack企业版；
   - 或执行`bash /opt/zstack*installer.bin` 安装ZStack社区版。

2. 安装ZStack时出现如下错误信息。

   现象：

   ```
   Fail Reason: /usr/local/zstack is existing. Please delete it manually before installing a new ZStack
   ```

   原因：

   此时系统已经存在ZStack，不允许再次安装。

   解决方案：

   - 如果打算升级 直接使用**-u**参数升级即可。
   - 如果打算重新安装，则需执行`rm -rf /usr/local/zstack; bash zstack-installer.bin -D`进行重新安装。

3. 安装部署失败，失败信息会打印到屏幕上。

   解决方案：

   可查看*/tmp/zstack_installation.log*，根据错误提示，尝试解决安装部署问题。

4. 升级时遇到ZStack ISO版本不匹配，会提示类似以下错误信息。

   现象：

   ```
   Reason: The current local repo is not suitable for ZStack installation.
   ```

```
Please download ZStack-x86-64-DVD-2.0.1.iso from http://www.zstack.io/product_downlo
ads/ and run
```

解决方案：

此时需执行以下步骤：

1. 在管理节点下载最新的ISO，例如在管理节点执行下载ISO：

```
wget http://cdn.zstack.io/product_downloads/iso/ZStack-x86_64-DVD-3.1.1-c74.iso
```

2. 执行以下命令进行升级，升级ISO里面的yum repo同步到本地，并且直接升级管理节点。

```
zstack-upgrade ZStack-x86_64-DVD-3.1.1-c74.iso
```

5. 升级ZStack过程中，因为二次开发或者调整过数据库而导致升级失败，希望恢复原本的ZStack。

前提：

ZStack在进行升级时，默认会备份当前核心文件和数据库到对应目录：

1. ZStack核心文件会备份在*/usr/local/zstack/upgrade/*目录下，以升级时的时间命名文件夹，假定为**2017-11-09-15-41-52**
2. 数据库默认备份在*/usr/local/zstack/db_backup/*，以升级时的时间命名文件夹，假定为**2017-11-09-15-42-43**，备份文件为**backup.sql**

恢复步骤：

1. 先备份之前版本的ZStack核心文件，执行

```
cp /usr/local/zstack/upgrade/2017-11-09-15-41-52 /root -r
```

2. 先备份之前版本的数据库，执行

```
cp /usr/local/zstack/db_backup/2017-11-09-15-42-43/backup.sql /root
```

3. 再次备份数据库，执行

```
zstack-ctl dump_mysql
```

4. 删除当前ZStack环境，执行

```
zstack-ctl stop
```

```
rm -rf /usr/local/zstack
```

5. 使用之前的安装包直接安装ZStack

```
bash ZStack-enterprise-installer.bin -D
```

6. 使用步骤1备份的ZStack核心文件恢复

```
zstack-ctl stop
cp /root/2017-11-09-15-41-52/zstack/
mv /usr/local/zstack/apache-tomcat/webapps/zstack /usr/local/zstack/apache-tomcat/
webapps/zstack-bk
cp /root/2017-11-09-15-41-52/zstack /usr/local/zstack/apache-tomcat/webapps  -r
chown zstack:zstack /usr/local/zstack/apache-tomcat/webapps/zstack -R
```

7. 恢复步骤2备份的数据库

```
cat /root/backup.sql |mysql -u root -pzstack.mysql.password zstack
```

8. 启动ZStack管理节点服务，此时ZStack已成功恢复至原本升级失败前的版本

```
zstack-ctl start
```

19.2 启动服务

ZStack相关的服务在管理节点重启后，会自动启动。

启动ZStack服务失败需检查的因素：

1. 数据库应正常运行：

   可通过systemctl status/start/stop/restart mariadb进行状态/启动/停止/重启检查。

2. 出现如下报错：

   现象：

   ```
   ERROR: failed to connect to the mysql server[hostname:10.0.0.18, port:3306, user:zstack,
    password:zstack.password]
   ```

   解决方案：

   - 需确保*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties*里面关于数据库的IP、用户名、密码均正确，且可使用*mysql*命令正常访问。
   - 例如，可通过mysql -u zstack -pzstack.password -h 10.0.0.18直接访问。

3. 出现如下报错：

现象：

```
8080 is occupied by some process. Please use netstat to find out and stop it
```

解决方案：

执行netstat -anp|grep 8080找到8080占用程序将其停止再启动ZStack。

4. 出现如下报错：

现象：

```
MN status: Unknown, the management node seems to become zombie as it stops respond
ing APIs
```

原因及解决方案：

一般是因为内存不足导致的消息总线不能正确处理，需扩大内存，此时不建议再将管理节点作为计算节点添加到ZStack使用。

19.3 zstack-ctl命令

ZStack提供*zstack-ctl*对服务或者资源进行命令行控制。

常用的*zstack-ctl*命令：

- 状态检查：zstack-ctl status
- 服务控制：zstack-ctl stop/start/stop_ui/start_ui/restart_node/
- 日志收集：zstack-ctl collect_log
- 备份数据库：zstack-ctl dump_mysql
- 恢复数据库： zstack-ctl restore_mysql -f back.gz --mysql-root-password password
- 管理节点IP变更：zstack-ctl change_ip
- 检查配置： zstack-ctl show_configuration
- 安装授权： zstack-ctl install_license -f license_key.txt
- 重置admin账户密码：zstack-ctl reset_password
- 修改数据库密码：zstack-ctl change_mysql_password --root-password zstack.mysql.password --user-name zstack --new-password password

注:

关于*zstack-ctl*命令的详细使用介绍，请参考官网文档《ctl命令使用手册》。

19.4 zstack-cli命令

ZStack提供*zstack-cli*命令行交互界面对ZStack内部各资源进行控制。

1. ***zstack-cli*登录**：

```
LogInByAccount accountName=admin password=password
```

初始密码为password，如果有修改，则需按照正确的密码登录。

2. ***zstack-cli*支持的关键字包括**：

- 资源关键字：

  zone cluster host vm primarystorage image L2 L3 backupstorage volume offering

- 操作关键字：

  add reconnect start stop destroy delete create get set update attach detach

3. **使用*zstack-cli*进行控制的技巧**：

- 输入资源关键字和操作关键字。
- 善用tab键。例如，输入集群的关键字cluster，点击两次tab键后，会列出cluster可支持的所有操作，如下：

  AttachL2NetworkToCluster
  AttachPrimaryStorageToCluster
  ChangeClusterState
  CreateCluster
  DeleteCluster
  DetachL2NetworkFromCluster
  DetachPrimaryStorageFromCluster
  GetCandidateZonesClustersHostsForCreatingVm
  GetVmStartingCandidateClustersHosts
  QueryCluster
  QueryVCenterCluster
  UpdateCluster

  此时假定打算再创建集群，根据上面列出的Cluster操作，那么输入CreateCluster后，再点击两次tab键，cli将列出CreateCluster参数。

4. **使用*zstack-cli*创建云主机的方法**：

```
zstack-cli CreateVmInstance name=ceph instanceOfferingUuid=$instanceoffer l3Netwo
rkUuids=$L3uuid imageUuid=$image
```

5. **使用*zstack-cli*查询运行中的云主机**：

```
zstack-cli QueryVmInstance state=“Running” name~=test limit=3 field=uuid
```

名字包含test，只显示3条记录，只显示其uuid。

注:

关于*zstack-cli*命令的详细使用介绍，请参考官网文档《 cli命令使用手册》。

19.5 重连物理主机

重连物理主机会重新部署代理程序进行相关检查。

重连物理主机失败需检查的因素：

1. 管理节点无法正常访问物理主机22端口，例如以下，需先解决管理节点可以正常ssh到物理主机的问题。

```
ssh: connect to host 192.168.0.65 port 22: Network is unreachable
```

2. 物理主机应可访问管理节点，以将agent代理的结果返回给管理节点。
3. 没有使用ZStack定制版ISO安装计算节点，导致升级失败，出现类似以下软件包安装冲突的错误，需要使用ZStack定制版ISO来重新安装系统，才可解决。

```
ERROR: command pkg_list=`rpm -q openssh-clients qemu-kvm bridge-utils wget qemu-img
libvirt-python libvirt nfs-utils vconfig libvirt-client net-tools iscsi-initiator-utils lighttpd dnsmasq
iproute sshpass rsync nmap | grep \"not installed\" | awk '{ print $2 }'` && for pkg in $pkg_list
; do yum --disablerepo=* --enablerepo=zstack-local install -y $pkg; done;failed!
```

4. 物理主机的libvirt服务状态应正常：

   可通过systemctl status/start/stop/restart libvirtd进行状态/启动/停止/重启检查。
5. 重连物理主机会检查其所属集群的网络挂载情况，假如集群挂载的二层网络指定的设备是eth1，但是物理主机的网卡设备号发生变化，不存在eth1，那么此物理主机将无法重连成功。
6. 如果物理主机系统盘的存储容量已经用完，此时物理主机将无法重连成功。
7. 对于要求挂载NFS主存储的物理主机，如果挂载失败，物理主机将无法重连成功，此时需要检查物理主机到NFS主存储的链路，例如以下错误，就需检查物理主机到NFS存储的连接。

```
failed to execute shell command: mount 192.168.18.242:/home/Storage/zhu /opt/zstack/
nfsprimarystorage/prim-751565713a6340da884c33a8668a8916
```

8. 使用分布式块存储的物理主机，如果存在存储网络，则要求物理主机可直接访问存储网络。
9. 如果使用VXLAN网络，其挂载集群时指定的VTEP IP应该存在，如果不存在，物理主机将无法重连成功。

19.6 重连主存储

重连主存储会重新部署代理程序进行相关检查。

重连主存储失败需检查的因素：

1. 本地存储一般处于可连接状态。
2. NFS主存储保证有可用物理主机可以连接此主存储。重连失败时，需检查NFS Server的IP地址、NFS共享目录、NFS挂载参数是否正确。
3. Ceph主存储需检查分布式块存储是否正常。重连失败时，需检查Ceph IP地址、Ceph SSH 端口、用户名、密码、用户名是否有sudo权限，Ceph集群状态是否正常。
4. Shared Mount Point主存储需在物理主机手动挂载此目录，建议在*/etc/rc.local*里进行定义，开机自启动挂载。

19.7 重连镜像服务器

重连镜像服务器会重新部署代理程序进行相关检查。

重连镜像服务器失败需检查的因素：

1. Sftp镜像服务器和镜像仓库需检查SSH端口号、用户名、密码、用户名是否拥有sudo权限。
2. Ceph镜像服务器需检查分布式块存储是否正常。重连失败时，需检查Ceph IP地址、Ceph SSH 端口、用户名、密码、用户名是否有sudo权限，Ceph集群状态是否正常。

19.8 云主机异常

创建云主机流程及创建失败分析

创建云主机的基本流程：

1. 根据选择的镜像选择可用的镜像服务器，此处需确保选择的镜像所在的镜像服务器处于可用已连接状态；
2. 根据选择的镜像服务器选择可用的集群，并基于对应的集群，基于计算规格，选择可用的物理主机，此处需确保有可用的物理主机处于可用已连接状态；
3. 根据选择的镜像的虚拟大小来选择可用的主存储，来判断主存储容量是否充足，此处需确保主存储可用已连接状态，且容量充足；
4. 根据选择的网络来配置相应的IP、MAC等，此处需确保网络正常，且IP地址池资源充足；
5. 从镜像服务器下载镜像到主存储，创建根云盘；
6. 给云主机分配IP；
7. 在物理主机上启动云主机。

创建失败需检查的问题：

1. 镜像服务器失联，检查镜像服务器可用并确保连接；

2. 主存储未挂载集群，导致找不到可用的物理主机，主存储需挂载集群；
3. 集群内没有可用的物理主机满足计算规格的定义，需确保物理主机可用，且资源满足；
4. 主存储容量不足以提供镜像需要的虚拟容量，需确保主存储容量充足；
5. 集群未挂载相应的网络，需确保集群已挂载对应的网络；
6. IP地址池资源不足，需确保IP范围充足；
7. 从主存储下载镜像到镜像服务器，确保链路正常；
8. 确保物理主机的分布式DHCP服务、dnsmasq服务正常，以正常方式提供DHCP IP分配服务；
9. 确保物理主机的Libvirtd服务正常，以正常提供虚拟化服务。

云主机相关异常处理

异常信息	异常原因及解决办法
“code”:”HOST.1005”,”description”:”Failed to start vm on hypervisor”, “details”:”failed to start ...., Libvirt error : internal error no supported architecture for os type ‘hvm’ ” 或"details": "failed to start vm on kvm host, because unable to start vm, libvirt error: invalid argument : could not find capabilities for domaintype =kvm "	• 原因： 需要物理主机支持并打开了硬件虚拟化（如vmx或者svm）的支持。出现该错误的原因通常是因为BIOS中没有打开CPU虚拟化。 • 解决方案： 重启系统，并进入BIOS打开CPU相关虚拟化支持。
“details”: "cannot find either 'vmx' or 'svm' in /proc/cpuinfo, please make sure you have enabled virtualization in your BIOS setting"	• 原因： 需要物理主机支持并打开了硬件虚拟化（如vmx或者svm）的支持。出现该错误的原因是用户添加的物理主机的CPU不支持硬件虚拟化功能。 通常是由于用户添加的物理主机是一个“云主机”导致的，需要打开对应“云主机”的嵌套虚拟化功能。 • 解决方案： 具体的打开办法，请联系“云主机”提供方。
"details": "the local primary storage has no hosts with enough disk capacity[xxx bytes] required by the vm[uuid:xxx]"	• 原因： 当前系统中（或者任何单独一台物理主机）没有足够的主存储容量（磁盘空间）。 ZStack在分配云主机和云盘时使用的是thin clone模式，也就是云主机使用多少，才分配多

异常信息	异常原因及解决办法
	少。但是在创建云主机的时候，会按照云主机最大申请的使用空间来扣除系统主存储的容量，以防最后云主机使用的空间超过系统可用空间。 此外，如果主存储为本地存储，由于云主机的磁盘不能够跨物理主机存储，所以如果每台物理主机的剩余空间都不足创建一台新的云主机，也会遇到此错误。 • 解决方案： 删除一些不需要使用的云主机、云盘，或者调整云主机使用的镜像大小。 在理解主存储超分的原理和使用方法的前提下，也可以增大主存储超分比例以获得更多超分空间。
"details": "unable to allocate hosts; due to pagination is enabled, there might be several allocation failures happened before; the error list is [{no host having cpu[x HZ], memory [xxx bytes] found}]"	• 原因： 当前系统中（或者任何单独一台物理主机）没有足够的内存。 • 解决方案： 删除一些不需要使用的云主机，或者调整云主机使用计算规格的大小。在理解内存超分的原理和使用方法的前提下，也可以增大存储超分比例以获得更多超分容量。
"details": "failed to start vm[uuid:xxx name:xxx] on kvm host[uuid:xxx, ip:x.x.x.x], because unable to start vm[uuid:xxx, name:xxx], libvirt error: internal error: early end of file from monitor: possible problem: Cannot set up guest memory 'pc.ram': Cannot allocate memory" set up guest memory 'pc.ram':Cannot allocate memory"	• 原因： 当前系统中实际可用物理内存不足以分配给需要创建的云主机。当这个错误出现时，就算提高内存超分比例，也没有办法创建更大容量的内存。 • 解决方案： 减小云主机的计算规格，增加物理主机的内存，或者增加物理主机的swap分区（会降低系统性能）。
"failed to migrate vm[uuid:xxx] from kvm host[uuid:xxx, ip:xxx] to dest host[ip:xxx], unable to migrate vm[uuid:xxx] to qemu+tcp://xxx/system, Unsafe migration:	• 原因： 当前的基础设置中，将云主机的磁盘缓存模式设置为其他模式，例如，writethrough或writeback，系统认为带缓存模式的迁移是不安全的。

异常信息	异常原因及解决办法
Migration may lead to data corruption if disks use cache != none"	• 解决方案： 需要将此基础设置的缓存模式修改为None模式才可迁移。
"description": "Failed to start vm on hypervisor",libvirt error: Unable to create tap device vnic15.0: Device or resource busy	• 原因： 此计算节点可能被重复添加，里面已经有使用了vnic15.0的云主机在运行，导致设备出现冲突。 • 解决方案： 建议添加物理主机时，需保持一个干净的环境，或清理掉其上已经运行的云主机。
Permission denied: '/opt/zstack/nfsprimarystorage/prim-cd8075752a0b4c669afa79acfc433ca5/dataVolumes'	• 原因： 创建云主机或数据盘时，NFS主存储的目录没有读写的权限， • 解决方案： 需在NFS服务器端开启读写权限。
internal error: unable to execute QEMU agent command 'guest-set-user-password': failed to set password: The user name could not be found.	• 原因： 修改云主机密码时，指定的用户名不存在。 • 解决方案： 需要指定已存在的用户名。

internal error: unable to execute QEMU agent command 'guest-set-user-password': The command guest-set-user-password has not been found	• 原因：
	修改云主机密码时，在云主机内部没有安装qemu-ga或者代理程序版本过低。
	• 解决方案：
	可执行qemu-ga -V检查版本。
	  • 在CentOS7.2里版本是2.3.0
	  • 在Windows 2012里版本是0.12.1

"description": "An operation failed","details": "unable to live migrate with local storage. The vm[uuid:0837761acdad4ffab2f75798cdb65c38] has volumes on local	• 解决方案： 本地存储的云主机在线迁移时，需要先卸载相关的数据云盘。

异常信息	异常原因及解决办法
storage,to protect your data, please stop the vm and do the volume migration"	
"libvirt error: error from service: ListActivatableNames: Connection is closed "或"libvirt error: Activation of org.freedesktop.machine1 timed out"	• 原因： 这类错误通常是由系统DBUS进程死掉或者DBUS运行异常引起的。 • 解决方案： - 方法1：重启ZStack物理主机，DBUS会自动恢复。 - 方法2：在物理主机上使用如下命令： 1. service systemd-machined restart 2. service libvirtd restart 3. 完成后用UI或者CLI重连出问题的物理主机。
{ "error": { "code": "HOST.1009", "description": "Failed to migrate vm on hypervisor", "details": "failed to migrate vm[uuid:90bb61f55e774f5f89c9e1ea46db7661] from kvm host[uuid:e5105c61114a4efe8bcc025f744226bd, ip:10.0.247.244] to dest host[ip:10.0.197.238], unable to migrate vm[uuid:90bb61f55e774f5f89c9e1ea46db7661] to qemu+tcp://10.0.197.238/system, internal error: Attempt to migrate guest to the same host localhost.domain.com" }, "createdTime": 1488170137857, "type": { "_name": "key.event.API.API_EVENT" }, "id": "e6bcd7c33ad9446b919e11cd647fc8dc" }	• 原因： 这是因为两台物理主机hostname相同，KVM在线迁移目前依靠hostname进行确认不同的物理主机，如果hostname相同，则会被认定为相同的物理主机。 • 解决方案： 请确保物理主机hostname不能相同。可以通过hostnamectl set-hostname your_new_hostname来设定。
all mons failed to execute http call[/ceph/primarystorageolume/clone	• 解决方案： 重连主备存储。
为什么冷迁移会失败？"SYS.1006" 简介: An operation failedfailed to execute bash [rsync -a --relative /data/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e/vol-3f1225391f414d84b1b025761440	• 原因： 权限属组问题。 Operation not permitted (1) rsync: recv_generator: mkdir "/data/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e/vol-3f1225391f414d84b1b025761440b297" failed: Permission

异常信息	异常原因及解决办法
b297/snapshots/c0bb52f90d194a55a0ae47468d503816.qcow2 --rsh="/usr/bin/sshpass -p mevoc0-_-03 ssh -o StrictHostKeyChecking=no -l mevoco" 10.20.40.32:/], return code: 23, stdout: , stderr: Warning: Permanently added '10.20.40.32' (ECDSA) to the list of known hosts. rsync: failed to set times on "/data": Operation not permitted (1) rsync: failed to set times on "/data/rootVolumes": Operation not permitted (1) rsync: failed to set times on "/data/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e": Operation not permitted (1) rsync: recv_generator: mkdir "/data/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e/vol-3f1225391f414d84b1b025761440b297" failed: Permission denied (13) *** Skipping any contents from this failed directory *** rsync error: some files/attrs were not transferred (see previous errors) (code 23) at main.c(1052) [sender=3.0.9] 详情: failed to execute bash[rsync -a --relative /data/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e/vol-3f1225391f414d84b1b025761440b297/snapshots/c0bb52f90d194a55a0ae47468d503816.qcow2 --rsh="/usr/bin/sshpass -p mevoc0-_-03 ssh -o StrictHostKeyChecking=no -l mevoco" 10.20.40.32:/], return code: 23, stdout: , stderr: Warning: Permanently added '10.20.40.32' (ECDSA) to the list of known hosts. rsync: failed to set times on "/data": Operation not permitted (1) rsync: failed to set times on "/data/rootVolumes": Operation not permitted (1) rsync: failed to set times on "/data/rootVolumes/acct-36c27e8ff05c4780bf6d2fa65700f22e": Operation not permitted (1) rsync: recv_generator: mkdir "/data/rootVolumes/acct-36c27e8	denied (13) *** Skipping any contents from this failed directory *** rsync error: some files/attrs were not transferred • 解决方案： 需要重新给正确的属组，确认要迁移的VM文件是不是root qemu组。

异常信息	异常原因及解决办法
ff05c4780bf6d2fa65700f22e/vol-3f12253 91f414d84b1b025761440b297" failed: Permission denied (13) *** Skipping any contents from this failed directory *** rsync error: some files/attrs were not transferred (see previous errors) (code 23) at main.c (1052) [sender=3.0.9]	
failed to start vm[uuid:4ef5a9e4ae6441 c7b046c384c3ae6f7f name:stack_local] on kvm host[uuid:d0d9800a09c34da4891e0 cc624a0d349, ip:192.168.1.166], because Traceback (most recent call last): File "/ var/lib/zstack/virtualenv/kvm/lib/python2.7 /site-packages/kvmagent/plugins/vm_plug in.py", line 2721, in start_vm self._start_vm (cmd) File "/var/lib/zstack/virtualenv/kvm /lib/python2.7/site-packages/kvmagent/ plugins/vm_plugin.py", line 2664, in _start_ vm 'unable to start vm[uuid:%s, name:%s], libvirt error: %s' % (cmd.vmInstanceUuid , cmd.vmName, str(e))) KvmError: unable to start vm[uuid:4ef5a9e4ae6441c7b046c 384c3ae6f7f, name:stack_local], libvirt error: internal error: early end of file from monitor, possible problem: qemu-kvm: / root/rpmbuild/BUILD/qemu-2.6.0/target- i386/kvm.c:1736: kvm_put_msrs: Assertion `ret == n' failed.	• 原因： 这是因为管理平台把host-passthrough开启而导致。 • 解决方案： 关闭此选项即可。
”code”:”SYS.1006”,description:An operation failed, details:failed to check physical network interfaces on lvm	• 原因： 检查物理机网卡失败。 • 解决方案： 此物理机对应集群已挂载此二层网络，添加物理机时，请确保物理机上存在该网卡。
description": "A message or a operation timeout","details": "[Async Http Timeout] url: http://10.10.10.253:7272/init, timeout after 300000[MILLISECONDS], command : {\"uuid\":\"78183b0a46094e30bc8a6	• 原因： 很可能是管理节点的IP地址无法访问出去。 一般出现这个情况是多网卡的服务器在安装管理服务时指定了第一个默认路由的网卡地址。 • 解决方案：

异常信息	异常原因及解决办法
128b30ee8cb\",\"restartDnsmasqAfterNumberOfSIGUSER1\":0}"	打开*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties* 修改**management.server.ip = xxx.xxx.xxx.xxx**这个IP地址 ，修改为可以访问出去的IP地址。
failed：Error in connection establishment: net::ERR_CONNECTION_REFUSED	• 解决方案： 打开*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties* 将**consoleProxyOverriddenIp =xxx.xxx.xxx.xxx**改为管理节点的IP地址，修改完后要重启节点才生效。
Could not access KVM kernel module: No such file or directory failed to initialize KVM : No such file or directory.	• 原因： 这个虚拟机不支持虚拟化技术。 • 解决方案： 需要先开启嵌套虚拟化。

19.9 日志分析

相关日志记录地址：

类型	日志路径	日志所在机器
管理节点日志	*/usr/local/zstack/apache-tomcat/logs/management-server.log*	管理节点
管理节点UI日志	*/usr/local/zstack/apache-tomcat/logs/zstack-ui.log*	管理节点
控制台代理日志	*/var/log/zstack/zstack-console-proxy.log*	管理节点
管理节点部署日志	*/var/log/zstack/deploy.log*	管理节点
shell命令日志	*/var/log/zstack/zstack.log*	物理主机
zstack kvmagent日志	*/var/log/zstack/zstack-kvmagent.log*	物理主机
VM对应的libvirt日志	*/var/log/libvirt/qemu/vm_uuid.log*	物理主机
系统基本日志	*/var/log/messages*	管理节点/物理主机等
镜像仓库日志	*/var/log/zstack/zstack-store/zstore.log*	镜像仓库

类型	日志路径	日志所在机器
Ceph 主存储日志	*/var/log/zstack/ceph-primarystorage.log*	Ceph Mon节点
Ceph 备份存储日志	*/var/log/zstack/ceph-backupstorage.log*	Ceph Mon节点
云路由器的日志	*/home/vyos/zvr/zvr.log*	云路由器
扁平网络的配置及日志	*/var/lib/zstack/dnsmasq/*	物理主机

日常运维出现错误时，进行错误分析的一般步骤如下：

1. 根据UI界面提示的错误信息进行简单分析。
   - 例如，创建云主机失败时提示的信息是no host found, 那么此时可能的原因就是选择的镜像所在的镜像服务器，可选的集群加上选择的网络进行筛选后，没有可用的物理主机。

     此时需要检查集群内是否有可用的物理主机，是否挂载相应的网络，集群是否挂载了相应的主存储。
2. 分析管理节点*/usr/local/zstack/apache-tomcat/logs/management-server.log*关于UI界面提示的错误信息。
   - 查询提示错误的信息，根据上下文进行分析，分析发生异常时的工作流。
   - 也可根据执行的操作API进行查询分析，例如创建云主机调用的API是APICreateVmInstance，在管理节点搜索这个API，往下逐步分析错误原因。
3. 再根据错误的具体信息，查看相关代理日志的错误信息。
   - 例如，在物理主机的*/var/log/zstack/zstack-kvmagent.log*查看对云主机进行生命周期控制时的代理错误日志。

19.10 端口占用

ZStack端口占用列表如下：

端口号	进程名	说明
8005	/bin/java	ZStack管理服务
8009	/bin/java	ZStack管理服务
8080	/bin/java	ZStack管理服务
8081	/bin/java	ZStack管理服务

端口号	进程名	说明
8090	nginx	ZStack管理服务（管理节点裸金属控制台代理）
5000	/bin/java	ZStack UI服务（HTTP方式）
5443	/bin/java	ZStack UI服务（HTTPS方式）
80	httpd	Web服务器
9100	node_exporter	监控数据采集
9103	collectd_expo	监控数据采集
7069	python	监控数据采集
8086	influxd	监控数据存储
8088	influxd	监控数据存储
9090	prometheus	promethus监控进程
9091	pushgateway	监控数据缓存
4900	consoleproxy	控制台代理
5900	qemu-kvm	kvm console服务
7758	python	控制台代理
53	dnsmasq	DHCP服务
4369	epmd	erlang port mapper daemon
7070	kvmagent	kvmagent代理服务
16509	libvirtd	libvirtd服务
5345	lttng-sessiond	内核跟踪框架
25	master	邮件服务器
3306	mysqld	MySQL进程
123	ntpd	NTP时间同步服务
7171	sftpbackupstorage	Sftp备份存储代理
7762	python	Ceph主存储
7761	python	Ceph镜像服务器
7770	python	部署服务器
7771	nginx	部署服务器代理服务

端口号	进程名	说明
7772	nginx	部署服务器代理服务
6080	websockify	部署服务器代理服务

19.11 网络脚本

ZStack定制的ISO提供了以下网络脚本方便配置网络：

1. zs-show-network用于显示网络状态，无须额外参数，显示网络连接及链路聚合状态。

```
[root@localhost ~]# zs-show-network
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: vmnic0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state
 UP qlen 1000
    link/ether fa:84:ba:34:92:00 brd ff:ff:ff:ff:ff:ff
    inet 172.20.54.194/16 brd 172.20.255.255 scope global vmnic0
       valid_lft forever preferred_lft forever
    inet6 fe80::f884:baff:fe34:9200/64 scope link
       valid_lft forever preferred_lft forever

-----------------------------------------------------------------
| Bond Name  | SLAVE         | BONDING_OPTS                    |
-----------------------------------------------------------------
```

2. zs-network-setting用于配置物理网卡网络命令。用法有两种：

   a. 方法一：

```
# 参数-i，意为对接口（interface）配置网络地址

zs-network-setting -i [interface] [ipaddress] [netmask] [gateway]
                       接口        地址          掩码         网关

# 例子1：zs-network-setting -i eth0 192.168.1.10 255.255.255.0 192.168.1.1
# 例子2：zs-network-setting -i eth0.10 192.168.1.10 255.255.255.0 192.168.1.1
```

   b. 方法二：

```
# 参数-b，意为基于接口（interface）创建网桥（bridge）并配置网络地址

zs-network-setting -b [interface] [ipaddress] [netmask] [gateway]
                       接口        地址          掩码         网关

# 例子1：zs-network-setting -b eth0 192.168.1.10 255.255.255.0 192.168.1.1
```

```
# 例子2：zs-network-setting -b eth0.10 192.168.1.10 255.255.255.0 192.168.1.1
```

3. zs-change-nic用于修改网卡名命令，修改网卡名后，脚本会将配置到*/etc/udev/rules.d/70-persistent-net.rules*，物理主机重启后命名仍保持新的命名。

```
# 参数-c，意为修改（change）物理网口名字

zs-change-nic -c [old-nic-name] [new-nic-name]
                 当前网卡名      新的网卡名

# 例子：zs-change-nic -c eth0 em01
```

4. zs-vlan用于配置VLAN接口。有两种用法：

   a. 方法一：创建VLAN

```
# 参数-c，意为创建（create）VLAN接口

zs-vlan -c [nic-name] [vlan]
           指定网卡   VLAN号

# 例子：zs-vlan -c zsnic0 10
```

   b. 方法二：删除VLAN

```
# 参数-d，意为删除（delete）VLAN接口

zs-vlan -d [nic-name] [vlan]
           指定网卡   VLAN号

# 例子1：zs-vlan -d zsnic0 10
# 例子2：zs-change-nic -c eth0 em01
```

注:

- 创建VLAN接口后，将会在*/etc/sysconfig/network-scripts/*创建对应的网络配置文件，物理主机重启后VLAN接口仍生效。删除VLAN接口后，对应网络配置将会删除。
- 创建VLAN接口后，若基于此端口与其他设备通信，需要参照网络设备厂商的VLAN配置手册，以允许该VLAN接口流量传输。
- 以下提供常见网络设备VLAN设定参考：
  - 华为：点击这里。
  - 华三：点击这里。
  - 思科：点击这里。
  - 瞻博：点击这里。

5. zs-bond-lacp用于创建删除Bonding链路聚合命令。有两种用法：

a. 方法一：创建Bonding 链路聚合

```
# 参数-c，意为创建（create）链路聚合接口

zs-bond-lacp -c [bond-name]
                聚合接口

# 例子：zs-bond-lacp -c bond0
```

b. 方法二：删除链路聚合

```
参数-d，意为删除（delete）链路聚合接口

zs-bond-lacp -d [bond-name]
                聚合接口

# 例子：zs-bond-lacp -d bond0
```

注:

本命令创建的接口是基于IEEE 802.3ad动态链路聚合协议（LACP），该接口需要管理员设定物理主机接入层网络交换机的端口组（Port-Group）。

6. zs-nic-to-bond用于配置链路聚合命令。

a.

```
# 参数-a，意为加载（attach）物理接口到聚合接口

zs-nic-to-bond -a [bond-name] [nic-name]
                  聚合接口      物理接口

# 例子：zs-nic-to-bond -a bond0 em1
```

b.

```
# 参数-d，意为从聚合接口卸载（detach）物理接口

zs-nic-to-bond -d [bond-name] [nic-name]
                  聚合接口      物理接口

# 例子：zs-nic-to-bond -d bond0 em1
```

注:

该命令执行后，会反馈执行接口，并显示聚合接口与物理接口的关系，例如：

```
-----------------------------------------------------------------------------
| Bond Name | SLAVE(s) | BONDING_OPTS |
-----------------------------------------------------------------------------
| bond0 | enp1s0f1 | miimon=100 mode=4 xmit_hash_policy=layer2+3 |
|       | enp1s0f0 |                                             |
-----------------------------------------------------------------------------
```

- 其中，bond0是聚合接口，enp1s0f0和enp1s0f1是物理接口，显示其绑定关系。

- 此外，enp1s0f0和enp1s0f1对应的接入网络设备的物理端口组成端口组（Port-Group），管理员需依照网络设备型号配置端口组。
- 以下提供常见网络设备端口组设定参考：
  - 华为：点击这里。
  - 华三：点击这里。
  - 思科：点击这里。
  - 瞻博：点击这里。

19.12 机房维护步骤

维护性关机

维护性关机前，需要确保云平台处于正常情况，且物理主机和主存储都处于已连接状态。维护性关机步骤如下：

- **普通场景**
  1. 将所有主存储进入维护模式。待所有主存储进入维护模式后，确保所有云主机已经关机。
  2. 将所有物理主机进入维护模式。
  3. 将所有服务器正常下电。
- **管理节点高可用场景**
  1. 将所有主存储进入维护模式。待所有主存储进入维护模式后，确保所有云主机已经关机。
  2. 在超融合节点执行zsha stop命令，关闭超融合。
  3. 将所有物理主机进入维护模式。
  4. 将所有服务器正常下电。

维护性关机后上电

- **普通场景**
  1. 将所有服务器上电。
  2. 登录管理节点执行zstack-ctl status 命令查看管理节点状态，等待ZStack服务启动成功。
  3. 登录ZStack云平台，确保物理主机和主存储是已连接状态，然后启用主存储。
- **管理节点高可用场景**
  1. 将所有服务器上电。
  2. 在超融合节点执行zsha status命令查看超融合状态，等待启动成功。

3. 登录管理节点执行zstack-ctl status 命令查看管理节点状态，等待ZStack服务启动成功。
4. 登录ZStack云平台，确保物理主机和主存储是已连接状态，然后启用主存储。

20 其他配置运维

本章主要针对高级用户，提供一些场景下的配置运维指南。

20.1 安装多个管理节点

自动安装

如果用户希望搭建一个高可用的产品级云环境，那么可以部署多个管理节点以保证管理节点的高可用。 如有对数据库和消息总线有高可用的需求，可参考ZStack 高可用集群快速配置进行配置。

用户通过安装部署已经安装完成一个管理节点，使用zstack-ctl add_multi_management命令安装。

使用方法如下：

```
zstack-ctl add_multi_management --host-list root:passwd1@host1_ip root:passwd2@host2_ip
```

注: 例如

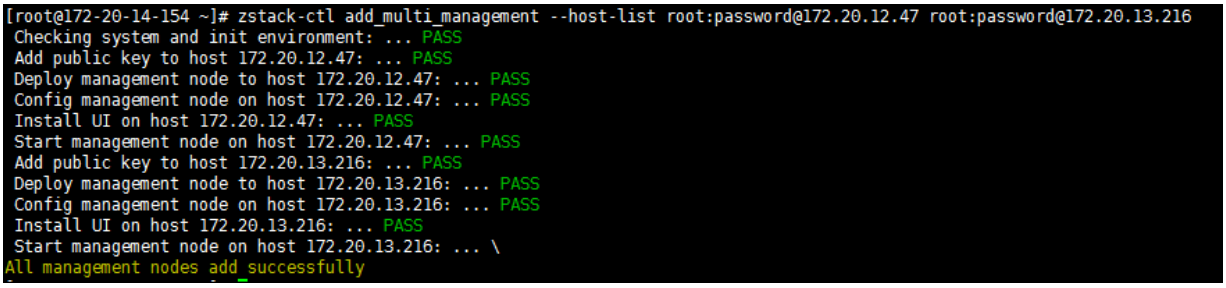
```
zstack-ctl add_multi_management --host-list root:password@172.20.12.47 root:passwor
d@172.20.13.216
```

如图 *122: 多管理节点安装界面*所示，*172.20.14.154*为第一个管理节点，使用该命令添加*172.20.12.47*和*172.20.13.216*两个管理节点。

安装完毕后，ZStack会使用这三台主机作为管理节点同时提供服务，任一管理节点服务中断，不影响其他管理节点的控制服务。

注: 此时Mysql、消息总线服务依然存在在第一台管理节点上。如有需求，可以将其分别配置。

图 122: 多管理节点安装界面



手动安装

当管理大量物理主机的时候，为了提高可用性，用户可以安装多个管理节点。多个管理节点之间关系平等，相互支撑。用户可以使用如下的方法安装：

```
zstack-ctl install_management_node --host=ip_of_machine_to_install_node_2 --yum=alibase
,aliepel
```

当新节点成功安装后，请在新节点上配置新管理节点的IP地址：

```
zstack-ctl configure management.server.ip=ip_of_management_node2
zstack-ctl save_config
```

可以重复这一步来安装更多的管理节点。

如果启动了多个管理节点，在批量创建云主机时，需要修改安装了mysql的管理节点的配置文件*/etc/my.conf*，将其中的最大连接数修改为适合的值，来增加可接受的最大并发数量。假如有三个管理节点，启动一百个云主机，最大并发数量至少需高于300，下例设置为500，可作为参考：

```
vim /etc/my.conf
max_connections = 500
```

如果用户购买了ZStack使用授权，请联系销售厂商给每一个管理节点单独安装一个授权协议。

多管理节点自动升级

ZStack一条命令即可完成多节点的升级：

```
zstack-ctl upgrade_multi_management_node --installer-bin zstack-installer.bin
```

20.2 配置独立的MySQL服务器

ZStack在安装过程中会配置一个本地的数据库。用户也可以安装独立的MySQL数据库。

安装独立的MySQL数据库后，用户需使用下面的ZStack的工具来初始化数据库，并进行对应的设置。

- **MYSQL_ROOT_PASSWORD**是MySQL的根用户密码；
- **MYSQL_ZSTACK_PASSWORD**是用户希望设置的ZStack用户的MySQL密码；
- **MYSQL_SERVER_IP**是mysql数据库的物理主机IP地址。

输入命令后，会要求用户输入MYSQL服务器的SSH密码用于远程登录：

```
sudo zstack-ctl deploydb --root-password="MYSQL_ROOT_PASSWORD" --zstack-password
="MYSQL_ZSTACK_PASSWORD" --host=” MYSQL_SERVER_IP”
```

20.3 zstack.properties核心配置文件

zstack.properties是ZStack的核心配置文件。它会存放在每一个管理节点中。

zstack.properties文件中会存放诸如数据库URL、用于数据库访问的用户名密码、消息总线的IP地址等信息。 每一个管理节点上的zstack.properties文件的内容基本上是一致的。它的路径可以通过zstack-ctl status来获得。

如果是默认安装的话，它会存放在*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties*

以下是zstack.properties文件内容的详细说明。

表 7: zstack.properties

类别	参数	解释
数据库	DB.url = jdbc:mysql://10.0.5.87:3306	数据库URL、端口
	DB.user = zstack	数据库用户名
	DB.password = zstack.password	数据库密码
Sftp镜像服务器	SftpBackupStorageFactory.agentPort = 7171	Sftp镜像服务器端口
Ansible	Ansible.cfg.forks = 100	设置Ansible的forks值
	Ansible.cfg.host_key_checking = False	设置Ansible的host_key_checking值
	Ansible.cfg.pipelining = True	设置Ansible的pipelining值
	Ansible.keepHostsFileInMemory = false	是否在内存中保留ansible/hosts
	Ansible.cfg.ssh_connection.ssh_args = -C -o ControlMaster=auto -o ControlPersist=1800s	Ansible的SSH连接参数

类别	参数	解释
消息总线	CloudBus.serverIp.0 = 10.0.5.87	CloudBus服务器IP地址
日志	org.jboss.logging.provider = slf4j	日志服务提供者
控制台	consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem	控制台证书
	consoleProxyOverriddenIp = 172.20.11.50	控制台代理对外IP地址
	consoleProxyPort = 4900	控制台代理端口
ZWatch/SNS	sns.systemTopic.endpoints.http.url = http://localhost:5000/zwatch/webhook	ZWatch通知的系统接收端
ZStack YUM	Ansible.var.zstack_repo = "zstack-mn,qemu-kvm-ev-mn"	ZStack使用的YUM源名称
管理节点服务	management.server.ip = 10.0.5.87	管理节点服务器IP地址
chrony	chrony.serverIp.0 = 10.0.5.87	chrony服务器IP地址
默认API超时设置	ApiTimeout.org.zstack.header.image.APIAddImageMsg = timeout::3h	添加镜像超时时间
	ApiTimeout.org.zstack.header.image.APICreateRootVolumeTemplateFromRootVolumeMsg = timeout::72h	从根云盘创建云盘镜像的超时时间
	ApiTimeout.org.zstack.header.image.APICreateDataVolumeTemplateFromVolumeMsg = timeout::72h	从云盘创建数据云盘镜像的超时时间
	ApiTimeout.org.zstack.header.volume.APICreateDataVolumeFromVolumeTemplateMsg = timeout::72h	从云盘镜像创建数据云盘的超时时间
	ApiTimeout.org.zstack.header.image.APICreateRootV	从云盘快照创建根云盘镜像的超时时间

类别	参数	解释
	olumeTemplateFromVolumeSnapshotMsg = timeout::3h	
	ApiTimeout.org.zstack.header.volume.APICreateDataVolumeFromVolumeSnapshotMsg = timeout::3h	从云盘快照创建数据云盘的超时时间
	ApiTimeout.org.zstack.header.volume.APICreateVolumeSnapshotMsg = timeout::3h	创建云盘快照的超时时间
	ApiTimeout.org.zstack.header.vm.APICreateVmInstanceMsg = timeout::3h	创建云主机的超时时间
	ApiTimeout.org.zstack.storage.primary.local.APILocalStorageMigrateVolumeMsg = timeout::24h	迁移本地存储上存放的云盘的超时时间
默认的KVM主机iptables规则	KvmHost.iptables.rule.0 = '-I INPUT -p tcp -m tcp --dport 1234 -j ACCEPT'	KVM计算节点预设iptables规则
	KvmHost.iptables.rule.1 = '-I INPUT -p tcp -m tcp --dport 2345 -j ACCEPT'	KVM计算节点预设iptables规则

20.4 zstack.ui.properties核心配置文件

zstack.ui.properties是ZStack UI的核心配置文件。它会存放在每一个管理节点中。

zstack.ui.properties文件中会存放诸如UI数据库URL、用于UI数据库访问的用户名密码、UI服务器端口等信息。 每一个管理节点上的zstack.ui.properties文件的内容基本上是一致的。

如果是默认安装的话，它会存放在*/usr/local/zstack/zstack-ui/zstack.ui.properties*

以下是zstack.ui.properties文件内容的详细说明。

表 8: zstack.ui.properties

类别	参数	解释
管理节点	mn_host = 127.0.0.1	管理节点IP，默认*127.0.0.1*

类别	参数	解释
	mn_port = 8080	管理节点端口，默认8080
Webhook主机	webhook_host = 127.0.0.1	Webhook主机IP，默认*127.0.0.1*
	webhook_port = 5000	Webhook主机端口，默认5000
UI服务器	server_port = 5000	UI服务器端口，默认5000
UI日志	log = /usr/local/zstack/apache-tomcat/logs	UI日志文件夹，默认*/usr/local/zstack/apache-tomcat/logs*
UI HTTPS	enable_ssl = false	启用/关闭HTTPS登录UI
	ssl_keyalias = zstackui	UI证书别名，默认zstackui
	ssl_keystore = /usr/local/zstack/zstack-ui/ui.keystore.p12	UI证书路径，默认*/usr/local/zstack/zstack-ui/ui.keystore.p12*
	ssl_keystore_type = PKCS12	UI证书类型，默认PKCS12
	ssl_keystore_password = password	UI证书私钥密码，默认password
数据库	db_url = jdbc:mysql://10.0.5.87:3306	UI数据库URL，默认*jdbc:mysql://10.0.46.243:3306*
	db_username = zstack_ui	UI数据库用户名，默认zstack_ui
	db_password = zstack.ui.password	UI数据库密码，默认zstack.ui.password
UI服务进程	catalina_opts = -Xmx4096m	UI服务进程最大可用内存

20.5 云平台硬件资源密码变更

对于ZStack云平台的硬件资源，如物理主机、Ceph主存储、镜像服务器等，在这些节点的操作系统内如果密码发生变化，需在ZStack云平台界面更改相应硬件资源的密码，以确保云平台使用正确的密码连接相应的硬件资源。否则会导致资源失联不可用，重连也会提示ssh连接错误。

更改密码的方法：在ZStack云平台界面，点击相应节点展开其详情页，点击相应节点IP旁边的编辑按钮进行更改，IP地址更改后，需重连生效。

20.6 管理节点更改物理环境

ZStack的授权与用户的物理主机的环境一一匹配。如果用户更新了管理节点物理主机硬件配置，可能会导致ZStack的授权失效，而启动失败。此时请联系ZStack的销售和技术支持获取帮助。

20.7 数据库备份与恢复

为保护数据安全，防止数据丢失，支持主动定期进行数据库备份。

- 可使用zstack-ctl dump_mysql命令对数据库进行备份。
- 可使用zstack-ctl restore_mysql -f back.gz --mysql-root-password password命令对数据库进行恢复。
- 默认使用*crontab*命令进行控制。
  - 可使用*crontab -l*命令查看管理节点相关的自动定时备份任务。
  - 可使用*crontab -e*命令在界面里修改备份策略，默认为每天的凌晨和中午12：30进行备份，并且最多保留最新的14次备份。
- 默认的数据库备份文件存放路径：*/var/lib/zstack/mysql-backup/*
- 建议用户使用异地备份策略来提高安全性。只要数据库文件存在，即使ZStack的相关机器挂掉，均可使用数据库文件进行恢复。
- 需注意，进行数据库备份的时候，可能会影响管理节点操作的流畅性。

20.8 管理节点灾难恢复

使用ZStack过程中，管理节点可能因为硬件故障或系统崩溃导致无法进入系统，此时只需在其他机器上重新安装ZStack，恢复相应的数据库即可对ZStack进行灾难恢复。

20.8.1 准备工作

定时备份数据库

ZStack云管理平台首次安装后，默认会自动备份数据库，默认每天凌晨12点半和中午12点半，各备份一次数据库，最多保留14次备份数据。可通过crontab -l查看。

```
30 0,12 * * * zstack-ctl dump_mysql --keep-amount 14
```

如果管理节点长期运行在高负载状态，建议调整备份频率和保留备份次数，通过crontab -e 修改为以下状态。表示每小时的30分，进行一次数据库备份，最多保留200次备份数据。

```
30 * * * * zstack-ctl dump_mysql --keep-amount 200
```

异地备份数据库

ZStack云管理平台的数据库默认备份在管理节点的/var/lib/zstack/mysql-backup/目录。为防止管理节点出现故障不能进入系统，建议在额外节点进行相应的数据库备份。

假定管理节点的IP地址为*172.20.12.16*，异地备份机器的IP地址为*172.20.12.75*，进行异地备份，请在异地备份机器*172.20.12.75*上执行以下步骤：

```
ssh-keygen
#在异地备份机器上生成ssh key公钥
ssh-copy-id root@172.20.12.16
#拷贝ssh key 公钥到管理节点，期间需手动输入yes和root密码
```

异地数据库冗余备份

如果有多台机器可做冗余备份，可以在其他机器上同时进行异地数据库备份，增加数据库的多备份。

在异地备份机器*172.20.12.75*上，通过crontab -e 修改*crontab*，使用*rsync*远程拷贝管理节点存放的数据库目录来进行定时异地备份。

```
50 * * * * rsync -av root@172.20.12.16:/var/lib/zstack/mysql-backup/ /mysql-backup/
#每小时的50分，将管理节点172.20.12.16的/var/lib/zstack/mysql-backup/目录，直接同步到异地备份机器的/mysql-backup/目录下。
```

20.8.2 管理节点灾难恢复

背景信息

假如管理节点因硬件或软件故障无法进入系统，可参考以下步骤进行恢复。

操作步骤

1. 安装管理节点操作系统。

   参考ZStack官方的ISO进行操作系统的安装，选择原本的管理节点重新安装管理节点操作系统，或选择新的机器作为管理节点。

2. 安装ZStack

   参考*ZStack*官网的安装文档进行安装。

   注: 请选择系统出现故障时的版本进行安装。假定在出现故障前，ZStack版本为2.2.3，则建议安装ZStack 2.2.3。待恢复数据库后，再进行升级ZStack到最新版本。

3. 恢复数据库。

   在异地备份的机器上，选择最后一次的数据库备份文件。其文件命名类似以下格式：

```
zstack-backup-db-2016-12-07_14-43-43.gz
#代表在2016年12月7日14点43分43秒进行的数据库备份
```

   将此文件拷贝到新安装的ZStack机器上。假定存放在*/root/*目录。执行以下命令进行数据库恢复。恢复数据库之前，ZStack会再次对当前的数据库进行备份。恢复过程中会停止相关的管理节点服务。

```
zstack-ctl restore_mysql -f /root/zstack-backup-db-2016-12-07_14-43-43.gz --mysql-root-
password zstack.mysql.password
#-f参数代表选择/root/zstack-backup-db-2016-12-07_14-43-43.gz进行数据库恢复
#--mysql-root-password zstack.mysql.password参数代表指定使用zstack.mysql.password
作为mysql的root密码进行恢复
```

   注:

   - 如果恢复前管理节点同时作为计算节点添加进入物理主机列表，那么此计算节点不可恢复，需手动删除。
   - 如果恢复前管理节点有修改过consoleProxyOverriddenIp 的值，同时需要在新管理节点修改以下文件的consoleProxyOverriddenIp配置以恢复原本设置。

     ```
     /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack
     .properties
     ```

   - 如果管理机器数据库备份未同步到异地备份机器上，就发生了灾难，无法修复。
   - 参考本文档的恢复方法，可能存在一个小时的数据误差。此时间段内创建的云主机，数据恢复后，可能会变成不受控制的云主机。但是其他云主机的状态会直接同步原本物理主机的状态。

20.9 本地存储空间扩容

前提条件

在使用ZStack产品的过程中， 如果存储空间容量不足，可通过以下方式进行存储空间扩容。

背景信息

以下为系统主存储空间*/zstack_ps*扩容的样例。

操作步骤

1. 设置待扩容的物理主机进入维护模式。
2. 插入新的大容量磁盘至物理主机，并进行分区格式化，假如设备名称为**/dev/sdc**
3. 创建新目录*/new_volume*，挂载此磁盘`mount /dev/sdc1 /new_volume`
4. 执行`rsync -a /zstack_ps /new_volume/`拷贝原始的磁盘文件至新磁盘。
5. 添加以下内容至*/etc/fstab*，将物理磁盘挂载点与*/zstack_ps*目录绑定。

```
/dev/sdc1 /new_volume auto defaults 0 0
/new_volume /zstack_ps none defaults,bind 0 0
```

6. 重启物理主机，使用`df -h /zstack_ps`检查扩容后的空间增量。

```
Filesystem Size Used Avail Used% Mounted on
/dev/vdb1 4.0T 304G 3.5T 8% /zstack_ps
```

7. 重启ZStack服务。

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

8. 重连Host继续使用ZStack。

后续操作

备份存储的扩容方法与此类似，只是无须对Host进行维护模式及重连的操作。

20.10 云主机根云盘扩容

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**，可按需进行根云盘扩容，更改容量即时生效。

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**，可按需进行根云盘扩容，更改容量即时生效。
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。

注:

- 扩容容量只增不减，增量不得小于4MB。单位包括：MB/GB/TB

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。
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。

21 常见问题

21.1 快速入门

1. Q：ZStack云平台能干什么？

   A：

   总的来说，可帮助用户便捷创建、管理业务云主机以及相关的网络存储资源，例如：

   - 可实时获取物理资源的使用情况，例如：处理器、内存、存储和网络等，用户只需负责创建业务云主机即可，当资源不够时云平台会立即发出告警。
   - 用户创建业务云主机，云平台可帮忙提前复制模板，修改xml文件等。
   - 用户创建业务云主机后，云平台可帮忙设置或修改相关IP地址。
   - 支持扁平网络、云路由网络和VPC网络，用户可以快速搭建灵活多样的网络场景，只需在UI界面进行鼠标操作，便能生成一套满足自己需求的网络架构。
   - 支持接管vCenter，一套平台同时管理KVM和VMware两套集群。支持vCenter的云主机到ZStack平台的V2V迁移。
   - 云平台支持不同账户看到不同的业务云主机。
   - 云平台还支持计费等高级功能。
   - 用户可在云平台上快速搭建灵活多样的网络场景，只需在UI界面进行鼠标操作，避免繁琐手动部署。
   - 用户可在云平台上直接给业务云主机添加防火墙，设置各种安全策略，简单快捷。
   - 支持企业管理、裸金属管理、迁移服务（V2V迁移）、灾备服务等高级功能

   除了上述列举，ZStack还有很多强大功能，更多精彩尽在ZStack企业版。

2. Q：ZStack有哪些文档？用户应该看什么？

   A：ZStack有如下文档：

   - **特性概览**：

     汇集各版本的特色功能介绍，用户可以了解ZStack每个版本的特色功能以及发展历程。
   - **产品手册**：

包括：**用户手册**、**运维手册**、**技术白皮书**、**cli命令使用手册**和**ctl命令使用手册**。这些手册主要介绍了ZStack的架构特点、功能优势、安装部署、使用指南、以及管理运维过程中的常见问题解决方案。若用命令行方式使用ZStack，将会展开另一片新天地。

- **产品教程**：

  包括：快速安装教程（新手快速入门）、升级教程、以及针对不同应用场景提供的实践教程，例如混合云使用教程、超融合产品使用教程、外接设备透传教程、桌面云VDI使用教程等。涵盖场景十分丰富多变，实践操作也很简单便捷，用户可分分钟快速上手。

- **开发手册**：

  它是ZStack的核心，主要从API层面带你认识ZStack，了解之后，会对ZStack有更深刻的认知。

- **常见问题**（FAQ）：

  摘选出用户在实际使用过程中的常见问题集锦，并给出解决方案。

- **博客**：

  更高的视角，更深入的探讨，它说的是ZStack，又不仅仅是ZStack，可帮助用户拓展视野，对云计算IaaS有更透彻的理解。

阅读建议如下：

- **对于小白用户**：
  - 首先应该了解IaaS的概念，了解什么是ZStack，它能用来干什么。
  - 然后可参考**快速安装教程**（**新手快速入门**），赶快安装一下吧。
  - 安装成功后，如何使用它呢？可查阅我们的产品教程，例如尝试部署一套无虚拟路由的扁平网络。
  - 如果成功创建了第一台云主机，就已成功迈出了第一步。
  - 接下来可尝试产品教程里的其他场景部署实践，将会对UI上的各种功能和名词有新的认识。
  - 认真阅读博客，认知会上升一个台阶。
- **对于开发者**：
  - 可能只关心部分功能点，可参考**开发手册**了解二次开发的API等。
  - 毫无疑问，也可参考**cli命令使用手册**，以cli方式部署一套ZStack环境。

  - **开发手册**和**cli命令使用手册**是必须的工具，部分问题在产品教程和博客中或许会找到答案。
- **对于老司机**：
  - 快速阅读安装部署文档后，选择一种合适的方案即可。
  - 可能更想研究**开发手册**和**博客**。
  - 在使用过程中，遇到问题都可以先参考**常见问题**（FAQ）。如果没有，欢迎在ZStack社区（qq群：443027683）中提问。

21.2 安装部署

1.

Q：ZStack支持哪些硬件环境？

A：ZStack支持带硬件虚拟化特性的x86和ARM架构服务器、工作站或台式机，支持主流的Intel或AMD的处理器。

2.

Q：ZStack支持哪些操作系统？

A：ZStack支持基于CentOS 7.2/7.4深度定制的ZStack定制版ISO。

- 基于CentOS 7.4深度定制的ZStack定制版ISO：

  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。初次安装推荐安装c74 ISO。
- 基于CentOS 7.2深度定制的ZStack定制版ISO：

  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，可将基于c72的旧版本升级至最新。

3.

Q：ZStack支持使用标准的CentOS 7.2/7.4系统安装么？

A：暂不支持，ZStack目前支持基于CentOS 7.2/7.4深度定制的ZStack定制版ISO。

4.

Q：安装部署ZStack需要多少台机器？

A：最小安装只需要一台机器，同时作为管理节点和计算节点；生产环境建议分离部署。ZStack只需一台管理节点，就可以管控所有的硬件资源。

5.

Q：安装部署ZStack，机器的最低配置要求多少？

A：4CPU、8G内存、200G主存储、200G镜像服务器空间。最小配置仅适用于测试环境。

6. Q：ZStack定制版ISO可以安装哪些模式？有哪些差异？

   A：ZStack定制版ISO支持以下几种模式：

   1. ZStack Enterprise Management Node：ZStack企业版管理节点模式

      安装基于CentOS 7.2/7.4深度定制的ZStack定制版ISO并安装ZStack企业版管理节点。
   2. ZStack Community Management Node：ZStack社区版管理节点模式

      安装基于CentOS 7.2/7.4深度定制的ZStack定制版ISO并安装ZStack社区版管理节点。
   3. ZStack Compute Node：ZStack计算节点模式

      安装基于CentOS 7.2/7.4深度定制的ZStack定制版ISO并安装ZStack计算节点必备软件包。
   4. ZStack Expert Node：ZStack专家模式

      安装基于CentOS 7.2/7.4深度定制的ZStack定制版ISO并配置本地源，用户可自定义系统用途。

7. Q：如何安装ZStack企业版？

   A：下载最新的*ZStack定制版ISO*，首次安装系统时，建议选择企业版管理节点模式。操作系统安装完毕后，重启系统会自动安装企业版管理节点。

8. Q：如何升级ZStack企业版？

   A：如需将已部署ZStack升级至最新版本，可参考以下两种方法进行升级（以c74版本为例）：

   - **增量升级**：

     1. 在*ZStack*官网获取最新的bin安装包：ZStack-installer-3.1.1.bin；
     2. 若数据库root密码为默认密码，请执行以下命令升级;

        ```
        bash ZStack-installer-3.1.1.bin -u
        ```

        若数据库root密码采用自定义非空密码，请执行以下命令进行升级：

        ```
        bash ZStack-installer-3.1.1.bin -u -P MYSQL_ROOT_PASSWORD
        ```
   - **离线升级**：

     1. 在*ZStack*官网获取最新的iso安装包：ZStack-x86_64-DVD-3.1.1-c74.iso；
     2. 获取最新的升级脚本：升级脚本；

3. 执行以下命令升级：

```
bash zstack-upgrade ZStack-x86_64-DVD-3.1.1-c74.iso
```

注: c72版本和c74版本升级方法相同，请获取c72版本对应的安装包进行升级。

9. Q：如何从专家模式升级到管理节点？

   A：依次执行如下命令，将专家模式升级为管理节点：

```
yum --disablerepo=* --enablerepo=zstack-local install zstack-manager
bash ZStack-installer-3.1.1.bin -E
```

10. Q：如何从专家模式升级到计算节点？

    A：依次执行如下命令，将专家模式升级为计算节点：

```
yum --disablerepo=* --enablerepo=zstack-local
qemu-kvm-ev groupinstall zstack-host
```

11. Q：如何从计算节点升级到管理节点？

    A：依次执行如下命令，将计算节点升级为管理节点：

```
rpm -e zstack-host
yum --disablerepo=* --enablerepo=zstack-local install zstack-manager
bash ZStack-installer-3.1.1.bin -E
```

12. Q：如何将管理节点从ZStack社区版升级到ZStack企业版？

    A：获取最新的企业版许可证，更换许可证即可。

13. Q：如何重新安装ZStack？

    A：

    1. 先执行以下命令删除原本的数据库：

```
rm -rf /usr/local/zstack
```

注: 此命令会删除该目录下所有数据，如需彻底重装ZStack，才可使用。

2. 再执行以下命令重装管理节点：

```
bash ZStack-installer-3.1.1.bin -D #安装ZStack企业版
```

14. Q：使用root安装ZStack为何启动服务提示非root？

A：

- **现象**：

  安装ZStack时，有时使用root登录，但是启动服务时，提示非root用户需使用sudo

  ```
  ERROR: please use sudo or root user FAIL
   Reason: failed to start zstack
  ```

  在Python命令行环境下执行以下命令会发现Python认定用户并非root用户

  ```
  import getpass
   user = getpass.getuser()
   print user
  ```

- **原因**：

  之前由普通用户切换root用户时，使用了su并非使用sudo su，su只是shell认为切换了root用户，但是相关的环境变量并没有切换。

- **说明**：

  - sudo允许命令在当前用户下以root的超级权限来执行。
  - su允许切换为root用户，但是相关的用户环境并没有切换到root下去。
  - sudo su以root权限切换到root用户下。

15. Q：ZStack如何自动多节点安装？

A：

- 部分用户会用到多管理节点做高可用等场景。多节点手动安装方法请参考：安装多个管理节点。
- 多管理节点的自动化安装方法：

- 执行以下命令：

```
zstack-ctl add_multi_management --host-list root:passwd1@host1_ip root:passwd2
@host2_ip
```

- 如果用户已经使用**ssh_key**来连接各个节点，可以用以下命令添加：`--ssh-key`，此处为保存**ssh_key**文本文件的绝对路径。

注: ZStack1.8版本支持该功能，ZStack2.0版本以后暂不支持该功能。

16.

Q：多节点部署可以有节点使用云主机吗？

A：可以，但是网络需要连通，建议云主机的节点使用桥接。云主机节点运行管理节点更为合适，配置不低于4CPU、8G内存。

17.

Q：能在ZStack的云主机上安装ZStack吗？

A：可以。在**全局设置**的**基础设置**中修改**云主机CPU模式**为**host-passthrogh**，透传物理主机的虚拟化特性。

18.

Q：当服务器有多个网卡时，安装ZStack报错怎么办？

A：多网卡的物理主机上使用命令安装，默认会选择一块网卡。如果出现安装错误，可以使用`-i 网卡IP` 命令指定一块网卡。

19.

Q：安装管理节点没有配置IP报错怎么处理？

A：

手动给物理机网卡配置IP地址后，执行`bash /opt/zstack-*installer.bin -E NIC_NAME`安装企业版管理节点 ；或执行`bash /opt/zstack-*installer.bin NIC_NAME`安装社区版管理节点。

20.

Q：一键安装ZStack后，启动时间过长怎么办？

A：

- **原因**：

  管理节点启动时间与节点配置资源有关，在云主机上安装ZStack才出现时间过长的情况。

- **解决方案**：

  建议使用虚拟环境时，配置CPU>4，内存>16G。

注:

时间过长不代表安装启动失败，time out报错后请先使用zstack-ctl status查看状态。如果为**stopped**状态，使用zstack-ctl start启动即可；如果为**unknown**状态，需要先使用zstack-ctl stop停止，再使用zstack-ctl start启动。

21.

Q：ZStack如何更改安装目录？

A：安装ZStack时，加上 **-r 目标目录**。例如：

```
bash zstack-installer.bin -r /home/zstack
```

22.

Q：基于**ZStack + Ceph**部署，创建vm、zstack-mn、qemu-kvm-ev-mn，离线安装时出现这个报错如何处理？

A：

- **现象**：

  报错如下：

```
"org.zstack.header.vm.APICreateVmInstanceEvent":{"success":false,"apiId":"9ebc212
f00ea45bbaa91e1e420230921","headers":{"schema":{}},"error":{"code":"SYS.1006
","cause":{"code":"HOST.1005","description":"Failed to start vm on hypervisor","details
":"failed to start vm[uuid:2da983e8b5a34a459bb71a0d705b0bba name:vm-qge5] on kvm
 host[uuid:b7a14605c6b042e0b2da17ae329ea70a, ip:10.79.186.30], because Traceba
ck (most recent call last):\n File \"/var/lib/zstack/virtualenv/kvm/lib/python2.7/site-package
s/kvmagent/plugins/vm_plugin.py\", line 2721, in start_vm\n self._start_vm(cmd)\n File
 \"/var/lib/zstack/virtualenv/kvm/lib/python2.7/site-packages/kvmagent/plugins/vm_plug
in.py\", line 2664, in _start_vm\n 'unable to start vm[uuid:%s, name:%s], libvirt error: %s
' % (cmd.vmInstanceUuid, cmd.vmName, str(e)))\nKvmError: unable to start vm[uuid
:2da983e8b5a34a459bb71a0d705b0bba, name:vm-qge5], libvirt error: internal error:
 early end of file from monitor, possible problem: 2017-03-12T10:49:18.661399Z qemu
-kvm: -drive file=rbd:pri-v-r-a5486c5605a8499dbe3ca79ee3ca87c4/a28d86db519c48
ef9e4c50a3f8e27305:id=zstack:key=AQD4HsVYwfgaMBAAxBNUtDw1wzhitURDrUM
M9g==:auth_supported=cephx\\;none:mon_host=10.79.186.112\\:6789,format=raw,if
=none,id=drive-virtio-disk0: error reading header from a28d86db519c48ef9e4c50a3f8e2
7305: Function not implemented\n"},"description":"An operation failed","details":"failed
 to start vm[uuid:2da983e8b5a34a459bb71a0d705b0bba name:vm-qge5] on kvm host
[uuid:b7a14605c6b042e0b2da17ae329ea70a, ip:10.79.186.30], because Traceback
 (most recent call last):\n File \"/var/lib/zstack/virtualenv/kvm/lib/python2.7/site-package
s/kvmagent/plugins/vm_plugin.py\", line 2721, in start_vm\n self._start_vm(cmd)\n File
 \"/var/lib/zstack/virtualenv/kvm/lib/python2.7/site-packages/kvmagent/plugins/vm_plug
in.py\", line 2664, in _start_vm\n 'unable to start vm[uuid:%s, name:%s], libvirt error: %s
' % (cmd.vmInstanceUuid, cmd.vmName, str(e)))\nKvmError: unable to start vm[uuid
:2da983e8b5a34a459bb71a0d705b0bba, name:vm-qge5], libvirt error: internal error:
 early end of file from monitor, possible problem: 2017-03-12T10:49:18.661399Z qemu
-kvm: -drive file=rbd:pri-v-r-a5486c5605a8499dbe3ca79ee3ca87c4/a28d86db519c48
ef9e4c50a3f8e27305:id=zstack:key=AQD4HsVYwfgaMBAAxBNUtDw1wzhitURDrUMM9g
==:auth_supported=cephx\\;none:mon_host=10.79.186.112\\:6789,format=raw,if=none
,id=drive-virtio-disk0: error reading header from a28d86db519c48ef9e4c50a3f8e27305:
```

```
 Function not implemented\n"},"createdTime":1489315754576,"type":{"_name":"key.event
.API.API_EVENT"},"id":"bb86a69de1c04043a9ae218ee510dae0"}}
```

- **原因**：

  rbd无法读取镜像文件头文件，很可能是Ceph存储本身的问题。

  ZStack定制版ISO的qemu-kvm 2.6.0安装时默认带**librbd 0.94**客户端。如果用户部署了Ceph**10.2.x**或着**12.2.x**，librbd老版本客户端不支持新版本的后端。

- **解决方案**：

  用户需在计算节点上手动安装或升级与所部署Ceph版本对应的librbd客户端包。

23.

Q：升级时，遇到ZStack定制版ISO版本不匹配怎么办？

A：

- **现象**：

  升级时遇到ZStack定制版ISO版本不匹配，会提示以下错误信息：

```
Reason: The current local repo is not suitable for ZStack installation.
Please download ZStack-x86_64-DVD-3.1.1-c74.iso from http://www.zstack.io/
product_downloads/ and run
#wget http://cdn.zstack.io/product_downloads/scripts/zstack-upgrade
#bash zstack-upgrade ZStack-x86_64-DVD-3.1.1-c74.iso
For more information, see http://www.zstack.io/support/tutorials/upgrade/
```

- **原因**:

  当前系统使用的ISO版本不适合升级此安装包，需要升级对应的ISO才可继续升级ZStack。

- **解决方案**：

  请执行以下部署：

  1. 执行如下命令，下载最新的升级脚本

     ```
     wget http://cdn.zstack.io/product_downloads/scripts/zstack-upgrade
     ```

  2. 执行如下命令，在管理节点下载最新的ISO：

     ```
     wget http://cdn.zstack.io/product_downloads/iso/ZStack-x86_64-DVD-3.1.1-c74.iso
     ```

  3. 执行升级，升级ISO里面的yum repo同步到本地，并且直接升级管理节点：

     ```
     bash zstack-upgrade ZStack-x86_64-DVD-3.1.1-c74.iso
     ```

24.

Q：ZStack版本升级时出现报错`The Operating System version is not suitable for zstack-enterprise installation.`怎么办?

A：请使用最新的*ZStack定制版ISO*安装升级。

25.

Q：升级ZStack过程中，因为二次开发或者调整数据库导致升级失败时，怎么恢复原本的ZStack？

A：

- **前提**：

  ZStack进行升级时，默认会备份当前ZStack核心文件和数据库到对应目录。

- **恢复步骤**：

  1. 备份之前版本的ZStack核心文件：

     ```
     cp /usr/local/zstack/upgrade/2017-11-09-15-41-52 /root -r
     ```

  2. 备份之前版本的数据库：

     ```
     cp /usr/local/zstack/db_backup/2017-11-09-15-42-43/backup.sql /root
     ```

  3. 再次备份数据库：

     ```
     zstack-ctl dump_mysql
     ```

  4. 删除当前ZStack环境：

     ```
     zstack-ctl stop
     rm -rf /usr/local/zstack
     ```

  5. 使用之前的安装包直接安装ZStack：

     ```
     bash ZStack-installer-3.1.1.bin -D
     ```

  6. 使用第一步备份的ZStack核心文件恢复：

     ```
     zstack-ctl stop
     cd /root/2017-11-09-15-41-52/zstack/
     mv /usr/local/zstack/apache-tomcat/webapps/zstack /usr/local/zstack/apache-tomcat/
     webapps/zstack-bk
     cp /root/2017-11-09-15-41-52/zstack /usr/local/zstack/apache-tomcat/webapps  -r
     chown zstack:zstack /usr/local/zstack/apache-tomcat/webapps/zstack -R
     ```

  7. 恢复第二步备份的数据库：

     ```
     cat /root/backup.sql |mysql -u root -p zstack.mysql.password zstack
     ```

  8. 启动ZStack管理节点服务，此时ZStack已成功恢复至原本升级失败前的版本

     ```
     zstack-ctl start
     ```

26.

Q：如何在温和情况下关闭swap分区？

A：依次执行如下命令：

```
sysctl -w vm.swappiness=0
echo "vm.swappiness = 0">> /etc/sysctl.conf
```

27. Q：如何修改管理节点IP地址？

    A：

    1. 执行命令zstack-ctl chang_ip --ip X.X.X.X更改管理节点IP
    2. 执行命令zstack-ctlrestart_node重启管理节点

28. Q：管理节点无法启动，重启提示没有可用空间，该如何处理？

    A：确认监控数据不需要的情况下，删除prometueus监控数据释放空间，依次执行如下命令：

```
[root@hostname ~]# zstack-ctl stop
[root@hostname ~]# ps -ef |grep prometheus
[root@hostname ~]# kill  -9 prometheus_pid
[root@hostname ~]# rm -rf /var/lib/zstack/prometheus/data
[root@hostname ~]# zstack-ctl start
```

29. Q：使用非官方ZStack安装计算节点，添加失败是什么原因？

    A：不支持使用非官方ISO安装计算节点，请使用ZStack定制版ISO安装。

30. Q：如何设置root密码？

    A：执行命令zstack-ctl reset_password 更改root账户的密码。如果不设置，密码默认为password

21.3 系统登录

1. Q：ZStack支持哪些浏览器？

   A：支持Chrome和Firefox浏览器。

2. Q：UI无法登录怎么办？

   A：请根据以下方法进行检查：

   1. 如果提示用户名/密码不正确，需要输入正确的用户名和密码。

2. 如果提示无法连接管理节点，需要通过zstack-ctl status命令确认管理节点服务是否运行正常。
3. 如果依然无法连接，可以使用如下命令，通过*cli*方式登录：

```
[root@localhost ~]# zstack-cli  #进入cli命令
admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
```

4. 检查相关的Java进程是否出现僵尸导致程序无法运行，此时需要重启管理节点机器。

3. Q：如何更改UI的Admin密码？

   A：有两种方法：

   - **UI方式**：

     在ZStack**首页**点击Admin信息的**修改密码**按钮进行修改。

   - **命令行方式**：

     依次执行以下命令：

```
[root@localhost ~]# zstack-cli  #进入cli命令
admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
admin>>> zstack-cli UpdateAccount uuid=36c27e8ff05c4780bf6d2fa65700f22e password=NEW_PASSWORD #修改密码（NEW_PASSWORD为新密码）
```

4. Q：如何修改UI界面默认的5000端口？

   A：依次执行以下命令：

```
[root@localhost ~]# zstack-ctl config_ui --server-port 8888  #修改UI服务端口为8888
[root@localhost ~]# zstack-ctl config_ui --webhook-port 8888  #改webhook主机端口，与UI服务端口保持一致
[root@localhost ~]# zstack-ctl stop_ui  #停止UI服务
[root@localhost ~]# zstack-ctl start_ui  #启动UI服务
```

5. Q：如何增加会话超时时间？

   A：

   - **UI方式**：

     在**设置** > **全局设置** > **基本设置**页面，调整**会话超时时间**。

   - **命令行方式**：

依次执行如下命令：

```
[root@localhost ~]# zstack-cli  #进入cli命令
admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
admin>>> zstack-cli UpdateGlobalConfig name=session.timeout category=identity value =720000 #将登录的过期时间改成200小时
```

6. Q：如何更改ZStack同时登录次数？

   A：

   - **UI方式**：

     在**设置** > **全局设置** > **高级设置**页面，修改**最大会话数**的值。

   - **命令行方式**

     1. 首先使用QueryGlobalConfig name~=session，可以看到关于最大会话数的限制为500。

        ```
        {
                "category": "identity",
                "defaultValue": "500",
                "description": "Max number of sessions management server accepts. \
        When this limit met, new session will be rejected",
                "name": "session.maxConcurrent",
                "value": "500"
        }
        ```

     2. 假如希望改成1000，可执行以下命令：

        ```
        UpdateGlobalConfig category=identity name="session.maxConcurrent" value=1000
        ```

7. Q：是否支持HTTPS方式登录UI？

   A：支持。以下介绍使用系统默认证书以HTTPS方式登录UI的方法：

   1. 在管理节点停止管理节点服务，执行：

      ```
      zstack-ctl stop
      ```

   2. 在管理节点配置证书，执行：

      ```
      openssl pkcs12 -in /usr/local/zstack/zstack-ui/ui.keystore.p12 -out /usr/local/zstack/zstack-ui/ui.keystore.pem -nodes
      ```

      注: 执行过程中要求输入默认密码：**password**

   3. 修改**zstack.properties**配置文件，将证书路径设置为绝对路径：

进入*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties*，添加一行记录：`consoleProxyCertFile = /usr/local/zstack/zstack-ui/ui.keystore.pem`

4. 配置HTTPS UI登录模式：

```
zstack-ctl config_ui --enable-ssl True
```

5. 启动管理节点管理服务，执行：

```
zstack-ctl start
```

8. Q：如何取消HTTPS方式，恢复HTTP方式登录UI？

   A：如需取消HTTPS登录，执行：

```
zstack-ctl config_ui --enable-ssl False
```

   并重启管理节点服务：

```
zstack-ctl stop_ui
zstack-ctl start_ui
```

21.4 云资源池

云主机

1. Q：如何检查一台云主机是否支持硬件虚拟化？

   A：在终端中执行egrep "vmx|svm" /proc/cpuinfo命令，如果有输出代表支持硬件虚拟化。

2. Q：ZStack的DHCP服务和目前机房的DHCP是否会出现冲突？

   A：ZStack的DHCP服务与目前机房已经配置的DHCP服务不冲突。但ZStack里面的云主机使用的网络段不可与当前环境内已经使用的IP范围重叠，如果发生重叠，可能发生IP地址冲突。

3. Q：如果扁平网络创建云主机时不设置云主机hostname，默认hostname是什么？

   A：如果镜像里原本的hostname是localhost，DHCP会主动将hostname修改成与IP地址相关。例如：云主机IP地址为*192.168.12.3*，那么云主机hostnme会变成**192-168-12-3**。

4. Q：*zstack-cli*里面设置扁平网络的hostname为何不生效？

   A：如果镜像里面原本的hostname不是localhost，那么DHCP将不会分配新的hostname，而是使用原本的hostname。

5. Q：如何修改控制台代理地址？

   A：

   - **UI方式**：

     在**平台管理** > **控制台代理**页面，设置控制台代理地址。无需重启管理节点，直接生效。

   - **命令行方式**：

     依次执行以下命令（MANAGEMENT_NODE_PUBLIC_IP_ADDRESS为控制台代理IP）：

     ```
     [root@localhost ~]# zstack-ctl configure consoleProxyOverriddenIp=MANAGEM
     ENT_NODE_PUBLIC_IP_ADDRESS
     [root@localhost ~]# zstack-ctl restart_node
     ```

6. Q：如何通过管理节点的公网IP连接内网IP上云主机的控制台？

   A：修改控制控制台代理地址即可，方法同上。

7. Q：控制台代理出现"description": "Cannot do an IO operation(e.g. network IO error, file IO error)"报错如何处理？

   A：

   - **现象**：

     ```
     "description": "Cannot do an IO operation(e.g. network IO error, file IO error)",
     "details": "I/O error on POST request for \"http://127.0.0.1:7758/console/establish\":\
     Connect to 127.0.0.1:7758 [/127.0.0.1] failed: Connection refused;
     nested exception is org.apache.http.conn.HttpHostConnectException: Connect to 127.0.0
     .1:7758 [/127.0.0.1] \
     failed: Connection refused","$$hashKey": "object:1344"
     ```

   - **解决方案**：

     删除*/var/lib/zstack/pickledb/*下面的*consoleProxy*文件，再次重连控制台代理。

8. Q：怎么从IP Range中保留一个IP地址，不让ZStack分配给云主机？

   A：

   - 目前还没有提供ReserverIpRange的API，如果希望ZStack从已经设置的IP Range中保留几个特定的IP地址，可以在UI界面创建指定的虚拟IP方式来保留IP使用。
   - 也可以用CreateVip这个API。

例如：使用如下命令把*a.b.c.d*的IP地址从指定的L3网络上用创建虚拟IP的方式保留：

```
[root@localhost ~]# zstack-cli  #进入cli命令
admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
admin>>> zstack-cli CreateVip l3NetworkUuid=YOU_L3_NETWORK_UUID name=for_reserver requiredIp=a.b.c.d
```

9.

Q：如何批量修改一批云主机的计算规格？

A：可通过UI和cli命令行两种方式进行修改：

- **UI方式**：

  在**云资源池** > **云主机**页面，同时选中多个云主机，点击**更多操作** > **修改计算规格**按钮，选择合适的计算规格进行修改。

- **命令行方式**：

  采用shell脚本配合*zstack-cli*命令进行批量修改，例如：将一批名字里包含Win7的云主机的计算规格全部修改为名字是Win7-Instance-Offering的计算规格

```
which jq || (echo "you need to install jq" && exit 1)
zstack-cli LogInByAccount accountName=admin password=password instance_offering_uuid=zstack-cli \
QueryInstanceOffering name=Win7-Instance-Offering |jq '.["inventories"][0].uuid' target_vms=zstack-cli zstack-cli \
QueryVmInstance name~=Win7|jq '.["inventories"][].uuid' for vm in $target_vms; do zstack-cli ChangeInstanceOffering \
instanceOfferingUuid=$instance_offering_uuid vmInstanceUuid=$vm echo "change vm: $vm instance offering to \
$instance_offering_uuid" zstack-cli StopVmInstance uuid=$vm zstack-cli StartVmInstance uuid=$vm done zstack-cli LogOut
```

10.

Q：如何解决qemu版本不匹配的问题？

A：

- **现象**：

  使用过程中，启动云主机时可能遇到类似这样的错误信息：

```
uses a qcow2 feature which is not supported by this qemu version: QCOW version 3
```

- **原因**：

  主要原因是qcow版本不一致。原始的qcow2创建版本使用的qemu-img为较新版本，现在创建时使用的为较旧版本，旧版本不支持新版本。

- **解决方案**：

在拥有较新版本的qemu-img里面进行兼容性转换，例如执行以下命令进行转换，转换完毕后，再重新添加镜像：

```
qemu-img convert -o compat=0.10 -f qcow2 -O qcow2 centos6-cloud-init.qcow2 centos-st
-ssh-key.qcow2
```

11.
Q：ZStack给云主机的MAC地址，可以手动修改吗？

A：可以。ZStack支持停止状态的云主机修改MAC地址。

12.
Q：ZStack如何修改云主机网卡的MAC地址?

A：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。

13.
Q：机房准备断电维护，上电后如何自动恢复云主机的业务？

A：可参考以下步骤：

1. 设置全部云主机高可用为**NeverStop**模式。
2. 全部物理主机进入维护模式。
3. 断电维护。
4. 上电后，物理主机启用，所有的云主机会自动恢复运行。

14.
Q：云主机卸载L3网络，并重新加载后，云主机的IP地址会发生变化吗？

A：在DHCP情况下会随机重新分配IP。

15.
Q：如何修改云主机的删除时延？

A：

- **UI方式**：

  在**设置** > **全局设置** > **基本设置**页面，修改**彻底删除时延**的值。

- **命令行方式**：

  依次执行以下命令：

```
[root@localhost ~]# zstack-cli  #进入cli命令
admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
```

```
admin>>> UpdateGlobalConfig category=vm name=expungePeriod value=3600  #将彻底删除时延设置成3600秒
```

16.
Q：ZStack能为已经运行的云主机加载或卸载ISO吗？

A：可以。在**云主机**页面，选中一个运行中的云主机，点击**更多操作**，选择加载/卸载ISO。

17.
Q：如何在一个VM上添加多块网卡？

A：

- **现象**：

  创建VM时，可能会遇到一个云主机挂载多个网络的情况，这时进入console可看到多块网卡，但没有发现IP。

- **原因**：

  每个网络对VM来说就是一块网卡，把网络加载到VM上，等价于把一块物理网卡插到一台Server上。因此使用 *ifconfig*命令就能看到eth设备了。如果没有看到IP，说明网卡插上了，但并没有配置好。

- **解决方案**：

  请仿照eth0的配置文件，为这个新网卡创建一个配置文件：

  1. 拷贝一份eth0：（以下示例是Centos 7.2环境，其他版本Linux路径和文件可能有变化）

     ```
     # 将配置文件中的eth0替换为eth1,并删除其中的uuid信息
     cp /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth1
     sed -i 's/eth0/eth1/g' ifcfg-eth0
     sed -i '/UUID*/d' /etc/sysconfig/network-scripts/ifcfg-eth1
     ```

  2. 将网络重启生效：

     ```
     /etc/init.d/network restart
     ```

  3. 用ifconfig查看，第二块网卡也有IP了。如果在云主机上挂载多个网络，重复以上操作即可。

18.
Q：如何将KVM上的云主机迁移到ZStack中？

A：

1. 通过libvirt导出云主机的镜像（.qcow2文件）。
2. 将镜像上传至一个http服务器中。
3. 使用ZStack镜像服务器导入镜像。

4. 通过镜像创建云主机。

注:

如果原来的云主机挂载了数据云盘，如何将数据云盘也迁移过来呢?

- **方法一**：

  与上述操作类似，需要先将数据盘生成镜像，同理导入，ZStack使用该镜像创建数据云盘，再将数据云盘挂载到云主机即可。

- **方法二**:

  先在ZStack中创建一个相同大小的数据云盘，找到对应的路径，将原云盘数据直接复制到新的路径下，最后再挂载到云主机上。

19.

Q：ZStack如何设置云主机启动顺序？

A：在**云资源池** > **云主机**页面，选择云主机名称，点击**更多操作** > **设置启动顺序**，选择需要的启动顺序。

20.

Q：如何在创建云主机时指定静态IP？

A：大多数情况下，云主机的IP地址由DHCP自动分配。对于需要静态IP的用户，可以使用以下方式来设置：

- **UI方式**：

  停止云主机，进入云主机详情页，在**配置信息**页面选中云主机挂载的某网卡点击**操作** > **设置静态IP**。

- **命令行方式**：

  - 可使用SetVmStaticIp来设置：

    ```
    SetVmStaticIp vmInstanceUuid=7c4162e8d32d4bea8f7e799024c6b735
    l3NetworkUuid=4d855bb0c72640f5a643ba8e88ae85df ip=10.141.13.85
    ```

  - 可使用systemTags=staticIp来设置：

    1. 开启DHCP服务（云路由网络或扁平网络都可以）。
    2. 执行以下命令：

    ```
    CreateVmInstance name=ceph-3
    instanceOfferingUuid=7ec8f1148f14452aa359607112ce7bbe
    l3NetworkUuids=f749ec8b1ea94676bda7a5968de6b947
    imageUuid=b6ebcfa021e24bc3b08a27216fd589a7
    ```

```
systemTags=staticIp::f749ec8b1ea94676bda7a5968de6b947::172.20.58.3
```

21.

Q：修改Windows云主机密码报错怎么办？

A：

- **现象**：

  修改Windows云主机密码时出现如下报错：

  ```
  return code: 1 stdout: stderr: error: internal error: unable to execute QEMU agent
   command 'guest-set-user-password':
  The command guest-set-user-password has not been found
  ```

- **原因**：

  可能原因是使用了错误的Windows Virtio驱动。

  解决方案：

  目前ZStack定制版ISO里已经集成了可用的Windows Virtio驱动，解压此ISO，添加此Windows Virtio驱动作为ISO镜像到镜像服务器中，然后挂载此ISO，安装对应的qemu-guest-agent即可。

22.

Q：误删除ssh key，如何恢复？

A：ssh key默认存放在目录：*/usr/local/zstack/apache-tomcat-7.0.35/webapps/zstack/WEB-INF/classes/ansible/rsaKeys*，如果用户不小心删除了ssh key，可以通过以下方式恢复：

1. 首先运行以下命令生成ssh key：

   ```
   ssh-keygen -f /usr/local/zstack/apache-tomcat-7.0.35/webapps/zstack/WEB-INF/classes/
   ansible/rsaKeys/id_rsa -N ''
   ```

2. 生成ssh key后，运行以下命令确保用户有权限访问：

   ```
   chown -R zstack.zstack /usr/local/zstack/apache-tomcat-7.0.35/webapps/zstack/WEB-
   INF/classes/ansible/rsaKeys
   ```

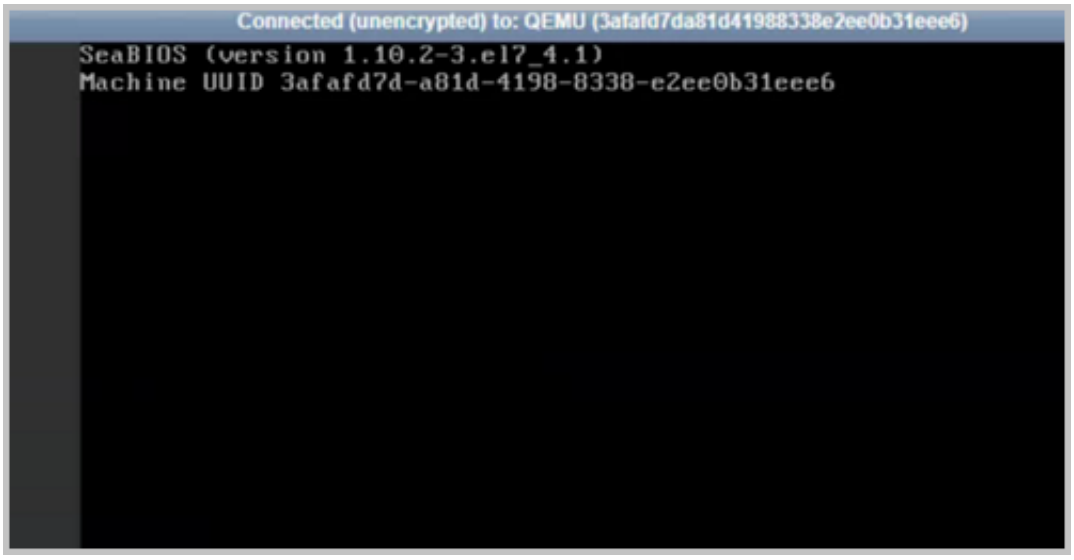
23.

Q：云主机控制台出现**Guest has not initialized the display (yet)**怎么办？

A：

- **现象及原因**：

  使用旧的服务器作为计算节点，可能会遇到因CPU型号过早，无法创建云主机或者创建的云主机不能显示console界面的问题，如下图所示：



- **解决方案**：

  出现这种情况，可以尝试如下设置：

  1. kvm-nested.conf里面第一行加上`ept=0`，如：

     ```
     options kvm_intel nested=1 ept=0
     #vim /etc/modprobe.d/kvm-nested.conf
     ```

  2. 关闭运行状态的VM，然后移除kvm_intel：

     ```
     #rmmod kvm_intel
     ```

  3. 最后重新加载kvm_intel：

     ```
     #modprobe kvm-intel ept=0 unrestricted_guest=0
     ```

24.

Q：CPU型号与Passthrough（支持嵌套虚拟化）的说明。

A：可使用以下方式设置云主机CPU模式：

- **UI方式**：

  在**设置** > **全局设置** > **高级设置**页面，修改**云主机CPU模式**的值为**host-model**。

- **命令行方式**：

  使用如下命令：

```
[root@localhost ~]# zstack-cli  #进入cli命令
admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
admin>>> UpdateGlobalConfig category=kvm name=vm.cpuMode value=host-model
```

三种云主机CPU模式：

- **none**：CPU型号为QEMU模拟器
- **host-model**：CPU类型为物理主机CPU类型
- **host-passthrough**：CPU型号跟物理主机CPU完全一样

注:

- 当模式为**host-model**和**host-passthrough**时，云主机可以获得嵌套虚拟化功能。
- 使用该功能可能会影响云主机热迁移。因为热迁移时会检查云主机CPU型号，如果两台物理主机的CPU型号不同，会导致云主机热迁移失败。

25.

Q：什么情况下云主机会变成**Paused**状态？

A：云主机内存过低时，创建或迁移云主机可能变成**Paused**状态。

26.

Q：出现这个IO报错这么处理？

A：

- **现象**：

  报错如下：

```
"description": "Cannot do an IO operation(e.g. network IO error, file IO error)", "details": "I/O error on POST request for \"http://127.0.0.1:7758/console/establish\": Connect to 127.0.0.1:7758 [/127.0.0.1] failed: Connection refused; nested exception is org.apache.http.conn.HttpHostConnectException: Connect to 127.0.0.1:7758 [/127.0.0.1] failed: Connection refused","$$hashKey": "object:1344"
```

- **解决方案**：

删除*zstack/pickledb/*下面的consoleProxy文件，且重连控制台代理生效。

27.

Q：为什么同一个网络段之间的云主机相互之间*ping*不通？

A：如果本物理主机上的云主机 IP互通，而且云主机所在网卡的物理主机之间也互通，应该是跨物理主机的云主机之间不通，很可能交换机出现问题。

28.

Q：如果网内没有自建DNS服务器，云主机怎么才能使用电信的DNS服务器IP地址来解析域名上网？

A：请在创建网络时指定DNS地址。

29.

Q：进行云主机相关操作时提示**libvirt error**如何解决？

A：

- **现象**：

  用户在进行云主机相关操作时，可能会遇到如下错误提示：

  ```
  libvirt error: error from service: ListActivatableNames: Connection is closed
  ```

  或

  ```
  libvirt error: Activation of org.freedesktop.machine1 timed out
  ```

- **原因**：

  这类错误通常是由系统DBUS进程死掉或者DBUS运行异常引起的。

- **解决办法**：

  方法1 ：重启物理主机，DBUS会自动恢复

  方法2 ：在物理主机上使用如下命令：

  ```
  service systemd-machined restart
  service libvirtd restart
  ```

  完成后用UI或者CLI重连出问题的物理主机。

30.

Q：云主机迁移失败的原因是什么？

A：

- **现象**：

```
{
  "error": {
    "code": "HOST.1009",
    "description": "Failed to migrate vm on hypervisor",
    "details": "failed to migrate vm[uuid:90bb61f55e774f5f89c9e1ea46db7661] from kvm
 host[uuid:e5105c61114a4efe8bcc025f744226bd, ip:10.0.247.244] to dest host[ip:10.0
.197.238], unable to migrate vm[uuid:90bb61f55e774f5f89c9e1ea46db7661] to qemu+tcp
://10.0.197.238/system, internal error: Attempt to migrate guest to the same host localhost
.domain.com"
  },
  "createdTime": 1488170137857,
  "type": {
    "_name": "key.event.API.API_EVENT"
  },
  "id": "e6bcd7c33ad9446b919e11cd647fc8dc"
}
```

- **原因**：

  出现这段错误是因为两台物理主机hostname相同，KVM云主机在线迁移目前依靠hostname进行确认不同的物理主机，如果hostname相同，则会被认定为相同的物理主机。

- **解决方案**：

  需确保物理主机的hostname不能相同。可以通过`hostnamectl set-hostname your_new_hostname`来设定。

31.

Q：为什么有的云主机关机时间比较久？

A：

- **原因**：

  这种情况一般出现在Guest OS为Linux的云主机上，这是因为缺少ACPID服务（用于处理电源相关事件的守护进程）。KVM云主机安装Linux系统默认是没有安装ACPID服务的，所以不会做处理，关机一分钟后被ZStack杀掉云主机进程强行关闭。

- **解决方案**：

  对于这种情况，只需在云主机里安装和启动ACPID服务即可，执行命令如下：

```
[root@kvm_client_00 ~]# yum install acpid -y
# 重新启动ACPID服务，安装后默认加入到开机启动。
[root@kvm_client_00 ~]# /etc/init.d/acpid restart
```

32.

Q：云主机高可用有哪几个阶段？

A：高可用状态的云主机失败重启涉及以下流程：

- 通过轮询、触发等机制检测云主机状态，如果确定云主机已停止，那么设置NeverStop的云主机将直接自动重启。
- 通过轮询、触发等机制检测云主机状态，如果不能确定云主机状态，将根据以下步骤进行检测：
  1. 根据已有网络配置，选择最精准的方法探测云主机所在的物理机的状态
  2. 如果物理机状态异常，设置NeverStop的云主机将尝试自动重启。

33.

Q：对于Ubuntu系统的云主机，当用户使用apt-get install qemu-guest在线安装qemu-ga时，安装完成后qemu-ga版本为2.0（版本过低），如何解决？

A：

1. 在Ubuntu依赖库官网搜索Ubuntu 16.04的qemu-ga版本，下载2.5版本的qemu-ga离线deb包：

   https://ubuntu.pkgs.org/16.04/ubuntu-universe-amd64/qemu-guest-agent_2.5+dfsg-5ubuntu10_amd64.deb.html

2. 安装2.5版本的qemu-ga离线deb包：

```
dpkg -i <package.deb>
  //<package.deb>
为下载的2.5版本的qemu-ga离线deb包
```

3. 在页面修改密码，无报错，修改完成。

34.

Q：ZStack云平台创建云主机失败的原因可能有哪些？

A：

- 镜导致找不到可用的物理机，主存储需挂载集群
- 集群内没有可用的物理机满像服务器失联，检查镜像服务器可用并确保连接
- 主存储未挂载集群，足计算规格的定义，需确保物理机可用，且资源满足
- 主存储容量不足以提供镜像需要的虚拟容量，需确保主存储容量充足
- 集群未挂载相应的网络，需确保集群已挂载对应的网络
- IP地址池资源不足，需确保IP范围充足
- 确保物理机的分布式DHCP服务dnsmasq服务正常，以正常提供DHCP IP分配服务
- 确保物理机的Libvirtd服务正常，以正常提供虚拟化服务

- 如果云主机一直处于启动中，需要检查使用此云主机的镜像是否巨大，镜像缓存的下载是否需要耗时很久。如果镜像缓存存在，需继续检查物理机的*/var/log/zstack/zstack-kvmagent.log*

35.
Q：云主机时间和物理时间不同步怎么调整？

A：执行命令timedatectl set-timezone Asia/Shanghai修改时区

36.
Q：云主机支持系统盘扩容吗？

A：支持。可使用LVM分区工具针对xfs+swap分区扩容。

37.
Q：GPU透传识别不到设备怎么解决？

A：

- 检查GPU是否在黑名单上
- lspci -s xx:xx -v检查GPU驱动信息，是否被物理机使用
- 启用物理机IOMMU，BIOS中打开Intel VT-d或AMD IOMMU选项

38.
Q：可以在创建云主机的时候设置账号和密码吗？

A：可以在创建云主机的时候通过Userdata注入到云主机来实现设置账户和密码，示例步骤如下：

1. 在云平台创建云主机，输入云主机名称
2. 选择计算规格、镜像、网络，镜像应选择已预装cloud-init的镜像
3. 点击**高级**，在**Userdata**栏中注入账户名和密码等信息
4. 点击**确定**按钮创建云主机

```
userdata注入示例：
#cloud-config
users:
- name: test
  shell: /bin/bash
  groups: root
  sudo: ['ALL=(ALL) NOPASSWD:ALL']
  ssh-authorized-keys:
     - ssh-rsa AAAAB3NzaC1LXCJfjroD1lTroot@10-0-0-18
bootcmd:
- echo 192.168.1.130 us.archive.ubuntu.com>> /etc/hosts
- mkdir /tmp/temp
write_files:
- path: /tmp/ZStack_config
  content: |
     Hello,world!
hostname: carl-test
disable_root: false
```

```
ssh_pwauth: yes
chpasswd:
  list: |
     root:123456
  expire: False
runcmd:
- curl http://soft.vpser.net/lnmp/lnmp1.4.tar.gz -o lnmp1.4.tar.gz&& tar zxf lnmp1.4.tar.gz &&
 cd lnmp1.4 && echo""|./install.sh lnmp
```

镜像

1.

Q：创建镜像的占用空间是怎样的？

A：

- 举例说明：一个host有800G的空间，创建了一个VM 400G，假定文件是A，然后创建了一镜像B，镜像B会上传到镜像服务器，这时镜像B的实际大小应该不是400G，比如只有10G。
- 用镜像B来创建一个新的VM C的时候，镜像B会从镜像服务器上下载到host上的一个cache目录。这个下载会消耗主存储的空间，等到下载成功，host的虚拟可用容量就小于400G了，这样创建VM C就失败了。

2.

Q：创建镜像时提示URL相关错误一般有哪些方法？

A：

- ZStack允许输入的URL格式为：
  - 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:

- 建议用户创建一个http服务器来下载镜像。
- 如果使用本地镜像，注意file后必须为绝对路径。

3.

Q：添加镜像超时怎么办？

A：

- **原因**：

  下载镜像时，有时因为镜像过大或者网络等原因导致镜像下载太慢超时报错。

- **解决方案**：

  如果执行了下载操作，就会在镜像服务器上启用http服务。当UI上显示超时，甚至关闭管理节点时（镜像服务器不在管理节点所在的host），并不影响服务继续运行。

  因此，如果时间过长不用担心。后台会自动下载完成，下次继续添加该镜像时会迅速完成。

4.

Q：出现cannot acquire state change lock的错误怎么办？

A：

- **原因**：

  出现这个错误属于小概率事件，是由libvirt引发的。出现这个问题后，该云主机上的后续操作只要调用到libvirtd就会失败。

- **解决办法**：

```
killall -9 libvirtd
# rm /var/run/libvirtd.pid
```

  完成后重连物理主机。

5.

Q：Windows内存监控没有数据如何解决？

A：PCI设备驱动（安装后叫VirtIO Balloon Driver）安装后，可能出现无法通过qemu获取内存信息的问题，解决方法如下：

1. 加载windows-virtio-driver的ISO镜像。
2. 以64位Windows 2012操作系统为例：将驱动文件夹*X:\Balloon\2k12R2\amd64*目录下的**BLNSVR.EXE**文件拷贝到*C:\Windows\System32*目录下。
3. 以管理员方式打开命令行程序并执行BLNSVR -I命令。

6. Q：封装Windows系统模板时，无法识别Virtio驱动怎么办？

   A：

   - **现象**：在安装过程中，无法识别ISO中加载的Virtio驱动，导致无法看到已加载的系统云盘。
   - **原因**：有可能所用的Windows ISO光盘不是从微软官方下载的，可能是通过其他工具后期定制的。
   - **解决方案**：使用官方直接下载的ISO。

7. Q：Windows virtio ISO的镜像在哪里可以找到？

   A：管理节点*/opt/zstack-dvd*目录，内置*zstack-windows-virtio-driver-2.1.iso*镜像

8. Q：如何设置单个云主机的写缓存？

   A：写缓存模式属于全局设置参数，修改后重启生效。如果需要为单个云主机设置写缓存，可以先修改缓存模式再创建云主机，再还原原来的缓存模式

9. Q：raw格式和qcow2的镜像格式区别是什么?

   A：

   - raw ：裸格式，创建时就需要指定存储容量，占用全部容量，不支持动态扩容，不支持快照，性能好
   - qcow2：quick copy on write 2, 写时复制，开始只占用少许容量，支持动态扩容，支持压缩，支持AES加密，支持快照，性能较好

云盘

1. Q：云盘可以建立在共享存储上，且可以进行任意挂载吗？

   A：ZStack可以给一个区域内不同集群添加不同主存储，主存储可以是本地存储也可以是共享存储。

- 如果主存储为共享存储，则云盘创建在共享存储上，云盘和物理主机无关 ，可以挂载到任意物理节点的云主机上。即：云盘的挂载不受物理主机的相关约束，而且不支持云盘迁移。
- 如果主存储为本地存储，挂载一个卸载过的云盘时，需要保证该云盘和目标云主机在相同的物理主机上。如果该云盘和目标云主机不在相同的物理主机上，需要将云盘和云主机迁移到相同的物理主机上。可以选择迁移云主机（需要首先停止云主机），也可以选择迁移云盘。

2.

Q：云主机上挂载新的L3网络时，为何只显示一个？

A：

- 动态挂载只是Qemu给云主机一个虚拟网卡，使用lspci可以看到此网卡，但是云主机的操作系统使用时，需要手动执行dhclient获取。
- 也可参考云主机里的 */etc/sysconfig/network-scripts/ifcfg-eth0*，对新增的eth1重新设置，再重启网络服务即可看到多网络路由。

3.

Q：QueryVolume actualSize为什么和实际文件大小不一致？

A：随着磁盘使用过程，这个**actualsize**可能会不断增加。

- **UI方式**：

  在**云资源池** > **云盘**页面，展开某一云盘详情页，然后点击**真实容量**后面的刷新按钮进行同步。

- **命令行方式**：

```
[root@localhost ~]# zstack-cli  #进入cli命令
admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
admin>>> SyncVolumeSize uuid=   #同步真实容量。需填写云主机UUID
```

4.

Q：云主机磁盘写满，无法启动怎么办？

A：可以扩大磁盘后启动，建议先备份镜像。

5.

Q：本地存储如何迁移云盘？

A：使用本地存储的用户，可使用如下方法迁移云盘：

在**云资源池** > **云盘**页面，选中待迁移的云盘，点击**更多操作** > **迁移**按钮，选择目标物理主机即可。

6.

Q：Windows安装Virtio驱动时，磁盘应该选择哪个驱动？

A：安装viostor存储控制器和vioscsi磁盘控制器。

7. Q：数据云盘是建立在主存储还是镜像服务器上？为什么建立的数据云盘在Windows上发现不了？

   A：数据云盘是建立在主存储上，需要在云主机里安装Virtio驱动。

8. Q：ZStack基于模版创建云主机，可否实现**母盘+增量盘**的模式？

   A：ZStack采用增量盘的模式。镜像从镜像服务器下发到主存储作为镜像缓存，以此为base创建云主机。这些云主机均使用同一base。

9. Q：加载云盘后修改Linux云主机的*/etc/fstab*文件，对该云主机在线创建镜像，使用该镜像创建其它云主机时，所创建的云主机会hang住无法启动，如何解决？

   A：

   - **原因**：

     云主机加载/卸载云盘是动态操作，而云主机的*/etc/fstab*是静态配置文件。如果加载云盘后修改云主机fstab文件，对该云主机在线创建镜像，使用该镜像创建其它云主机时，由于fstab文件没有相应的挂载信息，所创建的云主机会hang住无法启动。

   - **解决方案**：

     - Linux云主机加载云盘后不建议通过修改*/etc/fstab*文件方式挂载。
     - 推荐的做法：

       - 进入*/etc/rc.d/rc.local*执行*mount*命令来挂载云盘：

         ```
         # chmod +x /etc/rc.d/rc.local
         # mount -U 文件系统UUID 目标挂载路径
         ```

         注: 建议使用云盘的ID来挂载而非*/dev/vdb*类似的盘符来挂载。

计算规格/云盘规格

1. Q：如何使用Tag将Instance offering/Disk Offering绑定主存储？

   A：

1. 首先获取想要创建VM的Instance Offering和Primary Storage的uuid。

```
>>>QueryInstanceOffering name=large
{
    "inventories": [
        {
            "allocatorStrategy": "Mevoco",
            "cpuNum": 4,
            "cpuSpeed": 1,
            "createDate": "Aug 17, 2016 10:27:10 AM",
            "description": "",
            "lastOpDate": "Aug 17, 2016 10:27:10 AM",
            "memorySize": 8589934592,
            "name": "large",
            "sortKey": 0,
            "state": "Enabled",
            "type": "UserVm",
            "uuid": "a1faec292ec848be8f38e5519623cd84"
        }
    ],
    "success": true
}
```

```
>>>QueryPrimaryStorage
{
    "inventories": [
        {
            "attachedClusterUuids": [
                "facc2e1f277440a7958008625b5dd515"
            ],
            "availableCapacity": 100520272896,
            "availablePhysicalCapacity": 100556562432,
            "createDate": "Aug 16, 2016 1:45:41 PM",
            "description": "",
            "lastOpDate": "Aug 17, 2016 10:08:27 AM",
            "mountPath": "/zstack_ps",
            "name": "PS-1",
            "state": "Enabled",
            "status": "Connected",
            "systemUsedCapacity": 4609003520,
            "totalCapacity": 105175318528,
            "totalPhysicalCapacity": 105175318528,
            "type": "LocalStorage",
            "url": "/zstack_ps",
            "uuid": "a8d8010f36a74ac2b9086281fbfd9084",
            "zoneUuid": "b924468082be4019bcc6e3492f428b3c"
        }
    ],
    "success": true
}
```

2. 然后为Primary Storage创建一个UserTag，为Tag命名为forWebTierVM。

```
>>>CreateUserTag tag=forWebTierVM resourceType=PrimaryStorageVO resourceUuid=a8d8010f36a74ac2b9086281fb
fd9084
{
    "inventory": {
        "createDate": "Aug 17, 2016 10:47:16 AM",
        "lastOpDate": "Aug 17, 2016 10:47:16 AM",
        "resourceType": "PrimaryStorageVO",
        "resourceUuid": "a8d8010f36a74ac2b9086281fbfd9084",
        "tag": "forWebTierVM",
        "type": "User",
        "uuid": "12f2817d5a9c49f99d6c6213f5034323"
    },
    "success": true
}
```

3. 为Instance Offering创建SystemTag，绑定刚才创建的UserTag。

```
>>>CreateSystemTag tag=primaryStorage::allocator::userTag::forWebTierVM resourceType=InstanceOfferingVO
 resourceUuid=a1faec292ec848be8f38e5519623cd84
{
    "inventory": {
        "createDate": "Aug 17, 2016 10:47:55 AM",
        "inherent": false,
        "lastOpDate": "Aug 17, 2016 10:47:55 AM",
        "resourceType": "InstanceOfferingVO",
        "resourceUuid": "a1faec292ec848be8f38e5519623cd84",
        "tag": "primaryStorage::allocator::userTag::forWebTierVM",
        "type": "System",
        "uuid": "5a7cb1afd1464f6aa22c2b05722deba8"
    },
    "success": true
}
```

4. 在创建VM时指定Instance Offering，默认会使用绑定的Primary Storage创建Root Volume。

5. 使用Disk Offering创建Volume也可仿照上述方法绑定Primary Storage。

21.5 硬件设施

1. Q：如何检查一台物理机是否支持硬件虚拟化？

   A：在终端中执行egrep "vmx|svm" /proc/cpuinfo命令，如果有输出代表支持硬件虚拟化。

2. Q：如何在BIOS打开硬件虚拟化支持？

   A：BIOS中默认开启硬件虚拟化支持。如果有修改，需要在BIOS中打开**Intel Virtual Technology**或**Secure Virtual Machine**选项，保存并退出。

3. Q：ZStack的计算节点支持的Qemu和Libvirt版本是？

   A：目前Qemu默认支持Qemu 2.6.0版本； Libvirt支持1.3.3版本。可在计算节点执行virsh version进行检查：

   ```
   Compiled against library: libvirt 1.3.3
   Using library: libvirt 1.3.3
   Using API: QEMU 1.3.3
   Running hypervisor: QEMU 2.6.0
   ```

4. Q：管理节点重启后，为何物理机长时间处于连接中？

   A：管理节点机器或者服务重启后，需要重新建立与各硬件资源的连接，此过程需要耗时间重新部署相关代理程序。

5. Q：如果管理节点IP地址、数据库IP地址、消息总线IP地址发生变化，如何快速修改？

   A：执行如下命令修改管理节点IP地址：

   ```
   [root@localhost ~]# zstack-ctl change_ip --ip NEW_IP   # NEW_IP为新的管理节点IP地址
   [root@localhost ~]# zstack-ctl restart_node
   ```

   执行上述命令默认会将管理节点IP、消息总线IP和数据库IP地址都变更为最新。如果用户单独配置了消息总线和数据库的IP地址，需执行如下命令：

   ```
   [root@localhost ~]# zstack-ctl change_ip --ip NEW_IP --cloudbus_server_ip NEW_IP_1 --mysql_ip NEW_IP_2
   [root@localhost ~]# zstack-ctl restart_node
   ```

6. Q：如果计算节点IP地址发生变化，如何快速修改？

A：如果计算节点IP地址发生变化，可使用以下方式快速修改计算节点IP地址：

- **UI方式**：

  在**硬件设施** > **物理机**页面，展开物理机详情页，点击**物理机IP**旁边的**编辑**按钮进行快速修改。IP地址更新后，建议手动重连物理机生效。

- **命令行方式**：

  依次执行如下命令：

  ```
  [root@localhost ~]# zstack-cli  #进入cli命令
  admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
  admin>>> UpdateKvmHost uuid=HOST_UUID managementIp=NEW.HOST.IP.ADDRESS #修改计算节点IP地址
  ```

  命令执行完成后建议执行ReconnectHost命令，建议手动重连物理机生效。

7. Q：如果镜像服务器IP地址发生变化，如何快速修改？

   A：如果镜像服务器IP地址发生变化，可使用以下方式快速修改镜像服务器IP地址：

   - **UI方式**：

     在**硬件设施** > **镜像服务器**页面，展开镜像服务器详情页，点击**镜像服务器IP**旁边的**编辑**按钮进行快速修改。IP地址更新后，建议手动重连镜像服务器生效。

   - **命令行方式**：

     依次执行如下命令：

     ```
     [root@localhost ~]# zstack-cli  #进入cli命令
     admin>>> LogInByAccount accountName=admin password=password #登录cli，默认用户名密码为：admin/password
     admin>>> UpdateSftpBackupStorage uuid=BACKUP_STORAGE_UUID hostname=NEW.HOST.IP.ADDRESS #修改镜像服务器IP地址
     ```

     命令执行完成后建议执行ReconnectBackupStorage命令，建议手动重连镜像服务器生效。

8. Q：如何手动延长ZStack管理节点启动时间？

   A：

   - **现象**：

在云主机中运行ZStack，可能会遇到启动超时失败，但之后运行zstack-ctl status又显示为Running状态的情况。系统提示例如：

```
no management-node-ready message received within 120 seconds, \
please check error in log file /tmp/zstack_installation.log
```

- **解决方案**：

  使用如下的命令修改timeout时间（以300s为例）：

```
[root@localhost ~]# zstack-ctl start_node --timeout 300
```

9.

Q：为什么ZStack报告主存储、镜像服务器容量和物理机上看到的内容不一致？

A：

- ZStack使用的是**thin clone模式**（copy on write技术），所以VM可以很快被创建。在KVM环境下，不论VM的镜像文件是10G还是100G，VM创建的时候只有一个很小的qcow2独立文件被创建出来。这个qcow2文件和原始的镜像文件一起共同组成了新的VM的硬盘。当有新的数据产生的时候，该qcow2文件的大小会不断增加。文件大小的上限为原始VM的镜像文件的配置上限（例如：10G，20G）也同VM的操作系统启动后看到的硬盘的实际大小相一致。
- 由于ZStack默认不支持资源超分（超卖），所以在计算空间的时候，会按照VM使用空间的上限来扣除可用空间的数量。于是用户在系统上用*df*命令看到的可用空间可能还有很大，但是ZStack已经把VM未来可能会占用的所有空间都已经计算在内了。于是就会导致用户可能看到硬盘上还有很多空间，但是不能创建云主机。

10.

Q：如何把ZStack管理节点从一台物理机迁移到另一台物理机？

A：

1. 在原管理端备份数据库，备份文件提示导出至 */var/lib/zstack/mysql-backup/*：

```
[root@old-zstack ~]#zstack-ctl dump_mysql
Backup mysql successful! You can check the file at /var/lib/zstack/mysql-backup/zstack-backup-db-2016-07-05_18-13-11.gz
```

2. 停止原管理端服务：

```
[root@old-zstack ~]#zstack-ctl stop
```

3. 将备份数据库转移至新服务器，并在新管理端导入数据库：

```
[root@new-zstack ~]#zstack-ctl restore_mysql --from-file=/root/zstack-backup-db-2016-07-05_18-13-11.gz --mysql-root-password=zstack.mysql.password
the management node has been stopped
```

```
Starting recover data ...
Recover data successfully! You can start node by: zstack-ctl start
```

4. 导入许可证：

```
[root@new-zstack ~]# zstack-ctl install_license -f ZStack-license.txt
```

5. 启动新管理端服务：

```
[root@new-zstack ~]#zstack-ctl start
```

6. 这时，可直接登录ZStack的UI界面进行物理机、主存储、镜像服务器等硬件资源的管理，如果原有物理机的IP地址有变更可以直接在UI界面修改并重新连接。

11. Q：重新安装管理节点，如何恢复原来配置？

    A：执行以下命令`zstack-ctl dump_mysql --keep-amount 14`，备份原本的管理节点数据库，在*/var/lib/zstack/mysql-backup*目录下查看。

12. Q：如何为物理机设置保留内存？

    A：在**设置** > **全局设置** > **基础设置**页面，修改**物理机保留内存**的值。

13. Q：ZStack安装完成后，如何修改MySQL密码？

    A：执行如下命令进行修改MySQL密码：

```
[root@localhost ~]# zstack-ctl change_mysql_password --root-password zstack.mysql
.password --user-name zstack --new-password password
```

14. Q：物理机维护模式和停用有什么区别？

    A：

    - **进入维护模式**：

      表示对物理机进行系统维护，可对物理机进行停机、故障修复等操作。确认物理机进入维护模式后，如果主存储类型为本地存储，ZStack会主动停止该物理机上所有正在运行的云主机；如果存储类型为共享存储，云主机会自动迁移至其他物理机上。

    - **停用**：

      停止使用某个物理机，后续云主机不能在此物理机上创建，且已关闭的云主机不能再启动，目前允许中的云主机不受影响。

15. Q：物理机连不上有哪些原因？

A：物理机连不上请检查以下原因：

- 管理节点是否能正常访问物理机22端口。
- 是否正确使用*ZStack定制版ISO*安装系统。
- 物理机的libvirt服务状态是否正常。
- 物理机所属集群的网络挂载情况是否已发生变化。

  假如集群挂载的二层网络指定的设备是eth1，但是物理机的网卡设备号发生变化，不存在eth1，那么此物理机将无法重连成功。
- 物理机系统盘的存储容量是否已经用完。
- 对于要求挂载NFS主存储的物理机，如果挂载失败，物理机将无法重连成功，此时需要检查物理机到NFS主存储的链路。
- 使用分布式块存储的物理机，如果存在存储网络，则要求物理机可直接访问存储网络。
- 如果使用VXLAN网络，其挂载集群时指定的VTEP IP应该存在，如果不存在，物理机将无法重连成功。

16.

Q：使用ZStack企业版时，镜像服务器添加不上怎么办？

A：镜像服务器添加不上请检查以下因素：

- Sftp镜像服务器和镜像仓库需检查SSH端口号、用户名、密码、用户名是否拥有sudo权限。
- Ceph镜像服务器需检查分布式块存储是否正常。需检查Ceph IP地址、Ceph SSH 端口、用户名、密码、用户名是否有sudo权限，Ceph集群状态是否正常。

17.

Q：SSH连接超时如何解决？

A：

- **现象**：

  ZStack中很多服务需要SSH连接，包括添加物理机、存储、搭建管理节点HA等。由于用户网络等问题，这些服务的操作可能因为SSH连接超时而提示time out的错误。
- **原因**：

  主要是由于对IP地址进行DNS校验产生延时。
- **解决方案**：

  以搭建管理节点HA为例解决该问题：

1. 在需要SSH连接的第二个管理节点上，打开*/etc/ssh/sshd_config*。
2. 将UseDNS yes这一行使用**#**注释掉，连接SSH时就可以直接使用IP地址。

18.

Q：ZStack启动后提示MySQL is not running如何解决？

A：

- **现象**：

  使用zstack-ctl start启动ZStack时提示错误：

  zstack-ctl status查看状态时显示 MySQL is not running

- **解决方案**：

  先尝试检查*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties*的配置。

  例如：

  ```
  DB.url = jdbc:mysql://10.0.0.18:3306
  DB.user = zstack
  DB.password = zstack.password
  ```

  使用mysql -u zstack -pzstack.password -h 10.0.0.18 -P 3306检测能否访问。

19.

Q：ZStack的无状态是什么？

A：在无状态的服务情况下，请求者不再需要询问何处发送请求；当新的服务实例加入或旧的服务实例脱离的时候，服务也不再需要交换状态。

假如某个操作删除了物理机的br_eth0（即：物理机连接L2网络的网卡），由于ZStack里所有的物理机均无状态，只要重连物理机即可。其实物理机硬盘上没有固定的配置文件，它在内存中。重连物理机后会重新生成配置文件。

20.

Q：ZStack的存储如何计算？

A：ZStack的存储分为主存储和镜像服务器。（以下讨论均不涉及超分情况）

- 镜像服务器的计算相对简单，其总容量和真实容量对应实际的物理值（即与*df -h*命令结果相同）
- 主存储分为物理总容量、物理可用容量和总容量、可用容量。其中物理总容量、物理可用容量与镜像服务器的技术方法相同，为物理真实容量。这里需要理解的主存储的总容量（Total

Capacity）和可用容量（Available Capacity）。总容量与实际总容量相同，可用容量为总容量减去云盘的虚拟容量（Virtual Size）。

注:

- 例如：主存储为500G，使用一个大小为100G的镜像创建云主机，实际大小为3G。在主存储上看到的可用容量为500G-100G=400G，而它的物理真实容量为500G-3G=497G。
- ZStack主存储URL指定到某个分区的目录上，主存储的总容量为目录所属分区的总容量。
- ZStack只关心自己使用的容量（镜像、云盘、快照），其他用户在这个分区使用的空间不计入已使用的容量中。
- 因此，可用容量=所属分区的总容量 - 自己使用的容量。其中，主存储上的镜像和快照为真实容量，云盘为虚拟容量。
- 每次容量校准需要重连物理机。

21.

Q：ZStack备份需要备份哪些数据？

A：ZStack本身的备份只需备份数据库即可。

22.

Q：ZStack如何备份数据库？

A：

- 执行zstack-ctl dump_mysql命令，会执行一次备份；
- 执行crontab -l命令，每天凌晨以及中午12：30均会备份一次数据库。保留最新的14个备份，可根据需求进行调整，为安全考虑建议进行异地远程备份。

```
30 0,12 * * * zstack-ctl dump_mysql --keep-amount 14
```

23.

Q：升级之后为什么MySQL的连接数会增加？

A：不会增加。如果突发异常，可能会遇到三个节点，只能启动两个，第三个报Too many connections错误的情况。可以通过修改MySQL配置，确认host的libvirtd是否正常。

24.

Q：新添加物理机时出现如下报错如何处理？

A：

- **现象**：

新添加物理机时出现如下报错：

```
{"org.zstack.header.host.APIAddHostEvent":{"success":false,"apiId":"75b0774fc7b940
07ac1ba274e6ed5eb3","headers":{"schema":{}},"error":{"code":"HOST.1000","cause
":{"code":"HOST.1003","cause":{"code":"SYS.1006","description":"An operation failed
","details":", failed to check physical network interfaces[names : enp2s0] on kvm host
[uuid:fab977f38e024e6e86f048a4090845f8, ip:192.168.10.11]"},"description":"An error
 happened when connecting to host","details":"connection error for KVM host[uuid
:fab977f38e024e6e86f048a4090845f8, ip:192.168.10.11]"},"description":"Unable to add
 host","details":"connection error for KVM host[uuid:fab977f38e024e6e86f048a40908
45f8, ip:192.168.10.11]"},"createdTime":1489036864392,"type":{"_name":"key.event.API
.API_EVENT"},"id":"8f1d551677c44788953eae7255eda54b"}}
```

- **原因及解决方案**：

  没有enp2s0网卡，一个集群里hosts的网卡应该和存储一致。

25.

Q：CPU未开启虚拟化，添加物理机出现如下报错如何处理？

A：

1. 安装ZStack后，添加物理机出现如下报错：

```
ERROR:could not insert 'kvm_intel':Operation not supportednnnstdout
```

2. 查看开启虚拟化情况，如果有返回值，则表示开启成功。

```
cat /proc/cpuinfo | grep "vmx|svx"
```

3. 开启后再次添加该物理机失败，出现libvirt相关错误。使用systemctl status libvirtd.service查看，提示：

```
Failed to start Virtualization daemon
```

4. 此时需将物理机的*/etc/libvirt/libvirtd.conf*修改成以下内容：

```
listen_tls = 0
listen_tcp = 1
tcp_port = "16509"
auth_tcp = "none"
lock_manager = "lockd"
```

26.

Q：部署Shared Mount Point主存储对文件系统有什么要求？

A：Shared Mount Point主存储要求你的计算节点挂载同一个NFS服务，并且挂载到本地计算节点相同的目录。

27.

Q：Ceph环境下创建快照1、2、3，然后删除1，但2和3没有删除，是否正确？创建模板时会自动生成一个快照，创建VM时是把模板快照恢复到VM上吗？

A：Ceph类型是无树状，快照点之间没有依赖关系，恢复快照会丢失当前状态，使用了Ceph的Snap Clone方法。

28.

Q：Ceph计算节点出现could not get value of the secret for username zstack错误如何处理？

A：

- **现象**：

  当计算节点使用Ceph存储时，在创建、启动、迁移云主机时，出现以下错误：

  ```
  内部错误：could not get value of the secret for username 'zstack' using uuid 'ee5b6375
  -4564-446b-ac53-c94ea4e13904'
  ```

- **原因**：

  一般是计算节点连接Ceph时，丢失密钥，需要删除密钥，重连物理机。

- **解决方案**：

  需要进行以下步骤进行修复：

  1. 在出现问题的计算节点执行virsh secret-list获取其uuid。

     例如：获取uuid为03b5ee0d-df21-46d2-9927-7c930333cb70

     ```
     root@ceph-host ~]# virsh secret-list
      UUID                                   Usage
     --------------------------------------------------------------------------------
      03b5ee0d-df21-46d2-9927-7c930333cb70  ceph 03b5ee0d-df21-46d2-9927-7c93033
     3cb70
     ```

  2. 执行virsh secret-undefine 03b5ee0d-df21-46d2-9927-7c930333cb70删除其密钥。

     ```
     [root@ceph-host ~]# virsh secret-undefine 03b5ee0d-df21-46d2-9927-7c930333cb70
     Secret 03b5ee0d-df21-46d2-9927-7c930333cb70 deleted
     ```

  3. 执行/etc/init.d/zstack-kvmagent stop停止管理节点agent。

     ```
     [root@ceph-host ~]# /etc/init.d/zstack-kvmagent stop
     2017-05-08 10:07:57,590 DEBUG [zstacklib.utils.shell] /sbin/iptables-save
     2017-05-08 10:07:57,596 DEBUG [zstacklib.utils.iptables] removed empty chains:[]
     2017-05-08 10:07:57,598 DEBUG [zstacklib.utils.shell] /sbin/iptables-restore < /tmp/
     tmpBW4mWX
     Stop Daemon...
     Stop Daemon Successfully
     stop zstack kvm agent .... SUCCESS
     ```

  4. 在UI界面再次重连此计算节点，重连成功后，创建、启动、迁移云主机即可正常。

     注: 目前ZStack在UI已提供关闭CephX密钥认证选项。

29.

Q：主机的系统版本要一致吗？

A：建议管理主机和物理主机系统版本一致，所有物理主机系统版本必须一致。

30.

Q：备份管理节点需要备份哪些信息？

A：只需备份数据库。执行命令 `zstack-ctl dump_mysql`手动备份管理节点数据库。

31.

Q：如果一个集群挂载两个主存储，云盘如何分配？

A：

ZStack中，允许一个集群添加两个主存储。当主存储类型不同时，例如：一个LocalStorage和一个NFS。再次创建云主机，root盘将默认创建在LocalStorage，data盘将默认创建在NFS。

32.

Q：Dell服务器安装ZStack，遇到**dracut-initqueue timeout**， 安装了系统无法启动。

A：在BIOS里面，Boot Settings，从BIOS模式修改为UEFI模式，即可解决。

33.

Q：管理节点有多个网卡和IP，如何指定ZStack服务监听在哪个IP地址上？

A：当系统上有多个网卡和IP地址时（例如一个内网，一个外网），ZStack默认选择系统默认路由使用的网卡IP地址。

用户也可使用如下命令手动指定ZStack服务监听的IP地址：

```
[root@ceph-host ~]# zstack-ctl configure management.server.ip=${MANAGEMENT_IP}
```

其中，${MANAGEMENT_IP}是用户希望指定的IP地址。

34.

Q：如果两个物理机上的云主机网络不通，该如何排查？

A：根据网络类型不同，可按照如下步骤进行排查：

- 对于VLAN类型的网络，假设网卡为eth0，设备VLAN为25
  1. 执行命令`ifconfig br_eth0_25` 配置的IP分别为两个物理机上的不同网桥配置一个IP地址
  2. 在某一个物理机上使用`arping -I br_eth0_25` 配置的IP判断是否连通，如不通，需要进一步检查交换机是否配置正确
  3. 检查交换机是否设置了trunk口；是否允许了所有的VLAN；vlan database里面是否有vlan 25
  4. 测试通信后分别在两台物理机上执行命令`ip addr del` 配置的IP `dev br_eth0_25`删除IP配置

- 对于VXLAN类型的网络，建议检查VXLAN网络对应的VTEP IP地址是否正常通信

35.

Q：ZStack一个集群支持多个主存储吗？ 支持不同类型的主存储搭配使用吗？

A：ZStack支持一个主存储加载多个集群，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。

36.

Q：计算节点一直显示重连中但是却连接不上怎么处理？

A：登录该计算机点，依次执行如下命令，完成后在UI界面重连计算节点：

```
[root@10-0-5-87 ~]# service libvirtd restart
[root@10-0-5-87 ~]# service virtlogd restart
[root@10-0-5-87 ~]# /etc/init.d/zstack-kvmagent stop
```

37.

Q：如何恢复被误删除的镜像服务器上的镜像？

A：ImageStore类型的镜像服务器，可通过UI方式重新添加该镜像服务器。在**添加镜像服务器**界面，勾选**获取已有镜像**按钮。

38.

Q：物理机中可用量和可用物理容量有何差别？

A：

- 可用量是可用虚拟容量，创建存储设备资源如云盘时，可用量减少量为云盘规格容量；
- 可用物理容量实际只会减少云盘的真实容量，是因为采用qcow2类型的镜像，写时复制，当在云盘中新建数据时云盘真实容量才会增长。

39.

Q：物理机出现kvm_zap_rmapp导致内核崩溃致使宕机，怎么办？

A：

- **原因**：

内核执行kvm_zap_rmapp时崩溃。

受影响范围为：kernel-3.10.0-327.53.1.el7.x86_64之前的版本

注: ZStack CentOS 7.2内核版本为：3.10.0-327.36.1.el7.x86_64

具体可参考红帽官网文档。

- **解决方案**：
  - 可考虑将计算节点内核从原本的CentOS 7.2升级到ZStack最新的CentOS 7.4版本。
  - 也可参考以下方法临时解决：
    1. 在计算节点的kvm模块配置文件中加入options kvm_intel pml=0；
    2. 执行以下命令：

       ```
       echo "options kvm_intel pml=0" >>/etc/modprobe.d/kvm.conf
       ```

    3. 重启物理机。

21.6 网络

1. Q：ZStack支持哪些速率的网络接口？

   A：支持40G、千兆、万兆等，云平台环境建议千兆以上。

2. Q：同一个三层网络是否支持设置不同的子网掩码和网关？

   A：不支持，这种配置会造成网络异常。

3. Q：如何指定非默认路由的IP地址启动ZStack服务？

   A：依次执行如下命令：

   ```
   [root@localhost ~]# zstack-ctl configure management.server.ip=YOUR_EXPECTED_
   IP_ADDRESS  #设置管理节点的IP地址
   [root@localhost ~]# zstack-ctl restar_node  #重启管理节点服务
   ```

4. Q：如何释放Flat Network Service Provider（扁平网络服务模块）占用的IP？

   A：

   - **原因**：

     Flat Network Service Provider提供DHCP服务，所以会占用一个IP地址。

- **解决方案**：

  当用户不想使用该服务的时候，可以删除对应L3 network但是该provider所占用的IP地址并不会被主动释放。可用以下方法回收该IP地址，并消除对应的影响。

  在所有的物理节点上执行：

  1. ip netns
  2. 对所有输出的namespace执行ip netns delete xxxx，xxxx是步骤一输出的对应的namespace
  3. 执行ebtables -F
  4. 执行pkill dnsmasq，把所有DHCP server杀死

5. Q：ZStack只认eth0? 为何不支持em01？

   A：ZStack是根据用户的配置来确认网卡的名称， 要求同集群内所有的计算节点网卡编号一致。

   - 如果原本已添加eth0的二层网络，但是添加新的计算节点的网卡名称只有em01的网卡，却没有eth0的网卡。
   - 如果在添加二层网络时，选择了eth0，那么所有的计算节点要求使用同样的eth0来设置网络。
   - 用户也可以设置em01作为二层网络来添加，但是同样的要求所有的计算节点均配置em01的网络。
   - 用户可以删除L2重新配置。

6. Q：管理网络和数据网络放在一起会影响吗？

   A：建议分离，安全性会更高，网络负载分配更合理。如果网络资源不足，可以放在一起。

7. Q：为何我的IP Range中会少一个IP？DHCP服务的IP是多少？

   A：

   - 对于前一个问题，这个IP分配给云路由器或者DHCP Server了，云路由器的IP可以直接看到。

- 对于后一个问题，DHCP服务的IP， 登录后，可用*zstakc-cli*查询DHCP Server占用的IP地址：

  ```
  QuerySystemTag  resourceType="L3NetworkVO"
  ```

  这个IP是DHCP Server占用，用于分配DHCP IP地址，不应该释放。

8.
Q：ZStack如何修改L3的IP Range呢？

A：需要在L3网络中，添加新的IP Range然后删除原来的，云主机重启后会在新的IP Range里重新分配IP。

9. Q：ZStack如何设置静态IP？

A：在**云主机** > **配置信息**页面，点击网卡操作中的**设置静态IP**按钮，按要求设置静态IP。

注: 设置静态IP操作需要在云主机关机时执行。

10.
Q：万兆网卡只能识别一个模块是什么原因？

A：用户服务器新添加万兆网卡，一个网卡有两个光电模块。必须保证这两个光电模块的品牌型号一致，且与网卡匹配，才能同时识别。

11.
Q：创建云路由网络时报如下错误如何处理？

A：

- **现象**：

  创建云路由网络时报如下错误消息：

  ```
  "description": "A message or a operation timeout",
      "details": "[Async Http Timeout] url: http://10.10.10.253:7272/init, timeout after 300000 [MILLISECONDS], command: {\"uuid\":\"78183b0a46094e30bc8a6128b30ee8cb\", \"restartDnsmasqAfterNumberOfSIGUSER1\":0}"
    }
  ```

- **原因**：

  同时满足以下情况就会出现该问题：

  - 管理节点上有多块网卡；
  - 第一块网卡置了默认路由；
  - 第一块网卡设置的IP为内网IP，无法访问外网。

- **解决方案**：

增加或修改*/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties*文件中的参数**management.server.ip=xxx.xxx.xxx.xxx**，将其设置为可以访问外网的IP地址。

12.

Q：ZStack的DHCP服务由谁提供？

A：扁平网络、云路由网络、VPC网络都是由Flat Network Service Provider（扁平网络服务模块）提供分布式DHCP服务。

13.

Q：是怎样实现物理主机与云主机互通？

A：只要物理主机和云主机在一个大二层网络中，且处于相同的网络段，就可以互通。扁平网络、公有网络都可以。

14.

Q：ZStack对负载均衡是如何规划的？目前支持像Netscaler这样的商业方案吗？

A：ZStack使用vyos 提供负载均衡服务，主要是访问公网IP相关的服务，实际由后台一系列云主机提供服务。Netscaler更贴近于Web服务应用交付相关。

15.

Q：ZStack创建二层网络时，可以为一个物理网卡划分多个VLAN吗？对应交换机上要配置成trunk模式吗？

A：可以，**1- 4094**端口可用。ZStack支持一个网卡上创建多个L2 vlannetwork，要求连接交换机后配置成trunk且允许相应的vlan通过。

16.

Q：VLAN设置完成后不能通信，开了**iptables**，是不是要加什么配置才能让VLAN互相通信？

A：VLAN互相通信需要在交换机上配置。

17.

Q：如何登录云路由器？

A：登录云路由器需输入用户名和密码。在**设置** > **全局设置** > **基本设置**页界面，可对云路由器的登录密码进行设置。

- 云路由器管理员账户是：vyos，登录密码默认为**vrouter12#**。
- 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。

18.

Q：弹性IP不通该如何排查？

A：

- 检查云主机内部的默认网关是否配置，是否可达
- 检查物理链路是否可达。确保对应的二层网络在每个物理机上的接线完全一致

19.
Q：创建二层网络挂载集群失败，请问是什么问题？

A：检查网卡名填写正确，要求相同集群下的物理机具有相同的网卡名才能二层网络才能创建成功。

20.
Q：网卡bond设置错了，如何修改？

A：以bond0为例，执行如下命令：

```
[root@host ~]# zs-restore-network-setting -i bond0
[root@host ~]# zs-nic-to-bond -d bond0 em0
[root@host ~]# zs-bond-ab -d bond0
```

然后按照正确的步奏重新配置bond。

21.
Q：ZStack支持IPv6吗？

A：ZStack3.1.0及以后版本支持IPv6，创建云主机可选择IPv4、IPv6 或双栈类型的网络地址。

22.
Q：安全组的机制和默认规则是什么？

A：安全组基于白名单机制， 如果新建安全组没有设置任何规则，默认所有的外部访问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。

23.
Q：ZStack可以对网络和磁盘设置QoS吗？在哪里设置呢，范围多少？

A：支持。创建计算规格或云盘规格的时候支持设置QoS，也可在云主机配置界面进行修改。磁盘QoS设置范围为：1MB/S~100GB/S；网卡QoS设置范围为：8Kbps-30Gbps

21.7 vCenter

1.
Q：VMware ESXi设置云主机嵌套虚拟化的方法？

A：

- **方法一**：

登录VMware ESXi控制台打开VMware ESXi 5.0的ssh服务，用*ssh*登录 VMware ESXi 后在**config**文件（*vi /etc/vmware/config*），在末尾加入vhv.enable = “TRUE” 命令。

- **方法二**：

  如果不能重启整改ESXi，通过vSphere下载想要设置嵌套虚拟化的云主机的**config**文件（xxx.vmx），在该文件最后加上vhv.enable = "TRUE" 命令。

  注: 操作前需要停止云主机。添加设置后，把修改的**config**拷贝覆盖原有配置文件，重启云主机。

2.

Q：在VMware的嵌套虚拟化的云主机里创建ZStack的VR VM失败怎么办？

A：需要在VMware的vSwitch设备上打开混杂模式，并填写Vlan号。

3.

Q：vCenter云主机无法ping通网关？

A：使用vCenter创建的云主机作为ZStack的管理节点和计算节点时，需要把vSwitch属性的**安全** > **混杂模式**修改为**接受**。

4.

Q：在ZStack部署vCenter环境报错No dvSwitch found怎么办？

A：

- **现象**：

  报错如下：

```
  "org.zstack.vmware.APIAddVCenterMsg": {
    "domainName": "192.168.0.16",
    "name": "VC",
    "username": "administrator@vsphere.local",
    "password": "*******",
    "https": "true",
    "zoneUuid": "631998da879f4b63b484876138c87a6a",
    "session": {
      "uuid": "5cec7c53f71344858a30186dd0d8280a",
      "callid": "api-mMa45Vw7"
   }
  }
}
{
  "success": false,
  "apiId": "476e659189ef4097b98dcf0ed4adc51c",
  "headers": {
    "api-id": "476e659189ef4097b98dcf0ed4adc51c",
    "schema": {}
  },
  "session": {
    "callid": "api-mMa45Vw7",
    "uuid": "5cec7c53f71344858a30186dd0d8280a"
```

```
  },
  "error": {
    "code": "SYS.1006",
    "description": "An operation failed",
    "details": "No dvSwitch found",
    "$$hashKey": "object:672"
  },
  "createdTime": 1496300098050,
  "type": {
    "_name": "key.event.API.API_EVENT"
  },
  "id": "872c5d4ab75e4fd88a69bec0f90b41fe"
}
```


- **原因及解决方案**：

  vCenter环境需要先创建分布式交换机：VC CLUSTER HOST dvswitch。如果需要ZStack来接管vCenter，vCenter必须能先创建dvSwitch；ZStack创建云路由网络也基于dvSwitch。

5. Q：vCenter云主机无法打开控制台，如何解决？

   A：ZStack接管vCenter后，原本运行的vCenter云主机不能直接打开控制台，通过如下操作，即可打开控制台：

   - 通过ZStack重启vCenter云主机
   - 通过ZStack进行动态迁移vCenter云主机（基于共享存储）

6. Q：ZStack接管vCenter后，对原有的vCenter有影响么？

   A：ZStack仅接管vcenter资源，提供一个管理入口，并不影响其原有资源。

21.8 平台管理运维

1. Q：ZStack支持连接SPICE协议吗？

   A：支持。可使用以下方式修改云主机控制台模式：

   在**设置** > **全局设置** > **基本设置**页面，将云主机控制台模式从VNC修改为SPICE。

2. Q：当前有一个UUID，如何得知该UUID所属资源类型，以及如何查询该UUID资源的相关属性？

   A：可以先在*/usr/local/zstack/apache-tomcat/logs/management-server.log*里查看该UUID所属的资源类型，再用*zstack-cli*命令查询该UUID资源的相关属性。

3. Q：ZStack能和AD/LDAP连接吗？只能用API接口控制用户吗？

   A：

- ZStack可以和AD/LDAP连接，具体可参考官网教程《AD/LDAP 配置教程》。
- ZStack提供了RESTful API的调用文档，不限制语言，具体可参考开发手册的**AD/LDAP相关接口**章节。

4.

Q：如何设置管理节点 prometheus数据保留时间？

A：

- 执行命令`vim /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`进入修改配置文件页面，新增配置`Prometheus.retention = 876h0m0s`（设置监控数据保留时间为876小时）
- 执行`zstack-ctl restore_node`重启管理节点服务

5.

Q：企业版授权过期了会自动关闭云主机吗？

A：授权过期不会自动关闭云主机，但平台不能再进行任何操作。重新获取授权可继续使用。

21.9 高级功能

1.

Q：裸金属设备无法获取硬件信息，如何解决？

A：请检查以下事项，是否满足要求：

- 确保部署网络内除了部署服务器没有其它DHCP服务；
- 确保裸金属设备连接部署网络的网卡在BIOS中开启PXE功能；

  注:

  - 对于部分机型，还需确保该PXE网卡为首张启动网卡，或确保（启动顺位）在PXE网卡之前的所有网卡均关闭PXE功能。
- 确保裸金属设备的启动模式为Legacy。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

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

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

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

主存储（Primary Storage）

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

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。

镜像仓库（Image Store）

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

云主机（VM Instance）

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

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

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

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

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

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

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

VXLAN网络池（VXLAN Network Pool）

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

VXLAN网络（VXLAN）

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

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

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

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一个时间点上某一个磁盘的数据备份。包括自动快照和手动快照两种类型。