

天翼全栈混合云敏捷版 运维手册

产品版本：V4.1.3

文档版本：V4.1.3

版权声明

版权所有©中国电信股份有限公司云计算分公司。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

eCloud商标和其他中国电信股份有限公司云计算分公司商标均为中国电信股份有限公司云计算分公司的商标。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、服务或特性等应受中国电信股份有限公司云计算分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，中国电信股份有限公司云计算分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	2
3 产品功能	3
4 系统架构	36
4.1 Cloud功能架构	36
4.2 Cloud资源结构	38
5 网络配置	41
6 安装部署	44
6.1 环境准备	44
6.1.1 网卡归一化(可选)	54
6.2 安装Cloud	62
6.2.1 Cloud管理节点模式.....	64
6.2.2 Cloud计算节点模式.....	64
6.2.3 Cloud专家模式.....	64
6.3 管理Cloud	64
6.4 升级Cloud	65
7 系统登录	69
7.1 HTTPS方式登录UI	70
8 许可证管理.....	73
8.1 概述	73
8.2 管理许可证	76
9 Wizard引导设置.....	80
10 首页	85
11 大屏监控	92
12 资源中心	102
12.1 云资源池.....	102
12.1.1 云主机.....	102
12.1.2 云盘.....	119
12.1.3 镜像.....	125
12.1.4 计算规格	130
12.1.5 云盘规格	131
12.1.6 GPU规格.....	132
12.1.7 弹性伸缩组	133
12.1.8 快照.....	137
12.1.9 亲和组.....	141
12.2 硬件设施.....	143
12.2.1 区域.....	143
12.2.2 集群.....	145
12.2.3 物理机.....	150
12.2.3.1 物理机运维(扩展).....	156
12.2.3.1.1 物理机计划性关机.....	156

12.2.3.1.2 物理机扩容	157
12.2.3.1.3 物理机更换	157
12.2.3.1.4 重连物理主机	158
12.2.3.1.5 单个物理机运维	158
12.2.3.1.6 批量物理机运维	159
12.2.3.2 外接设备运维	162
12.2.3.2.1 GPU设备	162
12.2.3.2.2 vGPU设备	167
12.2.3.2.3 USB设备透传	167
12.2.3.2.4 SR-IOV网卡虚拟化	168
12.2.4 主存储	170
12.2.4.1 本地存储	173
12.2.4.2 NFS	174
12.2.4.3 Shared Mount Point	175
12.2.4.4 Ceph	175
12.2.4.5 Shared Block	177
12.2.4.6 主存储运维(扩展)	177
12.2.4.6.1 本地存储运维	177
12.2.4.6.2 NFS存储运维	178
12.2.4.6.3 Shared Mount Point存储运维	179
12.2.4.6.4 企业版Ceph存储运维	179
12.2.4.6.5 Shared Block存储运维	183
12.2.4.6.6 重连主存储	183
12.2.5 镜像服务器	184
12.2.5.1 ImageStore (镜像仓库)	187
12.2.5.2 Ceph	188
12.2.5.3 镜像服务器运维(扩展)	188
12.2.5.3.1 ImageStore镜像服务器运维	188
12.2.5.3.2 Ceph镜像服务器运维	189
12.2.5.3.3 重连镜像服务器	190
12.2.6 SAN存储	191
12.2.6.1 SAN存储运维(扩展)	192
12.3 网络资源	193
12.3.1 二层网络	194
12.3.2 VXLAN Pool	198
12.3.3 三层网络	200
12.3.4 VPC路由器	205
12.3.5 VPC路由器高可用组	207
12.3.6 路由器镜像	208
12.3.7 路由器规格	209
12.3.8 SDN控制器	210
12.3.9 管理网络	210
12.3.10 流量网络	211
12.4 网络服务	211
12.4.1 安全组	214
12.4.2 虚拟IP	216
12.4.3 弹性IP	218
12.4.4 端口转发	221
12.4.5 负载均衡	223
12.4.6 防火墙	227
12.4.7 IPsec隧道	229

12.4.8 OSPF区域	230
12.4.9 Netflow	230
12.4.10 端口镜像	231
12.4.11 路由表	231
12.5 资源编排	232
12.5.1 资源栈	233
12.5.2 资源栈模板	236
12.5.3 资源栈示例模板	238
12.5.4 可视化编排	241
12.6 裸金属管理	247
12.6.1 裸金属集群	250
12.6.2 部署服务器	252
12.6.3 裸金属设备	253
12.6.4 预配置模板	255
12.6.5 裸金属主机	258
12.7 弹性裸金属管理	262
12.7.1 部署网络	265
12.7.2 弹性裸金属集群	266
12.7.3 网关节点	267
12.7.4 裸金属节点	268
12.7.5 弹性裸金属实例	268
12.8 vCenter	271
12.8.1 基础资源	272
12.8.2 云主机	274
12.8.3 网络	276
12.8.4 云盘	277
12.8.5 镜像	278
13 平台运维	280
13.1 网络拓扑	280
13.2 云平台监控	284
13.2.1 性能分析	284
13.2.2 容量管理	285
13.2.3 管理节点监控	286
13.2.4 报警器	287
13.2.5 一键报警	288
13.2.6 资源分组	289
13.2.7 报警模板	289
13.2.8 消息模板	290
13.2.9 消息源	290
13.2.10 通知对象	290
13.3 消息日志	291
13.3.1 报警消息	291
13.3.2 操作日志	291
13.3.3 审计	293
13.4 灾备管理	296
13.4.1 备份任务	302
13.4.2 本地备份数据	305
13.4.3 本地备份服务器	307
13.4.4 远端备份服务器	308
13.5 定时运维	310

13.5.1 定时任务	310
13.5.2 定时器	311
13.6 标签管理	312
13.7 迁移服务	312
13.7.1 迁移任务	314
13.7.2 迁移服务器	318
14 运营管理	320
14.1 企业管理	320
14.1.1 组织架构	326
14.1.2 用户	328
14.1.3 成员组	330
14.1.4 角色	331
14.1.5 第三方认证	331
14.1.6 项目管理	332
14.1.7 工单管理	334
14.2 计费管理	335
14.2.1 计费价目	335
14.2.2 账单	336
14.3 访问控制	341
14.3.1 AccessKey管理	341
14.3.2 IP黑白名单	345
14.3.3 控制台代理	347
14.4 应用中心	348
15 设置	349
15.1 账户信息	349
15.2 主题外观	350
15.3 邮箱服务器	350
15.4 日志服务器	351
15.5 全局设置	351
15.6 场景封装	352
16 管理节点运维	360
16.1 管理节点高可用	360
16.1.1 多管理节点物理机高可用场景	360
16.2 管理节点灾难恢复	362
16.2.1 准备工作	362
16.2.2 管理节点灾难恢复	363
16.3 修改管理节点IP地址	364
16.3.1 单管理节点场景	364
16.3.2 多管理节点物理机高可用场景	366
16.4 切换管理节点	368
16.5 计算节点升级为管理节点	369
17 云平台基本运维	370
17.1 安装部署	370
17.2 启动服务	372
17.3 zstack-ctl命令	373
17.4 zstack-cli命令	374
17.5 云主机异常	375
17.6 日志分析	381
17.7 端口占用	382

17.8 网络脚本	383
17.9 删除资源	386
17.10 卸载资源	389
18 云平台其他运维	391
18.1 配置运维	391
18.1.1 普罗米修斯升级 (Prometheus)	391
18.1.2 zstack.properties核心配置文件	392
18.1.3 zstack.ui.properties核心配置文件	396
18.1.4 云平台硬件资源密码变更	397
18.1.5 管理节点更改物理环境	397
18.1.6 数据库备份与恢复	397
18.1.7 本地存储空间扩容	398
18.1.8 云主机根云盘扩容	399
18.2 Shared Block共享云盘升级	404
18.3 企业版Ceph变更时间	405
18.4 集群时间源变更	407
19 物理基础设施运维	410
19.1 机房电力运维	410
19.2 机房搬迁运维	411
19.3 交换机运维	411
20 常见问题	413
20.1 快速入门	413
20.2 安装部署	415
20.3 系统登录	421
20.4 云资源池	423
20.5 硬件设施	442
20.6 网络	451
20.7 裸金属管理	457
20.8 vCenter	458
20.9 平台管理运维	460

1 引言

产品版本

目前与本文档相对应的产品版本为：Cloud 4.1.3

读者对象

本文档详述了Cloud 4.1.3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：

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

2 概述

Cloud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Cloud快速构建自己的智能云数据中心，也可以在稳定的Cloud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。

3 产品功能

Cloud提供多种授权协议，不同授权协议提供的云平台功能范围不同。本章节主要针对**企业版 付费**云平台许可证以及一系列模块许可证提供的功能范围进行介绍。

企业版 付费 功能列表

类别	特性	Cloud企业版 付费
首页	自定义首页	提供多维度数据统计卡片，支持通过添加、拖拽卡片进行首页定制化
		为不同角色提供各自视角的默认首页
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
	云主机生命周期管理	支持云主机的创建、停止、启动、重启、恢复、暂停、关闭电源、删除等基本生命周期管理
	云主机控制台	不依赖远程工具，直接通过终端方式访问云主机
		控制台支持SPICE、VNC、SPICE+VNC三种模式，其中，SPICE协议支持SSL加密通道，进一步保障桌面安全
		支持设置控制台密码、支持强制设置控制台密码（通过全局设置控制）、支持设置控制台密码策略（包括：密码复杂度、密码长度；通过全局设置控制）
	克隆（不带数据云盘）	基于云主机快速克隆若干云主机
		LocalStorage/NFS/SMP/Ceph/Shared Block类型的主存储，支持在线/暂停/关机克隆
		在线克隆（支持ImageStore/Ceph类型的镜像服务器）
		关机克隆（支持ImageStore/Ceph类型的镜像服务器）
	整机克隆（带数据云盘）	同时克隆云主机的根云盘和数据云盘
		LocalStorage/NFS/SMP/Ceph/Shared Block类型的主存储，支持在线/暂停/关机克隆
		仅支持ImageStore类型的镜像服务器
		云主机加载共享云盘不支持整机克隆
	自定义标签	支持自定义云主机标签，方便快速查询定位资源
	冷迁移	云主机关机迁移（仅支持本地存储）

类别	特性	Cloud企业版 付费
		支持按目标计算节点负载高低冷迁移云主机
	在线迁移	云主机在线迁移（支持所有主存储类型）
		支持按目标计算节点负载高低在线迁移云主机
	存储迁移	支持云平台内跨同类型主存储冷迁移云主机，包括：Ceph主存储-Ceph主存储、NFS主存储-NFS主存储、Shared Block主存储-Shared Block主存储
		支持云主机不带云盘跨Ceph主存储-Ceph主存储冷迁移
		支持云主机不带云盘跨NFS主存储-NFS主存储冷迁移
		支持云主机不带云盘跨Shared Block主存储-Shared Block主存储冷迁移
		支持云主机带云盘（共享云盘除外）跨Shared Block主存储-Shared Block主存储冷迁移
		支持云平台内跨不同类型主存储热迁移云主机，包括：Ceph主存储-Shared Block主存储、本地存储-Shared Block主存储、本地存储-Ceph主存储、本地存储-NFS主存储、Shared Block主存储-NFS主存储、Ceph主存储-NFS主存储
		支持云主机带云盘（共享云盘除外）跨不同类型主存储热迁移
		云主机跨不同类型主存储热迁移后将不保留快照
		若已确保存储迁移后数据完整无损，可手动清理存储迁移保留的原始数据，释放存储空间
	修改计算规格	支持云主机在线/关机状态下修改计算规格（CPU/内存）
	设置GPU规格	支持云主机关机状态下设置GPU规格，包括：物理GPU规格的加载/修改/取消、vGPU规格的加载/修改/取消
	根云盘扩容	支持云主机在线/关机状态下根云盘扩容，即时生效
	数据云盘扩容	支持云主机在线/关机状态下数据云盘扩容，即时生效
	更换所有者	支持云主机在线/关机状态下更换所有者
	更换系统	支持云主机关机状态下更换操作系统
	重置云主机	支持恢复云主机状态为镜像初始状态，根云盘所有数据将被覆盖
	云主机启动顺序	支持调整云主机启动顺序，用于切换ISO引导
		支持网络、硬盘和光驱三种启动方式

类别	特性	Cloud企业版 付费
	指定物理机启动	支持为云主机指定物理机启动
	云主机高可用	当物理机故障时，云主机支持自动重启，UI支持展示恢复进度
	云主机时间同步	支持设置云主机基准时间是否与物理机保持一致
	SSH密钥注入	支持Linux和BSD操作系统SSH密钥注入
		支持创建和删除密钥
		默认禁用VyOS SSH认证方式登录，提升安全性
	修改云主机密码	支持Windows/Linux云主机在线状态下修改密码
	设置主机名	创建云主机支持设置主机名
	资源优先级	提供 正常 和 高 两种优先级，当出现资源竞争时，优先保证资源优先级为 高 的云主机的资源使用
	跨集群高可用	支持设置云主机跨集群高可用策略，策略开启表示云主机可跨集群自动迁移，策略关闭表示云主机将限制在策略生效时所在集群内活动
		目前适用场景：云主机高可用更换物理机启动、物理机进入维护模式触发迁移
		该策略只针对云主机自动迁移行为有影响，其它如：手动热迁移云主机、指定物理机启动云主机、基于动态资源调度策略迁移云主机等均不受影响
	USB重定向	支持将VDI客户端USB设备重定向至云主机
	云主机快照	做重要操作前，对根云盘或数据云盘在特定时间点进行临时状态保留，方便出现故障后迅速回滚
		支持单盘快照和快照组两种快照类型，其中快照组支持以组为单位批量恢复
		在线快照（支持ImageStore/Ceph类型的镜像服务器）
		关机快照（支持ImageStore/Ceph类型的镜像服务器）
		支持恢复快照后自动启动云主机
		支持批量删除云主机快照
		支持基于云主机快照创建云主机，或基于快照组创建带数据云盘的云主机
	云主机备份	支持云主机在线状态下创建备份

类别	特性	Cloud企业版 付费
		支持对云主机进行增量备份或全量备份
		支持云主机在线状态下带云盘（共享云盘除外）进行整机备份
		该功能由灾备服务模块提供
	云主机镜像	基于当前云主机制作模板镜像，方便定制化批量创建云主机
		在线创建云主机镜像（支持ImageStore/Ceph类型的镜像服务器）
		关机创建云主机镜像（支持ImageStore/Ceph类型的镜像服务器）
	基于ISO部署	基于ISO系统光盘创建云主机，引导安装系统
		允许单台云主机加载多个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
	绑定/解绑亲和组	支持云主机在线/关机状态下绑定亲和组/从亲和组解绑
	加载/卸载数据云盘	支持云主机在线/关机状态下加载/卸载数据云盘，支持优化驱动模型，支持SCSI WWN号唯一识别
	共享云盘	支持Ceph存储或Shared Block存储下，多台云主机共享使用同一数据云盘
	创建云盘镜像	支持云主机在线/关机状态下对加载的根云盘/数据云盘创建镜像
		为Shared Block主存储上的共享云盘创建镜像，需先停止所有加载该云盘的云主机
	设置云盘QoS	支持云主机在线/关机状态下对加载的根云盘/数据云盘进行限速
	加载/卸载网卡	支持云主机在线/关机状态下加载/卸载网卡，支持设置默认网卡
	设置网卡类型	支持云主机关机状态下设置网卡类型
		仅支持VF类型的网卡切换为vNIC类型
	设置网卡型号	支持云主机在线/关机状态下设置网卡型号，包括：virtio、rtl8139、e1000
		仅支持Linux和Paravirtualization操作系统
	修改网卡三层网络	支持修改云主机网卡的三层网络，修改后云主机网卡MAC地址和PCI地址等硬件信息不变

类别	特性	Cloud企业版 付费
	设置网络QoS	支持云主机在线/关机状态下对网卡进行限速
	自定义MAC地址	支持创建云主机时自定义MAC地址
		支持云主机关机状态下修改MAC地址
	自定义IP地址	支持创建云主机时自定义IP地址
		支持云主机关机状态下修改IP地址
	云主机多网关	支持zstack-clt工具开启云主机多网关功能，开启后云主机每个网口均有独立网关
	创建/删除虚拟光驱	支持云主机关机状态下创建/删除虚拟光驱，支持为单个光驱加载/卸载ISO
	加载/卸载外接设备	支持云主机在线/关机状态下加载/卸载块设备
		支持云主机在线/关机状态下加载/卸载物理GPU设备
		支持云主机关机状态下加载/卸载vGPU设备
		支持云主机在线/关机状态下加载/卸载USB设备
		支持云主机在线/关机状态下加载/卸载其它外接设备，例如Moxa卡等
	CPU绑定	支持云主机在线/关机状态下将虚拟CPU（vCPU）与物理机的物理CPU（pCPU）严格关联，可为云主机分配特定的pCPU，提高云主机性能
	云主机性能优化	支持Linux云主机安装性能优化工具（GuestTools），主要用于安装agent，提供内部监控
		支持Windows/Windows Virtio云主机安装性能优化工具（GuestTools），主要用于安装agent，提供内部监控，并支持一键安装Virtio驱动，有效提升云主机磁盘/网卡性能
	User Data导入	支持创建云主机时导入User Data，通过上传自定义的参数或脚本，对云主机进行定制化配置或完成特定任务
	BIOS模式	创建云主机会继承所选镜像的BIOS模式，包括：Legacy、UEFI
		创建云主机镜像以及克隆云主机，将继承原云主机BIOS模式
		支持云主机在线/关机状态下修改BIOS模式
	云主机QGA开关	灵活控制QEMU Guest Agent的状态，开启后云主机默认支持在线修改密码

类别	特性	Cloud企业版 付费
	云主机RDP模式开关	针对VDI用户界面，开启后默认以RDP模式打开控制台
	网卡防欺诈模式	提供防IP/MAC伪造和ARP欺骗功能，开启后云主机只能使用平台分配的IP/MAC地址与外界通信
	实时性能监控	外部监控：由libvirt从物理机处获取云主机性能数据，包括：CPU、内存、磁盘IO、网卡
		内部监控：由agent从云主机处获取云主机性能数据，包括：CPU、内存、磁盘容量，使用内部监控需在云主机内预先安装agent
	云主机NUMA开关	开启后支持云主机在线修改计算规格（CPU/内存）
	云主机Hyper-V开关	支持云主机开启或关闭Hyper-V模拟（仅限Windows云主机）
	网卡多队列数目	对云主机网卡开启多队列驱动支持，将Virtio类型的网卡流量分配给多个CPU处理，有效解决云主机CPU处理网络中断的性能瓶颈问题
	云主机显卡切换	支持设置云主机启动时默认的显卡类型，包括：qxl、cirrus、vga（通过全局设置控制）
	审计	支持对云主机的所有操作行为审计，有效保障云环境安全
	自定义主列表	支持自定义云主机主列表的展示条目
	导出CSV文件	支持云主机列表导出为CSV表格，方便统计分析以及问题诊断
	资源删除保护	支持对云主机进行删除策略控制，包括：立刻删除、延时删除、永不删除，降低误操作风险
		UI界面对云主机删除提供保护机制，系统提醒删除后果，用户需确认后才能进行删除，降低误操作风险
云盘	批量操作	批量管理云盘
	创建云盘	提供多种策略创建云盘，高效利用资源
	云盘生命周期管理	支持云盘的创建、启用、停用、删除等基本生命周期管理
	加载/卸载实例	支持云盘加载实例/从实例卸载
	云盘迁移	支持云盘迁移至其它计算节点（仅支持本地存储）
		支持按目标计算节点负载高低迁移云盘
	存储迁移	支持云平台内跨同类型主存储迁移云盘，包括：Ceph主存储-Ceph主存储、NFS主存储-NFS主存储、Shared Block主存储-Shared Block主存储

类别	特性	Cloud企业版 付费
		支持未加载任何实例的云盘跨Ceph主存储-Ceph主存储迁移
		支持未加载任何实例的云盘跨NFS主存储-NFS主存储迁移
		支持未加载任何实例的云盘跨Shared Block主存储-Shared Block主存储迁移
		支持加载已关机实例的云盘（共享云盘除外）跨Shared Block主存储-Shared Block主存储整机迁移
		若已确保存储迁移后数据完整无损，可手动清理存储迁移保留的原始数据，释放存储空间
	更改所有者	支持云盘更换所有者
	云盘扩容	支持未加载任何实例的云盘扩容
		支持加载已开机/关机实例的云盘扩容
		支持未加载任何实例或加载已关机实例的共享云盘扩容（仅支持Ceph主存储）
	自定义标签	支持自定义云盘标签，方便快速查询定位资源
	云盘备份	云盘需加载已开机实例才能备份
		支持对云盘进行增量备份或全量备份
		该功能由灾备服务模块提供
	云盘镜像	基于当前云盘制作模板镜像，方便定制化批量创建云盘
		支持未加载任何实例的云盘创建云盘镜像
		支持加载已开机/关机实例的云盘创建云盘镜像
		在Shared Block主存储下，支持未加载任何实例或加载关机实例的共享云盘创建云盘镜像
	云盘快照	做重要操作前，对根云盘或数据云盘在特定时间点进行临时状态保留，方便出现故障后迅速回滚
		支持恢复云盘快照
		支持批量删除云盘快照
	设置云盘QoS	支持对云盘进行限速
	共享云盘	支持Ceph存储或Shared Block存储下创建共享云盘
	审计	支持对云盘的所有操作行为审计，有效保障云环境安全

类别	特性	Cloud企业版 付费
	导出CSV文件	支持云盘列表导出为CSV表格，方便统计分析以及问题诊断
	资源删除保护	支持对云盘进行删除策略控制，包括：立刻删除、延时删除、永不删除，降低误操作风险
		UI界面对云盘删除提供保护机制，系统提醒删除后果，用户需确认后才能进行删除，降低误操作风险
镜像	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
		添加镜像支持Legacy、UEFI两种BIOS模式
	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
	镜像校验	支持导出镜像校验值，导出镜像后，提供该导出镜像的MD5值，通过MD5验证下载后镜像的完整性
	镜像平台	支持设置镜像的平台操作系统类型
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
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，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、首选上次所在物理机、随机分配
		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
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

类别	特性	Cloud企业版 付费
	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
GPU规格	GPU规格	自动扫描云平台中可用的物理GPU规格和vGPU规格并统一管理，创建云主机时支持指定规格为云主机添加GPU设备
		通过GPU规格为云主机加载GPU设备时，支持关机自动卸载高级功能
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
	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
		支持弹性伸缩组周期策略，创建弹性伸缩组时可以选择按分钟/小时/天/周/月执行扩缩容策略
		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
		支持根据云主机外部监控条目CPU使用率、内存使用率进行触发；支持根据云主机内部采集的内存和CPU监控数据进行触发
	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
		支持通过监控报警和站内信的形式发送消息通知
快照	快照统一管理	对云主机/云盘快照统一管理，所有存在快照的云主机/云盘都将展示在快照页面，且支持按快照数量或总容量排序，方便用户快速识别需要清理的快照，提高运维效率
	批量快照	支持对云主机及所加载云盘创建快照组，支持以快照组为单位统一恢复云主机及其所加载云盘
		支持解绑快照组，将快照组恢复为单盘快照
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

类别	特性	Cloud企业版 付费
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
	高级设置	以集群为粒度，设置内存超分率、物理机保留内存、CPU超分率等全局设置
		集群支持启用大页模式，有效降低云主机CPU性能损耗
		zero copy，用于设置该集群的物理机是否开启zero copy功能
物理机	虚拟化	支持KVM虚拟化技术，支持VMware虚拟化
	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、磁盘IO、磁盘容量和网络运行数据，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）
	物理GPU透传	支持物理机GPU设备携带其上全部外设（包括：GPU显卡、GPU声卡、以及其它GPU上的小设备）以组为单位整体透传，让云主机拥有高性能计算和图形处理能力
	vGPU	同时支持NVIDIA和AMD显卡虚拟化切割成vGPU，通过指定规格和指定设备两种方式为云主机加载vGPU

类别	特性	Cloud企业版 付费
	SR-IOV	支持物理网卡SR-IOV配置，既能够继承网卡直通的高性能优势，又同时支持物理网卡设备的跨虚拟机共享
	PCI设备白名单	通过设置PCI设备白名单，可以支持如IB卡，FPGA卡等外接PCI设备透传给云主机使用
	USB透传	支持直连和转发方式USB透传，满足多种USB应用场景
	Intel EPT硬件辅助	支持关闭Intel EPT硬件辅助虚拟化，解决CPU型号过旧创建云主机故障的问题
	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和登录操作审计
	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
主存储	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
		支持设置云盘预分配策略，可以选择厚置备或精简置备
	NFS存储	支持云盘存放到NFS协议存储，物理机共享访问
		共享文件系统管理节点高可用方案
		支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用
		支持实时查看主存储已用容量百分比趋势图
	共享挂载存储	支持云盘存放到POSIX兼容的共享存储，支持iSCSI/FC存储
		共享文件系统管理节点高可用方案
		支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用
		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

类别	特性	Cloud企业版 付费
		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
		支持iSCSI透传，透传的块设备可直接加载到云主机使用
		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
	Ceph存储	支持共享云盘
		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
		Ceph类型的主存储可通过添加pool扩容，支持指定pool创建云主机/云盘
		支持实时查看主存储已用容量百分比趋势图
		对接企业版Ceph，支持存储许可证服务有效期提醒
	多主存储支持	同一集群支持挂载多个本地存储
		同一集群支持挂载多个NFS存储
		同一集群支持挂载多个Shared Block存储
		同一集群支持挂载一个本地存储和一个NFS/SMP/Shared
		同一集群支持挂载一个Ceph存储和多个Shared Block存储
镜像服务 器	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

类别	特性	Cloud企业版 付费
	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
		同一管理节点下不同镜像仓库间支持镜像同步
	镜像仓库清理	可视化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
网络资源	二层网络	与本地存储、NFS、SMP、Ceph、Shared Block类型的主存储无缝支持
		支持VLAN二层隔离，VLAN 802.1q作为网络隔离手段
		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
		支持修改Vni名称。用户可自定义已创建的Vni名称，也可在创建Vni范围时设置Vni名称
	分布式扁平网络	支持硬件VXLAN网络，通过添加SDN控制器，可在云平台接管硬件交换机的SDN网络，降低网络延迟的同时提升VXLAN网络性能
		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

类别	特性	Cloud企业版 付费
		支持使用扁平网络创建负载均衡，通过流量分发扩展应用系统对内的服务能力
		负载均衡支持TCP/HTTP/HTTPS/UDP协议，支持TCP/UDP、http健康检查，
		负载均衡支持轮询、最小链接、源地址哈希和加权轮询算法
		负载均衡支持黑白名单，为负载均衡提供监听级别的访问控制
	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
		创建三层网络时，支持为DHCP服务指定IP地址，防止网络规划过程中IP冲突
	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
	MTU	自定义限制网络传输数据包的大小
	自定义网关	IP范围方式添加网络段支持自定义指定网关
		CIDR方式添加网络段支持自定义指定网关，使用CIDR的第一个或最后一个地址作为网关
	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、启动、停止、重启、迁移、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
		支持自定义开启或关闭SNAT网络服务
		支持OSPF动态路由协议
		支持组播功能，可将组播源发送的组播消息转发给云主机
		支持分布式路由高级功能，优化东西向流量
		创建单个VPC路由器支持指定默认IP
		默认VPC路由器的资源优先级高于云主机，优先保证VPC路由器的资源使用
		支持多运营商线路源进源出，大大提升了网络传输的效率

类别	特性	Cloud企业版 付费
		支持通过设置上行带宽和下行带宽的方式，设置该VPC路由器的QoS
		支持指定物理机创建VPC路由器
	VPC路由器高可用组	支持VPC路由器高可用功能，一个VPC路由器高可用组内部署一对互为主备的VPC路由器
		当主VPC路由器状态异常，秒级触发高可用切换，自动切换至备VPC路由器工作，保障业务持续稳定运行
		创建VPC路由器高可用组支持指定虚拟IP
	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
		支持为网络服务提供虚拟IP，用于内部私网的负载均衡网络服务
		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，支持TCP/UDP、http健康检查
		负载均衡支持轮询、最小链接、源地址哈希和加权轮询算法
		负载均衡支持黑白名单，为负载均衡提供监听级别的访问控制
		图形用户界面支持负载均衡器的即时流量监控
		支持添加IPv4、IPv6类型的网络
	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TCP/UDP、http健康检查
		负载均衡支持轮询、最小链接、源地址哈希和加权轮询算法
		负载均衡支持黑白名单，为负载均衡提供监听级别的访问控制

类别	特性	Cloud企业版 付费
		图形用户界面支持负载均衡器的即时流量监控
		支持基于云路由的IPsec隧道服务
		支持多个弹性IP绑定同一个云主机网卡
		支持一个云路由器接多个公有网络
		支持配置静态路由表
		支持分布式DHCP提升服务性能
	IP统计	支持在UI界面查看三层网络（私有网络、公有网络、VPC网络）的IP使用情况
		三层网络IP统计详情页，用户可快速查看已用IP及其关联资源，以及未被占用IP情况，从而提高IP规划效率
网络服务	安全组	支持基于TCP/UDP端口的安全策略
		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
	虚拟IP	支持对虚拟IP做QoS限制，对网络服务的高效分配管理
	负载均衡	性能共享性负载均衡提供基于路由器的负载均衡服务
		高性能实例型负载均衡更提供负载均衡实例节点，以虚机方式提供负载均衡服务
	防火墙	支持对VPC路由器配置防火墙，VPC防火墙创建后，路由器网卡的入方向将增加默认的系统规则集以保证业务正常运行，网卡的出入方向规则均可自由配置
		规则集是一组规则的集合，可与多个防火墙绑定实现规则的复用
		支持通过规则模板实现规则的快速创建
		IP集合和端口集合可简化规则创建的输入复杂度
		每条规则最多支持填写10条IP条目，减少规则配置的复杂度，提升功能易用性
	Netflow	VPC路由器新增Netflow网络服务，支持通过Netflow对VPC路由器网卡的进出流量进行分析监控
		支持Netflow V5、V9两种数据流输出格式

类别	特性	Cloud企业版 付费
	端口镜像	通过镜像端口对获取到的业务报文进行分析，方便企业对内部网络数据进行监控管理，快速定位网络故障
		支持配置独立的流量网络用于端口镜像传输数据
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User Data
		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
网络拓扑	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
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，指定所有者范围，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，指定所有者范围，对路由器CPU使用率、内存使用率、磁盘读速度、磁盘写速度、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	物理机性能统计	支持自定义时间段查看，指定资源范围，对物理机CPU使用率、内存使用率、磁盘读速度、磁盘写速度、磁盘用量、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

类别	特性	Cloud企业版 付费
	虚拟IP性能分析	支持自定义时间段查看，指定资源范围，指定所有者范围，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
容量管理	容量管理	提供统一视角查看平台物理资源使用状况，同时多维度展示资源占用TOP10
监控报警	大屏监控	多款华丽主题的大屏实时展示平台资源情况
		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
	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
		首页支持按时间段查看物理机负载可视化图形
	报警	通过丰富的报警条目，提供对云主机、路由器、镜像、镜像服务器、系统数据目录、物理机、三层网络、云盘、虚拟IP、主存储、监听器和项目资源等多种资源进行监控报警
		提供常用默认报警器，并支持用户对时序性数据和事件自行设置报警器，实时监控基础资源状态
		一键报警，提供一键开启/关闭监控报警服务，简化告警服务，快速建立关键资源报警服务
		资源分组，支持批量资源的划分，用户可按业务线划分集中管理某一类资源，结合报警模板使用提升运维效率
		报警模板，一组报警规则的集合，可应用于资源分组，实现批量管理报警规则
		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

类别	特性	Cloud企业版 付费
		报警消息收敛，事件报警消息策略调整为仅提示一次；资源报警器中报警周期类型新增一次选项，用户可根据自己的需求，灵活配置报警策略
		报警消息支持已读未读状态提示，方便用户快速定位问题
		报警恢复后支持消息提示
		报警消息支持中英双语，更加易读易懂，方便快速定位问题
		支持创建报警器自定义报警级别，方便云平台用户关注最紧急的报警消息
	多接收端	支持邮件/钉钉/HTTP应用/阿里云短信/Microsoft Teams等多种接收端
		邮箱接收端和阿里云短信接收端支持添加多个接收端地址
	报警消息模板	将报警消息推送至多种接收端时，可为各个接收端自定义报警消息的模板
	第三方消息纳管	支持将第三方平台（消息源）的报警消息添加至云平台进行纳管，添加消息源后将在云平台收到报警提示
		支持将第三方消息推送至各个接收端，进行消息的接收和查看
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
		支持用户按需配置日志保留时间
		支持展示执行任务的事件审计和登录操作审计
		全局设置支持对管理节点日志保留时间以及保留容量进行按需设置
		上传镜像、上传路由器镜像操作中断后支持从中断处进行续传
审计	资源审计	支持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
定时运维	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

类别	特性	Cloud企业版 付费
		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
标签管理	资源标签	自定义创建不同名称/颜色的标签，并绑定到云主机、云盘、物理机和裸金属，方便资源管理和资源搜索
		资源标签支持按绑定时间或名称进行排序
计费管理	自定义计费单价	支持自定义CPU、GPU、内存、系统云盘、数据云盘、公网IP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
	基于磁盘性能计费	不同类型的磁盘支持单独设置计费单价
	计费货币符号	支持对计费货币符号进行全局设置，支持的货币单位包括：人民币 ¥、美元 \$、欧元 €、英镑 £、澳元 A\$、港元 HK\$、日元 ¥、瑞士法郎 CHF、加拿大元 C\$
	账单	按计费单价和使用时间来统计并显示admin和所有租户的资源费用信息
		支持项目账单、部门账单（项目加载到部门）、账户账单
		系统默认全部账单每天零点生成一次，账单生成时间可通过全局设置修改
访问控制	AccessKey管理	生成可供其他平台调用API权限的AccessKey，且AccessKey具有该创建者完全的权限
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
子账户管理	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

类别	特性	Cloud企业版 付费
	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	支持二层网络和三层网络资源共享特性，可指定账户是否可使用
	全局配置	管理员可以直接在UI上对各种特性进行全局配置
		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
		支持全局配置场景化封装，基于用户实际生产场景需求，提供场景化的一键全局设置，方便快速将云平台设置为所需状态，提高运维效率
	修改admin账户密码	忘记admin账户的登录密码，可以使用zstack reset_password
		还原默认值
主题外观	主题外观	支持更改云平台主题色
		支持修改云平台UI图标及文字标题
日志服务器	日志服务器	通过该日志服务器，用户可便捷收集硬件资源系统日志，快速定位问题，提高云平台运维效率
平台设置	场景封装	基于实际生产场景需求，提供场景化的一键全局设置，方便快速将云平台设置为所需状态
	全局设置	基本设置涵盖日常生产运维中常用的全局设置
许可证管理	云平台许可证	云平台许可证（Base License）提供云平台的核心功能，可满足用户主流业务场景需求
		支持本地浏览器上传许可证
		支持许可证到期提醒
		企业单机免费试用版支持所有功能
		支持CPU授权、Host授权、VM授权三种授权方式

类别	特性	Cloud企业版 付费
	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
		包括：企业管理模块、VMware管理模块、弹性裸金属模块、阿里云混合云模块、裸金属管理模块、灾备服务模块、迁移服务模块、ARM64服务器管理、售后服务 (5x8、7x24)
		支持本地浏览器上传许可证
		许可证到期提醒
	CPU架构许可证	支持x86服务器架构许可证类型，支持区分KVM和vCenter为计算节点提供独立的CPU授权
		支持ARM64服务器管理许可证类型，提供计算服务
		支持MIPS服务器管理许可证类型，提供计算服务
	上传许可证	根据需求自由打包许可证，统一上传
	许可证授权记录	支持在UI查看云平台的历史授权信息
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
登录方式	TUI	支持常用运维操作，定制化OS界面
	图形界面	支持以HTTP/HTTPS方式访问图形界面的云管理平台，账户（用户名密码方式或AD/LDAP方式）和用户支持图形界面登录访问
	命令行	支持通过命令行方式访问云管理平台，命令行支持全功能访问，账户和用户支持命令行登录访问
	API接口	支持全功能的API交付，API支持消息总线访问和HTTP接口访问

类别	特性	Cloud企业版 付费
登录安全	登录安全	支持动态验证码验证，多次登录（6次）失败触发验证码验证，防止恶意登录
		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
		支持设置登录密码复杂度，用户可自定义设置密码长度范围，并使用数字、大小写和特殊字符组合的密码策略
		支持设置密码有效期，用户可自定义设置密码更新周期。建议定期修改云平台登录密码，保障登录安全
		支持设置历史密码检查，用户可自定义设置密码不重复次数
		支持设置锁定机制检查，用户可自定义设置连续登录失败次数上限、以及连续登录失败锁定用户时长；当连续登录失败次数超过设置值，用户账户将被锁定一段时间，保障登录安全
		支持登录IP黑白名单，用户可按需配置IP黑白名单，从而实现访客身份的识别和过滤，提升云平台访问控制安全
		支持开启同一用户禁止多会话策略，同一账户只允许存在一个会话连接，满足用户对特殊安全性场景的需求
		支持设置默认登录链接访问的登录界面，使登录入口更加清晰明了
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
全局搜索	云平台全信息搜索	支持搜索包括功能入口、所创资源、内置文档等在内的所有内容
操作助手	智能提示	对云平台核心操作给出智能的环境检查和操作指导
管理节点	多物理机管理节点高可用	支持多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，支持分别为主备管理节点添加许可证
		多管理节点高可用环境支持管理节点高可用监控与健康状态查询，并提供仲裁IP不可达、双管理节点数据库不同步默认资源报警器
	管理节点	管理节点支持不同版本源文件共存
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

类别	特性	Cloud企业版 付费
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
		支持企业版管理节点、社区版管理节点、计算节点、专家模式和精简专家模式多种安装模式
升级	无缝升级	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	支持指定只升级部署环境，通过专家模式自定义安装升级

VMware管理模块 功能列表

类别	特性	Cloud VMware管理模块
vCenter	管理vCenter	<p>通过VMware提供的公开API接口，接管多个VMware vCenter。良好地兼容和管理VMware vCenter Server虚拟化管理平台部分功能，实现多虚拟化平台的统一管理。</p> <ul style="list-style-type: none"> 支持接管VMware vCenter Server管理的vSphere服务器、云主机、云盘、镜像资源，并支持在虚拟数据中心对接管的资源执行常用操作 支持以vCenter为单位查看云主机、云盘、镜像等资源 支持手动同步全部/某个vCenter数据，保证信息一致性 支持全局设置中配置vCenter自动同步数据，配置完成后支持周期性自动同步全部vCenter数据
	vCenter多租户管理	<p>租户（普通账户/项目成员）支持管理已接管vCenter中的资源。</p> <ul style="list-style-type: none"> 租户支持对已接管vCenter中的云主机、云盘资源执行常用操作 租户支持使用admin共享的vCenter网络、镜像资源 租户视角的首页界面支持分别展示KVM和vCenter云主机的使用量 租户视角支持分别展示KVM和vCenter账单信息 项目成员支持通过工单审批方式申请vCenter云主机
	vCenter资源池	<ul style="list-style-type: none"> 已接管vCenter支持同步资源池及相关云主机信息，以层级形式展示 支持显示资源池的CPU容量限制、内存容量限制等资源配额信息

类别	特性	Cloud VMware管理模块
	ESX云主机	<ul style="list-style-type: none"> 支持ESX云主机相关生命周期管理，包括：创建、启动、停止、重启、暂停、恢复、关闭电源、删除 支持ESX云主机相关常规操作，包括：迁移、克隆、修改计算规格、设置高可用、打开控制台、设置控制台密码
	网络	<ul style="list-style-type: none"> 支持基于vSwitch/dvSwitch交换机创建网络 支持创建公有网络和私有网络，其中私有网络包括扁平网络、云路由两种类型 云路由支持所有网络服务，包括：虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道等
	存储	支持按datastore区分主存储和镜像服务器
	镜像	支持镜像相关生命周期管理，包括：添加、删除、启用、停用
	物理机	支持物理机相关生命周期管理，包括：维护模式
	云盘	支持云盘相关生命周期管理，包括：创建、删除、加载、卸载
	实时性能监控	采集ESX云主机CPU、内存、存储和网络相关数据，可视化方式实时显示性能监控图表

企业管理模块 功能列表

类别	特性	Cloud 企业管理模块
组织架构	用户	<ul style="list-style-type: none"> 用户是企业管理中的最基本单位 admin/平台成员可创建用户，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、邮箱地址和编号等 支持手动添加和模板导入两种方式创建用户，其中模板导入方式支持将用户的组织架构关系以及所属项目信息同步导入
	组织架构	<ul style="list-style-type: none"> 组织架构是企业管理中的基本单位，admin/平台管理员可以看到云平台所有组织架构树，普通平台成员/项目成员仅能看到所属组织架构架构树

类别	特性	Cloud 企业管理模块
		<ul style="list-style-type: none"> 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 弱化部门负责人与部门的绑定关系，允许部门不设置部门负责人 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
	角色	<ul style="list-style-type: none"> 角色表示权限的集合，为用户赋予权限可获得调用相关API进行资源操作的能力 企业管理租户与角色分离，角色可灵活绑定到企业管理租户或从企业管理租户解绑，分为系统角色和自定义角色 图形用户界面对企业管理租户进行API级别的权限控制，灵活适配各种场景的权限配置需求 允许超级管理员（admin）/平台管理员/普通平台成员对项目成员（项目负责人/项目管理员/普通项目成员）进行权限管理 平台管理员以用户形式存在，绑定平台管理员角色即可赋予身份并赋予相应的权限 提供平台管理员角色、项目负责人角色、项目管理员角色、监控大屏角色系统角色。其中，绑定监控大屏角色的用户仅拥有监控大屏查看权限，登录即可跳转到监控大屏界面
	第三方认证	<ul style="list-style-type: none"> 支持添加AD/LDAP服务器，成功添加ADLDAP服务器后，自动化批量导入第三方用户/组织（仅AD支持）至云平台 支持设置用户映射和组织映射（仅AD支持），根据配置的映射规则同步第三方用户/组织架构（仅AD支持） 支持自定义过滤规则，过滤不需要同步的用户
项目管理	项目	<ul style="list-style-type: none"> 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、加载部门、卸载部门

类别	特性	Cloud 企业管理模块
		<ul style="list-style-type: none"> 弱化项目负责人与项目的绑定关系，允许项目不设置项目负责人。 支持通过回收日期、费用阈值回收项目 支持使用官方提供的脚本批量创建项目
	项目模板	<ul style="list-style-type: none"> 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
	项目成员	<ul style="list-style-type: none"> 项目成员作为项目的基本组成人员，一般由admin/平台成员/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/平台成员/项目负责人/项目管理员进行相应控制
	成员组	<ul style="list-style-type: none"> admin/平台成员/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 支持以成员组为单位赋予角色，进行权限控制
	设置QoS	<ul style="list-style-type: none"> admin/平台成员可以对云主机、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 控制QoS设置范围，普通账户/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	<ul style="list-style-type: none"> 项目成员（项目负责人/项目管理员/普通项目成员）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	<ul style="list-style-type: none"> 支持admin或项目负责人通过并部署工单以及驳回工单 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或项目负责人进行一键审批，审批通过后，资源可自动部署成功并分发到项目中
	自定义流程管理	<ul style="list-style-type: none"> 支持admin为不同项目设置不同类型的自定义工单流程

类别	特性	Cloud 企业管理模块
		<ul style="list-style-type: none"> 支持多种工单类型，包括：申请云主机、删除云主机、修改项目周期、修改云主机配置、修改项目配额 自定义工单流程支持将项目成员添加到各审批环节 支持启用、停用、修改、删除自定义工单流程
独立区域管理	平台管理员	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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

灾备服务模块 功能列表

类别	特性	Cloud 灾备服务模块
灾备服务	备份	<ul style="list-style-type: none"> 支持为云主机、云盘和管理节点数据库创建备份任务，其中支持云主机的整机备份 支持对当前备份任务进行统一直观展示，方便用户快速掌控当前备份任务整体情况，提高管理运维效率 通过优化大文件备份机制，大幅提升了大文件备份性能，并且支持物理带库和虚拟带库 支持用户按周/天/小时为任务设置备份策略，已创建的备份任务支持更新备份策略 可按数量或时间保存备份文件数据 创建备份任务后支持立即备份及定时全量备份数据 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，支持主备无缝切换

类别	特性	Cloud 灾备服务模块
		<ul style="list-style-type: none"> 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和过期的临时数据，释放存储空间 备份任务支持设置磁盘QoS和网络QoS 备份任务支持查看备份进度 添加已有备份服务器，支持自动获取备份数据 支持对备份任务创建事件报警器，当备份任务执行失败，用户会在接收端接收到备份任务执行失败的报警详情
	还原	<ul style="list-style-type: none"> 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 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

迁移服务模块 功能列表

类别	特性	Cloud 迁移服务模块
迁移服务	迁移服务器	<ul style="list-style-type: none"> 迁移服务器与所征用物理机状态解耦。当迁移服务器为启用状态但所征用物理机为停用状态时，该迁移服务器将作为V2V迁移场景专用，其它业务云主机不会被调度至该迁移服务器上，有效提升迁移效率 迁移服务器支持设置单独的迁移网络，用于从源主存储迁移至迁移服务器的数据转化 迁移服务器支持实时容量监控，可选择不同的时间跨度来监控迁移服务器已使用容量百分比 支持展示迁移服务器总容量以及可用容量
	V2V迁移 (VMware)	<ul style="list-style-type: none"> 将已接管的vCenter云主机迁移至当前云平台

类别	特性	Cloud 迁移服务模块
		<ul style="list-style-type: none"> 支持对云主机进行一键式批量的V2V迁移，迁移后置备方式保持不变 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 安全又节省资源的迁移服务，迁移过程中的文件在源主存储中压缩保存 支持迁移的源vCenter平台版本包括：5.0、5.1、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、SLES 11/12/15、Ubuntu 12/14/16/18、Windows 7/2003/2008/2012/2016 源主存储类型无限制；目标主存储支持Ceph、SharedB lock、NFS和本地存储类型
	V2V迁移 (KVM)	<ul style="list-style-type: none"> 不需要接管，即可将云主机从KVM云平台在线迁移至当前云平台 运行、暂停状态的云主机均支持V2V迁移 (KVM) V2V迁移 (KVM)不限制主存储类型 迁移过程支持同时迁移加载的数据云盘，支持修改CPU、内存 迁移过程不同时迁移云主机快照 源主存储类型无限制；目标主存储支持Ceph、SharedB lock、NFS和本地存储类型

裸金属管理模块 功能列表

类别	特性	Cloud 裸金属管理模块
裸金属管理	裸金属集群	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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 支持独立部署PXE服务器
	裸金属设备	<ul style="list-style-type: none"> 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 可根据填写的网络段批量添加裸金属设备

类别	特性	Cloud 裸金属管理模块
		<ul style="list-style-type: none"> 支持通过模板导入方式批量添加裸金属设备 支持从控制台打开裸金属设备的IPMI管理界面（登录界面），输入已配置好的IPMI用户名和IPMI密码，即可登录
	裸金属主机	<ul style="list-style-type: none"> 支持使用ISO类型镜像为裸金属设备安装Linux操作系统 支持Ubuntu、CentOS、suse操作系统无人值守安装 支持为裸金属主机添加网络配置 支持内部负载实时监控（需安装agent），可查看裸金属主机CPU、内存、磁盘、网卡的各项性能指标 提供裸金属主机CPU、内存、磁盘、网卡相关监控条目 支持对裸金属主机资源定制化创建标签（仅支持管理员标签），并通过标签快速检索裸金属主机

弹性裸金属模块 功能列表

资源	功能介绍
部署网络	<p>创建弹性裸金属实例时，用于PXE流程及下载镜像的专属网络。</p> <ul style="list-style-type: none"> 将部署网络加载到弹性裸金属集群，为弹性裸金属集群中裸金属节点提供PXE服务。 支持IPv4类型的部署网络。 部署网络支持设置网关，若部署网络需要连接其他网络时可按需配置；若不需要连接其他网络，可暂时不用配置。
弹性裸金属集群	<p>为裸金属节点提供单独的集群管理。</p> <ul style="list-style-type: none"> 弹性裸金属集群和部署网络采用一对多关系，即一个弹性裸金属集群只允许加载一个部署网络；一个部署网络支持加载到多个弹性裸金属集群。 弹性裸金属集群支持加载二层网络，为集群中弹性裸金属实例提供大二层业务网络。同一二层网络上的弹性裸金属实例和云主机之间可以互相访问，无需通过网关进行路由。目前支持VLAN和NoVLAN类型的二层网络。 支持添加的主存储包括：Shared Block主存储、Ceph主存储。
网关节点	<p>云平台 and 弹性裸金属实例的流量转发节点。</p> <ul style="list-style-type: none"> 支持通过网关节点接管主存储，并为弹性裸金属实例分配主存储。 提供iPXE服务、DHCP服务等，可通过网关节点为弹性裸金属实例下发配置。

资源	功能介绍
	<ul style="list-style-type: none"> 裸金属集群和网关节点采用一对多关系。即一个弹性裸金属集群支持加载多个网关节点，但一个网关节点只能加载到一个弹性裸金属集群。
裸金属节点	<p>用于创建弹性裸金属实例，通过BMC接口以及IPMI配置进行唯一识别。</p> <ul style="list-style-type: none"> 支持添加任意x86架构的服务器作为裸金属节点。 支持按裸金属节点或按裸金属规格为弹性裸金属实例提供计算资源。 支持关机释放裸金属节点。弹性裸金属实例停止时自动释放弹性裸金属节点，供其他弹性裸金属实例使用，避免资源闲置。 裸金属节点和弹性裸金属实例——对应。即一台裸金属节点只能同时分配给一个弹性裸金属实例使用，一个弹性裸金属实例只能分配到一台弹性裸金属节点。
弹性裸金属实例	<p>性能媲美物理服务器的云实例，结合云平台中资源的弹性优势，可实现灵活申请，按需使用。</p> <ul style="list-style-type: none"> 支持常规生命周期管理，例如：启动、停止、重启、关闭电源等操作。 支持类似云主机的高级操作，例如：打开控制台、绑定标签、修改弹性裸金属实例密码、更换系统等。 支持回收站功能，已删除的弹性裸金属实例将移动到回收站，可按需恢复或彻底删除。为敏感操作提供保护，避免误操作带来的数据丢失风险。 支持使用云平台中的虚拟网络作为业务网络，包括：公有网络、扁平网络、VPC网络。 支持使用VPC网络提供的弹性IP网络服务。 支持使用云平台中的Shared Block主存储来存储数据，可使用虚拟云盘作为系统盘和数据盘。 支持在线快照功能。做重要操作前在特定时间点对弹性裸金属实例系统盘进行临时状态保留，方便出现故障后迅速回滚。 支持创建镜像操作。为弹性裸金属实例创建镜像，可用于创建新的弹性裸金属实例。 默认支持使用BIOS模式为UEFI的镜像创建弹性裸金属实例，支持手动修改为Legacy模式。 弹性裸金属实例支持监控报警功能。安装agent的弹性裸金属实例支持可视化实时查看CPU、内存、磁盘、磁盘容量、网卡相关监控图表。方便用户排查故障，提高运维效率。

资源	功能介绍
	<ul style="list-style-type: none">弹性裸金属实例支持负载均衡网络服务和防火墙网络服务。例如：负载均衡服务支持选择弹性裸金属实例作为后端服务器；防火墙规则对相关三层网络下的弹性裸金属实例生效。

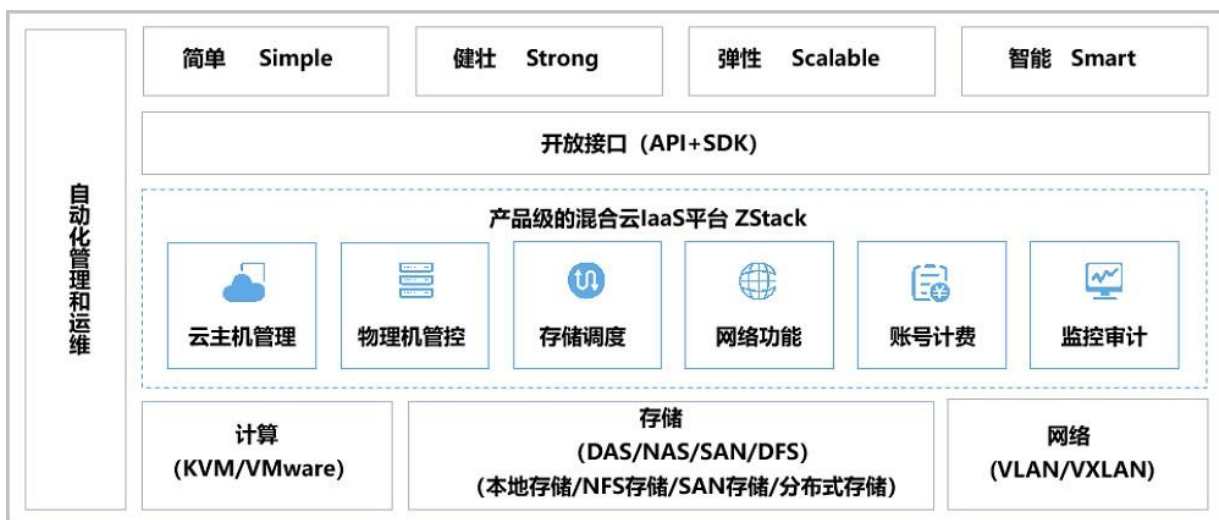
4 系统架构

Cloud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。

4.1 Cloud功能架构

Cloud功能架构如图 1: Cloud功能架构所示:

图 1: Cloud功能架构



Cloud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。

Cloud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。Cloud还提供了Java和Python的SDK，且支持RESTful APIs进行资源调度管理。基于Cloud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。

Cloud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。

- Cloud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。

- Cloud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。
- Cloud采用的插件机制，给每个插件设置相应的代理程序。Cloud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，Cloud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Cloud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。

- Cloud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。
- Cloud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。
- Cloud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。
- Cloud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。
- Cloud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。

- Cloud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。

- Cloud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。
- Cloud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。
- Cloud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。

- Cloud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。

- Cloud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。

- Cloud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Cloud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。

- Cloud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。

- Cloud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。

4.2 Cloud资源结构

Cloud在本质上是云资源的配置管理系统。

Cloud主要包括以下资源：

- 区域：Cloud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。VXLAN Pool支持软件SDN、硬件SDN两种类型。
- 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、HardwareVxlanNetwork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Cloud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VPC防火墙、安全组、虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道、流量监控等。
- VPC防火墙：负责管控VPC网络的南北向流量，通过配置规则集和规则来管控网络的访问控制策略。
- 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。
- 路由器规格：定义路由器使用的CPU、内存、路由器镜像、管理网络、公有网络等。
- VPC路由器：基于路由器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。提供各种网络服务，包括：DHCP、DNS、SNAT、路由表、弹性IP、端口转发、负载均衡、IPsec隧道、动态路由、组播路由、VPC防火墙、Netflow等。

Cloud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。

Cloud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。

Cloud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，Cloud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。

5 网络配置

Cloud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

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。

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。

业务网络：

- 计算节点和镜像服务器之间进行数据通讯的网络。
- 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服务器。

2. NAS/SAN +路由器网络架构

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Cloud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。

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。

业务网络：

- 计算节点和镜像服务器之间进行数据通讯的网络。
- 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，云主机可以通过路由器访问互联网，路由器网络使用路由器来提供各种网络服务，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，管理网络和业务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服务器。

3. Ceph+VXLAN路由器网络架构

此架构支持以下特性:

- 云主机数据存放在分布式存储，数据通过多副本或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。

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。
- 云主机可以通过路由器访问互联网，路由器网络使用路由器来提供各种网络服务，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

此架构支持以下特性:

- 云主机数据存放在分布式存储，数据通过多副本或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。

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。

业务网络：

- 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，管理网络和业务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。

6 安装部署

6.1 环境准备

前提条件

安装/升级Cloud需使用Cloud定制版ISO，特性如下：

1. Cloud定制版ISO提供以下两个版本：

- c76版：Cloud-x86_64-DVD-4.1.3-c76.iso
- c74版：Cloud-x86_64-DVD-4.1.3-c74.iso



注：

- c76在继承c74所有特性的基础上，使用更新的操作系统内核，并支持NVIDIA vGPU功能。
 - **初次安装Cloud，推荐安装c76 ISO。**如已部署Cloud云平台，可同版升级至最新版本，详情请参考《升级教程》。
2. 安装Cloud无需连接公网，也无须配置yum源，可完全离线安装。
3. 提供以下几种安装模式：企业版管理节点模式、计算节点模式、专家模式，用户请按需选择。
4. 默认选项：**DATE&TIME**为亚洲东八区，**LANGUAGE**为English(United States)，**KEYBOARD**为English(US)。

c74 ISO与c76 ISO的初始安装步骤基本相同，本教程以初装c76 ISO为例进行介绍，分为以下流程：

1. 准备文件。
2. 写入镜像。
3. 安装操作系统。

操作步骤

1. 准备文件。

安装Cloud前，请准备以下软件包，以便安装部署过程顺利执行：

- Cloud定制版ISO：
 - 软件名称（C76）：Cloud-x86_64-DVD-4.1.3-c76.iso
 - 下载地址：请联系官方技术支持获取

- Cloud安装包：
 - 软件名称：Cloud-installer-4.1.3.bin
 - 下载地址：请联系官方技术支持获取



注：软件下载后，请通过MD5校验工具核对校验码，以确保软件完整无损。

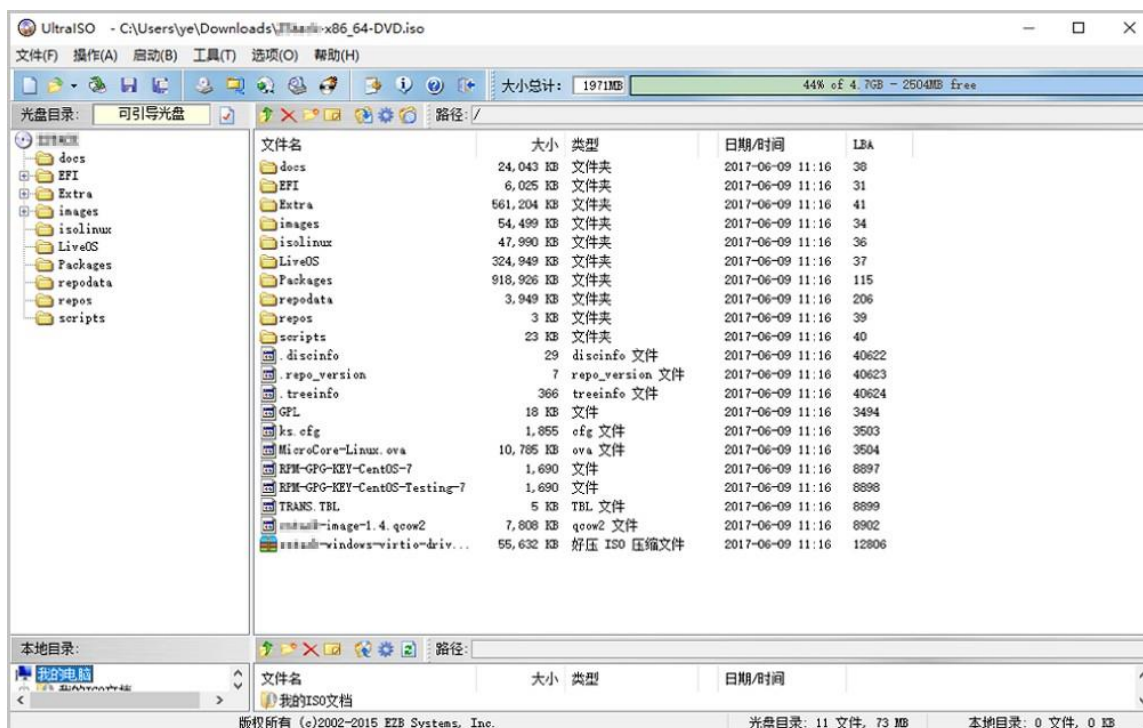
2. 使用UltraISO，将此ISO镜像刻录到U盘。

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 2: 在UltraISO打开ISO镜像所示：

图 2: 在UltraISO打开ISO镜像

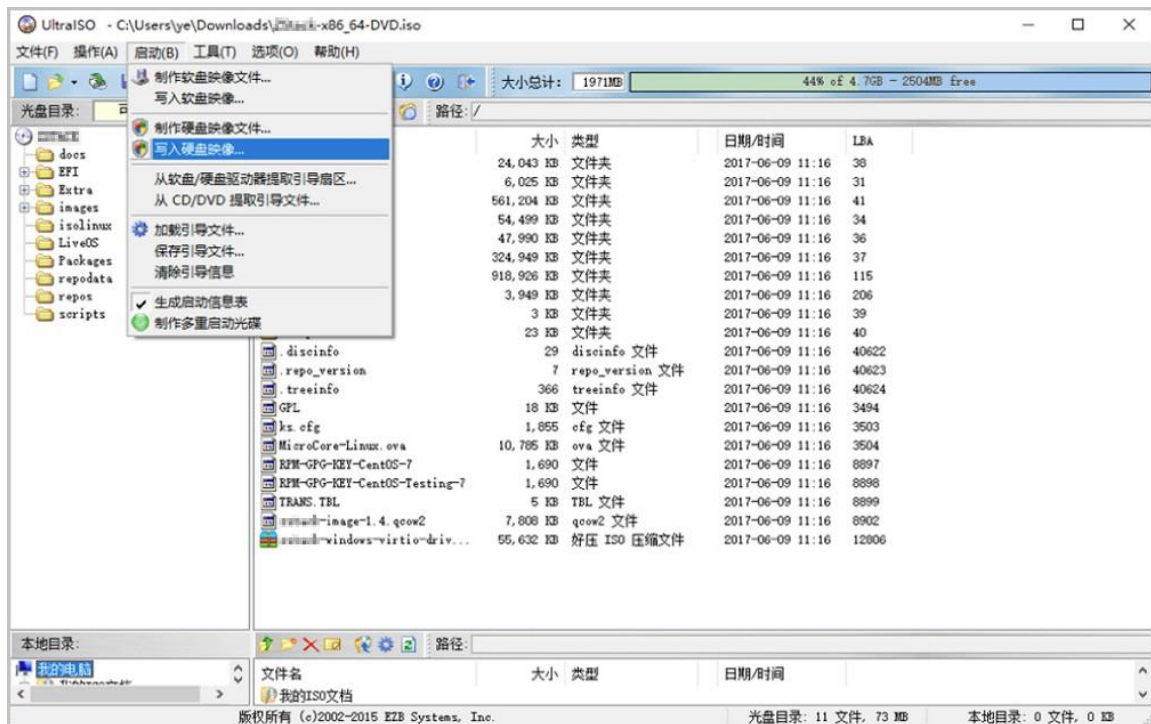


b) 写入镜像。

在UltraISO，点击**启动 > 写入硬盘映像**。

如图 3: 在UltraISO写入硬盘映像所示：

图 3: 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 4: 在UltraISO确认写入ISO镜像所示:

图 4: 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) 配置服务器。

- 确认服务器内硬盘的数据已备份，安装过程会覆盖写入。
- 进入BIOS，开启CPU VT和超线程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。
- 设置系统启动盘为第一启动顺序。

b) 选择引导项。

进入ISO系统引导界面，选择默认选项开始安装操作系统。



注:

- Cloud提供以下安装方式：图形界面方式、VNC方式和字符安装方式，用户可根据实际情况选择，建议使用图形界面安装。
- 若服务器无VGA接口，仅支持串口连接，用户可使用VNC方式或字符安装方式。

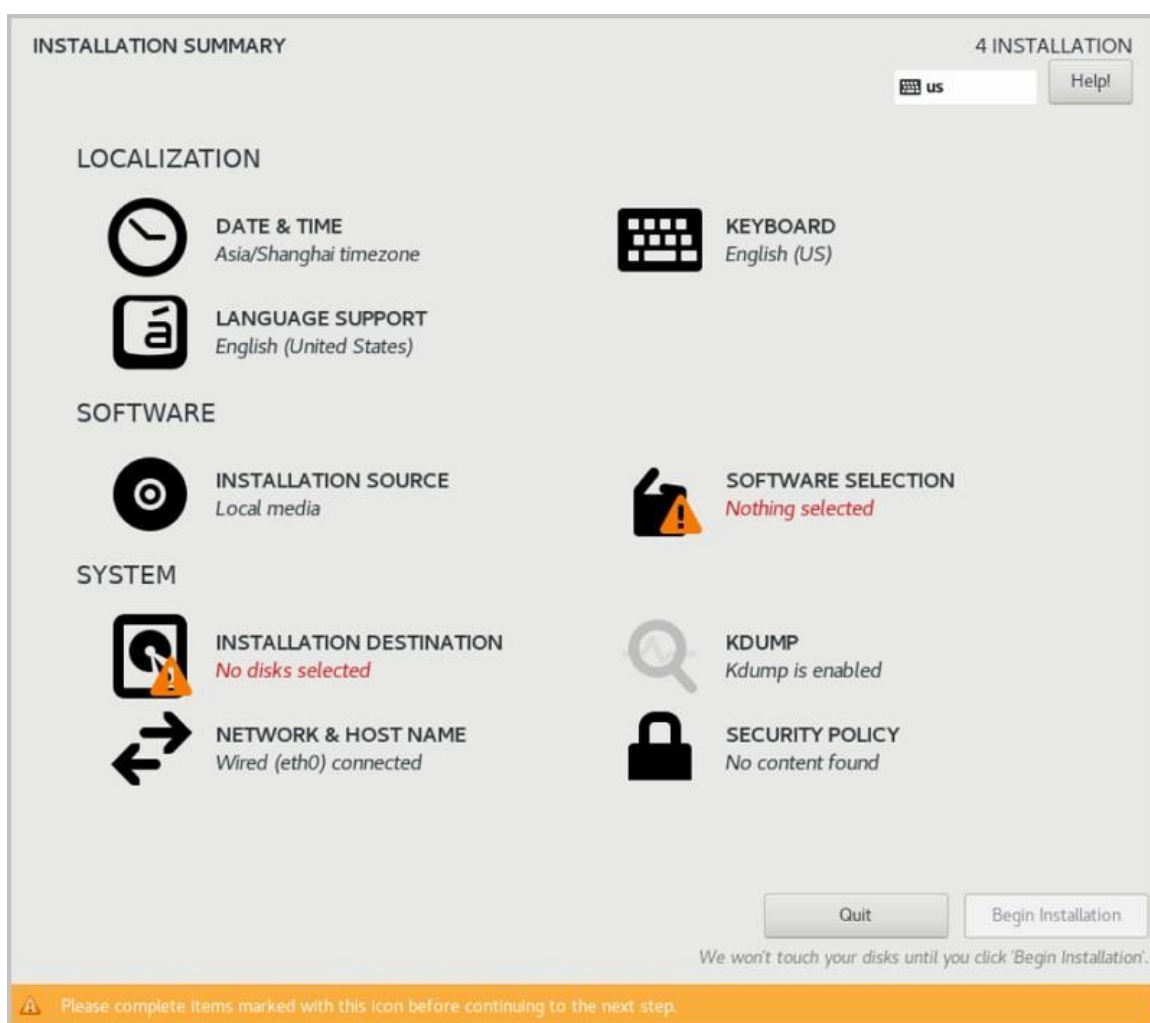
c) 安装配置汇总。

该页面展示系统安装配置，用户可按需修改，Cloud默认已配置以下内容：

- **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 5: 系统安装界面所示：

图 5: 系统安装界面



d) 选择安装模式。

在**安装配置汇总**界面，点击**SOFTWARE SELECTION**，进入**安装模式选择**界面，选择安装模式。

Cloud包含以下安装模式：

- Cloud Enterprise Management Node：企业版管理节点模式



注：首次安装建议选择此模式。

- Cloud Compute Node：计算节点模式
- Cloud Expert Node：专家模式



注：

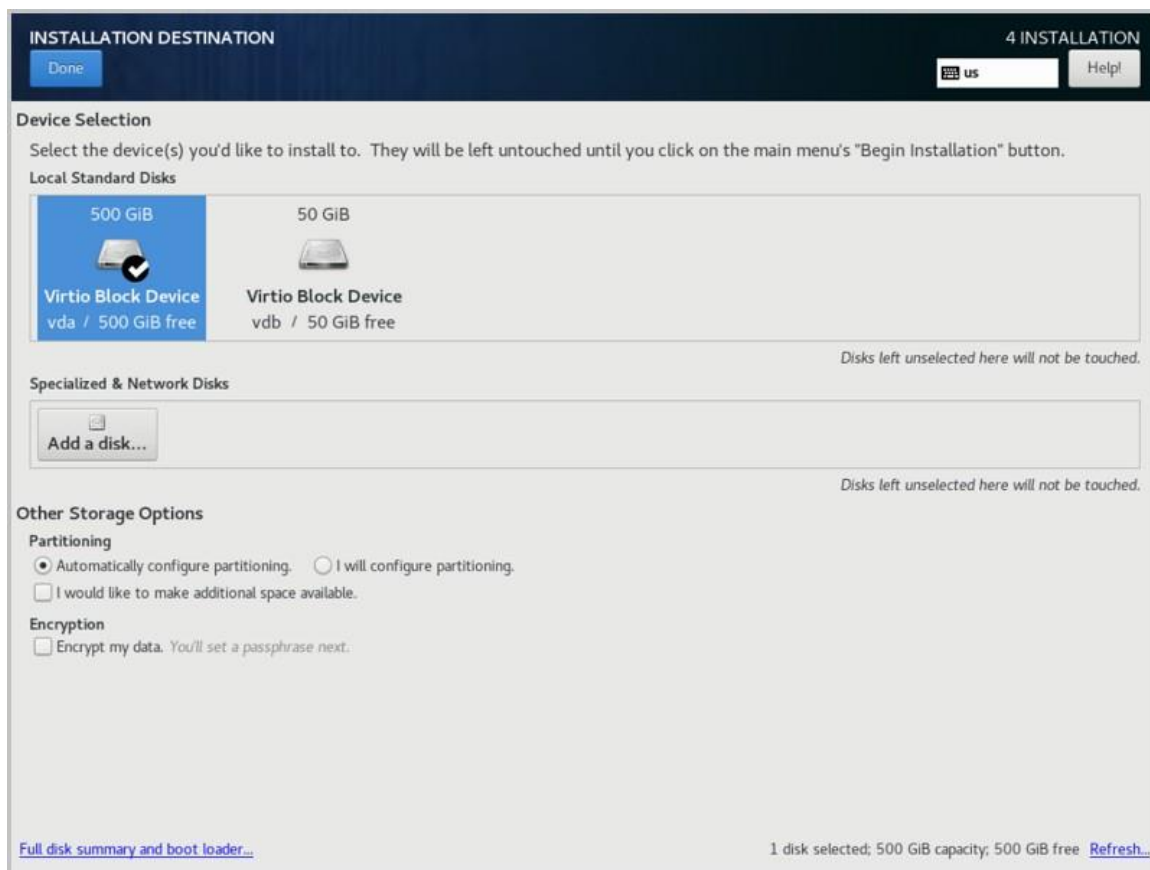
- 若选择该模式，系统安装后将进入终端界面，由用户自定义安装。除该模式外，其余模式将在系统安装完成后自动开始安装对应模式的云平台。
- **No ZStack Local Repo**选项表示精简安装，安装过程不拷贝ISO，并且不生成内部源。

e) 配置硬盘分区。

在**安装配置汇总**界面，点击**INSTALLATION DESTINATION**，进入**硬盘分区**界面。

如图 6: 默认磁盘分区所示：

图 6: 默认磁盘分区



注: 此处建议仅配置系统磁盘，其余磁盘可在系统安装后配置。

Cloud建议使用**Automatically configure partitioning.**选项自动配置磁盘分区。若用户需手动配置，可根据BIOS引导模式参考以下内容：

- UEFI 模式
 - `/boot`: 存放Linux 启动所需的核心文件，建议分配 1GB空间
 - `/boot/efi`: 存放UEFI启动引导文件，建议分配 500MB
 - `swap`: 交换区，建议分配 32GB
 - `/`: Linux系统根目录，建议分配全部剩余空间
- Legacy模式
 - `/boot`: 存放Linux 启动所需的核心文件，建议分配 1GB空间
 - `swap`: 交换区，建议分配 32GB
 - `/`: Linux系统根目录，建议分配全部剩余空间



注:

- 以上数值为Cloud建议分区容量（磁盘总容量大于300GB）。
- Legacy模式下，若系统盘容量大于2TB，需配置BIOS boot分区，以支持GPT分区。UEFI模式没有此限制，且支持GPT分区。

f) 配置网络。

本步骤将配置网卡静态IP地址以及网卡自动激活，该配置仅适用于POC测试。生产环境部署建议配置网卡归一化，详情请参考[网卡归一化\(可选\)](#)章节。

1. 配置静态IP地址。

- a. 在**安装配置汇总**界面，点击**NETWORK & HOST NAME > Ethernet (eth0) > Configure...**，弹出eth0配置界面。点击**IPv4 Settings > Method > Manual**，用于切换IP地址获取方式为手动指定。

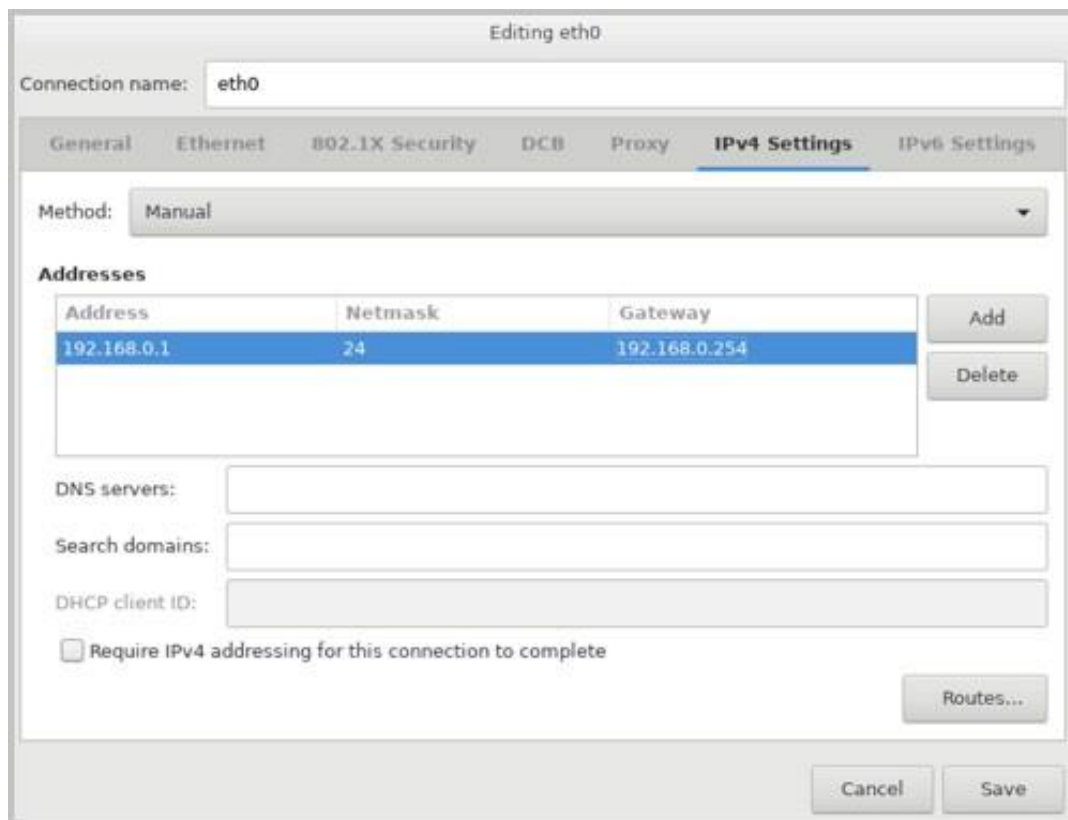


注：用户可按需配置IP地址获取方式，包括使用DHCP自动获取、手动指定等。

- b. 点击**Add**添加IP地址条目，根据按需配置IP地址、子网掩码、网关地址，完成后点击**save**保存配置。

如[图 7: 配置静态IP地址](#)所示：

图 7: 配置静态IP地址

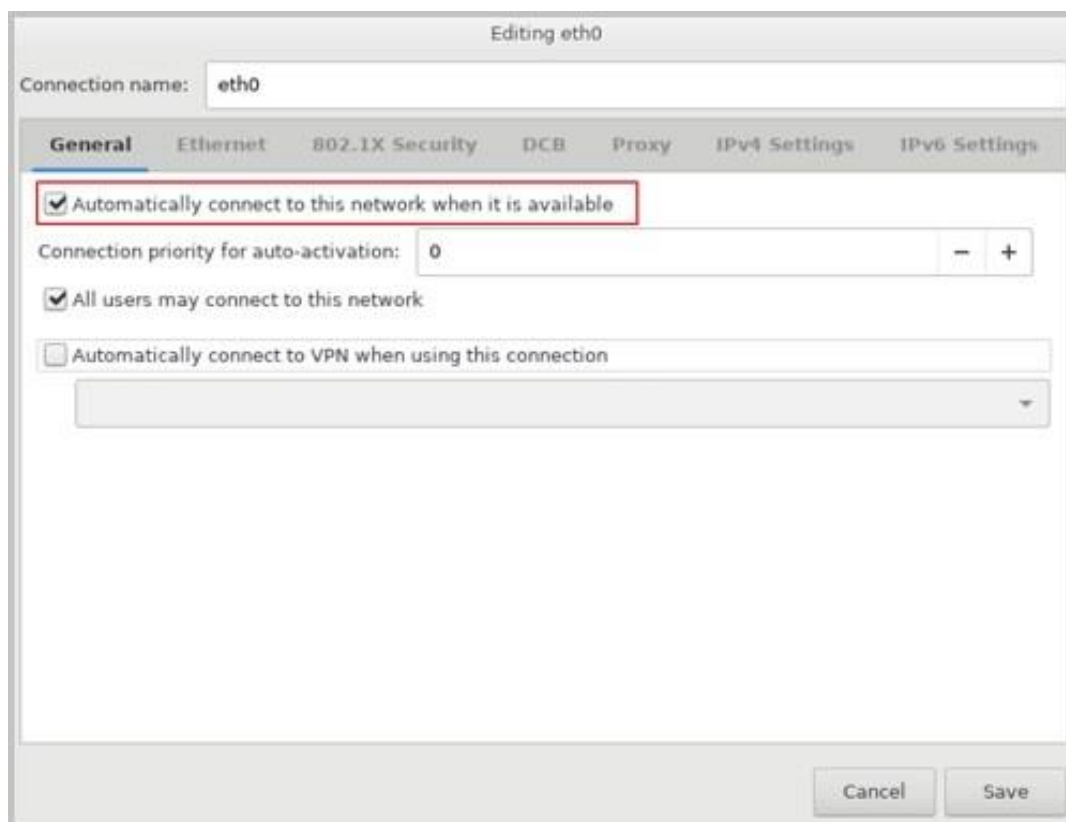


2. 配置网卡自动激活。

在eth0配置界面，点击**General > Automatically connect to this network when it is available > Save**，修改网卡自动激活。

如图 8: 配置网卡自动激活所示：

图 8: 配置网卡自动激活



g) 开始安装。

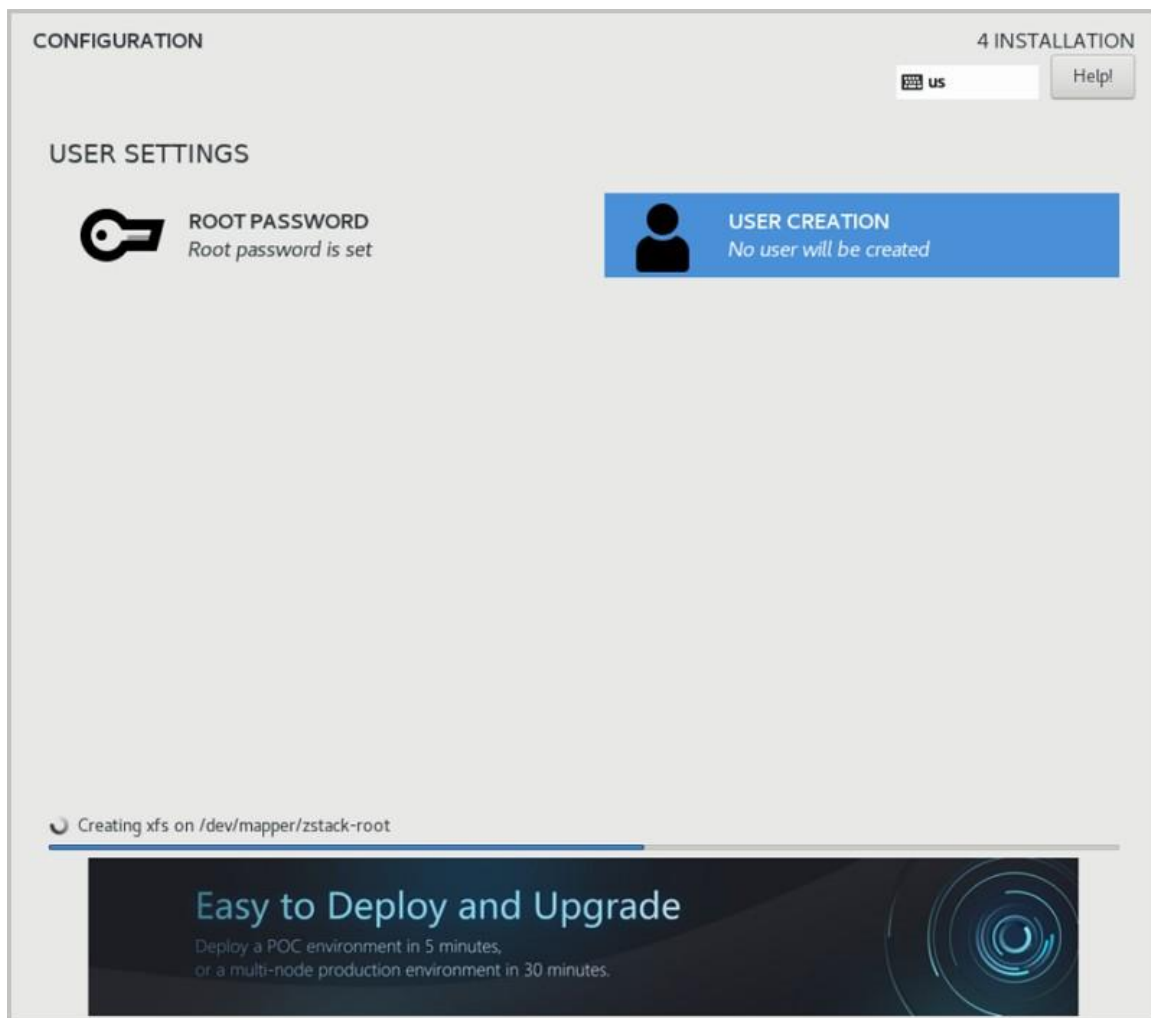
返回**安装配置汇总**界面，点击**Begin Installation**开始安装操作系统。

h) 设置密码。

安装过程自动进行，此时请点击**ROOT PASSWORD**，设置操作系统root用户密码。

如图 9: 设置密码所示：

图 9: 设置密码



i) 进入系统。

安装完成后，点击**重启**，即可启动进入Cloud定制版系统。

6.1.1 网卡归一化(可选)

本章节主要介绍网卡归一化配置方法，在实际生产环境中安装部署Cloud建议使用该方法。

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

用户可在Cloud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

用户可在安装操作系统时使用图形界面进行网卡归一化配置，流程如下：

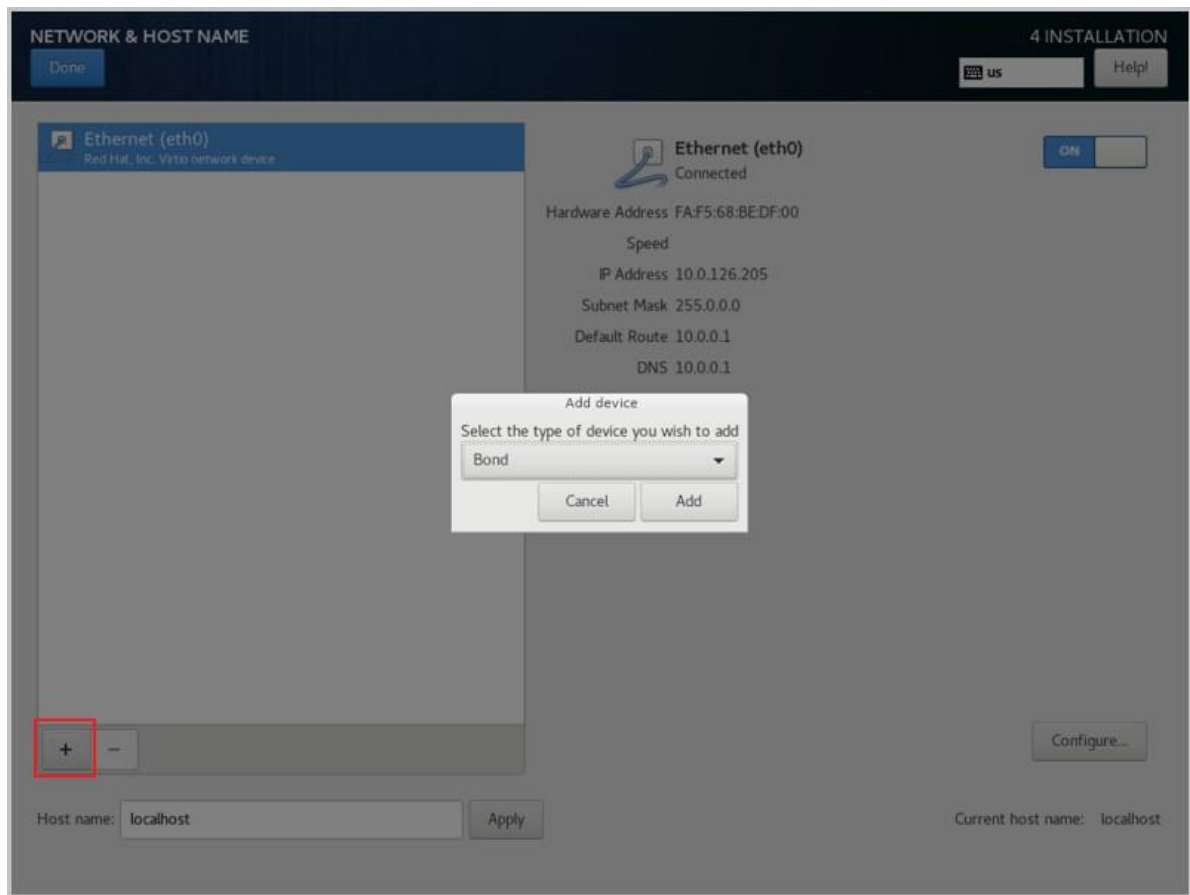
1. 添加Bond设备。
2. 添加Bond Slave。
3. 选择Bond模式。
4. 原网卡接口禁用IPv4。
5. 完成配置。
6. 配置Bond静态IP地址。
7. 配置网卡自动激活。

1. 添加Bond设备。

在**安装配置汇总**界面，点击**NETWORK & HOST NAME > Ethernet (eth0) > Configure...**，弹出**eth0**配置界面。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 10: 添加一个Bond设备所示：

图 10: 添加一个Bond设备

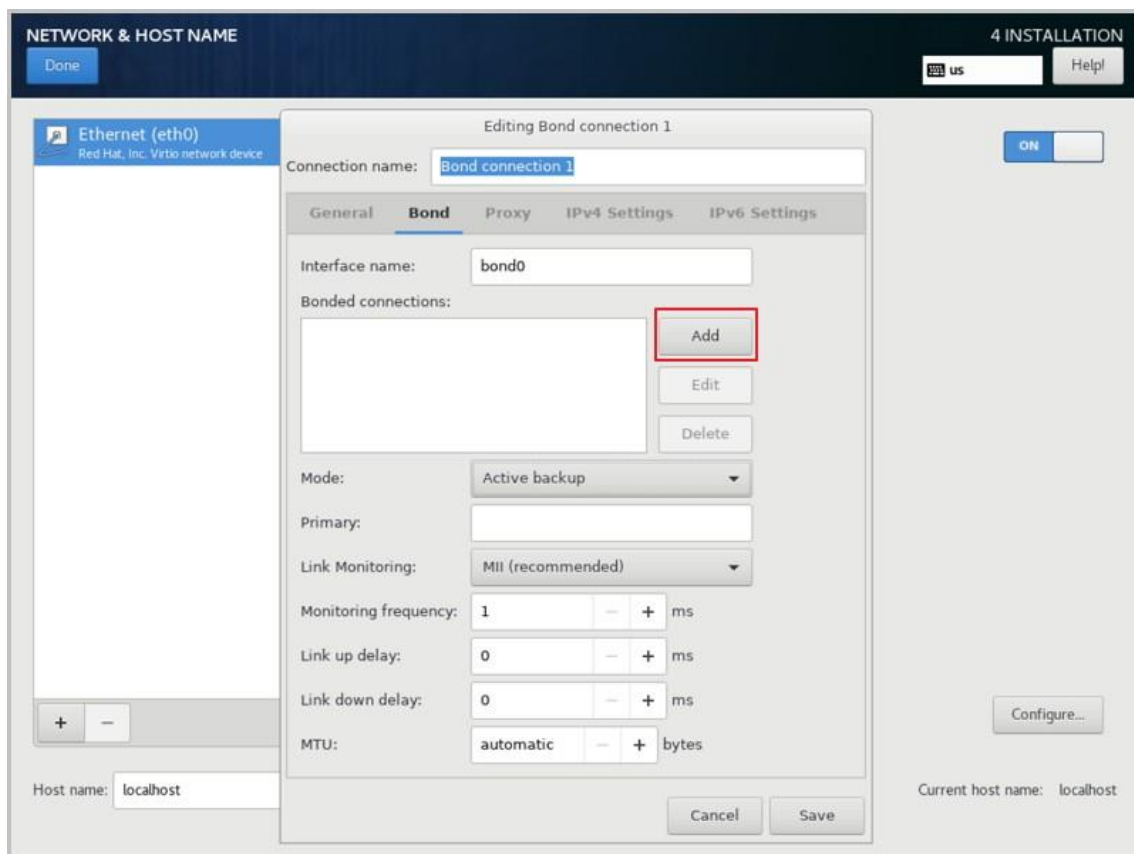


2. 添加Bond Slave。

- a. 在Bond配置界面，点击**Add**，添加Bond Slave。

如图 11: 添加Bond Slave所示:

图 11: 添加Bond Slave



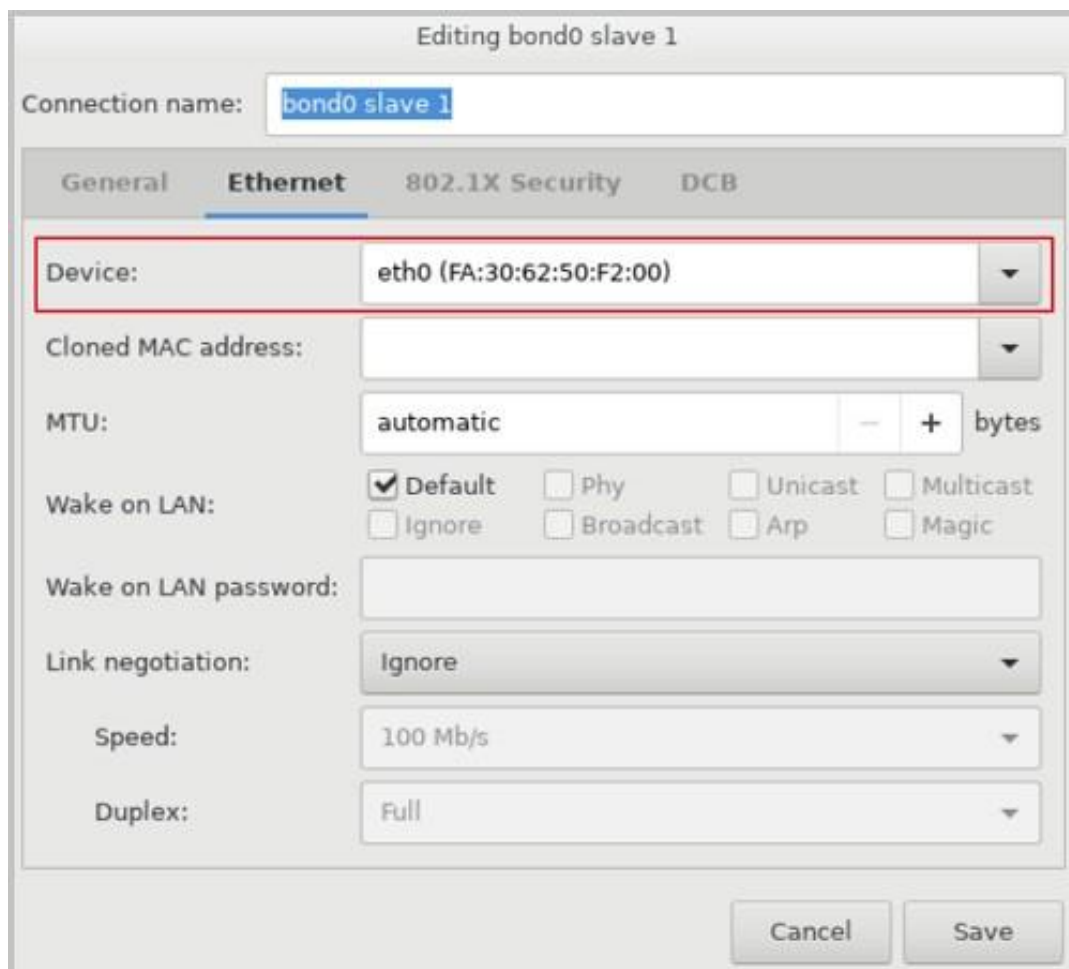
- b. 弹出**Choose a Connection Type**界面，在下拉菜单中选择Bond Slave连接类型，如Ethernet，点击**Create...**，如图 12: 选择Bond Slave连接类型所示：

图 12: 选择Bond Slave连接类型



- c. 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 13: 选择Bond Slave设备所示：

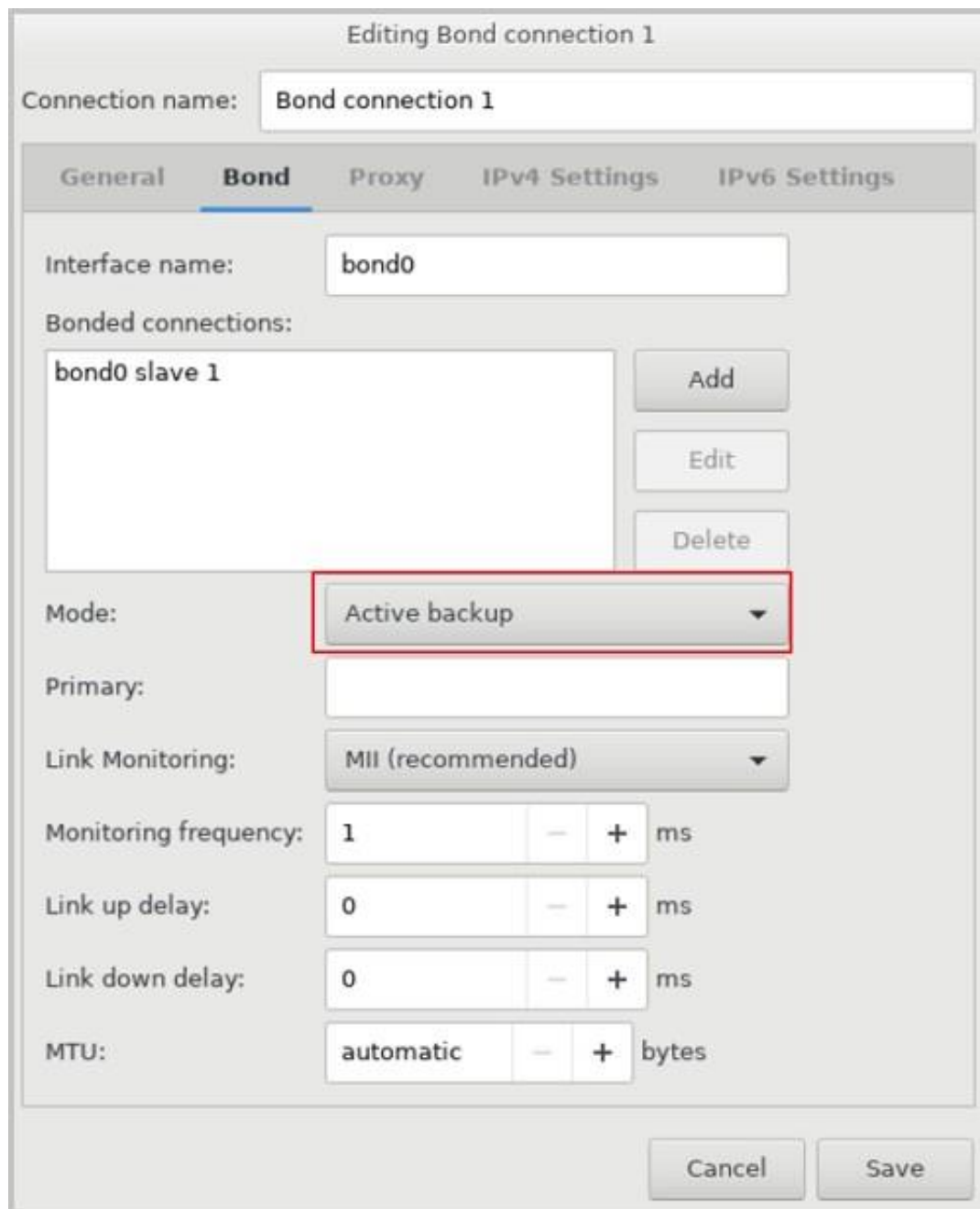
图 13: 选择Bond Slave设备



3. 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 14: 选择Bond模式所示：

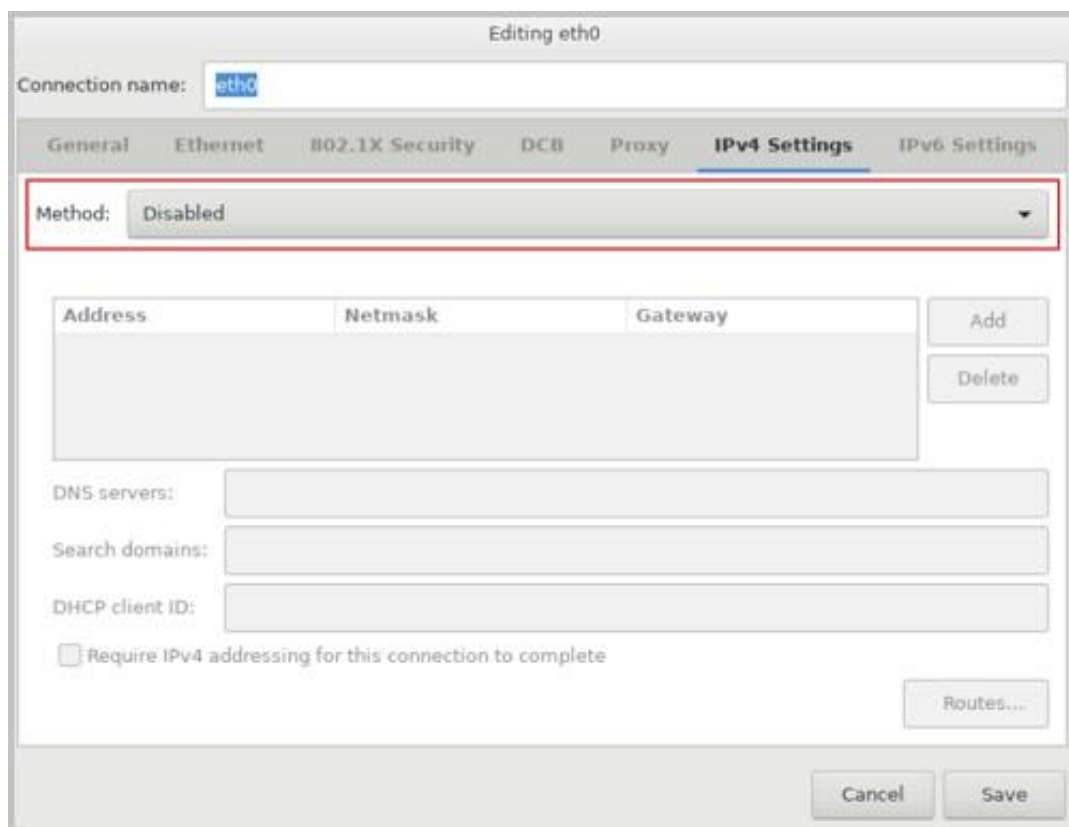
图 14: 选择Bond模式



4. 原网卡接口禁用IPv4。

- 选择Ethernet (eth0)，点击Configure... > IPv4 Settings，将Method参数值改为Disabled，点击Save，保存配置。
- 如图 15: 禁用IPv4所示：

图 15: 禁用IPv4



5. 完成配置。

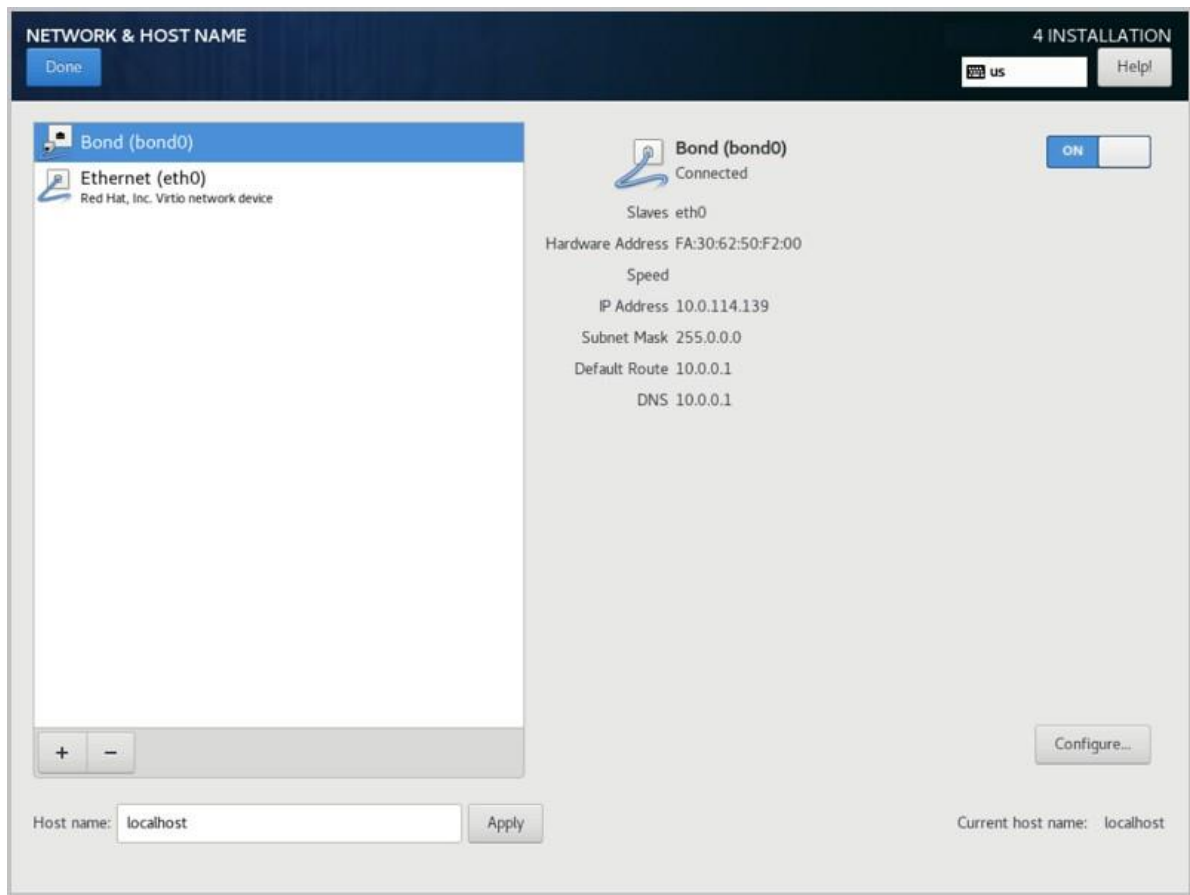
如图 16: 网卡归一化完成所示:



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Cloud无法正常安装。

图 16: 网卡归一化完成



6. 配置Bond静态IP地址。

- a. 在**安装配置汇总**界面，点击**NETWORK & HOST NAME** **Bond (bond0)** **Configure...**，弹出**Bond (bond0)** 配置界面。点击**IPv4 Settings > Method > Manual**，用于切换IP地址获取方式为手动指定。



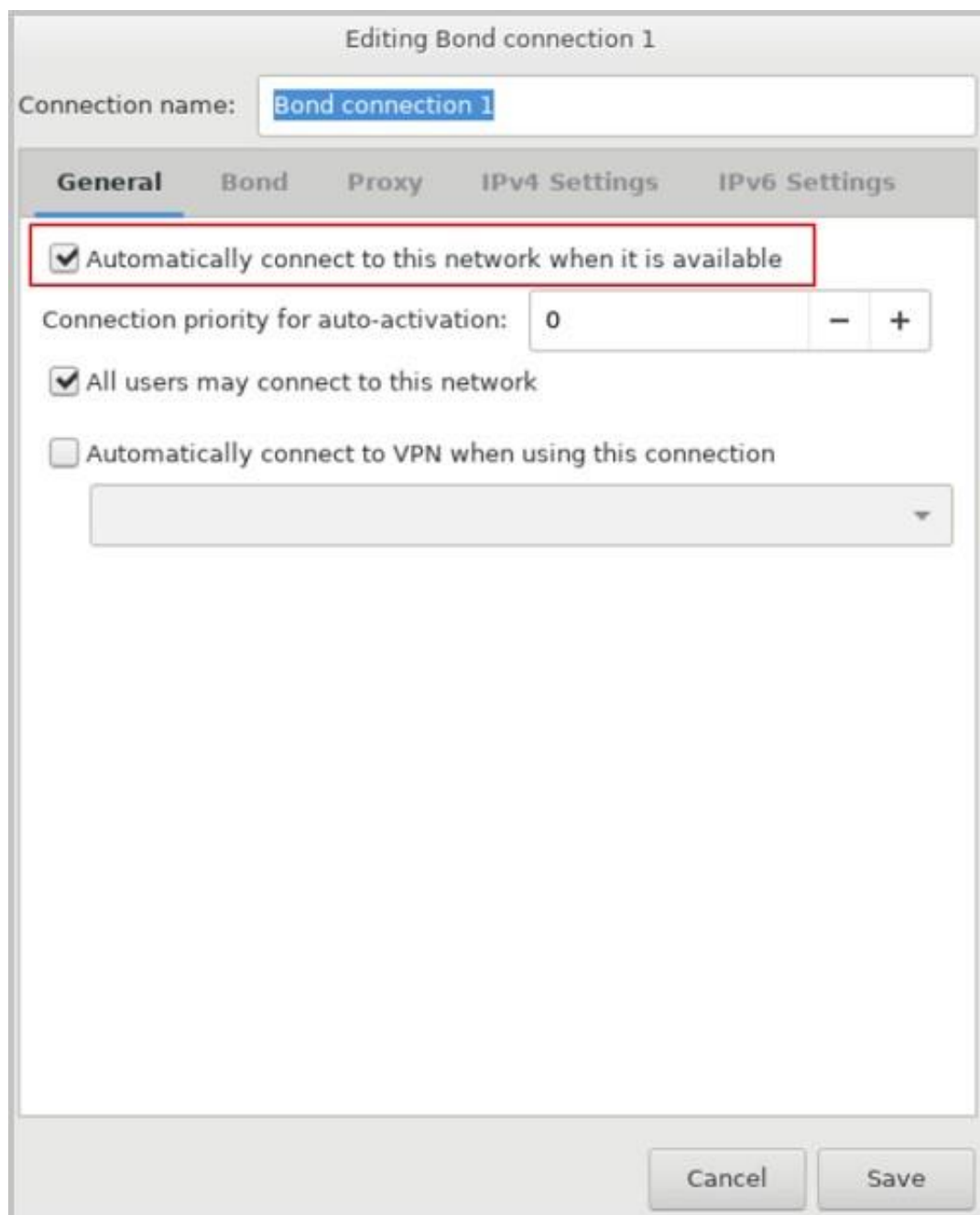
注：用户可按需配置IP地址获取方式，包括使用DHCP自动获取、手动指定等。

- b. 点击**Add**添加IP地址条目，根据按需配置IP地址、子网掩码、网关地址，完成后点击**save**保存配置。

7. 配置网卡自动激活。

在**Bond (bond0)** 配置界面，点击**General > Automatically connect to this network when it is available > Save**，修改网卡自动激活。

图 17: 配置网卡自动激活



6.2 安装Cloud

本节主要介绍Cloud 4.1.3的安装模式。

Cloud定制版ISO安装模式

Cloud定制版ISO提供以下安装模式：

- 企业版管理节点模式
- 计算节点模式

- 专家模式

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、CloudBus消息总线等依赖包
- 自动安装并启动Cloud

2. 计算节点模式

- 安装基础系统
- 安装Libvirt、Qemu等虚拟化组件

3. 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。

不同安装模式适用不同安装场景，如表 1: 安装场景所示：

表 1: 安装场景

模式	场景
企业版管理节点模式	仅适合安装企业版管理节点。
计算节点模式	适合安装云平台内除管理节点外的其他节点，例如：
专家模式	<ul style="list-style-type: none"> • 计算节点。 • 镜像仓库、Ceph镜像服务器节点、Ceph镜像服务器Mount节点。 • Ceph主存储节点、Ceph主存储Mount节点。 • PXE部署服务器节点、本地灾备服务器节点、远端备份服务器节点（异地）。

6.2.1 Cloud管理节点模式

自动安装Cloud管理节点

如果选择管理节点模式，重启后会自动安装Cloud管理节点。

6.2.2 Cloud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Cloud计算节点。



注：部分场景下，需要All-in-One模式来搭建Cloud，这时应选用Cloud管理节点模式安装。

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，仅与授权数量相关。

6.2.3 Cloud专家模式

如果用户选择专家模式，重启后会进入终端界面，用户可根据实际场景需求，自定义安装所需Cloud环境。

补充说明

专家模式支持精简安装，在选择安装模式步骤，勾选右侧**No ZStack Local Repo**表示精简安装。



注：精简专家模式安装过程不拷贝/opt/zstack-dvd/目录下的ISO、并且/etc/yum.repos.d/目录下不生成zstack-local.repo等配置文件。

6.3 管理Cloud

操作步骤

1. 首次安装后，系统自启动Cloud服务。
2. 管理节点重启后，Cloud服务将开机自启。
3. 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Cloud服务方法如下：

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

4. 用户可使用zstack-ctl status命令，查看Cloud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: 4.1.3 (ZStack-enterprise 4.1.3)
MN status: Running [PID:123135]
UI status: Running [PID:795] http://10.0.0.254:5000
```

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://10.0.0.254:5000
```

6. 在使用过程中如需重启管理节点服务，不重启Web UI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
```

6.4 升级Cloud

由于c74和c76版本ISO的升级步骤相同，因此以c76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c76版操作系统，将管理节点升级至最新的c76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，不支持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。
- 升级完成后，需及时清理浏览器缓存或刷新管理节点浏览器UI界面。

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，Cloud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Cloud），**增量升级**方案，用户只需要下载最新的Cloud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Cloud之前，请管理员准备好以下必要的软件包，建议将以上软件或脚本保存至管理节点所在的/root/目录下。
 - Cloud安装包：
 - 软件名称：Cloud-installer-4.1.3.bin

- 下载地址：请联系官方技术支持获取

2. 升级前，管理员需确保数据库已做好备份。

- 可执行以下命令，对数据库进行手动备份：

```
[root@zstack-1 ~]# zstack-ctl dump_mysql --file-name zstack-mysql-before-upgrade
```

注：

- 命令执行后，将会在`/var/lib/zstack/mysql-backup/`下创建数据库备份；
- 升级过程中，将升级Cloud代理服务器，不触及主存储和镜像服务器中的数据内容。
- 可使用Cloud提供的灾备服务，对数据库进行定时备份。

注：

- 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，且需在购买企业版云平台许可证基础上使用，不可单独使用。

3. 管理员执行以下命令升级Cloud管理服务。

```
[root@zstack-1 opt]# bash Cloud-installer-4.1.3.bin -u
```

注：

- 若数据库root密码采用系统默认密码，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 Cloud-installer-4.1.3.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Cloud的安装。
- 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。

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Cloud之前，请管理员准备好以下必要的软件包，建议将以上软件或脚本保存至管理节点所在的`/root/`目录下。

- Cloud定制版ISO:
 - 软件名称（C76）：Cloud-x86_64-DVD-4.1.3-c76.iso
 - 软件名称（C74）：Cloud-x86_64-DVD-4.1.3-c74.iso
 - 下载地址：请联系官方技术支持获取
- 升级脚本
 - 软件名称：Cloud-upgrade
 - 下载地址：请联系官方技术支持获取



注：升级脚本版本号需与ISO及bin包版本号保持一致。



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. 升级前，管理员需确保数据库已做好备份。

- 可执行以下命令，对数据库进行手动备份：

```
[root@zstack-1 ~]# zstack-ctl dump_mysql --file-name zstack-mysql-before-upgrade
```



注：

- 命令执行后，将会在/var/lib/zstack/mysql-backup/下创建数据库备份。
- 升级过程中，将升级Cloud代理服务器，不触及主存储和镜像服务器中的数据内容。
- 可使用Cloud提供的灾备服务，对数据库进行定时备份。



注：

- 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，且需在购买企业版云平台许可证基础上使用，不可单独使用。

3. 管理员执行以下命令升级Cloud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 Cloud-x86_64-DVD-4.1.3-c76.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 Cloud-x86_64-DVD-4.1.3-c76.iso
```

```
[root@zstack-1 opt]# bash Cloud-installer-4.1.3.bin -u
```

注：



- 若数据库root密码采用系统默认密码，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 Cloud-x86_64-DVD-4.1.3-c76.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 Cloud-x86_64-DVD-4.1.3-c76.iso
```

```
[root@zstack-1 opt]# bash Cloud-installer-4.1.3.bin -u -P
```

```
MYSQL_ROOT_PASSWORD
```

- 执行zstack-upgrade命令前需确认所准备的ISO是基于c76版，避免使用c74 ISO覆盖本地源。

注意事项

- Cloud升级过程支持自动升级libvirt版本，使用c74 ISO以及Qemu 2.9的用户，libvirt版本将默认自动升级至4.9.0。



注：

- 若用户部署使用开源版Ceph分布式存储，并开启CEPHX功能（即：Ceph密钥认证功能），云主机热插拔CD-ROM时会报错，这是由于新版libvirt暂不支持所致。如有需要可咨询官方技术支持获取帮助。
- Cloud 3.2.0开始，libvirt对共享云盘的格式更新为raw。因此，SharedBlock主存储上创建的共享云盘修改为raw格式，调整后此类共享云盘不支持创建快照、云盘扩容操作，以及当所加载云主机处于开机状态，不支持创建镜像操作。Cloud将会在后续版本中逐渐开放上述功能限制，请及时关注官方最新消息。
- 用户可自行关闭libvirt自动升级功能，设置方法如下：

进入/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/，在zstack.properties配置文件中设置如下参数：

```
updatePkgWhenConnect = false
```

```
# 关闭libvirt自动升级功能,默认为true.
```

设置后需重启管理节点生效。

7 系统登录

1. 支持HTTP与HTTPS两种方式登录UI管理界面。

- HTTP方式默认支持5000端口，输入相应的URL地址（http://management_node_ip:5000），即可打开UI管理界面（为了获取更好的产品体验，建议使用Chrome 49，Firefox 52 及以上版本的浏览器）。
- HTTPS方式默认不启用。。

2. 系统首次登录时，默认账户名：**admin**，默认初始密码：**password**。

3. Cloud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/LDAP服务器和AD/LDAP账户绑定。
- 项目登录：需添加企业管理模块License，输入用户名和密码登录。



注：若登录失败请检查管理节点服务，确保管理服务和UI服务均正常运行。

4. Cloud支持多种登录界面（主登录/项目登录），为了方便企业管理快速登录，在**设置 > 高级设置**中可设置UI登录界面模式。

在**高级设置**页面，设置**UI登录界面模式**的值即可。

- 若选择显示所有，通过默认登录链接 [http\(s\)://management_node_ip:port](http(s)://management_node_ip:port) 支持访问所有登录界面，包括：主登录界面和项目登录界面。
- 若选择项目登录，通过默认登录链接 [http\(s\)://management_node_ip:port](http(s)://management_node_ip:port) 仅支持访问项目登录界面。此时，针对主登录界面提供独立登录链接 [http\(s\)://management_node_ip:port/#/accountlogin](http(s)://management_node_ip:port/#/accountlogin)，请妥善保管。

5. 为进一步保障账户安全，Cloud支持双因子登录验证，开启双因子登录验证后，每次登录云平台均要求输入正确的账户名、密码以及身份验证器APP提供的6位安全码才能登录云平台。



注：

- 首次登录后不再展示身份验证二维码，请及时保存并妥善保管。
- 若管理员身份验证二维码丢失，请联系官方技术支持获取。
- 管理员登录后，可在账户详情页查看普通账户身份验证二维码，若普通账户二维码丢失，请联系管理员重新获取。
- 管理员登录后，可在项目详情页查看项目身份验证二维码，若项目二维码丢失，请联系管理员重新获取。
- 每个普通账户/项目需使用自己的身份验证二维码进行验证登录。

6. 为增加登录密码的安全性，云平台支持如下密码策略

- 开启连续登录失败锁定账户，锁定期间账户无法登录

在**设置 > 全局设置 > 基本设置**中可设置连续登录失败锁定账户。

- 在**基本设置**页面，将**连续登录失败锁定账户**设置为true打开此功能，默认为false。
- 在**基本设置**页面，设置**连续登录失败次数上限**可更改登录失败次数上限，默认6次。
- 在**基本设置**页面，设置**连续登录失败锁定账户时长**连续登录失败后账户锁定时间，默认10分钟。
- 开启密码更新周期，定期修改登录密码

在**设置 > 全局设置 > 基本设置**中可设置密码更新周期。

- 在**基本设置**页面，将**密码更新周期**设置为true打开此功能，默认为false。
- 在**基本设置**页面，设置**密码更新周期**，默认90天。
- 开启密码不重复次数，设置新密码不能与历史密码相同

在**设置 > 全局设置 > 基本设置**中可设置密码不重复次数。

- 在**基本设置**页面，将**密码不重复次数**设置为true打开此功能，默认为false。
- 在**基本设置**页面，设置**密码不重复次数**，例如：若为3，则新密码不能与之前3次已使用过的历史密码重复，默认为5。
- 开启密码强度，设置密码的长度范围，并可选择是否启用数字、大小写和特殊字符组合的策略

在**设置 > 全局设置 > 基本设置**中可设置密码强度。

- 在**基本设置**页面，将**密码强度**设置为true打开此功能，默认为false。
- 在**基本设置**页面，设置**密码强度**来选择密码长度范围、并选择是否启用数字、大小写和特殊字符组合的策略，默认为8-32。
- 设置禁止同一用户多会话连接开关，用于设置是否禁止同一用户多会话连接。开启后，则同一用户只能存在一个登录会话，历史会话将强制退出

在**设置 > 全局设置 > 基本设置**中可设置**禁止同一用户多会话连接开关**。

7. 首次登录成功后，可点击UI界面右上角的**个人中心 > 修改密码**。

7.1 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
$JAVA_HOME/bin/keytool -genkey -alias tomcat -storetype PKCS12 -keyalg RSA -keysize 2048 -keystore ./certs/keystore.p12 -validity 365
```



注: keytool默认无环境变量，需提前将JRE的安装路径添加到\$JAVA_HOME变量，例如:

```
echo "export JAVA_HOME=/usr/local/jdk1.8.0_181" >> /etc/profile
source /etc/profile
```

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 ./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
```


8 许可证管理

8.1 概述

许可证管理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功能。

在Cloud主菜单，点击**个人中心** > **许可证管理**，进入**许可证管理**界面。

授权协议说明

Cloud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）：**
 - 提供云平台的核心功能，可满足用户主流业务场景需求。
 - 主要包括：基础版、标准版、企业版-试用、企业版-付费。
- **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。需购买企业版云平台许可证基础上使用，不可单独使用。
 - 主要包括：VMware管理模块、企业管理模块、ARM64服务器管理模块、灾备服务模块、迁移服务模块、裸金属管理模块、弹性裸金属管理模块、阿里云混合云管理、5x8（7x24）小时售后服务。

具体授权协议说明：

表 2: 授权协议说明

基本类型	授权协议	授权协议说明
——	社区版	<p>为老师、学生、云计算爱好者等社区用户提供一个简单易得又功能完备的产品化私有云平台。</p> <ul style="list-style-type: none"> • 免费使用。 • 不限计算节点数量。 • 不限授权期限。 • 仅限使用云平台部分功能。 • 不提供官方售后技术支持服务。

基本类型	授权协议	授权协议说明
		<ul style="list-style-type: none"> 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）	基础版	<p>提供简便易用的企业级虚拟化平台，解决客户的虚拟化资源统一管理需求。</p> <ul style="list-style-type: none"> 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云平台的虚拟化核心功能。 不支持使用模块功能。 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。
	标准版	<p>提供完整的计算虚拟化、存储虚拟化及网络虚拟化功能，资源可按需分配、按需扩展，提供更灵活的业务解决方案。</p> <ul style="list-style-type: none"> 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云平台完整的计算虚拟化、存储虚拟化及网络虚拟化功能。 不支持使用模块功能。 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。
	企业版 试用	<p>提供完整的计算虚拟化、存储虚拟化及网络虚拟化功能，以及弹性伸缩、GPU、资源编排等强化功能。资源可按需分配、按需扩展，提供更灵活的业务解决方案。</p> <ul style="list-style-type: none"> 为期一年的试用。 可免费添加台 1 台物理机。 在许可证授权期限内可使用云平台的所有核心功能。 在许可证授权期限内可使用所有模块功能。 不提供官方售后技术支持服务。 适用于企业部署测试环境，不推荐生产环境使用。
	企业版 付费	<p>提供完整的计算虚拟化、存储虚拟化及网络虚拟化功能，以及弹性伸缩、GPU、资源编排等强化功能。资源可按需分配、按需扩展，提供更灵活的业务解决方案。</p> <ul style="list-style-type: none"> 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。


基本类型	授权协议	授权协议说明
		<ul style="list-style-type: none"> 在许可证授权期限内可使用云平台的所有核心功能。 在许可证授权期限内可按需购买并使用模块功能。 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。
模块许可证（Plus License）	VMware 管理	支持接管vCenter的全功能，为VMware计算节点提供独立的CPU授权。 <ul style="list-style-type: none"> 付费授权使用。 需购买企业版云平台许可证基础上使用，不可单独使用。 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。
	企业管理	提供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。 <ul style="list-style-type: none"> 付费授权使用。 需购买企业版云平台许可证基础上使用，不可单独使用。 在售后服务期内可获得官方售后技术支持服务。
	ARM64服务器管理	提供指定数量的ARM物理机许可，对ARM64服务器提供稳定的支持。 <ul style="list-style-type: none"> 付费授权使用。 需购买企业版云平台许可证基础上使用，不可单独使用。 在售后服务期内可获得官方售后技术支持服务。
	灾备服务	云主机数据在线备份到备份服务器。支持本地，跨地域和混合云多种备份场景，数据更可靠。 <ul style="list-style-type: none"> 付费授权使用。 需购买企业版云平台许可证基础上使用，不可单独使用。 在售后服务期内可获得官方售后技术支持服务。
	迁移服务	提供V2V的迁移功能，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。 <ul style="list-style-type: none"> 付费授权使用。 需购买企业版云平台许可证基础上使用，不可单独使用。 在售后服务期内可获得官方售后技术支持服务。

基本类型	授权协议	授权协议说明
	裸金属管理	<p>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。</p> <ul style="list-style-type: none"> • 付费授权使用。 • 需购买企业版云平台许可证基础上使用，不可单独使用。 • 在售后服务期内可获得官方售后技术支持服务。
	弹性裸金属管理	<p>提供指定数量弹性物理服务器的管理许可，在保证物理服务器高性能和稳定性的基础上，提高易用性和灵活性。</p> <ul style="list-style-type: none"> • 付费授权使用。 • 需购买企业版云平台许可证基础上使用，不可单独使用。 • 在售后服务期内可获得官方售后技术支持服务。
	阿里云混合云管理	<p>提供阿里云混合云的全部功能，实现控制面和数据面的互联互通。</p> <ul style="list-style-type: none"> • 付费授权使用。 • 需购买企业版云平台许可证基础上使用，不可单独使用。 • 在售后服务期内可获得官方售后技术支持服务。
	5x8（7x24）小时售后服务	<p>提供5x8或7x24小时的官方售后技术支持服务。</p> <ul style="list-style-type: none"> • 付费授权使用。 • 需购买企业版云平台许可证基础上使用，不可单独使用。

8.2 管理许可证

在Cloud主菜单，点击**个人中心 > 许可证管理**，进入**许可证管理**界面。

许可证支持以下操作：

操作	简介
上传许可证	<p>支持通过图形化界面添加许可证。</p> <p>注：</p>  <ul style="list-style-type: none"> • 支持以tar.gz压缩包形式一次性上传云平台许可证（Base License）和模块许可证（Plus License）。 • 若使用双管理节点环境，建议在虚拟IP所在的管理节点进行请求码下载和许可证上传操作，即可更新所有管理节点的许可授权信息。 • 可点击许可证管理界面右上角的刷新按钮，重新加载许可证。

操作	简介
	<ul style="list-style-type: none"> 仅admin拥有加载和删除许可证的权限，但云平台许可证（Base License）不支持删除。
下载请求码	下载生成许可证所需的请求码。
删除模块许可证	将已添加的模块许可证删除。

许可证状态说明

许可证存在以下状态：

操作	简介
有效	添加有效的云平台许可证，对应的位置将标注有效字样。
已过期	如果云平台许可证或模块许可证过期，对应的位置将标注过期字样且功能不可用。模块许可证过期后主菜单入口禁止访问。

许可证到期提醒

- 当许可证剩余使用期限不足15天时，登录云平台后将出现横幅提示。



注：

- 5x8（7x24）小时售后服务将在使用期限不足30天时进行提醒，请尽快联系云平台相关人员进行授权更新，以获得完善的官方售后技术支持服务。
- 点击横幅提示中的**去查看**，可直接跳转至**许可证管理**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授权更新，以继续使用本产品。

如图 18: 许可证即将过期所示：

图 18: 许可证即将过期



- 当平台许可证已过期，登录云平台后将自动跳转至**许可证管理**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授权更新，以继续使用本产品。

如图 19: 许可证已过期所示:

图 19: 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。
- 若您的云平台许可证（BaseLicense）已过期，但模块许可证（PlusLicense）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**企业版付费**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。

许可证授权记录

在Cloud主菜单，点击**个人中心 > 许可证管理 > 授权记录**，进入**授权记录**界面。

admin可通过图形化界面直观的看到云平台授权历史记录，包括产品许可类型、许可签发时间、许可到期时间、授权属性、授权额度、状态以及该许可上传时间。

如图 20: 授权记录所示:

图 20: 授权记录

授权记录

产品许可	签发时间	到期时间	授权属性	授权额度	状态	上传时间
 弹性裸金属管理	2021-04-19 20:38:53	2021-04-20 20:38:53	物理机数量	20	使用中	2021-04-19 20:3
 裸金属管理	2021-04-19 20:38:53	2021-04-22 20:38:53	物理机数量	20	使用中	2021-04-19 20:3
 5x8小时售后服务	2021-04-19 20:38:53	2021-05-03 20:38:53	-	-	使用中	2021-04-19 20:3
 ARM64服务器管理	2021-04-19 20:38:53	2021-04-23 20:38:53	物理机数量	20	使用中	2021-04-19 20:3
 企业版	2021-04-19 20:38:53	2021-05-03 20:38:53	CPU插槽数量	20	使用中	2021-04-19 20:3
 企业管理	2021-04-19 20:38:53	2021-05-01 20:38:53	-	-	使用中	2021-04-19 20:3
 混合云管理	2021-04-19 20:38:53	2021-04-28 20:38:53	-	-	使用中	2021-04-19 20:3
 迁移服务	2021-04-19 20:38:53	2021-04-21 20:38:53	-	-	使用中	2021-04-19 20:3
 VMware管理	2021-04-19 20:38:53	2021-04-24 20:38:53	CPU插槽数量	20	使用中	2021-04-19 20:3
 灾备服务	2021-04-19 20:38:53	2021-04-22 20:38:53	-	-	使用中	2021-04-19 20:3

第 1-10 项, 共 84 项

< 1 2 3 4 5 ... 9 > 10 条/页 跳至 页

9 Wizard引导设置

首次登录Cloud，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。
- 主存储和二层网络必须加载到本集群，才可提供云主机服务。

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Cloud定制版ISO安装CentOS 7.4或CentOS 7.6系统；
- BIOS需打开Intel VMX或AMD SVM的硬件虚拟化功。
- 需确保IP地址、SSH端口、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。
- 请确保物理机添加完成后，再创建或删除二层网络。

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镜像仓库采用镜像切分去重的方式，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此服务器的/zstack_bs目录来存储镜像文件。

2. 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主存储需输入与Ceph镜像服务器同一存储集群的监控节点上可被Cloud管理节点访问的管理IP地址、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。
- Cloud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。

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，Cloud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virtio-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。使用该台类型可以解决旧版本系统的兼容问题。
- - **URL**: 采用指定的URL路径来添加镜像, 支持以下格式:
 - HTTP/HTTPS格式:
 - 填写格式为: `http://host[:port]/path/file`或`https://host[:port]/path/file`
 - FTP格式:
 - 匿名模式: `ftp://hostname[:port]/path/file`
 - 非匿名模式: `ftp://user:password@hostname[:port]/path/file`
 - SFTP格式:
 - 指定密码模式: `sftp://user:password@hostname[:port]/path/file`
 - 免密模式: `sftp://user@hostname[:port]/path/file`
 - 镜像服务器上的绝对路径, 支持ImageStore镜像服务器
例如: `file:///path/file`



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ImageStore镜像服务器, 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。
- 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/dvd/image-1.4.qcow2`, 在镜像服务器的`/opt/dvd`目录下应存放有`image-1.4.qcow2`文件。
- 断点续传功能:
 - ImageStore类型的镜像服务器支持断点续传功能, 若由于网络波动等原因造成连接中断, 该任务将自动暂停。
 - 用户可点击**平台运维 > 消息日志 > 操作日志 > 当前任务 > 添加镜像 > 操作**, 对该任务进行取消、暂停或继续操作。
- **本地文件**: 选择当前浏览器可访问的镜像直接上传, 支持ImageStore和Ceph镜像服务器



注:

- ImageStore类型的镜像服务器支持断点续传功能, 若用户刷新浏览器、关闭浏览器或管理节点服务停止, 该任务将自动暂停, 反之则任务执行失败。
- 用户可点击**平台运维 > 消息日志 > 操作日志 > 当前任务 > 添加镜像 > 操作**, 对该任务进行取消、暂停或继续操作。

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。

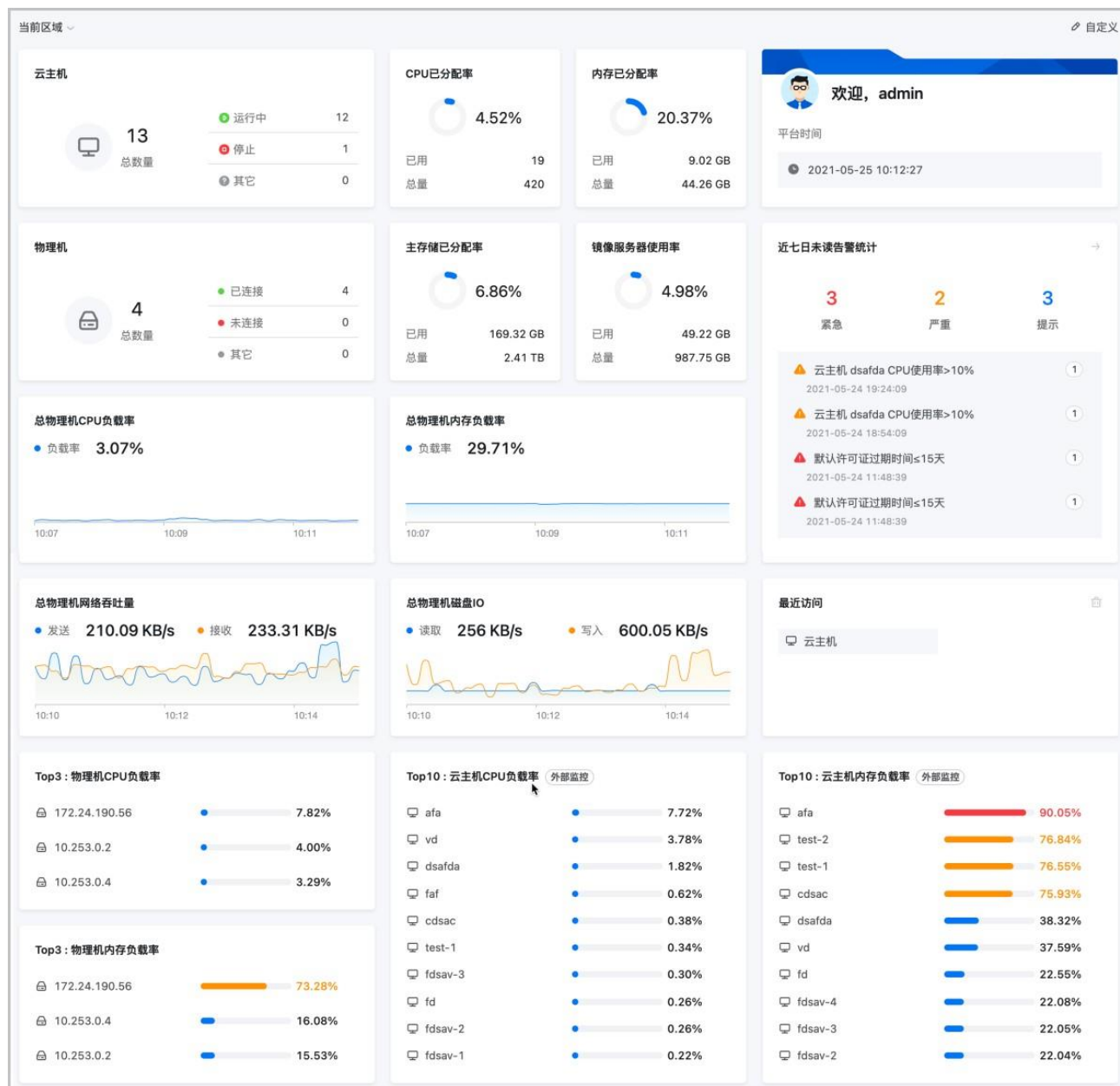
- 三层网络属于二层网络的子资源，创建时默认选择了已创建的二层网络。
- 初始化界面的网络配置默认采用扁平网络，可实现云主机和物理主机直接互通。
- 网络服务会根据选择的扁平网络，配置DHCP、弹性IP、安全组、UserData等网络服务。
- 扁平网络的网络服务采用分布式的DHCP、分布式的EIP结构。
- 扁平网络的DHCP服务也包含了DNS的功能。
- 添加三层网络的网络段可使用IP范围和CIDR（无域间路由）两种方式：
 - IP范围的添加可指定172.20.12.2到172.20.12.255，子网掩码指定255.255.0.0，网关指定172.20.0.1。
 - CIDR无域间路由可以使用，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。

10 首页

登录Cloud，或在Cloud主菜单点击**首页**，即可进入**首页**界面。

如图 21: 首页所示:

图 21: 首页



Cloud首页以卡片方式展示云平台内资源的状态统计、负载趋势、用量统计、资源TOP排行、最近访问、用户信息、近七日来读告警统计等信息。

- 每次进入或刷新首页均能获取最新数据并实时展示。此外，图表类模块默认30秒自动刷新一次数据。
- 首页默认展示多个常用模块，满足用户基本运维和平台管理需求。若需要自定义首页，可点击右上角**自定义**按钮进行设置，详情请参考**自定义首页**章节。
- 首页包括大、中、小三种固定尺寸的模块，用户可根据自己的喜好，随意拖动模块进行布局。
- 首页默认统计当前区域资源数据进行展示，可点击左上角切换按钮，统计所有区域的资源数据。

- 状态统计类图表采用统一的色彩规范，绿色表示正常状态、红色表示异常状态、灰色表示其他状态，方便用户快速识别资源健康状态。
- 百分比进度条包括蓝（小于60%）、黄（大于等于60%并且小于80%）、红（大于等于80%）三色，直观展示当前资源的使用状态。

在**首页**界面，点击**自定义**，进入自定义首页状态。

可参考以下步骤自定义首页：

1. 添加模块。

在自定义首页界面，点击右上角**添加模块**按钮，可参考**表 3: 首页模块列表**，按需添加需要展示在首页的模块。



注：首页最多添加30个模块；同一模块只可添加一次。

2. 模块布局。

首页包括大、中、小三种固定尺寸的模块，用户可根据自己的喜好，随意拖动模块进行布局。

3. 应用自定义首页。

模块添加完成，且完成模块布局的情况下，点击**保存**按钮，即可应用自定义首页。



注：若放弃当前自定义首页内容，可点击**取消**按钮；若期望使用系统默认首页配置，可点击**恢复默认**按钮。



Cloud支持多种类型、多种样式的功能模块，满足用户各类场景需求。模块列表如下：

表 3: 首页模块列表

类型	资源类型	监控条目	描述
资源状态统计	云主机	/	统计当前区域/所有区域内KVM云主机的数量，并直观展示KVM云主机总数量，以及不同状态（运行中、已停止、其他）KVM云主机的数量。
	物理机	/	统计当前区域/所有区域内物理机的数量，并直观展示物理机总数量，以及不同状态（已连接、未连接、其他）物理机的数量。
	主存储	/	统计当前区域/所有区域内主存储的数量，并直观展示主存储总数量，以及不同状态（已连接、未连接、其他）主存储的数量。
	镜像服务器	/	统计当前区域/所有区域内镜像服务器的数量，并直观展示镜像服务器总数量，以及不同状态（已连接、未连接、其他）镜像服务器的数量。
	物理GPU	/	统计当前区域/所有区域内物理GPU的数量，并直观展示物理GPU总数量，以及不同状态（已加载、空闲、其他）物理GPU的数量。

类型	资源类型	监控条目	描述
	vGPU	/	统计当前区域/所有区域内vGPU的数量，并直观展示vGPU总数量，以及不同状态（已加载、空闲、其他）vGPU的数量。
	VPC路由器	/	统计当前区域/所有区域内VPC路由器的数量，并直观展示VPC路由器总数量，以及不同状态（运行中、已停止、其他）VPC路由器的数量。
	云盘	/	统计当前区域/所有区域内数据云盘的数量，并直观展示数据云盘总数量，以及不同状态（已加载、未加载、其他）数据云盘的数量。
负载趋势	物理机用量趋势	总物理机CPU负载率	对当前区域/所有区域内全部物理机CPU资源使用情况进行统计分析，并以动态曲线图方式实时展示总物理机CPU负载率。 总物理机CPU负载率=全部物理机CPU负载率的平均值
		总物理机内存负载率	对当前区域/所有区域内全部物理机内存资源使用情况进行统计分析，并以动态曲线图方式实时展示总物理机内存负载率。 总物理机内存负载率=全部物理机内存负载率的平均值
		总物理机网络吞吐量（发送/接收）	对当前区域/所有区域内全部物理机网络吞吐情况进行统计分析，并以动态曲线图方式实时展示总物理机网络吞吐量（发送/接收）。 总物理机网络吞吐量=全部物理机网络吞吐量之和
		总物理机磁盘IO（写入/读取）	对当前区域/所有区域内全部物理机磁盘IO情况进行统计分析，并以动态曲线图方式实时展示总物理机磁盘IO（写入/读取）。 总物理机磁盘IO=全部物理机磁盘IO之和
	主存储用量趋势	主存储容量已用率	对当前区域/所有区域内主存储的使用情况进行统计分析，并以动态曲线图方式实时展示主存储容量已用率。 主存储容量已用率=全部主存储已用容量之和/全部主存储容量之和

类型	资源类型	监控条目	描述
	镜像服务器用量趋势	镜像服务器容量已用率	<p>对当前区域/所有区域内镜像服务器的使用情况进行统计分析，并以动态曲线图方式实时展示镜像服务器容量已用率。</p> <p>镜像服务器容量已用率=全部镜像服务器已用容量之和/全部镜像服务器容量之和</p>
用量统计	CPU已分配率	/	统计当前区域/所有区域内CPU使用情况，并直观展示CPU已分配百分比，以及CPU已用量和总量。
	内存已分配率	/	统计当前区域/所有区域内内存使用情况，并直观展示内存已分配百分比，以及内存已用量和总量。
	主存储已分配率	/	统计当前区域/所有区域内主存储的存储资源使用情况，并直观展示主存储已分配百分比，以及主存储已用量和总量。
	镜像服务器使用率	/	统计当前区域/所有区域内镜像服务器的存储资源使用情况，并直观展示镜像服务器使用百分比，以及镜像服务器已用量和总量。
	公有网络IP使用率-IPv4	/	统计当前区域/所有区域内IPv4类型公有网络的IP地址使用情况，并直观展示IP地址已用百分比，以及IP地址已用量和总量。
	扁平网络IP使用率-IPv4	/	统计当前区域/所有区域内IPv4类型扁平网络的IP地址使用情况，并直观展示IP地址已用百分比，以及IP地址已用量和总量。
	公有网络IP使用率-IPv6	/	统计当前区域/所有区域内IPv6类型公有网络的IP地址使用情况，并直观展示IP地址已用百分比，以及IP地址已用量和总量。
资源TOP排行	云主机（外部监控）	CPU平均使用率	通过外部监控对当前区域/所有区域内云主机CPU使用情况进行分析统计，筛选CPU平均使用率Top 3/Top 10的云主机进行展示。
		内存负载率	通过外部监控对当前区域/所有区域内云主机内存使用情况进行分析统计，筛选内存负载率Top 3/Top 10的云主机进行展示。

类型	资源类型	监控条目	描述
		磁盘读 IOPS	通过外部监控对当前区域/所有区域内云主机磁盘读IOPS情况进行分析统计，筛选磁盘读IOPS Top 3/Top 10的云主机进行展示。 磁盘读IOPS=云主机全部磁盘读IOPS之和
		磁盘写 IOPS	通过外部监控对当前区域/所有区域内云主机磁盘写IOPS情况进行分析统计，筛选磁盘写IOPS Top 3/Top 10的云主机进行展示。 磁盘写IOPS=云主机全部磁盘写IOPS之和
	云主机（内部监控）	CPU平均使用率	通过内部监控对当前区域/所有区域内云主机CPU使用情况进行分析统计，筛选CPU平均使用率Top 3/Top 10的云主机进行展示。  注：需为云主机安装Agent，以获取内部监控数据。
		内存负载率	通过内部监控对当前区域/所有区域内云主机内存使用情况进行分析统计，筛选内存负载率Top 3/Top 10的云主机进行展示。  注：需为云主机安装Agent，以获取内部监控数据。
		磁盘容量已用率	通过内部监控对当前区域/所有区域内云主机磁盘容量使用情况进行分析统计，筛选磁盘内存负载率Top 3/Top 10的云主机进行展示。 磁盘容量已用率=云主机所有磁盘使用容量之和/云主机所有磁盘容量之和
	VPC路由器（外部监控）	CPU平均使用率	通过外部监控对当前区域/所有区域内VPC路由器CPU使用情况进行分析统计，筛选CPU平均使用率Top 3/Top 10的VPC路由器进行展示。 云主机CPU平均使用率=每颗CPU使用率之和/CPU核数
		内存负载率	通过外部监控对当前区域/所有区域内VPC路由器内存使用情况进行分析统计，筛选内存负载率Top 3/Top 10的VPC路由器进行展示。

类型	资源类型	监控条目	描述
		磁盘读 IOPS	通过外部监控对当前区域/所有区域内VPC路由器磁盘读IOPS情况进行分析统计，筛选磁盘读IOPS Top 3/Top 10的VPC路由器进行展示。 磁盘读IOPS=VPC路由器全部磁盘读IOPS之和
		磁盘写 IOPS	通过外部监控对当前区域/所有区域内VPC路由器磁盘写IOPS情况进行分析统计，筛选磁盘写IOPS Top 3/Top 10的VPC路由器进行展示。 磁盘写IOPS=VPC路由器全部磁盘写IOPS之和
	VPC路由器（内部监控）	CPU平均使用率	通过内部监控对当前区域/所有区域内VPC路由器CPU使用情况进行分析统计，筛选CPU平均使用率Top 3/Top 10的VPC路由器进行展示。
		内存负载率	通过内部监控对当前区域/所有区域内VPC路由器内存使用情况进行分析统计，筛选内存负载率Top 3/Top 10的VPC路由器进行展示。
		磁盘容量已用率	通过内部监控对当前区域/所有区域内VPC路由器磁盘容量使用情况进行分析统计，筛选磁盘内存负载率Top 3/Top 10的VPC路由器进行展示。 磁盘容量已用率=VPC路由器所有磁盘使用容量之和/VPC路由器所有磁盘容量之和
	物理机	CPU平均使用率	对当前区域/所有区域内物理机CPU使用情况进行分析统计，筛选CPU平均使用率Top 3/Top 10的物理机进行展示。 物理机CPU平均使用率=每颗CPU使用率之和/CPU核数
		内存负载率	对当前区域/所有区域内物理机内存使用情况进行分析统计，筛选内存负载率Top 3/Top 10的物理机进行展示。
		磁盘读 IOPS	对当前区域/所有区域内物理机磁盘读IOPS情况进行分析统计，筛选磁盘读IOPS Top 3/Top 10的物理机进行展示。 磁盘读IOPS=物理机全部磁盘读IOPS之和

类型	资源类型	监控条目	描述
		磁盘写 IOPS	对当前区域/所有区域内物理机磁盘写IOPS情况进行分析统计，筛选磁盘写IOPS Top 3/Top 10的物理机进行展示。 磁盘写IOPS=物理机全部磁盘写IOPS之和
	云盘	真实容量	获取当前区域/所有区域内云盘的真实使用容量，筛选真实使用容量Top 3/Top 10的云盘进行展示。
	快照	容量	获取当前区域/所有区域内快照的容量，筛选容量Top 3/Top 10的快照进行展示。
	三层网络	可用IP百分比	对当前区域/所有区域内三层网络（公有网络、扁平网络、VPC网络）可用IP进行分析统计，筛选可用IP百分比Top 3/Top 10的三层网络进行展示。
	虚拟IP	上行网络流量	对当前区域/所有区域内虚拟IP的上行网络流量进行分析统计，筛选上行网络流量Top 3/Top 10的虚拟IP进行展示。
		下行网络流量	对当前区域/所有区域内虚拟IP的下行网络流量进行分析统计，筛选下行网络流量Top 3/Top 10的虚拟IP进行展示。
最近访问	/	/	显示6条最近访问的菜单记录。点击右上角删除按钮，支持清空记录。
用户信息	/	/	显示用户身份信息及云平台时间。
近七日未读告警统计	/	/	显示近七日最近4条报警消息。点击右上角跳转按钮，支持跳转到报警消息页面查看所有消息。

11 大屏监控

Cloud支持数据中心大屏监控功能，无论系统登入还是登出，大屏都能保持持续展示，数据实时刷新。

- 可通过以下两种方式登录监控大屏：
 - 点击UI界面右上角的大屏监控入口按钮，可在新页面打开大屏监控，对所有区域/指定区域的数据中心实时资源状态进行统一直观展示。如图 22: 大屏监控入口所示：

图 22: 大屏监控入口



- 绑定监控大屏角色的企业管理用户，登录后直接跳转监控大屏界面。
- 大屏监控支持经典款和科技款两种风格，支持在**设置 > 主题外观**界面进行自定义监控大屏标题、监控大屏主题。详情请参考**主题外观**章节。
- 每套Cloud在同一浏览器窗口仅允许打开一个大屏监控界面。

经典款大屏采用简约设计风格，包括负载Top5、负载统计、用量统计和资源总览信息展示，如图 23: [KVM大屏监控界面](#)和图 24: [vCenter大屏监控界面](#)所示：

图 23: KVM大屏监控界面



图 24: vCenter大屏监控界面



经典款大屏监控主要分为以下几个部分：

1. 大屏切换：虚拟化、区域切换

Cloud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。

如图 25: 大屏切换所示：

图 25: 大屏切换



- 支持切换KVM或vCenter虚拟化。
- 支持切换所有区域或某个区域。
- KVM大屏监控与vCenter大屏监控区别如下：
 - vCenter大屏监控资源总览中不包括集群信息展示。
 - vCenter大屏监控用量统计中不包括IPv6类型网络展示。

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

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

如图 26: 负载 Top5所示：

图 26: 负载 Top5

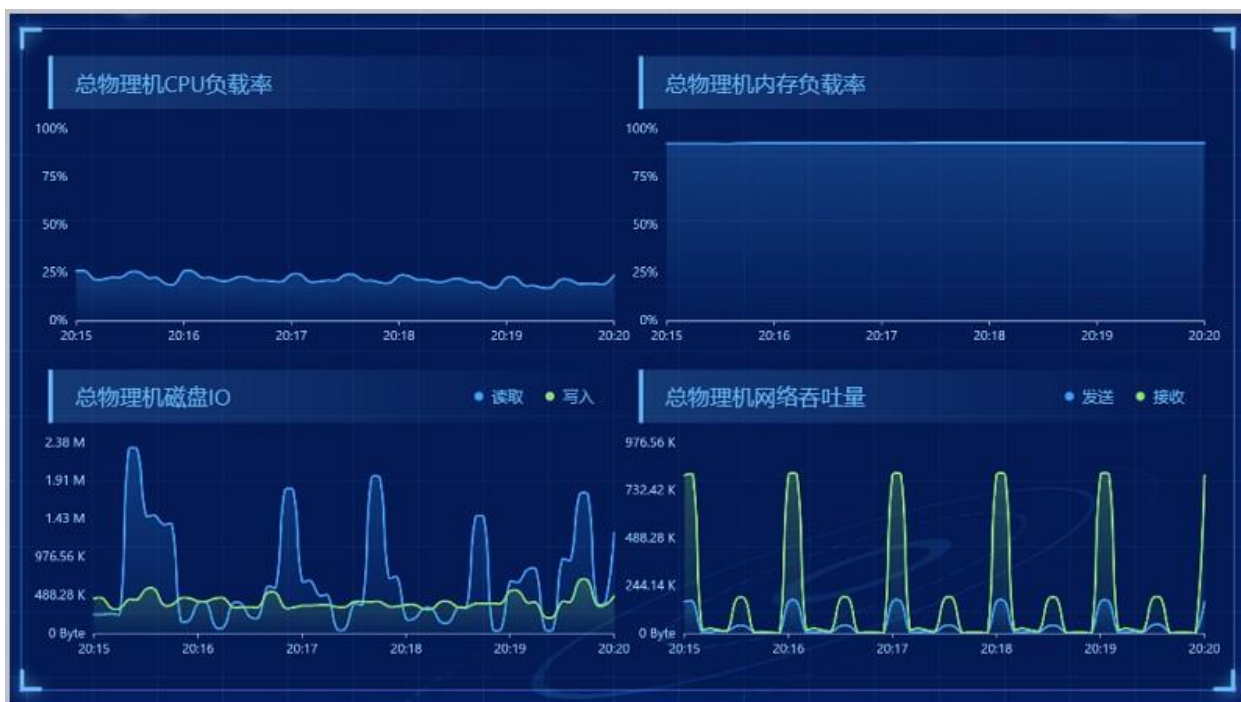


3. 物理机负载统计：总物理机CPU负载率、总物理机内存负载率、总物理机磁盘IO、总物理机网络吞吐量

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

如图 27: 负载统计所示：

图 27: 负载统计



4. 用量统计：CPU、内存、主存储、镜像服务器、私网IP、公网IP、GPU（vCenter大屏不包括GPU信息）、vGPU（vCenter大屏不包括vGPU信息）的实时资源用量统计

通过对所选虚拟化、区域中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、GPU、vGPU等资源，对它们的资源用量分别进行实时展示监控，实时显示的比例结合进度条的蓝、黄、红三色提示可直观告知用户当前资源的使用量。

如图 28: 用量统计所示:

图 28: 用量统计



- 其中KVM的私网IP、公网IP分别支持显示IPv4和IPv6资源使用情况，点击图表下方的小箭头进行切换。
- 若云平台未加载GPU和vGPU，用量统计中不显示GPU和vGPU的比例图表。
 - 不同颜色表示不同的比例范围：[0, 60)%-蓝色；[60, 80)%-黄色；[80, 100)%-红色。

5. 资源总览：云主机、物理机、镜像、集群（vCenter大屏不包括集群信息）的实时资源总览

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

如图 29: 资源总览所示：

图 29: 资源总览



科技款大屏采用机械设计风格，并加入动态效果，极具科技感。在经典款大屏信息展示（负载Top5、物理机负载统计、用量统计、资源总览）基础上，新增云主机负载统计、系统消息、账户总览和云主机标签云图信息展示，如图 30: KVM大屏监控界面和图 31: vCenter大屏监控界面所示：

图 30: KVM大屏监控界面



图 31: vCenter大屏监控界面



科技款大屏每隔21秒获取一次数据，主要分为以下几个部分：

1. 大屏切换：虚拟化、区域切换

Cloud大屏支持根据不同的虚拟化和区域显示，通过顶部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。

如图 32: 大屏切换所示：

图 32: 大屏切换



- 支持切换KVM或vCenter虚拟化。
- 支持切换所有区域或某个区域。
- KVM大屏监控与vCenter大屏监控区别如下：
 - vCenter大屏监控中不包括云主机标签云图。
 - vCenter大屏监控用量统计中不包括IPv6类型网络展示。

2. 负载趋势：总物理机的CPU负载、内存负载、磁盘IO、网络吞吐量

通过对所选虚拟化、区域中数据中心的全部物理的CPU、内存、磁盘、网络资源使用情况进行统计分析，以全部物理机的总CPU负载压力、总内存负载压力、总磁盘IO性能、以及总网络吞吐性能为指标，分别进行实时展示监控。

实时显示的动态曲线图结合不同监控项目的颜色区分，可直观告知用户当前全部物理机的整体资源使用状态以及性能状态。

如图 33: 负载趋势所示：

图 33: 负载趋势



负载趋势支持动态切换，每隔15秒对总物理机的负载统计图动态切换一次，也可手动点击切换。

3. 用量统计：CPU、内存、主存储、镜像服务器、私网IP、公网IP、GPU（vCenter大屏不包括GPU信息）、vGPU（vCenter大屏不包括vGPU信息）的实时资源用量统计

通过对所选虚拟化、区域中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、GPU、vGPU等资源，对它们的资源用量分别进行实时展示监控，实时显示的比例结合进度条的蓝、黄、红三色提示可直观告知用户当前资源的使用量。

如图 34: 用量统计所示：

图 34: 用量统计



- 用量统计信息每隔21秒推送一次，每次推送后可通过右下角的红色箭头或蓝色箭头，分别标识用量增减情况。
- 私网IP和公网IP支持切换IPv4、IPv6两种网络地址类型，默认15秒自动切换一次，支持手动点击切换。若仅存在一种网络地址类型，默认显示现有网络类型的用量统计信息，不支持自动切换。
- 若云平台未加载GPU和vGPU，用量统计中不显示GPU和vGPU的比例图表。
- 不同颜色表示不同的范围：[0, 60)%-蓝色；[60, 80)%-黄色；[80, 100]%-红色。

4. 资源总览：云主机、物理机、镜像、集群的实时资源总览

通过对所选虚拟化、区域中数据中心的云主机、物理机、镜像、集群的资源使用情况进行统计分析，对它们的资源总用量分别进行实时展示监控。

如图 35: 资源总览所示：

图 35: 资源总览



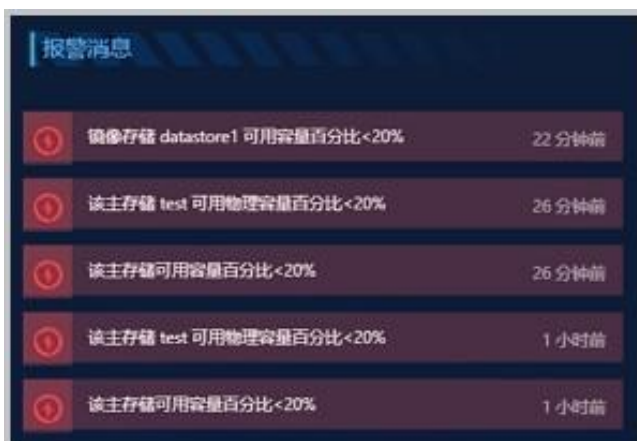
负载统计支持动态切换，每隔15秒动态切换一次，也可手动点击切换。

5. 报警消息：

通过对Cloud云平台中设置的报警消息收集，实时推送最新5条报警消息展示到大屏系统消息界面，可直观告知用户云平台当前存在哪些安全隐患。

如图 36: 报警消息所示：

图 36: 报警消息



- 系统消息展示云平台中KVM和vCenter的最新5条报警消息，不区分虚拟化和区域。
- 系统消息支持不同的标识：红色图标表示报警消息；蓝色图标表示报警恢复消息。

6. 账户总览：人员分布数量统计



- 负载Top5相关信息每隔21秒获取一次，支持进榜提示功能，每次获取Top5信息后，新进榜单的资源左侧提示new图标，持续5秒。
- 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。不同颜色表示不同的范围：[0, 60)%-蓝色；[60, 80)%-黄色；[80, 100)%-红色。



12 资源中心


12.1 云资源池


12.1.1 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。

云主机支持以下操作：




操作	描述	云主机状态
创建云主机	创建一个或多个云主机。	/
编辑	修改云主机的名称与简介。	运行中/已停止/已暂停
启动云主机	将处于停止状态的云主机启动。	已停止
停止云主机	将处于运行状态的云主机停止。	运行中
重启	将处于运行状态的云主机重启。	运行中
恢复	将处于暂停状态的云主机恢复。	已暂停
暂停	将处于运行状态的云主机暂停。 注： 暂停云主机并非真正停止云主机，若将已暂停云主机所在物理机停用，则影响业务运行。	运行中
关闭电源	将处于运行状态的云主机强制进入停止状态。  注： 正常状态下不建议执行关闭电源。	运行中
打开控制台	打开云主机控制台，可登录云主机系统。  注： <ul style="list-style-type: none"> 在云主机控制台，支持开机时设置Boot选项，点击ESC进入Boot选项菜单。 若无法打开云主机控制台，可尝试在<code>/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties</code>文件里将控制台代理IP地址改为当前管理节点IP地址。 	运行中
克隆	基于当前云主机计算规格，克隆出与当前云主机系统相同的云主机。	运行中/已停止/已暂停





操作	描述	云主机状态
	<ul style="list-style-type: none"> 在线克隆云主机，只针对克隆任务开始时已写入磁盘的数据，不包括实时缓存数据。为确保数据完整性，高IO的云主机建议将其暂停或关机后再克隆。 云主机配置、安装程序、密码等都会复制到新克隆出的云主机内，但并不考虑其他配置的复制，例如：标签、定时任务等。 克隆出的云主机处于启动状态，重启后控制台密码才会生效。 克隆云主机时，如果使用Shared Block类型的主存储，需要选择置备方式，包括厚置备、精简置备 <ul style="list-style-type: none"> 厚置备：预先分配需要的存储空间，提供充足的存储容量给云主机，保证存储性能 精简置备：按实际使用情况分配存储空间给云主机，实现更高的存储利用率 克隆云主机时，如果使用Ceph类型的主存储，支持指定存储池 <ul style="list-style-type: none"> 不带云盘克隆云主机时，支持指定Ceph存储池（根云盘池） 使用ImageStore类型的镜像服务器带云盘克隆云主机时，支持指定数据云盘池和根云盘池 克隆云主机时需避免对源云主机设置静态IP，否则将导致多台云主机IP相同，造成登录错误。 	
绑定标签	<p>为一个或多个云主机绑定标签。</p> <p> 注：</p> <ul style="list-style-type: none"> 单个资源最多支持绑定50个标签。反之，单个标签支持绑定的资源数量无限制。 标签-资源支持多对多绑定关系。 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。 管理员支持解绑/删除租户标签。 资源标签按照绑定时间或标签名称（符号>数字>中文>英文）进行排序，可在设置 > 平台设置 > 全局设置 > 基本设置中修改标签排序方式，默认按标签名称排序。 	运行中/已停止/已暂停




操作	描述	云主机状态
解绑标签	<p>解绑云主机上的标签。</p> <p> 注:</p> <ul style="list-style-type: none"> 管理员标签由管理员（admin/平台管理员）创建，归管理员所有，租户标签由租户（子账户/项目）创建，归租户所有。 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。 管理员支持解绑/删除租户标签。 项目内的标签归属于项目所有，项目内所有人（项目负责人/项目管理员/项目成员）均可操作。 标签暂不支持更改所有者操作。 资源更改所有者，其上所有租户标签将会解绑，管理员标签不受影响。 云平台无缝升级后，已有旧标签将自动更新，以最新方式展示标签。若有异常，请刷新浏览器或重新创建标签。 支持将单个资源上的批量标签解绑，也支持将单个标签上的批量资源解绑。 租户只能解绑所属租户资源上的标签，管理员可解绑所有资源上的标签。 	运行中/已停止/已暂停
云主机迁移	<p>将云主机迁移到其他计算节点。</p> <ul style="list-style-type: none"> - 本地存储场景：支持本地存储的云主机的热迁移和冷迁移。 - 共享存储场景：支持共享存储的云主机的热迁移。 - 热迁移：迁移运行状态下的云主机，主要是为拷贝CPU相关寄存器的状态及内存的信息。 <ul style="list-style-type: none"> ■ 本地存储热迁移不支持带有数据云盘的云主机的迁移。 ■ 本地存储热迁移不支持Windows云主机的迁移。 ■ 热迁移选择目标计算节点时，可按需启用自动收敛模式，保证处于高业务云主机迁移能顺利完成。 <ul style="list-style-type: none"> ■ 默认不启用，表示不启用自动收敛模式由全局设置auto-converge功能开关控制。 	运行中/已停止


操作	描述	云主机状态
	<ul style="list-style-type: none"> ■ 若云主机长时间处于高业务状态而影响迁移，可启用自动收敛模式，使云主机迁移能顺利完成。 ■ 热迁移具体步骤如下： <ol style="list-style-type: none"> 1. 在Cloud主菜单，进入设置 > 平台设置 > 全局设置 > 基本设置，将在线迁移设为true。 2. 将数据云盘从云主机上卸载。 3. 将云主机、数据云盘分别迁移至其它相同的计算节点。 4. 将卸载的数据云盘重新加载到该云主机。 - 冷迁移：迁移停止状态下的云主机。 <ul style="list-style-type: none"> ■ 冷迁移具体步骤如下： <ol style="list-style-type: none"> 1. 停止云主机。 2. 卸载云主机上的数据云盘。 3. 将云主机、数据云盘分别迁移至其它相同的计算节点。 4. 将卸载的数据云盘重新加载到该云主机。 - 支持按目标计算节点负载高低迁移云主机。 <ul style="list-style-type: none"> ■ 在目标计算节点的推荐列表，目标计算节点支持按CPU平均使用率或内存使用率排序（默认为内存使用率由低到高排序）。 ■ 若集群中计算节点规模较大，支持按Top20、Top50两种排序方式。 <p> 注：迁移云主机需要注意以下情况：</p> <ul style="list-style-type: none"> • 冷/热迁移前需确保云主机加载的数据云盘、ISO以及外接设备均已卸载。 • 热迁移前需确保云主机加载的VF类型网卡已卸载。 • 若加载块设备的云主机已部署微软故障转移群集的Master节点，热迁移云主机将导致故障转移群集不可用，请谨慎操作。 • 迁移的速度与两台计算节点的网络配置有关，如果网络配置较低，迁移速度可能较慢。 	





操作	描述	云主机状态
存储迁移	<p>云主机支持跨同类型主存储的冷迁移，以及跨不同类型主存储的热迁移。</p> <ul style="list-style-type: none"> 跨同类型主存储冷迁移：支持云主机跨同类型主存储的冷迁移，包括：Ceph主存储-Ceph主存储、NFS主存储-NFS主存储、Shared Block主存储-Shared Block主存储。 <p> 注：</p> <ul style="list-style-type: none"> 对于跨Ceph主存储的存储迁移： <ul style="list-style-type: none"> 云主机迁移前必须关机，并卸载所有数据盘。 两个Ceph主存储的MON节点之间需网络互通。 对于跨NFS主存储的存储迁移： <ul style="list-style-type: none"> 云主机迁移前必须关机，并卸载所有数据盘。 目标NFS主存储能够被挂载到待迁移云主机所在集群。 对于跨Shared Block主存储的存储迁移： <ul style="list-style-type: none"> 云主机迁移前必须关机。支持对带云盘的云主机进行整机迁移。 若云主机带共享云盘，不支持同时迁移该共享云盘。 目标Shared Block主存储能够被挂载到待迁移云主机所在集群。 目标主存储所挂载集群能够满足云主机的网络需求。 跨不同类型主存储热迁移：支持云主机跨不同类型主存储的热迁移，包括：Ceph主存储-Shared Block主存储、本地存储-Shared Block主存储、本地存储-Ceph主存储、本地存储-NFS主存储、SharedBlock主存储-NFS主存储、Ceph主存储-NFS主存储。 <p> 注：</p> <ul style="list-style-type: none"> 云主机迁移前不要关机。 仅支持对云主机进行整机迁移，若云主机带共享云盘，不支持同时迁移该共享云盘。 	运行中/已停止



操作	描述	云主机状态
	<ul style="list-style-type: none"> 运行中的云主机在存储迁移后将不会保留快照。 目标主存储所挂载集群能够满足云主机的网络需求。 <p> 注:</p> <ul style="list-style-type: none"> 存储迁移前需确保云主机加载的ISO、块设备、以及外接设备均已卸载。 对运行中云主机进行存储迁移前，需确保云主机加载的VF类型网卡已卸载。 	
修改计算规格	<p>修改云主机计算规格。</p> <p> 注: 修改后，新计算规格中仅CPU、内存和物理机分配策略对云主机生效。</p> <ul style="list-style-type: none"> Linux云主机支持在线/关机修改计算规格（CPU/内存） <ul style="list-style-type: none"> 开机修改: <ol style="list-style-type: none"> 在线修改云主机计算规格。在Cloud主菜单，点击设置 > 平台设置 > 全局设置 > 基本设置，将NUMA设为true。 重启云主机。 在云主机界面，选择某一运行中的云主机，点击操作 > 系统配置 > 修改计算规格，在打开的计算规格列表中选择。 关机修改: <p>在云主机管理界面，选择某一已停止的云主机，点击操作 > 系统配置 > 修改计算规格，在打开的计算规格列表中选择。</p> 也可在云主机详情界面直接修改CPU/内存，开启NUMA后支持在线修改。未开启时仅支持关机修改。 Windows云主机支持在线/关机修改计算规格（CPU/内存），修改方法同Linux云主机一致。 <p> 注:</p> <ul style="list-style-type: none"> 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。 	运行中/已停止


操作	描述	云主机状态
设置 GPU规格	<p>为云主机设置GPU规格，包括加载GPU规格、修改GPU规格、取消GPU规格。</p> <ul style="list-style-type: none"> • 设置物理GPU规格：为单个或多个云主机设置GPU规格 <p> 注：</p> <ul style="list-style-type: none"> • 已设置物理GPU规格、已设置物理GPU设备或运行中的云主机无法设置物理GPU规格。 • 未设置物理GPU规格或运行中的云主机无法修改物理GPU规格。 • 修改物理GPU规格后，下次启动云主机将使用最新物理GPU规格重新加载物理GPU设备，并卸载原物理GPU规格相关的物理GPU设备。 <ul style="list-style-type: none"> • 设置vGPU规格：为单个或多个云主机设置vGPU规格。 <p> 注：</p> <ul style="list-style-type: none"> • 已设置vGPU规格、已设置vGPU设备或运行中的云主机无法设置vGPU规格。 • 未设置vGPU规格或运行中的云主机无法修改vGPU规格。 • 修改vGPU规格后，下次启动云主机将使用最新vGPU规格重新加载vGPU设备，并卸载原vGPU规格相关的vGPU设备。 <ul style="list-style-type: none"> • 不设置：将单个或多个云主机的GPU规格取消。 <p>注：未加载GPU规格或运行中的云主机无法取消GPU规格。</p> <p></p>	已停止
系统扩容	<p>为云主机扩容根云盘容量。</p> <ul style="list-style-type: none"> • 在云主机运行或者停止状态下，点击系统扩容，可按需进行根云盘扩容，更改容量及时生效。 <p>在云主机管理界面，选择某一运行中/已停止的云主机，点击操作 > 系统配置 > 系统扩容，弹出系统扩容界面。可按需进行根云盘扩容，更改容量即时生效。</p> <p> 注：</p>	运行中/已停止


操作	描述	云主机状态
	<ul style="list-style-type: none"> 扩容容量只增不减，增量不得小于4MB。单位包括：MB/GB/TB。 系统扩容将触发一次该云主机系统云盘的自动快照，以保护数据安全。 	
更改所有者	将云主机的所有者更改。  注： 更改所有者，其上所有租户标签将会解绑，管理员标签不受影响。	运行中/已停止
更换系统	为云主机更换系统。 <ul style="list-style-type: none"> 将云主机停止后，点击更换系统，在弹出的更换系统界面，选择目标镜像即可，目标镜像需为Image类型。更换系统后，云主机保持关机状态。  注： <ul style="list-style-type: none"> 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。 在执行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。 	已停止
重置云主机	将云主机重置。  注： <ul style="list-style-type: none"> 如果云主机使用镜像创建，可重置该云主机到创建时的状态。 云主机必须处于已停止状态。在云主机管理界面，选择某一已停止的云主机，点击操作 > 系统配置 > 重置云主机，重启云主机后生效。 使用ISO安装创建的云主机不支持重置功能。 	已停止
设置启动顺序	为云主机设置启动顺序。 <ul style="list-style-type: none"> 如果在创建云主机时，镜像选择为ISO，云主机将首先从CdRom（光盘）启动。 	运行中/已停止


操作	描述	云主机状态
	<ul style="list-style-type: none"> 如果云主机创建之后加载ISO，云主机默认的启动顺序是：第一顺序为HardDisk（硬盘），第二顺序为CdRom（光盘）。 如果需要云主机从Network（网络）启动，需要手动设置第一启动顺序为Network（网络）。 如需更改启动顺序，例如通过ISO启动来修复硬盘，操作如下： 在云主机管理界面，选择某一云主机，点击操作 > 系统配置 > 设置启动顺序，以更改云主机启动顺序。 <p> 注：</p> <ul style="list-style-type: none"> 将运行中的云主机第一启动顺序设置为CdRom（光盘）或Network（网络），则只有通过重启、停止再启动操作，云主机才会从CdRom（光盘）或Network（网络）启动。 如果直接在云主机操作系统中通过 <code>reboot</code> 命令重启，云主机还是会从HardDisk（硬盘）启动。 	
指定物理机启动	<p>为云主机指定物理机启动。</p> <ul style="list-style-type: none"> 使用共享存储的云主机停止后，可以选择在指定的物理机上重新启动。 <p>在云主机管理界面，选择某一云主机，点击操作 > 系统配置 > 指定物理机启动，在打开的物理机列表选定后，该云主机可直接从选择的物理机启动。</p> <ul style="list-style-type: none"> 使用本地存储的云主机停止后，只能从该云主机根云盘所在的物理机启动。 	已停止
设置高可用	<p>为云主机设置高可用模式，包括启用高可用模式和禁用高可用模式。</p> <ul style="list-style-type: none"> 禁用高可用功能 启用高可用功能 <p>本地存储的云主机设置启用高可用模式：</p> <ul style="list-style-type: none"> 当所在物理机处于启用和已连接状态时，该云主机一直运行。即使强制关机，该云主机也会再次启动。 	运行中/已停止



操作	描述	云主机状态
	<p> 注: 如希望启用高可用功能的云主机本次关机不自动启动, 在弹出的停止云主机窗口, 启用对于启用高可用功能的云主机, 本次停止将不会自动重启即可。</p> <ul style="list-style-type: none"> 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。 <p>共享存储的云主机设置启用高可用模式:</p> <ul style="list-style-type: none"> 在已添加的物理机里, 只要有任意一台资源允许, 该云主机会一直运行。即使强制关机, 该云主机也会再次启动。 <p> 注: 如希望启用高可用功能的云主机本次关机不自动启动, 在弹出的停止云主机窗口, 启用对于启用高可用功能的云主机, 本次停止将不会自动重启即可。</p> <ul style="list-style-type: none"> 当所在物理机异常断电/断网时, 只要资源允许, 该云主机会迁移至其它物理机运行。 	
设置时间同步	<p>启用后云主机基准时间将与物理机保持一致, 默认启用</p> <p> 注: 若云主机处于运行中或已暂停状态, 必须重启云主机后生效。</p>	运行中/已停止/已暂停
设置SSH KEY	<p>为云主机设置SSH Key。</p> <p>在云主机管理界面, 选择某一云主机, 点击操作 > 系统配置 > 设置SSH KEY, 进入设置SSH KEY界面。在文本框中输入要设置的SSH KEY, 点击确认, 重启后生效。</p> <p> 注:</p> <ul style="list-style-type: none"> SSH Key注入需镜像提前安装Cloud-Init。 创建云主机时注入SSH KEY可以直接生效。 创建云主机后注入SSH KEY (包括云主机启动中或运行中时), 需要执行命令<code>rm -rf /var/lib/cloud/instances</code>清理配置并重启云主机才可生效。 	运行中/已停止
修改云主机密码	为云主机修改密码。	运行中


操作	描述	云主机状态
	<p>修改云主机密码需要满足以下几个条件：</p> <ul style="list-style-type: none"> 云主机处于运行中状态。 云主机已成功安装QGA并确保详情页QGA开关处于“已安装”。 <p>修改云主机密码需要注意以下情况：</p> <ul style="list-style-type: none"> 以下镜像类型支持修改云主机密码： <ul style="list-style-type: none"> CentOS 7.x\6.x（32位\64位） Ubuntu 16.x\15.x\14.x\13.x\12.x\（64位） Windows 2003\2008\7\10\2012\2016（64位） 若原云主机支持修改密码，创建云主机镜像、克隆操作将继承该功能。 使用Ceph类型镜像服务器添加镜像，已启用支持修改密码的qcow2镜像所创建的云主机，也支持该功能。 如果修改云主机密码失败，请先检查云主机中是否已安装Qemu Guest Agent，在终端手动检查QGA的运行状态是否正常。 	
设置控制台密码	<p>为云主机设置控制台密码。</p> <ul style="list-style-type: none"> 该密码为VNC协议的密码，不是云主机本身的密码。 设置完成后，重启云主机才可生效 	运行中/已停止
切换控制台模式	<p>为云主机切换控制台模式，包括VNC、SPICE、VNC+SPICE。</p>	运行中/已停止/已暂停
设置RDP模式	<p>为云主机设置RDP模式。</p> <p> 注：针对VDI用户界面，选择RDP模式后，默认以RDP模式打开控制台。</p>	运行中/已停止/已暂停
资源优先级	<p>为云主机设置资源优先级。</p> <p>支持正常、高两种优先级，默认为正常。当出现资源竞争时，优先保证资源优先级为高的云主机的资源使用</p> <p> 注：请仅对重要的云主机设置高资源优先级。</p>	运行中/已停止/已暂停
跨集群高可用策略	<p>为云主机设置跨集群高可用策略。</p> <ul style="list-style-type: none"> 策略默认开启，表示云主机可跨集群自动迁移。 	运行中/已停止/已暂停

操作	描述	云主机状态
	<ul style="list-style-type: none"> 该策略关闭后，云主机将限制在策略生效时所在集群内活动。 背景说明： <ul style="list-style-type: none"> 在3.8.0之前版本中，当云主机高可用策略触发或者云主机所在物理机进入维护模式时，系统会选择其他合适的物理机自动恢复（或迁移）该云主机，合适的物理机可能在当前集群、甚至跨集群（如果多个集群挂载了相同的三层网络和主存储）。 从3.8.0版本开始，云主机支持设置跨集群高可用策略，该策略关闭后，云主机将限制在策略生效时所在集群内活动。 目前适用场景：云主机高可用更换物理机启动、物理机进入维护模式触发迁移。 该策略只针对云主机自动迁移行为有影响，其它如：手动热迁移云主机、指定物理机启动云主机、基于动态资源调度策略迁移云主机等均不受影响。 启用后，上述适用场景的云主机活动将不受集群范围限制。 	
USB重定向	<p>为云主机设置USB重定向。</p> <ul style="list-style-type: none"> 当前支持兼容多种USB设备重定向，当用户需要使用VDI功能时，可将VDI客户端的USB设备重定向给VDI云主机。 需重启云主机生效。 	运行中/已停止/已暂停
创建快照	<p>为云主机创建快照。</p> <p>做重要操作前，对云主机根云盘或数据云盘在特定时间点进行临时状态保留，方便出现故障后迅速回滚。</p> <ul style="list-style-type: none"> 云主机快照包括单盘快照和快照组两种类型： <ul style="list-style-type: none"> 单盘快照：对云主机根云盘创建快照。 快照组：对云主机根云盘及所加载的数据云盘创建快照。支持以快照组为单位统一恢复。 <p>注：若云主机已加载共享云盘，不支持创建快照组。</p> <p> 支持对运行中或已停止的云主机或弹性裸金属实例创建快照。</p>	运行中/已停止/已暂停

操作	描述	云主机状态
	<ul style="list-style-type: none"> 弹性裸金属实例暂不支持创建快照组。 若云主机已加载共享云盘，不支持创建快照组。 在生产环境中，建议单块磁盘的快照数量尽量控制在5以内。快照过多会影响云主机/云盘/弹性裸金属实例的I/O性能、数据安全以及主存储容量。如需长期备份，建议使用灾备服务。 在生产环境中，为确保数据完整性，不建议对高I/O的云主机或弹性裸金属实例创建快照。当云主机或弹性裸金属实例内部进行高I/O操作时，对云主机或弹性裸金属实例创建快照，内存中存在部分数据没有落入硬盘，这部分数据将无法保存到快照中。 Ceph主存储上的云主机/云盘/弹性裸金属实例快照不占用容量，所显示的快照容量表示创建快照时云主机/云盘/弹性裸金属实例的真实容量。 Ceph主存储场景下，关于云主机/云盘/弹性裸金属实例快照容量无法获取的说明： <ul style="list-style-type: none"> Ceph开源版（H版）、Ceph企业版（3.2.0以下版本）均不支持获取云主机/云盘/弹性裸金属实例快照容量。 Ceph企业版（3.2.0及以上版本）由于RBD format影响，可能出现无法获取云主机/云盘/弹性裸金属实例快照容量。 Shared Block以及Ceph主存储上创建的共享云盘，不支持创建快照。 	
创建备份	<p>对运行中的云主机创建备份数据。</p> <ul style="list-style-type: none"> 云主机需处于开机状态，才可对其创建备份。 支持对云主机进行全量备份，若不选择全量备份，则表示对云主机进行增量备份。 支持对带云盘的云主机进行整机备份，若云主机带共享云盘，不支持同时备份该共享云盘。 	运行中
加载云盘	<p>将一个可用、未加载的云盘加载到云主机。</p> <p> 注：</p> <ul style="list-style-type: none"> 一台云主机最多可加载24个数据云盘。 如果主存储为本地存储，该云盘须与云主机在同一台物理机上。如果该云盘和云主机不在同 	运行中/已停止

操作	描述	云主机状态
	一个物理机上，需提前将该云盘迁移到云主机所在的物理机上。	
卸载云盘	<p>为已加载的云盘从云主机卸载。</p> <p>具体步骤如下：</p> <ol style="list-style-type: none"> 1. 在云主机管理界面，选择某一云主机，点击操作 > 云盘 > 卸载云盘，进入选择卸载云盘界面。 2. 从云盘列表选择需要卸载的云盘，点击确认。 	运行中/已停止
创建镜像	<p>创建云主机镜像。</p> <ul style="list-style-type: none"> • 创建云主机镜像操作说明： <ul style="list-style-type: none"> - 在云主机管理界面，选择某一云主机，点击操作 > 镜像与ISO > 创建镜像，弹出创建镜像界面，按需填写相关参数，创建云主机镜像。 - 进入镜像管理界面，点击操作按钮，按需操作云主机镜像。 	运行中/已停止
加载ISO	<p>为云主机加载ISO。</p> <p>Cloud支持挂载多个ISO，最多支持添加3个，不支持批量加载。具体步骤如下：</p> <ol style="list-style-type: none"> 1. 在云主机管理界面，选择某一云主机，点击操作 > 镜像与ISO > 加载ISO，进入加载ISO界面。 2. 在加载ISO列表，选择需要加载的ISO，点击确认按钮，进行加载。 3. 重复上述操作加载其他ISO。 <p> 注：加载ISO将按照云主机虚拟光驱名称顺序加载。</p>	运行中/已停止
卸载ISO	<p>将已添加的ISO镜像从云主机中卸载，支持批量卸载。</p> <ul style="list-style-type: none"> • 在云主机管理界面，选择某一云主机，点击操作 > 镜像与ISO > 卸载ISO，进入卸载ISO界面。 • 在卸载ISO列表勾选需要卸载的ISO，点击确认按钮，进行卸载。 	运行中/已停止
绑定亲和组	<p>绑定云主机到亲和组，组策略对该云主机即时生效。</p> <p>目前Cloud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)。</p>	运行中/已停止

操作	描述	云主机状态
	<ul style="list-style-type: none"> 反亲和组(非强制): 将亲和组内的云主机尽量分配到不同物理机上, 当没有更多物理机可分配时, 回归普通分配策略。 反亲和组(强制): 将亲和组内的云主机严格分配到不同物理机上, 当没有更多物理机可分配时, 则分配失败。 	
解绑亲和组	将云主机从亲和组解绑, 组策略对该云主机即时失效。	运行中/已停止
删除云主机	<p>删除选中的云主机, 支持三种云主机删除模式:</p> <ul style="list-style-type: none"> 立刻删除 (Direct) : 删除云主机后, 云主机相关资源立刻被删除。 延时删除 (Delay) : 删除云主机后, 云主机的启用状态会被标记为已删除, 并移至已删除页面。系统默认使用此种删除策略 <p> 注:</p> <ul style="list-style-type: none"> 系统默认24小时后会彻底删除这些云主机。 可在Cloud主菜单的设置 > 平台设置 > 全局设置 > 基本设置页面, 点击云主机删除策略, 更改彻底删除时延的时间。 永不删除 (Never) : 删除云主机后, 云主机相关资源永远不删除。 <p> 注:</p> <ul style="list-style-type: none"> 可在Cloud主菜单的设置 > 平台设置 > 全局设置 > 基本设置页面, 通过修改云主机删除策略的值来设置默认的云主机删除模式。 在删除云主机弹出的确认窗口, 若勾选同时删除已加载云盘, 会同时删除此云主机已加载的所有普通云盘, 不会删除共享云盘。 	运行中/已停止/已暂停
彻底删除/恢复云主机	<p>将已删除栏中的云主机彻底删除或恢复。</p> <ul style="list-style-type: none"> 彻底删除: 选择彻底删除后, 云主机相关资源会被彻底删除, 不可逆转, 请谨慎操作。 恢复: 	已删除

操作	描述	云主机状态
	<p>恢复后的云主机回到可用资源页面，且启用状态为已停止，用户可以重新启动该云主机。</p> <p> 注:</p> <ul style="list-style-type: none"> 删除云主机后，其IP地址会返回IP地址池中。恢复云主机，会为其重新分配IP地址。 云主机、镜像、云盘均支持恢复和彻底删除。 	

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。
- 设置主机名后请勿在User Data中再次设置主机名，避免冲突。
- 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/路由器网络、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。
 - Linux云主机可进入`/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透传功能需要提前在物理主机的BIOS里面打开IOMMU或者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。
- 建议将针对Linux云盘的开机自动挂载在/etc/rc.d/rc.local中写入，并提供可执行权限。不建议修改云主机的/etc/fstab文件，在动态卸载云盘后，否则在对云主机进行重启操作时，云主机会因为无法找到/etc/fstab定义的云盘信息而导致启动失败。

— 建议操作如下：

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 -t 云盘ID 目标挂载路径
```



注：建议使用云盘的文件系统UUID来挂载，而非/dev/vdb类似的盘符来挂载。

- 云主机继承其镜像的BIOS模式，包括Legacy、UEFI两种类型。



注：

- 需提前准备好相应镜像，添加镜像时需谨慎选择匹配的BIOS模式。
- 云主机详情页支持修改BIOS模式，请谨慎修改，模式不匹配可能导致云主机无法正常工作，修改后需重启云主机生效。
- 从Cloud 3.3.0开始：
 - 对于初装用户，若云主机为UEFI模式引导，其主板类型将默认为Q35主板，若云主机为Legacy模式引导，其主板类型将默认为i440FX；
 - 对于升级用户，从历史版本升级至3.3.0以及后续更高版本，对于UEFI模式引导的云主机，若之前主板类型为i440FX，升级后将默认修改为Q35；
 - 创建云主机推荐使用Legacy模式引导，确保使用稳定。若希望使用UEFI引导，建议从以下操作系统版本列表中选择相应的云主机镜像：

操作系统	BIOS模式	支持版本
Windows平台	UEFI	<ul style="list-style-type: none"> • Windows 8及以上版本

操作系统	BIOS模式	支持版本
	UEFI（兼容模块）	<ul style="list-style-type: none"> Windows 7 Windows Server 2008 R2
Linux平台	UEFI	<ul style="list-style-type: none"> CentOS 7.2 CentOS 7.3 CentOS 7.4及以上版本

- 全局设置打开NUMA选项后支持在线修改云主机的CPU和内存，需要注意以下情况：
 - 不建议在生产环境中对Windows云主机在线修改CPU和内存。
 - 只支持对运行中的云主机进行CPU、内存扩容；若需要缩容，需停止云主机。
 - 若对运行中的云主机进行内存扩容，但云主机没能自动激活新增内存，请尝试以下两条命令解决该问题：

```
% echo online > /sys/devices/system/memory/auto_online_blocks
% echo online > /sys/devices/system/memory/memoryXXX/state
```

详情请参考[how to online memory](#)。

- 若云主机需要使用IPv6网络，请注意以下情况：
 - 使用IPv6或IPv4+IPv6类型的网络创建云主机，需通过dhclient -6 NIC_NAME命令手动获取IP地址。
 - 推荐一台云主机仅使用一个IPv6地址，否则可能存在风险。
 - 若三层网络（公有网络、扁平网络、VPC网络）IP地址类型发生变化，需重启已使用该网络的云主机，配置才能生效。

12.1.2 云盘

云盘：为云主机提供存储，包括两种类型：根云盘、数据云盘。






注：云盘管理主要涉及数据云盘的管理。


云盘相关定义


- 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：云主机的数据云盘，用于云主机扩展的存储使用。

云盘支持以下操作：

操作	描述
创建云盘	<p>基于云盘规格创建一个新云盘。</p> <ul style="list-style-type: none"> 普通云盘和共享云盘均支持通过云盘规格或云盘镜像创建。 共享云盘支持Ceph主存储以及基于厚置备的Shared Block主存储，其他主存储类型暂不支持。 创建云盘时，若不指定主存储和云主机，创建的云盘处于未实例化栏中。
编辑云盘	修改云盘的名称和简介。
启用云盘	将处于停用状态的云盘启用。
停用云盘	停止使用某个云盘。
加载实例	<ul style="list-style-type: none"> 将选中的云盘作为数据云盘加载到指定的实例。 <ul style="list-style-type: none"> 若主存储为本地存储，如果加载一个卸载过的云盘，需要保证该云盘和目标云主机在同一台物理机上。如果该云盘和目标云主机不在同一台物理机上，需将云盘和云主机迁移到同一台物理机上。
卸载实例	<p>卸载实例的云盘。</p> <p> 注：此操作将导致云盘读写业务中断，可能影响业务连续性，请谨慎操作。</p>
云盘迁移	<p>将云盘迁移到其他计算节点。</p> <ul style="list-style-type: none"> 支持按目标计算节点负载高低迁移云盘。 <ul style="list-style-type: none"> 在目标计算节点的推荐列表，目标计算节点支持按CPU平均使用率或内存使用率排序（默认为内存使用率由低到高排序）。 若集群中计算节点规模较大，支持按Top20、Top50两种排序方式。 该迁移操作只针对本地主存储。
存储迁移	<p>支持云盘跨同类型主存储的迁移，包括：Ceph主存储-Ceph主存储、NFS主存储-NFS主存储、Shared Block主存储-Shared Block主存储。</p> <ul style="list-style-type: none"> Ceph主存储-Ceph主存储： <ul style="list-style-type: none"> 跨Ceph存储迁移的云盘要求没有被加载在任何云主机上。 所涉及的两个Ceph存储，要求彼此的MON节点可以互通。 NFS主存储-NFS主存储：

操作	描述
	<ul style="list-style-type: none"> 跨NFS存储迁移的云盘要求没有被挂载在任何云主机上。 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。 Shared Block主存储-Shared Block主存储： <ul style="list-style-type: none"> Shared Block存储上的云盘可以挂载在停止的云主机上进行跨Shared Block存储迁移。 未加载到云主机的共享云盘支持跨Shared Block存储迁移；已加载到云主机的共享云盘不支持跨Shared Block存储迁移。 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。 <p> 注：</p> <ul style="list-style-type: none"> 云盘存储迁移后原始数据保留在主存储中，可在主存储详情页的数据清理子页面查看。 支持清理操作。确认存储迁移后数据完整无损时，可手动清理原始数据。清理后不可恢复，请谨慎操作。
更改所有者	<p>可以更改云盘的所有者。</p> <ul style="list-style-type: none"> 更改所有者，其上所有租户标签将会解绑，管理员标签不受影响。
云盘扩容	<p>在云主机运行或者停止状态下，支持对根云盘/数据云盘扩容。</p> <ul style="list-style-type: none"> 扩容容量只增不减，增量不得小于4MB。更改容量即时生效。 新容量必须为4MB的整数倍，例如填写新容量为37MB，实际扩容到40MB。 在Shared Block主存储上创建的共享云盘，不支持云盘扩容。 在Ceph主存储上创建的共享云盘，需确保未加载到任何云主机或所加载云主机已关机，才可进行云盘扩容。 云盘扩容将触发一次该数据云盘的自动快照，以保护数据安全。
绑定标签	<p>为云盘绑定标签。</p> <ul style="list-style-type: none"> 资源标签按照绑定时间或标签名称进行排序，默认按标签名称排序，可在全局设置中修改标签排序方式。 <p> 注：</p> <ul style="list-style-type: none"> 按标签名称排序优先级为：符号，数字，中文，英文，英文不区分大小写。 历史版本（3.4.0及之前版本）升级到最新版本后，资源标签将默认按标签名称进行排序。

操作	描述
解绑标签	<p>将云盘上的标签解除绑定。</p> <p> 注:</p> <ul style="list-style-type: none"> 管理员标签由管理员（admin/平台管理员）创建，归管理员所有，租户标签由租户（子账户/项目）创建，归租户所有。 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。 管理员支持解绑/删除租户标签。 项目内的标签归属于项目所有，项目内所有人（项目负责人/项目管理员/项目成员）均可操作。 标签暂不支持更改所有者操作。 资源更改所有者，其上所有租户标签将会解绑，管理员标签不受影响。 云平台无缝升级后，已有旧标签将自动更新，以最新方式展示标签。若有异常，请刷新浏览器或重新创建标签。 支持将单个资源上的批量标签解绑，也支持将单个标签上的批量资源解绑。 租户只能解绑所属租户资源上的标签，管理员可解绑所有资源上的标签。
创建备份	<p>对云盘创建备份数据。</p> <ul style="list-style-type: none"> 云盘需加载到开机状态的云主机，才可对其创建备份。 支持对云盘进行全量备份和增量备份。默认对云盘进行增量备份。 支持将备份数据同步至远端备份服务器。
创建云盘镜像	<p>对当前云盘进行创建镜像操作，此镜像可用于创建新的云盘。</p> <ul style="list-style-type: none"> 支持创建云盘镜像，且支持为Ceph主存储上的云盘创建云盘镜像，并存储至镜像仓库类型的镜像服务器。 为Shared Block主存储上的共享云盘创建镜像，需先停止所有加载该云盘的云主机。
创建云盘快照	<p>做重要操作前，对根云盘或数据云盘在特定时间点进行临时状态保留，方便出现故障后迅速回滚。</p> <ul style="list-style-type: none"> 快照可以保存当前云盘的所有数据，用户可以使用快照快速得把云盘的状态恢复到历史的某个状态。若需长期备份，请选择灾备相关功能。 首次创建快照，可能需较久时间来进行快照存储。 共享云盘暂不支持创建快照。

操作	描述
设置云盘QoS	<p>通过设置总速度或读写速度的方式，设置云盘带宽上限。</p> <ul style="list-style-type: none"> 如果云盘规格中没有设置云盘QoS（默认无限制），普通账户/项目成员支持任意设置云盘QoS。 如果云盘规格中已设置云盘QoS，普通账户/项目成员支持设置云盘QoS，但设置上限不能超过云盘规格中规定的上限。 普通账户/项目成员设置云盘QoS的方式不可改变，与原方式保持一致（总速度或读写速度）。
删除云盘	<p>将云盘删除后，云盘会显示在已删除栏。</p> <p> 注：删除云盘需要注意以下情况：</p> <ul style="list-style-type: none"> 删除云盘将同时解除与云主机加载关系，中断云盘读写数据，请谨慎操作。 删除云盘将同时解除与弹性裸金属实例加载关系，中断云盘读写数据，请谨慎操作。
彻底删除/恢复云盘	<p>支持将已删除的云盘彻底删除或进行恢复操作，恢复后云盘将显示在可用栏。</p>

注意事项

使用云盘需注意：

- 不同Hypervisor上的云盘不可加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）云盘同一时间只能加载到一个云主机。Ceph类型的主存储和Shared Block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的不同云主机之间加载和卸载。
- 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I/O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.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: 建议使用云盘的文件系统UUID来挂载, 而非`/dev/vdb`类似的盘符来挂载。

12.1.3 镜像

镜像: 云主机或云盘使用的镜像模板文件, 包括两种类型: 系统镜像、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, 使用该平台类型可以兼容一些不支持Virtio驱动的低版本操作系统, 例如RHEL 5.8。
- 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:

- **URL:** 采用指定的URL路径来添加镜像, 支持以下格式:
 - HTTP/HTTPS格式:
 - 填写格式为: `http://host[:port]/path/file`或`https://host[:port]/path/file`
 - FTP格式:
 - 匿名模式: `ftp://hostname[:port]/path/file`
 - 非匿名模式: `ftp://user:password@hostname[:port]/path/file`
 - SFTP格式:

- 指定密码模式: `sftp://user:password@hostname[:port]/path/file`
- 免密模式: `sftp://user@hostname[:port]/path/file`
- 镜像服务器上的绝对路径, 支持ImageStore镜像服务器

例如: `file:///path/file`

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ImageStore镜像服务器, 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。
- 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/dvd/image-1.4.qcow2`, 在镜像服务器的`/opt/dvd`目录下应存放有`image-1.4.qcow2`文件。
- **本地文件:** 选择当前浏览器可访问的镜像直接上传, 支持ImageStore和Ceph镜像服务器



注:

- ImageStore类型的镜像服务器支持断点续传功能, 若用户刷新浏览器、关闭浏览器或管理节点服务停止, 该任务将自动暂停, 反之则任务执行失败。
- 用户可点击**平台运维 > 消息日志 > 操作日志 > 当前任务 > 添加镜像 > 操作**, 对该任务进行取消、暂停或继续操作。

镜像支持以下操作:

操作	描述
添加镜像	添加一个新的镜像到镜像服务器。
编辑镜像	修改镜像的名称与简介。
启用镜像	将处于停用状态的镜像启用。
停用镜像	将处于启用状态的镜像停用。停用后不能再用其创建云主机, 但不影响之前已创建的云主机。

操作	描述
导出镜像	<p>导出某个镜像。由于镜像可能较大，导出的时间会较长。导出后的镜像显示在导出记录栏。</p> <p> 注： 只有ImageStore类型镜像服务器上的镜像支持镜像导出及已导出镜像删除功能。</p>
存储迁移	<p>进行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。对于跨Ceph类型镜像服务器的数据迁移，要求两个Ceph镜像服务器的mon节点可以互通。</p> <p>注：</p> <ul style="list-style-type: none"> • 镜像存储迁移后原始数据保留在镜像服务器中，可在Ceph镜像服务器详情页的数据清理子页面查看。 • 支持清理操作，确认存储迁移后数据完整无损时，可手动清理原始数据。清理后不可恢复，请谨慎操作。 <p></p>
同步镜像	<p>同一管理节点下，将一个/多个镜像服务器中的镜像同步至指定镜像服务器。目前只支持ImageStore类型。</p> <p>注： 镜像服务器可以设置单独的镜像同步网络，以减轻管理网络压力。设置方法有如下两种：</p> <p></p> <ul style="list-style-type: none"> • 在添加镜像服务器时设置镜像同步网络。 • 在镜像服务器详情页设置镜像同步网络，设置后立即生效。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> • 全局共享：将资源共享给所有的项目和账户使用。 • 指定共享：将资源共享给指定的项目和账户使用。 • 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p>注：</p> <ul style="list-style-type: none"> • 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 • 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。 <p></p>
删除镜像	将镜像删除。删除后，镜像会显示在 回收站 栏。
恢复镜像	将已删除的镜像恢复。恢复后，镜像会显示在 可用资源 栏。
彻底删除镜像	将已删除的镜像彻底删除。只有回收站的镜像才支持彻底删除。

操作	描述
下载已导出镜像	<p>下载已导出的镜像。执行下载操作后，会直接在使用的浏览器中开始下载。</p> <p> 注：支持通过查看镜像的MD5值，校验下载的镜像和导出的镜像是否相同。</p>
删除已导出镜像	<p>将已导出的镜像删除。</p> <p> 注：在ImageStore镜像服务器中，镜像文件以增量形式存储，只有在使用时（例如创建云主机或者导出镜像）才会产生一个完整的镜像文件。该删除操作只删除该完整镜像。镜像服务器中的原有镜像保持不变。</p>

注意事项

使用镜像需注意：

- 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。
- 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。
 - Legacy：支持所有操作系统。为了确保使用稳定，推荐使用Legacy模式引导。
 - UEFI：支持Windows操作系统和CentOS操作系统。其中，Windows 7和Windows Server 2008 R2版本必须使用兼容模块 (CSM)。
 - 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。

- 若创建的云主机希望使用UEFI引导，建议从以下操作系统版本列表中选择相应的云主机镜像：

操作系统	BIOS模式	支持版本
Windows平台	UEFI	<ul style="list-style-type: none"> Windows 8及以上版本
	UEFI（兼容模块）	<ul style="list-style-type: none"> Windows 7 Windows Server 2008 R2
Linux平台	UEFI	<ul style="list-style-type: none"> CentOS 7.2 CentOS 7.3 CentOS 7.4及以上版本

- 对于使用UEFI引导模式的CentOS 7.4及以上版本Linux类型镜像，创建的云主机重启可能进入UEFI Shell，请参考以下方法，成功启动并进入操作系统：

- 方法一：添加脚本自动跳过UEFI Shell，直接进入操作系统。

在安装好的操作系统中，执行`vim /boot/efi/startup.nsh`命令，创建脚本并保存以下内容，后续重启云主机将跳过UEFI Shell，直接进入操作系统：

```
FS0:
CD EFI
CD centos
shimx64-centos.efi
```

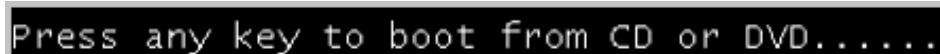
- 方法二：手动退出UEFI Shell。

若已经进入UEFI Shell，可手动执行以下命令，退出UEFI Shell：

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

- 对于使用UEFI引导模式的Windows云主机（例如：Windows Server 2012 R2、Windows Server 2016和Windows 10等版本），启动后会显示如下页面，需按任意键继续安装，否则将进入UEFI Shell，如图 40: 按下任意键继续所示：

图 40: 按下任意键继续



若进入UEFI Shell，需执行以下命令，才能成功启动进入操作系统：

```
Shell> fs0:
FS0:\> dir
FS0:\> cd EFI
FS0:\EFI> cd BOOT
FS0:\EFI\BOOT> BOOTX64.EFI
```

操作后请及时按任意键，否则会再次进入UEFI Shell。

12.1.4 计算规格

计算规格：云主机涉及的CPU数量、内存、网络设置等规格定义。

计算规格支持以下操作：

操作	描述
创建计算规格	创建计算规格。
编辑	修改计算规格的名称和简介。
启用计算规格	将处于停用状态的计算规格启用。
停用计算规格	将处于启用状态的计算规格停用。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> 全局共享：将资源共享给所有的项目和账户使用。 指定共享：将资源共享给指定的项目和账户使用。 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p>注：</p> <ul style="list-style-type: none"> 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除计算规格	删除计算规格时，会弹出确认删除窗口。

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

12.1.5 云盘规格

云盘规格：云盘涉及的容量大小的规格定义。

云盘规格可以用来创建根云盘和数据云盘。

云盘规格支持以下操作：



操作	描述
创建云盘规格	创建一个新的云盘规格。
编辑云盘规格	修改云盘规格的名称与简介。
启用云盘规格	将处于停用状态的云盘规格启用。
停用云盘规格	将处于启用状态的云盘规格停用。停用后不能再用其创建云盘，但不影响之前已创建的云盘。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> • 全局共享：将资源共享给所有的项目和账户使用。 • 指定共享：将资源共享给指定的项目和账户使用。 • 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p>注：</p> <ul style="list-style-type: none"> • 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 • 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除云盘规格	删除不需要的云盘规格。

12.1.6 GPU规格

GPU规格（GPU Specification）：物理GPU设备或vGPU设备涉及的GPU帧数、显存、分辨率等规格定义，包括两种类型：物理GPU规格、vGPU规格。


- 物理 GPU 规格：定义了物理 GPU 帧数、显存、分辨率等参数大小的规格。
- vGPU 规格：物理 GPU 被虚拟化切割成 vGPU 后，定义了 vGPU 帧数、显存、分辨率等参数大小的规格。

物理GPU规格支持以下操作：

操作	描述
启用物理GPU规格	启用处于停用状态的物理GPU规格。启用后，可用于为云主机分配物理GPU使用。
停用物理GPU规格	停用选中的物理GPU规格。停用后，不可以用于为云主机分配物理GPU使用。
设置ROM	<p>为物理GPU规格设置ROM，用于GPU透传功能。</p> <p> 注：</p> <ul style="list-style-type: none"> • 用户可自行在显卡供应商官网获取所需的ROM文件。 • 请务必上传与物理GPU匹配且版本信息正确的ROM文件，否则可能导致透传后的物理GPU不能正常工作。 • ROM文件上传成功后，将直接更新到已添加的规格对应的物理GPU设备中。 • 最新上传的ROM文件会覆盖之前上传的ROM文件。 • Cloud云平台已内置基础ROM文件，满足绝大部分物理GPU透传。若用户需要使用其他ROM文件，请自行在显卡供应商官网获取所需的ROM文件并上传。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> • 全局共享：将资源共享给所有的项目和账户使用。 • 指定共享：将资源共享给指定的项目和账户使用。 • 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p> 注：</p> <ul style="list-style-type: none"> • 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。

操作	描述
	<ul style="list-style-type: none"> 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。

vGPU规格支持以下操作：


操作	描述
启用vGPU规格	启用处于停用状态的vGPU规格。启用后，可用于为云主机分配vGPU使用。
停用vGPU规格	停用选中的vGPU规格。停用后，不可以用于为云主机分配vGPU使用。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> 全局共享：将资源共享给所有的项目和账户使用。 指定共享：将资源共享给指定的项目和账户使用。 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p> 注：</p> <ul style="list-style-type: none"> 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。

12.1.7 弹性伸缩组

弹性伸缩组：一组具有相同应用场景的云主机集合，可根据用户业务变化自动实现弹性伸缩或弹性自愈。

弹性伸缩组支持以下操作：

操作	描述
创建弹性伸缩组	创建一个新的弹性伸缩组。
编辑	修改弹性伸缩组的名称与简介。
启用弹性伸缩组	将处于停用状态的弹性伸缩组启用。
停用弹性伸缩组	将处于启用状态的弹性伸缩组停用。
修改镜像	修改用于创建弹性伸缩组的镜像。

操作	描述
	 注: 修改镜像仅对后续新生成的云主机生效，原有云主机镜像不变。
删除弹性伸缩组	删除弹性伸缩组。

功能特点

• 弹性伸缩

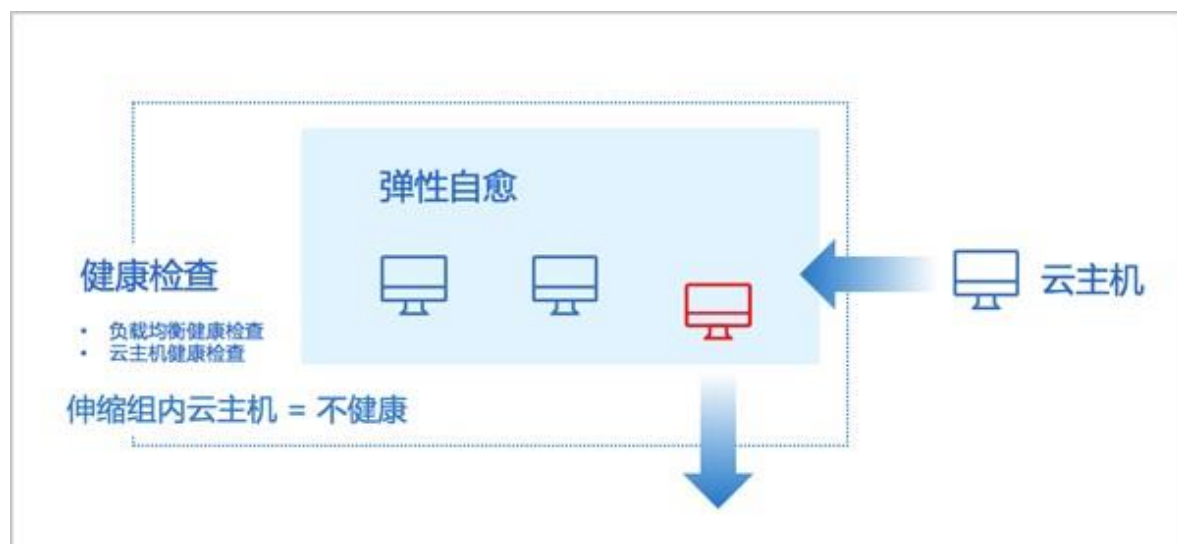
- 弹性伸缩包括弹性扩容和弹性缩容，前者在业务增长时自动增加云主机，后者在业务下降时自动减少云主机。
- 提供监控报警触发弹性伸缩，可自定义接收端类型，包括系统/邮箱/钉钉/HTTP应用/短信/Microsoft Teams。

• 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 41: 弹性自愈所示:

图 41: 弹性自愈



应用场景

以下介绍弹性伸缩组的三种典型应用场景:

- 弹性扩容:

某电商公司在双十一、春节等大型节日期间发起抢红包、秒杀等促销活动，负载激增，需及时、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。

- 弹性缩容:

当节假日过后，该电商公司的业务负载明显回落，需及时、自动减少云主机进行缩容，避免资源浪费。

- 弹性自愈:

为保障该电商公司核心业务的正常运作，要求处于健康运行的云主机数量不能低于某个阈值。

补充说明

弹性扩容触发条件:

- 伸缩组内云主机负载超过阈值时触发弹性扩容
 - 若伸缩组处于冷却时间内，则不执行弹性扩容。
 - 若伸缩组内云主机数量已达上限，则不再新增云主机。
 - 伸缩组内云主机的数量不会大于最大云主机数量。
- 伸缩组内云主机数量低于最小云主机数量时触发弹性扩容
 - 若伸缩组内云主机数量已达上限，则不再新增云主机。
 - 伸缩组内云主机的数量不会大于最大云主机数量。

弹性缩容触发条件:

- 伸缩组内云主机负载低于阈值时触发弹性缩容
 - 若伸缩组处于冷却时间内，则不执行弹性缩容。
 - 若伸缩组内云主机数量已达下限，则不再减少云主机。
 - 伸缩组内云主机的数量不会小于最小云主机数量。
- 伸缩组内云主机数量高于最大云主机数量时触发弹性缩容
 - 若伸缩组内云主机数量已达下限，则不再减少云主机。
 - 伸缩组内云主机的数量不会小于最小云主机数量。

弹性自愈触发条件: 云主机为不健康状态

- 云平台将删除不健康的云主机，若删除后伸缩组内云主机数量小于最小云主机数量，则执行弹性扩容策略，自动添加云主机。

关于弹性伸缩组，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 > 网络 > 负载均衡**，设置**负载均衡弹性伸缩组健康检查间隔**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 > 网络 > 负载均衡**，设置**负载均衡弹性伸缩组健康检查线程数**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 > 云资源池 > 弹性伸缩**，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 > 云资源池 > 弹性伸缩**，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 > 云资源池 > 弹性伸缩**，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。

注意事项

- 若弹性伸缩组重复执行伸缩策略，如不断创建和删除云主机，可能为以下原因：
 - 新创建的云主机无法在容忍时间内达到健康状态，云平台触发弹性自愈策略，删除不健康的云主机并重新创建，造成循环，需检查云主机健康检查策略或更改健康检查机制。
 - 缩容阈值或扩容阈值设置不合理。例如：设置触发条件为CPU低于40%缩容，CPU高于45%扩容，若伸缩组只有一台云主机，组内云主机平均CPU负载为60%，触发扩容后增加至两台云主机，组内云主机平均CPU负载降为30%，造成循环，需设置扩容缩容策略至合理的阈值范围。
- 若伸缩组未执行伸缩策略，但不断触发报警，可能为以下原因：
 - 最大云主机数量和扩容触发条件设置不合理，当伸缩组云主机数量已达上限，组内云主机平均负载仍然高于扩容阈值，则不断触发报警，需设置最大云主机数量和扩容触发条件至合理的阈值范围。
- 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。

- 弹性伸缩会自动释放云主机，建议不要对弹性伸缩组内云主机手动挂载云盘、网卡、安全组等。



注：若组内云主机保存有状态信息，相关数据将会丢失。

- 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。
- 若需要修改外部监控触发条目为内部监控使用条目，请删除弹性伸缩组并重新创建。
- 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。
- 目前支持扁平网络/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：系统/邮箱/钉钉/HTTP应用/短信/Microsoft Teams。
- 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。

12.1.8 快照

快照：某一时间点某一磁盘的数据状态文件。做重要操作前，对云主机根云盘或数据云盘做特定时间点的临时状态保留，方便出现故障后迅速回滚。如需长期备份，建议使用灾备服务。

快照类别

快照包括手动快照和自动快照两种类型：

- 手动快照：用户随时手动对云主机根云盘或数据云盘创建快照。
- 自动快照：通过定时任务创建快照，或系统在特定场景触发一次性自动快照。

- 通过定时任务创建快照，用户需提前创建定时快照策略，系统会在设置的时间点自动对相应资源创建快照。
- 系统在以下特定场景可能触发一次性自动快照：
 - 根云盘扩容
 - 数据云盘扩容
 - 重置云主机
 - 快照回滚



注:

- 系统默认快照回滚不会触发一次性自动快照。
- 用户可自行设置快照回滚是否触发一次性自动快照，设置方法：

进入**设置 > 平台设置 > 全局设置 > 高级设置 > 资源中心 > 云资源池 > 快照**，开启**自动创建云盘快照开关**即可。


- 在Ceph主存储上创建根云盘或数据云盘的镜像




快照视图

Cloud支持两种快照视图：列表视图和拓扑视图。

- 列表视图：以列表的方式展示快照信息，包括：快照名称、类型、容量、创建日期和支持的操作。
- 拓扑视图：以快照树的方式展示快照信息，包括：快照链和快照节点。支持定位到当前快照、还原画布、放大、缩写、全屏等操作。

快照支持以下操作：

操作	描述
创建云主机快照	<p>对运行中或已停止的云主机创建快照。</p> <p>云主机快照包括单盘快照和快照组两种类型：</p> <ul style="list-style-type: none"> • 单盘快照：对云主机根云盘创建快照。 • 快照组：对云主机根云盘及所加载的数据云盘创建快照。支持以快照组为单位统一恢复。 <p> 注：若云主机已加载共享云盘，不支持创建快照组。</p>
编辑云主机快照	修改云主机快照的名称与简介。

操作	描述
创建云主机	<p>基于快照创建云主机，点击后进入基于快照创建云主机界面，该界面除创建云主机常用配置外，还显示所选快照时间、云主机根盘所需空间以及是否同时创建数据云盘选项。</p> <p> 注:</p> <ul style="list-style-type: none"> 仅基于快照组创建云主机支持使用同时创建数据云盘功能。 创建时支持指定根云盘主存储，若未指定根云盘主存储，默认与原云主机根云盘所在主存储一致。 暂不支持指定数据云盘主存储，默认与原云主机的数据云盘所在主存储保持一致。
删除云主机快照	<p>删除不需要的快照。</p> <p>注:</p> <ul style="list-style-type: none"> 本地存储、NFS、SMP和Shared Block存储上创建的快照具有树状结构，删除根快照将同时删除其子分支上的快照，并解绑子分支上的快照组，请谨慎操作。 Ceph共享存储上创建的快照是独立的，不具有树状结构，删除某一快照不会影响其他快照。 批量删除树状结构的快照时，系统会根据所选快照，自动计算最终需要删除的快照并级联删除。 若待删除快照包含快照组类型的快照，需注意以下情况： <ul style="list-style-type: none"> 删除单个快照组类型的快照，将同时删除快照组内数据云盘对应的快照及子分支上的快照，请谨慎操作。 批量删除单盘快照及快照组类型快照，将同时删除其子分支上的单盘快照并解绑子分支上的快照组，请谨慎操作。 删除当前快照会消耗 I/O，请勿重启管理节点服务。 <p></p>
恢复云主机快照	<p>将数据恢复到所选快照节点。</p> <p>注:</p> <ul style="list-style-type: none"> 单盘快照仅支持将云主机根云盘恢复到快照节点。 快照组支持将组内的根云盘和数据云盘一起恢复到快照节点。 仅停止状态的云主机支持恢复快照操作。恢复快照前，请先停止云主机。 支持在快照恢复后选择是否自动启动云主机。 若云主机快照组显示不可恢复，可能存在以下原因： <ul style="list-style-type: none"> 快照组中的数据云盘快照被删除（至少一个数据云盘快照被删除），此时快照组不可恢复，仅支持单盘恢复。 <p></p>

操作	描述
	<ul style="list-style-type: none"> 云主机所加载的数据云盘被删除（至少一块数据云盘被删除），此时快照组不可恢复，仅支持单盘恢复。 云主机所加载的数据云盘被卸载（至少一块数据云盘被卸载），此时快照组不可恢复，仅支持单盘恢复。若将已卸载的数据云盘重新加载，则支持快照组恢复。 云主机新加载数据云盘，此时快照组不可恢复，仅支持单盘恢复。若将新加载的数据云盘卸载，则支持快照组恢复。
解绑快照组	将云主机快照恢复为单盘快照，并解除此云主机与相关云盘快照的组关系。解绑后不可批量恢复，请谨慎操作。

应用场景

快照功能适用于以下应用场景：

- 故障迅速还原：当生产环境出现异常故障，可使用快照回滚功能迅速还原至正常状态。该手段为临时方案，考虑到数据的长期完善保护，建议使用灾备服务。
- 数据开发：通过对生产数据创建快照，从而为数据挖掘、报表查询和开发测试等应用提供近实时的真实生产数据。
- 提高操作容错率：在系统升级或业务数据迁移等重大操作前，建议创建一份或多份快照。一旦升级或者迁移过程中出现任何问题，可以通过快照及时恢复到正常的系统数据状态。

注意事项

- 支持对运行中或已停止的云主机创建快照。
- 若云主机已加载共享云盘，不支持创建快照组。
- 在生产环境中，建议单块磁盘的快照数量尽量控制在5以内，快照过多会影响云主机/云盘的IO性能、数据安全以及主存储容量。如需长期备份，建议使用灾备服务。
- 在生产环境中，为确保数据完整性，不建议对高IO的云主机创建快照。当云主机内部进行高IO操作时，对云主机创建快照，内存中存在部分数据没有落入硬盘，这部分数据将无法保存到快照中。
- Ceph主存储上的云主机快照不占用容量，所显示的快照容量表示创建快照时刻云主机根云盘的真实容量。
- Ceph主存储场景下，关于云主机快照容量无法获取的说明：
 - Ceph开源版（H版）、Ceph企业版（3.2.0以下版本）均不支持获取云主机快照容量。

- Ceph企业版（3.2.0及以上版本）由于RBD format影响，可能出现无法获取云主机快照容量。
- 恢复云主机快照表示将数据恢复到所选快照节点，恢复快照前，需要停止云主机。
- 恢复云盘快照表示将云盘数据恢复到所选快照节点，恢复快照前，需要停止加载该云盘的云主机或将该云盘从云主机卸载。

12.1.9 亲和组

亲和组（Affinity Group）：一种针对IaaS资源的简单编排策略，可用于保障业务的高性能和高可用。

功能原理

目前，Cloud提供基于云主机的两种亲和组策略：

- 反亲和组（非强制）：

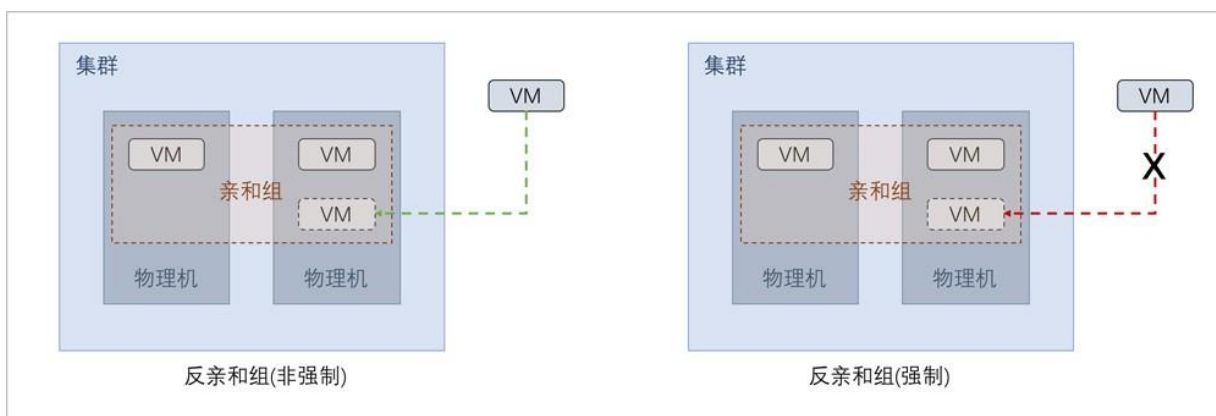
将亲和组内的云主机尽量分配到不同物理机上，当没有更多物理机可分配时，回归普通分配策略。

- 反亲和组（强制）：

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




如图 42: 反亲和组(非强制)与反亲和组(强制)所示：

图 42: 反亲和组(非强制)与反亲和组(强制)



亲和组支持的操作

亲和组支持以下操作：

操作	描述
创建亲和组	创建一个新的亲和组。
编辑亲和组	编辑亲和组的名称、简介信息。
启用亲和组	启用处于停用状态的亲和组。  注: 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。
停用亲和组	停用选中的亲和组。  注: 停用选中的亲和组，组内云主机将停止遵循所属亲和组策略，不影响正常业务。
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	将云主机从亲和组解绑，组策略即时生效。
删除亲和组	删除选中的亲和组。  注: 删除选中的亲和组，组内云主机下次启动时不再遵循亲和组策略。

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。

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VPC路由器默认都属于一个亲和组（可称之为系统组），采用反亲和组(非强制)策略，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。

12.2 硬件设施

12.2.1 区域

区域（Zone）：云平台内最大的一个资源定义，包括：集群、二层网络、主存储等资源。

功能原理

- 在数据中心的，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。

功能特点

- 区域隔离：

支持区域物理隔离，不同区域的主存储、物理机等物理子资源不互通，确保最大程度的稳定性和容错性。

可减少网络时延，提高访问速度。

- 资源管控：



每个区域可设置平台管理员。一个平台管理员可管理一个或多个区域。


每个项目的资源只能属于一个区域。

- 全局查看：

规划区域后，可在单独大屏查看某区域内所有的资源。支持按照KVM/vCenter分类进行查看资源使用情况。

区域支持以下操作：

操作	描述
创建区域	创建一个新的区域。
编辑区域	编辑区域的名称、简介信息。
启用区域	<p>启用处于停用状态的区域。</p> <p> 注：</p> <ul style="list-style-type: none"> 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。
停用区域	<p>停用选中的区域。</p> <p> 注：</p> <ul style="list-style-type: none"> 停用区域，将同时停用该区域内所有子资源。 停用区域会停用二层网络上加载的集群，导致二层网络和三层网络不可用，也不能用于创建云主机，但已有业务不受影响。

操作	描述
	<ul style="list-style-type: none"> 区域停用后，用户可手动重新启用区域内的某些集群，也可创建新的集群到当前的区域中，而无需重新启用整个区域。
删除区域	<p>删除选中的区域。</p> <p> 注：删除区域会删除集群、物理机、网络、主存储、已接管的vCenter等资源，同时还会删除各资源下的所有子级资源（如VPC路由器），请谨慎操作。</p>

注意事项

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. 一个区域可以加载一个或多个镜像服务器。
 - 一个区域中的资源，例如主存储，只能访问加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删除。删除后，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加载到一个区域不能再加载到其它区域。UI界面上，添加镜像服务器，默认会加载到当前区域。删除区域的同时会直接删除加载此区域的镜像服务器。

12.2.2 集群

集群：一组物理机（计算节点）的逻辑集合。在数据中心的，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. 集群需加载主存储、二层网络后，才可提供云主机服务。
5. 集群的规模，也就是每个集群中可以包含物理机的最大数量，没有限制。

集群和各个资源之间的关系定义如下。

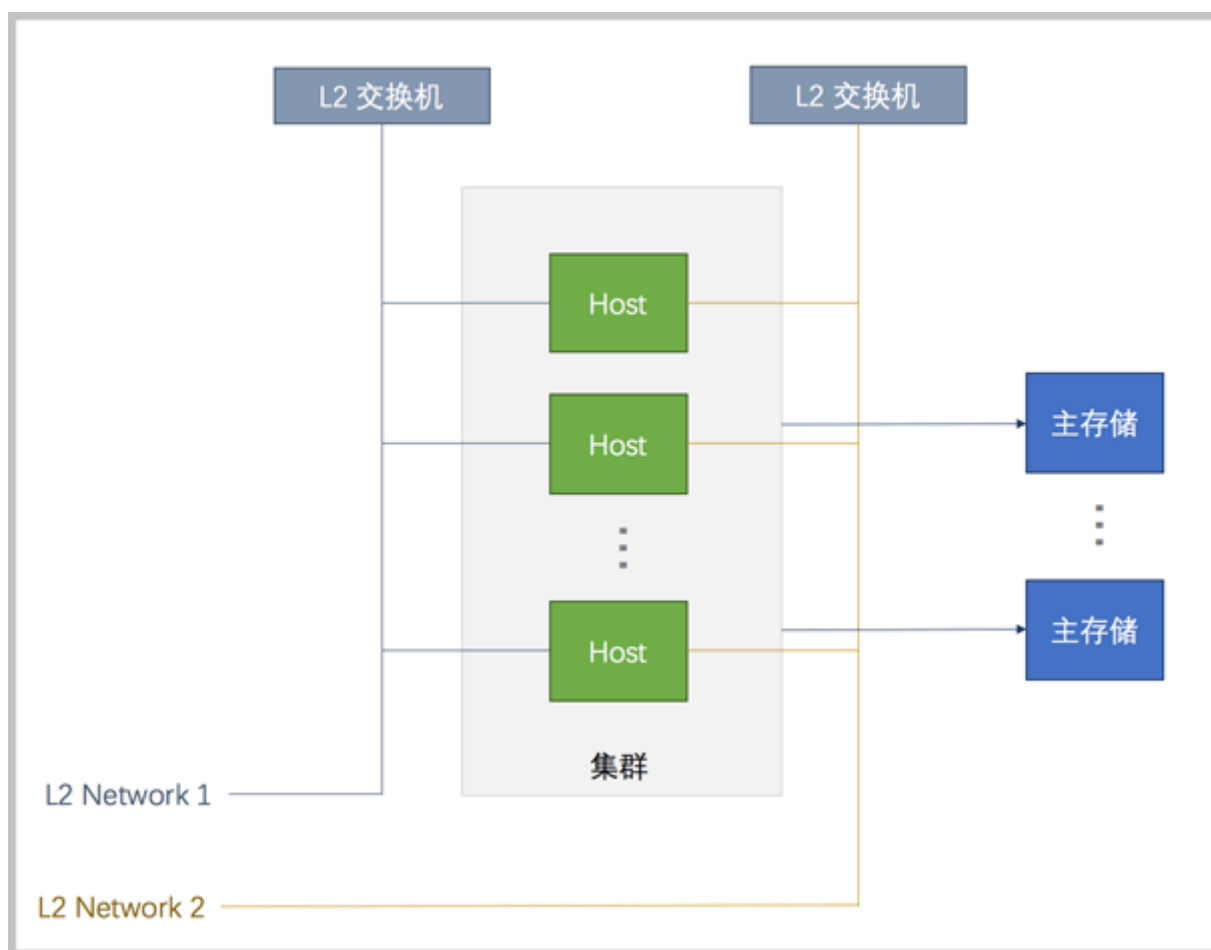
集群 | 区域

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

集群 | 主存储和二层网络

集群中可以加载或卸载主存储和二层网络。它们之间的结构关系如图 43: 集群、主存储、二层网络的关系所示：

图 43: 集群、主存储、二层网络的关系





注:

主存储和二层网络加载到集群时需注意:

1. 集群 | 主存储

- 一个主存储可以加载到多个集群。
- 一个集群可以加载多个主存储。

目前支持的同类型主存储场景如下:

- 一个集群可以加载一个或多个本地主存储。
- 一个集群可以加载一个或多个NFS主存储。
- 一个集群可以加载一个或多个Shared Block主存储。
- 一个集群可以加载一个Shared Mount Point主存储。
- 一个集群只能加载一个Ceph主存储。

目前支持的组合类型主存储场景如下:

- 一个集群可以加载一个本地主存储和一个NFS主存储。
- 一个集群可以加载一个本地主存储和一个Shared Mount Point主存储。
- 一个集群可以加载一个本地主存储和一个Shared Block主存储。
- 一个集群可以加载一个Ceph主存储和一个Shared Block主存储。
- 一个集群可以加载一个Ceph主存储和多个Shared Block主存储。

主存储与集群的依赖关系如表 4: 主存储与集群关系所示:

表 4: 主存储与集群关系

主存储	集群
Local Storage	支持加载一个或多个本地存储
NFS	支持加载一个或多个NFS
Shared Block	支持加载一个或多个Shared Block
Shared Mount Point	支持加载一个Shared Mount Point
Ceph	是加载到集群的Ceph, 有且仅有一个
Local Storage + NFS	支持加载1个Local Storage + 1个NFS
Local Storage + SMP	支持加载1个Local Storage + 1个Shared Mount Point

主存储	集群
Local Storage + Shared Block	支持加载1个Local Storage + 1个Shared Block
Ceph + Shared Block	<ul style="list-style-type: none"> 支持加载1个Ceph + 1个Shared Block 支持加载1个Ceph + 多个Shared Block

- 集群加载多个本地存储时，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，主存储可以从集群卸载。

2. 集群 | 二层网络

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

集群 | 镜像服务器

集群与镜像服务器没有直接依赖关系，一个镜像服务器可以为多个集群提供服务。



注：

- 集群中所加载的主存储和镜像服务器具有相关性。
- Ceph主存储支持与ImageStore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 5: 主存储与镜像服务器的关系所示：

表 5: 主存储与镜像服务器的关系

PS\BS	ImageStore	Ceph
Local Storage	○	×
NFS	○	×

Shared Mount Point	○	×
Ceph	○	○
Shared Block	○	×

集群 | 物理机

- 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。

集群 | 全局设置

- 集群详情页的高级设置项，可以在集群粒度设置内存超分率、CPU超分率、物理机保留内存等。此设置只对该集群内的资源生效，如不设置则默认使用全局设置的值。



注：高级设置的数值需要根据不同系统和应用的需求进行配置，数值过大可能会严重影响性能，请谨慎操作。

集群 | 动态资源调度

动态资源调度（Distributed Resource Scheduler，简称DRS）：该功能以集群为单位监控物理机CPU或内存负载情况，根据配置的调度策略给出调度建议，用户可按照调度建议手动迁移云主机，平衡集群负载的同时有效提高云平台稳定性。该功能为技术预览版。





请确保以下条件全部满足，动态资源调度功能才能正常工作：

- 确保集群内仅存在Ceph、Shared Block类型的主存储；
- 确保集群内所有物理机CPU型号一致；
- 确保集群内不存在已经绑定亲和组的云主机。

当以上条件全部满足，进入集群详情页的**高级设置**子页面，将**动态资源调度开关**开启，随后即可前往**动态资源调度**页面配置调度策略，配置策略完成后动态资源调度功能生效。

集群支持以下操作：

操作	描述
创建集群	在当前区域内创建一个新的集群。
编辑集群	修改集群的名称与简介。
启用集群	将处于停用状态的集群启用。
停用集群	将处于启用状态的集群停用。

操作	描述
	注:  <ul style="list-style-type: none"> 集群停用后，用户可手动重新启用集群内的某些物理机，也可添加新的物理机到当前的集群中，而无需重新启用整个集群。
加载二层网络	将二层网络加载到集群。
卸载二层网络	将二层网络从集群卸载。 注: 卸载二层网络后，相应的云主机网卡将被卸载，请谨慎操作。 
加载主存储	将主存储加载到集群。
卸载主存储	将主存储从集群卸载。 注: 将主存储从集群卸载，需要注意以下情况：  <ul style="list-style-type: none"> 此操作将导致该主存储上，与所选集群相关的云主机关机，影响业务运行，请谨慎操作。 此操作将导致该主存储上，与所选集群相关的VPC路由器被删除，相关云主机的网络服务异常，请谨慎操作。 此操作将导致该主存储上，与所选集群相关的云盘将不能正常使用，请谨慎操作。
删除集群	删除选中的集群。 注:  <ul style="list-style-type: none"> 删除集群，将同时删除该集群内所有物理机。 若主存储为本地存储（Local Storage），将同时删除物理机上的全部云主机、云盘和快照，请谨慎操作。

12.2.3 物理机

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。该硬件设施是云平台的核心资产，云主机运行在物理机之上。

如图 44: 物理机所示：

图 44: 物理机









添加物理机注意事项

添加物理机需注意：

- 管理节点的管理IP需正常访问物理机的SSH端口以部署代理程序。
- 物理机的用户名须拥有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。
- 添加或更改物理机的信息，需与实际环境相匹配。
- 物理机有一个字段managementIp，用于表示如果此物理机有多个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机发送ping命令以检查通道的健康状态；一旦某个物理机响应失败，或者ping命令超时，此物理机就会变为失联状态，失联后物理机上运行的云主机会变成unknown状态，待物理机恢复连接后，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机进行时间同步。

物理机支持以下操作：

操作	描述	物理机状态
添加物理机	添加一个或多个物理机。	/
编辑物理机	编辑物理机名称、简介信息。	/
启用物理机	将处于停用状态的物理机启用。	停用
停用物理机	<p>将处于启用状态的物理机停用。</p> <p> 注：物理机停用后，该物理机上原有资源不受影响，但申请新资源时不可作为候选物理机。</p>	启用
重连物理机	<p>重新连接物理机。</p> <p> 注：重连物理机操作一般用于物理机配置更新后。例如：物理机内存或者硬盘更新后，可通过重连物理机来更新数据库。</p>	ALL
进入维护模式	<p>物理机进入系统维护状态，可对此状态下的物理机进行物理停机、故障修复等操作。</p> <ul style="list-style-type: none"> 若主存储为本地存储：物理机进入维护模式后，其上云主机将停止。 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。 <p>注：共享存储场景下，物理机进入维护模式，用户可自行设置迁移云主机失败策略。设置方法： 进入设置 > 平台设置 > 全局设置 > 高级设置 > 物理机，设置维护模式下迁移云主机失败策略：</p> <p> </p> <ul style="list-style-type: none"> 若选择强制停止云主机：物理机进入维护模式，共享存储上的云主机会自动迁移到其它物理机上。未迁移的云主机将会被强制关闭。 若选择非强制停止云主机：物理机进入维护模式，共享存储上的云主机会自动迁移到其它物理机上。如果物理机上还运行中的云主机，则进入维护模式失败。 	已连接
绑定标签	<p>为物理机绑定标签，选中一个或多个物理机。</p> <p>注：</p> <p> </p> <ul style="list-style-type: none"> 单个资源最多支持绑定50个标签，反之，单个标签支持绑定的资源数量无限制。 标签-资源支持多对多绑定关系。 	ALL

操作	描述	物理机状态
	<ul style="list-style-type: none"> 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。 管理员支持解绑/删除租户标签。 资源标签按照绑定时间或标签名称（符号>数字>中文>英文）进行排序，可在设置 > 全局设置 > 基本设置中修改标签排序方式，默认按标签名称排序。 	
解绑标签	<p>解除绑定物理机上的标签。</p> <p>注:</p> <ul style="list-style-type: none"> 管理员标签由管理员创建，归管理员所有，租户标签由租户创建，归租户所有。 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。 管理员支持解绑/删除租户标签。 项目内的标签归属于项目所有，项目内所有人（项目负责人/项目管理员/项目成员）均可操作。  <ul style="list-style-type: none"> 标签暂不支持更改所有者操作。 资源更改所有者，其上所有租户标签将会解绑，管理员标签不受影响。 云平台无缝升级后，已有旧标签将自动更新，以最新方式展示标签。若有异常，请刷新浏览器或重新创建标签。 支持将单个资源上的批量标签解绑，也支持将单个标签上的批量资源解绑。 租户只能解绑所属租户资源上的标签，管理员可解绑所有资源上的标签。 	ALL
更新密码	更新物理机的密码，密码更新后将自动重连物理机。	/
删除物理机	<p>删除物理机。</p> <p>注: 删除物理机需要注意以下情况:</p>  <ul style="list-style-type: none"> 删除物理机，将会停止该物理机上所有云主机。 若主存储为本地存储: 	/

操作	描述	物理机状态
	<ul style="list-style-type: none"> 若物理机所属集群挂载了本地存储（Local Storage），将同时删除物理机上的全部云主机和云盘。 即使将已删除的物理机重新添加至云平台，系统也将重新部署该物理机，若之前数据库未备份，相关业务数据将无法恢复。 若主存储为共享存储： <ul style="list-style-type: none"> 若已关闭云主机高可用模式： 删除云主机所在的物理机后，相应的云主机会停止。 若已开启云主机高可用模式： 删除云主机所在的物理机后，如其它物理机资源允许，该物理机上设置高可用的云主机会先停止，然后迁移到其它物理机上自动启动，且不会影响数据安全性；若物理机资源不足，相应的云主机会停止。 删除物理机对共享存储上的数据云盘无影响。 若物理机已被征用为迁移服务器，删除物理机将同时删除相应的迁移服务器，且该迁移服务器上正在执行的迁移任务将自动取消。 	

物理机使用注意事项

使用物理机需注意：

- 物理机维护模式，主要用于管理员对物理机进行计划关机实施维护操作，例如：添加内存/添加硬盘/更换网卡等。
- 物理机维护模式，若主存储为本地存储，则会停止此物理机上所有云主机，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机上，如果其他物理机资源不足，则会停止这些云主机。
- 物理机添加内存规范操作流程为：
 - 将物理机进入维护模式。
 - 等待物理机上所有云主机自动迁移完成或者停机，对物理机进行 shutdown 关机操作。
 - 物理机下电，添加内存。

4. 物理机通电后，通过手动或IPMI启动，成功引导操作系统。
 5. 将物理机设置为启用状态。
- 物理机停用后，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机启动。
 - 物理机停用或维护后，此物理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。
 - 物理机失联或者进入维护模式后，才可删除物理机。
 - 删除本地存储上的物理机会直接彻底删除此物理机上所有的云主机或云盘。这里的删除，只是移除物理机、云主机、云盘等信息在Cloud中的记录，并不删除真实的数据。
 - 删除共享存储上的物理机，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机上重新启用或使用。
 - 删除物理机后，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，物理机的BIOS需开启VT-d功能，添加物理机时，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。

物理机运维异常检查事项

物理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。

- **物理机agent进程：**

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

- **物理机日志：**

在物理机检查`/var/log/zstack/zstack-kvmagent.log`是否存在异常。

- **物理机libvirt状态：**

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

- **物理机系统日志：**

在物理机检查`/var/log/messages`是否存在异常。

- **物理机与主存储连接：**

检查物理机是否与主存储连接是否出现异常。

12.2.3.1 物理机运维(扩展)

12.2.3.1.1 物理机计划性关机

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. 在管理节点上执行 `zstack-ctl stop` 命令，关闭管理节点服务。
4. 将所有服务器正常下电。

- 管理节点物理机高可用场景

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. 将所有物理主机进入维护模式。
3. 依次在两个管理节点上执行 `zsha2 stop-node` 命令，关闭管理节点服务。
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Cloud服务启动成功。
3. 登录Cloud云平台，启用所有主存储和所有物理机，确保物理机和主存储是已连接状态。

- 管理节点高可用场景

1. 将所有服务器上电。
2. 针对管理节点云主机高可用场景，在任一物理机上执行 `zsha status` 命令查看管理节点高可用服务状态，等待服务正常启动成功。
3. 针对管理节点物理机高可用场景，在两个管理节点执行 `zsha2 status` 命令查看管理节点高可用服务状态，等待服务正常启动成功。
4. 登录Cloud云平台，启用所有主存储和所有物理机，确保物理机和主存储是已连接状态。

12.2.3.1.2 物理机扩容

新增物理设备扩容计算资源

新增物理设备扩容计算资源步骤如下：

1. 新增物理设备扩容计算资源。
2. 按照用户手册进行安装部署服务器并配置网络。
3. 登录UI，在**添加物理机**界面，添加物理机，完成计算服务器扩容。详情请参考《用户手册》中**添加物理机**章节。



注：

- 企业版ceph分离/融合部署场景需要将此计算节点添加到存储作为网关角色使用（注意：需要提前配置好主机名、hosts文件、免密、防火墙、selinux、时间同步等）。
- 对接san存储场景需要提前配置好san设备lun映射到此物理机。

新增物理设备扩容存储资源

- **企业版ceph扩容存储：**
 1. 分离/融合部署场景。
 2. 准备官网发布ISO进行安装服务器，硬盘设置为直通模式。
 3. 按照用户手册进行安装部署服务器并配置网络；做好免密、时间同步、hostname等配置。
 4. 在企业版ceph**存储管理**界面依次执行以下操作：**添加此存储服务器为存储服务器** > **添加缓存盘** > **添加硬盘** > **添加拓扑** > **将硬盘添加到存储池内**，然后等待服务器自动平衡数据、重连Cloud主存储，完成存储扩容。
- **SAN设备扩容：**
 1. 联系SAN厂商进行扩容lun；
 2. 在Cloud云平台重连Shared Block类型对接的SAN做主存储，完成存储扩容。

12.2.3.1.3 物理机更换

更换物理机步骤如下：

1. 登录UI界面，将需要更换的物理机设置进入维护模式。



注：进入维护模式前，请迁移业务云主机。

2. 待物理机上无业务云主机后，删除该物理机。

3. 将新的物理机安装Cloud定制版操作系统（安装为计算节点）并配置基础网络。
4. 在**添加物理机**界面，添加这些新的物理机，详情请参考《用户手册》中**添加物理机**章节。

12.2.3.1.4 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Cloud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Cloud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。

12.2.3.1.5 单个物理机运维

修改物理机密码

- UI方式：

1. 登录云平台，物理机详情页，点击**密码**后面的修改按钮，重新设置物理机密码。
 2. 手动重连物理机，应用修改后的密码。
- 命令行方式：
 1. 执行如下命令以admin方式登录云平台：

```
[root@localhost ~]# zstack-cli
admin>> LoginByAccount accountName=admin password=PASSWORD #
PASSWORD为登录密码
```

2. 执行如下命令修改物理机密码：

```
admin>> UpdateKVMHost uuid=HOST_UUID password=NEW_PASSWORD #
HOST_UUID为物理机UUID；NEW_PASSWORD为新密码
```

物理机开启IOMMU功能

确保物理机BIOS已开启Intel VT-d / AMD IOMMU选项时，开启IOMMU功能才能生效，开启方法如下：

- 通过UI方式登录云平台，在物理机详情页的**基本属性**页面，将**IOMMU启动状态**调至**启动**，然后重启系统，指定物理机开启IOMMU功能。

12.2.3.1.6 批量物理机运维

批量添加物理机

Cloud支持UI和cli命令行两种方式批量添加物理机，具体方法如下：

- UI方式：
 1. 通过UI方式登录Cloud，在**添加物理机**界面，选择**模板导入**方式添加物理机。
 2. 点击**下载配置模板**按钮下载模板，并按照规定填写模板。
 3. 将填写好的模板添加到Cloud，点击**确定**按钮开始批量添加物理机。

详情请参考《用户手册》中**添加物理机**章节。

批量物理机执行免密等操作

批量物理机相互免密、时间同步、hostname配置流程如下：

1. 准备免密工具包，步骤如下：

```
#下载工具包
[root@localhost ~]# wget http://cdn.zstack.io/tools/zstack_tools.tar.gz
#解压工具包
[root@localhost ~]# tar zxvf zstack_tools.tar.gz
```

```
#进入工具包路径
[root@localhost ~]# cd zstack_tools/
```

2. 修改ansible/hosts.example下面的配置:



注:

- 在nodes下列出所有节点的管理网络IP地址。
- **ansible_user**代表ssh 用户名。
- **ansible_pass**代表ssh密码。
- 各物理机密码初始应配置相同密码，在chrony下面列出待配置的时间同步服务器，脚本会自动配置此节点作为时间同步服务器。

```
[root@localhost zstack_tools]# vim ansible/hosts.example
#修改成如下内容
#节点IP
[nodes]
10.10.0.11
10.10.0.12
10.10.0.13
#节点用户/密码
[nodes:vars]
ansible_user=root
ansible_ssh_pass=password
#时间同步服务器
[chrony]
10.10.0.13
#保存退出
编辑hostname前缀
修改ansible/group_vars/nodes下hostname前缀
vim ansible/group_vars/nodes
#修改如下内容
hostname_prefix: ceph-
#保存退出，各个hostname前缀会被配置为ceph-1，ceph-2类似格式
```

3. 执行以下命令，一键准备环境，此脚本会部署各节点之间SSH免密，时间同步，/etc/hosts，关闭防火墙等操作:

```
[root@localhost ~]# ./prepare.sh -i ./ansible/hosts.example
```

批量修改物理机密码和平台上物理机密码

批量修改云平台物理机系统密码和云平台上物理机密码（仅限KVM物理机，前提：加入云平台的物理机都采用root用户）流程如下:

• 方法一:

1. 执行如下命令以admin方式登录云平台:

```
[root@localhost ~]# zstack-cli
```

```
admin>> LoginByAccount accountName=admin password=PASSWORD #
PASSWORD为登录密码
```

2. 在管理节点依次执行如下命令，批量修改物理机root密码：

```
admin>> QueryHost fields=managementIp, "hypervisorType"=KVM
admin>> for i in $(zstack-cli QueryHost fields=managementIp, hypervisorType=KVM|awk
-F "\"" '/managementIp/ {print $4}');
do \
ssh $i -i \
/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/ansible/rsaKeys/
id_rsa 'echo "NEW_PSAAWORD" | passwd --stdin root';
done #NEW_PSAAWORD为新的密码
```

• 方法二：

1. 在管理节点执行以下zstack-cli命令批量修改云平台上的物理机密码：

```
[root@localhost ~]# for i in $(zstack-cli QueryHost fields=uuid, hypervisorType=KVM|awk
-F "\"" '/uuid/ {print $4}')
[root@localhost ~]# do zstack-cli UpdateKVMHost uuid=$i password=NEW_PSAAWORD
#NEW_PSAAWORD为新的密码
[root@localhost ~]# done
```

批量物理机创建sudo用户及云平台修改用户名密码

批量物理机创建sudo用户及修改云平台物理机用户名密码（仅限KVM物理机，前提：加入云平台的物理机都采用root用户）步骤如下：

- **方法一：**在管理节点执行以下命令批量创建test用户，将加入云平台的所有KVM物理机创建拥有sudo权限的test用户修改密码为NEW_PSAAWORD：

```
[root@localhost ~]# zstack-cli LoginByAccount accountName=admin password=password
admin>> for i in $(zstack-cli QueryHost fields=managementIp, hypervisorType=KVM|awk -F
"\"" '/managementIp/ {print $4}');
do \
ssh $i -i \
/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/ansible/rsaKeys/id_rsa \
'adduser test;echo "NEW_PSAAWORD" | passwd --stdin test;echo "test ALL=(ALL)
NOPASSWD: ALL" >>/etc/sudoers;' #NEW_PSAAWORD为新的密码
admin>> done
```

- **方法二：**在管理节点执行以下zstack-cli命令批量修改云平台上的物理机用户名
为NEW_NAME，密码为NEW_PSAAWORD：

```
[root@localhost ~]# for i in $(zstack-cli QueryHost fields=uuid, hypervisorType=KVM|awk -F
"\"" '/uuid/ {print $4}')
[root@localhost ~]# do
[root@localhost ~]# zstack-cli UpdateKVMHost uuid=$i password=password123
username=test
```



```
[root@localhost ~]# done
```

12.2.3.2 外接设备运维

12.2.3.2.1 GPU设备

GPU设备包括物理GPU和vGPU，作用于不同的场景：

- 物理GPU：直接透传到云主机，让云主机享有物理机强劲的GPU并行计算能力，不仅适用于3D渲染、高清转解码场景，还适用于诸多高性能计算（HPC）场景，如：机器学习、医疗成像、石油勘探数据分析、比特币挖掘等具有大量密集运算特点的场景。
- vGPU：物理GPU虚拟化切割后的产物，可加载到云主机使用，分别加载到不同云主机使用，在满足GPU使用场景的情况下，扩展GPU数量，避免GPU资源浪费。

注意事项

使用物理GPU透传功能需注意以下情况：

- Cloud支持以下型号的物理GPU透传：

NVIDIA	AMD
<ul style="list-style-type: none"> • Tesla T4 • Tesla M10/M60 • Tesla P100/P40/P6/P4 • Tesla V100 • RTX 6000/8000 • 等等... 	<ul style="list-style-type: none"> • FirePro S7150 • FirePro S7150X2



注：NVIDIA显卡支持透传的型号较多，仅列举常用显卡，更多详情请参考[NVIDIA官方文档](#)。

- 使用物理GPU需要提前完成以下准备工作：
 - 确保物理机BIOS中开启Intel VT-d / AMD IOMMU功能，且物理机内核已开启IOMMU支持。
 - 按需设置全局设置：进入**设置 > 平台设置 > 全局设置**界面，按需调整全局设置，以下几个全局设置与物理GPU透传相关：
 - PCI设备热插拔开关：用于设置是否允许云主机热插拔GPU设备，默认为true。若热插拔时出现硬件兼容性错误，或不支持该硬件设备时，建议关闭此功能（设置为false）。
 - GPU设备配额：用于设置账户/项目使用GPU设备（包括：物理GPU和vGPU）数量配额，默认为20。

- 已安装最新版本Cloud，并部署完成创建云主机必要的资源。
- Cloud云平台已内置基础ROM文件，满足绝大部分物理GPU透传。若用户需要使用其他ROM文件，请自行在显卡供应商官网获取所需的ROM文件并上传。
- 请务必上传与物理GPU匹配且版本信息正确的ROM文件，否则可能导致透传后的物理GPU不能正常工作。
- 最新上传的ROM文件会覆盖之前上传的ROM文件。
- 添加物理主机时，请勾选扫描物理主机的IOMMU设备，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。

使用vGPU需要注意以下情况：

- Cloud支持对以下型号显卡进行虚拟化切割：

NVIDIA	AMD
<ul style="list-style-type: none"> • Tesla T4 • Tesla M10/M60 • Tesla P100/P40/P6/P4 • Tesla V100 • RTX 6000/8000 • 更多请参考NVIDIA官方文档 	<ul style="list-style-type: none"> • FirePro S7150 • FirePro S7150X2



注: NVIDIA显卡支持虚拟化切割的型号较多, 仅列举常用显卡, 更多详情请参考 [NVIDIA 官方文档](#)。

- 使用vGPU功能需要提前准备以下工作:
 - 确保物理机BIOS中开启Intel VT-d / AMD IOMMU功能, 且物理机内核已开启IOMMU支持。
 - 按需设置全局设置: 进入**设置 > 平台设置 > 全局设置**界面, 按需调整全局设置, 以下几个全局设置与物理GPU透传相关:
 - PCI设备热插拔开关: 用于设置是否允许云主机热插拔GPU设备, 默认为true。若热插拔时出现硬件兼容性错误, 或不支持该硬件设备时, 建议关闭此功能(设置为false)。
 - GPU设备配额: 用于设置账户/项目使用GPU设备(包括: 物理GPU和vGPU)数量配额, 默认为20。
 - 已安装最新版本Cloud, 并部署完成创建云主机必要的资源。

Cloud云平台已内置基础ROM文件, 满足绝大部分物理GPU透传。若用户需要使用其他ROM文件, 请自行在显卡供应商官网获取所需的ROM文件并上传。

- 请务必上传与物理GPU匹配且版本信息正确的ROM文件, 否则可能导致透传后的物理GPU不能正常工作。
- 最新上传的ROM文件会覆盖之前上传的ROM文件。
- 添加物理主机时, 请勾选扫描物理主机的IOMMU设备, 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。

使用vGPU需要注意以下情况：

- Cloud支持对以下型号显卡进行虚拟化切割：

NVIDIA	AMD
<ul style="list-style-type: none"> Tesla T4 Tesla M10/M60 Tesla P100/P40/P6/P4 Tesla V100 RTX 6000/8000 更多请参考NVIDIA官方文档 	<ul style="list-style-type: none"> FirePro S7150 FirePro S7150X2



注：NVIDIA显卡支持虚拟化切割的型号较多，仅列举常用显卡，更多详情请参考[NVIDIA官方文档](#)。

- 使用vGPU功能需要提前准备以下工作：

1. 使用vGPU功能需要做以下基础准备工作：

- 确保物理机BIOS中开启Intel VT-d / AMD IOMMU功能，且物理机内核已开启IOMMU支持。
- 确保物理机BIOS中开启SR-IOV和Memory Mapped I/O above 4GB功能。
- 按需设置全局设置：进入**设置 > 全局设置 > 高级设置**界面，按需调整全局设置，以下几个全局设置与物理GPU透传相关：
 - PCI设备热插拔开关：用于设置是否允许云主机热插拔GPU设备，默认为true。若热插拔时出现硬件兼容性错误，或不支持该硬件设备时，建议关闭此功能（设置为false）。
 - GPU设备配额：用于设置账户/项目使用GPU设备（包括：物理GPU和vGPU）数量配额，默认为20。
- 已安装最新版本Cloud，并部署完成创建云主机必要的资源。

2. NVIDIA vGPU需要额外做以下准备工作：

- NVIDIA vGPU功能依赖CentOS 7.6版本内核，请使用c76版本ISO。

- 若使用NVIDIA vGPU，请参考[NVIDIA官方文档](#)提前购买License，搭建License Server并导入License。

3. AMD vGPU需要额外做以下准备工作：

确保高级设置**云主机Hyper-V开关**状态为false，否则云主机无法正常加载AMD vGPU驱动。可通过以下几种方式按需关闭该高级设置：

- 进入云主机详情页的**高级设置**页面，针对单个云主机关闭**云主机Hyper-V开关**。
- 进入集群详情页的**高级设置**页面，针对集群关闭**云主机Hyper-V开关**。
- 进入**设置 > 全局设置 > 基本设置 > 资源中心 > 云主机**页面，针对整个云平台关闭**云主机Hyper-V开关**。
- 添加物理主机时，请勾选扫描物理主机的IOMMU设备，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。
- 物理GPU执行虚拟化切割前请确保满足以下条件：
 - 确保此物理GPU型号支持虚拟化切割。
 - 物理GPU未透传给云主机使用。
 - 确保物理机BIOS中开启Intel VT-d / AMD IOMMU功能，且物理机内核已开启IOMMU支持。
 - 确保云平台中添加的物理机IOMMU就绪状态为“可用”。
- NVIDIA 物理GPU和AMD 物理GPU切割方式不同：NVIDIA 物理支持每个核心独立切割；AMD 物理GPU仅支持同时切割物理机上所有AMD 物理GPU。
 - 切割规格显示此物理GPU可被切割的所有规格列表。例如：GRID M60-2A(4ins-2048 MiB -1280*1024)表示将一个核心的物理GPU虚拟化切割成4个帧数为60FPS、显存为2048MB、分辨率为1280*1024的vGPU。
 - 若需要将vGPU还原成物理GPU，请点击**操作 > 虚拟化还原**按钮执行操作。虚拟化还原NVIDIA vGPU需确保此物理GPU相关的vGPU已经全部从云主机卸载。
 - 若需要将vGPU还原成物理GPU，请点击**操作 > 虚拟化还原**按钮执行操作。虚拟化还原AMD vGPU需确保当前物理机上所有AMD vGPU全部已经从云主机卸载。

- 一台云主机支持同时加载一个vGPU，暂不支持将物理GPU和vGPU同时加载到同一台云主机使用。
- 若需要释放GPU设备，选中GPU设备，点击**操作 > 卸载**按钮，释放GPU设备。
- 执行加载、卸载vGPU操作前，请确保云主机状态为**已停止**。

12.2.3.2.2 vGPU设备

Cloud支持vGPU功能，通过GPU虚拟化技术，将物理GPU切割成更细粒度的 vGPU，形成vGPU资源池。用户可使用vGPU规格快速创建轻量的vGPU云主机，实现更灵活弹性的资源部署、提高资源利用率、以及节约成本。该功能适用于云游戏、VDI、VR/AR、AI推理以及机器学习教学等轻量级GPU计算场景。

Cloud支持对以下型号显卡进行虚拟化切割：

NVIDIA	AMD
<ul style="list-style-type: none"> • Tesla T4 • Tesla M10/M60 • Tesla P100/P40/P6/P4 • Tesla V100 • RTX 6000/8000 • 更多请参考NVIDIA官方文档 	<ul style="list-style-type: none"> • FirePro S7150 • FirePro S7150X2



注：NVIDIA显卡支持虚拟化切割的型号较多，仅列举常用显卡，更多详情请参考[NVIDIA官方文档](#)。

12.2.3.2.3 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。USB设备透传包括以下几种模式：

- 直连：将USB设备加载到此物理机上的云主机，迁移云主机时需要卸载此USB设备；
- 转发：将USB设备加载到此物理机所在区域内的云主机，迁移云主机时不需要卸载此USB设备。

注意事项

使用USB设备透传需要注意以下情况：

- USB默认设备名采用厂商名+编号的形式，支持修改设备名（点击**操作 > 修改设备名**），建议用户自行修改设备名，提高USB设备辨识度。

- USB版本根据USB插入的接口决定。例如：USB3.0设备插入USB2.0接口时，USB版本显示2.00。
- 同一个USB设备只能透传给一台云主机使用。
- 同一台云主机最多支持加载1个USB1.0设备、最多支持加载6个USB2.0设备、最多支持加载4个USB3.0设备。
- 运行中状态或本地存储已停止状态的云主机只支持加载云主机所在物理机上的可用USB设备，不支持跨物理机加载USB设备。
- 共享存储上已停止状态的云主机支持加载云主机所在集群内某台物理机上的多个USB设备。
- 若需要卸载USB设备，点击**操作** > **卸载**按钮执行卸载操作。
- Windows XP、Windows Server 2003 R2、Windows Server 2008 R2和Windows 7系统，不支持USB 3.0设备的直接加载，需要手动安装驱动。请从以下路径获取驱动文件并双击安装：http://cdn.zstack.io/tools/renesas_usb30_21390.exe
- 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 Server 2003 R2、Windows Server 2008 R2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。

12.2.3.2.4 SR-IOV网卡虚拟化

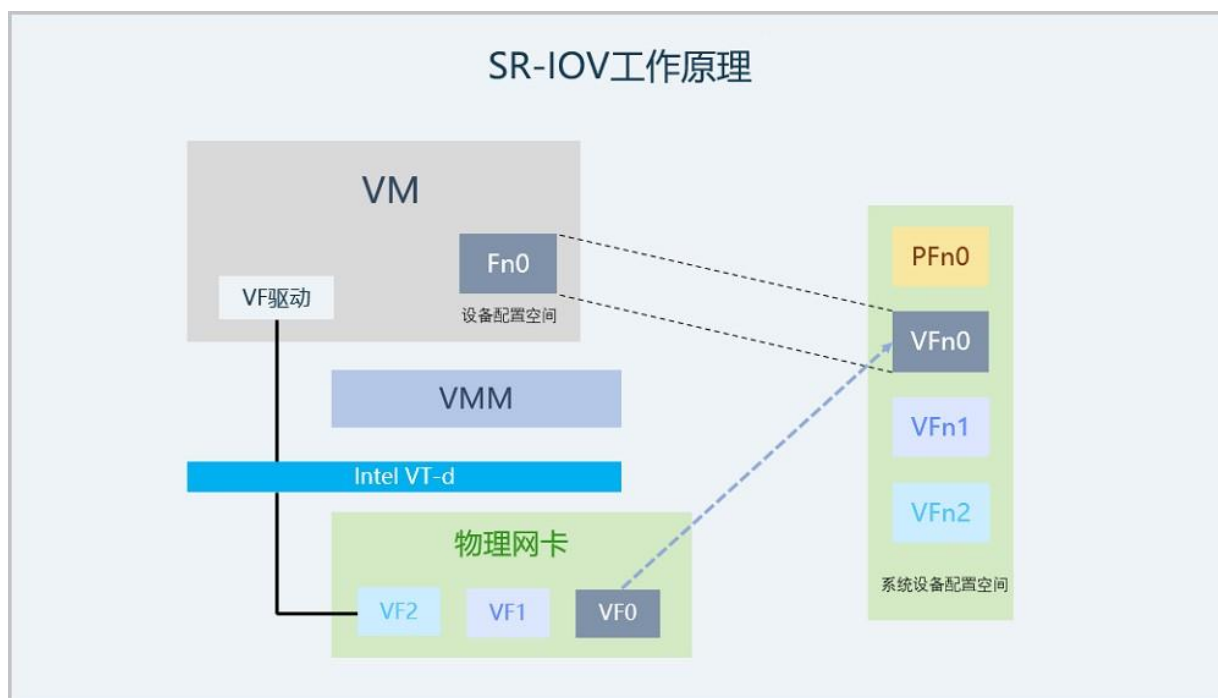
SR-IOV（Single Root I/O Virtualization）是一种基于硬件的虚拟化解决方案，它允许多个云主机高效共享PCIe设备，且同时获得与物理设备性能媲美的I/O性能，能有效提高性能和可伸缩性。

Cloud支持基于SR-IOV规范，将一张物理网卡虚拟化切割成多张VF类型网卡，直接分配给云主机使用。实现弹性灵活使用资源的同时，提高资源利用率、节约成本。相比传统的vNIC虚拟化网卡，VF网卡具有以下功能优势：

- VF网卡可直接分配给云主机，越过虚拟化层，缩短数据传输路径，使云主机获得接近物理设备的I/O性能。
- 明显减少对物理机CPU资源的消耗，即使物理机CPU压力较大，也能有效减少网络丢包，提高传输效率。
- VF网卡可直接分配给云主机，越过虚拟化层，缩短数据传输路径，使云主机获得接近物理设备的I/O性能。
- 明显减少对物理机CPU资源的消耗，即使物理机CPU压力较大，也能有效减少网络丢包，提高传输效率。

如图 45: SR-IOV工作原理所示:

图 45: SR-IOV工作原理



注意事项

- 使用SR-IOV功能前须严格确保准备工作全部完成，否则此功能无法正常使用。
- 若VF网卡已分配给云主机使用，请勿卸载物理网卡驱动，否则可能导致VF网卡强行回收。
- 若物理网卡已配置bond，继续使用SR-IOV功能可能导致VF与vNIC网卡相互通信受影响，推荐使用方式如下：
 - 推荐针对单个物理网卡配置bond，并继续使用SR-IOV功能。
 - 多个物理网卡配置bond时，推荐仅对其中一个物理网卡进行SR-IOV切割。
- VF网卡不支持QoS功能。
- 使用启用SR-IOV功能的三层网络创建的云主机，暂时不支持使用以下网络服务：
 - 使用公有网络/扁平网络创建的云主机，其VF网卡不支持使用安全组和弹性IP网络服务。
 - 使用路由器网络/VPC网络创建的云主机，其VF网卡不支持使用安全组网络服务。
- 运行状态且加载VF网卡的云主机不支持迁移、存储迁移操作。须停用云主机或卸载VF网卡才能执行这些操作。
- 停用云主机将自动释放VF网卡；启用云主机时重新获取，若无可用VF网卡，将导致启用云主机失败。

12.2.4 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。

主存储支持的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。



主存储与集群的依赖关系：

表 6: 主存储与集群关系

主存储	集群
Local Storage	支持加载一个或多个本地存储
NFS	支持加载一个或多个NFS
Shared Block	支持加载一个或多个Shared Block
Shared Mount Point	支持加载一个Shared Mount Point
Ceph	是加载到集群的Ceph，有且仅有一个
Local Storage + NFS	支持加载1个Local Storage + 1个NFS
Local Storage + SMP	支持加载1个Local Storage + 1个Shared Mount Point
Local Storage + Shared Block	支持加载1个Local Storage + 1个Shared Block
Ceph + Shared Block	<ul style="list-style-type: none"> • 支持加载1个Ceph + 1个Shared Block • 支持加载1个Ceph + 多个Shared Block

主存储支持以下操作：

操作	描述
添加主存储	添加一个主存储到系统中。
编辑主存储	修改主存储的名称与简介。
启用主存储	将处于停用状态的主存储启用。
停用主存储	将处于启用状态的主存储停用。停用主存储后，将无法基于该主存储创建新的云主机、云盘、快照，原有资源不受影响。
重连主存储	<p>重新连接主存储。重连主存储会更新主存储相关的存储信息。</p> <p> 注： 如果有任意一台物理机正常连接到主存储，该主存储的就绪状态会显示为已连接。</p>
进入维护模式	<p>将主存储进入维护模式。</p> <p>注：</p> <p> </p> <ul style="list-style-type: none"> 进入维护模式将同时停止该主存储上的云主机等相关资源。 进入维护模式后，该主存储上的云盘将不能使用。
创建云盘	<p>在主存储上创建一个云盘，此云盘为实例化云盘。</p> <p> 注： 共享云盘支持Ceph存储以及Shared Block存储，其他类型的主存储暂不支持。</p>
加载集群	<p>将主存储加载到指定的集群上。一个集群可以加载多个主存储。</p> <p>目前支持的同类型主存储场景如下：</p> <ul style="list-style-type: none"> 一个集群可以加载一个或多个本地主存储。 一个集群可以加载一个或多个NFS主存储。 一个集群可以加载一个或多个Shared Block主存储。 一个集群可以加载一个Shared Mount Point主存储。 一个集群只能加载一个Ceph主存储。 <p>目前支持的组合类型主存储场景如下：</p> <ul style="list-style-type: none"> 一个集群可以加载一个本地主存储和一个NFS主存储。 一个集群可以加载一个本地主存储和一个Shared Mount Point主存储。 一个集群可以加载一个本地主存储和一个Shared Block主存储。 一个集群可以加载一个Ceph主存储和一个Shared Block主存储。 一个集群可以加载一个Ceph主存储和多个Shared Block主存储。
卸载集群	将主存储从指定的集群卸载。

操作	描述
	<p>注:</p> <p>将主存储从集群卸载，需要注意以下情况：</p> <ul style="list-style-type: none"> 此操作将导致该主存储上，与所选集群相关的云主机关机，影响业务运行，请谨慎操作。 此操作将导致该主存储上，与所选集群相关的VPC路由器被删除，相关云主机的网络服务异常，请谨慎操作。  此操作将导致该主存储上，与所选集群相关的云盘将不能正常使用，请谨慎操作。 <p>将主存储从弹性裸金属集群卸载，需要注意以下情况：</p> <ul style="list-style-type: none"> 此操作将导致该主存储上，与所选弹性裸金属集群相关的弹性裸金属实例将关机，影响业务运行，请谨慎操作。 此操作将导致该主存储上，与所选弹性裸金属集群相关的云盘将不能正常使用，请谨慎操作。
删除主存储	<p>将主存储删除。</p> <p>注: 删除主存储需要注意以下情况：</p> <ul style="list-style-type: none"> 执行删除操作前请从所有集群卸载该主存储，否则不能删除。  删除主存储是非常危险的操作，此操作会直接删除该主存储上的所有资源，如云主机、弹性裸金属实例、云盘、快照等，即使重新添加此主存储，也无法自动识别原有的文件。
数据清理	<p>清理跨Ceph存储迁移、跨NFS存储迁移以及跨Shared Block迁移保留的原始数据。在主存储详情页的数据清理子页面，点击清理按钮，清理存储迁移保留的原始数据，清理后不可恢复，请谨慎操作。</p>

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。
- 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。
- 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。
- Cloud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Cloud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。

12.2.4.1 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，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，不支持从其他物理机启动，不支持指定物理主机启动，支持设置高可用级别为NeverStop，设置高可用级别为NeverStop后，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。

- 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。

12.2.4.2 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支持输入IP，输入格式为：*NFS_Server_IP:/NFS_Share_folder*
- 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。
- Cloud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。

12.2.4.3 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Cloud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。

12.2.4.4 Ceph

Ceph主存储：Ceph集群提供的分布式块存储作为主存储。Cloud主存储支持对接以下版本Ceph：

- Ceph开源版：J版本、L版本和N版本。

- Ceph企业版：所有已发布的Ceph企业版。若更关注数据安全和IO性能，推荐使用Ceph企业版，详情请联系官方技术支持获取帮助。

Ceph分布式存储特性

- 云盘存放在分布式存储，数据通过多副本或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Cloud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，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Cloud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，MonIP表示存储网络的监控节点IP，可以通过ceph -s读取。
- 对使用企业版Ceph的用户，当分布式存储许可证过期时间小于等于15天时，将在界面进行提示，为不影响您的售后服务，请尽快联系云平台相关人员进行授权更新。

12.2.4.5 Shared Block

Shared Block（共享块存储）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：
 - 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
 - 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
- 支持Windows故障转移群集的云主机平滑热迁移



注：从Cloud 3.9.0版本开始，Cloud针对Windows故障转移群集做了特定支持，云主机热迁移不会产生任何不良影响。

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。

12.2.4.6 主存储运维(扩展)

12.2.4.6.1 本地存储运维

本地主存储扩容

本地主存储扩容步骤如下：

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（假定设备名称为/dev/sdc）。
3. 创建新目录/new_volume，执行命令mount /dev/sdc1 /new_volume挂载此磁盘。
4. 执行命令rsync -a /zstack_ps /new_volume/拷贝原始的磁盘文件至新磁盘。

5. 添加内容至`/etc/fstab`，并将物理磁盘挂载点与`/zstack_ps`目录绑定。
6. 重启物理机，然后使用`df -h /zstack_ps`命令检查扩容后的空间增量。
7. 重启Cloud管理节点服务。
8. 重连物理机，继续使用Cloud。

维护本地主存储

计划性维护主存储将停止此存储上所有云主机，请Admin提前迁移重要云主机。计划性维护主存储步骤如下：

1. 通过UI方式登录Cloud，在**主存储**界面，点击**进入维护模式**按钮，将主存储进入维护模式。
2. 进入主存储后台进行维护操作。
3. 维护完成后，通过UI方式，在**主存储**界面，点击**启动**按钮，启动维护完成的主存储。

12.2.4.6.2 NFS存储运维

NFS存储扩容

扩容已有NFS存储容量步骤如下：

1. 对原NFS共享目录进行扩容，请联系官方技术支持。
2. 在管理节点重连NFS存储。
3. 重连物理机，继续使用Cloud。

使用新目录提供NFS步骤如下：

1. 选择NFS存储集群的物理机，挂载新的NFS存储至该物理机的`/NFS_volume`目录，参考命令：`mount NFS_IP:/<url>/NFS_volume`。
2. 执行命令`rsync-a/NFS_ps/NFS_volume/`拷贝原始的磁盘文件至新磁盘。
3. 更新NFS配置文件，改写共享目录名称。
4. 在管理节点配置重连NFS存储。
5. 重连物理机，继续使用Cloud。

维护NFS存储

计划性维护主存储将停止此存储上所有云主机，请Admin提前迁移重要云主机。计划性维护主存储步骤如下：

1. 通过UI方式登录Cloud，在**主存储**界面，点击**进入维护模式**按钮，将主存储进入维护模式。
2. 进入主存储后台进行维护操作。

3. 维护完成后，通过UI方式，在**主存储**界面，点击**启动**按钮，启动维护完成的主存储。

12.2.4.6.3 Shared Mount Point存储运维

Shared Mount Point存储扩容

在线扩容已有Shared Mount Point存储容量步骤如下：

1. 保证正常业务运行情况下质询对应存储厂商在线扩容方式。
2. 待存储厂商完成存储在线扩容后验证是否扩容成功。
3. 重连此主存储并识别扩容后新容量，完成在线扩容。

离线扩容已有Shared Mount Point存储容量步骤如下：

1. 通过UI登录Cloud云平台，将此主存储进入维护模式。
2. 将Shared Mount Point主存储进行下电扩容。
3. 上电此主存储，并在计算节点上确保已经识别到扩容后的存储容量。
4. 通过UI登录Cloud云平台，启用主存储，完成扩容。

维护Shared Mount Point存储

计划性维护主存储将停止此存储上所有云主机，请Admin提前迁移重要云主机。计划性维护主存储步骤如下：

1. 通过UI方式登录Cloud，在**主存储**界面，点击**进入维护模式**按钮，将主存储进入维护模式。
2. 进入主存储后台进行维护操作。
3. 维护完成后，通过UI方式，在**主存储**界面，点击**启动**按钮，启动维护完成的主存储。

12.2.4.6.4 企业版Ceph存储运维

如需进行企业版Ceph存储运维，请联系官方技术支持。

Ceph存储扩容

Ceph存储扩容步骤如下：

1. 在Ceph存储相应的物理机添加需要扩容的硬盘。
2. 进入Ceph平台的**硬盘管理**添加硬盘，待添加成功后刷新存储池。
3. 通过UI方式登录Cloud云平台，重连Ceph主存储。

Ceph存储变更管理IP地址

Ceph存储变更管理IP地址步骤如下：

1. 获取网络修改工具: `network-tool-1.1.tar.gz` (请联系官方技术支持获取)



注: 该离线修改网络工具不支持文件网关、块存储客户端组、对象存储S3网关、对象路由、NFS网关服务的地址修改。若需要修改以上服务, 请先删除挂载这些服务的相关网络, 待其他网络修改完成后在对应网络重新添加这些服务。

2. 执行以下命令, 查看master db所在的服务器:

```
[root@managementnode ~]# xms-manage db list
```

3. 上传`network-tool-1.1.tar.gz`工具包, 并依次执行以下命令, 在master db所在的服务器上执行停止集群服务的工具:

```
#解压工具包
[root@localhost ~]# tar xzf network-tool-1.0.tar.gz
#运行脚本
[root@localhost ~]# ./prepare.sh
```

脚本执行之后, 需手动输入UI的账号密码, 并输入yes确认, 该脚本会停止所有的服务。

4. 手动修改所有服务器的网卡地址。



注: 不能修改服务器的主机名。

5. 修改脚本的网络文件配置。需要修改`/opt/sds/network-tool/conf/network.conf`中的各网络信息, 修改`/opt/sds/network-tool/conf/hosts`中的主机管理网 IP 信息。
6. 执行命令`./modify-network.sh`, 运行服务修改脚本。修改完成后, 等待Ceph状态健康即可。



注:

- 脚本文件执行成功之后, xdc 恢复很慢, 可能需要等待5min, 需要等待Ceph和 xdc 恢复之后再进行创建操作。验证方法: 进行创建块存储卷操作。
- 脚本执行过程中ceph.conf 还没更新完, 可能会出现重起 osd的现象, 会导致脚本执行完成后, 查看ceph 状态出现osd down error。

解决办法: 先查看`/etc/ceph/ceph.conf` 地址是否更新, 如果是, 执行命令`systemctl restart ceph-osd.target`重启服务 (重启osd的命令)。

7. 修改管理节点IP地址。根据管理节点存在形式, 可通过如下方法进行修改:

- **管理节点为物理机**修改方法如下:

通过UI方式登录云平台, 在主存储详情页的**监控节点**界面, 删除旧的监控节点IP。

- **管理节点为云主机**修改方法如下:

1. 执行命令 `zsha export-config`，导出管理节点云主机配置文件到目录：`/tmp/current.config.json`。
2. 执行 `vim /tmp/current.config.json` 命令，进入配置文件编辑模式，调整配置文件中的 Node、MonAddrs、Chronyservers 选项。
3. 配置文件调整完成后，执行 `zsha import-config /tmp/current.config.json` 命令，重新导入配置文件。
4. 执行 `zsha start` 命令，启动管理节点服务。
5. 通过 UI 方式登录云平台，在主存储详情页的**监控节点**界面，删除旧的监控节点 IP。

Ceph 存储更换物理机

若超融合服务器故障，先确认故障点并修复，可能存在的故障如下：

- 若网卡故障，请更换网卡。
- 若进程异常，请修复进程。
- 若服务器部分硬盘故障，请更换部分硬盘。
- 若服务器操作系统损坏，请修复操作系统。
- 若操作系统无法修复，请重装操作系统。

故障排除后，根据以下步骤更换物理机：

1. 通过 UI 方式登录云平台，将故障物理机进入维护模式。
2. 将所有有用业务云主机迁移后，删除此物理机。
3. 通过 UI 方式登录企业版 Ceph，将存储 pool 内故障服务器上所有硬盘踢除。
4. 设置存储平台禁止数据恢复、服务器拓扑处移除此故障服务器。
5. 删除故障服务器 osd 硬盘、删除故障服务器缓存盘、删除故障服务器。
6. 维护或者更换故障服务器，然后重新部署新服务器。



注：重新部署新服务器需要注意以下情况：

1. 安装操作系统后配置网络与原服务器一致。
2. 进行初始化安装存储服务器（免密、hosts 域名解析、时间同步）。
7. 在企业版 Ceph 的**存储管理**界面添加新服务器、添加新缓存盘、添加新 osd 硬盘。
8. 将新服务器拖拽至拓扑图内。
9. 在 pool 内添加新服务器硬盘。
10. 在平台设置存储自恢复带宽 QoS，开启数据自恢复。

11. 通过UI方式登录Cloud云平台，在**物理机**界面，手动添加此物理机。

12. 检测数据平衡，待数据自动平衡完成后，故障更换操作完成。

Ceph存储新增计算节点

Ceph存储新增计算节点步骤如下：

1. 为新的计算节点安装操作系统，并配置网络与之前一致。
2. 进行初始化安装存储服务器（免密、hosts域名解析、时间同步）。
3. 通过UI方式登录企业版Ceph，在存储管理上添加新服务器（网关服务器）。
4. 通过UI方式登录Cloud云平台，在**物理机**界面，手动添加此物理机为计算节点，完成Ceph存储新增计算节点。

Ceph存储新增存储节点

Ceph存储新增存储节点步骤如下：

1. 新增存储节点安装操作系统后配置网络与原节点一致。
2. 进行初始化安装存储服务器（免密、hosts域名解析、时间同步）。
3. 通过UI方式登录企业版Ceph，在存储管理上添加新服务器（存储服务器）、添加新缓存盘、添加新osd硬盘。
4. 将新服务器拖拽入拓扑内。
5. 在pool内添加新服务器硬盘。
6. 在平台设置存储自恢复带宽QoS，开启数据自恢复。
7. 待存储自动平衡完数据后本次操作完成。

维护企业版Ceph存储

计划性维护主存储将停止此存储上所有云主机，请Admin提前迁移重要云主机。计划性维护主存储步骤如下：

1. 通过UI方式登录Cloud，在**主存储**界面，点击**进入维护模式**按钮，将主存储进入维护模式。
2. 进入主存储后台进行维护操作。
3. 维护完成后，通过UI方式，在**主存储**界面，点击**启动**按钮，启动维护完成的主存储。

维护企业版Ceph注意事项

- 通过浏览器（推荐Firefox或Chrome）访问企业版Ceph网页控制台：<http://管控节点IP:8056/>（管理节点+端口）。

- 通过UI方式可在**主存储**详情页，已创建的存储池获取其UUID。也可以在后台执行 `ceph osd pool ls` 命令查看此 pool uuid。
- 添加主存储和镜像服务器时，未指定企业版Ceph存储的pool，会导致Ceph主存储间歇性失联、不可用。

12.2.4.6.5 Shared Block存储运维

Shared Block扩容

底层FCSAN扩容步骤如下：

1. 扩容前请先与存储提供厂商确认最佳扩容方案。
2. 确认不影响业务情况下进行存储扩容。
3. 存储扩容完成后，通过UI方式登录云平台，在主存储详情页刷新容量，容量正常显示表示存储扩容完成。

维护Shared Block存储

计划性维护主存储将停止此存储上所有云主机，请Admin提前迁移重要云主机。计划性维护主存储步骤如下：

1. 通过UI方式登录Cloud，在**主存储**界面，点击**进入维护模式**按钮，将主存储进入维护模式。
2. 进入主存储后台进行维护操作。
3. 维护完成后，通过UI方式，在**主存储**界面，点击**启动**按钮，启动维护完成的主存储。

12.2.4.6.6 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。

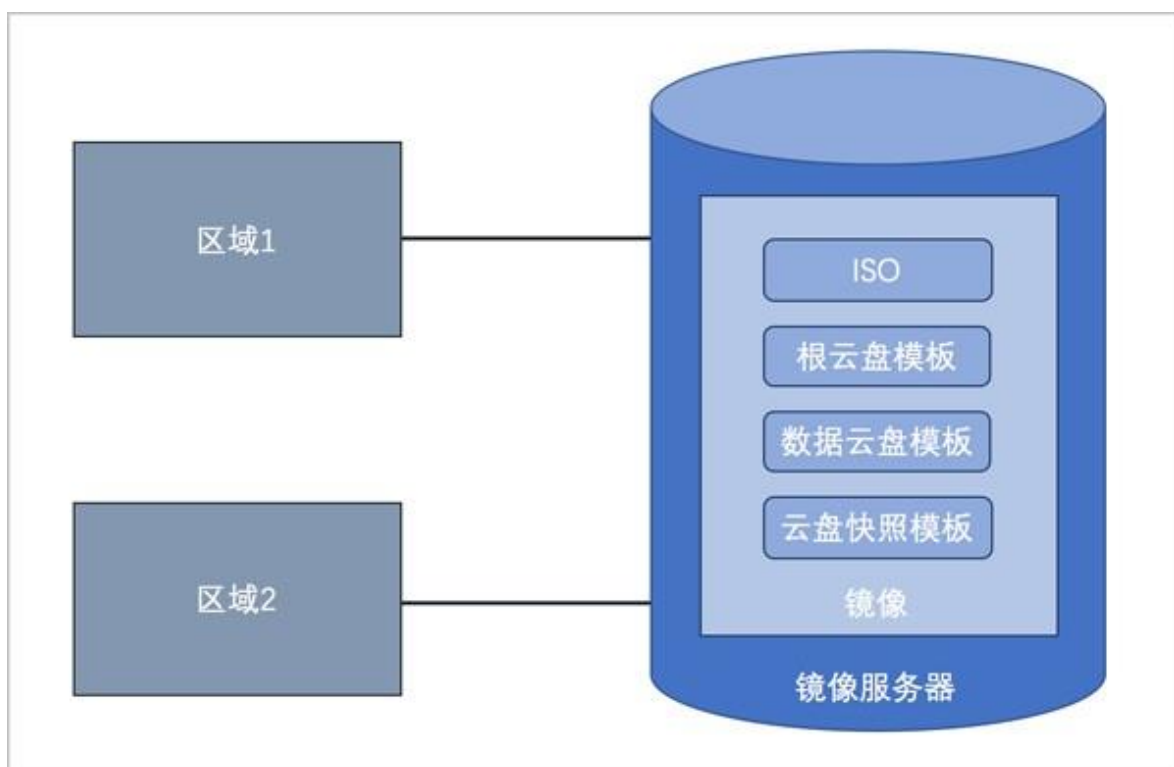
12.2.5 镜像服务器

镜像服务器（Backup Storage）：用于存储云主机镜像模板（含ISO）的存储服务器。

- 镜像服务器加载到区域之后，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 46: 镜像服务器所示：

图 46: 镜像服务器



- 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，默认会加载到当前区域。删除区域的同时会直接删除加载此区域的镜像服务器。

镜像服务器相关定义

镜像服务器支持以下类型：

1. ImageStore（镜像仓库）：

- 以镜像切片方式存储镜像文件，支持增量存储。
- 支持云主机的在线/关机快照、在线/关机创建镜像。
- 不带数据云盘云主机时，支持在线/暂停/关机。

- 整机时，LocalStorage、NFS、SMP、Ceph、Shared Block类型的主存储，支持在线/暂停/关机。
- 同一管理节点下的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. 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。
- 不带数据云盘云主机时，支持在线/暂停/关机。
- 不支持整机。
- 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`

则需在镜像服务器上执行:

```

rbd export -p bak-t-c9923f9821bf45498fdf9cdfa1749943 --image 61ece0adc7244b0cbd12dafbc5494f0c --path /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

```

3. AliyunEBS镜像服务器:

- 以对象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。
- 不带数据云盘云主机时，支持在线/暂停/关机。
- 不支持整机。
- 导出镜像需在镜像服务器上导出（如有需求请咨询官方技术支持获取帮助）。

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的关系](#)所示:



表 7: 主存储与镜像服务器的关系



PS\BS	ImageStore	Ceph
Local Storage	○	×

NFS	○	×
Shared Mount Point	○	×
Ceph	○	○
Shared Block	○	×

- 当主存储为LocalStorage、NFS、Shared Mount Point类型时，镜像服务器的默认类型为ImageStore。
- 当主存储为NFS或Shared Mount Point类型时，可将相应共享目录手动加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ImageStore类型的镜像服务器。
- 当主存储为Shared Block类型时，镜像服务器的默认类型为ImageStore。
- 当主存储为AliyunNAS类型时，镜像服务器的默认ImageStore。
- 当主存储为AliyunEBS类型时，镜像服务器的默认类型为AliyunEBS。

镜像服务器支持以下操作：

操作	描述
创建镜像服务器	创建一个新的镜像服务器。
编辑镜像服务器	编辑镜像服务器的名称、简介信息。
启用镜像服务器	启用处于停止状态的镜像服务器。
停用镜像服务器	<p>停用选中的镜像服务器。</p> <p> 注： 停用镜像服务器将不能添加新镜像，已添加镜像不受影响，仍可用于创建云主机，不影响正常业务。</p>
重连镜像服务器	<p>重连选中的镜像服务器，重连镜像服务器会更新镜像服务器上相关的存储信息。</p> <p> 注：</p> <ul style="list-style-type: none"> • 重连过程中其上资源暂时无法操作。 • 如果任意一台物理机正常连接到镜像服务器，该镜像服务器的就绪状态就会显示为已连接。
数据清理	清理镜像服务器中已被彻底删除的无效数据和过期的临时数据，释放存储空间。

操作	描述
	 注: <ul style="list-style-type: none"> 将某镜像文件（包括普通镜像和路由器镜像）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，清理完毕后，界面会显示本次清理释放的空间大小。 仅ImageStore类型的镜像服务器支持该操作。 数据清理期间，请避免执行写入数据相关操作。
更新密码	更新镜像服务器的密码，更新密码后需要手动重连镜像服务器。
删除镜像服务器	删除选中的镜像服务器。  注: <ul style="list-style-type: none"> 删除镜像服务器将删除此镜像服务器上的所有镜像文件（包括普通镜像和路由器镜像），请谨慎操作。 删除操作只是删除镜像服务器和镜像在Cloud中的记录，并不移除真实的数据。

注意事项

关于镜像服务器支持和快照的关系：

- 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、Ceph均支持。
- 在线创建镜像：镜像仓库、Ceph支持。
- 关机创建镜像：镜像仓库、Ceph均支持。

12.2.5.1 ImageStore（镜像仓库）

ImageStore（镜像仓库）以镜像切片方式存储镜像文件，当主存储为本地存储（LocalStorage）、NFS、Shared Mount Point、Ceph、SharedBlock类型时，可匹配ImageStore类型镜像服务器使用。

- 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、Ceph、Shared Block类型的主存储，支持在线/暂停/关机克隆。
- 同一管理节点下的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。

12.2.5.2 Ceph

Ceph镜像服务器以Ceph分布式块存储方式存储镜像文件，当主存储为Ceph类型时，可匹配Ceph类型镜像服务器使用。

Cloud镜像服务器支持对接以下版本Ceph：

- Ceph开源版：J版本、L版本和N版本。
- Ceph企业版：所有已发布的Ceph企业版。若更关注数据安全和IO性能，推荐使用Ceph企业版，详情请联系官方技术支持获取帮助。

注意事项

- 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。
- 不带数据云盘克隆云主机时，支持在线/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`

则需在镜像服务器上执行：

```
rbd export -p bak-t-c9923f9821bf45498fdf9cdfa1749943 --image 61ece0adc7244b0cbd12dafbc5494f0c --path /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
```

12.2.5.3 镜像服务器运维(扩展)

12.2.5.3.1 ImageStore镜像服务器运维

ImageStore镜像服务器扩容

ImageStore镜像服务器扩容步骤如下：

1. 停用本地镜像服务器。
2. 添加新的大容量磁盘至物理机，并进行分区格式化，假定设备名称为/dev/sdc。
3. 创建新目录/new_volume，执行命令mount /dev/sdc1 /new_volume挂载此磁盘。
4. 执行命令rsync -a /zstack_bs /new_volume/拷贝原始的磁盘文件至新磁盘。
5. 添加内容至/etc/fstab，并将物理磁盘挂载点与/zstack_ps目录绑定。
6. 重启物理机，使用df -h /zstack_bs检查扩容后的空间增量。
7. 重启Cloud管理节点服务。
8. 重连物理机继续使用Cloud。

维护ImageStore镜像服务器

ImageStore镜像服务器计划性维护步骤如下：

1. 停用ImageStore镜像服务器。
2. 在**镜像服务器**界面，选中ImageStore镜像服务器，点击**数据清理**按钮，清理镜像服务器中已被彻底删除的无效数据和过期的临时数据，释放存储空间。
3. 清理完成后，启用ImageStore镜像服务器，继续使用。

12.2.5.3.2 Ceph镜像服务器运维

如需进行Ceph镜像服务器运维，请联系官方技术支持。

Ceph镜像服务器扩容

Ceph镜像服务器扩容步骤如下：

1. 在Ceph存储相应的物理机添加需要扩容的硬盘。
2. 进入Ceph平台的**硬盘管理**添加硬盘，待添加成功后刷新存储池。
3. 通过UI方式登录Cloud云平台，重连Ceph镜像服务器。

Ceph镜像服务器变更IP地址

1. 获取网络修改工具：network-tool-1.1.tar.gz（请联系官方技术支持获取）



注：该离线修改网络工具不支持文件网关、块存储客户端组、对象存储S3网关、对象路由、NFS网关服务的地址修改。若需要修改以上服务，请先删除挂载这些服务的相关网络，待其他网络修改完成后在对应网络重新添加这些服务。

2. 执行以下命令，查看master db所在的服务器：

```
[root@managementnode ~]# xms-manage db list
```

3. 上传network-tool-1.1.tar.gz工具包，并依次执行以下命令，在master db所在的服务器上执行停止集群服务的工具：

```
#解压工具包
[root@localhost ~]# tar xzf network-tool-1.0.tar.gz
#运行脚本
[root@localhost ~]# ./prepare.sh
```

脚本执行之后，需手动输入UI的账号密码，并输入yes确认，该脚本会停止所有的服务。

4. 手动修改所有服务器的网卡地址。



注：不能修改服务器的主机名。

5. 修改脚本的网络文件配置。需要修改/opt/sds/network-tool/conf/network.conf中的各网络信息，修改/opt/sds/network-tool/conf/hosts中的主机管理网 IP 信息。
6. 执行命令./modify-network.sh，运行服务修改脚本。修改完成后，等待Ceph状态健康即可。



注：

- 脚本文件执行成功之后，xdc恢复很慢，可能需要等待5min，需要等待Ceph和xdc恢复之后再进行创建操作。验证方法：进行创建块存储卷操作。
- 脚本执行过程中ceph.conf还没更新完，可能会出现重起osd的现象，会导致脚本执行完成后，查看ceph状态出现osd down error。

解决办法：先查看/etc/ceph/ceph.conf地址是否更新，如果是，执行命令systemctl restart ceph-osd.target重启服务（重启osd的命令）。

7. 修改镜像服务器的监控节点：

通过UI方式登录云平台，在镜像服务器详情页的**监控节点**界面，删除旧的监控节点IP。

12.2.5.3.3 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. 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。

12.2.6 SAN存储

SAN存储分为iSCSI存储（iSCSI Storage）和FC存储（FC Storage）：

- iSCSI存储（iSCSI Storage）：基于iSCSI协议构建的SAN存储。用户可将iSCSI存储上划分的块设备添加为Shared Block主存储，或直接透传给云主机使用。
- FC存储（FC Storage）：基于FC协议构建的SAN存储。用户可将FC存储上划分的块设备添加为Shared Block主存储，或直接透传给云主机使用。

iSCSI存储支持以下操作：

操作	描述
添加iSCSI存储	添加一个新的iSCSI存储。
编辑	修改iSCSI存储的名称。
启用iSCSI存储	将处于停用状态的iSCSI存储启用。
停用iSCSI存储	将处于启用状态的iSCSI存储停用。
加载集群	将iSCSI存储加载到集群。
卸载集群	将iSCSI存储从已加载的集群上卸载。
同步数据	同步iSCSI存储上的数据。
删除iSCSI存储	<p>删除iSCSI存储。</p> <p>注：</p> <ul style="list-style-type: none"> • iSCSI存储从集群卸载后才能删除，卸载集群会断开物理机与iSCSI存储的连接。 • 块设备作为主存储使用，删除iSCSI存储将会使主存储失联。 • 块设备透传给云主机使用，删除iSCSI存储将会有数据丢失风险。

FC存储支持以下操作：

操作	描述
同步设备信息	手动刷新FC存储列表，识别最新的FC存储列表。

应用场景

- 将iSCSI磁盘或FC磁盘直接透传给云主机使用。
- 以共享块的方式，将iSCSI磁盘或FC磁盘添加为Shared Block主存储。

注意事项

iSCSI存储:

- 未被加载到云主机的磁盘，支持添加为Shared Block主存储。
- 添加为主存储的LUN不可用于其他用途。
- 未添加为主存储的磁盘支持加载到云主机。
- 一个磁盘支持加载到多个云主机，一个云主机支持加载多个磁盘。

FC存储:

- 集群状态正常且未被加载到云主机的块设备，支持添加为Shared Block主存储。
- 添加为主存储的LUN不可用于其他用途。
- 未添加为主存储的块设备支持加载到云主机。
- 一个块设备支持加载到多个云主机，一个云主机支持加载多个块设备。

12.2.6.1 SAN存储运维(扩展)

iSCSI存储运维

iSCSI存储计划性运维步骤如下:

1. 添加新iSCSI设备到Cloud云平台。
2. 在iSCSI的server端配置远端可访问服务器IP等信息，确保iSCSI服务端能正常访问iSCSI服务器。
3. 通过UI方式登录云平台，在**SAN存储 > iSCSI存储**界面，添加iSCSI服务器。
4. 输入登录iSCSI存储登录信息进行登录。
5. 完成后勾选iSCSI存储同步数据即可。

FC-SAN存储运维

FC-SAN存储计划性运维步骤如下:

1. 添加FC-SAN存储到Cloud云平台。
2. 联系存储厂商将FC-SAN映射到物理服务器上，确保服务器上能正常识别到此FC-SAN划分的存储lun。
3. 通过UI方式登录云平台，在**SAN存储 > FC存储**界面查看映射的FC-SAN存储。
4. 完成扫描后可点击**同步设备信息**按钮同步存储数据。

12.3 网络资源

网络资源主要涉及以下内容：

- 二层网络资源
- 三层网络资源
- 路由资源
- SDN控制器
- 专用网络

二层网络资源

二层网络资源包括VXLAN Pool和二层网络。

- 二层网络对应于一个二层广播域，支持L2NoVlanNetwork、L2VlanNetwork、VxlanNetwork、HardwareVxlanNetwork类型。
- L2NoVlanNetwork和L2VlanNetwork作为一组，与计算节点的端口在交换机端的设置应相同。
- 软件SDN类型的VXLAN Pool和VxlanNetwork共同提供了VxlanNetwork类型的配置，在使用VxlanNetwork前，需要先建立VXLAN Pool。创建完毕VXLAN Pool后，可指定或随机选择Vni来创建VxlanNetwork。
- 硬件SDN类型的VXLAN Pool和HardwareVxlanNetwork共同提供了HardwareVxlanNetwork类型的配置，在使用HardwareVxlanNetwork前，需要先建立VXLAN Pool。创建完毕VXLAN Pool后，可指定或随机选择Vni来创建HardwareVxlanNetwork。

三层网络资源

三层网络作为二层网络的子资源，主要基于二层网络提供给云主机的网络配置，包括IP地址范围，网关，DNS，网络服务等。

路由资源

Cloud使用定制的Linux云主机作为路由设备提供云主机网络服务。相关路由资源主要包括：VPC路由器、高可用组、路由器镜像、路由器规格。

SDN控制器

通过添加SDN控制器，可在云平台接管硬件交换机的SDN网络，从而降低网络延迟，提升VXLAN网络性能。

专用网络

用于管控云平台相关物理资源和提供专用网络服务，包括：管理网络、流量网络。专用网络不能用于创建云主机。

网络使用流程

先创建二层网络，再创建三层网络，最后使用这些网络提供的各种网络服务。

网络架构模型

支持两种基本网络架构模型：扁平网络、VPC

1. 扁平网络

- 扁平网络支持以下网络服务：DHCP、弹性IP、安全组、User Data等；
- 扁平网络的网络服务采用分布式的DHCP、分布式的EIP结构；
- 扁平网络的DHCP服务也包含了DNS的功能；
- 初始化引导设置使用的网络模型就是采用了扁平网络；
- 支持基于VxlanNetwork或HardwareVxlanNetwork的扁平网络架构。

2. VPC

- VPC支持以下网络服务：DHCP、DNS、SNAT、路由表、弹性IP、端口转发、负载均衡、IPsec隧道、安全组、动态路由、组播路由、VPC防火墙、Netflow等；
- VPC的DHCP服务默认采用分布式的DHCP；
- VPC主要使用定制的Linux云主机作为VPC路由器提供网络服务；
- 网络服务（端口转发、负载均衡、IPsec隧道、路由表等）可以同时作用在一个VPC的多个子网上，进一步提升网络效率；
- 支持基于VxlanNetwork的VPC网络架构；
- 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。

网络协议

Cloud公有网络、扁平网络和VPC网络支持IPv4和IPv6两种网络协议，用户可按需创建IPv4、IPv6或IPv4+IPv6类型的网络。

12.3.1 二层网络

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

- VLAN、VXLAN、或者SDN等能提供二层隔离技术都可作为二层网络。

- 二层网络负责为三层网络提供二层隔离。

二层网络主要支持的四种类别

二层网络主要支持以下四种类别：

1. VxlanNetwork

VxlanNetwork类型表示使用软件SDN类型VxlanNetworkPool指定的Vni来创建VXLAN网络。

- 需基于软件SDN类型VxlanNetworkPool创建VxlanNetwork。
- 每个VxlanNetwork对应了软件SDN类型VxlanNetworkPool里的一个Vni。
- VxlanNetwork是使用UDP封装在三层物理网络上建立的二层逻辑网络。
- VxlanNetwork可跨越物理三层网络。
- 使用IP多播封装广播和多播报文。
- 使用24位VxlanNetwork标识符，最大支持16M个逻辑网络。
- 可用于创建三层网络。

2. 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。
- 创建二层网络，会根据输入的网络设备创建网桥。

3. L2VlanNetwork

VlanNetwork类型表示相关的物理机对应的网络设备需设置VLAN。

- 如需云主机网络和物理机网络互通，则需在交换机端设置Trunk模式。
- 从逻辑上划分虚拟局域网，支持1-4094个子网。
- 创建二层网络，会根据输入的网络设备创建VLAN设备，并基于此VLAN设备创建网桥。

4. HardwareVxlanNetwork

HardwareVxlanNetwork类型表示使用硬件SDN类型VxlanNetworkPool指定的Vni来创建VXLAN网络。

- 需基于硬件SDN类型VxlanNetworkPool创建HardwareVxlanNetwork。
- 每个HardwareVxlanNetwork对应了硬件SDN类型VxlanNetworkPool里的一个Vni。
- HardwareVxlanNetwork是使用UDP封装在三层物理网络上建立的二层逻辑网络。

- HardwareVxlanNetwork可跨越物理三层网络。
- 使用IP多播封装广播和多播报文。
- 可用于创建三层网络。



注:

- 在添加NoVlanNetwork和VlanNetwork时，需要输入网卡设备名称。
- 在CentOS 7系列系统中，ethx格式的网卡名称会在系统重启后导致网卡顺序随机改变，建议将各计算节点的网卡设备名称修改成非ethx格式，例如，可修改成em01格式。尤其是带多网卡的云主机环境中。

二层网络与集群、三层网络、云主机之间的关系

二层网络与集群、三层网络、云主机之间存在以下关系：

- 如果集群已加载二层网络，但物理机不存在此二层设备，则物理机不能添加进入对应集群。
- 如果集群未加载二层网络，但物理机不存在此二层设备，则集群不能加载此二层网络。
- 如果某物理机存在此二层设备，但设备接线与集群内其他物理机接线不一致，则创建出的云主机IP不能正常工作。
- 一个二层网络可用于创建多个三层网络，若二层网络为HardwareVxlanNetwork类型，创建的私有网络仅支持扁平网络及相应网络服务，不支持VPC网络。
- 删除二层网络，其对应的子资源三层网络将被删除，使用此三层网络的云主机的网卡也将被删除，请慎重操作。
- 删除二层网络，会删除使用此二层网络的VPC路由器和路由器规格。
- 删除公有网络对应的二层网络，其对应的路由器的一切服务均会被删除，包括VPC路由器、路由器规格、虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道、NetFlow等。
- 一个软件类型的VXLAN Pool可以创建多个VxlanNetwork，这些VxlanNetwork可以分别应用于扁平网络或VPC网络。
- VxlanNetwork下的云主机无法被外部的网络直接访问，需要通过弹性IP或者端口转发等服务进行间接访问。
- 一个硬件类型的VXLAN Pool可以创建多个HardwareVxlanNetwork，这些HardwareVxlanNetwork目前仅支持应用于扁平网络。

表 8: 管理L2NoVlanNetwork/L2VlanNetwork类型的二层网络




操作	描述
创建二层网络	创建一个L2NoVlanNetwork或L2VlanNetwork类型的二层网络。
编辑二层网络	修改二层网络的名称与简介。
加载集群	加载二层网络到集群。
卸载集群	将二层网络从集群卸载。  注： 卸载集群后，相应云主机的网卡将被卸载，请谨慎操作。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> 全局共享：将资源共享给所有的项目和账户使用。 指定共享：将资源共享给指定的项目和账户使用。 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p>注：</p> <ul style="list-style-type: none">  将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除二层网络	删除二层网络会删除其下三层网络及相关的 VPC 路由器，并卸载相应云主机的网卡，请谨慎操作。

表 9: 管理VxlanNetwork类型的二层网络

操作	描述
创建二层网络	创建一个VxlanNetwork类型的二层网络。
编辑二层网络	修改二层网络的名称与简介。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> 全局共享：将资源共享给所有的项目和账户使用。 指定共享：将资源共享给指定的项目和账户使用。 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p> 注：</p>

操作	描述
	<ul style="list-style-type: none"> 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除二层网络	删除二层网络会删除其下三层网络及相关的 VPC 路由器，并卸载相应云主机的网卡，请谨慎操作。

表 10: 管理HardwareVxlanNetwork类型的二层网络

操作	描述
创建二层网络	创建一个HardwareVxlanNetwork类型的二层网络。
编辑二层网络	修改二层网络的名称与简介。
删除二层网络	删除二层网络会删除其下三层网络及相关的 VPC 路由器，并卸载相应云主机的网卡，请谨慎操作。

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，Cloud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，Cloud会创建一个新的名为eth0.2016.2016的网络设备。
- CloudCTStack_Agile专有云支持一个二层网络用于创建多个三层网络，但若非特殊业务需求，不推荐多个三层网络共用一个二层网络。

12.3.2 VXLAN Pool


VXLAN Pool：在一组VXLAN隧道端点（VTEP）之上创建的VXLAN网络的集合，同一个VXLAN网络池内VXLAN网络标识符（VNI）不能重复。

- 使用VXLAN网络前需先建立VXLAN Pool。
- VXLAN Pool不能用于创建三层网络，只表示VXLAN网络的集合。

- VXLAN Pool支持两种类型：软件SDN、硬件SDN
 - 软件SDN类型：
 - 软件SDN类型VXLAN Pool的Vni范围支持1-16777214。
 - 加载的集群内物理机在指定的CIDR应有IP作为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，本云平台对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与集群进行加载时，检查的是VTEP相关的IP地址，与物理的二层设备无关。
 - 硬件SDN类型：
 - 需提前添加SDN控制器到云平台。
 - 硬件SDN类型VXLAN Pool支持的Vni范围取决于SDN控制器对应的虚拟分布式交换机。
 - 加载的集群内物理机网卡应与SDN控制器管理下的交换机相连。
 - 若使用VCFC配置硬件SDN，需提前在VCFC上配置VLAN与VXLAN的映射表，才能配置成功。

VXLAN Pool支持以下操作：

操作	描述
创建VXLAN Pool	创建一个VXLAN Pool。
编辑VXLAN Pool	修改VXLAN Pool的名称与简介。
加载集群	加载VXLAN Pool到集群。 <ul style="list-style-type: none"> • 软件SDN类型VXLAN Pool：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。 • 硬件SDN类型VXLAN Pool：加载的集群内物理机网卡应与SDN控制器管理下的交换机相连。
卸载集群	从集群卸载VXLAN Pool。
设置共享模式	设置该资源的共享模式。目前支持以下三种模式：

操作	描述
	<ul style="list-style-type: none"> 全局共享：将资源共享给所有的项目和账户使用。 指定共享：将资源共享给指定的项目和账户使用。 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p>注：</p>  <ul style="list-style-type: none"> 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除VXLAN Pool	删除VXLAN Pool，其对应的子资源VXLAN网络将被删除，相关的三层网络和云主机的网卡也将被删除。

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。


12.3.3 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。

三层网络相关定义

- 公有网络：一般表示可直接访问互联网的网络，由于公有网络是一个逻辑概念，在无法连接互联网的环境中，用户也可以自定义该网络。

- 可用于扁平网络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。
 - 扁平网络：可与物理机网络直通，也可直接访问互联网的网络。云主机可使用扁平网络提供的分布式EIP访问公有网络。
 - 扁平网络支持以下网络服务：DHCP、弹性IP、安全组、UserData等。
 - 扁平网络的网络服务采用分布式的DHCP、分布式的EIP结构。
 - 扁平网络的DHCP服务也包含了DNS的功能。
 - VPC网络：云主机使用的私有网络，可通过VPC路由器访问互联网。
 - VPC网络作为VPC的私有网络，使用VPC路由器提供以下网络服务：DHCP、DNS、SNAT、路由表、安全组、弹性IP、端口转发、负载均衡、IPsec隧道、动态路由、组播路由、VPC防火墙、Netflow等。
 - 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。
 - 专用网络：
 - 管理网络：管理控制云平台相关物理资源的网络，例如：配置访问物理机、主存储、镜像服务器、VPC路由器时使用的网络。
-  **注：**创建VPC路由器时需要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。
- 流量网络：端口镜像的专用网络，用于将网卡的网络流量镜像到远端。不能作为其他网络使用，不能用于创建云主机。
 - 特定场景网络：
 - 存储网络：用于表示共享存储指定的存储网络，可使用此存储网络来判断云主机健康状态。建议提前规划单独的存储网络，避免潜在风险。
 - VDI网络：在创建集群时，可指定VDI网络的CIDR，此网络用于VDI连接的协议流量。如果不设置，VDI将默认使用管理网络。
 - 迁移网络：在创建集群时，可指定迁移网络的CIDR，此网络用于云主机在当前云平台内迁移。如果不设置，云主机迁移将默认使用管理网络。
 - 镜像同步网络：同一管理节点下的ImageStore类型的镜像服务器间镜像同步使用的网络。
 - 如果已部署镜像同步单独使用的网络，在添加镜像仓库时，可指定镜像同步网络的CIDR。

- 如果不设置，镜像同步将默认使用管理网络。
- 如果源镜像仓库和目标镜像仓库均设置镜像同步网络，起作用的是目标镜像仓库的镜像同步网络。
- 数据网络：计算节点和镜像服务器之间进行数据通讯的网络。
 - 使用单独的数据网络，可避免网络拥塞，提高传输效率。
 - 如果不设置，将默认使用管理网络。
- 备份网络：Cloud提供灾备服务高级功能。在本地灾备场景下，本地云主机/云盘/数据库备份到本地备份服务器、以及本地备份数据从本地备份服务器还原至本地时使用的网络。
 - 如果已部署本地灾备单独使用的网络，在添加本地备份服务器时，可指定备份网络的CIDR。
 - 使用单独的备份网络，可避免网络拥塞，提高传输效率。
 - 如果不设置，本地灾备将默认使用管理网络。




注:



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），且需在购买企业版云平台许可证基础上使用，不可单独使用。

公有网络支持以下操作：

操作	描述
创建公有网络	创建一个新的公有网络。
添加DNS	添加DNS：添加一个IPv4或IPv6类型的DNS服务器地址。 <ul style="list-style-type: none"> • IPv4类型：例如可指定223.5.5.5、8.8.8.8或114.114.114.114 • IPv6类型：例如可指定240C::6644或240C::6666
设置共享模式	设置当前公有网络的共享模式，包括： <ul style="list-style-type: none"> • 全局共享：将公有网络共享给全部项目/普通账户使用（若已安装企业管理模块许可证） • 指定共享：将公有网络共享给指定项目/普通账户使用（若已安装企业管理模块许可证） • 不共享：该公有网络仅admin可使用 <p>注：</p> <ul style="list-style-type: none"> • 修改共享模式将召回共享资源的使用权限。




操作	描述
	<ul style="list-style-type: none"> 修改共享模式，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除	<p>将公有网络删除。</p> <p> 注： 删除公有网络会卸载正在使用此网络的云主机网卡，并删除相应的路由器、网络服务和路由器规格，请谨慎操作。</p>

扁平网络支持以下操作：

操作	描述
创建扁平网络	创建一个新的扁平网络。
添加DNS	<p>添加DNS：添加一个IPv4或IPv6类型的DNS服务器地址。</p> <ul style="list-style-type: none"> IPv4类型：例如可指定223.5.5.5、8.8.8.8或114.114.114.114 IPv6类型：例如可指定240C::6644或240C::6666
设置共享模式	<p>设置当前扁平网络的共享模式，包括：</p> <ul style="list-style-type: none"> 全局共享：将扁平网络共享给全部项目/普通账户使用（若已安装企业管理模块许可证） 指定共享：将扁平网络共享给指定项目/普通账户使用（若已安装企业管理模块许可证） 不共享：该扁平网络仅admin可使用 <p>注：</p> <p> </p> <ul style="list-style-type: none"> 修改共享模式将召回共享资源的使用权限。 修改共享模式，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除	<p>将扁平网络删除。</p> <p> 注： 删除扁平网络会卸载正在使用此网络的云主机网卡，并删除相应的路由器、网络服务和路由器规格，请谨慎操作。</p>

VPC网络支持以下操作：

操作	描述
创建VPC网络	创建一个新的VPC网络。

操作	描述
设置共享模式	<p>设置当前VPC网络的共享模式，包括：</p> <ul style="list-style-type: none"> 全局共享：将VPC网络共享给全部项目/普通账户使用（若已安装企业管理模块许可证） 指定共享：将VPC网络共享给指定项目/普通账户使用（若已安装企业管理模块许可证） 不共享：该VPC网络仅admin可使用 <p>注：</p> <p> 修改共享模式将召回共享资源的使用权限。</p> <p> 修改共享模式，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。</p>
加载VPC路由器	加载VPC路由器到VPC网络。
卸载VPC路由器	将VPC网络的VPC路由器卸载。
删除	<p>将VPC网络删除。</p> <p> 注： 删除VPC网络会卸载正在使用此网络的云主机网卡。</p>

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VPC网络，或指定扁平网络、VPC网络混合使用。
- 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，若二层网络为HarewareVxlanNetwork类型，创建的私有网络仅支持扁平网络及相应网络服务。

创建公有网络或三层时，支持指定DHCP服务IP，根据选择添加网络段方法（IP范围、CIDR），需要注意以下情况：

- IP范围：**

注：

- 若首次创建三层网络并启用DHCP服务，或对已启用DHCP服务的三层网络添加首个网络段，支持自定义设置DHCP服务IP。
- 若三层网络已存在DHCP服务IP，添加网络段不允许自定义设置DHCP服务IP。

- DHCP服务IP可以在添加的IP范围之内或之外，但必须在添加的IP范围所属的CIDR内，且未被占用。
- 起始IP和结束IP内的IP网络段，不允许包含链路本地地址 (169.254.0.0/16) 的IP地址。
- 若留空不填，将由系统在添加的IP范围内随机指定。
- **CIDR:**



注:

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

若三层网络使用IPv6协议，需要注意以下情况：

- 若三层网络（公有网络、扁平网络、VPC网络）IP地址类型发生变化（例如：由IPv4变为IPv4+IPv6），需重启已使用该网络的云主机，配置才能生效。
- 若对已加载VPC路由器的VPC网络添加新类型的网络段（例如：IPv4类型VPC网络新添加IPv6网络段），需重启VPC路由器，否则可能导致网络不通。
- 若路由器规格中三层网络使用的公有网络存在IPv6网络段，创建VPC路由器时，请务必使用最新版本的路由器镜像。
- 使用IPv6或IPv4+IPv6类型的网络创建云主机，需通过dhclient -6 NIC_NAME命令手动获取IP地址。
- 推荐一台云主机仅使用一个IPv6地址，否则可能存在风险。

12.3.4 VPC路由器

一个定制的云主机，用于提供多种网络服务。包括虚拟IP，弹性IP，IPsec隧道，端口转发，负载均衡，DHCP等服务，同时支持设置组播路由。VPC路由器支持内外部全方面实时监控，并提供配套报警服务，同时支持设置跨集群高可用策略，充分保障网络核心资源高可用性。



VPC路由器特性


基于路由器规格直接创建的VPC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路由器规格的VPC路由器。

- 须提前创建路由器规格所需的公有网络和管理网络、路由器镜像资源。
- VPC路由器可灵活挂载或卸载VPC网络或其他公有网络。
- 路由器规格定义的公有网络和管理网络，不可卸载。
- 同一个路由器规格可以创建多个VPC路由器，这些VPC路由器共享使用同一个路由器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路由器拥有高于云主机的资源优先级，当物理机负载率过高，出现资源竞争时，资源优先级顺序为（从低到高）：优先级为**正常**的云主机 < 优先级为**高**的云主机 < VPC路由器。例如：当物理机出现CPU资源竞争时，较于普通云主机，VPC路由器具备更高的CPU资源抢夺能力。

VPC路由器支持以下操作：

操作	描述
编辑VPC路由器	修改VPC路由器的名称与简介。
创建VPC路由器	创建一个VPC路由器。
启动VPC路由器	将停止状态的VPC路由器启动。
停止VPC路由器	将运行中的VPC路由器停止。 注： 停止VPC路由器将同时停止路由器上的所有网络服务，请谨慎操作。 
重启	重启VPC路由器。
重连	重连VPC路由器。 注：  <ul style="list-style-type: none"> • 目前管理节点升级重启后，VPC路由器可自动升级。
迁移	VPC路由器支持在线迁移。 <ul style="list-style-type: none"> • 本地存储上的VPC路由器在线迁移，需在Cloud主菜单，点击设置 > 平台设置 > 全局设置 > 基本设置，将本地存储在线迁移设为true。
打开控制台	通过终端访问VPC路由器。
设置/取消控制台密码	支持设置/取消VPC路由器的控制台密码，重启生效。
设置跨集群高可用策略	该策略默认开启，表示VPC路由器可跨集群自动迁移。该策略关闭后，VPC路由器将限制在策略生效时所在集群内活动。 <ul style="list-style-type: none"> • 背景说明：

操作	描述
	<ul style="list-style-type: none"> 在3.8.0之前版本中，当VPC路由器高可用策略触发或者VPC路由器所在计算节点进入维护模式时，系统会选择其他合适的计算节点自动恢复（或迁移）该VPC路由器，合适的计算节点可能在当前集群、甚至跨集群（如果多个集群挂载了相同的三层网络和主存储）。 从3.8.0版本开始，VPC路由器支持设置跨集群高可用策略，该策略关闭后，VPC路由器将限制在策略生效时所在集群内活动。 目前适用场景：VPC路由器高可用更换物理机启动和物理机进入维护模式触发迁移。 该策略只针对VPC路由器自动迁移行为有影响，其它如：手动热迁移VPC路由器、指定物理机启动VPC路由器均不受影响。 开启后，上述适用场景的VPC路由器活动将不受集群范围限制。
删除	<p>删除VPC路由器。</p> <p> 注：删除VPC路由器会导致相关的云主机网络服务不可用，需重新创建VPC路由器，并加载云主机使用的VPC网络，重启云主机才可恢复网络服务，请谨慎操作。</p>

注意事项

使用VPC路由器需注意：

- 需先建立路由器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共享路由器规格，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。

12.3.5 VPC路由器高可用组

一对互为主备的VPC路由器，当主VPC路由器状态异常，自动切换至备VPC路由器，为业务高可用提供保障。


- 以下VPC路由器配置，修改任一VPC路由器，将同步修改其伙伴路由器：

- 增加或删除网络。
- 配置网络服务：EIP、PF、LB、IPsec、VipQos、DNS、SNAT、OSPF、Multicast以及分布式路由。
- 以下操作只对一个路由器生效：
 - 重启、重连、删除以及打开控制台
- 支持普通路由器添加至VPC路由器高可用组

注:

- 该普通路由器需实现管理网络和公有网络分离。
- 添加至VPC路由器高可用组前需停止该VPC路由器。
- 高可用组内的VPC路由器将只展示在高可用组详情页中，在路由器列表不单独展示。

VPC路由器高可用组支持以下操作：

操作	描述
编辑VPC路由器高可用组	修改VPC路由器高可用组的名称与简介。
创建VPC路由器高可用组	创建一个VPC路由器高可用组。
添加VPC路由器	<p>添加VPC路由器到高可用组中。添加VPC路由器可选择新建路由器或导入已有路由器。</p> <ul style="list-style-type: none"> • 若选择新建路由器，创建完成后需在高可用组详情页，待确定VPC路由器主备关系后设置DNS，以确保VPC路由器正常运行。 • 若选择导入已有路由器，导入的VPC路由器需处于停止状态，且公有网络和系统网络分离。
删除	<p>删除VPC路由器高可用组。</p> <p> 注：删除VPC路由器高可用组，将同步删除组内所有VPC路由器，导致相关云主机的网络服务异常，请谨慎操作。</p>

12.3.6 路由器镜像


封装网络服务，用于创建VPC路由器/负载均衡实例，包括两种类型：VPC路由器镜像、高性能实例型负载均衡镜像。路由器镜像不能直接用于创建业务云主机。

路由器镜像特性

VPC路由器镜像只能用于创建VPC路由器，提供各种网络服务。

高性能实例型负载均衡镜像封装了高性能实例型负载均衡服务，只能用于创建负载均衡实例。所创建的负载均衡实例是一个定制的云主机，负载均衡服务独享该实例性能。

路由器镜像支持以下操作：



操作	描述
编辑路由器镜像	修改路由器镜像的名称和简介。
添加路由器镜像	添加一个路由器镜像。
启用路由器镜像	启用后，创建路由器时，此镜像可作为候选使用。
停用路由器镜像	停用后，创建路由器时，此镜像将不再作为候选使用。
导出路由器镜像	导出路由器镜像。 <ul style="list-style-type: none"> 仅 ImageStore 镜像服务器支持通过 UI 导出镜像。 对于 Ceph 镜像服务器，需在 Ceph 镜像服务器上执行 rbd 命令将 Ceph 镜像导出。 已经导出的镜像不支持重复导出。
删除	将路由器镜像删除。 <div>  注：删除路由器镜像可能导致无法创建路由器，请谨慎操作。 </div>

12.3.7 路由器规格

定义VPC路由器使用的CPU、内存、镜像、管理网络、公有网络配置，用于创建VPC路由器，为公有网络/VPC网络提供多种网络服务。一个路由器规格可以创建一个或多个VPC路由器，这些VPC路由器共享使用该路由器规格里定义的公有网络段和管理网络段，且该公有网络段和管理网络段不可从这些VPC路由器卸载。

路由器规格支持以下操作：

操作	描述
编辑路由器规格	修改路由器规格的名称与简介。
创建路由器规格	创建一个路由器规格。
启用路由器规格	启用后，创建路由器时，此规格可作为候选使用。
停用路由器规格	停用后，创建路由器时，此规格将不再作为候选使用。
设置共享模式	设置当前路由器规格的共享模式。

操作	描述
	 注: <ul style="list-style-type: none"> 修改共享模式将修改共享资源的使用权限。 原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除	将路由器规格删除。  注: 删除路由器规格可能导致无法创建路由器，请谨慎操作。

12.3.8 SDN控制器



SDN控制器：云平台支持添加外部SDN控制器来控制外部交换机等网络设备。通过添加SDN控制器，可在云平台接管硬件交换机的SDN网络，从而降低网络延迟，提升VXLAN网络性能。

- 需提前规划管理网络，并完成SDN控制器的基础配置，才能添加SDN控制器到云平台。
- 目前仅支持添加H3C SDN控制器：VCFC。



注: 使用VCFC配置硬件SDN，需提前在VCFC上配置VLAN与VXLAN的映射表，才能配置成功。


SDN控制器支持以下操作：

操作	描述
添加SDN控制器	将SDN控制器添加到云平台。  注: 需提前规划管理网络，并完成SDN控制器的基础配置，才能添加SDN控制器到云平台。
编辑SDN控制器	修改SDN控制器的名称与简介。
删除SDN控制器	将SDN控制器删除。  注: 删除SDN控制器，会同时删除与该SDN控制器相关的硬件SDN类型的VXLAN Pool，从而删除该VXLAN Pool下所有VXLAN网络及其相关三层网络，请谨慎操作。

12.3.9 管理网络

管理控制云平台相关物理资源的网络，例如：配置访问物理机、主存储、镜像服务器、VPC路由器时使用的网络。

管理网络支持以下操作：

操作	描述
创建管理网络	创建一个新的管理网络。
删除	将管理网络删除。  注： 删除管理网络会删除相关的路由器。


12.3.10 流量网络

端口镜像的专用网络，用于将网卡的网络流量镜像到远端。



注： 流量网络不能作为其他网络使用，不能用于创建云主机。

流量网络支持以下操作：

操作	描述
创建流量网络	创建一个新的流量网络。
删除	将流量网络删除。  注： 删除流量网络会删除相关的路由器。

12.4 网络服务

云平台为云主机提供以下网络服务：安全组、虚拟IP、弹性IP、端口转发、负载均衡、防火墙、IPsec隧道、OSPF区域、Netflow、端口镜像、路由表。

支持以下两种网络架构模型：

- 扁平网络
- 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. VPC Router（VPC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。
- 负载均衡：将虚拟IP地址的访问流量分发到一组后端的云主机上，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VPC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。

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。
- VPC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。
 - 路由表: 通过路由表，用户可管理自定义路由。
 - 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: 将虚拟IP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。

高级网络服务

- 动态路由: 支持OSPF动态路由协议，用于单一自治系统内决策路由，适用于VPC网络场景。
- 组播路由: 将组播源发送的组播消息转发给云主机，在发送端和接收端实现点对多点连接，适用于VPC网络场景。
- VPC防火墙: 通过对VPC路由器接口处南北向流量进行过滤，有效保护整个VPC通信安全及VPC路由器安全，适用于VPC网络场景。
- 端口镜像: 将云主机网卡的网络流量复制一份到远端，对端口上的业务报文进行分析，方便对网络数据进行监控管理，适用于扁平/VPC网络场景。

- Netflow：通过Netflow对VPC路由器网卡的进出流量进行分析监控，支持Netflow V5、V9两种数据流输出格式，适用于VPC网络场景。

12.4.1 安全组

安全组：为云主机提供三层网络安全控制，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。

功能特点

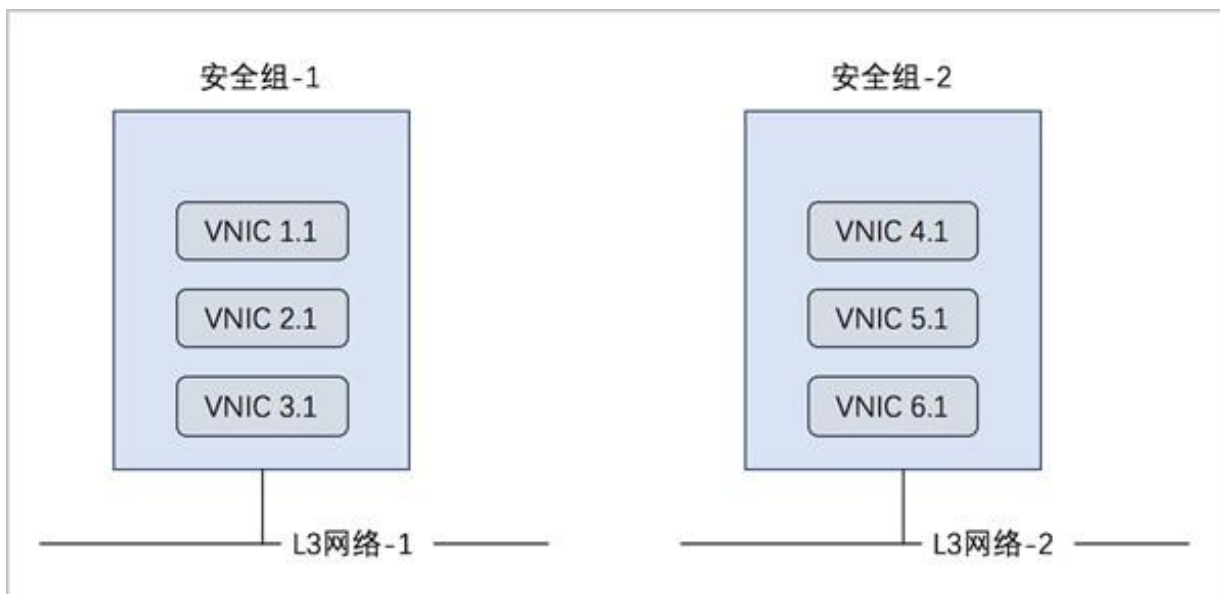
- 安全组规则按数据包的流向分为两种类型：
 - 入方向：代表数据包从外部进入云主机。
 - 出方向：代表数据包从云主机往外部发出。
- 安全组规则对通信协议支持以下类型：
 - ALL：表示涵盖所有协议类型，此时不能指定端口。
 - TCP：支持1-65535端口。
 - UDP：支持1-65535端口。
 - ICMP：默认起始结束端口均为-1，表示支持全部的ICMP协议。
- 安全组规则支持对数据源的限定，目前源可以设置为CIDR和安全组。
 - CIDR作为源：仅允许指定的CIDR才可通过。
 - 安全组作为源：仅允许指定的安全组内云主机通过。



注：若两者都设置，只取两者交集。

如图 47: 安全组所示：

图 47: 安全组



安全组支持以下操作:

操作	描述
创建安全组	创建一个新的安全组。
启用安全组	启用安全组，将启用所有的安全组规则和相关安全组服务。
停用安全组	停用安全组，停用后，安全组规则和相关安全组服务不再生效。
加载三层网络	安全组支持加载多个三层网络，它们会共享相同的安全组规则。
卸载三层网络	将安全组上的三层网络卸载。
删除安全组	删除安全组，将自动删除所有的安全组规则和相关安全组服务。

注意事项

- 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。
- 若使用安全组同时使用其他网络服务（如负载均衡、路由表等），需确保其他网络服务所需要的安全组规则已添加至该安全组中。

- 公有网络、扁平网络和VPC网络均支持安全组服务，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安全组规则被更新。

12.4.2 虚拟IP

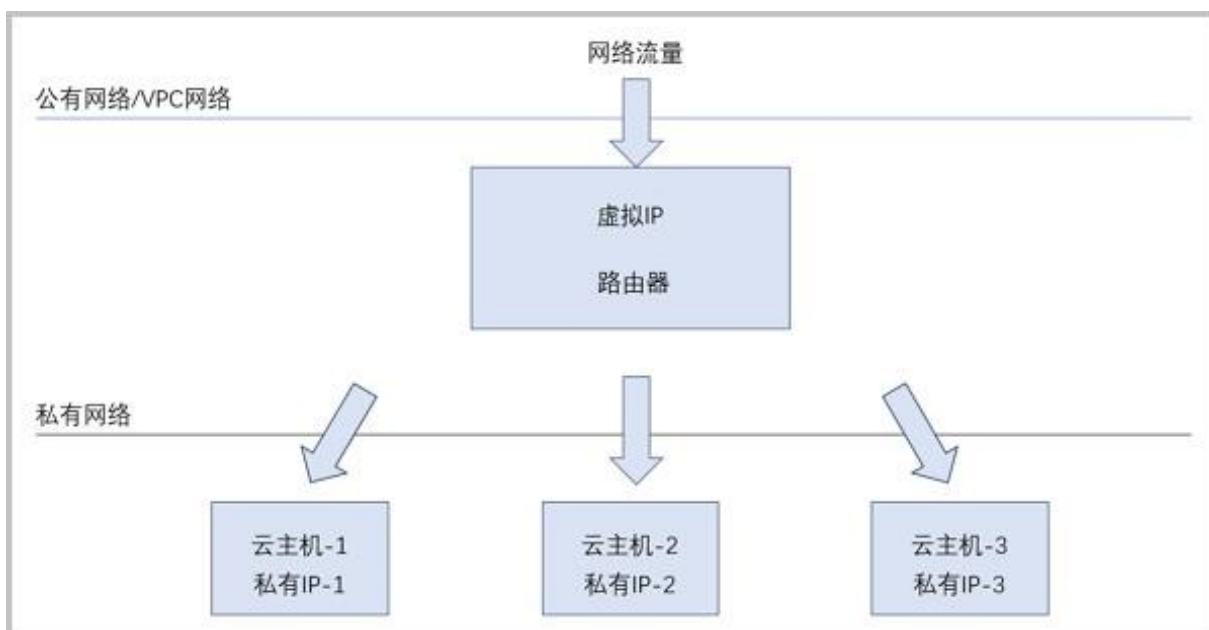
虚拟IP（VIP）：在桥接网络环境中，使用虚拟IP地址提供弹性IP、端口转发、负载均衡、IPsec隧道等网络服务，数据包会被发送到虚拟IP，再路由至云主机网络。

- 公有网络创建的虚拟IP支持为扁平网络提供弹性IP、负载均衡网络服务。
- 公有网络创建的虚拟IP支持为VPC网络提供弹性IP、端口转发、负载均衡、IPsec隧道网络服务。
- VPC网络创建的虚拟IP支持为VPC网络提供负载均衡网络服务。
- 扁平网络创建的虚拟IP支持为扁平网络提供弹性IP、负载均衡网络服务。

支持虚拟IP提供性能共享型负载均衡服务。性能共享型负载均衡通过VPC路由器提供负载均衡服务，访问流量经由VPC路由器分发给后端服务器。当VPC路由器上承载多业务运行，负载均衡服务需与其它业务共享VPC路由器性能。

如[虚拟IP提供性能共享型负载均衡服务](#)所示：

图 48: 虚拟IP提供性能共享型负载均衡服务




虚拟IP相关定义

- 公网虚拟IP：使用公有网络创建的虚拟IP，支持自定义创建或跟随路由器自动创建
 - 公网虚拟IP支持为扁平网络提供弹性IP、负载均衡网络服务。支持为VPC网络提供弹性IP、端口转发、负载均衡、IPsec隧道网络服务。
 - 公网虚拟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，但不同类型服务不能使用相同的端口号。
 - 公网虚拟IP支持QoS、监控数据、性能TOP 5、性能分析、报警功能。
- VPC网络虚拟IP：使用VPC网络创建的虚拟IP，仅支持自定义创建
 - VPC网络虚拟IP支持为VPC网络提供负载均衡网络服务。
 - VPC网络虚拟IP暂不支持QoS、监控数据、性能TOP 5、性能分析、报警功能。
- 扁平网络虚拟IP：使用扁平网络创建的虚拟IP，支持自定义创建或跟随路由器自动创建
 - 扁平网络虚拟IP支持为扁平网络提供弹性IP、负载均衡网络服务。
 - 扁平网络虚拟IP支持QoS、监控数据、性能TOP 5、性能分析、报警功能。
- 自定义虚拟IP：用户手动创建的虚拟IP，支持自定义创建公网虚拟IP、VPC网络虚拟IP、扁平网络虚拟IP
 - 一个自定义公网虚拟IP仅用于一个弹性IP服务实例。
 - 自定义虚拟IP不支持跨VPC路由器使用。
 - 使用弹性IP、端口转发、负载均衡、IPsec隧道时，可选择**创建虚拟IP**重新创建自定义虚拟IP提供服务，也可选择**已有虚拟IP**中的已有自定义虚拟IP提供服务。
- 系统虚拟IP：VPC路由器成功创建后，系统使用路由器加载的三层网络自动创建的虚拟IP，支持跟随路由器自动创建公网虚拟IP或扁平网络虚拟IP
 - 系统虚拟IP与VPC路由器一一对应，路由器每加载一条公有网络，系统将自动创建一个系统虚拟IP。且系统虚拟IP与VPC路由器的默认IP相同。
 - 默认公有网络创建的系统虚拟IP，用于提供源地址转换服务。
 - 使用弹性IP、端口转发、负载均衡、IPsec隧道时，可选择**已有虚拟IP**中的自定义/系统虚拟IP提供服务。

自定义虚拟IP支持以下操作：

操作	描述
创建虚拟IP	创建一个新的虚拟IP。

操作	描述
编辑虚拟IP	编辑虚拟IP的名称、简介信息。
删除虚拟IP	删除选中的虚拟IP。  注: <ul style="list-style-type: none"> 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。

12.4.3 弹性IP


弹性IP（EIP）：基于网络地址转换（NAT）功能，将一个网络的IP地址转换成另一个网络的IP地址，从而可通过其他网络访问内部私有网络。

弹性IP相关定义

- 公网弹性IP：基于公有网络创建的公网虚拟IP提供弹性IP服务
 - 内部私有网络是隔离的网络空间，不能被外部网络访问，通过公网弹性IP可对公有网络的访问直接关联到内部私网的云主机IP。
 - 公网弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
 - 公网弹性IP支持绑定私有网络（扁平网络/VPC网络）创建的云主机：
 - 基于分布式EIP实现的公网弹性IP地址，可通过公有网络访问扁平网络。
 - 可通过VPC路由器使用公有网络访问VPC网络。
- 扁平网络弹性IP：基于扁平网络创建的扁平网络虚拟IP提供弹性IP服务
 - 不同网段的扁平网络之间存在三层隔离，不能直接访问，通过扁平网络弹性IP可对一个扁平网络的访问直接关联到另一个扁平网络创建的云主机IP。
 - 扁平网络弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
 - 扁平网络弹性IP支持绑定其他扁平网络创建的云主机。

弹性IP支持以下操作：

操作	描述
创建弹性IP	创建一个新的弹性IP。
编辑弹性IP	编辑弹性IP的名称、简介信息。
绑定网卡	将弹性IP绑定到网卡。

操作	描述
	<p>设置方法：</p> <p>在弹性IP管理界面，选择一个弹性IP，选择绑定网卡，给网卡绑定弹性IP。</p> <p>选择需要绑定的网卡，点击确定按钮，完成绑定网卡操作。点击取消按钮，可取消绑定网卡，取消后也可在弹性IP操作中重新绑定。</p>
解绑网卡	<p>将弹性IP与网卡解绑。</p> <p>设置方法：</p> <p>在弹性IP管理界面，选择一个弹性IP，选择解绑网卡，给网卡解绑弹性IP。</p> <p>选择需要的网卡，点击确定按钮，完成卸载网卡操作。点击取消按钮，可取消解绑网卡，取消后也可在弹性IP操作中重新解绑。</p>
更改所有者	更改弹性IP的所有者。
删除弹性IP	<p>删除选中的弹性IP。</p> <p> 注：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，请勾选同时删除虚拟IP。</p>

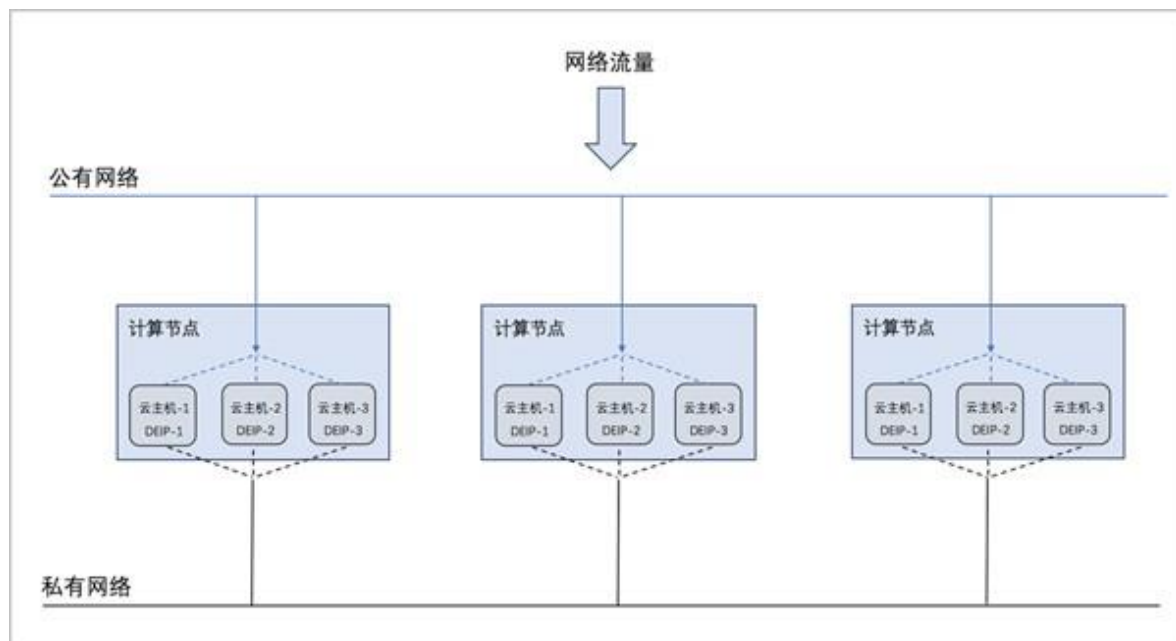
应用场景

- 扁平网络下弹性IP：

以公网弹性IP为例，扁平网络下弹性IP的应用场景。

如图 49: 扁平网络下弹性IP的应用场景所示：

图 49: 扁平网络下弹性IP的应用场景

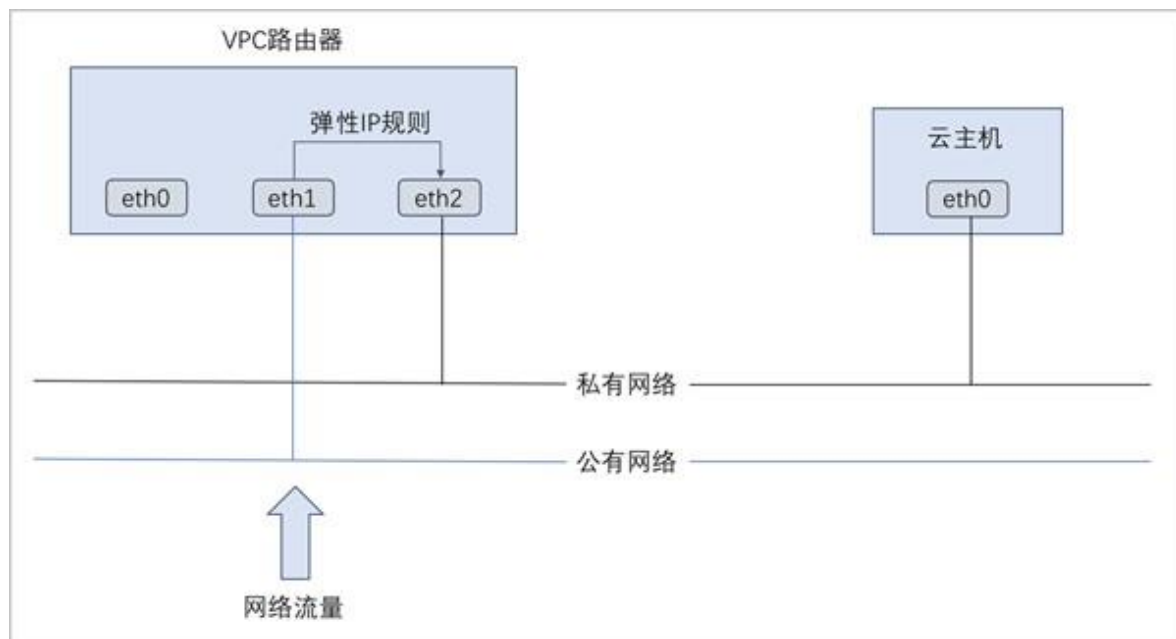


- 公有网络可通过防火墙连接到互联网。
- 扁平网络为各个计算节点内云主机提供IP地址，此IP地址默认情况下无法连接到互联网。
- 每个计算节点分别部署分布式EIP，可分别独立实现公有网络与扁平网络的绑定。
- VPC下弹性IP：

VPC下弹性IP的应用场景。

如 [VPC下弹性IP的应用场景](#) 所示：

图 50: VPC下弹性IP的应用场景



注意事项

使用弹性IP时，需注意：

- 一个实例接口在同一时间只能绑定一个弹性IP。
- 绑定和解绑弹性IP实时生效。
- 绑定和解绑弹性IP不影响实例的运行。

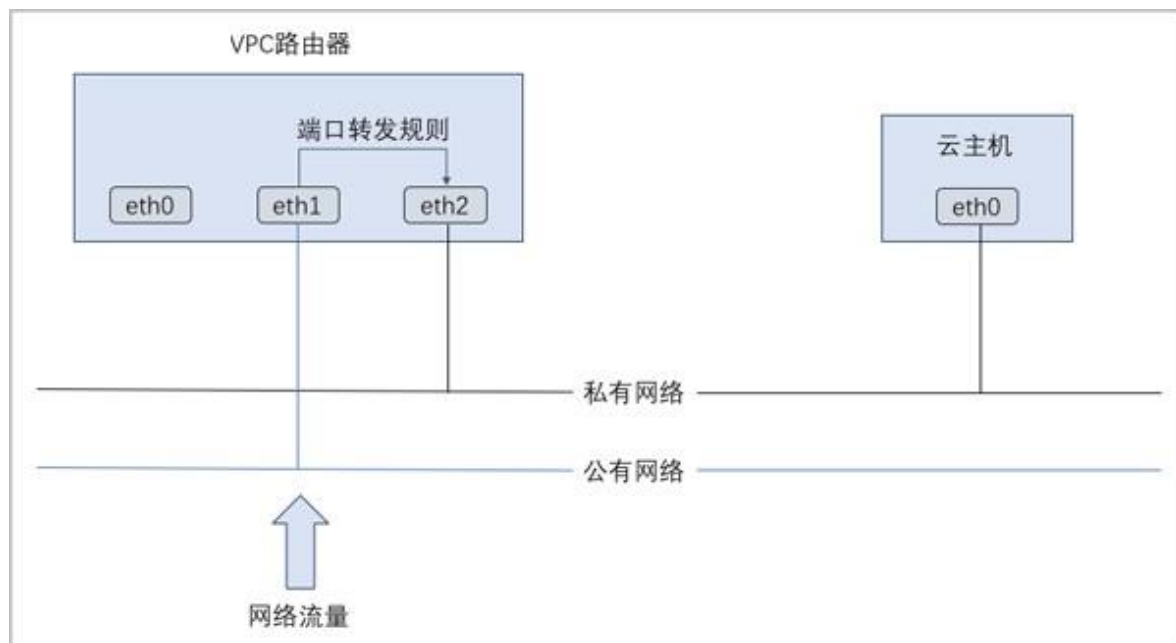
12.4.4 端口转发

端口转发：基于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VPC路由器提供。

端口转发规则创建于VPC路由器公有网络和云主机私有网络之间，如图 51: 端口转发所示：

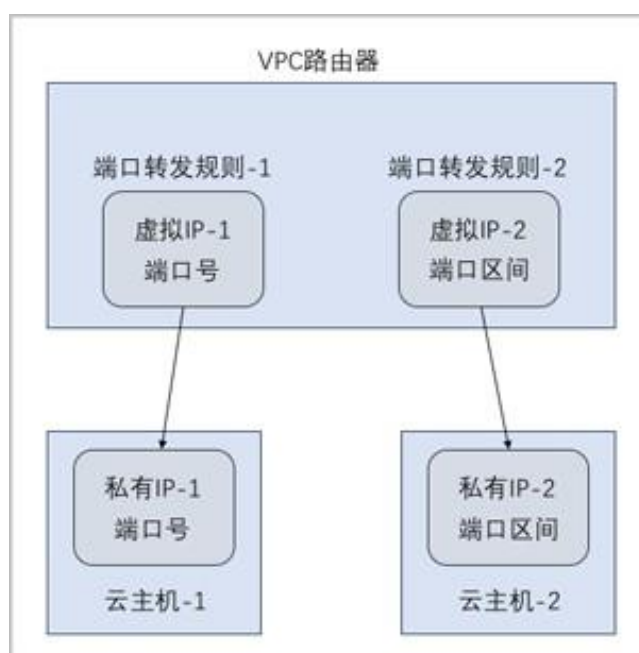
图 51: 端口转发



- 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 52: 虚拟IP-端口转发所示:

图 52: 虚拟IP-端口转发



在Cloud主菜单，点击**资源中心 > 网络服务 > 基础网络服务 > 端口转发**，进入**端口转发**界面。

端口转发规则支持以下操作：

操作	描述
创建端口转发规则	创建一个端口转发规则。
编辑端口转发规则	修改端口转发规则的名称与简介。
绑定云主机网卡	将端口转发规则绑定到云主机网卡。
解绑云主机网卡	将端口转发规则与云主机网卡解绑。
删除端口转发规则	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。

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。

12.4.5 负载均衡

负载均衡：将虚拟IP的访问流量分发到后端服务器上，自动检测并隔离不可用的后端服务器，从而提高业务的服务能力和可用性。

云平台支持两种类型的负载均衡服务：

- 性能共享型：通过VPC路由器提供负载均衡服务，访问流量经由VPC路由器分发给后端服务器。当VPC路由器上承载多业务运行，负载均衡服务需与其它业务共享VPC路由器性能。
- 高性能实例型：通过负载均衡实例提供负载均衡服务，访问流量经由负载均衡实例分发给后端服务器。负载均衡实例是一个定制的云主机，负载均衡服务独享该实例性能。

负载均衡相关定义

- 前端网络：负载均衡的前端网络，负载均衡将来自该网络的客户端请求按照指定策略分发给后端服务器。
 - 性能共享型负载均衡：前端网络支持公有网络、VPC网络两种类型。
 - 高性能实例型负载均衡：前端网络支持公有网络、扁平网络、VPC网络三种类型。
- 后端网络：负载均衡的后端网络，负责处理负载均衡分发前端请求的后端服务器所在的网络。
 - 性能共享型负载均衡：
 - 若前端网络为公有网络，后端网络可为挂载该公有网络的VPC路由器下的所有VPC网络。
 - 若前端网络为VPC网络，后端网络可为挂载该VPC网络的VPC路由器下的所有VPC网络。
 - 高性能实例型负载均衡：
 - 若前端网络为公有网络，后端网络可为扁平网络，或挂载该公有网络的VPC路由器下的所有VPC网络。
 - 若前端网络为扁平网络，后端网络需为同一扁平网络。
 - 若前端网络为VPC网络，后端网络需为同一VPC网络。
- 负载均衡实例：一个定制的云主机，专用于提供负载均衡服务。
- 高性能实例型负载均衡镜像：封装了高性能实例型负载均衡服务，只能用于创建负载均衡实例，不能直接用于创建业务云主机。
 - 该镜像是官方定制封装的镜像，可直接从官网获取，并添加至云平台。
- 负载均衡实例规格：定义负载均衡实例使用的CPU、内存、镜像、管理网络配置，用于创建负载均衡实例，为公有网络/扁平网路/VPC网络提供负载均衡服务。
- 监听器：负责监听负载均衡的前端请求，按照指定策略分发给后端服务器，且监听器会对后端服务器进行健康检查。
 - 监听器支持TCP/HTTP/HTTPS/UDP四种协议。
 - 一个负载均衡可绑定多个监听器，一个监听器仅可绑定到一个负载均衡。
 - 若监听器采用加权轮询的负载均衡算法，可在后端服务器组详情页中，对每台后端服务器单独设置权重值。
- 证书：当负载均衡监听器使用HTTPS协议，需绑定证书使用。支持上传证书和证书链。
- 后端服务器组：一组负责处理负载均衡分发的前端请求的后端服务器。负载均衡实例进行流量分发时，流量分配策略以后端服务器组为单位生效。

- 一个负载均衡可绑定多个后端服务器组，一个后端服务器组仅可绑定到一个负载均衡。
- 一个后端服务器组可绑定同一负载均衡下的多个监听器。
- 创建负载均衡会自动创建一个默认为空的后端服务器组。
- 后端服务器：负责处理负载均衡分发的前端请求的服务器。支持添加云主机或云平台之外的服务器作为后端服务器。

负载均衡使用流程

性能共享型负载均衡的基本使用流程：

1. 创建性能共享型负载均衡。
2. 创建并加载监听器，指定公网端口到云主机端口的对应关系，设置规则及算法等。
3. 选择指定三层网络的云主机网卡绑定到监听器，使负载均衡生效。

高性能实例型负载均衡的基本使用流程：


1. 创建高性能实例型负载均衡实例。
2. 创建并加载监听器，指定公网端口到后端服务器端口的对应关系，设置规则及算法等。
3. 创建并加载后端服务器组，使负载均衡生效。

负载均衡支持以下操作：

操作	描述
创建负载均衡	创建一个负载均衡。
编辑负载均衡	修改负载均衡的名称与简介。
删除负载均衡	删除负载均衡，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。

证书支持以下操作：

操作	描述
创建证书	<p>创建一个新的证书。</p> <p>注：</p> <ul style="list-style-type: none"> • 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。 • 只支持PEM格式，请确保填写的证书正文、私有密钥和证书链符合格式要求。

操作	描述
编辑	修改证书的名称和简介。
删除证书	<p>删除已添加的证书。</p> <p> 注: 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。</p>

负载均衡实例规格支持以下操作:

操作	描述
创建负载均衡实例规格	创建一个新的负载均衡实例规格。
编辑	修改负载均衡实例规格的名称和简介。
设置共享	<p>设置该资源的共享模式。目前支持以下三种模式:</p> <ul style="list-style-type: none"> 全局共享: 将资源共享给所有的项目和账户使用。 指定共享: 将资源共享给指定的项目和账户使用。 不共享: 将已共享的资源进行召回。召回后, 其他项目和账户将无法使用此资源。 <p>注:</p> <ul style="list-style-type: none"> 将全局共享模式修改为指定共享之后, 资源仅对指定的项目或账户可见。 修改共享模式后, 原项目/账户已使用的资源将继续保留且不受影响, 直到被释放。
删除负载均衡实例规格	删除已创建的负载均衡实例规格。

监听器支持以下操作:

操作	描述
创建监听器	创建一个监听器。
编辑	修改监听器的名称与简介。
绑定证书	当监听协议为HTTPS, 需绑定一个证书或证书链到监听器。当监听协议为TCP/HTTP/UDP, 不支持绑定证书。
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, 不支持解绑证书。
删除监听器	删除监听器, 将自动删除其提供的负载均衡服务。

后端服务器组支持以下操作：

操作	描述
创建后端服务器组	创建一个后端服务器组。
删除后端服务器组	删除已创建的后端服务器组。

注意事项

- 一个负载均衡器加载监听器指定的云主机网卡必须属于同一个路由器。
- 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。
- VPC路由器提供的系统虚拟IP支持用于负载均衡服务。

12.4.6 防火墙

防火墙：负责管控VPC网络的南北向流量，通过配置规则集和规则来管控网络的访问控制策略，可有效保护整个VPC的通信安全以及VPC路由器安全。

VPC路由器的每个网卡流量方向上均可绑定规则和规则集

- 入方向：作用于通过网络进入VPC路由器的流量。
- 出方向：作用于从VPC路由器通过网络向外发出的流量。

防火墙规则集：规则集是规则的集合，包含了一组规则，需要绑定到VPC路由器网卡的某个方向上才能生效。

防火墙规则：

- 防火墙规则支持自定义优先级，数字越小表示优先级越高，支持的优先级范围：1001-2999。
- 防火墙规则支持对数据来源和去向进行限制：
 - 源IP和目的IP支持输入固定IP地址、IP范围或CIDR，支持混合输入。
 - 若输入多个IP地址，且包含一个或多个CIDR格式，则CIDR格式仅支持/24掩码范围，若仅输入一个CIDR则不限制掩码范围。
 - 支持最多添加10条，以英文逗号分隔。

规则模板：将一组规则保存为模板，向防火墙或规则集添加规则时可直接选用该模板。

IP/端口集合：将一组IP或端口进行保存，在向防火墙或规则集添加规则时可直接选用已建好的IP/端口集合。

防火墙与安全组的区别：防火墙管控南北向流量，作用范围是整个VPC，与作用于云主机虚拟网卡、侧重于保护VPC内部东西向通信安全的安全组相辅相成，二者互为补充，具体区别如下：

对比项	安全组	防火墙
作用范围	云主机虚拟网卡	整个VPC网络
部署方式	分布式	集中式
部署位置	云主机	VPC路由器
配置策略	仅支持允许策略	可自定义允许、丢弃或拒绝策略
优先级	按照配置顺序	自定义优先级顺序
规则匹配	源IP、源端口、协议	源IP、源端口、目的IP、目的端口、协议、报文状态

防火墙支持以下操作：

操作	描述
创建防火墙	创建一个新的防火墙。
删除	删除防火墙。

规则集支持以下操作：

操作	描述
创建规则集	创建一个新的规则集。
同步配置	修改规则集中的规则后，需要点击同步配置生效。
添加规则	选择规则集并添加规则。
绑定网络	为规则集绑定网络。
解绑网络	将规则集与网络解绑
删除	删除规则集。

注意事项

防火墙注意事项：

- 一个VPC路由器只能创建一个防火墙。

- 一个网卡包含入（inbond）、出（outbond）两个防护方向，每个防护方向只能设置一个规则集。
- VPC防火墙的防护机制会限制外部通过非EIP方式访问内部云主机，对于使用静态路由、OSPF的用户，若停用优先级9999的规则，则静态路由、OSPF服务将无法使用。若仍需使用静态路由、OSPF服务，请在停用后手动配置公有网络网卡入方向放行规则。

规则集注意事项：

- 一个规则集下最多可以挂载9999个规则。
- 仅支持新建出方向规则集，作用于网卡出方向。
- 规则集的出入方向是针对VPC路由器而言，请谨慎操作。
- 入方向规则集已由系统默认创建，支持在入方向规则集中添加自定义规则，入方向规则集不支持删除操作。
- 同一出方向规则集可以在多个网卡上复用。

规则注意事项：

- 规则隶属于规则集，不能复用在多个规则集上。
- 系统规则是支持系统服务的预置规则，优先级范围：1-1000、4000-9999；自定义规则支持的优先级范围：1001-2999，系统预留优先级范围：3000-3999，数字越小表示优先级越高。
- 不支持添加、修改或删除系统规则操作。

12.4.7 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）。

- **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）。

IPsec隧道支持以下操作：

操作	描述
创建IPsec隧道	创建一个IPsec隧道。
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。

12.4.8 OSPF区域

OSPF协议按照一定标准将一个自治系统划分为不同区域，用于分层管理路由器。

OSPF区域支持以下操作：

操作	描述
创建OSPF区域	创建一个OSPF区域。
删除	将已创建的OSPF区域删除。删除OSPF区域后，对应的路由器将删除OSPF配置和路由信息，这些路由器上的云主机将无法通过OSPF与外部互通，请谨慎操作。

12.4.9 Netflow

通过Netflow对VPC路由器网卡的进出流量进行分析监控，支持两种数据流输出格式：V5、V9。

Netflow支持以下操作：

操作	描述
创建Netflow	创建一个Netflow。
删除	将Netflow删除。

注意事项

- 一个Netflow可以监测多个VPC路由器上多条网络的流量，一个VPC路由器的所有网络只能加载同一个Netflow。
- 需要正确配置收集器的IP和端口，否则可能造成收集数据丢包。
- Netflow可以收集VPC路由器的南北向流量和跨网络的东西向流量，在分布式路由模式下，跨网络的东西向流量可能因为优化而造成采集数据失真。

- Netflow监测VPC高可用组内的路由器时，会持续监测主路由器的网络流量，保证数据完整。
- Netflow监测VPC路由器的网络流量时，会占用VPC路由器的性能，请选择合适的监测方案以降低对VPC路由器性能的影响，具体关联如下：
 - Netflow监测的VPC网络数量越多，对VPC路由器性能影响越大。
 - 流导出间隔越小，对VPC路由器性能影响越大，同时业务网络带宽压力也越大。
 - 用户需使用稳定的网络，使VPC路由器的公网可以正常访问到收集器，以保证Netflow服务正常运行。

12.4.10 端口镜像

将云主机网卡的网络流量复制一份到远端，对端口上的业务报文进行分析，方便对网络数据进行监控管理，在网络故障时可以快速定位故障。

端口镜像支持以下操作：

操作	描述
创建端口镜像	创建一个端口镜像。
启用端口镜像	启用端口镜像。
停用端口镜像	停用端口镜像。
删除	删除端口镜像。

12.4.11 路由表

用户自定义配置路由信息，包括目标网段、下一跳地址、路由优先级。

路由表支持以下操作：

操作	简介
创建路由表	创建一个路由表。
添加路由条目	自定义添加路由条目到路由表。
加载路由设备	支持路由表加载VPC路由器。
卸载路由设备	支持路由表卸载VPC路由器。
删除	删除此路由表。

12.5 资源编排

资源编排：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 53: 资源编排所示：

图 53: 资源编排



功能特点

- 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。
- 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。
- 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。
- 如果不再需要某资源栈，可一键删除该栈及栈内所有资源。

- 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。
- 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。

12.5.1 资源栈

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（以及资源间的依赖关系），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

在Cloud主菜单，点击**资源中心** > **资源编排** > **资源栈**，进入**资源栈**界面。点击**创建资源栈**，弹出**创建资源栈**界面。

创建资源栈

创建资源栈分为以下三步：

1. 资源栈配置。

可参考以下示例输入相应内容：

- **区域**：自动显示当前区域
- **名称**：设置资源栈名称

支持1~128字符，输入内容只能包含中文汉字、英文字母、数字和以下7种英文字符“-”、“_”、“.”、“(”、“)”、“:”、“+”。

- **简介**：可选项，可留空不填
- **超时设置**：设置创建资源栈的超时时限，超时将失败，默认为60分钟
- **失败回滚**：设置创建失败是否清理已创建的资源，默认开启
- **创建方式**：选择创建资源栈方式，本章节以创建LNMP为例。支持以下三种方式：
 - **资源栈模板**：使用系统模板或自定义模板创建资源栈



注：如何创建自定义模板，请参考[资源栈模板](#)章节。

- **上传文件**：使用已定义的UTF8编码格式模板文件创建资源栈



注: 关于模板语法的详细介绍, 请参考[资源栈模板语法](#)章节。

- **自定义文本:** 在文件编辑器中编辑模板创建资源栈



注: 关于模板语法的详细介绍, 请参考[资源栈模板语法](#)章节。

如图 54: 基础配置所示:

图 54: 基础配置

2. 模板配置。

模板配置项与所选的模板有关, 不同类型的资源栈需要输入的参数不同, 本章节以创建LNMP为例。

可参考以下示例输入相应内容:

- **镜像:** 选择创建云主机的镜像
- **计算规格:** 选择创建云主机的计算规格
- **网络:** 选择创建云主机的网络



注:

- 该功能通过调用DecodeStackTemplateAPI实现。
- 开始创建资源栈前, 可点击[预览查看](#)将要创建的资源列表。

- 创建资源栈需要一定时长，请等待创建完成。

如图 55: 模板配置所示:

图 55: 模板配置

3. 确认信息。

查看将要创建的资源栈，支持跳转修改。

如图 56: 确认信息所示:

图 56: 确认信息

查看资源栈信息

在**资源栈**界面，选择某一资源栈，查看其详情页，可查看当前创建的资源栈状态和信息，包括：总览、资源、事件、审计。

- 总览：显示资源栈当前状态、所有者、UUID、模板内容等信息，其中模板内容支持修改
- 资源：显示资源栈所包括的全部资源信息
- 事件：显示资源栈生命周期中发生的每一个事件
- 审计：查看此资源栈的相关操作

删除资源栈

如果不再使用某一资源栈，可将该资源栈删除。



注：

- 删除资源栈默认会删除栈内编排创建的所有资源，包括云主机或云盘。
- 若资源栈所对应的模板事先已设置DeletionPolicy为Retain，栈内编排创建的所有资源将会被保留，详情可参考[资源\(Resources\)](#)章节。

12.5.2 资源栈模板

资源栈模板：一个UTF8编码格式的文件，基于模板可快速创建资源栈，用户在模板中定义所需的云资源、资源间的依赖关系、资源配置等，资源编排将解析模板，自动完成所有资源的创建和配置。

资源栈模板支持以下操作：

- 创建资源栈模板
- 查看模板信息
- 启用模板
- 停用模板
- 从模板创建资源栈
- 修改模板
- 删除模板

创建资源栈模板

在Cloud主菜单，点击**资源中心 > 资源编排 > 资源栈模板**，进入**资源栈模板**界面。点击**创建资源栈模板**，弹出**创建资源栈模板**界面。

可参考以下示例输入相应内容：

- **名称：**设置资源栈模板名称

支持1~128字符，输入内容只能包含中文汉字、英文字母、数字和以下7种英文字符“-”、“_”、“.”、“(”、“)”、“:”、“+”。

- **简介：**可选项，可留空不填

- **创建方式：**选择创建资源栈方式。支持以下两种方式：

- **自定义文本：**在文件编辑器中编辑模板创建资源栈



注：关于模板语法的详细介绍，请参考[资源栈模板语法](#)章节。

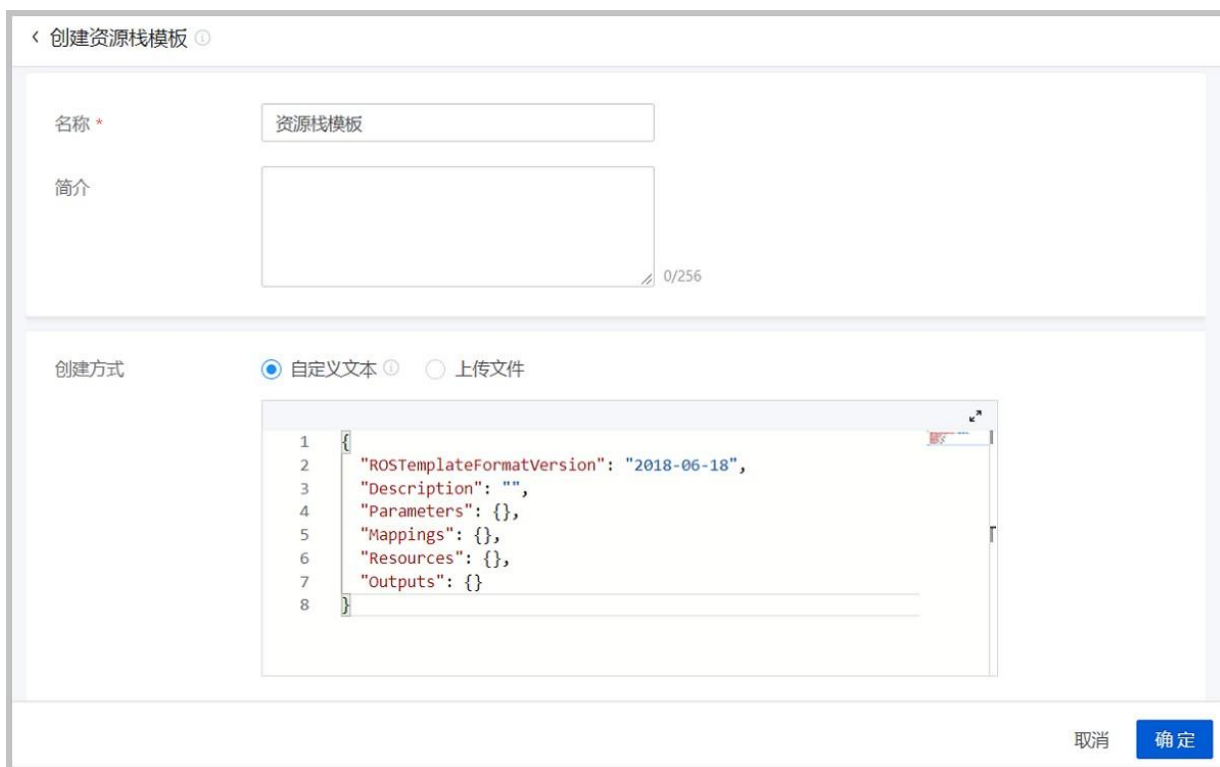
- **上传文件：**使用已定义的UTF8编码格式模板文件创建资源栈



注：关于模板语法的详细介绍，请参考[资源栈模板语法](#)章节。

如图 57: 创建资源栈模板所示：

图 57: 创建资源栈模板



查看模板信息

在**资源栈模板**界面，选择某一模板，展开其详情页，可查看当前创建的模板状态和信息，包括：基本属性、资源栈模板内容、审计。

- 基本信息：显示模板当前状态、名称、简介、模板UUID、MD5码等信息，其中名称和简介支持修改
- 资源栈模板内容：显示模板具体内容，关于模板语法的详细介绍，请参考[资源栈模板语法](#)章节
- 审计：查看此模板的相关操作

启用/停用模板

- 启用模板：将已停用的模板启用
- 停用模板：将模板停用，停用的模板不能创建资源栈

修改模板

支持在文件编辑器中修改模板。

从模板创建资源栈

在[资源栈模板](#)界面，选择需生成的资源栈模板，点击**更多操作 > 生成资源栈**，弹出**创建资源栈**界面。可参考[资源栈](#)章节填写参数。

删除模板

如果不再使用某一模板，可将该模板删除。

约束条件

- 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。

12.5.3 资源栈示例模板

资源栈模板支持以下操作：

- 查看示例模板信息
- 使用示例模板创建资源栈

查看示例模板信息

在Cloud主菜单，点击**资源中心 > 资源编排 > 资源栈模板**，进入[资源栈模板](#)界面。点击**创建资源栈模板**，弹出**创建资源栈模板**界面，选择某一示例模板，进入其详情页，可查看模板状态和信息，包括：总览、审计。

- 总览：显示示例模板的启用状态、UUID、MD5码、模板内容等信息
- 审计：查看此模板的相关操作

使用示例模板生成资源栈

使用示例模板生成资源栈分为以下三步：

1. 资源栈配置。

可参考以下示例输入相应内容：

- **区域：**自动显示当前区域
- **名称：**设置资源栈名称
- **简介：**可选项，可留空不填
- **超时设置：**设置创建资源栈的超时时限，超时将失败，默认为60分钟
- **失败回滚：**设置创建失败是否清理已创建的资源，默认开启

如图 58: 资源栈配置所示：

图 58: 资源栈配置

2. 模板配置。

模板配置项与所选的模板有关，不同类型的资源栈需要输入的参数不同，本章节以ZStack .System.v4.EIP模板为例。

可参考以下示例输入相应内容：

- **计算规格：**选择创建云主机的计算规格
- **镜像：**选择创建云主机的计算镜像

- **私有网络**：选择创建云主机的私有网络
- **公有网络**：选择创建弹性IP的公有网络

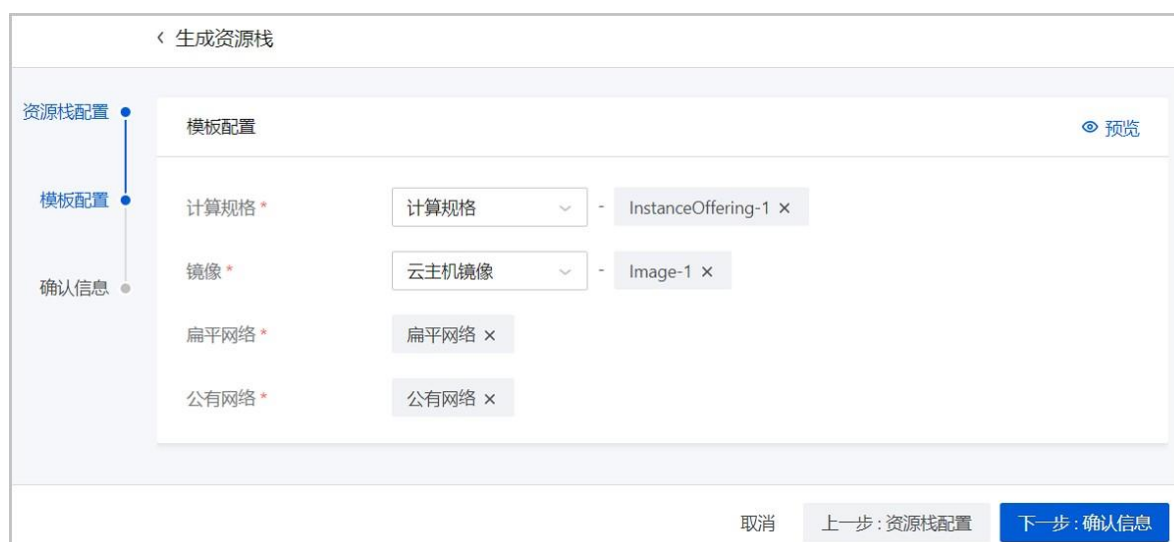


注：

- 该功能通过调用DecodeStackTemplateAPI实现。
- 开始创建资源栈前，可点击**预览**查看将要创建的资源列表。
- 创建资源栈需要一定时长，请等待创建完成。

如图 59: 模板配置所示：

图 59: 模板配置



3. 确认信息。

查看将要创建的资源栈，支持跳转修改。

如图 60: 确认信息所示：

图 60: 确认信息

生成资源栈

资源栈配置
模板配置
确认信息

资源栈配置
区域: ZONE-1
名称: ZStack.System.v4.EIP
超时设置: 60
失败回滚: 开启
创建方式: 资源栈模板
模板名称: ZStack.System.v4.EIP

模板配置
计算规格: InstanceOffering-1
镜像: Image-1
扁平网络: 扁平网络
公有网络: 公有网络

取消
上一步: 模板配置
确定

注意事项

示例模板不允许修改模板内容。

12.5.4 可视化编排

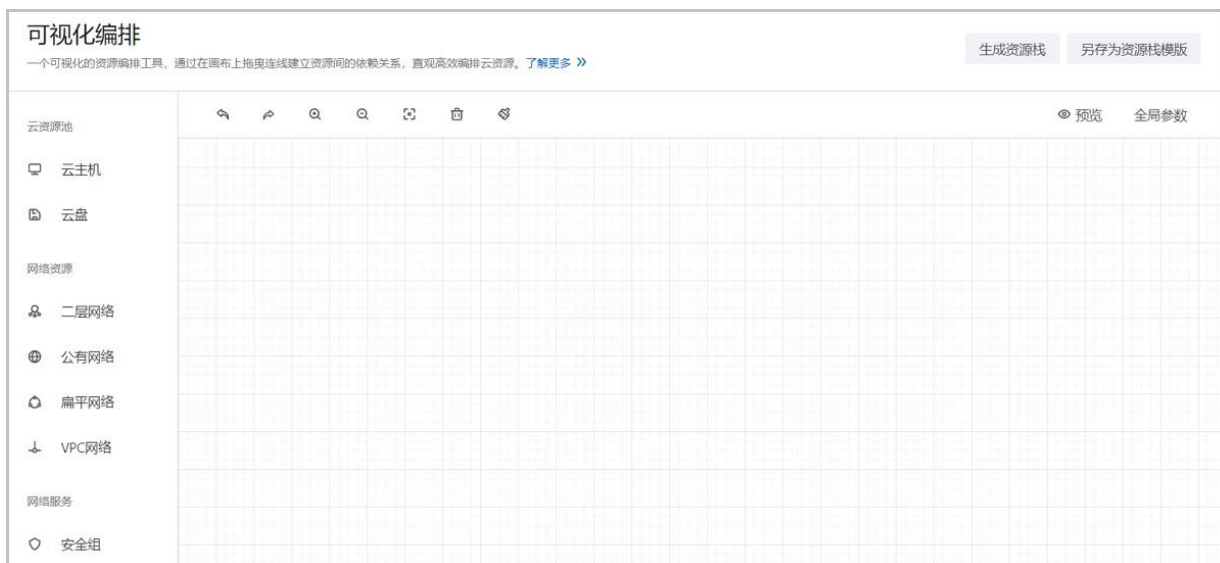
使用可视化编排，可以更直观高效地创建资源栈模板以及显示资源栈结构。打开可视化编排，通过拖曳资源到画布中适当位置，连线创建资源间的依赖关系，并输入需要的参数，即可快速创建资源栈模板，高效编排云资源。

可视化编排界面

在Cloud主菜单，点击**资源中心 > 资源编排 > 可视化编排**，进入**可视化编排**界面。

如图 61: 可视化编排所示:

图 61: 可视化编排



可视化编排界面分为三个部分：

- 顶部菜单：可视化资源编辑器的功能菜单。包括：预览模板、生成资源栈、另存为资源栈模板。
- 左侧菜单：可视化资源编辑器支持的资源列表。可通过拖拽连线直观呈现云资源间的关系，高效编排云资源。目前支持以下资源：
 - 云资源池：云主机、云盘
 - 网络资源：二层网络、公有网络、扁平网络、VPC网络
 - 网络服务：安全组、弹性IP、端口转发、负载均衡、监听器
 - 网络设备：VPC路由器
- 中间部分：可视化资源编辑器的画布，在此进行可视化资源编排。
 - 支持撤销、重做、放大、缩小、适应画布、删除、清除、预览、全局参数操作。
 - 当画布中资源布局足够多时，可通过拖动缩略框调整画布位置，也可通过滚动鼠标放大缩小画布。

可视化编排

可视化编排分为三个步骤：拖拽资源到画布、编辑资源属性、资源连线

1. 拖拽资源到画布。

以创建扁平网络为例，从左侧资源列表拖拽云主机、扁平网络、二层网络到画布。

如图 62: 拖拽资源所示：

图 62: 拖拽资源



2. 编辑资源属性。

资源拖拽至画布后，点击资源图标，可进行属性编辑。

如图 63: 编辑属性所示：

图 63: 编辑属性



3. 资源连线。

每个资源属性编辑完成后，从连接点通过单击+的方式对资源进行连线。

如图 64: 资源连线所示：

图 64: 资源连线



可视化编排操作

可视化资源编辑器顶部的功能菜单，可对已编辑好的资源进行以下操作。包括：生成资源栈、另存为资源栈模板、预览模板、设置全局参数。

- **生成资源栈：**

点击**生成资源栈**按钮，将跳转到**生成资源栈**界面，输入资源栈名称，点击**下一步 > 确定**按钮，可将编辑好的图形化资源栈模板生成资源栈。

如图 65: 生成资源栈所示：

图 65: 生成资源栈

生成资源栈

区域

ZONE-1

名称 * ①

资源栈-扁平网络

简介

超时设置 * ①

60 分

失败回滚

☒

创建方式 *

☐ 资源栈模板
 ☐ 上传文件
 ☒ 自定义文本

```

1 {
2   "ZstackTemplateFormatVersion": "2018-06-18",
3   "Description": "",
4   "Resources": {
5     "vm-88481a69-d383-4d8e-a769-2d64007c41c4": {
6       "Type": "Zstack::Resource::VmInstance",
7       "Properties": {
8         "dataDiskOfferingUuids": [],
9         "systemTags": [],
10        "l3NetworkUuids": [
11          {
12            "Fn::GetAtt": [
13              "flat.network-f1bd7555-a109-4ae7-b885-f2d6e9ea7",
14              "uuid"
15            ]
16          }
17        ]
18      }
19    }
20  }
21 }
```

取消

下一步: 模板配置

• 另存为资源栈模板:

点击**另存为资源栈模板**按钮，将跳转到**创建资源栈模板**界面，输入资源栈模板名称，点击**确定**按钮，可将编辑好的图形化资源栈另存为资源栈模板。

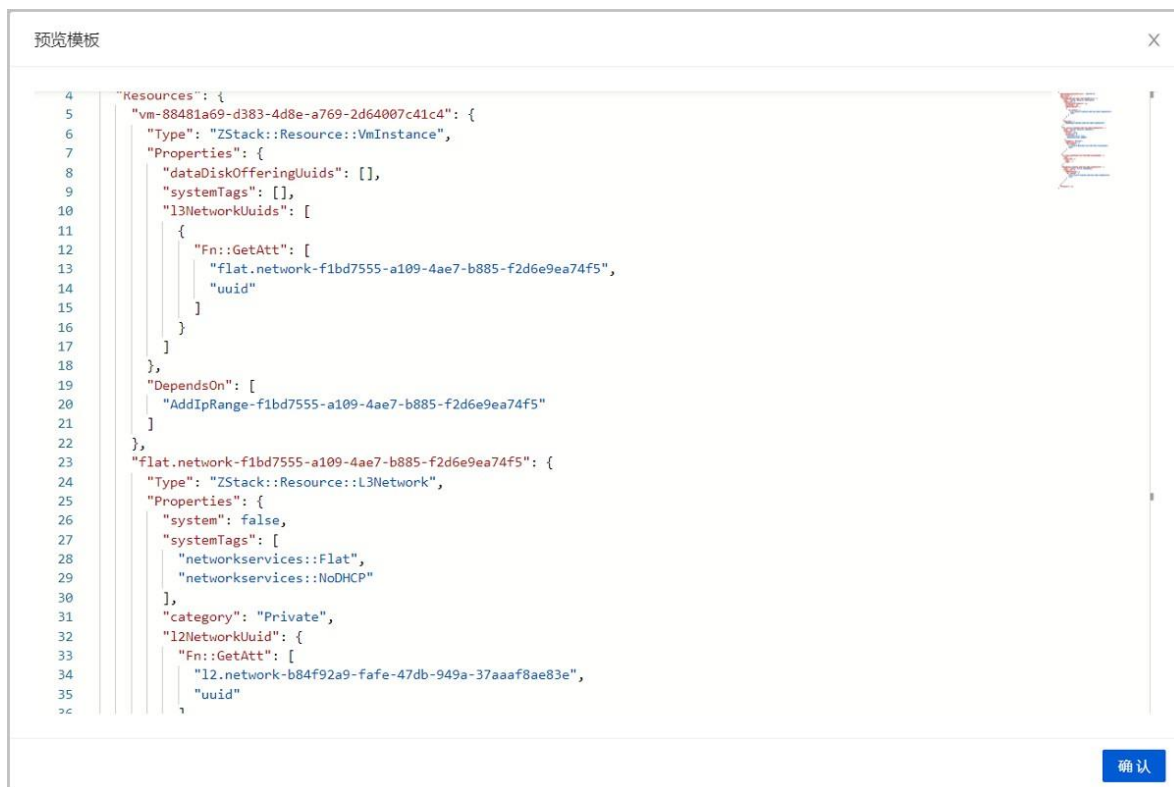
如图 66: 另存为资源栈模板所示:

图 66: 另存为资源栈模板

- **预览模板:**

如图 67: 预览模板所示:

图 67: 预览模板



12.6 裸金属管理

Cloud提供裸金属管理服务，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，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。通过预配置模板，可实现无人值守批量安装裸金属主机操作系统，支持为裸金属主机配置业务网络，并对裸金属主机进行全生命周期管理。



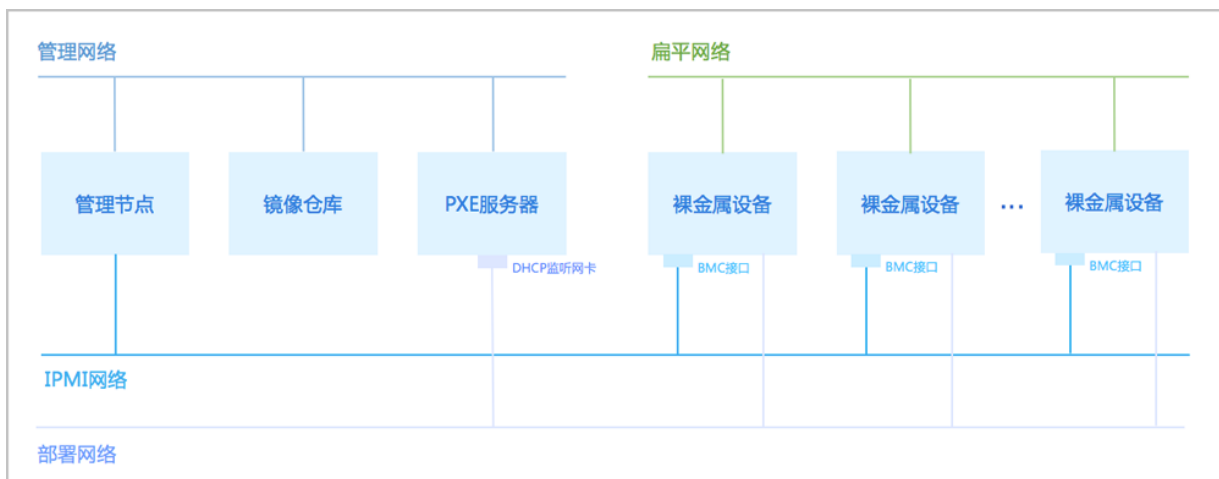
注：裸金属管理服务以单独的功能模块形式提供，需提前购买裸金属管理模块许可证（Plus License），且需在购买企业版云平台许可证基础上使用，不可单独使用。

功能原理

裸金属管理服务的基本原理是：部署服务器提供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，裸金属设备从部署服务器中下载相关软件包，用于裸金属主机的系统安装。

如图 68: 裸金属管理网络拓扑所示：

图 68: 裸金属管理网络拓扑



裸金属管理相关定义

- 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。
- 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部署服务器，避免与其他服务相互干扰，同时提高部署效率。
 - 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Cloud定制版ISO（推荐c76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。

- 裸金属设备：可用于创建裸金属主机，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。
- 预配置模板：可用于快速生成预配置文件，实现无人值守批量安装裸金属主机操作系统。
 - 需提前在云平台中准备好预配置模板。
 - 预配置模板包括以下两种类型：
 - 系统模板：由云平台默认提供，包含基础的系统变量，适用于简单的无人值守部署场景。
 - 自定义模板：支持上传自定义模板文件，采用UTF8编码格式，除了包含基础的系统变量，可按需自定义变量，适用于复杂的无人值守部署场景。
- 裸金属主机：裸金属设备的云实例。裸金属设备添加完成后可用于创建裸金属主机。
 - 通过预配置模板，可快速生成预配置文件，实现无人值守批量安装裸金属主机操作系统。
 - 支持自定义安装操作系统，目前支持的操作系统版本包括：本云平台定制版操作系统、以及主流的Linux发行版操作系统（RHEL/CentOS系列、Debian/Ubuntu系列、SUSE/openSUSE系列等），要求为ISO格式，且为非Live CD。
 - 支持为裸金属主机配置业务网络，目前支持扁平网络场景，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。需提前将裸金属设备所在的裸金属集群挂载相应的二层网络。

功能特点

- 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。
- 推荐独立部署部署服务器，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，彻底避免DHCP冲突，由于每个裸金属集群均可挂载独立的部署服务器，避免单点故障，大幅提升部署效率。
- 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。
- 通过预配置模板，可快速生成预配置文件，实现无人值守批量安装裸金属主机操作系统。

- 支持自定义安装操作系统，目前支持的操作系统版本包括：本云平台定制版操作系统、以及主流的Linux发行版操作系统（RHEL/CentOS系列、Debian/Ubuntu系列、SUSE/openSUSE系列等）。
- 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。

应用场景

- 高安全严监管场景：

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，进一步保障关键核心业务系统和数据的可靠性及安全合规性。

。

- 高性能计算场景：

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，适用于高性能要求、高吞吐量、按照访问需求获取的对计算性能有较高要求的业务场景。虚拟化带来的性能损耗和超线程对业务性能有一定影响，部署一定规模的裸金属集群可以满足高性能计算的要求。

- 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云主机上，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。

12.6.1 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：

操作	描述
创建裸金属集群	创建一个新的裸金属集群。
编辑裸金属集群	编辑裸金属集群的名称、简介信息。
启用裸金属集群	启用处于停用状态的裸金属集群。
停用裸金属集群	停用选中的裸金属集群。  注: 停用裸金属集群会停用该集群内所有的裸金属设备, 请谨慎操作。
加载二层网络	加载二层网络到裸金属集群。  注: 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。
卸载二层网络	将二层网络从裸金属集群卸载。
加载部署服务器	加载部署服务器到裸金属集群。  注: 一个裸金属集群只允许加载一个部署服务器, 一个部署服务器可同时加载到多个裸金属集群。
卸载部署服务器	将部署服务器从裸金属集群卸载。  注: 卸载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。
删除裸金属集群	删除选中的裸金属集群。  注: 删除裸金属集群会删除该集群内所有的裸金属设备和裸金属主机, 请谨慎操作。

注意事项

- 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。
- 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。
- 停用裸金属集群会停用该集群内所有的裸金属设备, 请谨慎操作。
- 卸载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。
- 删除裸金属集群会删除该集群内所有的裸金属设备和裸金属主机, 请谨慎操作。


12.6.2 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Cloud定制版ISO（推荐c76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：

操作	描述
创建部署服务器	创建一个新的部署服务器。
编辑部署服务器	编辑部署服务器的名称、简介信息。
启用部署服务器	启用处于停用状态的部署服务器。
停用部署服务器	停用选中的部署服务器。 注： 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。
删除部署服务器	删除选中的部署服务器。 注： 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。
加载裸金属集群	加载裸金属集群到部署服务器。 注： 一个裸金属集群只允许加载一个部署服务器，一个部署服务器可同时加载到多个裸金属集群。
卸载裸金属集群	将裸金属集群从部署服务器卸载。

操作	描述
	 注: 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。
重连部署服务器	重连选中的部署服务器。

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。





12.6.3 裸金属设备

裸金属设备：可用于创建裸金属主机，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：



操作	描述
添加裸金属设备	添加一个新的裸金属设备。
编辑裸金属设备	编辑裸金属设备的名称、简介信息。
启用裸金属设备	启用已停用的裸金属设备。

操作	描述
停用裸金属设备	<p>停用选中的裸金属设备。</p> <p> 注： 停用裸金属设备将不能用于创建裸金属主机。</p>
裸金属设备开机	通过IPMI启动裸金属设备。
裸金属设备关机	通过IPMI对裸金属设备进行shutdown关机操作。
重启裸金属设备	重启选中的裸金属设备。
获取硬件信息	<p>手动获取裸金属设备的硬件信息。</p> <p> 注： 裸金属设备会先重启，再尝试获取硬件信息，需要一段时间，请耐心等待。</p>
打开控制台	<p>打开控制台，可直接跳转至该裸金属设备的IPMI管理界面（登录界面），输入已配置好的IPMI用户名和IPMI密码，即可登录。</p> <p> 注： 不同厂商服务器的IPMI登录界面风格不同。</p>
删除裸金属设备	<p>删除选中的裸金属设备。</p> <p> 注： 删除裸金属设备将同时删除使用裸金属设备创建的裸金属主机。</p>

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	<p>裸金属设备未能获取硬件信息。</p> <p>注：</p> <ul style="list-style-type: none"> 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。 <p></p>
PXE启动中	部署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。


部署状态	备注
	<p>注:</p> <p>请检查以下事项，是否满足要求：</p> <ul style="list-style-type: none"> • 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。 <p> 注:</p> <ul style="list-style-type: none"> • 对于部分机型，还需确保该PXE网卡为首张启动网卡，或确保（启动顺序）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。 <p></p>
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
<ul style="list-style-type: none"> • 启用 • 停用 	<ul style="list-style-type: none"> • 已开机 • 重启中 • 已关机

12.6.4 预配置模板



预配置模板：通过预配置模板，可快速生成预配置文件，实现无人值守批量安装裸金属主机操作系统。

- 需提前在云平台中准备好预配置模板。
- 预配置模板包括以下两种类型：
 - 系统模板：由云平台默认提供，包含基础的系统变量，适用于简单的无人值守部署场景。
 - 自定义模板：支持上传自定义模板文件，采用UTF8编码格式，除了包含基础的系统变量，可按需自定义变量，适用于复杂的无人值守部署场景。

系统模板支持以下操作：

操作	描述
下载系统模板	<p>下载选中的系统模板。</p> <p> 注：系统模板一直处于启用状态，且不允许做任何修改。</p>

自定义模板支持以下操作：

操作	描述
添加自定义模板	添加一个新的自定义模板。
编辑自定义模板	编辑自定义模板的名称、简介信息。
启用自定义模板	启用处于停用状态的自定义模板。
停用自定义模板	<p>停用选中的自定义模板。</p> <p> 注：停用自定义模板将不能用于无人值守批量安装裸金属主机操作系统。</p>
删除自定义模板	删除选中的自定义模板。
下载自定义模板	<p>下载选中的自定义模板。</p> <p> 注：支持将自定义模板下载到本地进行修改。</p>

注意事项

- 使用系统模板需要注意以下情况：
 - 系统模板一直处于启用状态，且不允许任何修改。
 - 系统模板包含基础的系统变量，适用于简单的无人值守部署场景。
 - 系统变量举例（要求全部大写，连接符使用下划线）：

```

REPO_URL
# 使用所选ISO镜像创建的安裝源地址
# 可注释，并手动指定--url指向其它源

USERNAME
# 系统用户名
# 操作系统为RHEL/CentOS系列、或SUSE/openSUSE系列，系统默认用户名为root，仅需指定密码
# 操作系统为Debian/Ubuntu系列，需自定义用户名和密码

PASSWORD
  
```

```
# 与系统用户名相应的密码
NETWORK_CFGS
# 用户在UI上输入的网卡UUID和网络UUID
# 执行分配算法（或用户指定IP）后替换
FORCE_INSTALL
# 部署过程中是否自动覆盖磁盘原始数据
PRE_SCRIPTS
# 部署前执行脚本
POST_SCRIPTS
# 部署后执行脚本
```

- 不同类型的模板，遵循不同的语法规则：
 - 对于kickstart类型的模板，可查看[Red Hat官网文档](#)了解kickstart语法规则；
 - 对于preseed类型的模板，可查看[Ubuntu官网文档](#)了解preseed语法规则；
 - 对于autoyast类型的模板，可查看[SUSE官网文档](#)了解autoyast语法规则。
- 使用自定义模板需要注意以下情况：
 - 支持主流的Linux发行版操作系统：RHEL/CentOS系列、Debian/Ubuntu系列、SUSE/openSUSE系列；
 - 模板类型必须与所选操作系统匹配，否则无法成功添加预配置模板；
 - 模板类型与操作系统匹配建议如下：
 - 若选择Cloud定制版操作系统，建议选择kickstart模板类型；
 - 若选择RHEL/CentOS系列操作系统，建议选择kickstart模板类型；
 - 若选择Debian/Ubuntu系列操作系统，建议选择preseed模板类型；
 - 若选择SUSE/openSUSE系列操作系统，建议选择autoyast模板类型。
 - 自定义模板除了包含基础的系统变量，可按需自定义变量，适用于复杂的无人值守部署场景。
 - 系统变量举例（要求全部大写，连接符使用下划线）：

```
REPO_URL
# 使用所选ISO镜像创建的安裝源地址
# 可注释，并手动指定--url指向其它源
USERNAME
# 系统用户名
# 操作系统为RHEL/CentOS系列、或SUSE/openSUSE系列，系统默认用户名为root，仅需指定密码
# 操作系统为Debian/Ubuntu系列，需自定义用户名和密码
PASSWORD
```

```
# 与系统用户名相应的密码
NETWORK_CFGS
# 用户在UI上输入的网卡UUID和网络UUID
# 执行分配算法（或用户指定IP）后替换
FORCE_INSTALL
# 部署过程中是否自动覆盖磁盘原始数据
PRE_SCRIPTS
# 部署前执行脚本
POST_SCRIPTS
# 部署后执行脚本
```

- 自定义变量举例（要求全部小写，连接符使用下划线）：

```
hostname
# 物理机名称

keyboard
# 键盘

timezone
# 时区
```

- 不同类型的模板，遵循不同的语法规则：

- 对于kickstart类型的模板，可查看[Red Hat官网文档](#)了解kickstart语法规则；
- 对于preseed类型的模板，可查看[Ubuntu官网文档](#)了解preseed语法规则；
- 对于autoyast类型的模板，可查看[SUSE官网文档](#)了解autoyast语法规则。



- 停用的自定义模板不能用于无人值守批量安装裸金属主机操作系统。



12.6.5 裸金属主机

裸金属主机：裸金属设备的云实例。裸金属设备添加完成后可用于创建裸金属主机。

- 通过预配置模板，可快速生成预配置文件，实现无人值守批量安装裸金属主机操作系统。
- 支持自定义安装操作系统，目前支持的操作系统版本包括：本云平台定制版操作系统、以及主流的Linux发行版操作系统（RHEL/CentOS系列、Debian/Ubuntu系列、SUSE/openSUSE系列等），要求为ISO格式，且为非Live CD。
- 支持为裸金属主机配置业务网络，目前支持扁平网络场景，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。需提前将裸金属设备所在的裸金属集群挂载相应的二层网络。

裸金属主机支持以下操作：

操作	描述
创建裸金属主机	创建一个新的裸金属主机。
编辑裸金属主机	编辑裸金属主机的名称、简介信息。
启用裸金属主机	启动选中的裸金属主机。
停止裸金属主机	停止选中的裸金属主机。
重启裸金属主机	重启选中的裸金属主机。
绑定标签	<p>将标签绑定到裸金属主机。</p> <p> 注:</p> <ul style="list-style-type: none"> 裸金属主机仅支持绑定管理员标签。 单个资源最多支持绑定50个标签，反之，单个标签支持绑定的资源数量无限制。 标签-资源支持多对多绑定关系。 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。 管理员支持解绑/删除租户标签。 资源标签按照绑定时间或标签名称（符号>数字>中文>英文）进行排序。设置方法： 进入设置 > 平台设置 > 全局设置 > 基础设置 > 平台运维 > 标签，设置标签排序方式，默认按标签名称排序。
解绑标签	<p>将标签从裸金属主机解绑。</p> <p> 注:</p> <ul style="list-style-type: none"> 管理员标签由管理员创建，归管理员所有，租户标签由租户创建，归租户所有。 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。 管理员支持解绑/删除租户标签。 项目内的标签归属于项目所有，项目内所有人（项目负责人/项目管理员/项目成员）均可操作。 标签暂不支持更改所有者操作。 资源更改所有者，其上所有租户标签将会解绑，管理员标签不受影响。 云平台无缝升级后，已有旧标签将自动更新，以最新方式展示标签。若有异常，请刷新浏览器或重新创建标签。

操作	描述
	<ul style="list-style-type: none"> 支持将单个资源上的批量标签解绑，也支持将单个标签上的批量资源解绑。 租户只能解绑所属租户资源上的标签，管理员可解绑所有资源上的标签。
打开控制台	<p>打开当前裸金属主机的控制台。</p> <ul style="list-style-type: none"> 若部署时间过长，请进入控制台查看安装情况。 部署完成后，可通过控制台对裸金属主机执行各种操作。 <p> 注:</p> <ul style="list-style-type: none"> 确保裸金属主机对应的裸金属设备所在集群已挂载部署服务器，否则无法打开控制台； 若操作系统为Debian/Ubuntu系列，不支持打开控制台，可外接显示器查看安装情况； 若操作系统为SUSE/openSUSE系列，打开控制台会强制要求输入密码，预置控制台密码为：password。
删除裸金属主机	<p>删除选中的裸金属主机。</p> <p> 注:</p> <ul style="list-style-type: none"> 删除裸金属主机支持两种策略：立刻删除、延时删除。默认为延时删除。 <ul style="list-style-type: none"> 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，即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。 用户可自行设置裸金属主机的删除策略。设置方法： 进入设置 > 平台设置 > 全局设置 > 基础设置 > 平台策略 > 删除策略，设置裸金属主机的裸金属主机删除策略即可。 删除裸金属主机将同时关机裸金属设备，可能会影响正常业务运行，请谨慎操作。

注意事项

- 创建裸金属主机：

- 一台裸金属设备只允许创建一台裸金属主机；
- 最大允许一次性批量创建50台裸金属主机；
- 裸金属设备需事先已获取硬件信息，否则备选列表无法看到该裸金属设备；
- 需提前在镜像服务器中准备好镜像，支持ImageStore类型镜像服务器，要求为ISO格式，且为非Live CD；
- 目前支持的操作系统版本包括：
 - 本云平台定制版操作系统；
 - 主流的Linux发行版操作系统：RHEL/CentOS系列、Debian/Ubuntu系列、SUSE/openSUSE系列等。
- 需提前在云平台中准备好预配置模：
 - 所选预配置模板的操作系统必须与所选镜像匹配；
 - 若操作系统为SUSE/openSUSE系列，裸金属主机打开控制台会强制要求输入密码，预置控制台密码为：**password**。
- 操作系统为RHEL/CentOS系列、或SUSE/openSUSE系列，系统默认用户名为root，仅需指定密码；
- 操作系统为Debian/Ubuntu系列，需自定义用户名和密码；
- 裸金属主机需有可用网卡用于配置业务网络；
- 使用相同配置要求裸金属主机之间网卡数量相同、网卡名称相同；
- 目前支持扁平网络场景，且支持VLAN二层隔离；
- 需提前将裸金属设备所在的裸金属集群挂载相应的二层网络；
- 裸金属主机创建后会自动重启，然后基于预配置模板进行无人值守批量安装操作系统；
- 若部署时间过长，请进入控制台查看安装情况；
- 部署完成后，裸金属主机自动重启，就绪状态显示为**已部署**。
- 打开控制台：
 - 确保裸金属主机对应的裸金属设备所在集群已挂载部署服务器，否则无法打开控制台；
 - 若操作系统为Debian/Ubuntu系列，不支持打开控制台，可外接显示器查看安装情况；
 - 若操作系统为SUSE/openSUSE系列，打开控制台会强制要求输入密码，预置控制台密码为：**password**。
- 删除裸金属：
 - 删除裸金属主机支持三种策略：立刻删除，延时删除，永不删除。默认为延时删除。

- 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。
- 用户可自行设置裸金属主机的删除策略，设置方法：
- 进入**设置 > 全局设置 > 高级设置**，设置裸金属主机的**删除策略**即可。
- 恢复/彻底删除裸金属主机：
 - 裸金属主机恢复后回到**可用**页面，且启用状态为**已停止**，可手动重启该裸金属主机；
 - 删除裸金属主机后，其IP地址会返回IP地址池中，恢复裸金属主机，PXE服务器的DHCP服务会为其重新分配IP地址；
 - 彻底删除裸金属主机，该操作不可逆转，请谨慎执行。
 - Cloud支持监控裸金属主机的实时状态。监控方式为内部监控，通过agent从裸金属主机内部获取监控数据，并在UI界面实时展示各种负载的性能指标，包括：CPU、内存、磁盘容量、磁盘IO、网卡。



注：查看裸金属监控数据需确保已预先安装agent。

12.7 弹性裸金属管理

弹性裸金属管理：不仅可为应用提供专属物理服务器，保障核心应用的高性能和稳定性，而且结合云平台中资源的弹性优势，可实现灵活申请，按需使用。弹性裸金属管理融合了物理机和云主机各自的优点，业务应用不仅可以使⽤物理机超强超稳的计算能力，而且可以使⽤云平台内主存储、三层网络等资源。避免虚拟化开销的同时，突破云资源与物理资源的边界，提高云资源的可用性，特别适合部署传统的非虚拟化场景应用。



注：弹性裸金属管理服务以单独的功能模块形式提供，需提前购买弹性裸金属管理模块许可证，且需在购买企业版云平台许可证基础上使用，不可单独使用。

相关定义

- 部署网络：创建弹性裸金属实例时，用于PXE流程及下载镜像的专属网络。
 - 搭建弹性裸金属管理环境前，需提前准备规划部署网络，目前仅支持IPv4类型。
 - 部署网络性能要求较高，推荐至少使用万兆网卡。
 - 部署网络支持设置网关，若部署网络需要连接其他网络时可按需配置；若不需要连接其他网络，可暂时不用配置。
- 弹性裸金属集群：为裸金属节点提供单独的集群管理。
 - 弹性裸金属集群必须加载部署网络，才能为弹性裸金属集群中裸金属节点提供PXE服务。
 - 弹性裸金属集群和部署网络采用一对多关系，即一个弹性裸金属集群只允许加载一个部署网络：一个部署网络支持加载到多个弹性裸金属集群。
 - 弹性裸金属集群支持加载二层网络，为集群中弹性裸金属实例提供大二层业务网络。同一二层网络上的弹性裸金属实例和云主机之间可以互相访问，无需通过网关进行路由。目前支持VLAN和NoVLAN类型的二层网络。
- 网关节点：云平台 and 弹性裸金属实例的流量转发节点。
 - 裸金属集群和网关节点采用一对多关系。即一个弹性裸金属集群支持加载多个网关节点，但一个网关节点只能加载到一个弹性裸金属集群。
 - 通过网关节点接管主存储，并为弹性裸金属实例分配主存储。
 - 提供iPXE服务、DHCP服务等，可通过网关节点为弹性裸金属实例下发配置。
- 裸金属节点：用于创建弹性裸金属实例，通过BMC接口以及IPMI配置进行唯一识别。
 - 要求管理节点连接到IPMI网络，通过IPMI远程控制裸金属节点。
 - 要求裸金属节点配备BMC接口，配置IPMI地址、端口、用户名、密码，并连接至IPMI网络。
 - 裸金属节点和弹性裸金属实例一一对应。即一台裸金属节点只能同时分配给一个弹性裸金属实例使用，一个弹性裸金属实例只能分配到一台弹性裸金属节点。
 - 支持按裸金属节点或按裸金属规格为弹性裸金属实例提供计算资源。
 - 支持关机释放裸金属节点。弹性裸金属实例停止时自动释放弹性裸金属节点，供其他弹性裸金属实例使用，避免资源闲置。
- 弹性裸金属实例：性能媲美物理服务器的云实例，结合云平台中资源的弹性优势，可实现灵活申请，按需使用。
 - 弹性裸金属实例的计算资源由裸金属节点提供，存储资源由云平台中的Shared Block主存储或Ceph主存储提供，PXE流程由部署网络提供，业务网络由云平台中的三层网络提供。

- 推荐使用已安装agent的镜像创建弹性裸金属实例，否则无法执行打开控制台、修改弹性裸金属实例密码、加/卸载云盘、加/卸载网络操作。
- 弹性裸金属实例默认使用BIOS模式为UEFI的镜像创建弹性裸金属实例：若需要使用BIOS模式为Legacy的镜像，请联系官方技术支持获取帮助。
- 支持为弹性裸金属实例配置业务网络，将裸金属节点所属集群加载二层网络，即可实现同一二层网络上的弹性裸金属实例和云主机之间可以互相访问，无需通过网关进行路由。

应用场景

- 高安全严监管场景

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

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业务性能有一定影响，部署一定规模的裸金属集群可以满足高性能计算的要求。

- 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云主机上，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。

注意事项

使用弹性裸金属管理功能需要注意以下情况：

- 准备的服务器至少需要一张PXE启动的网卡做网络管理。且确保使用服务器第一张网卡的第一个网口作为部署网卡。
- 裸金属节点目前支持所有x86 CPU架构服务器、以及鲲鹏等主流国产化ARM服务器。
- 网关节点目前支持所有x86 CPU架构服务器。若存在裸金属节点使用ARM CPU架构，需同时为网关节点添加ARM版本repo源。
- 物理网络环境包括：管理网络、存储网络、部署网络、IPMI网络、业务网络等。其中，部署网络性能要求较高，推荐至少使用万兆网络。
- 确保部署网络内不存在其他DHCP服务，避免DHCP冲突。
- 目前支持的业务网络包括：扁平网络、公有网络、VPC网络。若使用VPC网络作为业务网络，需确保VPC网络对应二层网络所使用的网卡名称与网关节点上的网卡名称匹配。

- 弹性裸金属镜像需安装agent或相关依赖包，否则部分功能无法正常使用。
- 目前支持的主存储包括：Shared Block主存储和企业版Ceph主存储。其中，企业版Ceph主存储要求使用4.2.0.300及以上版本。
- 若使用企业版Ceph主存储，需登录企业版Ceph管理节点，将网关节点添加为网关服务器角色，并确保配置正确。
- 同一弹性裸金属集群加载主存储存在限制，详情请参考[表 11: 主存储与弹性裸金属集群组合关系](#)。

表 11: 主存储与弹性裸金属集群组合关系

主存储搭配方式	弹性裸金属集群组合限制
Ceph	同一弹性裸金属集群，有且只能加载一个Ceph主存储。
Shared Block	同一弹性裸金属集群，支持加载一个或多个Shared Block主存储。
Ceph+Shared Block	同一弹性裸金属集群，支持加载一个Ceph主存储 + 一个或多个Shared Block主存储。

- 弹性裸金属实例支持主流x86操作系统和部分ARM操作系统。如[表 12: 操作系统清单](#)所示：


表 12: 操作系统清单

CPU架构	操作系统类型	操作系统
x86	Windows	<ul style="list-style-type: none"> • Windows 2012 • Windows 2016 • Windows 2019
	Linux	<ul style="list-style-type: none"> • CentOS 7 • CentOS 8 • Ubuntu 18LTS • Ubuntu 20LTS
ARM	Linux	<ul style="list-style-type: none"> • CentOS 7 • 麒麟V10

12.7.1 部署网络

在Cloud主菜单，点击[资源中心](#) > [弹性裸金属管理](#) > [网络资源](#) > [部署网络](#)，进入[部署网络](#)界面。



部署网络支持以下操作：



操作	描述
创建部署网络	创建一个新的部署网络。
编辑部署网络	编辑部署网络的名称、简介信息。
删除部署网络	删除未加载弹性裸金属集群的部署网络。  注： 若部署网络已加载弹性裸金属集群，需为相关弹性裸金属集群更改部署网络才能继续执行此操作。

12.7.2 弹性裸金属集群

在Cloud主菜单，点击**资源中心** > **弹性裸金属管理** > **硬件资源** > **弹性裸金属集群**，进入**弹性裸金属集群**界面。

弹性裸金属集群支持以下操作：

操作	描述
创建弹性裸金属集群	创建一个新的弹性裸金属集群。
编辑弹性裸金属集群	编辑弹性裸金属集群的名称、简介信息。
启用弹性裸金属集群	启用处于停用状态的弹性裸金属集群。启用后该弹性裸金属集群可作为候选被使用。
停用弹性裸金属集群	停用处于启用状态的弹性裸金属集群。停用后该弹性裸金属集群不可继续作为候选被使用。  注： 已经使用该弹性裸金属集群的资源可以正常使用，不受影响。
加载二层网络	将二层网络加载到弹性裸金属集群，为集群内弹性裸金属实例提供业务网络。
更改部署网络	为弹性裸金属集群更改部署网络。 注： 更改部署网络需要注意以下情况： <ul style="list-style-type: none"> 此操作将卸载弹性裸金属实例相关网卡，并使用最新部署网络重新分配网卡。 若使用该部署网络的弹性裸金属实例正在运行，无法更改部署网络。 
加载主存储	将主存储加载到弹性裸金属集群，为集群内弹性裸金属实例提供存储资源。

操作	描述
	 注： 目前支持加载Shared Block类型、Ceph类型的主存储。
删除弹性裸金属集群	删除不需要的弹性裸金属集群。  注： 删除弹性裸金属集群将同时删除其下弹性裸金属节点、网关节点，且停止弹性裸金属实例，影响业务运行，请谨慎操作。

12.7.3 网关节点

在Cloud主菜单，点击**资源中心** > **弹性裸金属管理** > **硬件资源** > **网关节点**，进入**网关节点**界面。






网关节点支持以下操作：

操作	描述
添加网关节点	添加一个新的网关节点。
编辑网关节点	编辑网管节点的名称、简介信息。
启用网关节点	启用处于停用状态的网关节点。启用后该网关节点可作为候选被使用。
停用网关节点	停用处于启用状态的网关节点。停用后该网关节点不可继续作为候选被使用。  注： 已经使用该网关节点的资源可以正常使用，不受影响。
重连网关节点	重新连接网关节点。该操作将获取网关节点最新配置，不影响业务运行。 
修改密码	修改网关节点密码。若网关节点服务器密码变更，需执行该操作更新密码，否则网关节点将失联。
更改弹性裸金属集群	 为网关节点更换弹性裸金属集群。 注： 此操作将停止所选网关节点相关弹性裸金属实例，影响业务正常运行，请谨慎操作。
删除网关节点	删除不需要的网关节点。 注： 删除网关节点将同时停止该网关节点相关弹性裸金属实例，影响业务正常运行，请谨慎操作。

12.7.4 裸金属节点

在Cloud主菜单，点击**资源中心** > **弹性裸金属管理** > **硬件资源** > **裸金属节点**，进入**裸金属节点**界面。





裸金属节点支持以下操作：






操作	描述
添加裸金属节点	添加一个新的裸金属节点。
编辑裸金属节点	编辑裸金属节点的名称、简介信息。
启用裸金属节点	启用处于停用状态的裸金属节点。启用后该裸金属节点可作为候选被使用。
停用裸金属节点	<p>停用处于启用状态的裸金属节点。停用后该裸金属节点不可继续作为候选被使用。</p> <p> 注： 已经使用该裸金属节点的资源可以正常使用，不受影响。</p>
开机裸金属节点	将关机状态的裸金属节点开机。
关机裸金属节点	<p>将开机状态的裸金属节点关机。</p> <p> 注： 关机裸金属节点将同时停止相关弹性裸金属实例，可能影响业务正常运行，请谨慎操作。</p>
重启裸金属节点	<p>重新启动开机状态的裸金属节点。</p> <p> 注： 此操作将停止所选裸金属节点相关弹性裸金属实例，影响业务正常运行，请谨慎操作。</p>
获取硬件信息	<p>重启裸金属节点并获取硬件相关信息。</p> <p> 注： 此操作将重启裸金属节点，同时停止相关弹性裸金属实例，影响业务正常运行，请谨慎操作。</p>
打开控制台	打开裸金属节点控制台。
删除裸金属节点	<p>删除不需要的裸金属节点。</p> <p> 注： 此操作将停止所选裸金属节点相关弹性裸金属实例，影响业务正常运行，请谨慎操作。</p>



12.7.5 弹性裸金属实例

在Cloud主菜单，点击**资源中心** > **弹性裸金属管理** > **虚拟资源** > **弹性裸金属实例**，进入**弹性裸金属实例**界面。

弹性裸金属实例支持以下操作：

操作	描述	弹性裸金属实例状态
创建弹性裸金属实例	创建一个新的弹性裸金属实例。	/
编辑弹性裸金属实例	编辑弹性裸金属实例的名称、简介信息。	/
启动弹性裸金属实例	<p>将停止状态的弹性裸金属实例启动。</p> <p> 注： 批量启动弹性裸金属实例时，若弹性裸金属实例未关联规格或裸金属节点，将无法批量启动。请单个启动并关联规格或裸金属节点。</p>	已停止
停止弹性裸金属实例	<p>将启动状态的弹性裸金属实例停止。此操作将同时中断业务，请确保无业务运行再执行此操作。</p> <p> 注： 若弹性裸金属实例相关网关节点未连接，此弹性裸金属实例将无法关机。</p>	运行中
重启弹性裸金属实例	将处于运行状态的弹性裸金属实例重启。此操作将同时中断业务，请确保无业务运行再执行此操作。	运行中
关闭电源	将处于运行状态的弹性裸金属实例强制进入停止状态。	运行中
获取就绪状态	<p>手动获取弹性裸金属就绪状态。</p> <p>注： 获取裸金属就绪状态需要注意以下情况：</p> <ul style="list-style-type: none"> 系统默认1分钟刷新一次弹性裸金属实例的就绪状态，执行此操作可立刻刷新就绪状态。 若弹性裸金属实例未安装agent将一直处于失联状态，请使用已安装agent的镜像重新创建弹性裸金属实例。 <p></p>	/
打开控制台	<p>打开弹性裸金属控制台。</p> <p> 注： 若弹性裸金属实例未安装agent，将无法执行此操作。若需要使用该功能，请使用已安装agent的镜像重新创建弹性裸金属实例。</p>	运行中
绑定标签	为一个或多个弹性裸金属实例绑定标签，可用于标记资源，以及使用标记快速筛选资源。	/

操作	描述	弹性裸金属实例状态
	 注: 单个资源最多支持绑定50个标签。反之，单个标签支持绑定的资源数量无限制。	
解绑标签	解绑弹性裸金属实例上的标签。	/
加载云盘	为弹性裸金属实例加载一块云盘。目前仅支持加载Shared Block主存储上的云盘。  注: 若运行状态的弹性裸金属实例未安装agent，将无法执行此操作。若需要使用该功能，请使用已安装agent的镜像重新创建弹性裸金属实例。	运行中/已停止
卸载云盘	将不需要的云盘从弹性裸金属实例卸载。  注: 弹性裸金属卸载云盘需要注意以下情况： <ul style="list-style-type: none"> 若运行状态的弹性裸金属实例未安装agent，将无法执行此操作。若需要使用该功能，请使用已安装agent的镜像重新创建弹性裸金属实例。 从运行中的弹性裸金属实例卸载云盘，可能影响业务连续性，请谨慎操作。 	运行中/已停止
更换系统	为停止状态的弹性裸金属实例更换操作系统系统。  注: 弹性裸金属更换操作系统需要注意以下情况： <ul style="list-style-type: none"> 确保目标镜像需为Image类型。更换系统后，弹性裸金属实例保持停止状态。 此操作将同时彻底删除原根云盘数据，请务必提前备份远根云盘数据，以免丢失。 跨平台更换系统，可能导致数据盘的分区格式无法识别。 	已停止
修改弹性裸金属实例密码	为弹性裸金属实例修改密码。  注: 若运行状态的弹性裸金属实例未安装agent，将无法执行此操作。若需要使用该功能，请使用已安装agent的镜像重新创建弹性裸金属实例。	运行中
创建镜像	为弹性裸金属实例创建镜像，可用于创建新的弹性裸金属实例。	已停止
创建快照	做重要操作前，在特定时间点对弹性裸金属实例系统盘进行临时状态保留，方便出现故障后迅速回滚。	运行中/已停止

操作	描述	弹性裸金属实例状态
	 注： 目前仅支持为弹性裸金属实例创建单盘快照。	
删除弹性裸金属实例	<p>此操作将立即释放裸金属节点、网关节点和 IP 地址资源，并将弹性裸金属实例移动至回收站。</p> <p>注： 删除弹性裸金属实例，需要注意以下情况：</p> <ul style="list-style-type: none"> 若弹性裸金属实例相关网关节点未连接，此弹性裸金属实例将无法删除。 回收站默认延时 7 天彻底删除弹性裸金属实例。实例删除策略支持立即删除、延时删除、永不删除三种，可在全局设置中按需修改。 	/
彻底删除/恢复弹性裸金属实例	<p>将已删除栏中的弹性裸金属实例彻底删除或恢复。</p> <ul style="list-style-type: none"> 彻底删除： 选择彻底删除后，弹性裸金属实例相关资源会被彻底删除，不可逆转，请谨慎操作。 恢复： 恢复后的弹性裸金属实例回到可用资源页面，且启用状态为已停止，用户可以重新启动该弹性裸金属实例。 <p> 注： 删除弹性裸金属实例后，其 IP 地址会返回 IP 地址池中。恢复弹性裸金属实例，会为其重新分配 IP 地址。</p>	已删除

12.8 vCenter

VMware vCenter Server 是 VMware vCenter 的集中式管理平台。

针对用户已经部署 VMware vCenter Server 的应用场景，Cloud 支持通过 VMware 提供的公开 API 接口纳管 VMware vCenter，可以良好地兼容和管理 VMware vCenter Server 虚拟化管理平台部分功能，实现多虚拟化平台的统一管理。

支持对现有数据中心中的 VMware 虚拟化环境进行管理，能够查看 VMware vCenter Server 所管理的 vSphere 服务器资源和虚拟机资源，能够在虚拟数据中心中使用 VMware vSphere 资源，并在 VMware vCenter 集群中完成对云主机的常用操作。

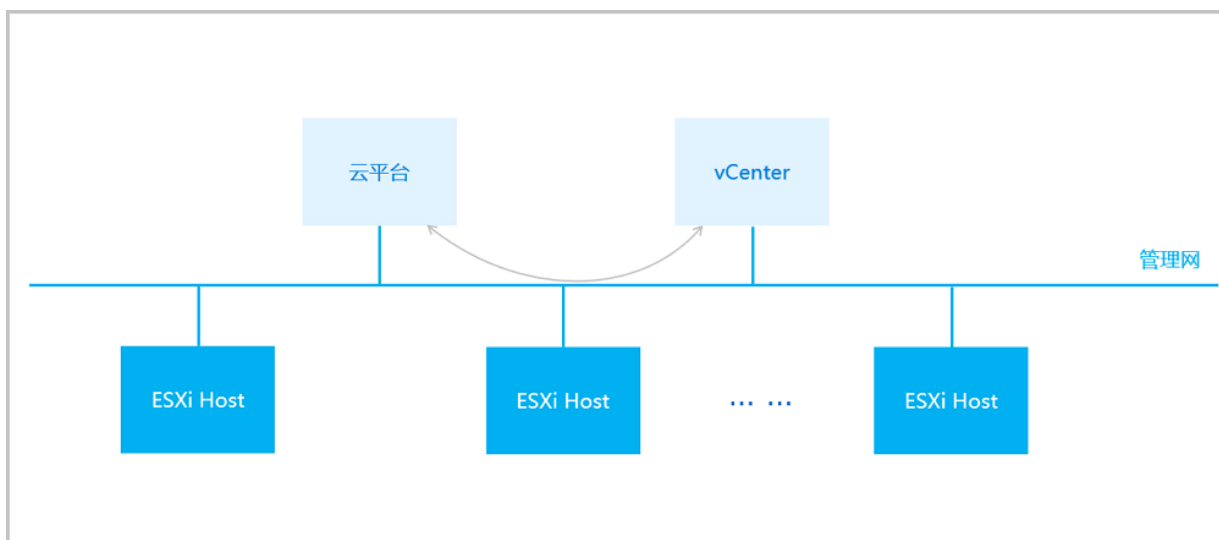
目前，Cloud 支持的 vCenter 版本包括 5.5、6.0、6.5 和 6.7。

外部访问原理

Cloud通过异步事件监听方式，发送云资源控制请求到vCenter，并接收返回的事件内容。Cloud支持接收vCenter主动推送的内容，实现双向信息同步功能。

Cloud管控vCenter逻辑图如图 69: Cloud管控vCenter逻辑图所示：

图 69: Cloud管控vCenter逻辑图



12.8.1 基础资源

首次添加vCenter后，Cloud会自动同步vCenter的集群、物理机、虚拟机、模板、存储、网络等资源。使用过程中，需要点击**同步数据**按钮，将vCenter的资源手动同步至本地。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Cloud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Cloud，未添加到dvSwitch中的物理机，其相关资源不能导入Cloud。

— 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），满足以上条件的同一集群下的物理机，其相关资源（其上所有虚拟机、相同的端口组）才能导入Cloud。



注：Cloud仅接管虚拟机网络，不接管VMkernel或管理网络。

Cloud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vSAN、FC、iSCSI和NFS存储。



注：目前不支持存储集群（Datastore Cluster）。

- vCenter需配置分布式交换机（dvSwitch）或标准交换机（vSwitch）的端口组信息。

— dvSwitch场景：

只有添加到dvSwitch中的物理机，其相关资源才能导入Cloud，未添加到dvSwitch中的物理机，其相关资源不能导入Cloud。

— 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），满足以上条件的同一集群下的物理机，其相关资源（其上所有虚拟机、相同的端口组）才能导入Cloud。



注：Cloud仅接管虚拟机网络，不接管VMkernel或管理网络。

- vCenter已有的模板虚拟机，需要转换为【模板】类型。

vCenter基础资源支持以下操作：

操作	描述
添加vCenter	添加vCenter到当前云平台。 添加vCenter后，Cloud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。
编辑	修改vCenter的名称与简介。
同步数据	 注： <ul style="list-style-type: none"> • 远端vCenter上已部署的vCSA（vCenter Server Appliance）不会同步至本地，避免误操作。 • Cloud支持指定时间间隔自动同步vCenter数据，设置方法如下：

操作	描述
	进入 设置 > 平台设置 > 全局设置 > 高级设置 > 资源中心 > vCenter ，设置vCenter 自动同步数据 即可。
删除vCenter	将vCenter删除。 删除vCenter会同步删除vCenter相关资源的本地记录，远端vCenter上的真实资源不受影响。

注意事项



- 如果远端vCenter上的物理机处于维护模式状态，通过同步数据，可在本地查看该资源状态。
- 通过Cloud创建的vCenter云主机不显示资源池属性，也不在上述**资源池**页面展示。
- 历史版本（低于Cloud3.3.0）升级至最版本后，需点击**同步数据**按钮，才能查看到vCenter资源池信息。


12.8.2 云主机

在Cloud主菜单，点击**资源中心 > vCenter > 云主机**，进入**云主机**界面。

vCenter云主机支持以下操作：

操作	描述
创建vCenter云主机	本地创建vCenter云主机。
编辑	修改vCenter云主机的名称与简介。
启动vCenter云主机	将处于停止状态的vCenter云主机启动。
停止vCenter云主机	将处于运行状态的vCenter云主机停止。 注： 若云主机启用了高可用功能，停止云主机后，云主机将不会自动重启。
重启vCenter云主机	将处于运行状态的vCenter云主机重启。
恢复vCenter云主机	将处于暂停状态的vCenter云主机恢复。
暂停vCenter云主机	将处于运行状态的vCenter云主机暂停。 注： 暂停vCenter云主机并非真正停止云主机，若将已暂停云主机所在物理机停用，则影响业务运行。
关闭电源	将处于运行状态的vCenter云主机强制进入停止状态。

操作	描述
	 注： 正常状态下不建议执行此操作。
打开控制台	<p>打开vCenter云主机的控制台，可登录云主机系统。</p> <p>注：</p> <ul style="list-style-type: none"> Cloud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： <ul style="list-style-type: none"> 通过Cloud创建的vCenter云主机 通过Cloud重启的vCenter云主机 通过Cloud进行动态迁移的vCenter云主机（基于共享存储）
克隆	<p>基于当前vCenter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。</p> <ul style="list-style-type: none"> vCenter云主机支持在线克隆、关机克隆。 带数据云盘的vCenter云主机暂不支持整机克隆。 vCenter云主机支持克隆为云主机（暂不支持克隆为模板）。
vCenter云主机迁移	<p>将vCenter云主机迁移到别的计算节点中。</p> <ul style="list-style-type: none"> 目前仅支持热迁移。 共享存储支持带数据云盘的vCenter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vCenter云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。 <ul style="list-style-type: none"> 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。
修改计算规格	支持离线修改vCenter云主机CPU/内存。
更改所有者	<p>更改vCenter云主机的所有者。</p> <p> 注： Cloud对接管的vCenter支持多租户管理，普通账户/项目成员可对vCenter云主机进行相关操作。</p>
设置高可用	设置vCenter云主机的高可用级别。

操作	描述
	<p>计划性维护或突发情况导致云主机异常关机时，该策略可触发云主机自动重启，提高云主机可用性。</p> <p>注：</p> <ul style="list-style-type: none"> 若物理机正常运行，启用高可用的云主机异常关机均能自动重启。 若物理机异常或进入维护模式，启用高可用的云主机若使用本地存储，异常关机后无法自动重启；若使用共享存储，异常关机后均能自动重启。  可通过全局设置（云主机高可用全局开关）全局控制云主机高可用功能是否可用。默认开启，若关闭将不允许为云主机设置高可用。 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，Cloud的高可用设置与其无关，不受影响。
设置控制台密码	<p>设置vCenter云主机的控制台密码。</p> <ul style="list-style-type: none"> 该密码为VNC协议的密码，不是云主机本身的密码。 设置完成后，重启云主机才可生效。
加载云盘	加载可用的云盘至当前vCenter云主机。
卸载云盘	将加载的云盘从vCenter云主机卸载。
删除vCenter云主机	删除vCenter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vCenter云主机	从删除状态恢复vCenter云主机。
彻底删除vCenter云主机	将删除状态的vCenter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。

12.8.3 网络

在Cloud主菜单，点击**资源中心** > **vCenter** > **网络**，进入**网络**界面。

vCenter网络支持以下操作：

操作	描述
创建vCenter网络	创建一个vCenter网络，网络类型包括：公有网络、扁平网络、VPC网络。
编辑	修改vCenter网络的名称与简介。

操作	描述
添加网络段	给vCenter网络添加网络段。IPv4 类型的公有网络支持地址池功能，可同时添加普通网段和地址池网段。扁平网络和VPC网络仅支持普通网段。
添加DNS	给vCenter网络添加DNS。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> 全局共享：将资源共享给所有的项目和账户使用。 指定共享：将资源共享给指定的项目和账户使用。 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p>注：</p> <ul style="list-style-type: none"> 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
删除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vCenter网络时，会将相关vCenter云主机相应网卡卸载。）

12.8.4 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。

vCenter云盘支持以下操作：

操作	描述
创建vCenter云盘	基于云盘规格或云盘镜像创建一个新的vCenter云盘。
编辑	修改vCenter云盘的名称与简介。
启用vCenter云盘	将处于停用状态的vCenter云盘启用。
停用vCenter云盘	停止使用vCenter云盘。
加载vCenter云盘	将vCenter云盘作为数据云盘加载到指定的vCenter云主机。
卸载vCenter云盘	卸载vCenter云主机的云盘。

操作	描述
	 注: 从运行中的云主机卸载云盘可能影响业务连续性，请谨慎操作。
更改所有者	将vCenter云盘的所有者更改。  注: Cloud对接管的vCenter支持多租户管理，普通账户/项目成员可对vCenter云盘进行相关操作。
删除vCenter云盘	将vCenter云盘删除后，云盘会显示在 回收站 栏。  注: 删除云盘后，该云盘与云主机的IO读写将中断，云盘将不可使用，恢复后才可继续挂载。
恢复vCenter云盘	恢复已删除的vCenter云盘。恢复后将显示在 可用资源 栏。
彻底删除vCenter云盘	将已删除的vCenter云盘彻底删除。  注: 彻底删除云盘后，云盘相关资源会被彻底删除，不可逆转，请谨慎操作。

使用说明

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。

使用vCenter云盘，需注意：

- 不同Hypervisor上的云盘不可加载到不同类型的云主机上。例如，KVM云主机的云盘不能加载到vCenter云主机上。
- 云盘可在相同类型Hypervisor的不同云主机之间加载和卸载。
- 云盘同一时间只能加载到一个云主机。
- 云盘占用空间采用虚拟容量来计算。创建云盘时占用的是云盘的虚拟容量大小，本身只占用少量实际容量。随着写入文件数量的增加，实际容量会逐步增加。
- 根云盘作为vCenter云主机的附属，不能卸载。

12.8.5 镜像

Cloud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镜像支持以下操作：

操作	描述
添加vCenter镜像	添加vmdk格式的本地镜像到vCenter，目前不支持加添ISO格式。
编辑	修改vCenter镜像的名称与简介。
启用vCenter镜像	将处于停用状态的vCenter镜像启用。启用后，镜像可作为候选使用。
停用vCenter镜像	将处于启用状态的vCenter镜像停用。停用后，镜像不可再作为候选使用。
设置共享模式	<p>设置该资源的共享模式。目前支持以下三种模式：</p> <ul style="list-style-type: none"> 全局共享：将资源共享给所有的项目和账户使用。 指定共享：将资源共享给指定的项目和账户使用。 不共享：将已共享的资源进行召回。召回后，其他项目和账户将无法使用此资源。 <p>注：</p> <ul style="list-style-type: none"> 将全局共享模式修改为指定共享之后，资源仅对指定的项目或账户可见。 修改共享模式后，原项目/账户已使用的资源将继续保留且不受影响，直到被释放。
更改所有者	<p>更改vCenter镜像的所有者。</p> <p>注： Cloud对接管的vCenter支持多租户管理，普通账户/项目成员可使用admin共享的vCenter镜像。</p>
删除vCenter镜像	删除vCenter镜像，会同时删除本地记录和远端vCenter上的真实镜像资源。
恢复vCenter镜像	将已删除的vCenter镜像恢复。恢复后，镜像会显示在 可用资源 栏。
彻底删除vCenter镜像	将已删除的镜像彻底删除。只有回收站的镜像才支持彻底删除。

13 平台运维

13.1 网络拓扑

全局拓扑界面

在Cloud主菜单，点击**平台运维** > **网络拓扑** > **全局拓扑**，进入**全局拓扑**界面。

如图 70: 全局拓扑所示：


图 70: 全局拓扑



全局拓扑支持的操作

全局拓扑支持以下操作：

操作	描述
查看	<ul style="list-style-type: none">支持对整个云平台网络拓扑的直观查看。直连云主机可显示该网络直接连接云主机的数量。
刷新	可显示当前最新全局拓扑。
导出图片	支持当前全局拓扑以png格式图片导出。
显示/隐藏云主机	支持显示或隐藏网络拓扑中的云主机。 注： 若网络直连云主机数量超过50台，则网络拓扑不显示直连云主机，用户可手动点击+显示该网络下所有直连云主机。
搜索	搜索框支持按资源类别以及资源属性进行搜索。

操作	描述
	注:  <ul style="list-style-type: none"> 资源类别目前支持：扁平网络、VPC网络、公有网络、VPC路由器、云主机。 资源属性目前支持：资源名称和资源UUID。
适应画布	可自动将网络拓扑缩放到适合大小。
放大	可将网络拓扑进行放大查看。
缩小	可将网络拓扑进行缩小查看。
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。
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 路由器/云主机状态显示定义

路由器/云主机状态显示定义

路由器/云主机状态	状态标识颜色
已创建	蓝色
启动中	蓝色
运行中	绿色
停止中	红色
已停止	红色
重启中	蓝色
删除中	中性色
已删除	中性色
迁移中	蓝色
彻底删除中	中性色
暂停中	黄色
已暂停	黄色
从暂停状态恢复中	中性色
云盘迁移中	中性色
未知	中性色

自定义拓扑界面

在Cloud主菜单，点击**平台运维** > **网络拓扑** > **自定义拓扑**，进入**自定义拓扑**界面。

如图 70: 全局拓扑所示：

图 71: 自定义拓扑



自定义拓扑支持的操作

自定义拓扑支持以下操作：

操作	描述
自定义资源	支持自定义网络拓扑，可添加或删除显示的资源，例如扁平网络、VPC网络、公有网络、VPC路由器、云主机等。
查看	支持查看自定义网络拓扑。
刷新	可显示当前最新自定义拓扑。
导出图片	支持当前自定义拓扑以png格式图片导出。
搜索	<p>搜索框支持按资源类别以及资源属性进行搜索。</p> <p>注：</p> <ul style="list-style-type: none"> 资源类别目前支持：扁平网络、VPC网络、公有网络、VPC路由器、云主机。 资源属性目前支持：资源名称和资源UUID。
适应画布	可自动将网络拓扑缩放到适合大小。

操作	描述
放大	可将网络拓扑进行放大查看。
缩小	可将网络拓扑进行缩小查看。
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。
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 路由器/云主机状态显示定义

路由器/云主机状态显示定义

路由器/云主机状态	状态标识颜色
已创建	蓝色
启动中	蓝色
运行中	绿色
停止中	红色
已停止	红色
重启中	蓝色
删除中	中性色
已删除	中性色
迁移中	蓝色
彻底删除中	中性色
暂停中	黄色
已暂停	黄色
从暂停状态恢复中	中性色
云盘迁移中	中性色
未知	中性色

13.2 云平台监控

13.2.1 性能分析

通过列表方式展示云平台核心资源的性能监控指标，支持外部和内部两种监控方式，方便用户掌控云平台性能状态，提高运维效率。

可使用资源筛选查看以下资源子页面：

- 云主机/路由器页面：

云主机/路由器页面分为外部监控和内部监控：

- 外部监控页面通过对当前区域全部云主机/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、磁盘读/写速度、网卡出/入速度为指标进行展示，可直观掌控云平台内资源的性能指标。
- 内部监控页面通过对当前区域全部云主机/路由器的插件状态、操作系统、默认IP、CPU、内存、磁盘使用情况进行统计分析，以插件状态、操作系统、默认IP、CPU使用率、内存使用率、磁盘使用率为指标进行展示，可直观掌控云平台内资源的性能指标。



注：

- 在云主机页面点击**停止**按钮，支持停止云主机。
- 如果存在多个CPU，外部监控CPU利用率可能会超过100%。
- 对于内存数据而言，内部监控比外部监控拥有更好的准确性，推荐在监控内存数据时使用内部监控。
- 物理机页面：

通过对当前区域全部物理机的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、磁盘读/写速度、磁盘用量、网卡出/入速度为指标进行展示，可直观掌控云平台内资源的性能指标。
- 三层网络页面：

对当前区域全部三层网络的IPv4类型地址使用情况进行统计分析，以已用IP数量、已用IP百分比、可用IP数量、可用IP百分比为指标进行展示，可直观告知运维人员当前三层网络的IP资源使用情况。
- 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、上行网络入包速率为指标进行展示，可直观告知运维人员当前哪些虚拟IP出现传输性能瓶颈。

- 镜像服务器页面：

通过对当前区域全部镜像服务器容量进行统计分析，以镜像存储可用容量百分比信息为指标进行展示，可直观告知运维人员镜像服务器存储使用情况。

补充说明

- 支持自定义统计数据范围（默认1分钟），通过右上方按钮指定起始时间，自定义查看不同时间段内性能分析数据。
- 左侧筛选器支持按资源范围、按筛选条目筛选出需要查看的性能分析列表。其中，云主机、路由器和虚拟IP还支持按所有者筛选性能分析列表。
- 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。
- 普通账户/项目成员支持查看性能分析，与admin视角类似，在该页面可直观便捷查看本账户内云主机、路由器、三层网络、虚拟IP资源实时使用情况。
- 选择时间段查看性能分析数据，该数据为所选时间段内的采样平均值，如需获取当前具体数值请进入资源详情页进行查看。

13.2.2 容量管理

通过可视化方式展示云平台核心资源的容量信息，方便用户掌控云平台容量使用情况，提高运维效率。

支持对云平台核心资源物理容量信息进行直观展示，包括：以卡片形式展示各种核心资源详细物理容量信息，以及核心资源容量TOP 10，方便用户整体掌控当前云平台核心资源物理容量使用情况，提高运维效率。

容量管理界面主要分为上下两个版块：

- 上方版块：以卡片形式展示各种核心资源详细容量信息，包括：主存储、镜像服务器、计算节点、云主机、云盘、镜像、快照、管理节点。
- 下方版块：对各种核心资源容量信息进行TOP 10排序，包括：物理机、主存储、镜像服务器、镜像、云主机、云盘、快照。

**注:**

- 本界面展示的资源容量信息均为资源的真实物理容量。
- 本界面数据均为静态数据，每次刷新页面会获取最新数据。
- 目前支持统计以下主存储类型：本地存储、Shared Block、Ceph。
- 目前支持统计以下镜像服务器类型：镜像仓库、Ceph。

注意事项:

- 若存在主存储、镜像服务器失联，将影响相关资源容量统计卡片以及资源容量 TOP 10 中的统计数据准确性；
- 若对主存储、镜像服务器执行删除、重连等操作，需等待片刻并刷新容量管理界面，获取最新数据。

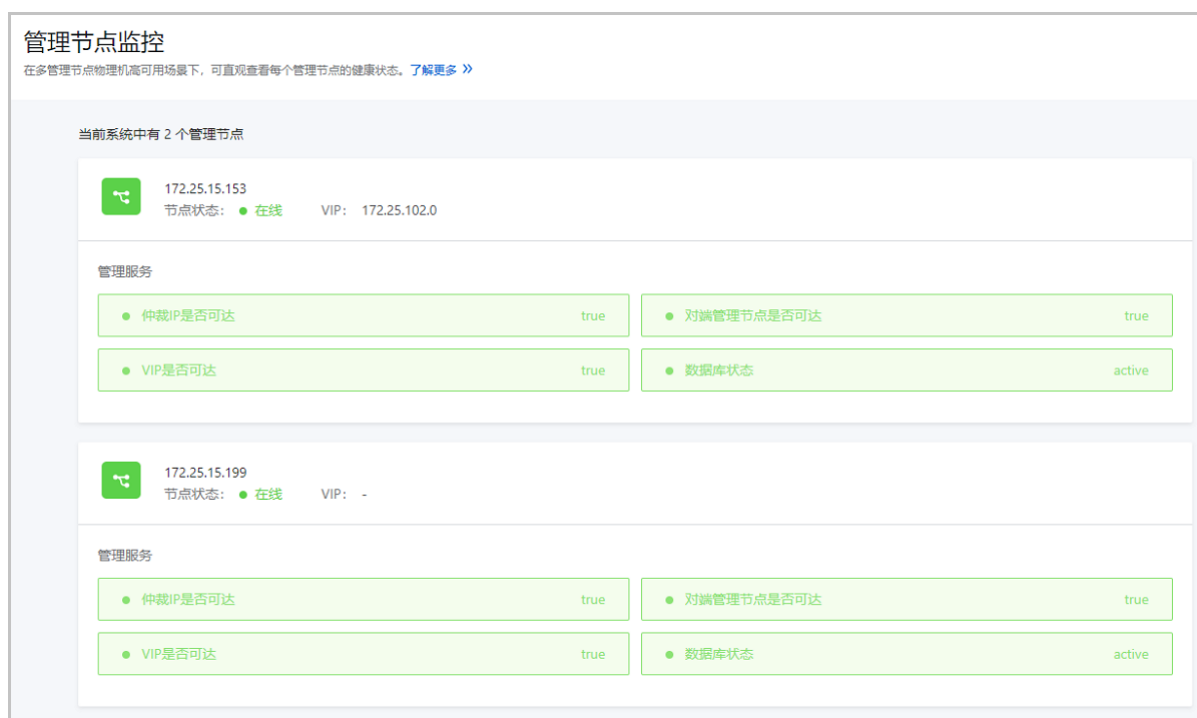
13.2.3 管理节点监控

在多管理节点物理机高可用场景下，可直观查看每个管理节点的健康状态。

在Cloud主菜单，点击**平台运维** > **云平台监控** > **监控图表** > **管理节点监控**，进入**管理节点监控**界面。

如图 72: 管理节点监控所示：

图 72: 管理节点监控



管理节点监控支持显示多个管理节点的管理节点IP、节点状态、VIP和管理服务状态，主要包括以下几种管理服务：

- 仲裁IP是否可达：

监控用于判断主备管理节点的仲裁IP是否可达，若不可达可能导致管理节点高可用功能失效。

- 对端管理节点是否可达：

监控备管理节点是否可达，若备管理节点不可达，无法与备管理节点通信。

- VIP是否可达：

监控VIP是否可达，若VIP不可达，主管理节点不能通过VIP访问UI界面。

- 数据库状态：

监控数据库状态，若数据库异常或多管理节点数据库不同步，可能存在数据丢失风险，请及时恢复故障。

注意事项

- 此页面包括：绿色、红色、灰色三种颜色。其中，绿色表示正常；其他颜色均表示异常。若出现异常状态，请及时查找原因解决问题。
- 多管理节点采用主备模式，主管理节点只有一个。显示VIP的为管理节点，未显示VIP的均为备管理节点。
- 若所有备管理节点状态异常，主管理节点故障后，无法切换且管理节点宕机。因此，若发现存在管理节点异常，请及时处理。

13.2.4 报警器

用于监控并响应时序性数据和事件的状态变化，支持资源报警器、事件报警器和扩展报警器。

报警器支持以下操作：

表 13: 资源报警器

操作	描述
创建资源报警器	创建一个新的资源报警器。
启用资源报警器	将停止状态的资源报警器启用。
停用资源报警器	将正在使用的资源报警器停用。
编辑资源报警器	修改资源报警器的名称和简介。

操作	描述
添加通知对象	给选中的资源报警器添加通知对象。
移除通知对象	将通知对象从资源报警器移除。
删除	删除一个资源报警器，删除报警器的同时将移除其上所有资源并 不再报警，请谨慎操作。

表 14: 事件报警器

操作	描述
创建事件报警器	创建一个新的事件报警器。
编辑事件报警器	修改事件报警器的名称和简介。
添加通知对象	给选中的事件报警器添加通知对象。
移除通知对象	将通知对象从事件报警器移除。
删除	删除一个事件报警器，删除报警器的同时将移除其上所有资源并 不再报警，请谨慎操作。

表 15: 扩展报警器

操作	描述
创建扩展报警器	创建一个新的扩展报警器。
编辑扩展报警器	修改扩展报警器的名称和简介。
添加通知对象	给选中的扩展报警器添加通知对象。
移除通知对象	将通知对象从扩展报警器移除。
删除	删除一个扩展报警器，删除报警器后将不再接收扩展报警消息， 请谨慎操作。

13.2.5 一键报警

将种类繁多的资源监控项进行归纳整合，用于快速建立各种资源的监控报警服务。

一键报警支持以下操作：


操作	描述
开启一键报警	开启所选资源一键报警功能，系统将自动创建多个报警器。
启用资源报警器	将停止状态的资源报警器启用。

操作	描述
停用资源报警器	将正在使用的资源报警器停用。
编辑资源报警器	修改资源报警器的名称和简介。
添加通知对象	给选中的资源报警器添加通知对象。
移除通知对象	将通知对象从资源报警器移除。
删除	删除一个资源报警器，删除报警器的同时将移除其上所有资源并 不再报警，请谨慎操作。

13.2.6 资源分组

按照业务对资源进行分组，关联报警模板后，报警规则将直接作用于组内全部资源。

资源分组支持以下操作：


操作	描述
绑定标签	为资源分组绑定标签。
解绑标签	解绑资源分组上的标签。
设置规则模板	为当前资源分组绑定规则模板。  注： 一个规则模板可以绑定多个资源分组。
删除	删除资源分组，将同步删除组内资源关联的报警器，请谨慎操作。

13.2.7 报警模板

一组报警器规则的通用模板，关联资源分组后，将对组内资源创建相应的报警器进行监控。

报警模板支持以下操作：

操作	描述
绑定标签	为报警模板绑定标签。
解绑标签	解绑报警模板上的标签。
设置共享	设置当前报警模板的共享模式。
克隆	基于当前报警模板，克隆完全相同的报警模板。
绑定资源分组	为当前报警模板绑定资源分组。

操作	描述
	 注： 一个报警模板可以绑定多个资源分组。
解绑资源分组	解绑报警模板上的资源分组。
删除	删除报警模板，将解除与资源分组的绑定关系，已生成的报警器不受影响。

13.2.8 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。

消息模板支持以下操作：

操作	描述
创建消息模板	创建一个消息模板。
设置为默认	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消息模板取消默认设置。
删除	删除当前消息模板。

13.2.9 消息源

用于连接扩展消息源，接管扩展报警消息并结合报警器统一推送至各类通知对象。

消息源支持以下操作：

操作	描述
启用消息源	启用当前消息源，可以通过配置扩展报警器来接收消息。
停用消息源	停用当前消息源，使用该消息源的扩展报警器将无法接收消息。
删除	删除当前消息源。

13.2.10 通知对象

用户获取订阅主题信息的方式，通知对象类型包括：系统、邮箱、钉钉、HTTP应用、短信、Microsoft Teams。

通知对象支持以下操作：

操作	描述
启用通知对象	将已停用的通知对象启用。
停用通知对象	将正在使用的通知对象停用。
添加报警器	向选中的通知对象中添加报警器。
移除报警器	将报警器从通知对象中移除。
删除	删除一个通知对象。

13.3 消息日志

13.3.1 报警消息

报警器触发时发送的即时提示消息。

报警消息包括以下两个子页面：

- 云平台：展示当前云平台的全部报警消息。
- 扩展报警消息：展示扩展报警消息，需要在**设置 > 平台设置 > 全局设置 > 高级设置**中开启**扩展报警开关**，才能使用扩展报警消息功能。

注意事项

- 消息已读未读的对象为消息本身，拥有操作权限的任何角色，首次阅读消息或对消息标记为已读后，该消息已读未读状态将同步更新至其他角色。
- admin/平台管理员对所有消息可见，支持对admin/普通账户/项目产生的报警消息**全部标记已读**操作，标记后消息已读未读状态同步更新。
- 普通账户之间对消息的标记是独立的，不同账户间互相不可见，仅能标记自己报警器产生的报警。
- 企业管理中，报警消息以项目为单位。项目成员/项目管理员/项目负责人中任何人首次阅读消息或对消息标记为已读后，该消息已读未读状态将同步更新至该项目中的其他人。
- 使用第三方报警消息需要保证云平台与第三方搭建完成。
- 第三方报警消息仅支持admin使用。

13.3.2 操作日志

操作日志：云平台运行过程中变化的一种抽样，内容为指定对象的某些操作及其操作结果按时间的有序集合。通过操作日志，可快速查看云平台的历史操作与当前任务。可结合云平台审计功能进行细粒度操作追踪与问题排查，进一步提高运维效率。

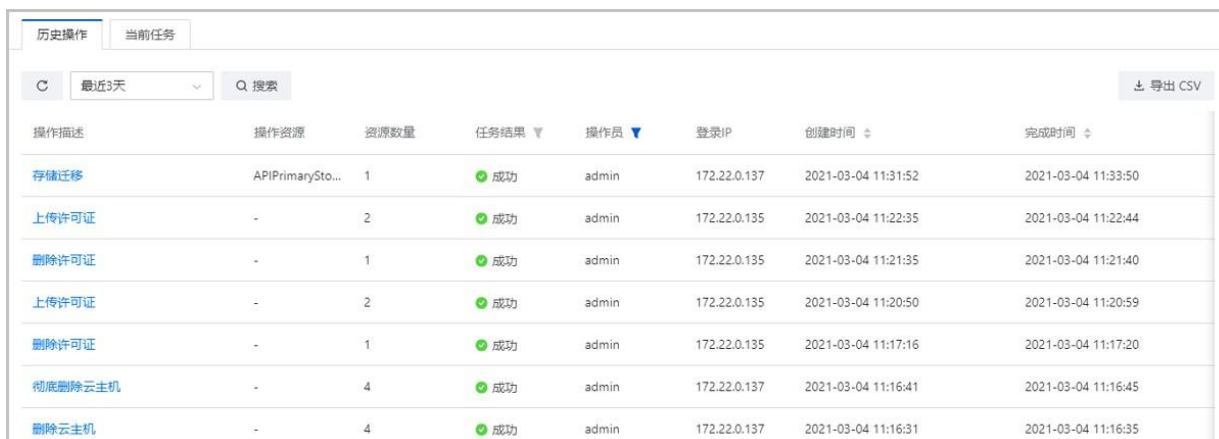
操作日志界面包括两个子页面：历史操作、当前任务。

操作日志界面：历史操作

在操作日志界面，点击**历史操作**，进入**历史操作**子页面。

如图 73: 操作日志界面：历史操作所示：

图 73: 操作日志界面：历史操作



操作描述	操作资源	资源数量	任务结果	操作员	登录IP	创建时间	完成时间
存储迁移	APIPrimarySto...	1	成功	admin	172.22.0.137	2021-03-04 11:31:52	2021-03-04 11:33:50
上传许可证	-	2	成功	admin	172.22.0.135	2021-03-04 11:22:35	2021-03-04 11:22:44
删除许可证	-	1	成功	admin	172.22.0.135	2021-03-04 11:21:35	2021-03-04 11:21:40
上传许可证	-	2	成功	admin	172.22.0.135	2021-03-04 11:20:50	2021-03-04 11:20:59
删除许可证	-	1	成功	admin	172.22.0.135	2021-03-04 11:17:16	2021-03-04 11:17:20
彻底删除云主机	-	4	成功	admin	172.22.0.137	2021-03-04 11:16:41	2021-03-04 11:16:45
删除云主机	-	4	成功	admin	172.22.0.137	2021-03-04 11:16:31	2021-03-04 11:16:35

历史操作子页面针对已完成操作提供日志查看，可查看该操作的操作描述、操作资源、资源数量、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。

- 支持选择时间段，查看所选时间段已完成操作的日志。可选的时间段包括：最近3天、最近7天、最近1个月。
- 支持自定义时间段，查看所设时间段已完成操作的日志。
- 支持通过输入操作描述/操作员/登录IP，搜索已完成的操作日志。
- 支持通过任务结果和操作员，对已完成的操作进行筛选。其中任务结果包括：成功、失败、已取消、正在取消、异常、超时。
- 支持按创建时间对已完成的操作进行排序。
- 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。

操作日志界面：当前任务

在操作日志界面，点击**当前任务**，进入**当前任务**子页面。

如图 74: 操作日志界面：当前任务所示：

图 74: 操作日志界面：当前任务

历史操作		当前任务	
C		搜索	
<input type="checkbox"/>	操作描述	任务进度	创建时间
<input type="checkbox"/>	添加镜像	进行中 89%	2020-12-31 14:06:00
<input type="checkbox"/>	删除云主机		2020-12-28 21:00:18

当前任务子页面针对当前正在进行中的操作提供日志查看，可查看该操作的操作描述、任务进度、任务创建时间，可取消正在进行中的任务。

- 通过进度条实时展示任务进度，可点击任务后的x按钮取消进行中的任务。



注：仅部分任务支持取消操作。

- 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。

注意事项

操作日志默认保留90天。用户可自行设置操作日志的保留时间上限。设置方法：

- 进入**设置 > 平台设置 > 全局设置 > 基本设置 > 平台运维 > 监控报警**，设置**操作日志保留时间**即可，默认为90天。

若操作日志过多，建议适当缩短操作日志的保留时间，以降低管理节点的负荷。

13.3.3 审计

审计（Audit）：实时监控并记录云平台的所有活动，可用于操作追踪、等保合规、安全分析、问题排查、自动运维等场景。通过审计功能，可持续监控并保留针对云平台的所有操作，包括通过控制台、API服务、开发者工具对云平台的访问和使用等行为。

工作原理

安装Cloud后，审计功能被立即启用，可在审计页面进行查看。当Cloud中触发操作时，操作将被记录至审计页面。通过审计页面，可轻松查看云平台操作的所有记录。

功能特性

- 多维度查询：

支持两种操作审计：资源操作和登录操作，从操作时段、资源类型、API名称、操作员、消耗时间、登录IP、固定时间段/自定义时间段等维度查询历史操作活动。



注：可选择的时间跨度：最近3天、最近7天、最近30天、自定义。

- 装机即用：

无需额外配置，审计功能默认追踪并记录所有操作记录。



注：UI界面支持最多显示300条审计信息。详情请参考《用户手册》中[查看审计](#)章节。

- 自主管理：
 - 审计事件可以将记录并保存到数据库。
 - 通过数据库，可对这些审计事件的数据进行管理，例如：权限管理、连续检索、高效查询和数据分析等。
- 超长保留：

审计记录可保留1年。
- 审计日志导出：

支持导出当前/全部页面审计记录。

应用场景

- 操作追踪：
 - 当资源出现异常变更时，通过审计功能记录的操作可快速定位问题。
 - 当一台云主机停机时，可通过审计功能定位停机的操作员、操作时间和完成时间。
 - 同时，通过操作日志可查看相应操作员的IP地址。
- 等保合规：
 - 审计功能可满足合规审计要求，帮助获取每个用户/项目成员/子账户的详细操作记录。
 - 若企业管理/子账户管理服务中的用户/项目成员/子账户停止某云主机，可通过审计功能定位该服务中的用户/项目成员/子账户信息。
 - 企业管理中，审计管理员可针对用户的操作行为进行审计和安全控制。详情请参考[三员分立使用教程](#)。
- 安全分析：

审计功能会对用户各类操作进行详细的记录和保存。用户可针对这些操作进行权限管理。
- **资源操作审计**提供调用API操作的审计信息，可查看该调用API名称、资源类型、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。

如图 75: 资源操作审计所示:

图 75: 资源操作审计

API名称	资源类型	消耗时间	任务结果	操作员	开始时间	完成时间
LogOut	SessionVO	0.01秒	成功	admin	2021-02-23 20:25:34	2021-02-23 20:25:34
LoginByAccount	SessionVO	0.01秒	成功	admin	2021-02-23 20:25:34	2021-02-23 20:25:34
LogOut	SessionVO	0.01秒	成功	admin	2021-02-23 20:25:34	2021-02-23 20:25:34
LoginByAccount	SessionVO	0.02秒	成功	admin	2021-02-23 20:25:33	2021-02-23 20:25:33
CreateVmInstance	VmInstanceVO	1分钟18秒	成功	admin	2021-02-23 20:16:09	2021-02-23 20:17:27
CreateVmInstance	InstanceOfferingV...	1分钟18秒	成功	admin	2021-02-23 20:16:09	2021-02-23 20:17:27
CreateVmInstance	L3NetworkVO	1分钟18秒	成功	admin	2021-02-23 20:16:09	2021-02-23 20:17:27
CreateVmInstance	ClusterVO	1分钟18秒	成功	admin	2021-02-23 20:16:09	2021-02-23 20:17:27

- 支持设置任务时间段，可查看所设时间段内调用API的所有审计信息及详情。



注:

- UI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。
- 可选择的时间跨度：最近3天、最近7天、最近30天、自定义。

- 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。



注: 用户可自行设置审计搜索是否区分大小写。设置方法:

进入**设置 > 平台设置 > 全局设置 > 高级设置 > 平台运维 > 监控报警**，设置**审计搜索区分大小写开关**即可，默认为False。

- 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。
- **登录操作审计**提供登录登出API操作的审计信息，可查看该调用API名称、操作员、消耗时间、登录IP、浏览器类型、任务结果、任务创建/完成时间，以及API行为的消息详情。

如图 76: 登录操作审计所示:

图 76: 登录操作审计

API名称	操作员	消耗时间	登录IP	浏览器	任务结果	开始时间	完成时间
LogOut	admin	0.01秒	未知	未知	成功	2021-02-23 20:25:34	2021-02-23 20:25:34
LoginByAccount	admin	0.01秒	未知	未知	成功	2021-02-23 20:25:34	2021-02-23 20:25:34
LogOut	admin	0.01秒	未知	未知	成功	2021-02-23 20:25:34	2021-02-23 20:25:34
LoginByAccount	admin	0.02秒	未知	未知	成功	2021-02-23 20:25:33	2021-02-23 20:25:33
LogOut	admin	0.01秒	未知	未知	成功	2021-02-23 20:17:18	2021-02-23 20:17:18
LoginByAccount	admin	0.01秒	未知	未知	成功	2021-02-23 20:17:17	2021-02-23 20:17:17
LoginByAccount	admin	0.01秒	未知	未知	成功	2021-02-23 20:16:03	2021-02-23 20:16:03
LoginByAccount	admin	0.01秒	未知	未知	成功	2021-02-23 20:15:58	2021-02-23 20:15:58

- 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:

- UI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。
- 可选择的时间跨度：最近3天、最近7天、最近30天、自定义。

- 支持通过输入操作员/API名称/登录IP/浏览器类型，搜索调用API的审计信息。



注：用户可自行设置审计搜索是否区分大小写。设置方法：

进入**设置 > 平台设置 > 全局设置 > 高级设置 > 平台运维 > 监控报警**，设置**审计搜索区分大小写开关**即可，默认为False。

- 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。

13.4 灾备管理

灾备管理：灾备管理以业务为中心，融合定时增量备份、定时全量备份等多种灾备技术到云平台中，支持本地灾备、异地灾备等多种灾备方案，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，且需在购买企业版云平台许可证基础上使用，不可单独使用。

应用场景

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。



注：若同时拥有企业管理模块许可证，企业管理中的项目成员（项目负责人/项目管理员/普通项目成员）支持对项目中的云主机/云盘资源进行本地灾备。

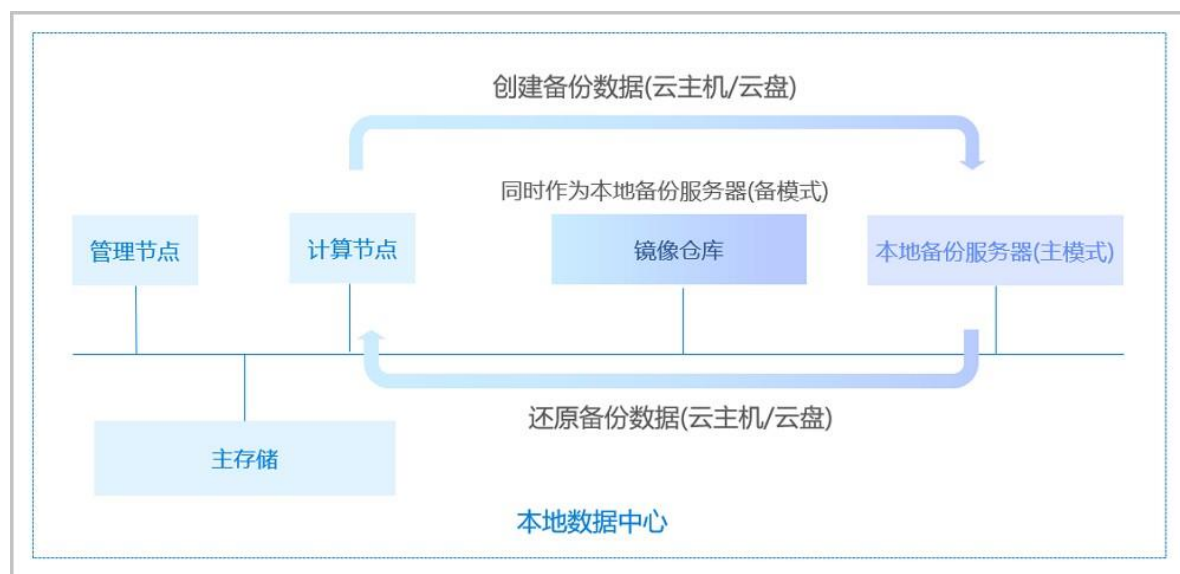
• 本地灾备：

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（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。

如图 77: 本地灾备场景 1 所示：

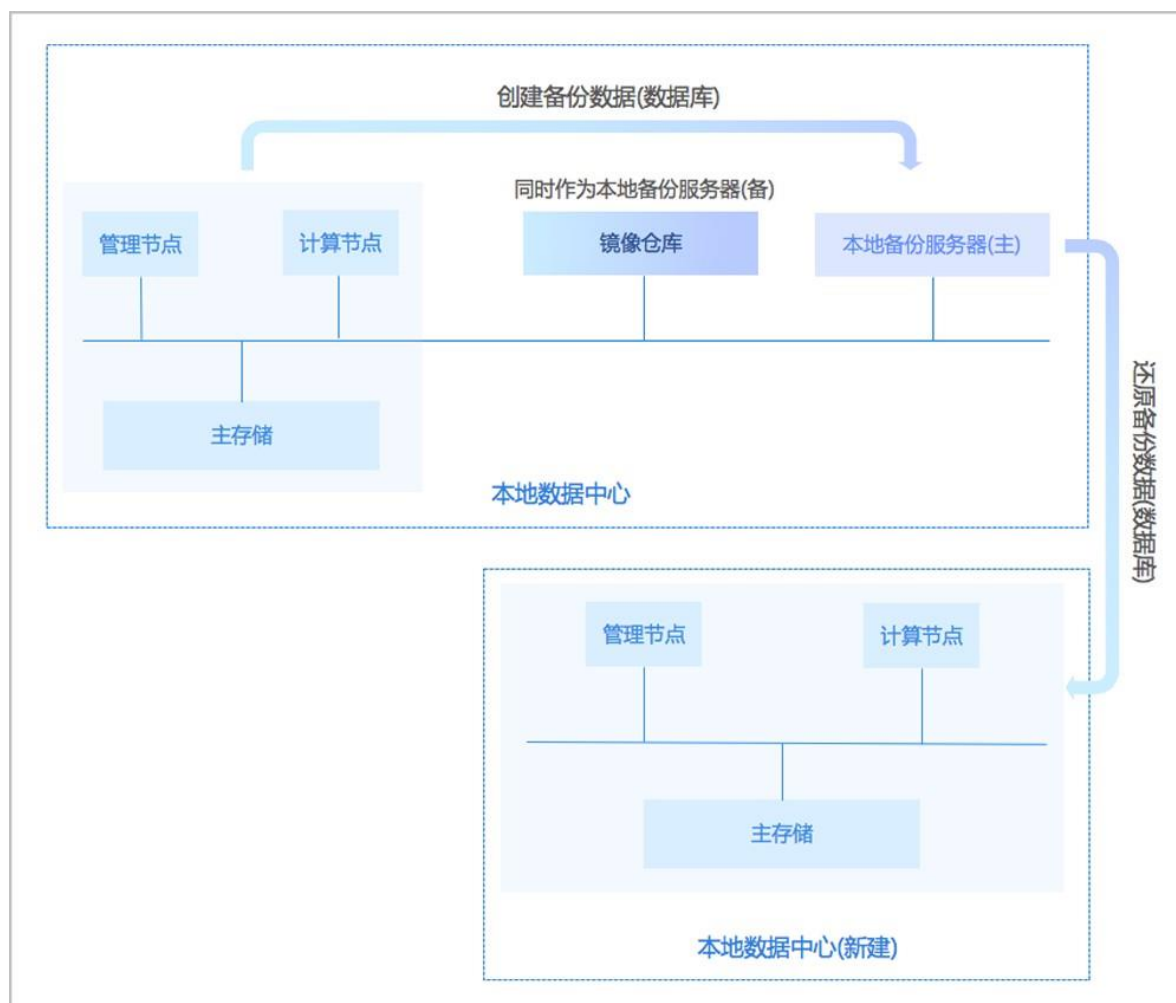
图 77: 本地灾备场景 1



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。

如图 78: 本地灾备场景 2 所示：

图 78: 本地灾备场景 2



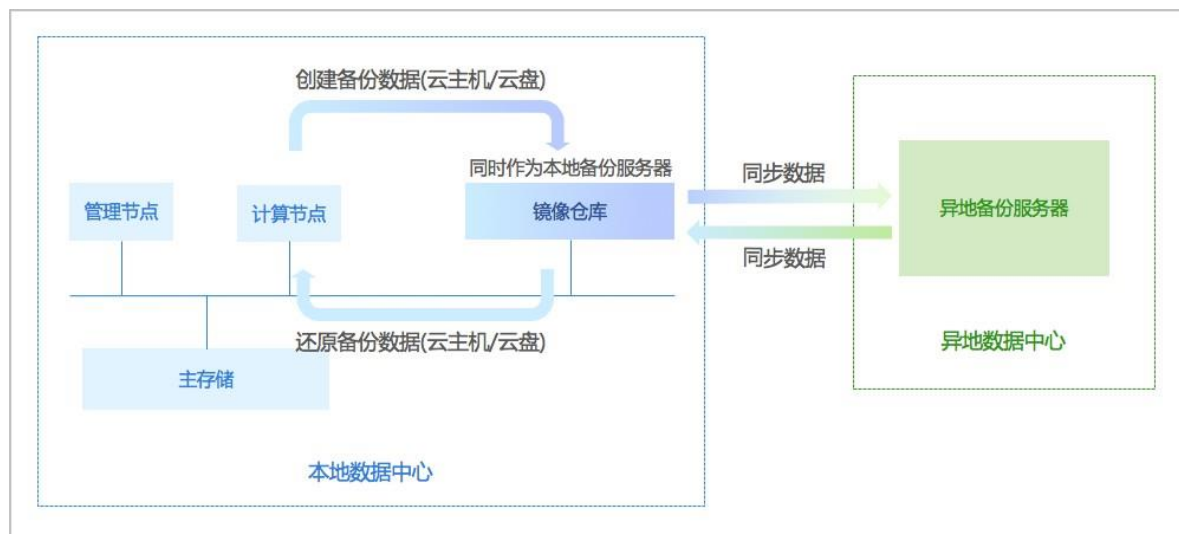
• 异地灾备:

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。

如图 79: 异地灾备场景 1 所示:

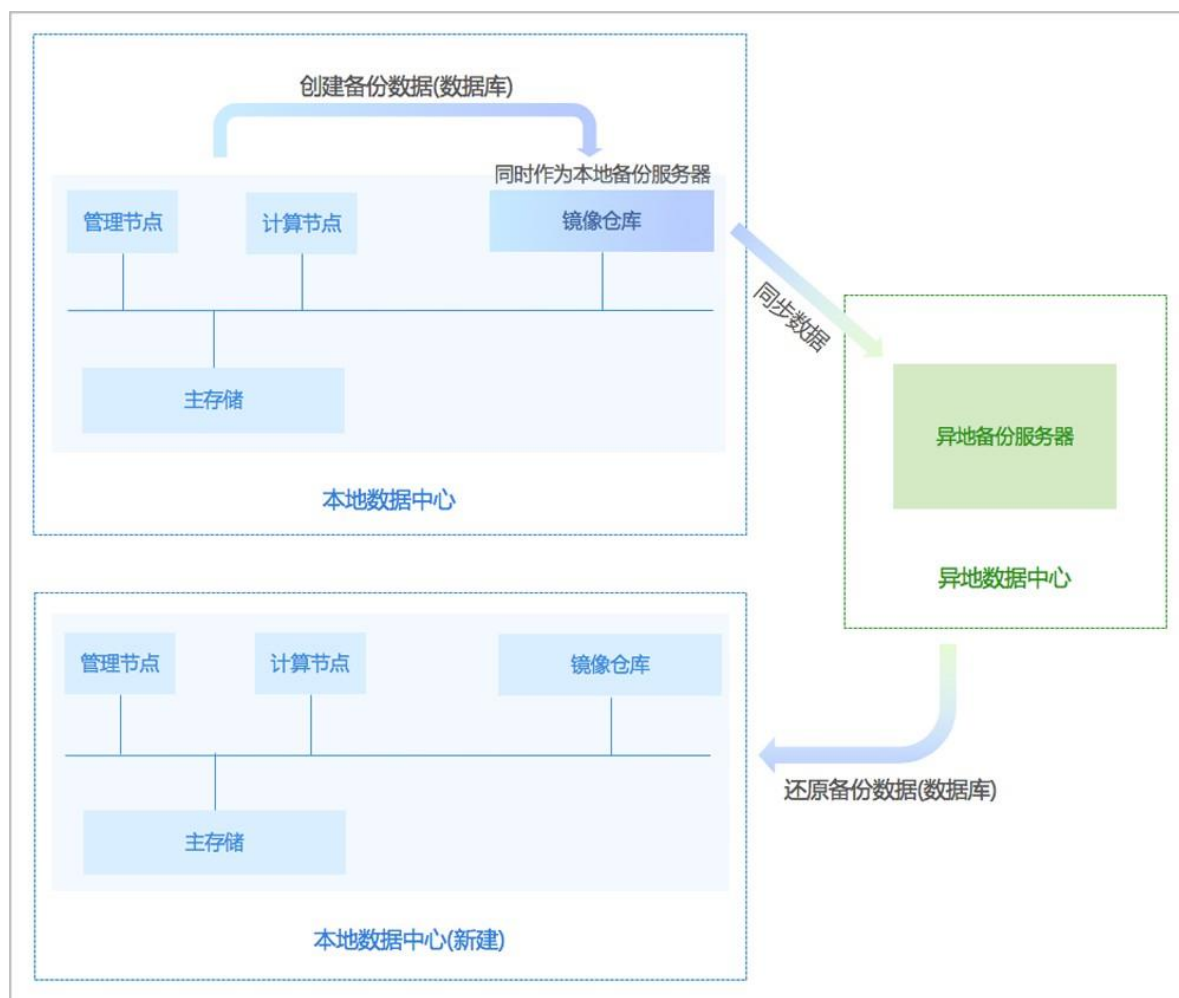
图 79: 异地灾备场景1



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。

如图 80: 异地灾备场景2所示:

图 80: 异地灾备场景2



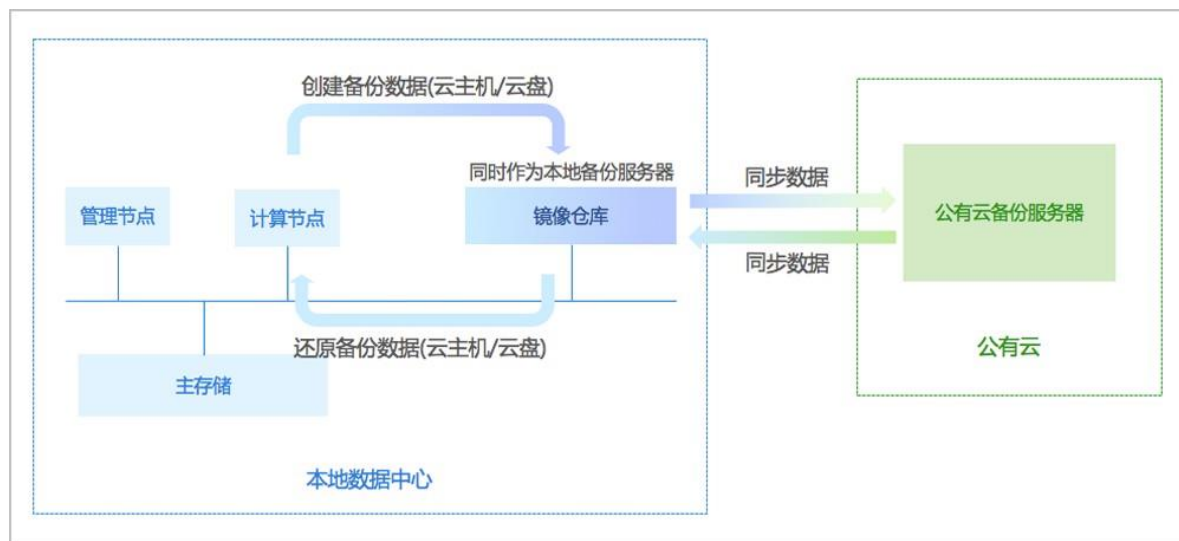
• 公有云灾备:

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。

如图 81: 公有云灾备场景 1 所示:

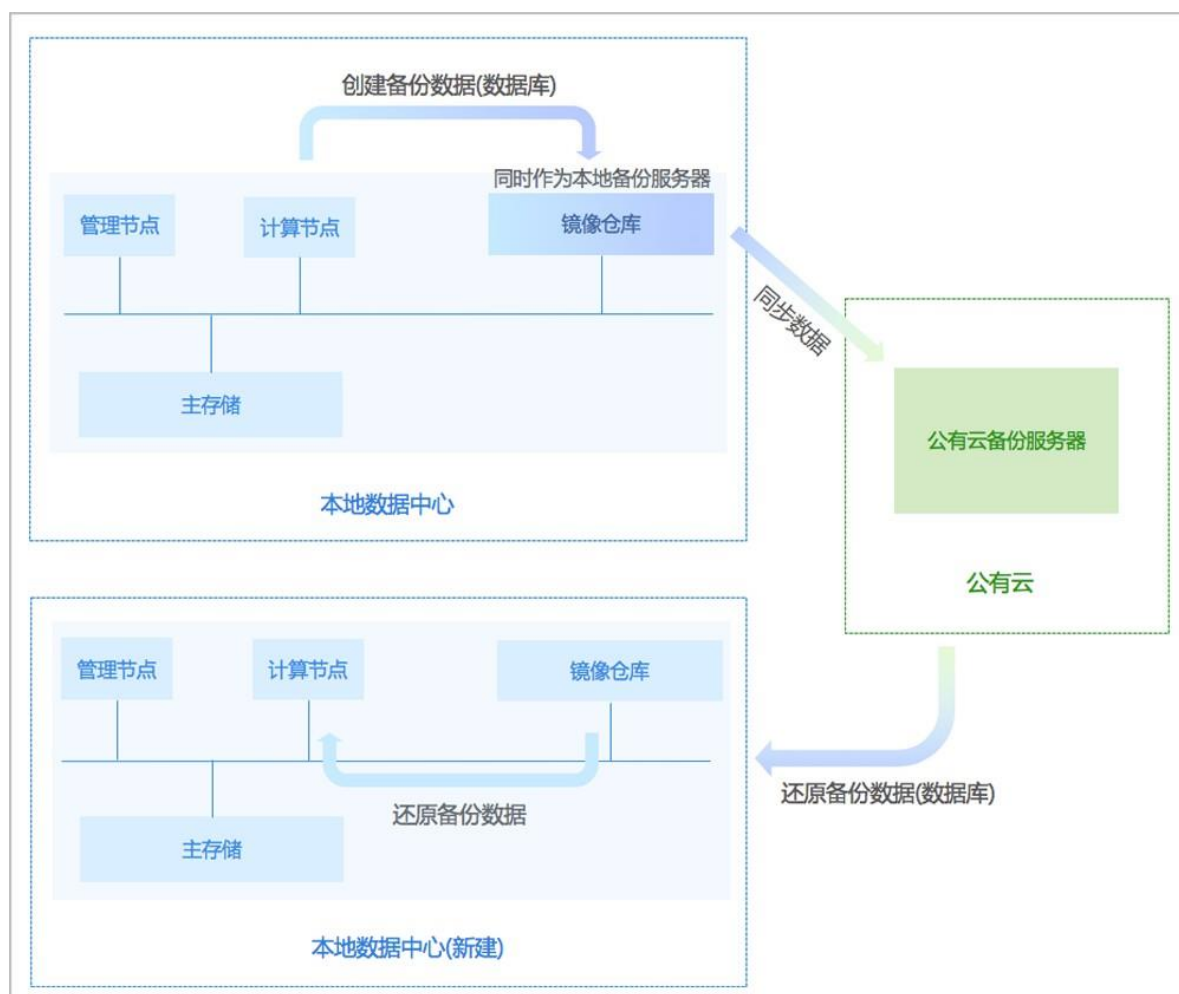
图 81: 公有云灾备场景1



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。

如图 82: 公有云灾备场景2所示:

图 82: 公有云灾备场景2



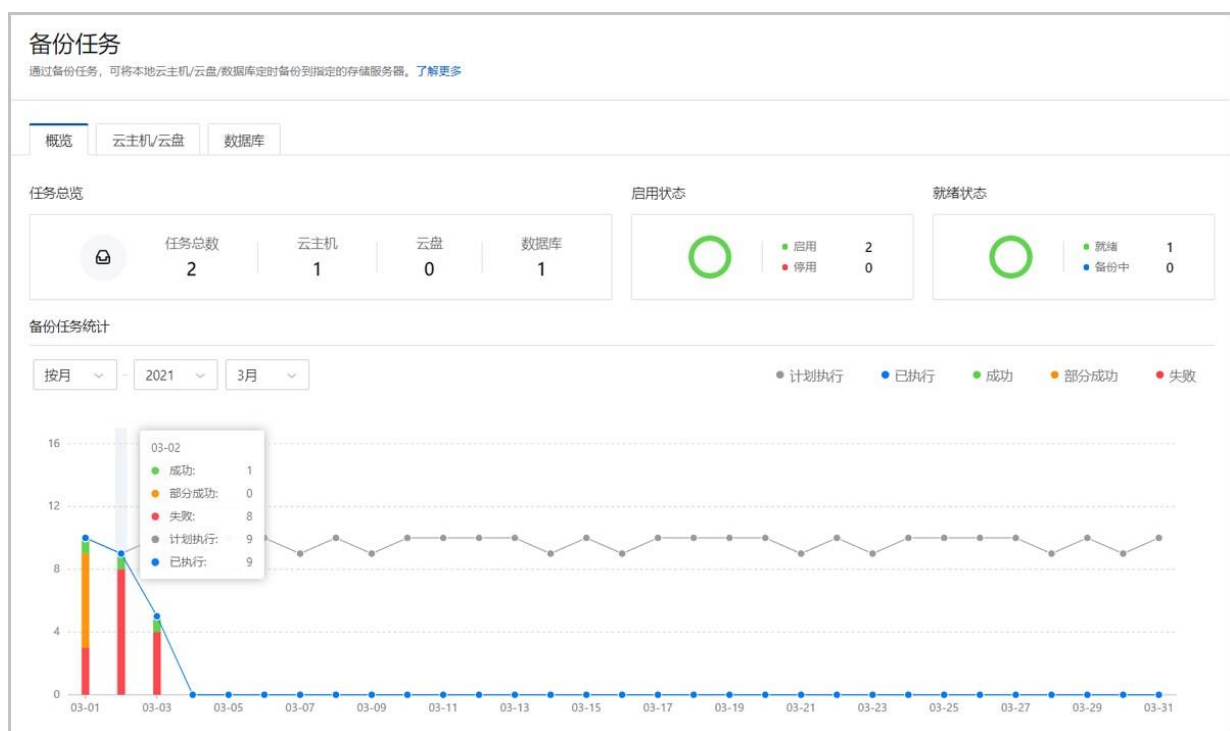
13.4.1 备份任务

备份任务概览页通过可视化视图直观展示当前云平台核心资源备份任务的数量统计、状态统计，以及执行情况统计。

在Cloud主菜单，点击**平台运维** > **灾备管理** > **备份任务**，进入**备份任务**界面，默认进入备份任务概览页面。

如图 83: 备份任务概览页所示：

图 83: 备份任务概览页



任务总览

Cloud以卡片形式展示了备份任务的数量、启用状态和就绪状态。

- 任务总览：采取总分形式，展示当前云平台已有的备份任务总数量，以及云主机、云盘、数据库各自的备份任务数量。
- 启用状态：展示备份任务启用状态，绿色表示已启用，红色表示停用。
- 就绪状态：展示备份任务就绪状态，绿色表示已就绪，蓝色表示备份中。

备份任务统计

备份任务统计以时间段为坐标横轴，备份任务数量为坐标纵轴，图形化直观展示备份任务的执行情况。

支持按年、按月或按日查看备份任务统计图表，用户可按需自行选择时间段进行查看，图表数据释义如下：

- 蓝色：表示所选时间段内，已执行完毕的备份任务数量。
- 绿色：表示所选时间段内，已执行成功的备份任务数量。
- 黄色：表示所选时间段内，对于包含多个资源的备份任务，其中部分资源备份已执行成功的备份任务数量。可在备份记录中查看具体备份结果。
- 红色：表示所选时间段内，已执行失败的备份任务数量。
- 灰色：表示所选时间段内，计划执行的备份任务数量。



注：

- 切换备份任务统计的时间段，备份记录的时间段将联动变化。
- 将光标移至统计图表中，可以展示当前日期的备份任务执行情况。

备份记录

展示当前时间段内全部备份任务的备份记录，包括：执行时间、名称、备份对象、备份方式、资源数量、任务结果和任务耗时，并支持查看备份任务详情。

如图 84: 备份任务详情所示：

图 84: 备份任务详情



任务详情					✕	
	备份数据	资源名称	任务耗时	任务结果		
>	zstack-db-4.0.0-20210303000000.gz	管理节点数据库	5秒	成功		
>	zstack-db-4.0.0-20210304000000.gz	管理节点数据库	6秒	成功		
>	zstack-db-4.0.0-20210305000000.gz	管理节点数据库	4秒	成功		
>	zstack-db-4.0.0-20210306000000.gz	管理节点数据库	5秒	成功		
>	zstack-db-4.0.0-20210307000000.gz	管理节点数据库	5秒	成功		
>	zstack-db-4.0.0-20210308000000.gz	管理节点数据库	6秒	成功		
>	zstack-db-4.0.0-20210309000000.gz	管理节点数据库	5秒	成功		
>	zstack-db-4.0.0-20210310000000.gz	管理节点数据库	5秒	成功		
第 1 项, 共 1 项					< 1 > 10 / page	

补充说明

- 备份任务概览页数据为静态数据，每次进入页面获取一次最新数据。
- 支持对灾备任务设置事件报警器，当备份任务失败时将触发报警。

云主机/云盘备份任务支持以下操作：


操作	描述
启用备份任务	将处于停用状态的备份任务启用。
停用备份任务	将处于启用状态的备份任务停用，相应资源停止定时备份行为，此时不可对其创建新的备份任务。
设置备份策略	支持对备份任务更新备份策略，包括：备份方式、备份保留策略、增量备份策略、全量备份策略（若已自定义设置）。

操作	描述
	 注： 新设置的备份策略不影响已经触发的备份任务。
设置备份服务器	设置备份任务所对应的本地备份服务器或远端备份服务器。
手动执行	支持立即执行一次当前备份任务，会在备份数据链中产生新的备份数据。 注： <ul style="list-style-type: none"> 若备份方式为：增量+系统默认全量，将手动执行一次备份任务，备份方式与即将执行的下一次备份方式相同，不支持全量备份。 若备份方式为：增量+自定义全量，勾选全量备份，将手动执行一次全量备份；若不勾选，将手动执行一次备份任务，备份方式与即将执行的下一次备份方式相同。
删除备份任务	删除备份任务，相应资源停止定时备份行为，此时可对其创建新的备份任务。 注：  <ul style="list-style-type: none"> 对于已创建备份任务的资源，不可再对其创建新的备份任务。 当删除该资源的备份任务后，则可对其创建新的备份任务。




13.4.2 本地备份数据

在Cloud主菜单，点击**平台运维 > 灾备管理 > 备份任务**，进入**备份任务**界面。

云主机/云盘备份数据支持以下操作：

操作	描述
还原备份数据	将云主机/云盘的本地备份数据恢复至本地。
同步到远端	 将云主机/云盘的备份数据同步到指定的远端备份服务器。 注： 需提前添加远端备份服务器到Cloud私有云平台，且只允许添加一个。
更改所有者	修改备份数据的所有者。
删除备份数据	删除本地云主机/云盘的本地备份数据。 注： 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，请选择 同步删除远端备份数据 。

数据库备份数据支持以下操作：

操作	描述
恢复备份数据	将本地数据库的本地备份数据还原至本地。
扫描备份数据	<p>扫描本地备份服务器，将本地备份服务器上已有的本地备份数据库获取至本地。</p> <p> 注：对于新添加的本地备份服务器，可手动执行扫描数据库备份操作，确保数据库的本地备份数据在本地备份服务器中的记录与本地记录保持一致。</p>
导出备份数据	导出本地数据库备份数据。
同步到远端	<p>将本地数据库的备份数据同步到指定的远端备份服务器。</p> <p> 注：需提前添加远端备份服务器到Cloud私有云平台，且只允许添加一个。</p>
删备份数据除	<p>删除本地数据库的本地备份数据。</p> <p> 注：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，请选择同步删除远端备份数据。</p>

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Cloud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。
- 还原云盘备份数据时，如果云盘使用Shared Block类型的主存储，需要选择置备方式，包括精简置备、厚置备
 - 精简置备：按实际使用情况分配存储空间给云盘，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给云盘，保证存储性能
- 恢复数据库后，平台所有资源会变为创建备份时的状态。请在本地备份服务器中点击“扫描备份数据”以获取当前真实备份数据信息。


13.4.3 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。
- 支持清理已被彻底删除的无效备份数据和过期的临时数据，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：

操作	描述
启用本地备份服务器	将已停用的本地备份服务器启用。
停用本地备份服务器	<p>将已启用的本地备份服务器停用。</p> <p> 注：</p> <ul style="list-style-type: none"> • 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。
重连本地备份服务器	 重连本地备份服务器，会更新本地备份服务器上备份数据在本地的记录信息。
扫描备份数据	<p>扫描云主机、云盘、数据库中未被删除的备份数据。</p> <p>注：已删除的备份数据无法通过扫描恢复。</p>
数据清理	<p>清理本地备份服务器中已被彻底删除的无效备份数据和过期的临时数据，释放存储空间。</p> <p> 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，此时执行数据清理操作可释放本地备份服务器的存储空间。</p>
修改密码	修本地备份服务器的密码。
删除本地备份服务器	将本地备份服务器删除。

操作	描述
	 注: 删除本地备份服务器会中止服务器上的备份任务，请谨慎操作。

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和过期的临时数据，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。

13.4.4 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：

操作	描述
启用远端备份服务器	将已停用的远端备份服务器启用。
停用远端备份服务器	将已启用的远端备份服务器停用。  注： 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。
修改密码	修远端备份服务器的密码。
重连远端备份服务器	重连远端备份服务器，会更新远端备份服务器上备份数据在本地的记录信息。
数据清理	清理远端备份服务器中已被彻底删除的无效备份数据和过期的临时数据，释放存储空间。  注： 例如，将某个云主机/云盘的远端备份数据彻底删除，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，就可释放远端备份服务器的存储空间。
删除远端备份服务器	将远端备份服务器删除。  注： 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。

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和过期的临时数据，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。

13.5 定时运维

Cloud提供两种定时运维服务：定时任务和定时器。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。

定时运维相关定义

- 定时任务：一种预设任务，在指定时间执行指定行为。与定时器配合使用。
 - 加载到定时器上的任务条目。
 - 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。
 - 删除定时器后，该定时器上的定时任务将被卸载，定时任务可重新加载到其它定时器上。
 - 定时任务的操作支持完整计入审计服务中。
- 定时器：承载定时任务的容器，尤其适用于长时间运行的操作。
 - 承载定时任务的容器。
 - 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。
 - 删除定时器后，该定时器上的定时任务将被卸载，定时任务可重新加载到其它定时器上。
 - 定时器的操作支持完整计入审计服务中。

注意事项

在生产环境中，建议单块磁盘的快照数量尽量控制在5以内，快照过多会影响云主机/云盘的IO性能、数据安全以及主存储容量，不建议进行高频的定时快照备份。如需长期备份，请选择灾备相关功能。




关于灾备服务的定时备份功能，详情可参考《[灾备服务使用教程](#)》。

13.5.1 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。

定时任务支持以下操作：

操作	描述
创建定时任务	创建一个新的定时任务。
编辑定时任务	编辑定时任务的名称、简介信息。

操作	描述
启用定时任务	启用处于停用状态的定时任务。  注： 启用定时任务，启动后该定时任务生效。
停用定时任务	停止选中的定时任务。  注： 停用定时任务，停用后该定时任务不生效。
加载定时器	将定时任务加载到运行的定时器上。
卸载定时器	将定时任务从定时器上卸载。
删除定时任务	删除选中的定时任务。  注： 删除该定时任务，不可恢复，请谨慎操作。

注意事项


在生产环境中，建议单块磁盘的快照数量尽量控制在5以内，快照过多会影响云主机/云盘的IO性能、数据安全以及主存储容量，不建议进行高频的定时快照备份。如需长期备份，请选择灾备相关功能。

关于灾备服务的定时备份功能。

13.5.2 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。

定时器支持以下操作：

操作	描述
创建定时器	创建一个新的定时器。
编辑定时器	编辑定时器的名称、简介信息。
删除定时器	删除选中的定时器。  注： 删除定时器后，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。

13.6 标签管理

标签：一种资源标记，便于快速搜索和资源聚合。支持对资源定制化创建标签，可通过标签类型及标签名称快速过滤出所需资源。

- 用户可根据自己的业务逻辑创建不同颜色、简约样式、精简定义的标签，并绑定到资源，通过标签快速筛选出所需资源，提高检索效率。
- 标签分为管理员标签和租户标签两种类型：
 - 管理员标签：由管理员创建，归管理员所有，支持绑定到云主机、云盘、物理机、裸金属主机、弹性裸金属实例。
 - 租户标签：由租户创建，归租户所有，支持绑定到云主机、云盘。
- 目前云主机、云盘、物理机、裸金属主机、弹性裸金属实例支持绑定/解绑标签。

标签支持以下操作：

操作	描述
创建标签	创建一个新的标签。
编辑	修改标签的名称与简介。
删除标签	删除已创建的标签。标签删除后，已绑定该标签的资源同步解绑此标签。

注意事项

- 管理员标签由管理员创建，归管理员所有，租户标签由租户创建，归租户所有。
- 租户创建的标签只能绑定到所属租户的资源，管理员标签可绑定到所有资源。
- 管理员支持解绑/删除租户标签。
- 项目内的标签归属于项目所有，项目内所有人（项目负责人/项目管理员/项目成员）均可操作。
- 标签暂不支持更改所有者操作。
- 资源更改所有者，其上所有租户标签将会解绑，管理员标签不受影响。
- 云平台无缝升级后，已有旧标签将自动更新，以最新方式展示标签。若有异常，请刷新浏览器或重新创建标签。

13.7 迁移服务

迁移服务：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。

目前支持以下类型的源平台迁移：

- 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：5.0、5.1、5.5、6.0、6.5、6.7，且vCenter服务器（vCenter Server）和ESXi主机（ESXi Host）版本需保持一致。
- 基于KVM的源云平台的云主机迁移至当前云平台。

如图 85: 迁移服务所示:

图 85: 迁移服务



功能特点

- 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单独的迁移网络以及网络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。
- 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。

注意事项

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，且需在购买企业版云平台许可证基础上使用，不可单独使用。

13.7.1 迁移任务

目前支持将VMware或KVM源云平台的云主机迁移至当前云平台。

源云平台: VMware

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。

- 迁移前，请对已接管的vCenter执行**同步数据**操作，将vCenter资源最新状态手动同步至本地。
- 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。
- 支持迁移的源vCenter平台版本包括：5.0、5.1、5.5、6.0、6.5、6.7，且vCenter服务器（vCenter Server）和ESXi主机（ESXi Host）版本需保持一致。
- 迁移的源vCenter云主机系统支持：RHEL/CentOS 4.x/5.x/6.x/7.x、SLES 11/12/15、Ubuntu 12 /14/16/18、Windows 7/Server 2003 R2/Server 2008 R2/Server 2012 R2/Server 2016。
- 云主机在V2V迁移过程中将强制关闭，注意业务影响。



注：云主机先尝试温和关闭，若失败再执行强制关闭。

- 迁移的源存储类型无限制，目标主存储支持LocalStorage、NFS、Ceph以及Shared Block类型。
- 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。
- 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。

将已接管的vCenter云主机迁移至当前云平台，需注意：

- 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。
- V2V迁移过程中，不能重启迁移服务器，否则会导致迁移任务失败。
- V2V迁移完成后，目标云主机按照源云主机光驱个数设置同样个数的光驱启动（最大允许设置3个光驱）。
- 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）。
- 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，需按照源云主机盘符顺序手动修改盘符，建议在迁移前记录源云主机盘符顺序。

- 对于带云盘的Linux/Windows云主机（云盘为SCSI模式），迁移过程中可自动识别云盘模式，迁移完成后可对目标云主机设置云盘模式。
 - Windows云主机：迁移后云盘模式默认为非VirtioSCSI。
 - Linux云主机：迁移后云盘模式默认为VirtioSCSI。

注:

若kernel版本较老，如RHEL6.2（kernel 2.x），不支持云盘为VirtioSCSI模式，迁移完成后需手动修改云盘模式为非VirtioSCSI。

例如：迁移完成后，若目标云主机无法启动，报错为无法找到硬盘，且kernel版本较老（如kernel 2.x），原因可能为老版本Virtio驱动不支持SCSI，此时需手动修改云盘模式为非VirtioSCSI，重启后可进入系统。

- 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CentOS 7.4及以上版本UEFI引导的Linux云主机，迁移后启动将进入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
```

若后续重启云主机需要绕过UEFI Shell自动进入操作系统，可执行vim /boot/efi/startup.nsh命令，创建脚本并保存以下内容：

```
FS0:
CD EFI
CD 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 > 平台设置 > 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 > 平台设置 > 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。
- V2V迁移任务的**迁移状态**总结如下：

迁移状态	备注
成功	vCenter云主机迁移至当前云平台操作成功
失败	vCenter云主机迁移至当前云平台操作失败
迁移中	<p>vCenter云主机正在迁移至当前云平台，该过程分为以下三个阶段：</p> <ol style="list-style-type: none"> 1. 数据转化：vCenter云主机文件转换格式并存储至迁移服务器缓存路径。 2. 数据下载：将迁移服务器缓存路径中的云主机文件下载至目标主存储。 3. 资源配置：在目标云平台中创建并配置对应的计算、存储、网络资源。
已取消	vCenter云主机迁移至当前云平台操作已取消

源云平台: KVM

通过创建迁移任务，可将基于KVM的源云平台的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。
- 支持对正在运行或已暂停的云主机进行迁移，待迁移的云主机请不要关机。
- 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。
- 迁移的源主存储类型无限制，目标主存储支持LocalStorage、NFS、Ceph以及Shared Block类型。
- 针对不同类型源主存储/目标主存储，libvirt和Qemu版本需满足以下要求：
 - 源主存储或目标主存储任一为Ceph类型：libvirt要求1.2.16及以上版本，Qemu要求1.1及以上版本，才可进行V2V迁移。
 - 源主存储和目标主存储均为非Ceph类型：libvirt要求1.2.9及以上版本，Qemu要求1.1及以上版本，才可进行V2V迁移。


将基于KVM的源云平台的云主机迁移至当前云平台，需注意：

- 对于高IO的云主机，为确保数据完整性，建议将其暂停后再迁移。当云主机内部进行高IO操作时，对云主机进行V2V迁移，内存中存在部分数据没有落入硬盘，V2V迁移完成后，这部分数据存在丢失风险。
- V2V迁移过程中，源云主机请不要关机。
- V2V迁移过程中，不能重启迁移服务器，否则会导致迁移任务失败。

- V2V迁移完成后，已暂停的源云主机需手动开启。
- 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。
- 用户可自行设置同一时刻最多允许运行的V2V迁移任务。
- 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。
- V2V迁移任务的**迁移状态**总结如下：

迁移状态	备注
成功	基于KVM的源云平台的云主机迁移至当前云平台操作成功
失败	基于KVM的源云平台的云主机迁移至当前云平台操作失败
迁移中	<p>基于KVM的源云平台的云主机正在迁移至当前云平台，该过程分为以下三个阶段：</p> <ol style="list-style-type: none"> 1. 数据转化：基于KVM的源云平台的云主机文件转换格式并存储至迁移服务器缓存路径。 2. 数据下载：将迁移服务器缓存路径中的云主机文件上传至目标主存储。 3. 资源配置：在目标云平台中创建并配置对应的计算、存储、网络资源。
已取消	基于KVM的源云平台的云主机迁移至当前云平台操作已取消

迁移任务支持以下操作：

操作	描述
重启迁移任务	<p>迁移任务执行失败后，可将其重新启动。</p> <p>注：</p> <ul style="list-style-type: none"> • 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。 <p> 用户可自行设置迁移数据缓存留存时限，设置方法：</p> <p>进入设置 > 平台设置 > 全局设置 > 高级设置 > 平台运维 > 迁移服务，设置V2V迁移数据缓存留存时限即可，默认为86400秒（即1天）。</p>


操作	描述
编辑	编辑迁移任务的名称和简介。
删除迁移任务	迁移任务执行完成后，可将其删除。

13.7.2 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 16: 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。

- 迁移服务器类型需与迁移任务源云平台类型保持一致。
- 支持对迁移服务器设置单独的迁移网络以及网络QoS，控制传输瓶颈，提高迁移效率。

迁移服务器支持以下操作：

操作	描述
启用迁移服务器	将已停用的迁移服务器启用。
停用迁移服务器	 将已启用的迁移服务器停用。 注： 若在V2V迁移任务执行过程中将迁移服务器停用，迁移任务不受影响。
设置网络带宽	设置迁移服务器的上行/下行带宽。
删除迁移服务器	 将迁移服务器删除。 注： <ul style="list-style-type: none"> 删除本地备份服务器，将中止该服务器上的备份任务。

操作	描述
	<ul style="list-style-type: none">删除本地备份服务器，将删除服务器上备份数据的本地记录，真实数据不受影响。但重新添加此本地备份服务器，备份数据的本地记录无法自行恢复，请谨慎操作。

注意事项

- 创建迁移任务时，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。
- 迁移服务器类型需与迁移任务源云平台类型保持一致。
- 同一台物理机，不允许既作为VMware平台类型的迁移服务器，又作为KVM平台类型的迁移服务器。
- 若已选择多台湾云主机，则相应创建的多个迁移任务均使用这台迁移服务器。
- V2V迁移过程中，云主机系统和数据先缓存在迁移服务器中，再导入目标主存储。
- 若在V2V迁移任务执行过程中将迁移服务器停用，迁移任务不受影响。
- 删除迁移服务器会导致正在执行的迁移任务自动取消，已迁移完成的资源不受影响。

14 运营管理

14.1 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，且需在购买企业版云平台许可证基础上使用，不可单独使用。

企业管理相关定义

- 人员与权限：企业管理体系以人员和权限为基础进行构建，根据实际需求搭建部门与角色，对用户赋予多样化的权限。
- 组织架构：企业管理中的基本单位，由自定义创建或通过第三方认证同步，分为未分组部门和自定义部门，支持自定义新团队和子部门。其中，新团队通常指一个公司或者子公司，其下可创建多级部门。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。



注：项目成员仅支持查看所在团队的组织架构树。

- 用户：表示自然人，是企业管理中的最基本单位。Cloud云平台用户包括本地用户和第三方用户：
 - 本地用户：云平台中创建的用户，支持加入组织、加入项目、绑定角色等操作。
 - 第三方用户：通过第三方认证同步到云平台的用户，支持加入组织、加入项目、绑定角色、变更为本地用户等操作。



注：

- 企业管理用户需从项目登录入口登录云平台，其中本地用户从本地用户入口登录；第三方用户从AD/LDAP入口登录。
- admin/平台管理员支持查看所有用户列表。
- 若云平台已创建组织架构树，平台成员仅支持查看所属组织架构的用户列表；若云平台未创建任何组织架构树，平台成员支持查看所有用户。
- 成员组：有双重含义，既表示一组自然人的集合，也表示一组项目成员的集合，支持以成员组为单位进行权限控制。

- 角色：权限的集合，为用户和成员组赋予权限可获得调用相关API进行资源操作的能力。包括平台角色和项目角色两类。
 - 平台角色：用户绑定平台角色后，将拥有对应区域的管理权限。平台角色的权限仅在用户自身管控的区域内生效。
 - 项目角色：用户加入项目并绑定项目角色后，将拥有该项目的使用权限，管控项目内的数据。



注：

- 同一用户支持同时绑定两种角色类型。
- 同一用户支持绑定多个平台角色或项目角色。
- 在一个项目内，若用户绑定了多个项目角色，拥有的权限为所有项目角色的全集。
- 第三方认证：云平台提供的第三方登录认证服务，支持无缝接入第三方登录认证系统，相应账户系统将直接登录云平台，便捷使用云资源，目前支持添加AD/LDAP服务器。
 - AD认证：

AD (Active Directory) 是面向Windows Standard Server、Windows Enterprise Server以及Windows Datacenter Server的目录服务，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。

通过AD服务器可将AD用户/组织同步到Cloud云平台用户列表/组织架构，并支持使用指定的AD登录属性直接登录Cloud云平台。
 - LDAP认证：

LDAP (Lightweight Directory Access Protocol) 是轻量目录访问协议，可提供标准的目录服务，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。

通过LDAP服务器可将LDAP用户同步到Cloud云平台用户列表，并支持使用指定的LDAP登录属性直接登录Cloud云平台。
- 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。
- 项目：项目是租户的一种，指在特定时间、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。
 - 创建项目需指定资源配额、回收策略，添加项目成员等。

- 云平台内的基本资源（计算规格、镜像、网络等），建议提前共享或创建。
- 工单审批：为了更高效地为每个项目提供基础资源支持，项目成员（项目负责人/项目管理员/普通项目成员）可对云平台资源提出工单申请，根据每个项目自定义工单审批流程，对工单进行审批，最终由admin或项目负责人审批，支持申请云主机、删除云主机、修改云主机配置、修改项目周期和修改项目配额五种工单类型。
- 流程管理：为了更高效对项目提供基础资源支持，工单审批引入流程管理，包括默认流程和自定义流程两种类型。
 - 默认流程：项目成员提交工单--->admin审批工单。此流程适用于以下几种场景：
 - 未设置工单流程的工单，将使用默认流程提交工单。
 - 修改项目周期类型的工单，将使用默认流程提交工单。
 - 修改项目配额类型的工单，将使用默认流程提交工单。
 - 删除自定义工单流程，将使用默认流程自动重新提交工单。
 - 自定义流程：项目成员提交工单--->自定义审批工单--->admin/项目负责人审批工单。此流程适用于以下几种场景：
 - 申请云主机、删除云主机、修改云主机配置类型的工单，优先使用设置的自定义工单流程提交工单。
 - 修改有效状态的工单流程，将使用修改后的自定义工单流程自动重新提交工单。
 - 修改已失效状态的工单流程，需要使用修改后的自定义工单流程手动重新提交工单。
- 我的审批：仅admin/项目负责人拥有审批权限，可通过或驳回申请。若审批通过，资源会自动部署并下发至项目生效。



注：平台管理员/普通平台成员没有工单审批权限，暂无我的审批菜单。

账号体系相关定义

- admin：超级管理员，拥有所有权限，通常由IT系统管理员拥有。
- 本地用户：云平台中创建的用户，支持加入组织、加入项目、绑定角色等操作。
- 第三方用户：通过第三方认证同步到云平台的用户，支持加入组织、加入项目、绑定角色、变更为本地用户等操作。
- 平台成员：绑定了平台角色的用户，包括平台管理员和普通平台成员。
- 平台管理员：绑定平台管理员角色的用户，带有区域属性的管理员，拥有全部的界面权限，管控所分配区域的数据中心。

- 部门负责人：组织架构中负责管理部门的用户，拥有查看部门账单权限。
- 项目成员：加入项目的用户，作为项目的基本组成人员，包括项目负责人、项目管理员和普通项目成员。
- 项目负责人：拥有项目负责人角色的用户，负责管理项目内的用户，在项目中拥有最高权限。
- 项目管理员：拥有项目管理员角色的用户，协助项目负责人管理项目，同一项目可指定一个或多个项目成员作为项目管理员。
- 根角色：根角色用于限制自定义角色的权限范围，自定义角色的权限继承自根角色，为根角色权限的子集。
- 配额：配额是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。
- 项目回收策略：创建项目需指定项目回收策略，包括无限制、指定时间回收和指定费用回收三种。
 - 无限制：创建项目后，项目内资源默认一直处于启用状态。
 - 指定时间回收：
 - 项目有效期限不足14天时，项目成员登录云平台后智能操作助手将弹出**项目即将过期**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：禁止项目成员登录、禁止项目成员登录且停止项目资源、删除项目。
 - 指定费用回收：项目费用达到限额时，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：禁止项目成员登录、禁止项目成员登录且停止项目资源、删除项目。

平台/项目身份权限

- 平台身份：包括admin、平台管理员、普通平台成员，权限上存在略微差异，如下：

名称	区别
admin	超级管理员，拥有所有权限。
平台管理员	<p>平台管理员主要是带有区域属性的管理员，协助admin共同管理云平台。除以下权限外，平台管理员拥有和admin同样的权限：</p> <ul style="list-style-type: none"> • 带有区域属性，仅支持管控所属区域内的资源，且不支持创建区域、删除区域相关权限。 • 不支持工单审批相关权限，我的审批菜单不可见。 • 不支持许可证管理相关权限，不支持上传许可证等操作。

名称	区别
普通平台成员	<p>平台管理员以外的平台成员，除以下权限外，普通平台成员拥有和admin同样的权限：</p> <ul style="list-style-type: none"> 不支持工单审批相关权限，我的审批菜单不可见。 仅支持查看所属组织架构的用户。 未赋予的权限。

- 项目身份：包括项目负责人、项目管理员、项目成员，权限如下：
 - 项目负责人可指定一个或多个项目成员作为项目管理员，协助管理项目。
 - 除项目负责人可对项目管理员进行管控外，项目管理员拥有和项目负责人相同的全部权限。

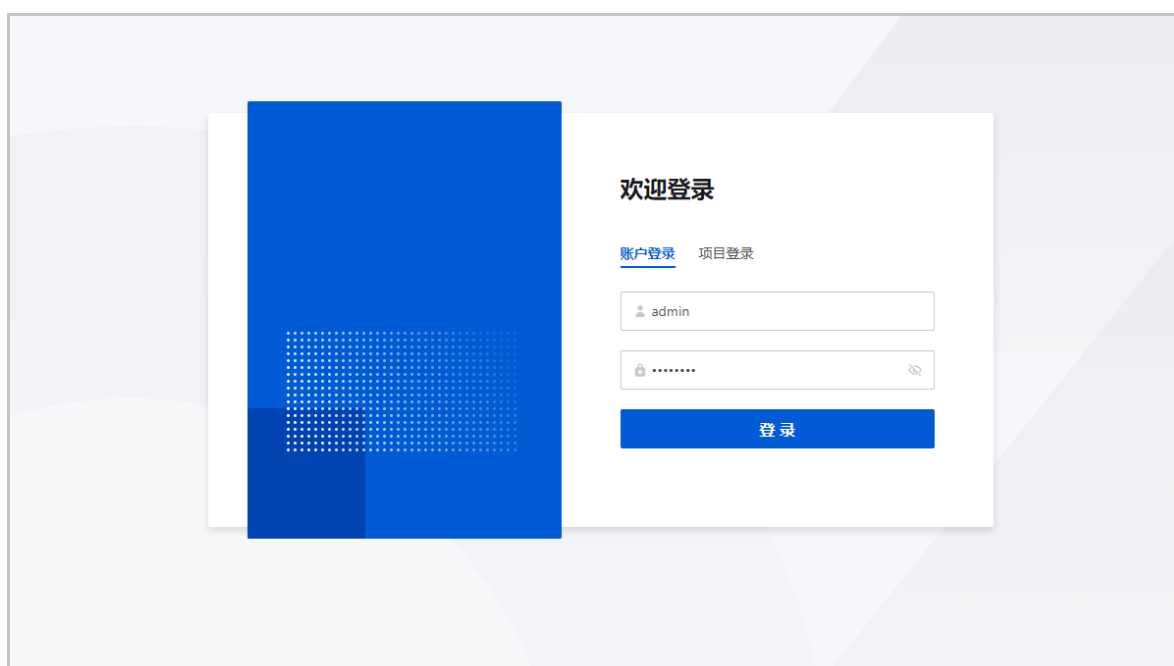
企业管理各账号登录云平台

- 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://management_node_ip:5000/#/login），admin输入相应用户名和密码登录云平台。如

图 86: 主登录页面所示:

图 86: 主登录页面



- 企业管理中的用户（平台管理员/平台成员/项目负责人/项目管理员/普通项目成员）从项目登录入口登录云平台

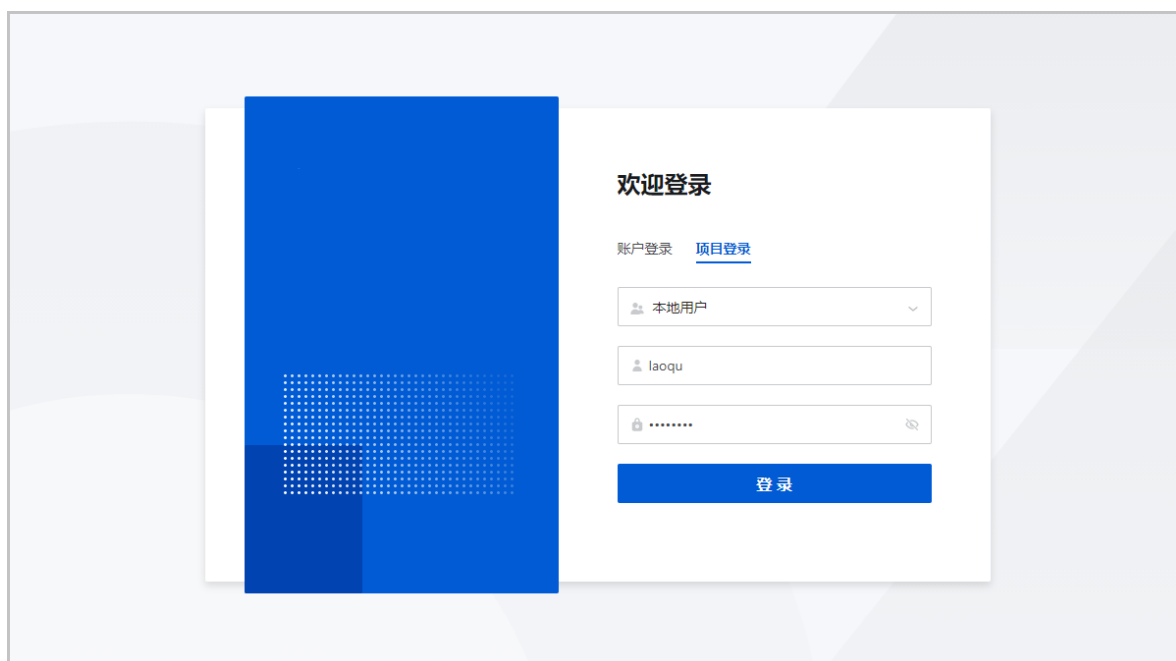
使用Chrome浏览器或FireFox浏览器打开项目登录界面（http://management_node_ip:5000/#/project），输入相应用户名和密码登录云平台。其中，包括两种入口：

- 本地用户：云平台创建的用户，通过本地入口登录。
- AD/LDAP用户：通过第三方认证同步到云平台的第三方用户，通过AD/LDAP用户入口登录。

登录成功后，选择需要管理的平台或项目，即可登录到对应的管理界面。

如图 87: 项目登录页面所示：

图 87: 项目登录页面



企业管理子功能

企业管理主要包括**平台管理**、**项目管理**、**工单管理**、**独立区域管理**、**第三方认证**子功能。

• 平台管理：

为了更高效地管理云平台，平台成员（平台管理员/普通平台成员）可配合超级管理员共同维护云平台。Cloud提供平台管理员角色、监控大屏角色等系统角色方便用户使用，也可创建自定义角色满足各种使用场景，细粒度到API级别。

• 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。

- **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（项目负责人/项目管理员/普通项目成员）可对云平台资源提出工单申请，根据每个项目自定义工单审批流程，对工单进行审批，最终由admin或项目负责人审批，支持申请云主机、删除云主机、修改云主机配置、修改项目周期和修改项目配额五种工单类型。

- **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。

- **第三方认证:**

第三方认证是Cloud云平台提供的第三方登录认证服务，支持无缝接入第三方登录认证系统，相应账户系统可通过云平台登录页面直接登录，便捷使用云资源，目前支持添加AD/LDAP服务器。

企业管理使用流程

可参考以下步骤使用企业管理功能:

1. admin创建组织架构树;
2. admin创建用户并将用户加入对应的组织架构;
3. admin指定部门负责人;
4. admin全局共享基本资源;
5. admin创建项目并指定项目负责人;
6. 项目负责人创建自定义角色;
7. 项目负责人为项目添加成员并绑定角色;
8. 登录云平台。

14.1.1 组织架构

企业管理为企业用户提供组织架构管理功能，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。主要涉及以下概念:

- **组织:**

组织是企业管理中组织架构的基本单位，由自定义创建或通过第三方认证同步，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。

- **用户:**

表示自然人，是企业管理中的最基本单位，拥有平台管理员、项目管理员、部门负责人等多种属性。

• 部门负责人：

组织架构中负责管理部门的用户，拥有查看部门账单权限。

组织架构树

- 组织架构树以层级折叠方式展示，可直观查看企业组织架构全貌。
- 组织可分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门。
- 组织架构树中，顶级部门/部门的部门负责人图标右下角有红色五角星标识。
- 通过第三方认证同步的组织，单独创建一棵组织架构树。
- 支持添加多个组织架构树：不同组织架构树中的用户相互不可见。
- admin/平台管理员支持查看所有组织架构树；平台成员仅支持查看所属组织架构树。

组织架构支持以下操作：

操作	描述
添加子部门	在组织架构中添加新的子部门。
编辑	修改组织架构的名称和简介。
更换部门负责人	重新指定部门负责人。
移动部门	更改子部门的上级部门。
添加成员	添加新的成员到组织。
移除成员	将成员从组织移除。  注： 若该成员为部门负责人，从部门移除将同时移除部门负责人身份。
加入项目	添加成员至指定项目中。
删除	删除当前组织架构。  注： 删除部门将同时删除其下所有子部门，请谨慎操作。

注意事项

不同视角对组织架构树的可见程度略有区别：

- admin/平台管理员支持查看所有组织架构树。

- 普通平台成员/项目负责人/项目管理员仅支持查看所属组织架构树。
- 普通项目成员不可查看组织架构树。

14.1.2 用户

用户表示自然人，是企业管理中的最基本单位，拥有平台管理员、项目管理员、部门负责人等多种属性。

Cloud云平台用户有两种分类方式：

- 方式一：根据来源分类

- 本地用户：

云平台中创建的用户，支持加入组织、加入项目、绑定角色等操作。

- 第三方用户：

通过第三方认证同步到云平台的用户，支持加入组织、加入项目、绑定角色、变更为本地用户等操作。



注：企业管理用户需从项目登录入口登录云平台，其中本地用户从本地用户入口登录；第三方用户从AD/LDAP入口登录。

- 方式二：根据是否加入项目分类

- 平台成员：


未加入项目的用户，包括平台管理员和普通平台成员。

- 项目成员：



加入项目的用户，作为项目的基本组成人员，包括项目负责人、项目管理员和普通项目成员。

本地用户支持以下操作：

操作	描述
创建用户	基于员工基本信息创建用户。
编辑	修改名称和简介。
修改密码	修改用户登录密码。
加入部门	将用户加入到一个或多个部门。
加入成员组	将用户加入到一个或多个成员组。

操作	描述
修改平台角色	为用户绑定一个或多个平台角色。
加入项目	将用户加入到一个或多个项目。
设置管理区域	设置用户所管理的区域，设置后，用户将只可管控指定的区域。
删除	<p>将用户删除</p> <p> 注:</p> <ul style="list-style-type: none"> 若删除用户为部门负责人/项目负责人/项目管理员，移除用户将同时移除部门负责人/项目负责人/项目管理员身份。 若删除用户属于工单流程环节，从项目移除用户后工单流程将不可用，且该流程相关工单全部撤回。

第三方用户支持以下操作：

操作	描述
加入部门	将用户加入到一个或多个部门。
加入成员组	将用户加入到一个或多个成员组。
修改平台角色	为用户绑定一个或多个平台角色。
加入项目	将用户加入到一个或多个项目。
设置管理区域	设置用户所管理的区域，设置后，用户将只可管控指定的区域。
变更为本地用户	<p>同步AD服务器后不存在的用户将变更为已删除状态并无法登录，此时支持变更为本地用户操作，将已删除状态的AD用户变更为云平台本地用户。</p> <p> 注:</p> <ul style="list-style-type: none"> 变更为本地用户后，继承用户原有数据，例如：所在项目、拥有的权限等可以继续使用。 变更为本地用户后，需要在本地用户列表执行修改密码操作，即可正常登录云平台。
删除	<p>将用户删除</p> <p> 注:</p> <ul style="list-style-type: none"> 若删除用户为部门负责人/项目负责人/项目管理员，移除用户将同时移除部门负责人/项目负责人/项目管理员身份。

操作	描述
	<ul style="list-style-type: none"> 若删除用户属于工单流程环节，从项目移除用户后工单流程将不可用，且该流程相关工单全部撤回。

注意事项

- admin/平台管理员支持查看所有用户列表。
- 若云平台已创建组织架构树，平台成员仅支持查看所属组织架构的用户列表；若云平台未创建任何组织架构树，平台成员支持查看所有用户。
- 若云平台已创建组织架构树，项目负责人/项目管理员仅支持查看所在组织架构树的用户。
- 若云平台未创建任何组织架构树，项目负责人/项目管理员支持查看所有用户。
- 模板导入方式创建用户需要注意以下情况：
 - 组织架构必须为已有组织，输入格式：以符号"/"分隔，例如Company/Dev；
 - 若组织架构路径重复，附带顶级部门uuid，例如Company(f11444d42701483791370e9f8b9300b9)/Dev；
 - 同时加入多个组织，以"&&"分隔，例如Company/Dev&&Company/QA。
 - 项目必须为已有项目，加入单个项目时，直接输入项目名称，例如project-01；
 - 同时加入多个项目，以"&&"分隔，例如project-01&&project-02。

14.1.3 成员组

在Cloud主菜单，点击**运营管理** > **企业管理** > **人员与权限** > **成员组**，进入**成员组**界面。

成员组支持以下操作：

操作	描述
创建成员组	创建成员组，对成员进行分组管理。
编辑	修改名称和简介。
添加用户	为成员组添加用户。
加入项目	将成员组加入指定项目。
删除	删除成员组，将解除相应成员间的组关系。

14.1.4 角色

角色表示权限的集合，为用户赋予权限可获得调用相关API进行资源操作的能力。包括系统角色和自定义角色两类。


- **系统角色：**

系统角色是云平台预置的特殊角色，随版本升级更新权限内容，并自动勾选相关新增权限，不支持手动配置。

- **自定义角色：**

自定义角色是自定义创建的角色，随版本升级自动更新权限内容，升级后的新增权限需要手动配置。

角色支持以下操作：

操作	描述
创建角色	创建一个新的角色。
编辑	修改名称和简介。
修改界面权限	修改角色的界面权限。
删除	删除角色。  注： 删除角色后，相关用户将自动解绑此角色，请谨慎操作。

14.1.5 第三方认证

第三方认证是Cloud云平台提供的第三方登录认证服务，支持无缝接入第三方登录认证系统，相应账户系统将直接登录云平台，便捷使用云资源，目前支持添加AD/LDAP服务器。

- **AD认证：**

AD (Active Directory) 是面向Windows Standard Server、Windows Enterprise Server以及Windows Datacenter Server的目录服务，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。



通过AD服务器可将AD用户/组织同步到Cloud云平台用户列表/组织架构，并支持使用指定的AD登录属性直接登录Cloud云平台。

- **LDAP认证：**

LDAP (Lightweight Directory Access Protocol) 是轻量目录访问协议，可提供标准的目录服务，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。

通过LDAP服务器可将LDAP用户同步到Cloud云平台用户列表，并支持使用指定的LDAP登录属性直接登录Cloud云平台。

第三方认证服务器支持以下操作：

操作	描述
编辑	修改名称和简介。
同步	同步第三方认证服务器将重新获取最新用户列表及组织架构。  注： 同步后不存在的用户将变更为已删除状态并无法登录。
测试连接	检查第三方认证服务器的连通性，若连接失败，可能存在以下原因： <ul style="list-style-type: none"> 第三方认证服务器IP端口验证失败，请检查第三方认证服务器是否正常工作以及是否有IP或端口变更。 用户DN或密码连接失败，请更换最新拥有查询基本DN范围内所有用户权限的用户DN及密码。
删除	删除添加的第三方认证服务器。  注： 删除第三方认证服务器将同时删除同步到云平台的第三方用户/组织，源第三方认证服务器中的用户/组织不受影响。

14.1.6 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：项目是租户的一种，指在特定时间、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。
 - 创建项目需指定资源配额、回收策略，添加项目成员等。

- 云平台内的基本资源（计算规格、镜像、网络等），建议提前共享或创建。
- 项目成员：加入项目的用户，作为项目的基本组成人员，包括项目负责人、项目管理员和普通项目成员。
- 项目负责人：拥有项目负责人角色的用户，负责管理项目内的用户，在项目中拥有最高权限。
- 项目管理员：拥有项目管理员角色的用户，协助项目负责人管理项目，同一项目可指定一个或多个项目成员作为项目管理员。
- 配额：配额是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。
- 项目回收策略：创建项目需指定项目回收策略，包括无限制、指定时间回收和指定费用回收三种。
 - 无限制：创建项目后，项目内资源默认一直处于启用状态。
 - 指定时间回收：
 - 项目有效期限不足14天时，项目成员登录云平台后智能操作助手将弹出**项目即将过期**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：禁止项目成员登录、禁止项目成员登录且停止项目资源、删除项目。
 - 指定费用回收：项目费用达到限额时，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：禁止项目成员登录、禁止项目成员登录且停止项目资源、删除项目。

项目支持以下操作：

操作	描述
创建项目	创建新的项目。
编辑	修改名称和简介。
启用项目	将已停用的项目启用。
停用项目	将启用的项目停用。
停止所有资源	停止项目资源将停止项目内所有云主机和路由器资源，但项目仍可正常登录，请谨慎操作。
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。
添加用户	为项目添加用户。

操作	描述
设置部门	项目加载部门后，支持查看部门账单，移除部门会将项目账单将从部门账单中移除。
更换计费价目	为项目更换计费价目，并使用更换后的价目进行计费。
设置项目负责人	设置项目的负责人。
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。
删除	<ul style="list-style-type: none"> 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。 项目内的VPC路由器停止后，其上的网络服务将停止，云主机将不能访问外网。


14.1.7 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（项目负责人/项目管理员/普通项目成员）可对云平台资源提出工单申请，根据每个项目自定义工单审批流程，对工单进行审批，最终由admin或项目负责人审批，支持申请云主机、删除云主机、修改云主机配置、修改项目周期和修改项目配额五种工单类型。

工单流程支持以下操作：

操作	描述
创建工单流程	创建一个新的工单流程。
编辑	修改名称和简介。
启用工单流程	启用工单流程，此时该工单流程可用。
停用工单流程	停用工单流程，此时该工单流程不可用。工单流程停用后，未走完的工单将不可操作，重新启用后恢复操作。
修改工单流程	<p>支持增加或删除工单类型；支持添加或移除工单流程环节。</p> <p> 注：</p> <ul style="list-style-type: none"> 修改有效状态的工单流程，将使用修改后的自定义工单流程自动重新提交工单。

操作	描述
	<ul style="list-style-type: none"> 修改已失效状态的工单流程，需要使用修改后的自定义工单流程手动重新提交工单。 删除工单流程中工单类型，等同于删除此类型的自定义工单流程，修改后将使用默认流程自动重新提交工单。 为工单流程新增工单类型，等同于为此类型的工单新建自定义工单流程，修改后将使用自定义工单流程重新提交工单。
删除	工单流程删除后，使用此流程的项目将使用默认流程(提交->admin)，所有正在使用此流程的工单将按默认流程重新提交。

工单审批：

我的审批界面分为**待办事项**、**已办事项**、**已归档**三个子页面：

- 待办事项：

该页面显示待处理的工单，可审批通过或驳回申请；

- 已办事项：

该页面显示已处理的工单，审批通过或驳回的工单均属于已处理工单；

- 已归档：

该页面显示已归档的工单，项目成员删除已处理的工单后，admin可在已归档页面查看该条工单信息。

admin可在**我的审批**界面处理工单，可选择通过或驳回

- 通过：通过工单，系统将按配置自动创建资源给申请人



注：部署资源过程中，支持admin对资源进行高级设置。

- 驳回：驳回工单，可标注驳回原因

14.2 计费管理

14.2.1 计费价目

计费价目：一张包含不同资源计费单价的集合表，资源单价基于资源规格、资源使用时间而设置。

Cloud提供准公有云计费方式体验，将各资源计费单价汇总为一份计费价目，绑定到项目/账户即可按量生成计费账单。目前支持计费的资源类型包括：处理器、内存、根云盘、数据云盘、GPU设备、公网IP（云主机IP）、公网IP（虚拟IP）。

计费价目注意事项

- 一条计费价目支持绑定到多个项目/账户；同一项目/账户只能且必须绑定一条计费价目。
- 系统提供一条默认计费价目，不支持删除。升级云平台场景，将根据原有计费设置自动创建默认计费价目并绑定所有项目/账户。
- 默认计费价目暂不支持删除。
- 正在被项目/账户使用的计费价目无法删除，请为所有相关项目/账户更换计费价目再执行此操作。
- 公网IP需设置QoS才可按计费单价进行计费。
- IPv6类型的虚拟IP暂不支持计费。
- 计费价目支持通过高级参数方式对根云盘/数据云盘按照磁盘性能计费，其配置条目依赖计算规格/云盘规格高级参数中的`priceUserConfig`信息，请确保配置严格一致，否则不能生成计费账单。
- 删除截止至今的价目历史，将删除价目记录；同时，相关账单立即生成一次且不再继续计费。
- 删除其他价目历史，仅删除价目记录，不影响计费和账单生成。

14.2.2 账单

账单：按计费价目在指定时间段统计的资源费用，计费精确至秒级。账单类型包括：项目账单、部门账单、账户账单。

包括以下几种形式的账单：

- 汇总账单
- 资源账单
- 账单明细

汇总账单

在Cloud主菜单，点击**运营管理 > 计费管理 > 账单**，进入**账单**界面。

如图 88: 汇总账单所示：

图 88: 汇总账单

计费账户	总额	处理器/内存	根云盘	数据云盘	GPU设备	公网IP (云主机IP)	公网IP (虚拟机IP)
子账户-B	¥ 9.90	¥ 0.00	¥ 0.00	¥ 0.00	¥ 0.00	¥ 0.00	¥ 9.90
子账户-A	¥ 4.03	¥ 4.02	¥ 0.00	¥ 0.00	¥ 0.00	¥ 0.01	¥ 0.00
admin	¥ 0.00	¥ 0.00	¥ 0.00	¥ 0.00	¥ 0.00	¥ 0.00	¥ 0.00

第 1-3 项, 共 3 项

汇总账单显示指定时间段内项目/部门/账户的计费账单，方便用户快速了解近期消费情况。

默认显示一周内（截至当前时刻7天内）的计费账单，支持选择不同的时间段或自定义时间段查看账单。可选的时间段包括：最一周内（截至当前时刻7天内）、一月内（截至当前时刻30天内）、三月内（截至当前时刻90天内）。

- 项目：以列表方式实时显示指定时间段内不同项目的计费账单。



注：

- 项目账单依赖企业管理模块License，请提前获取并安装。
- 为项目绑定计费价目并以资源为单位设置计费单价，即可开始计费并生成项目账单。
- admin/平台成员/项目成员支持查看项目账单。
- 部门：以组合列表方式实时显示指定时间段内不同部门的计费账单。



注：

- 部门账单依赖企业管理模块License，请提前获取并安装。
- 项目加载到部门即可获取项目相关计费数据（包括历史费用）并按部门生成账单。
- 计费数据与项目直接相关，部门卸载项目后，相关计费数据（包括历史费用）将全部从部门账单移除。
- admin/平台成员/部门负责人支持查看部门账单。
- 账户：以列表方式实时显示指定时间段内不同账户的计费账单。



注：

- 为账户绑定计费价目并以资源为单位设置计费单价，即可开始计费并生成账户账单。
- admin/平台成员/账户支持查看账户账单。

Cloud对接管的vCenter支持多租户管理，普通账户支持分别展示KVM和vCenter的计费账单。

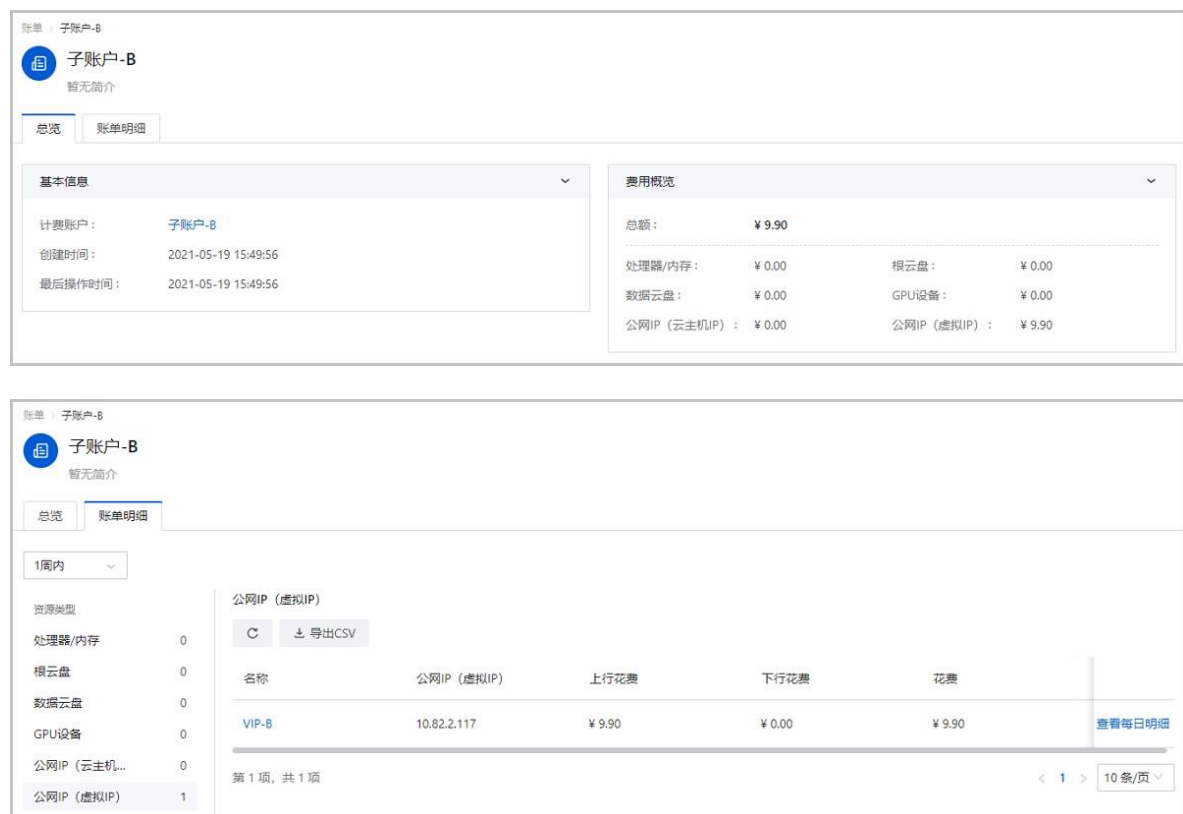
Cloud对接管的vCenter支持多租户管理，项目成员支持分别展示KVM和vCenter的计费账单。

资源账单

以资源列表方式查看账单，包括以下情况：

- 项目/账户详情页支持查看账单总览和账单明细。**账单明细**子页面支持以资源为粒度查看资源账单，如图 89: 账单总览和账单明细所示：

图 89: 账单总览和账单明细



账单总览

子账户-B
暂无简介

总览 账单明细

基本信息

计费账户: 子账户-B
创建时间: 2021-05-19 15:49:56
最后操作时间: 2021-05-19 15:49:56

费用概览

总额: ¥ 9.90

处理器/内存: ¥ 0.00 根云盘: ¥ 0.00
数据云盘: ¥ 0.00 GPU设备: ¥ 0.00
公网IP (云主机IP): ¥ 0.00 公网IP (虚拟IP): ¥ 9.90

账单明细

1周内

资源类型

处理器/内存 0
根云盘 0
数据云盘 0
GPU设备 0
公网IP (云主机IP) 0
公网IP (虚拟IP) 1

公网IP (虚拟IP)

名称 公网IP (虚拟IP) 上行花费 下行花费 花费

VIP-B 10.82.2.117 ¥ 9.90 ¥ 0.00 ¥ 9.90

第 1 项, 共 1 项

10 条/页

注:

- 区别于实时计费，账单明细采用定时输出账单方式。默认每天零点生成一次账单，用户可自行设置账单生成时刻。设置方法：
进入**设置 > 平台设置 > 全局设置 > 高级设置 > 运营管理 > 计费账单**，设置**账单生成触发时刻**即可，默认为零点。
- 普通账户/项目成员支持查看账单详情，与admin视角类似，可以查看本账户内处理器、内存、根云盘、数据云盘、GPU设备、公网IP（云主机IP）、公网IP（虚拟IP）的账单明细。
- 部门详情页分为两个部分：
 - 费用概览**：支持查看直属项目计费和下级部门计费

— 直属项目账单明细：支持以项目列表方式查看直属项目账单

如图 90: 部门账单详情页所示：

图 90: 部门账单详情页

项目	部门	账户
资料部	1周内	
费用概览		
总额 ¥ 26.69	处理器/内存： ¥ 26.69	根云盘： ¥ 0.00
	GPU设备： ¥ 0.00	数据云盘： ¥ 0.00
	公网IP（云主机IP）： ¥ 0.00	公网IP（虚拟IP）： ¥ 0.00
	直属项目计费： ¥ 26.69	下级部门计费： ¥ 0.00
直属项目账单明细		
导出CSV		
计费项目	总额	处理器/内存
项目-3	¥ 26.69	¥ 26.69
		根云盘
		数据云盘
		GPU设备
		公网IP（云主机IP）
		公网IP（虚拟IP）
第 1 项，共 1 项		10 条/页



注：

- 直属项目计费：仅显示加载到此部门中所有项目的计费总额。
- 下级部门计费：所有下级部门中加载项目的计费总和。

账单明细

项目/账户支持指定资源查看账单明细，点击资源账单后面的[查看每日明细](#)即可查看。

如图 91: 账单明细所示：

图 91: 账单明细

账单	子账户-B
子账户-B	暂无简介
总览	账单明细
1周内	
资源类型	公网IP（虚拟IP）
处理器/内存	0
根云盘	0
数据云盘	0
GPU设备	0
公网IP（云主机...）	0
公网IP（虚拟IP）	1
	导出CSV
名称	公网IP（虚拟IP）
上行花费	下行花费
花费	
VIP-B	10.82.2.117
¥ 9.90	¥ 0.00
¥ 9.90	
查看每日明细	
第 1 项，共 1 项	10 条/页

账单明细			
每日明细: VIP-8			
C 上行带宽 下行带宽 1周内 导出CSV			
开始时间	截止时间	上行带宽	花费
2021-05-19 15:55:28	2021-05-19 16:12:22	2.93 Gbps	¥ 9.90
第 1 项, 共 1 项 < 1 > 10 条/页			



注:

- 区别于实时计费，账单明细采用定时输出账单方式。默认每天零点生成一次账单，用户可自行设置账单生成时刻。设置方法：

进入**设置 > 平台设置 > 全局设置 > 高级设置 > 运营管理 > 计费账单**，设置**账单生成触发时刻**即可，默认为零点。

- 项目/账户更换计费价目，相关资源将立即生成一次账单。
- 删除计费价目中截止至今的历史价目，相关资源将立即生成一次账单。
- 普通账户/项目成员支持查看账单详情，与admin视角类似，可以查看本账户内云主机、根云盘、数据云盘、GPU设备、公网IP（云主机IP）、公网IP（虚拟IP）的账单明细。

补充说明

- 若在全球设置中关闭**计费功能开关**，系统将停止对资源进行计费，关闭后不再生成新的账单。
- 云主机已删除但未彻底删除时，将立即释放计算资源（处理器、内存）和IP资源（云主机IP）。因此，处理器、内存、公网IP资源不再进行计费。
- 云主机/云盘已删除但未彻底删除时，仍占据物理存储资源（根云盘/数据云盘）。因此，根云盘/数据云盘将继续计费直至被彻底删除。
- 停止状态的云主机依然占用存储资源和IP资源。因此，根云盘、数据云盘、公网IP将继续进行计费。
- 未实例化的云盘不进行计费，一旦被实例化即刻开始计费。例如：某账户/项目名下的数据云盘已实例化但未被加载到云主机，依然进行计费。
- 更改资源所有者操作：以更改时间为分割点，更改前的费用保留于旧账户/项目，更改后在新账户/项目进行计费。

14.3 访问控制

14.3.1 AccessKey管理

AccessKey管理：访问云平台API的身份凭证，具有该云平台完全的权限，包括：AccessKey ID（访问密钥 ID）和AccessKey Secret（秘密访问密钥）。

Cloud提供两种AccessKey：本地AccessKey和第三方AccessKey：

- Cloud本地AccessKey：

Cloud授权第三方用户调用Cloud API来访问Cloud云资源的安全凭证，需严格保密。

- 第三方AccessKey：

第三方用户授权Cloud用户调用第三方API来访问第三方云资源的安全凭证，需严格保密。



注：

- AccessKey是云平台对API请求进行安全验证的关键因子，请妥善保管。
- 若某一AccessKey出现泄漏风险，建议及时删除该AccessKey并生成新的AccessKey。

创建本地AccessKey

在Cloud主菜单，点击**运营管理 > 访问控制 > AccessKey 管理**，进入**AccessKey 管理**界面。点击**生成AccessKey**，将生成一个AccessKey。

注意事项

- Admin/平台管理员可以创建多个AccessKey，租户（子账户/项目成员）可以创建两个AccessKey。
- Admin/平台管理员可以随时启用、停用或者删除自己创建的AccessKey以及租户创建的AccessKey。
- 租户可以随时启用、停用或者删除自己创建的AccessKey。
- AccessKey具有该创建者完全的权限。

如图 92: 创建本地AccessKey所示：

图 92: 创建本地AccessKey

AccessKey ID	AccessKey Secret	启用状态	所有者	创建时间	操作
<input type="checkbox"/> c2npLsrSa70xKyNvaM5H	*****	● 启用	admin	2021-03-01 14:35:51	...

第 1 项, 共 1 项

< 1 > 10 条/页

第三方平台使用AccessKey调用Cloud API

创建AccessKey后，第三方平台可以使用AccessKey调用Cloud API，方法如下：

- SDK方式：

以创建云主机（CreateVmInstance）为例，使用AccessKey调用Cloud API时，需输入`accessKeyId`和`accessKeySecret`，示例如下：

- Java SDK

```
CreateVmInstanceAction action = new CreateVmInstanceAction();
action.name = "vm1";
action.instanceOfferingUuid = "ae97ced44efc3314b8f7798972b4ba1a";
action.imageUuid = "da119f7906513eccabf271991c35a65e";
action.l3NetworkUuids = asList("cc0e4c5e77df3af68e59668e7f9e06c5");
action.dataDiskOfferingUuids = asList("19d22d051b063d379a2816daaf431838", "905d94a6abb5398fa1995f6398e3f6fc");
action.clusterUuid = "a0468dc645223f67bd0f2ab95276bbae";
action.description = "this is a vm";
action.strategy = "InstantStart";
action.accessKeyId = "Fnxc7KIQAAdGTvXfx8OjC";
action.accessKeySecret = "Do0AJUGVPrt9iJZlc1QOtk7kzEusYidyqJxSmKOb";
CreateVmInstanceAction.Result res = action.call();
```

- Python SDK

```
CreateVmInstanceAction action = CreateVmInstanceAction()
action.name = "vm1"
action.instanceOfferingUuid = "ae97ced44efc3314b8f7798972b4ba1a"
action.imageUuid = "da119f7906513eccabf271991c35a65e"
action.l3NetworkUuids = ["cc0e4c5e77df3af68e59668e7f9e06c5"]
action.dataDiskOfferingUuids = ["19d22d051b063d379a2816daaf431838", "905d94a6abb5398fa1995f6398e3f6fc"]
action.clusterUuid = "a0468dc645223f67bd0f2ab95276bbae"
action.description = "this is a vm"
action.strategy = "InstantStart"
action.accessKeyId = "Fnxc7KIQAAdGTvXfx8OjC"
action.accessKeySecret = "Do0AJUGVPrt9iJZlc1QOtk7kzEusYidyqJxSmKOb"
CreateVmInstanceAction.Result res = action.call()
```

- 直接调用Cloud RESTful API方式：

- 创建AccessKey：

```
CreateAccessKey accountUuid=df4fb9bbff14e97a67ab894c7b8c528 userUuid=df4fb9bbff14e97a67ab894c7b8c528
```

```
{
  "inventory": {
    "AccessKeyId": "N3Tf05yXZUmSjCf6mYIB",
    "AccessKeySecret": "XAlrsYvswmnEV3X1KWNs1WfZHD6aBIlphml0rX9S",
    "accountUuid": "dff4fb9bbff14e97a67ab894c7b8c528",
    "createDate": "Sep 6, 2018 1:50:06 PM",
    "lastOpDate": "Sep 6, 2018 1:50:06 PM",
    "userUuid": "dff4fb9bbff14e97a67ab894c7b8c528",
    "uuid": "ae353717ca7b4182bb87fb5d010235e8"
  },
  "success": true
}
```

2. 生成date:

```
python get_time.py
Thu, 06 Sep 2018 13:54:10 PRC
```

```
import datetime
import time

date = time.time()
#EEE, dd MMM yyyy HH:mm:ss z
str = datetime.datetime.fromtimestamp(date).strftime('%a, %d %b %Y %H:%M:%S PRC')
print str
```



注: 时间格式必须为EEE, dd MMM yyyy HH:mm:ss zzz。

3. 生成digest:

```
# python get_accesskey.py "N3Tf05yXZUmSjCf6mYIB" "XAlrsYvswmnEV3X1KWNs1WfZHD6aBIlphml0rX9S" \
"GET" "" "application/x-www-form-urlencoded" "Thu, 06 Sep 2018 13:54:10 PRC" "/v1/vm-instances"
args: Namespace(Content_MD5='', Content_Type='application/x-www-form-urlencoded', \
acesskey_id='N3Tf05yXZUmSjCf6mYIB', acesskey_secret='XAlrsYvswmnEV3X1KWNs1WfZHD6aBIlphml0rX9S', \
date='Thu, 06 Sep 2018 13:54:10 PRC', method='GET', uri='/v1/vm-instances')
Signature: S3vm7u7/+n+slQe72lgia08l30U=
Authoration ZStack N3Tf05yXZUmSjCf6mYIB:S3vm7u7/+n+slQe72lgia08l30U=
```

```
#!/usr/bin/python
import base64
import hmac
import sha
import argparse
from hashlib import sha1

parser = argparse.ArgumentParser(description='calculate cloud access key digit.')
parser.add_argument('acesskey_id')
parser.add_argument('acesskey_secret')
parser.add_argument('method')
parser.add_argument('date')
parser.add_argument('uri')

args = parser.parse_args()

print "args: %s" % args
```




```
h = hmac.new(args.aceskey_secret, args.method + "\n"
              + args.date + "\n"
              + args.uri, sha1)
Signature = base64.b64encode(h.digest())
print "Signature: %s" % Signature
print "Authoration %s" % ("ZStack " + args.aceskey_id + ":" + Signature)
```

4. 发送请求

```
curl -H "Authorization:ZStack N3Tf05yXZUmSjCf6mYIB:S3vm7u7/+n
+slQe72lgia08l30U=" \
-H "Content-Type:application/x-www-form-urlencoded" \
-H "Date:Thu, 06 Sep 2018 13:54:10 PRC" \
-X GET http://172.20.11.134:8080/zstack/v1/vm-instances
```

本地AccessKey支持以下操作:

操作	描述
生成本地AccessKey	生成一个新的本地AccessKey。
启用本地AccessKey	启用处于停用状态的本地AccessKey。
停用本地AccessKey	停用选中的本地AccessKey。
删除本地AccessKey	删除选中的本地AccessKey。  注: 删除本地AccessKey, 将不能调用API来访问本地云资源。

添加第三方AccessKey

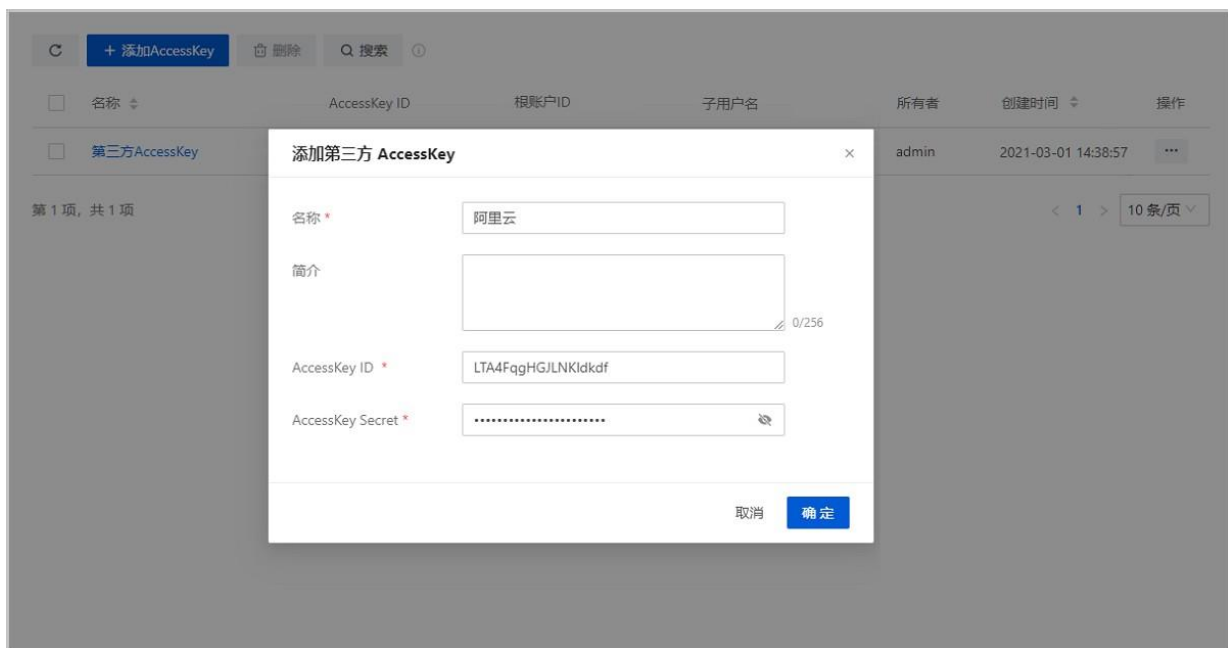
在Cloud主菜单, 点击**运营管理 > 访问控制 > AccessKey 管理**, 进入**AccessKey 管理**界面。点击**添加AccessKey**, 弹出**添加AccessKey**界面。

可参考以下示例设置相应内容:


- **名称:** 设置第三方AccessKey名称
- **简介:** 可选项, 可留空不填
- **AccessKey ID和AccessKey Secret:** 输入已在第三方申请好的AccessKey ID和AccessKey Secret

如图 93: 添加第三方AccessKey所示:

图 93: 添加第三方AccessKey



第三方Accesskey支持以下操作:

操作	描述
添加第三方AccessKey	添加一个新的第三方AccessKey。
删除第三方AccessKey	<p>删除选中的第三方AccessKey。</p> <p> 注: 删除AccessKey将清除该AccessKey相关的本地资源记录，且该AccessKey授权的API访问权限失效，第三方公有云资源不受影响。</p>

注意事项

- admin/平台管理员可以随时删除自己添加的第三方AccessKey以及租户添加的第三方AccessKey。
- 租户可以随时删除自己添加的第三方AccessKey。

14.3.2 IP黑白名单

IP黑白名单（IP Blocklist/Allowlist）：云平台登录IP的黑白名单，通过对访客身份的识别和过滤，进一步提升云平台访问控制安全。Cloud支持配置登录IP黑白名单，对云平台登录IP进行防护。用户可按需配置IP黑白名单，从而实现对访客身份的识别和过滤，提升云平台访问控制安全。



注: 用户可自行设置启用IP黑白名单功能。设置方法:

进入设置 > 平台设置 > 全局设置 > 基本设置 > 平台策略 > 云平台登录策略，设置云平台登录IP黑白名单即可，默认为False。

添加IP黑名单/白名单

在IP黑白名单页面，可以选择添加IP黑名单或IP白名单，添加方式一致，以添加IP黑名单为例：

在Cloud主菜单，点击运营管理 > 访问控制 > IP黑白名单，进入IP黑白名单界面，点击添加IP黑名单，弹出添加IP黑名单界面。

可参考以下示例输入相应内容：

- **名称：**设置IP黑名单名称
- **简介：**可选项，可留空不填
- **IP地址：**输入需要加入IP黑名单的IP地址

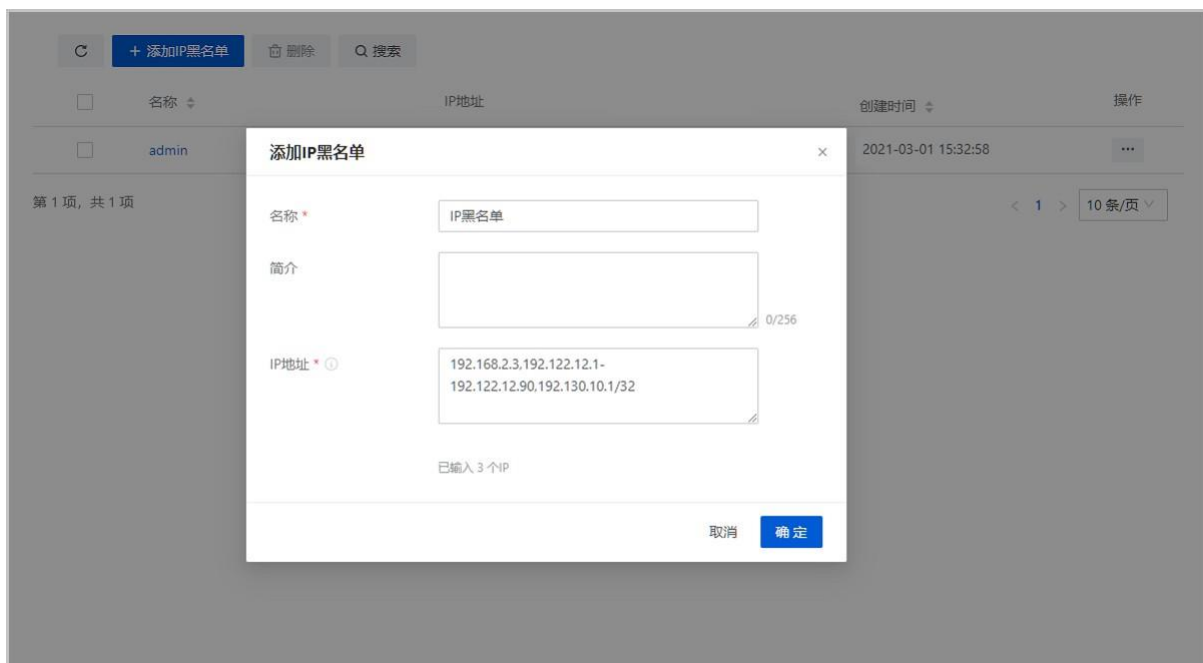


注：

- 支持输入固定IP地址、IP地址范围、IP/掩码格式，添加多个需要以英文逗号分隔开。
- 支持最多添加100条。

如图 94: 添加IP黑名单所示：

图 94: 添加IP黑名单





The screenshot shows a web interface for managing IP blacklists. A modal dialog titled '添加IP黑名单' (Add IP Blacklist) is open. It contains the following fields:

- 名称 (Name):** IP黑名单
- 简介 (Introduction):** (Empty text area)
- IP地址 (IP Address):** 192.168.2.3, 192.122.12.1-192.122.12.90, 192.130.10.1/32

Below the IP address field, it says '已输入 3 个IP' (3 IPs entered). At the bottom of the dialog are '取消' (Cancel) and '确定' (Confirm) buttons. The background interface shows a table with columns for Name, IP Address, Creation Time, and Action, with one entry 'admin'.

表 17: 管理IP黑白名单

操作	描述
添加IP黑/IP白名单	添加一个新的IP黑/白名单。  注: 添加IP黑/白名单, 该名单将立即生效, 名单中的IP地址将被拒绝/允许访问云平台, 请谨慎操作。
编辑IP黑/白名单	编辑IP黑/IP白名单的名称、简介信息。
删除IP黑/白名单	删除选中的IP黑/白名单。  注: 删除IP黑/白名单, 该名单将失效, 访问云平台IP无限制, 请谨慎操作。

注意事项

IP黑白名单实现机制如下:

- 若未添加任何IP黑白名单, 默认允许全部IP访问。
- 若只添加IP黑名单, 则黑名单的IP访问将被拒绝, 其余IP允许访问。
- 若只添加IP白名单, 则白名单的IP允许访问, 其余IP允许访问。
- 若IP黑白名单均添加, 则白名单优先于黑名单, 例如: 同一个IP同时添加在黑白名单中, 则来自该IP的请求将被允许。

14.3.3 控制台代理

控制台代理 (Console Proxy): 可通过代理地址登录云主机控制台。UI界面上显示了当前控制台代理的信息, 即打开云主机的控制台时使用的代理信息。

在Cloud主菜单, 点击**运营管理 > 访问控制 > 控制台代理**, 进入**控制台代理**界面。



如图 95: 控制台服务界面所示:

图 95: 控制台服务界面

	重连 					
<input type="checkbox"/>	管理IP	控制台代理地址	启用状态	就绪状态	创建时间	操作
<input type="checkbox"/>	172.24.251.15	172.24.251.15	 启用	 已连接	2021-01-20 21:55:43	
第 1 项, 共 1 项					< 1 >	10 条/页

- 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。
- 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。

控制台代理支持以下操作：

操作	描述
重连控制台代理	重连控制台代理。  注： 若云主机控制台打开失败，需进行重连操作。重连后状态显示为 启用 和 已连接 时，控制台可以正常打开。
设置控制台代理地址	设置控制台代理地址。  注： 支持在UI界面上设置控制台代理地址。 <ul style="list-style-type: none"> • 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。

14.4 应用中心

应用中心：提供云平台增强功能以及第三方应用的快速访问。

应用支持以下操作：

操作	描述
添加应用	添加一个新的应用。
修改应用	可修改该应用的类型、名称、简介、URL、共享权限。
删除应用	将该应用删除。

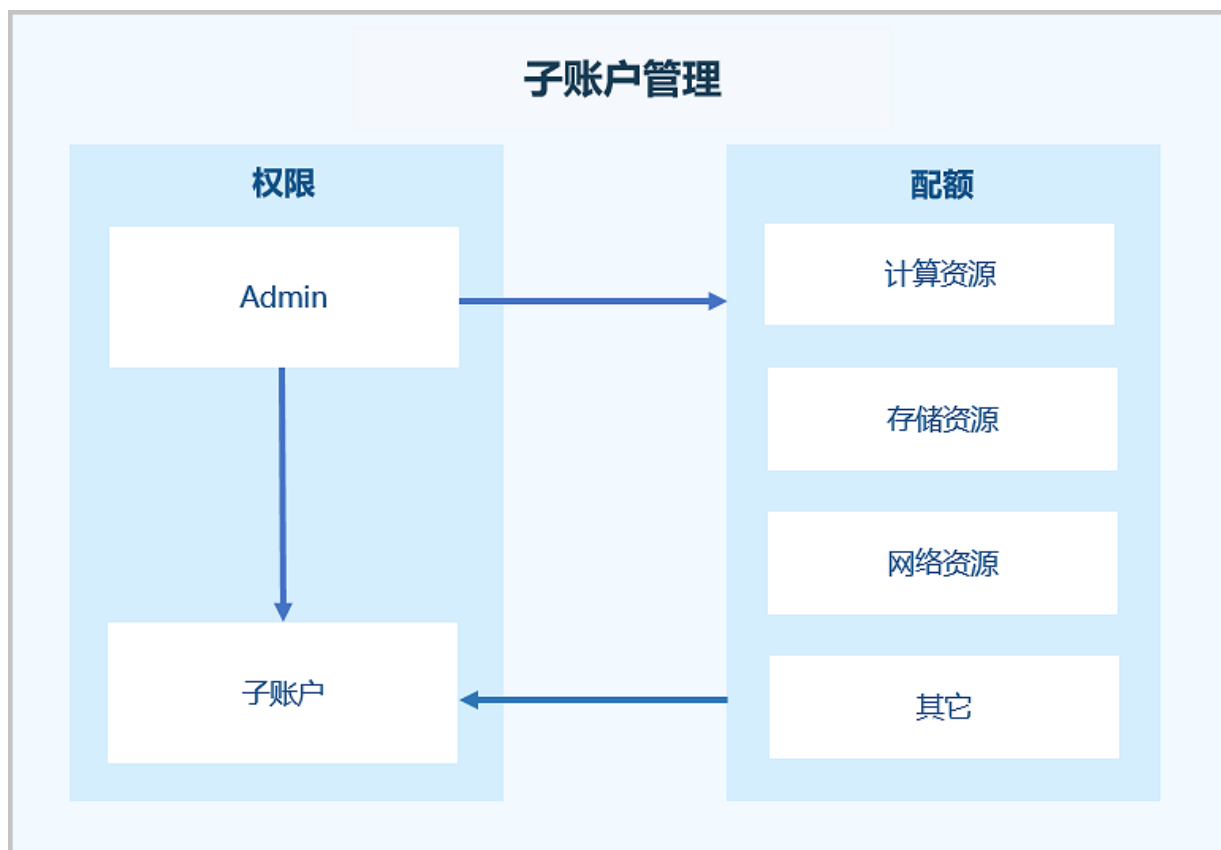
15 设置

15.1 账户信息

子账户：子账户是租户的一种，由admin创建与管理，子账户对自己创建的虚拟资源拥有管理权限。子账户对作用域的资源可以进行创建、删除、分享、召回等操作，实现对资源归属及权限控制的细粒度划分。

如图 96: 子账户管理所示：

图 96: 子账户管理



子账户相关定义

- **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、镜像等其他资源给子账户，而子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子账户进行资源总量控制。

- admin账户创建VxlanNetworkPool后，子账户可以基于VxlanNetworkPool创建VxlanNetwork。
- 更改云主机所有者会更改云主机的EIP所有者属性。
- **子账户：**由admin账户创建。
 - 子账户拥有对自己创建的云主机、镜像、云盘、安全组的管理权限。子账户可以对admin账户共享的资源进行读操作，但不可以进行删除操作。
 - 删除子账户会导致此账户下的所有资源被删除，例如，云主机、云盘、镜像等。
 - 子账户名称不可重复。
 - 子账户首页看到的资源是admin账户分配的资源配额的上限。
 - 子账户创建云主机前，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。
 - 子账户可以添加自有的镜像文件，也可由admin账户提前共享。
- **子账户配额：**

简称配额，是admin账户对子账户的资源总量进行控制的衡量标准，包括计算资源、存储资源、网络资源和其它。

admin账户通过配置以上各参数来对各个普通账户的资源总额进行控制。若执行资源删除操作，但还未彻底删除时，会占用主存储资源和云盘数量。

15.2 主题外观

主题外观：用户可自定义设置云平台主题外观。详情可参考《[定制化主题外观](#)》章节。

15.3 邮箱服务器

云平台报警选择邮箱类型的通知对象，需设置邮箱服务器，用来发送报警邮件。

注意事项

- 从Cloud 3.3.0开始，支持设置AD/LDAP、邮箱服务器的接连超时时间，设置方法如下：
进入 `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`，在 `zstack.properties` 配置文件中设置如下参数：
 - # 设置AD/LDAP连接超时时间
`Ldap.addServer.connectTimeout = XX`
 - # 设置邮箱服务器连接超时时间


```
SNS.addEmailPlatform.connectTimeout = XX
```

- # 设置邮箱服务器读取数据超时时间

```
SNS.addEmailPlatform.readTimeout = XX
```



注:

- 系统默认上述三个参数的超时时间均为5000（单位默认为ms）。
- 若需修改超时时间，可通过zstack-ctl configure命令进行修改，例如：

```
[root@localhost ~]# zstack-ctl configure Ldap.addServer.connectTimeout = 10000
[root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.connectTimeout = 10000
[root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.readTimeout = 10000
```

设置完成后使用zstack-ctl restart_node命令重启管理节点生效。

15.4 日志服务器

日志服务器：添加日志服务器至云平台，可用于收集管理节点日志，快速定位问题，提高云平台运维效率。

注意事项

- 需要设置日志级别与日志服务器的配置完全一致，才能正常接收日志信息。
- 请按实际情况填写相关信息，如有疑问请联系相关日志服务器提供商。

15.5 全局设置

提供平台层面的功能特性设置，一经设置，云平台全局范围内生效。

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

全局设置包括**基本设置**与**高级设置**。Cloud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。

资源高级设置

Cloud支持使用高级设置对资源进行细粒度的特性配置，用户可根据自身需求搜索并且修改对应的设置。默认使用全局设置的值。

15.6 场景封装

基于用户实际生产场景需求，提供场景化的一键全局设置，方便快速将云平台设置为所需状态，提高运维效率。

支持以下四种场景封装模板：

- 生产推荐配置
- 高可用快速恢复
- 云主机性能调优
- 云平台安全配置

场景封装模板 | 云主机性能调优

本模板适用于云主机高性能场景，具体介绍如下：

- **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。
 - **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。



- 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。
- **支持内核aio：**

在QEMU存储驱动中使用内核异步IO。
- **SharedBlock云盘预分配策略：**

用于设置SharedBlock中云盘的预分配策略，可选策略为none, metadata。
- **云主机Hyper-V开关：**

云主机Hyper-V模拟的开启或关闭。

场景封装模板 | 高可用快速恢复

本模板适用于云主机高可用场景，具体介绍如下：

- **异常物理机检查间隔：**

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：**

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。

- **判定物理机成功连接时间：**

单位为秒，用于判定物理机成功连接的时间，如果物理机在此时间内成功返回，则表示连接成功。

- **物理机成功次数：**

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。

- **判定物理机成功尝试几率：**

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。

- **物理机自检间隔：**

设置物理机状态自检的间隔。

- **物理机自检最大尝试次数：**

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：**

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：**

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。

- **永不停止云主机扫描间隔：**

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。

- **永不停止云主机尝试的延迟时间：**

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。

- **云主机高可用策略：**

用于设置云主机高可用触发策略。可选策略为：保守策略、激进策略。保守策略：管理节点不会对未知状态的云主机主动触发高可用迁移，且self fencer不会强制停止云主机。激进策略：只要满足高可用条件，就可对云主机触发高可用迁移。

- **物理机连接状态快速探测开关：**

用于设置是否开启物理机连接状态快速探测。若为true，则会缩短探测物理机连接状态的时间间隔。

- **检查计算节点失败阈值：**

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。

- **物理机重连SSH超时阈值：**

单位为秒，用于设置重连物理机时测试物理机SSH超时的时间。若时间结束仍未SSH成功则表示物理机重连失败。

场景封装模板 | 生产推荐配置

本模板适用于生产环境场景，具体介绍如下：

- **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。
- 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。
- 若资源已单独设置该选项，此全局设置将不对该资源生效。

- **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）。
- 如果主存储可用空间为2T，设置为1.1，那么Cloud会认为系统可以分配2.2T主存储空间给云主机使用。
- 用户需理解并设置正确的主存储使用阈值后再进行配置：
 - 设置[1.0, 1.2]：数值过大会影响云主机IO性能
 - 设置1.2以上：数值过大可能会严重影响存储压力或导致磁盘容量快速占满，导致系统IO错误

- 若资源已单独设置该选项，此全局设置将不对该资源生效。
- **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）。
 - 如果物理内存为4G，设置为1.1，那么Cloud会认为系统可以分配4.4G内存给云主机使用。
 - 该数值需要根据不同系统和应用的需求进行配置：
 - 设置[1.0, 1.2]：数值过大会影响云主机内存性能
 - 设置1.2以上：数值过大可能会严重影响物理机内存性能，导致系统OOM（内存溢出）
 - 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。
 - 若资源已单独设置该选项，此全局设置将不对该资源生效。
- **本地存储在线迁移：**
 - 本地存储在线迁移的全局设置打开或关闭。
 - 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。
- **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。
 - 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。
 - 如果物理机的CPU为四核八线程，Cloud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。
 - 该数值需要根据不同系统和应用的需求进行配置：
 - 设置10以上：数值过大可能会严重影响物理机性能，导致业务性能卡顿
 - 虚拟CPU的总数可以在首页的处理器的总量查看。
 - 若资源已单独设置该选项，此全局设置将不对该资源生效。
- **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。
 - 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！

• **云主机跨集群高可用开关:**

用于设置云主机跨集群高可用功能是否启用。若为true，表示允许跨集群探测物理机，实现云主机跨集群高可用。注意：需提前确认集群间连通性良好，才可启用该功能。

• **主存储保留容量:**

- 用于设置主存储的保留容量。
- 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。

• **镜像服务器保留容量:**

- 用于设置镜像服务器在使用是的保留使用容量。
- 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。

• **监控数据保留周期:**

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。

• **租户云盘快照数量配额:**

设置账户的云盘快照配额。

• **物理机密码加密存储开关:**

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。

场景封装模板 | 云平台安全配置

本模板适用于强安全性的云平台场景，具体设置如下：

- **云平台登录IP黑白名单:**

默认为false，用于设置是否开启IP黑白名单功能，开启后，云平台将对登录IP进行防护。

- **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。

- **禁止同一用户多会话连接开关:**

默认为false，用于设置是否禁止同一用户多会话连接。若为true，则同一用户只能存在一个登录会话，历史会话将强制退出。

- **会话超时时间:**

- 设定Cloud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。

- **SSL证书检查开关:**

用于设置是否开启跳过LDAP SSL证书的所有检查的开关。若为true，表示跳过所有LDAP SSL证书的检查。

- **云平台登录验证码策略:**

用于设置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。

- **云平台登录密码更新周期:**

- **云平台登录密码更新周期开关:**

默认为false，用于设置是否启用密码更新周期开关。若为true，表示允许设置密码更新周期。当密码使用时间达到所设置的密码更新周期，重新登录将提示修改密码。

- **密码更新周期:**

默认为90天，用于设置需要重设密码的周期。

- **云平台登录密码不重复次数:**

- **云平台登录密码不重复次数开关:**

默认为false，用于设置是否启用密码不重复次数开关。若为true，表示允许设置密码不重复次数。在所设置的密码不重复次数范围内，重设密码时，新密码不能与之前已使用过的历史密码重复。密码不重复次数可配置。

- **密码不重复次数:**

默认为5，用于设置密码不重复次数，例如：若为3，则新密码不能与之前3次已使用过的历史密码重复。

- **云平台连续登录失败锁定用户：**

- **云平台登录连续登录失败锁定账户开关：**

默认为false，用于设置是否启用连续登录失败锁定账户开关。若为true，表示连续登录失败次数，账户将被锁定一段时间。连续登录失败次数上限可配置。

- **连续登录失败次数上限：**

默认为6，用于设置连续登录失败次数上限。当连续登录失败次数超过设置值，账户将被锁定一段时间。

- **连续登录失败锁定账户时长：**

默认为10分钟，当连续登录失败触发账户锁定，用于设置账户的锁定时长。

- **云平台登录密码强度：**

- **云平台登录密码强度开关：**

默认为false，用于设置是否启用密码强度开关。若为true，表示允许设置密码强度，包括设置密码长度范围，并可选择是否启用数字、大小写和特殊字符组合的策略。

- **密码强度：**

默认为8-32，用于设置密码长度范围，并可选择是否启用数字、大小写和特殊字符组合的策略。

- **云平台登录双因子认证开关：**

默认为false，登录管理节点时，是否开启双因子认证。

- **VNC控制台密码强度：**

- **VNC控制台密码开关：**

默认为false，用于设置是否启用密码登录VNC控制台。

- **VNC控制台密码强度：**

默认为6-32，用于设置VNC密码的长度范围，并支持选择是否启用数字、大小写和特殊字符组合的策略。

- **云主机密码强度：**

- **云主机密码强度开关：**

默认为false，用于设置是否启用密码登录云主机。

— 云主机密码强度：

默认为8-18，用于设置云主机密码的长度范围，并支持选择是否启用数字、大小写和特殊字符组合的策略。



注：设置云主机密码需确保云主机镜像中已安装cloud-init，且cloud-init推荐版本为：0.7.9、17.1、19.4、19.4以后版本。

16 管理节点运维

本章主要针对Cloud管理节点运维给出处理方法。

注意事项

若需要对管理节点进行运维，需要注意以下事项：

- 管理节点运维前（升级、重启），请将**设置 > 全局设置 > 高级设置**中的**云主机高可用全局开关**设置为**false**，待运维完成后，将修改恢复为**true**。

16.1 管理节点高可用

16.1.1 多管理节点物理机高可用场景

概述

Cloud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Keepalived触发VIP（Virtual IP）迁移，然后尝试恢复宕机服务。

本章节以双管理节点物理机高可用为例，简单概述安装部署、升级步骤，以及多管理节点物理机高可用相关注意事项。详情请参考《多管理节点物理机高可用教程》。

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Cloud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Cloud。
 3. 对新增管理节点安装最新版Cloud。
 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Cloud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Cloud。
 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，在主管理节点中执行以下命令，就可完成高可用套件升级：

```
[root@localhost ~]# ./zsha2 upgrade-ha
```

- 管理节点升级

在双管理节点高可用场景下，需先升级高可用套件，才可升级管理节点。

管理员只需在一个管理节点中执行以下命令，就可对两个管理节点进行升级：

- 若选择从bin包升级，请执行：

```
[root@localhost ~]# zsha2 upgrade-mn -peerpass password ./Cloud-installer-4.1.3.bin
```

- 若选择从ISO升级，请执行：

```
[root@localhost ~]# zsha2 upgrade-mn -peerpass password ./Cloud-x86_64-DVD-4.1.3-c76.iso
```



注：-peerpass为可选参数，可设置Peer管理节点SSH登录密码。

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Cloud 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Cloud配套使用。
- 两个管理节点安装的Cloud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。

16.2 管理节点灾难恢复

使用Cloud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，此时需准备两台服务器，并安装Cloud管理节点物理机高可用环境，然后使用远程数据库备份文件恢复Cloud管理节点服务，即可对Cloud进行灾难恢复。



注:

- 建议新准备的服务器与原管理节点服务器型号、配置均相同。
- 若原本的管理节点仅发生操作系统故障，也可以使用原本的管理节点服务器，重新安装Cloud。

16.2.1 准备工作

本地备份数据库

Cloud云管理平台首次安装后，默认每天凌晨12点半和中午12点半自动备份一次数据库，备份数据默认存放在管理节点的/var/lib/zstack/mysql-backup/目录，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

为防止管理节点出现故障不能进入系统，建议配置远程数据库备份。

假定管理节点的IP地址为172.20.12.16，异地备份服务器的IP地址为172.20.12.75，进行异地备份，请在管理节点172.20.12.16上执行以下步骤：

```
#在管理节点上生成ssh key公钥
ssh-keygen
#拷贝ssh key 公钥到异地备份服务器节点，期间需手动输入yes和root密码
```

```
ssh-copy-id root@172.20.12.75
```

异地数据库冗余备份

如果有多台服务器可做冗余备份，可以在异地备份服务器上同时进行异地数据库备份，增加数据库的多备份。

在异地备份服务器 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。

```
#每天凌晨12点和中午12点，将管理节点数据库直接备份到异地备份服务器的/var/lib/zstack/
from-zstack-remote-backup/目目录下，最多保留24份
0 0,12 * * * zstack-ctl dump_mysql --host root@172.20.12.75 --d --keepamount 24
```

16.2.2 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 Cloud 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，或选择新的服务器作为管理节点。

2. 安装 Cloud



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，Cloud 版本为 3.8.0，则建议安装 Cloud 3.8.0。

3. 更新许可证

Cloud 安装完成后，需更新许可证再继续其他操作。

4. 恢复数据库。

在异地备份服务器上，选择最后一次数据库备份文件。其文件命名类似以下格式：

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

将此文件拷贝到新安装的 Cloud 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，Cloud 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
```

- 如果管理节点数据库备份未同步到异地备份服务器上，就发生了灾难，无法修复。
- 参考本文档的恢复方法，数据库备份的时间点到管理节点发生灾难的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。

16.3 修改管理节点IP地址

使用Cloud过程中，当管理节点IP发生变化时，需要手动修改。根据部署方式不同，主要分为单管理节点、多管理节点物理机高可用两个场景。

16.3.1 单管理节点场景

若管理节点所在服务器的IP地址发生变化，请参考以下步骤修改管理节点IP地址：

1. 在管理节点执行以下命令备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. 依次执行以下命令，手动修改所有服务器的网卡地址(假设bond0为管理网络)：

```
[root@localhost ~]# zs-network-setting -i br_bond0 172.31.250.100 255.255.255.0 172.31
.250.1 #根据实际情况填写
```

3. 依次执行以下命令，修改管理节点IP：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理
节点IP地址
```



```
[root@localhost ~]# zstack-ctl restart_node #重启管理节点，配置生效
```

补充说明

若管理节点所在服务器同时被添加为其他节点，需要在UI上更新相应节点的IP地址，操作流程如下：



注：修改物理机IP可能会导致物理机失联，请谨慎操作。

- 场景一：管理节点、计算节点、镜像服务器（ImageStore类型）共用服务器

1. 登录UI界面，在**硬件设施**界面，将需要修改物理机进入维护模式并停用镜像服务器。
2. 在管理节点执行以下命令备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

3. 依次执行以下命令，手动修改所有服务器的网卡地址(假设bond0为管理网络)：

```
[root@localhost ~]# zs-restore-network-setting -i br_bond0 #清除网桥上IP
[root@localhost ~]# zs-show-network #查看是否成功清除IP
[root@localhost ~]# zs-network-setting -i br_bond0 172.31.250.100 255.255.255.0 172.31.250.1 #根据实际情况填
```

4. 依次执行以下命令，修改管理节点IP：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理节点IP地址
[root@localhost ~]# zstack-ctl restart_node #重启管理节点服务，配置生效
```

5. 登录UI界面，依次修改对应物理机IP、镜像服务器IP。



注：

- 修改物理机IP可能会导致物理机失联，请谨慎操作。
- 修改镜像服务器IP后，重连过程中其上资源暂时无法操作。
- 场景二：管理节点、存储节点（Ceph分离部署）共用服务器

1. 在管理节点执行以下命令备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. 执行Ceph存储变更管理IP地址操作。
3. 依次执行以下命令，修改管理节点IP：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理节点IP地址
```

```
[root@localhost ~]# zstack-ctl restart_node #重启管理节点，配置生效
```

- 场景三：复杂的混合场景

管理节点、计算节点、存储节点（Ceph分离部署）、镜像服务器共用服务器。

1. 在管理节点执行以下命令备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. 登录UI界面，在**硬件设施**界面，将需要修改物理机进入维护模式并停用镜像服务器。
3. 执行Ceph存储变更管理IP地址操作。
4. 依次执行以下命令，修改管理节点IP：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理节点IP地址
```

```
[root@localhost ~]# zstack-ctl restart_node #重启管理节点，配置生效
```

5. 登录UI界面，依次修改对应物理机IP、镜像服务器IP、更改ceph主存储监控节点IP。



注：

- 修改物理机IP可能会导致物理机失联，请谨慎操作。
- 修改镜像服务器IP后，重连过程中其上资源暂时无法操作。
- Ceph主存储/镜像服务器监控节点IP不支持修改，请联系官方技术支持获取帮助。

16.3.2 多管理节点物理机高可用场景

若管理节点所在服务器的IP地址发生变化，请参考以下步骤，修改管理节点IP：

1. 在某个管理节点，执行以下命令，备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. 分别在多个管理节点依次执行以下命令，手动修改所有服务器的网卡地址(假设bond0为管理网络)：

```
[root@localhost ~]# zs-restore-network-setting -i br_bond0 #清除网桥上IP
[root@localhost ~]# zs-show-network #查看是否成功清除IP
[root@localhost ~]# zs-network-setting -i br_bond0 172.31.250.100 255.255.255.0 172.31.250.1 #根据实际情况填
```

3. 分别在多个管理节点依次执行如下命令，修改管理节点IP地址：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理节点IP地址
```

```
[root@localhost ~]# zstack-ctl restart_node #重启管理节点，配置生效
```

4. 在备份数据库的管理节点通过**install_ha**命令重新安装高可用套件。

补充说明

若管理节点所在服务器同时被添加为其他节点，需要同时修改IP地址，操作流程如下：

- 场景一：管理节点、计算节点、镜像服务器共用服务器

1. 登录UI界面，在**硬件设施**界面，将需要修改物理机进入维护模式并停用镜像服务器。
2. 在某个管理节点下执行以下命令，备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

3. 分别在多个管理节点依次执行以下命令，手动修改所有服务器的网卡地址(假设bond0为管理网络)：

```
[root@localhost ~]# zs-restore-network-setting -i br_bond0 #清除网桥上IP
[root@localhost ~]# zs-show-network #查看是否成功清除IP
[root@localhost ~]# zs-network-setting -i br_bond0 172.31.250.100 255.255.255.0 172.31.250.1 #根据实际情况填
```

4. 分别在多个管理节点依次执行如下命令，修改管理节点IP地址：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理节点IP地址
[root@localhost ~]# zstack-ctl restart_node #重启管理节点，配置生效
```

5. 通过备份数据库的管理节点IP登录UI界面，依次修改对应物理机IP、镜像服务器IP。
6. 在备份数据库的管理节点通过 `install_ha` 命令重新安装高可用套件。

- 场景二：管理节点、存储节点（Ceph分离部署）共用服务器

1. 在某个管理节点，执行以下命令，备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. 通过VIP登录UI界面，在**硬件设施**界面，修改物理机进入维护模式、停用主存储、停用镜像服务器；在**云资源池**界面，关闭云主机
3. 执行Ceph存储变更管理IP地址操作。
4. 分别在多个管理节点依次执行如下命令，修改管理节点IP地址：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理节点IP地址
[root@localhost ~]# zstack-ctl restart_node #重启管理节点，配置生效
```

5. 在备份数据库的管理节点通过 `install_ha` 命令重新安装高可用套件。



注：Ceph场景修改IP为重操作，请联系官方技术支持获取帮助。

- 场景三：复杂的混合场景

管理节点、计算节点、存储节点（Ceph分离部署）、镜像服务器共用服务器。

1. 在某个管理节点，执行以下命令，备份数据库：

```
[root@localhost ~]# zstack-ctl dump_mysql
```

2. 通过VIP登录UI界面，在**硬件设施**界面，修改物理机进入维护模式、停用主存储、停用镜像服务器；在**云资源池**界面，关闭云主机
3. 执行Ceph存储变更管理IP地址操作。



注：Ceph场景修改IP为重操作，请联系官方技术支持获取帮助。

4. 分别在多个管理节点依次执行如下命令，修改管理节点IP地址：

```
[root@localhost ~]# zstack-ctl change_ip --ip 172.31.250.110 # 172.31.250.110为新的管理节点IP地址
```

```
[root@localhost ~]# zstack-ctl restart_node #重启管理节点，配置生效
```

5. 通过备份数据库的管理节点IP登录UI界面，依次修改对应物理机IP、镜像服务器IP、更改ceph主存储监控节点IP。



注：若镜像服务器为Ceph类型需更改Ceph类型镜像服务器监控节点IP，请联系官方技术支持获取帮助。

6. 在备份数据库的管理节点通过`install_ha`命令重新安装高可用套件。
7. 通过VIP登录UI界面，在**硬件设施**界面，启用镜像服务器、主存储、物理机；在**云资源池**界面，开启云主机。

16.4 切换管理节点

管理节点切换步骤如下：

1. 登录原管理节点，执行如下命令，备份原管理节点数据库并拷贝到`/root/`目录：

```
[root@localhost ~]# zstack-ctl dump_mysql #备份数据库，假定数据库备份文件为/var/lib/zstack/mysql-backup/zstack-backup-db-2018-12-13_17-57-52.gz
[root@localhost ~]# cp /var/lib/zstack/mysql-backup/zstack-backup-db-2018-12-13_17-57-52.gz /root #将备份文件拷贝到/root/目录
```

2. 在新管理节点安装相同版本的Cloud（确保版本的相同）并添加License许可；

3. 在原管理节点，执行如下命令，停止管理节点服务：

```
[root@localhost ~]# zstack-ctl stop
```

4. 在原管理节点，执行如下命令，拷贝原管理节点数据库备份文件到新管理节点：

```
[root@localhost ~]# scp /root/zstack-backup-db-2018-12-13_17-57-52.gz root@新管理节点IP:/root
```

5. 在新管理节点，执行如下命令，恢复数据库：

```
[root@localhost ~]# zstack-ctl restore_mysql -f /root/zstack-backup-db-2018-12-13_17-57-52.gz --mysql-root-password zstack.mysql.password
#zstack.mysql.password为数据库密码
```

6. 在新管理节点，执行如下命令，启动管理节点：

```
[root@localhost ~]# zstack-ctl start
```

7. （可选）确保新管理节点上服务无误后，执行如下命令，删除原管理节点上相关目录以保证数据安全：

```
[root@localhost ~]# rm -rf /usr/local/zstack
```

16.5 计算节点升级为管理节点

若需要将计算节点升级为管理节点，请按照以下步骤进行操作：

1. 在待升级计算节点，依次执行如下命令，确定进程是否空闲：

```
[root@localhost ~]# lsof +d /usr/local/zstack/ #进行使用查看
[root@localhost ~]# ps aux|grep usr.local.zstack #查看是否有进程使用此文件夹
```

2. 停止待升级为管理节点的物理机。
3. 在原管理节点执行以下命令，停止管理节点：

```
[root@localhost ~]# zstack-ctl stop
```

4. 在待升级计算节点，依次执行如下命令，停止Agent服务：

```
[root@localhost ~]# systemctl stop zstack-sharedblock-agent;
[root@localhost ~]# /etc/init.d/zstack-network-agent stop;
[root@localhost ~]# kill -15 `pgrep dnsmasq`
```

5. 在待升级计算节点，依次执行如下命令，升级为管理节点：

```
[root@localhost ~]# mv /usr/local/zstack/ /mnt/ # mv /usr/local/zstack/ /mnt/
[root@localhost ~]# bash Cloud-install.bin -E #升级为管理节点
[root@localhost ~]# cp -r /mnt/zstack/* /usr/local/zstack/ #复制之前文件到/usr/local/zstack/
```

6. 启用物理机及后续可选操作（例如：将此管理节点替换原管理节点、或者部署多管理节点）。

17 云平台基本运维

本章主要针对Cloud基本操作异常给出处理办法。

17.1 安装部署

安装部署以及升级Cloud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Cloud。

原因：

- 不满足最低硬件需求（4核CPU/8G内存）
- 安装操作系统时，没有设置合适的IP地址，Cloud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Cloud；

2. 安装Cloud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Cloud，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Cloud ISO版本不匹配，会提示类似以下错误信息。

现象：

```
mount: /dev/loop0 is write-protected, mounting read-only /root
```



```
Current release c76 not matched the new ISO c74,  
Use Cloud-upgrade -r xxx.iso to update current repo,  
Use Cloud-upgrade -a/--add_repo xxx.iso to add a new repo
```

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/Cloud-x86_64-DVD-4.1.3-c76.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。

```
Cloud-upgrade Cloud-x86_64-DVD-4.1.3-c76.iso
```

5. 升级Cloud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Cloud。

前提:

Cloud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. Cloud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Cloud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Cloud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Cloud

```
bash Cloud-installer.bin -D
```

6. 使用步骤1备份的Cloud核心文件恢复

```
zstack-ctl stop
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Cloud管理节点服务，此时Cloud已成功恢复至原本升级失败前的版本

```
zstack-ctl start
```

6. 若采用all in one方式安装Cloud，初始化结束后，建议对**物理机保留内存**进行设置，设置方式如下：

- 全局设置粒度：

进入**设置 > 平台设置 > 全局设置 > 基本设置**，设置**物理机保留内存**，默认为1G。



注：若集群（或物理机）已单独设置该选项，此全局设置将不对该集群（或物理机）生效。

- 集群粒度：

进入**硬件设施 > 集群**，选择某一集群，进入集群详情页，在**高级设置**子页面，设置**物理机保留内存**，默认为1G。



注：若物理机已单独设置该选项，此集群高级设置将不对该物理机生效。

- 物理机粒度：

目前支持CLI方式对单台物理机设置保留内存：

```
UpdateResourceConfig category=kvm name=reservedMemory resourceUuid=e2f4836
723a2490095768fe611c540b1 value=10G
# resourceUuid为物理机资源UUID, value为物理机保留内存
```

17.2 启动服务

Cloud相关的服务在管理节点重启后，会自动启动。

启动Cloud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 -an|grep 8080`找到8080占用程序将其停止再启动Cloud。

4. 出现如下报错:

现象:

```
MN status: Unknown, the management node seems to become zombie as it stops responding 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Cloud使用。

17.3 zstack-ctl命令

Cloud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/start_node/stop_node/restart_node/`
- 日志收集: `zstack-ctl configured_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`
- UI配置检查: `zstack-ctl show_ui_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《CTL命令使用手册》。

17.4 zstack-cli命令

Cloud提供zstack-cli命令行交互界面对Cloud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:

```
CreateVmInstance name=ceph instanceOfferingUuid=$instanceofferUuid l3NetworkUuids=$L3Uuid imageUuid=$imageUuid
```

5. 使用zstack-cli查询运行中的云主机:

```
QueryVmInstance state= "Running" name~=test limit=3 fields=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《CLI命令使用手册》。

17.5 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. 根据选择的镜像关联此镜像所在镜像服务器，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服务IP分配服务；
9. 确保物理主机的Libvirt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
<pre>"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 "</pre>	<ul style="list-style-type: none"> 原因： <p>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。</p> 解决方案： <p>重启系统，并进入BIOS打开CPU相关虚拟化支持。</p>
<pre>"details" : "cannot find either 'vmx' or 'svm' in /proc/cpuinfo, please make sure you have enabled virtualization in your BIOS setting"</pre>	<ul style="list-style-type: none"> 原因： <p>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。</p> <p>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。</p> 解决方案： <p>具体的打开办法，请联系“云主机”提供方。</p>
<pre>"details": "the local primary storage has no hosts with enough disk capacity[xxx bytes] required by the vm[uuid:xxx]"</pre>	<ul style="list-style-type: none"> 原因： <p>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）。</p>

异常信息	异常原因及解决办法
	<p>Cloud</p> <p>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。</p> <p>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。</p> <ul style="list-style-type: none"> 解决方案： <p>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。</p> <p>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。</p>
<p>"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}]"</p>	<ul style="list-style-type: none"> 原因： <p>当前系统中（或者任何单独一台物理主机）没有足够的CPU或内存。</p> <ul style="list-style-type: none"> 解决方案： <p>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。</p>
<p>"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"</p>	<ul style="list-style-type: none"> 原因： <p>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。</p> <ul style="list-style-type: none"> 解决方案： <p>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）。</p>
<p>"failed to migrate vm[uuid:xxx] from kvm host[uuid:xxx, ip:xxx] to dest host[ip:xxx"</p>	<ul style="list-style-type: none"> 原因：

异常信息	异常原因及解决办法
], unable to migrate vm[uuid:xxx] to qemu +tcp://xxx/system, Unsafe migration: Migration may lead to data corruption if disks use cache != none"	<p>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。</p> <ul style="list-style-type: 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	<ul style="list-style-type: none"> • 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'	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> • 在CentOS7.2里版本要求2.3.0 • 在Windows Server 2012 R2里版本要求0.12.1 • Ubuntu 14.04里版本要求2.5（默认2.0，需手动升级）

异常信息	异常原因及解决办法
<p>"libvirt error: error from service: ListActivatableNames: Connection is closed"</p> <p>"或"libvirt error: Activation of org.freedesktop.machine1 timed out"</p>	<ul style="list-style-type: none"> 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: <ul style="list-style-type: none"> 方法1: 重启Cloud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: <ol style="list-style-type: none"> 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。
<pre>{ "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" }, "createTime": 1488170137857, "type": { "_name": "key.event.API.API_EVENT" }, "id": "e6bcd7c33ad9446b919e11cd647fc8dc" }</pre>	<ul style="list-style-type: none"> 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。
<p>all mons failed to execute http call[/ceph/primarystoragevolume/clone]</p>	<ul style="list-style-type: none"> 解决方案: 重连主备存储。
<p>failed to start vm[uuid:4ef5a9e4ae6441c7b046c384c3ae6f7f name:stack_local] on kvm host[uuid:d0d9800a09c34da4891e0cc624a0d349, 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_plugin.py", line 2721, in start_vm self._start_vm(cmd) File "/var/lib/zstack/virtualenv/kvm</p>	<ul style="list-style-type: none"> 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。

异常信息	异常原因及解决办法
<pre>/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.vmlInstanceUuid , 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.</pre>	
<pre>" code" : " SYS.1006" ,description:An operation failed, details:failed to check physical network interfaces on lvm</pre>	<ul style="list-style-type: none"> 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。
<pre>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 128b30ee8cb","restartDnsmasqAfterNu mberOfSIGUSER1":0}"</pre>	<ul style="list-style-type: none"> 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: 打开 <code>/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties</code> 修改 <code>management.server.ip = xxx.xxx.xxx.xxx</code> 这个IP地址，修改为可以访问出去的IP地址。
<pre>failed: Error in connection establishment: net::ERR_CONNECTION_REFUSED</pre>	<ul style="list-style-type: none"> 原因: 未设置控制台代理 解决方案: 登录UI，在 平台管理 > 控制台代理 页面，设置控制台代理地址

异常信息	异常原因及解决办法
Could not access KVM kernel module: No such file or directory failed to initialize KVM : No such file or directory.	<ul style="list-style-type: none"> 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。

17.6 日志分析

相关日志记录地址：

类型	日志路径	日志所在服务器
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
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
VPC路由器的日志	/home/vyos/zvr/zvr.log	VPC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。

17.7 端口占用

Cloud端口占用列表如下：

端口号	进程名	说明
25	master	邮件服务器
53	dnsmasq	DHCP服务
80	httpd	Web服务器
123	ntpd	NTP/Chrony时间同步服务
3306	mysqld	MySQL进程
4100~4200	usbredirserve	USB重定向服务
4369	epmd	erlang port mapper daemon
4900	consoleproxy	控制台代理
5000	/bin/java	CloudUI服务（HTTP方式）
5345	lttng-sessiond	内核跟踪框架
5443	/bin/java	Cloud UI服务（HTTPS方式）
5900	qemu-kvm	KVM控制台服务
6080	websockify	部署服务器代理服务
7069	python	监控数据采集
7070	kvmagent	KVM Agent代理服务

端口号	进程名	说明
7272	zstack-vyos agent	VPC路由器代理服务
7758	python	控制台代理服务
7761	python	Ceph镜像服务器
7762	python	Ceph主存储
7770	python	部署服务器
7771	nginx	部署服务器代理服务
7772	nginx	部署服务器代理服务
8000	zstore	镜像仓库zstore进程占用
8001	zstore	镜像仓库zstore进程占用
8005	/bin/java	Cloud管理服务
8080	/bin/java	Cloud管理服务
8081	/bin/java	Cloud管理服务
8086	influxd	监控数据存储
8088	influxd	监控数据存储
8090	nginx	Cloud管理服务（管理节点裸金属控制台代理）
9090	prometheus	Prometheus主监控进程
9091	pushgateway	监控数据缓存（管理节点）
9092	pushgateway	监控数据缓存（计算节点）
9093	pushgateway	监控数据缓存（裸金属部署服务器）
9100	node_exporter	监控数据采集
9103	collectd_expo	监控数据采集
16509	libvirtd	libvirtd服务
18081	zstack-hamon	多管理节点高可用监控服务

17.8 网络脚本

Cloud定制版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 [ mimon=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](#)。

17.9 删除资源

删除操作属于Cloud云平台中的高危操作，直接影响数据面，操作不慎可能造成数据丢失等严重损失，本章节主要针对高危删除操作进行总结。

表 18: 删除场景梳理

操作	注意事项
删除区域	删除区域将同时删除其下所有子资源，例如：集群、物理机、网络、主存储、vCenter等，请谨慎操作。
删除集群	<ul style="list-style-type: none"> 删除集群将同时删除其下所有物理机； 若集群中已加载本地存储，删除集群将同时删除相关物理机上的全部云主机和云盘，请谨慎操作。
删除物理机	<ul style="list-style-type: none"> 删除物理机会停止物理机上所有云主机； 若集群中已加载本地存储，删除集群将同时删除相关物理机上的全部云主机和云盘，请谨慎操作。 若物理机已被指定为迁移服务器，删除物理机将同时删除相应的迁移服务器，且自动取消该迁移服务器上正在执行的迁移任务，请谨慎操作。
删除主存储	删除主存储将会删除其上所有资源，例如：云主机、云盘、快照等，请谨慎操作。
删除镜像服务器	删除镜像服务器将删除此服务器上所有镜像，请谨慎操作。
删除VXLAN Pool	删除VXLAN Pool将同时删除此Pool下所有VxlanNetwork及其相关三层网络。
删除二层网络	删除二层网络会删除其下三层网络及相关的路由器，并卸载相应云主机的网卡。
删除公有网络	删除公有网络会卸载正在使用此网络的云主机网卡，并删除相应的路由器、网络服务和路由器规格，请谨慎操作。
删除系统网络	删除系统网络将同时删除相关的路由器。
删除私有网络	删除私有网络会卸载正在使用此网络的云主机网卡。
删除vCenter	删除 vCenter 会删除与 vCenter 相关的资源，请谨慎操作。
删除部署服务器	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。
删除VPC路由器	删除VPC路由器，会导致相关的云主机网络服务不可用，需重启云主机才可恢复网络服务，请谨慎操作。
删除路由器镜像	删除路由器镜像可能导致无法创建路由器，请谨慎操作。
删除路由器规格	删除路由器规格可能导致无法创建路由器，请谨慎操作。

操作	注意事项
删除云主机	<ul style="list-style-type: none"> 删除云主机后，云主机相关资源立刻被删除； 删除云主机后，云主机的启用状态会被标记为已删除，并移至已删除页面，系统默认24小时后彻底删除该云主机； 如果选择彻底删除后，云主机相关资源会被彻底删除，不可逆转，请谨慎操作； 删除云主机时勾选已加载云盘，会删除此云主机已加载的所有普通云盘，不会删除共享云盘。
删除云盘快照	<ul style="list-style-type: none"> 本地存储、NFS、SMP和Shared Block存储上创建的快照有树状结构，删除树根快照，删除快照将同时删除其子分支上的快照，请谨慎操作； 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； Shared Block主存储上创建的共享云盘，不支持创建快照。
删除光驱	删除光驱会将该光驱内已有ISO卸载。
删除弹性伸缩组	删除伸缩组，将一并删除组内全部云主机，请谨慎操作。
删除安全组	删除安全组，将自动删除所有的安全组规则和相关安全组服务。
删除虚拟IP	删除虚拟IP会删除其相关的网络服务。
删除弹性IP	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。
删除端口转发	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。
删除负载均衡器	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。
删除监听器	删除监听器，将自动删除其提供的负载均衡服务。
删除IPsec隧道	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。
删除报警器	删除报警器的同时将移除报警器上所有资源并不再报警，请谨慎操作。
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。
删除资源栈	删除资源栈默认会彻底删除栈内编排创建的所有资源，包括云主机或云盘，请谨慎操作。
删除计费设置	<ul style="list-style-type: none"> 删除历史计费设置，不影响相应账单计费；

操作	注意事项
	<ul style="list-style-type: none"> 删除当前使用的计费设置，相应账单会立即生成一次（计费时间段为：最近一次账单生成时刻 - 删除操作生效时刻），且不再继续计费。
删除AccessKey	删除AccessKey后，通过该AccessKey授权的API访问权限失效，无法打开控制台，请谨慎操作。
删除账户	删除策略是直接删除时，账户下的云主机和云盘将彻底删除；若为延迟删除，账户下的云主机和云盘状态为已删除状态，资源所有者变更为admin。
删除企业管理中的用户	删除用户会导致其所在的工单流程不可用，请谨慎操作。

17.10 卸载资源

卸载操作属于Cloud云平台高危操作，本章节主要对高危卸载操作进行总结。

表 19: 卸载场景梳理

操作	注意事项
从主存储卸载集群	将集群从主存储卸载有以下影响，请谨慎操作： <ul style="list-style-type: none"> 该主存储上的所有云主机和VPC路由器将关机； 该主存储上的所有云盘不能正常使用。
从集群卸载二层网络	从集群卸载二层网络后，相应云主机的网卡将被卸载，请谨慎操作。
从集群卸载主存储	将主存储从集群卸载有以下影响，请谨慎操作： <ul style="list-style-type: none"> 该主存储上的所有云主机和VPC路由器将关机； 该主存储上的所有云盘不能正常使用。
卸载裸金属集群	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。
从VXLAN Pool卸载集群	从VXLAN Pool卸载集群后，相应云主机的网卡将被卸载，请谨慎操作。
从二层网络卸载集群	从二层网络卸载集群后，相应云主机的网卡将被卸载，请谨慎操作。
从VPC网络卸载VPC路由器	请确保无云主机使用此VPC网络，再从VPC网络卸载VPC路由器。
卸载云盘	<ul style="list-style-type: none"> 将之前添加的云盘从云主机卸载，支持运行和停止状态的云主机卸载云盘。

操作	注意事项
	<ul style="list-style-type: none">从运行中的云主机卸载云盘可能影响业务连续性，请谨慎操作。
云主机卸载网卡	<ul style="list-style-type: none">云主机支持动态卸载网卡（卸载网络）；卸载网卡会解绑相关的网络服务，请谨慎操作。
卸载ISO	<ul style="list-style-type: none">将已添加的ISO镜像从云主机中卸载，支持运行和停止状态的云主机卸载ISO，支持批量卸载；从运行中的云主机卸载ISO可能影响业务连续性，请谨慎操作。
卸载块设备	卸载云主机上已加载的块设备，支持运行和停止状态的云主机卸载块设备。
卸载物理GPU	<ul style="list-style-type: none">云主机卸载物理机GPU设备，支持热插拔；对运行中的云主机卸载物理GPU，可能导致云主机蓝屏以及暂停，建议关机后再卸载物理GPU。
卸载vGPU设备	将vGPU设备从云主机卸载。注意：执行加载、卸载vGPU操作前，请确保云主机状态为已停止。
卸载USB设备	云主机卸载USB设备,支持运行和停止状态的云主机卸载USB设备。

18 云平台其他运维

18.1 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。

18.1.1 普罗米修斯升级 (Prometheus)

Cloud支持Prometheus，用于数据监控相关功能。提供两个版本Prometheus的支持，根据Cloud支持程度不同，如下：

- Prometheus-1.8.2: Cloud所有版本支持。
- Prometheus-2.9.2: Cloud 3.5.0版本及以后版本支持，在系统稳定性、资源使用优化，以及功能性方面都有很大的提升。

版本升级机制

Cloud版本升级应该注意以下情况：

- Cloud 3.5.0之前版本升级到Cloud 3.5.0及之后版本，默认继续使用Prometheus-1.8.2。
- Cloud 3.5.0及之后版本，升级后Prometheus继承原来版本。
- 初装Cloud 3.5.0及之后版本，默认使用Prometheus-2.9.2。

Prometheus版本切换

Cloud 3.5.0及之后版本同时支持两个版本的Prometheus，可通过如下方法进行版本切换：

- 依次执行如下命令，将Prometheus-1.8.2切换为Prometheus-2.9.2：

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=2.x
[root@localhost ~]# zstack-ctl restart_node
```



注：Cloud 3.5.0之前版本升级到Cloud 3.5.0及之后版本，再启用Prometheus-2.9.2将导致旧的监控无法显示。若启用Prometheus-2.9.2的同时保证旧的监控数据依旧生效，请依次执行如下命令：

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=2.x-compatible
[root@localhost ~]# zstack-ctl restart_node
```

- 依次执行如下命令，将Prometheus-2.9.2切换为Prometheus-1.8.2：

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=1.8.2
```

```
[root@localhost ~]# zstack-ctl restart_node
```

- 依次执行如下命令，禁用Prometheus，禁用后监控数据不可用：

```
[root@localhost ~]# zstack-ctl configure Prometheus.versionMode=none
[root@localhost ~]# zstack-ctl restart_node
```

全局设置

Prometheus支持以下两个全局设置，请管理员在**设置 > 全局设置 > 高级设置**进行配置：

- **监控数据保留周期：**监控数据在本地保留的月数，最多保留12月，默认：6月。
- **监控数据保留大小：**对于Prometheus-2.9.2，通过设置监控数据保留大小实现对监控目录使用空间的限制，默认：50G。

18.1.2 zstack.properties核心配置文件

zstack.properties是Cloud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*

zstack.properties参数说明

以下是**zstack.properties**文件内容的详细说明。

表 20: zstack.properties

类别	参数	解释
数据库	<ul style="list-style-type: none"> • 单管理节点：DB.url = jdbc:mysql://管理节点真实IP:3306 • 双管理节点：DB.url = jdbc:mysql://VIP:3306 	数据库URL、端口
	DB.user = zstack	数据库用户名
	DB.password = REoVaLs+sSFz5WKl8KVzjPQOt0gyL7Mpkklx6PJNB6urlpkp4U1rQsDkHGekirfG	数据库密码。默认zstack.password

类别	参数	解释
		 注： 为了保障账户安全，云平台已通过加密方式保存数据库密码。
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
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	<ul style="list-style-type: none"> 单管理节点: sns.systemTopic.endpoints.http.url = http://localhost:5000/zwatch/webhook 双管理节点: sns.systemTopic.endpoints.http.url = http://VIP:5000/zwatch/webhook 双管理节点: ticket.sns.topic.http.url = http://VIP:5000/zwatch/webhook 	ZWatch通知的系统接收端

类别	参数	解释
Cloud YUM	Ansible.var.zstack_repo = "zstack-mn,qemu-kvm-ev-mn"	Cloud使用的YUM源名称
管理节点服务	<ul style="list-style-type: none"> 单/双管理节点: management.server.ip = 管理节点真实IP 双管理节点: management.server.vip = VIP 	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
镜像仓库服务器	imagestore.backupstorage.primary.storage.priority = [{"PS\\": "Ceph\\", "priority\\": "5"}], [{"PS\\": "LocalStorage\\", "priority\\": "10"}]	指定了镜像服务器是镜像仓库类型的主存储分配优先级, 数字越小表示优先级越高。

注意事项

- 历史版本（3.2.0之前）可以在zstack.properties配置API的默认超时时间，例如：

```
ApiTimeout.org.zstack.header.image.APIAddImageMsg = timeout::3h
```

3.2.0兼容这种方式。当升级到3.2.0及后续版本时，在创建对应API的全局配置时，使用zstack.properties中配置的API timeout值作为该API全局配置的默认值。



注：升级到3.2.0后，通过zstack.properties配置API timeout的方式已不再需要，所有API的超时可通过全局配置设置。

- 从Cloud 3.3.0开始，支持设置AD/LDAP、邮箱服务器的接连超时时间，设置方法如下：

进入/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties，在zstack.properties配置文件中设置如下参数：

- Ldap.addServer.connectTimeout = XX

- # 设置AD/LDAP连接超时时间
- SNS.addEmailPlatform.connectTimeout = XX
设置邮箱服务器连接超时时间
- SNS.addEmailPlatform.readTimeout = XX
设置邮箱服务器读取数据超时时间



注:

- 系统默认上述三个参数的超时时间均为5000（单位默认为ms）；
- 若需修改超时时间，可通过zstack-ctl configure命令进行修改，例如：

```
[root@localhost ~]# zstack-ctl configure Ldap.addServer.connectTimeout = 10000
[root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.connectTimeout = 10000
[root@localhost ~]# zstack-ctl configure SNS.addEmailPlatform.readTimeout = 10000
```

设置完成后使用zstack-ctl restart_node命令重启管理节点生效。

- 从Cloud 3.3.0开始，支持设置ivshmem设备（虚拟PCI设备，实现云主机与物理机之间内存共享）的内存名称，设置方法如下：

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

，在zstack.properties配置文件中设置如下参数：

```
Kvm.ivshmem.dev.prefix = nu_fsec-$prefix$VMUUID
# 设置共享内存名称
```

- Cloud 3.7.1开始，支持设置多管理节点高可用场景下监控服务zstack-hamon端口，设置方法如下：

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

，在zstack.properties配置文件中设置如下参数：

```
Prometheus.zsha2ExporterPort = 18081
# 设置多管理节点高可用场景下监控服务zstack-hamon端口
# 默认端口18081为prometheus的exporter
```

- Cloud 3.9.0开始，支持在镜像服务器为本地存储时设置主存储优先级，设置方法如下：

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

，在zstack.properties配置文件中设置如下参数：

```
imagestore.backupstorage.primary.storage.priority = [{"PS":"Ceph\\", "priority":"10"}, {"PS":"LocalStorage\\", "priority":"1"}]
# 配置云主机使用本地主存储
```

- Cloud 3.10.0开始，支持设置日志语言，方法如下：

进入 `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`，在 `zstack.properties` 配置文件中设置如下参数：

```
locale = en
```

18.1.3 zstack.ui.properties核心配置文件

`zstack.ui.properties` 是 Cloud 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 21: `zstack.ui.properties`

类别	参数	解释
管理节点	<ul style="list-style-type: none"> 单管理节点: <code>mn_host = 127.0.0.1</code> 双管理节点: <code>mn_host = 管理节点真实IP</code> 	管理节点IP <ul style="list-style-type: none"> 单管理节点默认为 127.0.0.1 双管理节点默认为管理节点真实IP
	<code>mn_port = 8080</code>	管理节点端口，默认 8080
Webhook 主机	<ul style="list-style-type: none"> 单管理节点: <code>webhook_host = 127.0.0.1</code> 双管理节点: <code>webhook_host = VIP</code> 	Webhook 主机IP <ul style="list-style-type: none"> 单管理节点默认为 127.0.0.1 双管理节点默认为 VIP
	<code>webhook_port = 5000</code>	Webhook 主机端口，默认 5000
UI 服务器	<code>server_port = 5000</code>	UI 服务器端口，默认 5000
UI 日志	<code>log = /usr/local/zstack/apache-tomcat/logs</code>	UI 日志文件夹，默认 <code>/usr/local/zstack/apache-tomcat/logs</code>
UI HTTPS	<code>enable_ssl = false</code>	启用/关闭 HTTPS 登录 UI
	<code>ssl_keyalias = zstackui</code>	UI 证书别名，默认 <code>zstackui</code>
	<code>ssl_keystore = /usr/local/zstack/zstack-ui/ui.keystore.p12</code>	UI 证书路径，默认 <code>/usr/local/zstack/zstack-ui/ui.keystore.p12</code>

类别	参数	解释
数据库	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
	db_url = jdbc:mysql://10.0.5.87:3306	UI数据库URL，默认jdbc:mysql://10.0.46.243:3306
数据库	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

18.1.4 云平台硬件资源密码变更

对于Cloud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Cloud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Cloud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。

18.1.5 管理节点更改物理环境

Cloud的授权与用户的物理主机的环境——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Cloud的授权失效，而启动失败。此时请联系官方技术支持获取帮助。

18.1.6 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Cloud的相关服务器挂掉，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。

18.1.7 本地存储空间扩容

前提条件

在使用Cloud产品过程中，如果本地存储空间容量不足，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/`cloud_ps`扩容的样例。

操作步骤

1. 设置待扩容的物理机进入维护模式：
2. 插入新的大容量磁盘至物理机，并进行分区格式化，假定设备名称为/`dev/sdc`：
3. 创建新目录/`new_volume`，并执行以下命令挂载此磁盘：

```
mount /dev/sdc1 /new_volume
```

4. 执行以下命令，拷贝原始的磁盘文件至新磁盘：

```
rsync -a /cloud_ps /new_volume/
```

5. 执行以下命令，将挂载目录/`cloud_ps`和/`new_volume`均卸载：

```
umount /cloud_ps  
umount /new_volume
```

6. 执行以下命令，将新的大容量磁盘挂载到原本的主存储目录：

```
mount /dev/sdc1 /cloud_ps
```

7. 修改/`etc/rc.d/rc.local`，添加以下内容：

```
mount /dev/sdc1 /cloud_ps
```

8. 针对/`etc/rc.d/rc.local`，赋予可执行权限：

```
chmod +x /etc/rc.d/rc.local
```

9. 在云平台界面启用物理机，并重连物理机，启动其上的云主机，检查磁盘扩容后，数据依然可用。

10. 正常恢复后，原本的磁盘及其内部数据可不再留存，用于其他用途。

18.1.8 云主机根云盘扩容

Cloud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：

- 新容量必须大于当前容量，且增量不得小于4MB。
- 新容量必须为4MB的倍数，例如：填写新容量为37MB，实际扩容到40MB。

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GPartedISO，下载路径可参考GParted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 swspace 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 swspace 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 00"
#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。

18.2 Shared Block共享云盘升级

如需对Shared Block共享云盘升级，请根据以下步骤进行操作：

1. 执行以下命令，查询需要被更新的已被卸载的Shared Block共享云盘，并确定这些云盘需要进行格式转换：

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation convert_volume --admin-password password
```

2. 执行以下命令，将查询到的需要转换格式的Shared Block共享云盘，由qcow2格式转换为raw格式：

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation convert_volume --admin-password password --dryrun False
```

3. 执行以下命令，查询可以被删除的原qcow2格式的Shared Block共享云盘：

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation delete_qcow2_volume --admin-password password
```

4. 确保格式转换后数据完整性，然后执行以下命令，删除原qcow2格式的Shared Block共享云盘：

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation delete_qcow2_volume --admin-password password --dryrun False
```

5. 执行以下命令，将Shared Block共享云盘中的快照创建成镜像文件，留作备份：

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation commit_snapshot_to_image --admin-password password --backup-storage-uuid XXXXX --dryrun False
```

6. 执行以下命令，删除原qcow2格式的快照：

```
[root@localhost ~]# zstack-ctl fix_sharedvolume --operation delete_shared_volume_snapshots --admin-password password --dryrun False
```

18.3 企业版Ceph变更时间

针对不同版本企业版Ceph，变更时间操作方法不同，若需要对企业版Ceph变更时间，**请联系官方技术支持**进行操作，推荐方法如下：

- 企业版Ceph 3.1.9及以上版本，请按照以下步骤进行操作：



注：企业版Ceph变更时间前需要进行以下准备工作：

- 确保Ceph状态为**ok**，UI服务器状态均为健康。
- 规划好时间服务器角色分配，避免二次变更。

1. 在所有客户端节点，使用如下命令查看Ceph集群内时间同步情况，确保时间同步：

```
[root@ Ceph ~]# chronyc sources -v #输出为*表示时间同步正常
```

2. 手动变更时间服务节点时间，然后执行如下命令重启时间服务进程：



注: 此时不要将此节点client端指向自己。

```
[root@ Ceph ~]# service chronyd restart
```

- 待时间服务节点时间正常后，在Ceph集群其他节点依次执行如下命令，重启服务器的chronyd服务，并检查结果：

```
[root@ Ceph-1 ~]# service chronyd restart
```

```
[root@ Ceph-1 ~]# chronyc sources -v #输出为*表示时间同步
```

- 在每台Ceph集群的节点上执行如下命令，重启xmsd服务：

```
[root@ Ceph-1 ~]# systemctl restart xmsd
```

- 执行以下命令，将更改后的当前时间写入服务器硬件时间：

```
[root@ Ceph ~]# hwclock -w
```

- 确保时间变更成功后，在管理节点的配置文件（`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`）中指定时间节点IP：`chrony.serverip.0 = XXX`（XXX为时间服务节点IP），然后执行命令`service chronyd restart`重启管理节点时间服务。



注: 时间变更操作完成后，可参考以下方法进行检查：

- 使用`ceph -s`命令，确认Ceph状态是否为ok。
 - 使用`chronyc sources -v`命令，确认时间是否同步（输出为*）。
 - 确认修改后时间是否达到预期，确认存储UI下每台服务器状态为健康，确认存储池状态为健康。
- 企业版Ceph 3.1.9以下版本，请按照以下步骤进行操作：
 - 停止所有业务云主机（含管理节点云主机）；
 - 调整时间同步；
 - 执行命令`systemctl restart xmsd`重启各节点的xmsd服务；
 - 确保时间变更成功后，在管理节点的配置文件（`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`）中指定时间节点IP：`chrony.serverip.0 = XXX`（XXX为时间服务节点IP）；
 - 执行命令`service chronyd restart`重启管理节点时间服务。

18.4 集群时间源变更

Cloud采用chrony时间同步服务确保整个集群节点时间一致性。集群内物理机默认根据云平台管理节点`zstack.properties`配置文件中指定的时间源进行时间同步。

集群时间源变更操作步骤

假定集群环境信息如下：

表 22: 物理机配置信息

节点	IP	备注
物理机1	192.168.100.1	集群内时间源A
物理机2	192.168.100.2	集群内时间源B
物理机3	192.168.100.3	时间源待变更物理机3
物理机4	192.168.100.4	时间源待变更物理机4

若集群需变更时间源，请参考以下步骤进行操作：

1. 进入管理节点配置文件`/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties`，修改/增加以下参数，指定时间源服务器IP：

```
[root@localhost ~]# cd /usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/
[root@localhost ~]# vim zstack.properties
...
chrony.serverip.0 = 192.168.100.1
chrony.serverip.1 = 192.168.100.2
...
```

注:

- `zstack.properties`配置文件只配置一个内部时间源，建议按照以上命令配置两个内部时间源服务器。
 - 若为双管理节点架构，需同时进入两个管理节点的`zstack.properties`配置文件进行配置。
2. 分别进入两个时间源服务器`/etc/chrony.conf`配置文件，增加如下内容，将时间源服务器与公网时间源服务器进行时间同步：

```
[root@localhost ~]# cd /etc/
[root@localhost ~]# vim chrony.conf
...
server ntp.aliyun.com iburst
server 0.centos.pool.ntp.org
local stratum 10
```

```
allow 0.0.0.0/0
...
```



注:

- *ntp.aliyun.com* 和 *ntp.aliyun.com* 分别为公网时间源服务器，也可使用其他公网时间源服务器。
- 建议集群内的时间源服务器与公网或企业内部时间源服务器同步。

3. 分别进入两个时间源服务器执行以下命令，重启chrony时间同步服务:

```
[root@localhost ~]# systemctl restart chronyd
```

4. 分别进入两个时间源服务器执行以下命令，确认时间是否同步:

```
[root@localhost ~]# chronyc sources -v //输出为*表示时间同步正常
```

5. 分别进入两个时间源服务器执行以下命令，将更改后的当前时间写入服务器硬件时间:

```
#集群内时间源服务器与外部时间源服务器完成时间同步
[root@localhost ~]# hwclock -w
```


6. 在Cloud管理节点分别执行以下命令，重启管理节点服务，使新配置内容生效:

- 单管理节点:

```
[root@localhost ~]# zstack-ctl stop && zstack-ctl start
```

- 双管理节点:

```
[root@localhost ~]# zsha2 stop-node && zsha2 start-node
```

-  **注:** 管理节点服务重启完成后，所有物理机的时间源会自动修改为**zstack.properties**配置文件中指定的时间源，并重启物理机的chrony时间同步服务。同时会自动重连所有硬件资源，请在云平台确认所有硬件设施连接状态均恢复为已连接。

7. 随机选择一台物理机执行以下命令，确认时间是否同步:

```
#输出为*表示时间同步正常
[root@localhost ~]# chronyc sources -v
```



注: 若该台物理机时间同步成功，则可确认所有物理机时间同步成功。

8. （可选）在各台物理机上分别执行以下命令，将更改后的当前时间写入物理机硬件时间：

```
[root@localhost ~]# hwclock -w
```



注：用户可根据自身业务情况选择执行该命令。若选择不执行该命令，需确保以上操作均准确无误。

注意事项

修改物理机时间，默认Windows云主机时间会随物理机时间变更，可能影响上层业务。若不希望云主机时间随物理机时间修改而变更，可任选以下方法：

- 可关闭云主机时间同步策略。



注：关闭云主机同步策略，重启后生效。

- 在云主机系统内单独指定时间源。



注：Windows系统默认的时间同步间隔为7天，通过修改系统注册表，修改Windows系统自动同步间隔，提高同步次数保证时钟的精度。

19 物理基础设施运维

本章主要针对物理基础设施给出的运维方法。生产环境的运维操作，需要参考此文档所述流程进行规范化操作，否则会引发不可控风险。

19.1 机房电力运维

机房计划性关机下电

机房计划性关机下电步骤如下：

1. 停止所有运行的业务。
2. 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。
3. 将所有物理主机进入维护模式。
4. 停止管理节点，不同场景停止管理节点的方法如下：
 - 若采用单管理节点方案，执行 `zstack-ctl stop` 停止管理节点
 - 若采用多管理节点物理机高可用方案，在每个管理节点执行 `zsha2 stop-node` 停止管理节点并关闭 `zsha2` 服务
5. 确保云平台主存储没有IO操作后，在各物理机执行 `poweroff` 正常关闭所有物理机。
6. 关闭存储（NFS/Ceph/SAN/SMP等）。
7. 关闭交换机及其他硬件设施。

机房计划性上电开机

机房计划性上电开机步骤如下：

1. 开启交换机电源。
2. 开启存储电源（NFS/Ceph/SAN/SMP等）。
3. 开启服务器电源。
4. 检查管理节点服务状态，确保管理节点服务启动成功。不同场景检查管理节点的方法如下：
 - 若采用单管理节点方案，执行 `zstack-ctl status` 查看管理节点状态
 - 若采用多管理节点物理机高可用方案，在其中一个节点执行 `zsha2 status` 查看高可用状态和管理节点状态
5. 登录Cloud云平台，启用所有主存储和所有物理机，确保物理机和主存储是已连接状态。
6. 启动业务云主机，恢复业务。

机房意外断电恢复

机房意外断电恢复步骤与计划性上电步骤相同，如下：

1. 开启交换机电源。
2. 开启存储电源（NFS/Ceph/SAN/SMP等）。
3. 开启服务器电源。
4. 检查管理节点服务状态，确保管理节点服务启动成功。不同场景检查管理节点的方法如下：
 - 若采用单管理节点方案，执行 `zstack-ctl status` 查看管理节点状态
 - 若采用多管理节点物理机高可用方案，在其中一个节点执行 `zsha2 status` 查看高可用状态和管理节点状态
5. 登录Cloud云平台，启用所有主存储和所有物理机，确保物理机和主存储是已连接状态。
6. 启动业务云主机，恢复业务。

19.2 机房搬迁运维

机房搬迁请参考以下步骤操作：

1. 将所有电源正常关闭。
2. 标记所有交换机接线接入端和物理机接入端接口。
3. 封装打包服务器，搬迁服务器到新机房并接线。
4. 将所有电源开启。
5. 检查网络、云平台及业务云主机恢复状态。

19.3 交换机运维

管理网络交换机运维

管理网络交换机运维，可能影响业务正常运行，**请谨慎操作**。若必须运维，建议调整在业务波谷进行。运维步骤如下：

1. 云平台全局设置关闭云主机高可用。
2. 停止管理节点，不同场景停止管理节点的方法如下：
 - 若采用单管理节点方案，执行 `zstack-ctl stop` 停止管理节点
 - 若采用多管理节点物理机高可用方案，在每个管理节点执行 `zsha2 stop-node` 停止管理节点并关闭zsha2服务
3. 调整重启相关的管理交换机。

4. 检查交换机接入端的所有硬件资源IP连通性（物理机、主存储、镜像服务器），确保所有接入端管理网络正常通信。



注：若存在节点无法连通管理节点，请处理故障后继续进行后续操作。

5. 启动并检查管理节点服务状态，确保管理节点服务启动成功。不同场景启动检查管理节点的方法如下：
 - 若采用单管理节点方案，执行 `zstack-ctl start` 启动管理节点服务，执行 `zstack-ctl status` 查看管理节点状态
 - 若采用多管理节点物理机高可用方案，在两个管理节点分别执行 `zsha2 start-node` 启动管理节点服务，在其中一个节点执行 `zsha2 status` 查看高可用状态和管理节点状态
6. 确保所有物理机和主存储均是已连接，云平台全局设置开启云主机高可用。

业务网络交换机运维

业务网络交换机运维建议调整在业务波谷进行，避免影响重要业务。运维步骤如下：

1. 将接入此交换机相关的物理机进入维护模式。
2. 调整重启相关的业务交换机。
3. 启用处于维护模式状态的某一物理机，检查连通性。例如：使用此物理机创建一个测试云主机，检查此云主机与其他业务云主机连通性，连通表示此物理机对应的交换机接口配置正确可用，如果不可达，则需继续排查连通性。
4. 重复步骤3，依次检查连通性，确保所有的业务网络均可用；

存储网络交换机运维

存储网络交换机运维会直接影响所有业务，必须停止业务后进行操作。运维步骤如下：

1. 将云平台上所有与此存储交换机关联的主存储进入维护模式。
2. 登录企业版存储UI，点击**设置 > 禁止数据恢复 > 禁止按钮**。
3. 调整重启相关的存储交换机。
4. 确保所有存储节点的存储网络可互相连通并可达。
5. 登录企业版存储UI，点击**设置 > 允许数据恢复 > 启用按钮**。
6. 启用处于维护模式状态的主存储，确保主存储是已连接状态。
7. 启动已经停止的业务云主机。

20 常见问题

20.1 快速入门

1.

Q: Cloud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。
- 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Cloud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。
- 云平台还支持计费高级功能。
- 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,Cloud还有很多强大功能,更多精彩尽在Cloud。

2.

Q: Cloud有哪些文档? 用户应该看什么?

A: Cloud有如下文档:

- **版本特性:**

汇集各版本的特色功能介绍,用户可以了解Cloud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Cloud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Cloud,将会展开另一片新天地。

- **实践教程:**

针对不同应用场景提供实践教程，例如：《快速安装教程（新手快速入门）》、《升级教程》、《混合云使用教程》、《多管理节点物理机高可用教程》、《企业管理使用教程》、《灾备服务使用教程》、《迁移服务使用教程》、《裸金属管理使用教程》等。涵盖场景十分丰富多变，实践操作也很简单便捷，协助用户分分钟快速上手。

- **开发手册:**

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

- **常见问题:**

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Cloud，又不仅仅是Cloud，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Cloud，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？可查阅我们的实践教程，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。
- 接下来可尝试实践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Cloud环境。
- **开发手册**和**cli命令使用手册**是必须的工具，部分问题在实践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**。

20.2 安装部署

1. Q: Cloud支持哪些硬件环境？

A: Cloud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: Cloud支持哪些操作系统？

A: Cloud支持基于CentOS 7.4/7.6深度定制的Cloud定制版ISO。

3. Q: Cloud支持使用标准的CentOS 7.4/7.6系统安装么？

A: 暂不支持，Cloud目前支持基于CentOS 7.4/7.6深度定制的Cloud定制版ISO。

4. Q: 安装部署Cloud需要多少台服务器？

A: 最小安装只需要一台服务器，同时作为管理节点和计算节点；生产环境建议分离部署。Cloud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Cloud，服务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: Cloud定制版ISO可以安装哪些模式？有哪些差异？

A: Cloud定制版ISO支持以下几种模式：

1. NOLOGO Management Node: Cloud管理节点模式

安装基于CentOS 7.4/7.6深度定制的Cloud定制版ISO并安装Cloud管理节点。

2. NOLOGO Compute Node: Cloud计算节点模式

安装基于CentOS 7.4/7.6深度定制的Cloud定制版ISO并安装Cloud计算节点必备软件包。

3. NOLOGO Expert Node: Cloud专家模式

安装基于CentOS 7.4/7.6深度定制的Cloud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Cloud？

A: 请联系官方技术支持获取最新的Cloud定制版ISO。首次安装系统时，建议选择管理节点模式。操作系统安装完毕后，重启系统会自动安装管理节点。

8.

Q: 如何升级Cloud?

A: 如需将已部署Cloud升级至最新版本, 可参考以下两种方法进行升级 (以c76版本为例):

• 增量升级:

1. 请联系官方技术支持获取最新的bin安装包: Cloud-installer-4.1.3.bin
2. 若数据库root密码为默认密码, 请执行以下命令升级:

```
[root@localhost ~]# bash Cloud-installer-4.1.3.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:

```
[root@localhost ~]# bash Cloud-installer-4.1.3.bin -u -P MYSQL_ROOT_PASSWORD
```

• 离线升级:

1. 请联系官方技术支持获取最新的iso安装包: Cloud-x86_64-DVD-4.1.3-c76.iso
2. 获取最新的升级脚本: 请联系官方技术支持获取。
3. 执行以下命令升级:

```
[root@localhost ~]# bash Cloud-upgrade Cloud-x86_64-DVD-4.1.3-c76.iso
```



注: c74版本和c76版本升级方法相同, 请获取c74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:

```
[root@localhost ~]# yum --disablerepo=* --enablerepo=zstack-local install zstack-manager
[root@localhost ~]# bash Cloud-installer-4.1.3.bin -E
```

10.

Q: 如何从专家模式升级到计算节点?

A: 执行如下命令, 将专家模式升级为计算节点:

```
[root@localhost ~]# 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:

```
[root@localhost ~]# rpm -e zstack-host
[root@localhost ~]# yum --disablerepo=* --enablerepo=zstack-local install zstack-manager
```

```
[root@localhost ~]# bash Cloud-installer-4.1.3.bin -E
```

12.

Q: 如何重新安装Cloud?

A:

1. 先执行以下命令删除原本的数据库:

```
[root@localhost ~]# 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Cloud, 才可使用。

2. 再执行以下命令重装管理节点:

```
[root@localhost ~]# bash Cloud-installer-4.1.3.bin -D
```

13.

Q: 使用root安装Cloud为何启动服务提示非root?

A:

• 现象:

安装Cloud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。

14.

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。

15.

Q: 能在Cloud的云主机上安装Cloud吗?

A: 可以。在**全局设置的基本设置**中修改**云主机CPU模式**为**host-passthrough**, 透传物理主机的虚拟化特性。

16.

Q: 一键安装Cloud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Cloud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。

17.

Q: Cloud如何更改安装目录?

A: 安装Cloud时, 加上 **-r 目标目录**。例如:

```
[root@localhost ~]# bash Cloud-installer.bin -r /home/zstack
```

18.

Q: 升级时, 遇到Cloud定制版ISO版本不匹配怎么办?

A:

• **现象:**

升级时遇到Cloud定制版ISO版本不匹配, 会提示以下错误信息:

```
mount: /dev/loop0 is write-protected, mounting read-only
/root
Current release c76 not matched the new ISO c74,
Use Cloud-upgrade -r xxx.iso to update current repo,
```

```
Use Cloud-upgrade -a/--add_repo xxx.iso to add a new repo
```

- **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Cloud。

- **解决方案:**

请执行以下部署（以c76为例）：

1. 执行如下命令，下载最新的升级脚本

```
wget http://cdn.zstack.io/product_downloads/scripts/Cloud-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/Cloud-x86_64-DVD-4.1.3-c76.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 Cloud-upgrade Cloud-x86_64-DVD-4.1.3-c76.iso
```

19.

Q: Cloud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Cloud定制版ISO安装升级。

20.

Q: 升级Cloud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Cloud?

A:

- **前提:**

Cloud进行升级时，默认会备份当前Cloud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Cloud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Cloud环境:

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

5. 使用之前的安装包直接安装Cloud:

```
bash Cloud-installer-4.1.3.bin -D
```

6. 使用第一步备份的Cloud核心文件恢复:

```
zstack-ctl stop
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Cloud管理节点服务, 此时Cloud已成功恢复至原本升级失败前的版本

```
zstack-ctl start
```

21.

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:

- **原因:** Cloud 3.5.0之前版本使用prometheus 1.8.2, 可能出现监控数据占满根空间的情况。



注: Cloud 3.5.0及之后版本使用prometheus 2.9.2, 支持设置保留策略(默认保留50G监控数据), 不再出现此问题。

- **解决方案:** 确认监控数据不需要的情况下, 彻底删除prometheus监控数据, 释放空间。

– 单管理节点环境, 依次执行如下命令, 删除prometheus监控数据:

```
[root@hostname ~]# du -sh /var/lib/zstack/prometheus/data/ //查看监控数据大小
```



```
[root@hostname ~]# zstack-ctl stop
[root@hostname ~]# kill -9 `ps -ef |grep prometheus|awk '{print $2}'`
[root@hostname ~]# rm -rf /var/lib/zstack/prometheus/data
[root@hostname ~]# zstack-ctl start
```

- 双管理节点环境，分别在两个管理节点依次执行如下命令，删除prometheus监控数据：

```
[root@mn-1 ~]# du -sh /var/lib/zstack/prometheus/data/ //查看监控数据大小
[root@mn-1 ~]# zsha2 stop-node
[root@mn-1 ~]# kill -9 `ps -ef |grep prometheus|awk '{print $2}'`
[root@mn-1 ~]# rm -rf /var/lib/zstack/prometheus/data
[root@mn-1 ~]# zsha2 start-node
```

22.

Q：使用非官方Cloud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Cloud定制版ISO安装。

23.

Q：嵌套虚拟化环境中成功安装Cloud云平台，但在Cloud云平台中添加物理机时出现报错ERROR:could not insert 'kvm_intel':Operation not supported stdout，如何解决？

A：在KVM、VMWARE、VirtualBox、Hyperv、XEN等其他虚拟化环境中通过嵌套虚拟化搭建Cloud时，需在相应虚拟化平台的虚拟化引擎设置中开启虚拟化Intel VT-x/EPT或AMD-V/RVI(V)特性。

20.3 系统登录

1.

Q：Cloud推荐使用哪些浏览器？

A：为了获取更好的产品体验，请使用Chrome 49，Firefox 52 及以上版本的浏览器。

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服务。

3.

Q: 如何更改UI的admin密码?

A: 有三种方法:

- **UI方式:**

在Cloud**首页**点击admin信息的**修改密码**按钮进行修改。

- **CTL命令行方式:**

执行以下命令, 更改UI的admin密码:

```
[root@localhost ~]# zstack-ctl reset_password --password NEW_PASSWORD #更改密码 (NEW_PASSWORD为新密码)
```

- **CLI命令行方式:**

依次执行以下命令, 更改UI的admin密码:

```
[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>>> 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>>> 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Cloud同时登录次数?

A:

• UI方式:

在**设置 > 平台设置 > 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: 如何切换后端环境语言?

A: Cloud UI界面语言和后端环境语言相互独立。其中, 后端环境语言默认为中文, 请依次执行以下命令进行切换:

```
[root@localhost ~]# zstack-ctl configure locale=en_US #切换语言, en_US表示英文;
zh_CN表示中文
[root@localhost ~]# zstack-ctl restart_node #重启管理节点, 配置生效
```

8.

Q: 是否支持HTTPS方式登录UI?

A: Cloud支持设置HTTPS方式登录UI, 以及恢复HTTP方式登录。

20.4 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: Cloud的DHCP服务和目前机房的DHCP是否会出现冲突?

A: Cloud的DHCP服务与目前机房已经配置的DHCP服务不冲突。但Cloud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hostname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=MANAGEMENT_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: 修改控制台代理地址即可, 方法同上。

7.

Q: 怎么从IP Range中保留一个IP地址, 不让Cloud分配给云主机?

A:

- 目前还没有提供ReserverIpRange的API, 如果希望Cloud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>>> CreateVip l3NetworkUuid=YOU_L3_NETWORK_UUID name=for_reserver requiredIp=a.b.c.d
```

8.

Q：如何批量修改云主机的计算规格？

A：在**资源中心 > 云资源池 > 虚拟资源 > 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。

9.

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
```

10.

Q：Cloud给云主机的MAC地址，可以手动修改吗？

A：可以。Cloud支持停止状态的云主机修改MAC地址。

11.

Q：Cloud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。

12.

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: 机房计划性下电/上电、机房意外断电恢复的详细步骤。

13.

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。

14.

Q: 如何修改云主机的删除时延？

A:

- UI方式:

在**设置 > 平台设置 > 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
```

15.

Q: Cloud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。

16.

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。

17.

Q: 如何将KVM上的云主机迁移到Cloud中?

A: Cloud提供V2V迁移服务, 支持将基于KVM的源云平台的云主机及数据完整迁移至Cloud云平台。

18.

Q: Cloud如何设置云主机启动顺序?

A: 在**资源中心 > 云资源池 > 虚拟资源 > 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。

19.

Q: 如何在创建云主机时指定IP?

A: 大多数情况下, 云主机的IP地址由DHCP自动分配。对于需要指定IP的用户, 可参考以下步骤设置: 停止云主机, 然后进入云主机详情页, 在**配置信息**页面选中云主机挂载的某网卡点击**操作 > 设置指定IP**。

20.

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Cloud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。

21.

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/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/webapps/zstack/WEB-INF/classes/ansible/rsaKeys/id_rsa -N "" //命令中""为两个英文双引号
```

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/webapps/zstack/WEB-INF/classes/ansible/rsaKeys
```

22.

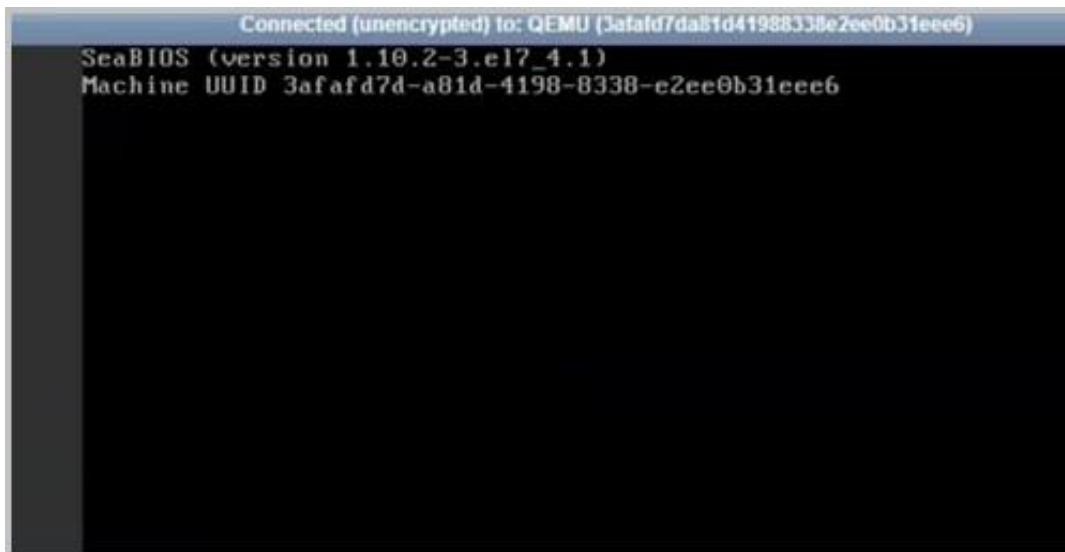
Q: 云主机控制台出现**Guest has not initialized the display (yet)**怎么办？

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
```

23.

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：在**设置 > 平台设置 > 全局设置 > 基本设置**页面，修改**云主机CPU模式**的值为**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。

24.

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。

25.

Q: 控制台代理出现IO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。

26.

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。

27.

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。

28.

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"
  },
}
```

```
"createTime": 1488170137857,
  "type": {
    "_name": "key.event.API.API_EVENT"
  },
  "id": "e6bcd7c33ad9446b919e11cd647fc8dc"
}
```

• **原因：**

两台物理机hostname相同。KVM云主机在线迁移依靠hostname进行确认物理机，若hostname相同即被认定为同一台物理机。

• **解决方案：**

建议对物理机设置不同的hostname。若遇到以上报错，请联系官方技术支持获取帮助。

29.

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Cloud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
```

30.

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。

31.

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。

32.

Q: Cloud云平台创建云主机失败的原因可能有哪些？

A:

- 镜像服务器失联，请确保镜像服务器可用并正常连接。
- 主存储未挂载集群，导致找不到可用的物理机，请确保主存储已挂载集群。
- 集群内没有可用的物理机满足计算规格的定义，请确保物理机可用，且资源满足。
- 主存储容量不足以提供镜像需要的虚拟容量，请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
- 镜像服务器与主存储链路异常，请确保镜像服务器下载镜像到主存储的链路正常。
- 确保物理机的分布式DHCP服务dnsmasq服务正常，以正常提供DHCP服务IP分配服务
- 确保物理机的Libvirt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

33.

Q: 在企业版Ceph主存储上创建云主机失败，该怎么处理？

A:

- 现象：

在企业版Ceph主存储上创建云主机，报错如下：

```

错误原因：failed to start vm[uuid:09779ea6fb6e4ae2ad6b239bf7dce7ee name:test]
on kvm host[uuid:8a769650069f40a7ac97c7b98ce650d5, ip:192.168.5.252], because
Traceback (most recent call last): File "/var/lib/zstack/virtualenv/kvm/lib/python2.7/
site-packages/kvmagent/plugins/vm_plugin.py", line 4708, in start_vm self._start_vm
(cmd) File "/var/lib/zstack/virtualenv/kvm/lib/python2.7/site-packages/kvmagent/plugins
/vm_plugin.py", line 4628, 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:09779ea6fb6e4ae2ad6b239bf7dce7ee, name:test], libvirt error: internal error: qemu
unexpectedly closed the monitor: 2021-01-13T10:14:38.093540Z qemu-kvm: -drive file
=rbd:pool-b35d1f59707e4c6aabdf74457daccf7133ff2b026449f8987ec8c0a10dbdee
:id=zstack:auth_supported=cephx\none:mon_host=172.25.15.120\;6789\;172.25.15.163
\;6789\;172.25.12.55\;6789,file.password-secret=virtio-disk0-secret0,format=raw,if=none
,id=drive-virtio-disk0: error reading header from 7133ff2b026449f8987ec8c0a10dbdee:
No such file or directory
    
```

• 原因：

企业版Ceph中，非Mon节点以外的物理机缺少网关服务器角色，导致云主机创建成功但无法正常启动。

• 解决方案：

登录企业版Ceph管理节点，将Mon节点以外的物理机，添加为网关服务器角色。

34.

Q：云主机的系统时间和物理机的系统时间有什么关系？

A：为了保障云主机时间同步正确，强烈建议为云主机配置独立的时间同步服务器。若为在云主机没配置时间同步服务器，不同操作系统的云主机时间同步机制如下：

- Linux云主机内部系统时间，会随着创建、启动、重启等操作，读取物理机时间作为时钟。云主机时间比物理机时间滞后还是提前，都会生效。
- 创建Windows云主机会自动读取物理机的时间作为时钟。
- 当Windows云主机内部系统时间比物理机时间滞后时，Windows云主机内部系统时间，会随着启动、重启等操作，读取物理机的时间作为时钟。
- 当Windows云主机内部系统时间比物理机时间提前时，启动、重启等操作无法读取物理机的时间。有可能与Windows系统许可策略有关，例如180天的试用过期后，每1小时会关机一次，倒退时间会逃避微软许可策略。



注：

- 底层物理机的时间源一般由管理节点配置文件的 `/usr/local/zstack/apache-tomcat/webapps/zstack/WEB-INF/classes/zstack.properties` 里面的 `chrony.serverlp.0 = 172.20.0.10` 的选项来定义（假设时间同步服务器为 172.20.0.10）。

- 管理节点将会同步所有的物理机采用相同的时间源，云主机在创建、启动时将跟随物理机的时间源。

35.

Q: 云主机支持系统盘扩容吗？

A: 支持。详情请参考《用户手册》的**系统扩容**章节。

36.

Q: GPU透传识别不到设备怎么解决？

A:

- `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 / AMD IOMMU选项

37.

Q: 可以在创建云主机的时候设置账户/密码吗？

A:

- 方法一：在**创建云主机 > 标准创建 > 系统配置 > SSH登录方式**列，选择**密码**按钮，支持设置云主机密码：
 - Linux镜像：固定用户名root，支持设置SSH密钥和密码。
 - window镜像：固定用户名administrator，仅支持设置密码。
- 方法二：在**创建云主机 > 标准创建 > 系统配置 > User Data**或**创建云主机 > 快捷创建 > User Data**列，通过Userdata注入方式设置账户/密码。

详情请参考《用户手册》的**创建云主机**章节。

38.

Q: 云主机ssh慢怎么解决？

A:

1. 在ssh服务器上更改/etc/ssh/sshd_config文件中配置如下：

```
UseDNS no
#GSSAPI options
GSSAPIAuthentication no
```

2. 执行命令`/etc/init.d/sshd restart`重启sshd服务。

39.

Q: 远程桌面Windows Server云主机时**提示CredSSP加密Oracle修正**，如何解决？

A: 请参考以下步骤启用加密Oracle修正：

1. 在企业版Windows操作系统的运行界面（windows+R），输入gpedit.msc并点击**确定**按钮，打开**本地组策略编辑**界面。
2. 点击**计算机配置 > 管理模板 > 系统 > 凭证分配 > 加密Oracle修正**按钮，进入**加密Oracle修正**界面。
3. 将**加密Oracle修正**配置修改为**已启用**，点击**应用**按钮，启用加密Oracle修正。



注：若应用后配置未生效，请重启操作系统。

40.

Q：使用三层网络创建Windows和Linux云主机，Windows云主机网络不可用，而Linux云主机可正常通信，原因是什么？

A：新创建的Windows云主机需安装对应版本的virtio网卡驱动并重启。

41.

Q：云主机使用共享存储且CPU模式设置为host-passthrough，在相同集群内在线热迁移失败，如何处理？

A：

• **现象：**

迁移时报如下错误消息：

```
Assertion `ret == cpu > kvm_msr_buf->nmsrs` failed
```

- **原因：**对端物理机的CPU型号和当前服务器CPU型号不同。
- **解决方案：**迁移到使用相同CPU的物理机，或者关闭云主机进行迁移。

42.

Q：使用UEFI模式引导的云主机，操作系统安装完成后进行重启，自动进入**UEFI shell**界面，该如何解决？

A：使用**vim /boot/efi/startup.nsh**命令写入以下内容并保存，然后重启云主机，即可正常启动。

```
FS0:
CD EFI
CD centos
shimx64-centos.efi
```

镜像

1.

Q：创建镜像的占用空间是怎样的？

A：

- **前提：**主存储未超分或者主存储使用厚置备：使用ImageStore类型的主存储。
- **举例说明：**假设主存储有800G的空间，创建一个400G的VM（假定为A），对A创建镜像（假定为B，B的实际大小并非400G，假定为10G）；用B创建新的VM（假定为C），此时B会从镜像服务器上下载到主存储的cache目录（需要消耗主存储的空间10G），镜像下载成功后，主存储的虚拟可用容量就仅剩390G，而创建VM需要400G容量，因此C无法成功创建。

2.

Q：创建镜像时提示URL相关错误一般有哪些方法？

A：

- Cloud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: 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程序并执行BLNSVR -I命令。

5.

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镜像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:** 从微软官网下载相应的ISO文件。

6.

Q: Windows virtio ISO的镜像在哪里可以找到?

A: 以c76版本为例, 在管理节点/opt/zstack-dvd/x86_64/c76/目录, 内置zstack-windows-virtio-driver.iso镜像

7.

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

8.

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

9.

Q: 对于安装Ubuntu 18版本操作系统的云主机, 若grub配置了splash选项, 云主机无法启动, 该如何解决?

A:

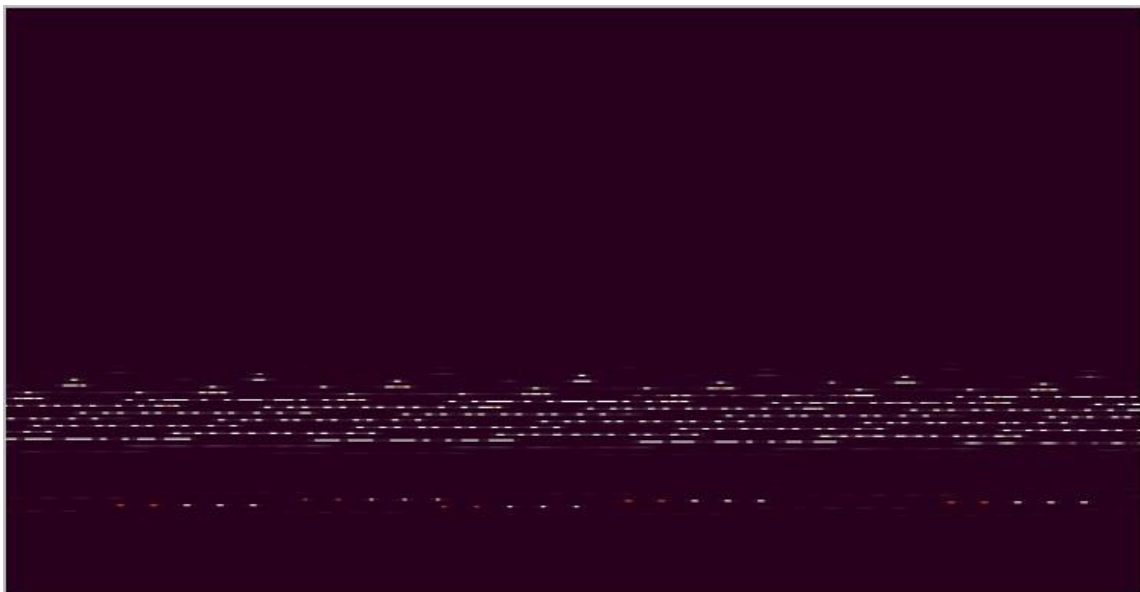
- **现象:** 对于安装Ubuntu 18版本操作系统的云主机, 若grub配置了splash选项, 云主机无法启动, 启动页面花屏, 如图 97: 云主机grub配置splash选项和图 98: 云主机启动页面花屏所示:

图 97: 云主机grub配置splash选项

```
setparams 'Ubuntu'

recordfail
load_video
gfxmode $linux_gfx_mode
insmod gzio
if [ x$grub_platform = xxen ]; then insmod xzio; insmod lzopio; fi
insmod part_msdos
insmod ext2
set root='hd0,msdos1'
if [ x$feature_platform_search_hint = xy ]; then
    search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 69d43d6c-eb78-4480-aa20-7d23c79f3bd0
else
    search --no-floppy --fs-uuid --set=root 69d43d6c-eb78-4480-aa20-7d23c79f3bd0
fi
linux    /boot/vmlinuz-4.15.0-20-generic root=UUID=69d43d6c-eb78-4480-aa20-7d23c79f3bd0 ro splash_ $vt_handoff
initrd   /boot/initrd.img-4.15.0-20-generic
```

图 98: 云主机启动页面花屏



- **解决方案：**请进入**设置 > 平台设置 > 全局设置 > 基本设置**，将**显卡类型**设置为vga，即可正常启动云主机。



注：该问题仅出现在Ubuntu 18版本中，Ubuntu 18之前的版本均无该问题。

10.

Q: Windows云主机无法设置分辨率怎么办？

A: CloudUI界面，进入**设置 > 平台设置 > 全局设置 > 基本设置**页面，将**云主机启动显卡类型**设置为**vga**，然后重启云主机。

11.

Q: Ceph主存储的云主机，创建镜像到ImageStore镜像服务器时间很长，为什么？

A: Ceph存储卷采用raw格式，创建镜像需要做全量数据拷贝。可以在创建云主机镜像后导出镜像，自行转换为qcow2格式，最后重新导入ImageStore镜像服务器。

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: Cloud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: 云主机上加载新的L3网络时，为何只显示一张网卡？

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，可通过以下方法识别网卡：

- 方法一：重启云主机，重启云主机将自动获取网卡信息。
- 方法二：手动配置网卡，无需重启云主机，步骤如下：
 1. 参考云主机里的 `/etc/sysconfig/network-scripts/ifcfg-eth0`，对新增的eth1网卡添加配置文件 `ifcfg-eth1`；
 2. 打开eth1网卡配置文件 `ifcfg-eth1`，并设置必要参数，例如：

```
[root@VM-web ~]# cd /etc/sysconfig/network-scripts/
[root@VM-web network-scripts]# vim ifcfg-eth1
...
TYPE=Ethernet
BOOTPROTO=dhcp
NAME=eth1
DEVICE=eth1
ONBOOT=yes
...
```

完成后输入命令:wq保存并退出。

3. 执行 `systemctl restart network` 重启网络配置生效，即可识别新添加网卡。

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，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。

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**资源中心 > 云资源池 > 虚拟资源 > 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viosstor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: Cloud基于模版创建云主机，可否实现**母盘+增量盘**的模式？

A: Cloud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：建议使用云盘的文件系统UUID来挂载，而非/dev/vdb类似的盘符来挂载。

10.

Q: 为何云盘的真实容量会大于分配容量？

A: 当云盘是qcow2格式时，云盘的真实容量会累加快照容量。

20.5 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: Cloud的计算节点支持的Qemu和Libvirt版本是?

A: 可在计算节点执行 `virsh version` 命令, 查看Qemu和Libvirt版本。

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: 修改管理节点IP地址、数据库IP地址、消息总线IP地址的详细步骤, 请参考修改管理节点IP地址 [修改管理节点IP地址](#) 章节。

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: 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, 修改后物理机会自动重连。

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: 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, 修改后镜像服务器会自动重连。

8.

Q: 如何手动延长Cloud管理节点启动时间?

A:

- **现象:**

在云主机中运行Cloud，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：如何把Cloud管理节点从一台物理机迁移到另一台物理机？

A：将管理节点迁移到另一台物理机的详细步骤，请参考[切换管理节点](#)章节。

10.

Q：重新安装管理节点，如何恢复原来配置？

A：重新安装管理节点后恢复原来配置的详细步骤，请参考[计算节点升级为管理节点](#)章节。

11.

Q：如何为物理机设置保留内存？

A：

- 方法一：在**设置 > 平台设置 > 全局设置 > 基本设置**页面，修改**物理机保留内存**的值，全局设置物理机保留内存。
- 方法二：在集群详情页的**高级设置**页面，修改**物理机保留内存**的值，以集群为单位设置物理机保留内存。

12.

Q：Cloud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
```

13.

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，Cloud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，云主机自动迁移至其他物理机上。

注:

- 共享存储场景下，物理机进入维护模式，用户可自行设置迁移云主机失败策略；
- 设置方法：

进入**设置 > 平台设置 > 全局设置 > 高级设置**，设置**维护模式下迁移云主机失败策略**：

- 若选择**强制停止云主机**：

物理机进入维护模式，共享存储上的云主机会自动迁移到其它物理机上。未迁移的云主机将会被强制关闭。

- 若选择**非强制停止云主机**：

物理机进入维护模式，共享存储上的云主机会自动迁移到其它物理机上。如果物理机上还存在运行中的云主机，则进入维护模式失败。

• 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，目前运行中的云主机不受影响。

14.

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Cloud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。

15.

Q: 使用Cloud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：

- 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。

16.

Q: SSH连接超时如何解决？

A:

- **现象：**

Cloud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ssh服务器上更改/etc/ssh/sshd_config文件中配置如下：

```
UseDNS no
#GSSAPI options
GSSAPIAuthentication no
```

2. 执行命令/etc/init.d/sshd restart重启sshd服务。

17.

Q: Cloud启动后提示MySQL is not running如何解决？

A:

- **现象：**

使用zstack-ctl start启动Cloud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。

18.

Q: Cloud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Cloud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。

19.

Q: Cloud备份需要备份哪些数据?

A: Cloud本身的备份只需备份数据库即可。

20.

Q: Cloud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
```

21.

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,
    "apild": "75b0774fc7b94007ac1ba274e6ed5eb3",
    "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:fab977f38e024e6e86f048a4090845f8, ip:192.168.10.11]",
          "createTime": "1489036864392",
          "type": {
            "_name": "key.event.API_EVENT",
            "id": "8f1d551677c44788953eae7255eda54b"
          }
        }
      }
    }
  }
}
```

• 原因及解决方案:

该物理机没有enp2s0网卡, 请确认网卡名是否填写正确。

22.

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Cloud后, 添加物理机出现如下报错:

```
ERROR:could not insert 'kvm_intel':Operation not supportednndstdout
```

2. 执行cat /proc/cpuinfo | grep "vmx|svm" 命令, 查看开启虚拟化情况:

- 如果有返回值, 表示开启成功。
- 如果没有返回值, 表示没有开启虚拟化, 需在BIOS中打开虚拟化选项。

23.

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。

24.

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。

25.

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-df21-46d2-9927-7c930333cb70
```

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Cloud在UI已提供关闭CephX密钥认证选项。

26.

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。

27.

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。

28.

Q: 如果一个集群挂载两个主存储, 云盘如何分配?

A:

Cloud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。

29.

Q: Dell服务器安装Cloud, 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。

30.

Q: 管理节点有多个网卡和IP, 如何指定Cloud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), Cloud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Cloud服务监听的IP地址:

```
[root@ceph-host ~]# zstack-ctl configure management.server.ip=${MANAGEMENT_IP} //  
${MANAGEMENT_IP}是用户希望指定的IP地址  
[root@ceph-host ~]# zstack-ctl restart_node //重启管理节点服务
```

31.

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

32.

Q: Cloud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: Cloud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。
- 一个集群只能挂载一个Ceph主存储。

33.

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 ~]# kill -HUP `pgrep collectdmon`
[root@10-0-5-87 ~]# service virtlogd restart
[root@10-0-5-87 ~]# service libvirtd restart
[root@10-0-5-87 ~]# service zstack-kvmagent restart
```

34.

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。

35.

Q: 物理机中可用量和可用物理容量有何差别?

A:

- 可用量: 扣除超分后, 该物理机上的剩余虚拟容量, 计算方式: 可用量 = 总容量 - 云盘 (根云盘 + 数据云盘) / 超分率 - 快照 - 镜像缓存 - 系统已用容量。
- 可用物理容量: 该物理机上各本地存储URL指定分区目录下的可用真实容量总和, 可执行以下命令查看: df /主存储挂载路径URL, 例如: df /zstack_ps。

36.

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: Cloud 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Cloud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。

37.

Q: ImageStore类型镜像服务器容量使用过高, 如何清理空间?

A: 删除无用镜像, 点击**硬件设施 > 镜像服务器 > 镜像服务器操作 > 数据清理**, 完成无效数据的清理。

38.

Q: AMD GPU执行虚拟化切割操作报错怎么解决?

A:

- **现象:** AMD GPU执行虚拟化切割操作, 提示如下报错:

```
failed to remove gim.ko, , modprobe: FATAL: Module gim not found
```

- **解决方案:** 依次执行以下命令即可解决:

```
[root@localhost ~]# wgethttps://github.com/GPUOpen-LibrariesAndSDKs/MxGPU-Virtualization/archive/master.zip #下载依赖包
[root@localhost ~]# unzip master.zip #解压文件
[root@localhost ~]# cd MxGPU-Virtualization-master
[root@localhost MxGPU-Virtualization-master]# make
[root@localhost MxGPU-Virtualization-master]# cp gim.ko /lib/modules/3.10.0-693.11.1.el7.x86_64/
[root@localhost MxGPU-Virtualization-master]# depmod
[root@localhost MxGPU-Virtualization-master]# modprobe gim
```

20.6 网络

1.

Q: Cloud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`kill dnsmasq`, 把所有DHCP server杀死

4.

Q: Cloud只认eth0? 为何不支持em01?

A: Cloud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。

- 如果已添加eth0的二层网络, 但新计算节点的网卡为em01 (非eth0), 会导致添加物理失败。
- 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。

5.

Q: 管理网络和业务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。

6.

Q: 为何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地址被分配给路由器或者DHCP Server使用, 路由器的IP可以直接看到。

- 对于后一个问题，DHCP Server占用的IP，用于分配DHCP服务IP地址且无法释放，DHCP服务IP可在对应三层网络的详情页查看。

7.

Q: Cloud如何修改L3的网络段（IP Range）呢？

A: Cloud仅支持添加、删除网络段操作，若需要修改L3网络段，需先添加新的网络段，再删除旧的网络段。操作完成后，重启云主机即可在新添加的网络段里重新分配IP。



注：删除网络段需要注意以下情况，请谨慎操作：

- 删除网络段会导致使用该网络段的云主机网卡被卸载，请谨慎操作。
- 若三层网络已有DHCP服务IP，且DHCP服务IP在所选网络段内，删除网络段会依然保留DHCP服务IP，若三层网络下全部网络段均删除，DHCP服务IP会被释放。

8.

Q: Cloud如何设置云主机指定IP？

A: 在云主机详情页的**配置信息**页面，选中网卡下的一个网络，点击网卡旁边的**操作 > 设置指定IP**按钮，为云主机设置指定IP。



注：设置指定IP操作需要在云主机关机时执行。

9.

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。

10.

11.

Q: Cloud的DHCP服务由谁提供？

A: 扁平网络、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。

12.

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。

13.

Q: Cloud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: Cloud使用VPC路由器提供负载均衡服务，主要是访问虚拟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。

14.

Q: Cloud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。Cloud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。

15.

Q: VLAN设置完成后不能通信，系统启用iptables后，是否需要增加配置才能让VLAN互相通信？

A: VLAN互相通信需要在交换机上配置。

16.

Q: 如何登录VPC路由器？

A: 登录路由器需输入用户名和密码。在**设置 > 平台设置 > 全局设置 > 基本设置**页界面，可对路由器的登录密码进行设置。

- 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重启路由器，该密码才会生效。
- 该操作对所有路由器生效。

17.

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

18.

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。

19.

Q: 网卡bond设置错了，如何修改？

A: 以bond0为例，依次执行如下命令，删除设置错的bond:

```
[root@host ~]# ip link set br_XXX down //停止创建的网桥
[root@host ~]# brctl delbr br_XXX //删除网桥
```

```
[root@host ~]# rm -f /etc/sysconfig/network-scripts/ifcfg-br_XXX //删除网桥配置文件
[root@host ~]# zs-vlan -d bond0 XX //删除VLAN子接口
[root@host ~]# zs-bond-ab -d bond0 //删除错误的bond
```

然后再参考最开始配置网络添加bond。

20.

Q: Cloud支持IPv6吗?

A: Cloud3.1.0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。

21.

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。

22.

Q: Cloud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

23.

Q: 一个云主机的IP可以绑定多个弹性IP吗?

A: 可以。云主机多出口的场景下, 可以设置多个弹性IP来提供不同场景访问的需求。

24.

Q: 无法使用SR-IOV功能对物理网卡进行切割, 该如何处理?

A:

- 被切割的网卡需要在硬件层面支持切割
- BIOS中打开Intel VT-d和SR-IOV设置
- 修改物理机IOMMU启动状态为启用状态。



注: 更改物理机IOMMU启动状态需重启物理机, 可通过IOMMU就绪状态进行验证。

25.

Q: 服务器网卡使用bond并且配置为LACP模式, 云主机之间的网络波动较大, 如何排查?

A:

1. 确保配置的LACP正常聚合成功, 以及交换机配置正常
2. 确保同一bond网卡型号一致。



注: 可使用 `lspci |grep -i net` 检查。

26.

Q: VPC路由器可以指定公有网络IP为默认IP吗?

A: 创建VPC路由器时, 可以指定公有网络作为VPC路由器的默认IP。

27.

Q: VPC路由器可以绑定多个公有网络吗? 需要注意哪些事项?

A: VPC路由器可以绑定多个公有网络。Cloud 3.9.0之后版本支持公网的源进源出。若绑定多个公有网络, 建议启用源进源出, 确保数据进出一致。

28.

Q: VPC路由器规格有最低限制吗?

A: 生产环境下, VPC路由器规格建议不低于4核4G。

29.

Q: 负载均衡监听器显示后端云主机健康状况异常, 如何排查?

A: 可分别排查云主机运行状态、网络、业务端口、业务运行状态是否正常。

30.

Q: VPC路由器之间如何实现互通?

A: VPC路由器之间可通过静态路由或动态路由 (OSPF) 实现互通

- 生产环境下, 若VPC路由器绑定较多子网, 或与物理环境互通, 物理核心交换机子网很多, 推荐使用动态路由实现网络互通。
- 若VPC路由器绑定的子网不多, 或对网络转发性能要求高, 推荐使用静态路由。

31.

Q: VPC路由器下云主机如何可访问互联网?

A:

- VPC路由器绑定可访问互联网的公有网络, 默认该路由器下云主机可访问互联网。
- 为云主机绑定弹性公网IP, 该云主机可访问互联网。



注: 若VPC路由器公有网络是真实公网地址段, 绑定弹性IP的云主机可以同时被互联网访问。

32.

Q: VPC如何实现和物理网络实现三层互通?

A: VPC和物理网络之间可通过静态路由实现三层互通。

33.

Q: 如何查看VPC路由器相关日志?

A: 可使用sudo权限到zvr路径下查看zvr.log。

34.

Q: 如何排查VPC路由器创建超时?

A:

- 检查路由器规格关联的管理网络和管理节点能否双向互通, 若网络不通, VPC路由器会创建超时。
- 检查上传的VPC路由器镜像版本是否和当前云平台版本一致。
- 检查管理节点负载是否太高, 处理消息出现卡队列的情况。

35.

Q: 如何排查VPC下云主机到网关不通?

A:

- 检查云主机操作系统内部的IP地址、掩码和网关配置是否正确, 网卡状态是否UP, 网络服务是否正常。
- 将云主机迁移到和VPC路由器相同的宿主机上测试, 若网络能通, 说明源宿主主机上联交换机的VLAN信息配置有误。
- 检查VPC路由器运行状态是否正常。

36.

Q: 如何排查VPC下云主机弹性IP不通?

A:

1. 用公有网络创建云主机, 测试能否访问公有网络云主机IP地址。若无法访问, 需要检查公有网络地址段、掩码、网关配置、以及公有网络上联交换机配置等。
2. 若可直接访问公有网络, 需要检查VPC下云主机操作系统内部的IP地址、掩码和网关配置是否正确, 网卡状态是否UP, 以及网络服务是否正常。
3. 若VPC下云主机系统内部正常, 需要检查网卡的bond绑定关系、vnic、物理机网络服务等是否正常。
4. 若以上三步仍未解决, 可解绑弹性IP, 再重新绑定进行测试。

20.7 裸金属管理

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。

20.8 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Cloud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Cloud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Cloud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,
  "apild": "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Cloud来接管vCenter, vCenter必须能先创建dvSwitch; Cloud创建路由器网络也基于dvSwitch。

5.

Q: vCenter云主机无法打开控制台, 如何解决?

A: Cloud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Cloud重启vCenter云主机
- 通过Cloud进行动态迁移vCenter云主机 (基于共享存储)

6.

Q: Cloud接管vCenter后, 对原有的vCenter有影响么?

A: Cloud仅接管vcenter资源, 提供一个管理入口, 并不影响其原有资源。

20.9 平台管理运维

1.

Q: Cloud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: Cloud能和AD/LDAP连接吗? 只能用API接口控制用户吗?

A:

- Cloud可以通过以下两种方式和AD/LDAP连接:
 - 云平台账户连接方式可参考《AD/LDAP 配置教程》;
 - 企业管理用户连接方式可参考《企业管理使用教程》。
- Cloud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**和**第三方认证**章节。

3.

Q: 如何设置管理节点 prometheus数据保留时间?

A: 在**全局设置 > 高级设置**页面, 修改**监控数据保留周期**和**监控数据保留大小**的值, 用于设置管理节点 prometheus数据保留时间。

4.

Q: 云平台UI首页中的监控数据不能正常显示如何解决?

A: 可以尝试重启 prometheus服务来获取监控数据, 重启 prometheus服务具体方法如下:

- 3.1.0 版本之前, 在管理节点kill prometheus进程, 等待管理节点重新自动拉起(大约30s)监控服务。
- 3.1.0 及其以后版本, 在管理节点执行systemctl restart prometheus命令重启监控服务。

5.

Q: 全局设置中CPU超分的计算方法是怎样的?

A: CPU超分用于控制分配给云主机的虚拟CPU数量。计算公式: 物理CPU总线程 * CPU超分率 = 可分配的虚拟CPU数量。

- 假设使用12核24线程的物理CPU, 若云平台全局设置中CPU超分率设置为10, 那么可分配给云主机使用的vCPU的数量为240核。

- CPU超分率数值过大可能会严重影响物理机性能，导致业务性能卡顿。

6.

Q：全局设置中内存超分的计算方法是怎样的？

A：用于控制分配给云主机的虚拟内存容量。计算公式：物理内存容量 * 内存超分率 = 可分配的虚拟内存容量。

- 假设物理内存128G，若云平台全局设置中内存超分率设置为2，那么可分配给云主机使用的内存为256G。
- 内存超分率数值过大可能会严重影响物理机内存性能，导致系统OOM（内存溢出）。不建议内存超分，若确实需要，请勿超过1.2。

7.

Q：全局设置中主存储超分的计算方法是怎样的？

A：用于控制分配给云主机的虚拟主存储可用空间。计算公式：物理主存储可用空间 * 主存储超分率 = 可分配的虚拟主存储可用空间。

- 假设主存储物理容量2T，若云平台全局设置中主存储超分率为2，超分后主存储容量不变，但创建的云盘、快照等占用主存储的容量是实际申请容量的一半。比如创建100G的云盘（raw格式）实际主存储上扣除的容量为50G。
- 主存储超分率数值过大可能会严重影响存储压力或导致磁盘容量快速占满，导致系统IO错误。不建议主存储超分，若确实需要，请勿超过1.2。

8.

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。

9.

Q：云平台UI登录密码忘记后如何重置？

A：在管理节点执行`zstack-ctl reset_password --password NEW_PASSWORD`，`NEW_PASSWORD`替换为新密码。

10.

Q：如何在计算节点上修改管理IP地址？

A：

1. 计算节点进入维护模式；



注：确保云主机已迁移至其他物理机或处于已关机状态。

2. 通过接入显示器或者使用IPMI登录至计算节点系统；

3. 修改管理网卡配置文件中的静态IP地址；
4. 重启网络服务；
5. 登录云平台，点击**硬件设施 > 物理机**，在**物理机详情**页面修改物理机IP地址为新IP地址，点击**启用**；
6. 等待物理机重连完毕。