



UCloudStack 用户手册

产品版本：V1.16.0

文档版本：202007

1 产品简介

- 1.1 产品概述
- 1.2 核心优势
- 1.3 产品架构

2 主账号

- 2.1 主账号注册登录
- 2.2 OAuth 登录认证
- 2.3 找回密码

3 虚拟机

- 3.1 概述
- 3.2 创建虚拟机
 - 3.2.1 前提条件
 - 3.2.2 创建操作
- 3.3 查看虚拟机
 - 3.3.1 虚拟机列表
 - 3.3.2 虚拟机详情信息
 - 3.3.2.1 虚拟机概览
 - 3.3.2.2 虚拟机硬盘
 - 3.3.2.3 虚拟机网络
 - 3.3.2.4 外网 IP 管理
 - 3.3.2.4.1 绑定外网 IP
 - 3.3.2.4.2 解绑外网 IP
 - 3.3.2.4.3 设为默认出口
 - 3.3.2.5 弹性网卡管理
 - 3.3.2.6 虚拟机操作日志
- 3.4 VNC 登录
- 3.5 启动/关机/断电/重启
- 3.6 制作镜像
- 3.7 重装系统
- 3.8 重置密码
- 3.9 修改配置
- 3.10 热升级
- 3.11 修改告警模板
- 3.12 绑定外网 IP
- 3.13 修改安全组
 - 3.13.1 修改外网安全组
 - 3.13.2 修改内网安全组
- 3.14 修改名称和备注
- 3.15 删除虚拟机
- 3.16 远程登录
 - 3.16.1 远程登录 Linux
 - 3.16.2 远程登录 Windows
- 3.17 系统盘扩容
 - 3.17.1 Linux 系统盘分区扩容
 - 3.17.2 Windows 系统盘分区扩容

4 自制镜像管理

- 4.1 查看自制镜像
- 4.2 从镜像创建虚拟机
- 4.3 导入镜像

- 4.4 下载镜像
- 4.5 删除自制镜像
- 4.6 修改名称和备注

5 弹性网卡

- 5.1 创建弹性网卡
- 5.2 查看网卡
- 5.3 绑定网卡
- 5.4 解绑网卡
- 5.5 修改安全组
- 5.6 删除网卡
- 5.7 修改名称和备注

6 云硬盘

- 6.1 云硬盘概述
- 6.2 创建云硬盘
- 6.3 查看云硬盘
- 6.4 绑定云硬盘
- 6.5 解绑云硬盘
- 6.6 格式化并挂载数据盘
 - 6.6.1 Linux 虚拟机
 - 6.6.2 windows 虚拟机
- 6.7 扩容云硬盘
 - 6.7.1 扩容云盘容量
 - 6.7.2 磁盘分区扩容
 - 6.7.2.1 裸磁盘扩容 (Linux)
 - 6.7.2.2 单分区扩容 (Linux)
 - 6.7.2.3 单分区扩容 (Windows)
 - 6.7.2.4 多分区扩容 (Linux)
 - 6.7.2.5 多分区扩容 (Windows)
 - 6.7.2.6 2TB 磁盘分区扩容 (Linux)
 - 6.7.2.7 2TB 磁盘分区扩容 (Windows)
- 6.8 硬盘克隆
- 6.9 删除云硬盘
- 6.10 修改名称和备注
- 6.11 快照管理
 - 6.11.1 快照概述
 - 6.11.2 创建快照
 - 6.11.3 查看快照信息
 - 6.11.4 回滚快照
 - 6.11.5 删除快照
 - 6.11.6 修改快照名称

7 私有网络

- 7.1 VPC 简介
 - 7.1.1 概述
 - 7.1.2 VPC 逻辑结构
 - 7.1.3 VPC 连接
 - 7.1.4 功能与特性
- 7.2 创建 VPC
- 7.3 查看私有网络
 - 7.3.1 私有网络列表

7.3.2 私有网络详情

7.4 修改名称和备注

7.5 删除私有网络

7.6 添加子网

7.7 删除子网

7.8 修改子网名称

8 外网弹性 IP

8.1 EIP 简介

8.1.1 概述

8.2.2 物理架构

8.2.3 逻辑架构

8.2.4 功能特性

8.2 申请外网 IP

8.3 查看外网 IP

8.3.1 外网 IP 列表

8.3.2 外网 IP 详情

8.4 绑定外网 IP

8.5 解绑外网 IP

8.6 调整带宽

8.7 修改告警模板

8.8 修改外网 IP 名称

8.9 删除外网 IP

9 安全组

9.1 安全组简介

9.1.1 概述

9.1.2 安全组规则

9.2 安全组管理

9.2.1 创建安全组

9.2.2 查看安全组

9.2.2.1 安全组列表

9.2.2.2 安全组详情

9.2.2.3 已绑定资源

9.2.3 修改安全组名称

9.2.4 删除安全组

9.3 安全组规则管理

9.3.1 新建规则

9.3.2 查看规则

9.3.3 编辑规则

9.3.4 删除规则

10 负载均衡

10.1 负载均衡简介

10.1.1 概述

10.1.2 应用场景

10.1.3 架构原理

10.1.4 功能特性

10.1.5 负载均衡隔离性

10.2 负载均衡管理

10.2.1 使用流程

10.2.2 创建负载均衡

- 10.2.3 查看负载均衡
 - 10.2.3.1 负载均衡列表
 - 10.2.3.2 负载均衡详情
- 10.2.4 修改告警模板
- 10.2.5 修改安全组
- 10.2.6 修改名称和备注
- 10.2.7 删除负载均衡
- 10.3 VServer 管理
 - 10.3.1 添加 VServer
 - 10.3.1.1 添加 TCP 监听器
 - 10.3.1.2 添加 UDP 监听器
 - 10.3.1.3 添加 HTTP 监听器
 - 10.3.1.4 添加 HTTPS 监听器
 - 10.3.2 查看 VServer
 - 10.3.2.1 VServer 列表
 - 10.3.2.2 VServer 详情
 - 10.3.3 修改 VServer
 - 10.3.4 修改告警模板
 - 10.3.5 删除 VServer
- 10.4 服务节点管理
 - 10.4.1 添加服务节点
 - 10.4.2 查看服务节点
 - 10.4.3 启用/禁用
 - 10.4.4 修改服务节点
 - 10.4.5 删除服务节点
- 10.5 内容转发规则管理
 - 10.5.1 添加内容转发规则
 - 10.5.2 查看内容转发规则
 - 10.5.3 修改内容转发规则
 - 10.5.4 删除内容转发规则
- 10.6 SSL 证书管理
 - 10.6.1 证书格式要求
 - 10.6.1.1 Root CA 机构颁发的证书
 - 10.6.1.2 中级机构颁发的证书
 - 10.6.1.3 RSA 私钥
 - 10.6.1.4 客户端证书
 - 10.6.2 创建 SSL 证书
 - 10.6.2.1 创建服务器证书
 - 10.6.2.2 创建客户端证书
 - 10.6.3 查看 SSL 证书
 - 10.6.3.1 SSL 证书列表
 - 10.6.3.2 SSL 证书详情
 - 10.6.4 删除 SSL 证书

11 NAT 网关

- 11.1 NAT 网关简介
 - 11.1.1 概述
 - 11.1.2 应用场景
 - 11.1.3 架构原理
 - 11.1.4 功能特性

- 11.2 使用流程
 - 11.3 创建 NAT 网关
 - 11.4 查看 NAT 网关
 - 11.4.1 NAT 网关列表
 - 11.4.2 NAT 网关详情
 - 11.5 修改告警模板
 - 11.6 删除 NAT 网关
 - 11.7 修改名称和备注
 - 11.8 修改安全组
 - 11.9 白名单管理
 - 11.9.1 添加白名单
 - 11.9.2 查看白名单
 - 11.9.3 移除白名单
- ## 12 IPSecVPN 服务
- 12.1 产品简介
 - 12.1.1 背景
 - 12.1.2 概述
 - 12.1.3 逻辑架构
 - 12.1.4 VPN 隧道建立
 - 12.1.5 VPN 隧道参数
 - 12.1.6 应用场景
 - 12.2 使用流程
 - 12.3 VPN 网关
 - 12.3.1 创建 VPN 网关
 - 12.3.2 查看 VPN 网关
 - 12.3.2.1 VPN 网关列表
 - 12.3.2.2 VPN 网关详情
 - 12.3.3 修改名称和备注
 - 12.3.4 修改告警模板
 - 12.3.5 删 除 VPN 网关
 - 12.4 对端网关
 - 12.4.1 创建对端网关
 - 12.4.2 查看对端网关
 - 12.4.3 修改名称和备注
 - 12.4.4 删 除 对端网关
 - 12.5 VPN 隧道
 - 12.5.1 VPN 隧道配置流程
 - 12.5.2 创建 VPN 隧道
 - 12.5.2 查看 VPN 隧道
 - 12.5.2.1 VPN 隧道列表
 - 12.5.2.2 VPN 隧道详情
 - 12.5.3 下载 VPN 隧道配置
 - 12.5.4 修改隧道网段策略
 - 12.5.5 修改 IKE 策略配置
 - 12.5.6 修改 IPSec 策略配置
 - 12.5.7 修改名称和备注
 - 12.5.8 修改告警模板
 - 12.5.9 删 除 VPN 隧道
 - 12.6 VPN 管理员指南

12.6.1 UCloud 公有云 IPSecVPN

12.6.1.1 前提条件

12.6.1.2 配置公有云网关

12.6.1.3 配置验证

12.6.2 Cisco 防火墙配置

12.6.2.1 前提条件

12.6.2.2 配置防火墙

12.6.2.3 配置验证

12.6.3 StrongSwan 配置

12.6.3.1 前提条件

12.6.3.2 配置 StrongSwan

12.6.3.3 配置验证

12.6.4 VPC 到 VPC 的 VPN 连接

12.6.4.1 前提条件

12.6.4.2 配置 VPN 网关和隧道

12.6.4.3 配置连接验证

12.7 常见问题

13 弹性伸缩

13.1 产品简介

13.1.1 概述

13.1.2 逻辑架构

13.1.3 伸缩组工作流程

13.1.4 伸缩器工作流程

13.1.5 功能特性

14 MySQL 服务

15 Redis 服务

16 定时器

16.1 产品简介

16.1.1 概述

16.1.2 功能特性

17 监控告警

17.1 监控图表

17.2 告警模板

17.2.1 创建告警模板

17.2.2 查看告警模板

17.2.2.1 告警模板列表

17.2.2.2 告警模板详情

17.2.3 查看资源

17.2.4 删除告警模板

17.2.5 告警规则管理

17.2.5.1 创建规则

17.2.5.2 查看规则

17.2.5.3 更新规则

17.2.5.4 删除规则

17.2.6 查看绑定资源

17.3 通知组管理

17.3.1 创建通知组

17.3.2 查看通知组

17.3.2.1 通知组列表

17.3.2.2 通知组详情

17.3.3 更新通知组

17.3.4 删除通知组

17.3.5 通知人管理

17.3.5.1 添加通知人

17.3.5.2 更新通知人信息

17.3.5.3 删除通知人

17.4 告警记录

18 操作日志

18.1 资源操作日志

18.2 全局操作日志

19 回收站

19.1 回收站概述

19.2 查看回收站资源

19.3 恢复资源

19.4 续费资源

19.5 销毁资源

20 账号管理

20.1 账号信息

20.2 账户安全

20.2.1 修改登录密码

20.2.2 开通登录保护

20.2.2.1 开通步骤

20.2.2.2 关闭登录保护

20.2.2.3 功能应用

20.2.2.4 登录保护 FAQ

20.2.3 API 密钥

20.3 子账号管理

20.3.1 添加账户

20.3.2 查看账户

20.3.2.1 子账号列表

20.3.2.2 子账号详情

20.3.3 冻结账户

20.3.4 解冻账户

20.3.5 权限管理

20.4 查看配额

21 计费管理

21.1 资源计价器

21.2 订单管理

21.3 交易管理

版权声明

版权所有 © 优刻得科技股份有限公司 2020 保留一切权利。

未经本公司书面许可，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。

UCloudStack 商标和 UCloud 商标为优刻得科技股份有限公司所有。对于本手册中可能出现的其它公司的商标及产品标识，由各自权利人拥有。

注意您购买的产品、服务或特性等应受优刻得科技股份有限公司商业合同和条款约束，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权利范围之内。除非合同另有约定，优刻得科技股份有限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它原因，本文档内容会不定期更新，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。

本文档描述 UCloudStack (v1.16.0) 云平台的功能说明和操作指南，适用于需深入了解平台并使用控制台管理资源的租户，开发者可参考 UCloudStack API 开发者文档。

1 产品简介

1.1 产品概述

UCloudStack 企业私有云平台，提供虚拟化、SDN 网络、分布式存储、数据库缓存等核心服务的统一管理、资源调度、监控日志及运营运维等一整套云资源管理能力，助力企业数字化转型。



虚拟化



SDN



分布式存储



数据库服务



缓存服务



云管平台



平台基于 UCloud 公有云基础架构，复用内核及核心虚拟化组件，将公有云架构私有化部署，具有自主可控、稳定可靠、持续进化及开放兼容等特点，企业可通过控制台或 APIs 快速构建资源及业务，支持与公有云无缝打通，灵活调用公有云能力，帮助企业快速构建安全可靠的业务架构。

UCloudStack 定位为轻量级交付，3 节点即可构建生产环境且可平滑扩容，不强行绑定硬件及品牌，兼容 X86 和 ARM 架构，并提供统一资源调度和管理，支持纯软件、超融合一体机及一体机柜多种交付模式，有效降低用户管理维护成本，为用户提供一套安全可靠且自主可控的云服务平台。

1.2 核心优势

- 自主可控——基于公有云架构，复用核心虚拟化组件自主研发，可控性高且可靠性经上万家企业验证。
- 稳定可靠——平台服务高可用，虚拟资源智能调度，数据存储多副本，自愈型分布式网络，为业务保驾护航。
- 简单易用——3 节点构建生产环境，规模轻量可水平扩展，支持业务平滑迁移，助力企业轻松上云。
- 开放兼容——不绑定硬件品牌，兼容 X86 和 ARM 架构及生态适配，设备异构搭建统一管理。

1.3 产品架构



UCloudStack 平台整体产品架构由基础硬件设施、虚拟核心引擎、智能调度系统、核心产品资源、统一云管平台及运维管理平台组成，为平台租户、管理员及运营人员提供云平台管理和服务。

- **基础设施：**用于承载 UCloudStack 平台的服务器、交换机及存储设备等。
 - 平台支持并兼容通用 X86、ARM 及 MIPS 架构硬件服务器，不限制服务器和硬件品牌；
 - 支持 SSD、SATA、SAS 等磁盘存储，同时支持计算存储超融合节点及对接磁盘阵列设备，无厂商锁定；
 - 支持华为、思科、H3C 等通用交换机、路由器网络设备接入，所有网络功能均通过 SDN 软件定义，仅需物理交换机支持 Vlan、Trunk、IPv6、端口聚合、堆叠等特性；
 - 支持混合云接入并适配客户现有硬件资源，充分利用资源的同时，无缝对接现有资源服务。
- **虚拟核心引擎：**承载平台核心的操作系统内核、虚拟化计算、存储、网络的实现和逻辑。
 - 内核模块：承载云平台运行的服务器操作系统及内核模块，复用公有云深度优化的 Linux 内核；同时兼容 ARM 生态的 UOS、银河麒麟等操作服务器操作系统及内核；
 - 虚拟化计算：通过 KVM、Libvirt 及 Qemu 实现计算虚拟化，支持标准虚拟化架构，提供虚拟机全生命周期管理，兼容 X86 和 ARM 架构体系，支持热升级、重装系统、CPU 超分、GPU 透传、在线迁移、宕机迁移、反亲和部署等特性，并支持导入导出虚拟机镜像满足业务迁移上云需求；
 - 分布式网络 SDN：通过 OVS + VXLAN 实现虚拟网络，纯软件定义分布式网络，提升网络转发性能的同时对传统数据中心物理网络进行虚拟化，为云平台资源提供 VPC 隔离网络环境、

- 弹性网卡、外网IP、NAT网关、负载均衡、防火墙、VPN连接、混合云接入及网络拓扑等网络功能，并支持 IPv4&IPv6 双栈；
 - 分布式存储 SDS：基于 Ceph 实现分布式高性能存储，为平台提供块存储服务，支持云盘在线扩容、克隆、快照及回滚功能；同时底层数据多副本存储并支持数据重均衡和故障重建能力，保证性能和数据安全性。
- 智能调度系统**
 - 支持反亲和性调度部署策略，保证业务的高可用性和高可靠性；
 - 支持在线迁移技术，实时感知物理机状态和负载信息；
 - 物理主机故障或超过负载时，自动迁移虚拟机至低负载物理主机；
 - 创建虚拟机时，根据业务调度策略，自动启动虚拟机至低负载健康的物理主机；
 - 支持计算额度分配和资源抢占，保障公平的前提下，有效共享物理资源；
 - 支持平台虚拟资源的网络流表控制及下发，保证分布式网络架构的性能及可用性。
 - 核心产品资源**
 - 地域（数据中心）**：数据中心指资源部署的物理位置分类，数据中心之间相互独立，如无锡数据中心、上海数据中心等。平台支持多数据中心管理，使用一套管理平台管理遍布各地数据中心的私有云平台；
 - 集群**：用于区分不同资源在一个数据中心下的分布情况，如 x86 计算集群、ARM 计算集群、SSD 存储集群 及 SATA 存储集群，一个数据中心可以部署多个集群；
 - 多租户**：平台支持多租户模式，提供租户隔离功能、子账号、权限控制、配额配置及价格配置等功能；
 - 子账号及权限**：支持一个租户拥有多个子账号，支持资源隔离并可对子账号进行资源管理的权限控制；
 - 计量计费**：支持按需、按月、按年三种计费方式，支持过期续费及回收策略，同时提供完整的计费订单及消费明细；
 - 弹性计算**：运行在物理主机上的虚拟机，支持从镜像创建、重启/关机/启动、删除、VNC 登陆、重装系统、重置密码、热升级、绑定外网 IP 及安全组、挂载数据盘及反亲和策略部署等虚拟机全生命周期功能，同时支持将虚拟机制作为镜像及磁盘快照能力，提供快捷的业务部署及备份能力；
 - GPU 虚拟机**：平台提供 GPU 设备透传能力，支持用户在平台上创建并运行 GPU 虚拟机，让虚拟机拥有高性能计算和图形处理能力；
 - 弹性伸缩**：支持弹性伸缩功能，用户可通过定义弹性伸缩策略，在业务需求增长时自动增加计算资源（虚拟机）以保证计算能力；在业务需求下降时自动减少计算资源以节省成本。基于负载均衡和健康检查机制，可同时适用于请求量波动和业务量稳定的业务场景；
 - 镜像**：虚拟机运行时所需的操作系统，提供 CentOS、Windows、Ubuntu 等常用基础操作系统镜像；支持将虚拟机导出为镜像，通过自制镜像重建虚拟机；同时支持镜像的导入导出，便于用户自定义镜像；
 - 云硬盘**：一种基于分布式存储系统为虚拟机提供持久化存储空间的块设备。具有独立的生命周期，支持随意绑定/解绑至多个虚拟机使用，基于网络分布式访问，并支持容量扩容、克隆、快照等特性，为虚拟资源提供高安全、高可靠、高性能及可扩展的磁盘；
 - 快照**：提供磁盘快照及快照回滚能力，可应用于容灾备份及版本回退等业务场景，降低因误操作、版本升级等导致的数据丢失风险；
 - VPC 网络**：软件定义虚拟专有网络，用于租户间数据隔离，提供自定义 VPC 网络、子网规划及网络拓扑；
 - 外网 IP**：用于虚拟机、负载均衡、NAT 网关及 VPN 网关等资源的外网 IP 接入，用于与平台外网络进行连接，如虚拟机访问互联网或访问 IDC 数据中心的物理机网络；支持同时绑定多个外网 IP 至虚拟资源，并提供 IPv6 网络连接服务；

- **安全组**: 虚拟防火墙，提供出入双方向流量访问控制规则，定义哪些网络或协议能访问资源，用于限制虚拟资源的网络访问流量，支持 TCP、UDP、ICMP 及多种应用协议，为云平台提供必要的安全保障；
- **弹性网卡**: 一种可随时附加到虚拟机的弹性网络接口，支持绑定和解绑，可在多个虚拟机间灵活迁移，为虚拟机提供高可用集群搭建能力，同时可实现精细化网络管理及廉价故障转移方案；
- **NAT 网关**: 企业级 VPC 网关，为云平台资源提供 SNAT 和 DNAT 代理，支持自动和白名单两种网络出口模式，并为 VPC 网络提供端口映射代理服务，使外部网络通过 NAT 网关访问虚拟机和 MySQL。
- **负载均衡**: 基于 TCP/UDP/HTTP/HTTPS 协议将网络访问流量在多台虚拟机间自动分配的控制服务，类似于传统物理网络的硬件负载均衡器。用于多台虚拟机间实现流量负载及高可用，提供内外网 4 层和 7 层监听及健康检查服务；
- **IPSecVPN**: 提供 IPSecVPN 网关服务，通过 IPSec 协议加密的隧道技术，将 UCloudStack 与 UCloud 公有云、IDC 数据中心、第三方公有云的内网打通，在互联网上为两个私有网络提供安全通道，通过加密保证连接的安全；同时 IPSecVPN 服务还可作为 UCloudStack 平台 VPC 间通信的桥梁；
- **数据库服务**: 企业级 MySQL 数据库服务，提供双主热备高可用集群方案，支持对数据库集群的快速部署、容灾、监控、备份恢复、归档、账号权限、扩容及迁移等功能；
- **缓存服务**: 企业级 Redis 缓存服务，提供多主多从高可用集群架构，支持主从热备、容灾切换、备份恢复、故障迁移、扩容、数据归档、账号权限、数据持久化及监控告警等全套缓存解决；
- **监控告警**: 支持虚拟机、弹性伸缩、磁盘、弹性 IP、NAT 网关、负载均衡、IPSecVPN、MySQL、Redis 等资源各维度监控数据收集及展示，同时可通过告警模板快速配置资源监控指标的告警策略和通知规则；
- **操作日志**: 云平台所有资源及云平台自身的操作和审计日志，支持多时间跨度的日志收集和展示，提供操作失败原因；
- **回收站**: 资源删除后暂存的位置，支持回收资源、恢复资源及彻底删除资源等操作；
- **定时器**: 提供定时器任务执行功能，可用来定期执行一系列任务，支持定时创建快照，可在指定的周期重复执行，也可仅执行一次，且每个任务支持多个资源批量操作。

- **统一云管平台**

- UCloudStack 平台提供 Web 控制台和 API 接口两种方式接入和管理云平台；
 - 通过 WEB 控制台用户可快捷的使用并管理云平台资源，如虚拟机、弹性 IP、负载均衡、计费等；
 - 开发者可通过 APIs 自定义构建云平台资源，支持无缝迁移上云。
- **运维管理平台**: 为云平台管理员提供的运维运营管理平台，包括租户管理、资源管理、账务管理、监控告警、日志审计、系统管理及部署升级等功能模块。
 - **租户管理**: 用于管理整个云平台的租户及账号信息，提供创建/冻结租户及充值功能，支持查看租户拥有资源信息、订单记录、交易记录及配额价格等信息，同时支持修改租户的资源配置及产品价格；
 - **资源管理**: 支持查看并管理平台所有物理资源和虚拟资源：
 - 物理资源包括物理数据中心、集群、宿主机资源、存储资源、网络 IP 网段资源池及镜像资源池等；
 - 虚拟资源包括所有租户及子账号所拥有的资源，包括虚拟机、VPC、负载均衡、外网 IP、弹性网卡、弹性伸缩、NAT 网关、MySQL、Redis、IPSecVPN、监控告警、安全组、回收站等；

- **账务管理**: 支持查看平台所有订单记录、交易记录、充值记录及全局产品价格，支持配置平台整体产品价格，同时支持财务报表导出；
 - **平台监控告警**: 提供 UCloudStack 自身物理设备、组件及所有虚拟资源的监控数据，并支持自定义监控报警和通知；
 - **日志事件**: 提供平台所有租户、子账号及管理员的操作日志和审计信息，可进行多维度的筛选和搜索；
 - **系统管理**: 提供云平台全局配置、规格配置和配额管理功能。
 - 全局配置包含邮箱设置、回收策略、网络设置、计费、资源管理、配额设置、登录态、控制台及网站设置等；
 - 规格配置支持对虚拟机的 CPU 内存规格、磁盘容量范围、外网 IP 带宽及 MySQL/Redis 内存规格进行自定义配置；
 - 全局配额支持查看并修改全局每个地域虚拟资源的配额值。
 - **部署升级**: 平台支持自动化脚本安装物理服务器节点，包括操作系统、云平台组件及管理服务等。
- **基础监控服务**: 云平台基础硬件资源的外围监控服务，包括云平台接入的所有网络设备、服务器、磁盘阵列等硬件设备的运行状态和性能指标进行监控告警，同时也可对集群中 MySQL、Redis、MongoDB 等常用服务进行监控和告警。

2 主账号

2.1 主账号注册登录

UCloudStack 云平台支持多租户模式，租户即为主账号，平台管理员可通过管理员控制台自主创建主账号并为主账号充值，同时平台提供自助注册流程，用户可通过注册链接，自动化的进行注册并使用云平台。可通过平台注册链接进入账号页面，进行简单的账号注册。



1. 如上图注册界面所示，注册需要的信息如下：

- 登录邮箱：用于登录云平台的邮箱账号，邮箱账号需要支持接收验证邮件；
 - 登录密码：密码须包含有大小写字母、数字、符号中的两种，密码长度为6-20个字符；
2. 提交注册后，平台会给邮箱账号发送激活邮件，您可以登录邮箱完成激活操作；
3. 点击邮箱中“**UCloudStack 激活账户**”邮件的链接后，完成注册，如下图所示。

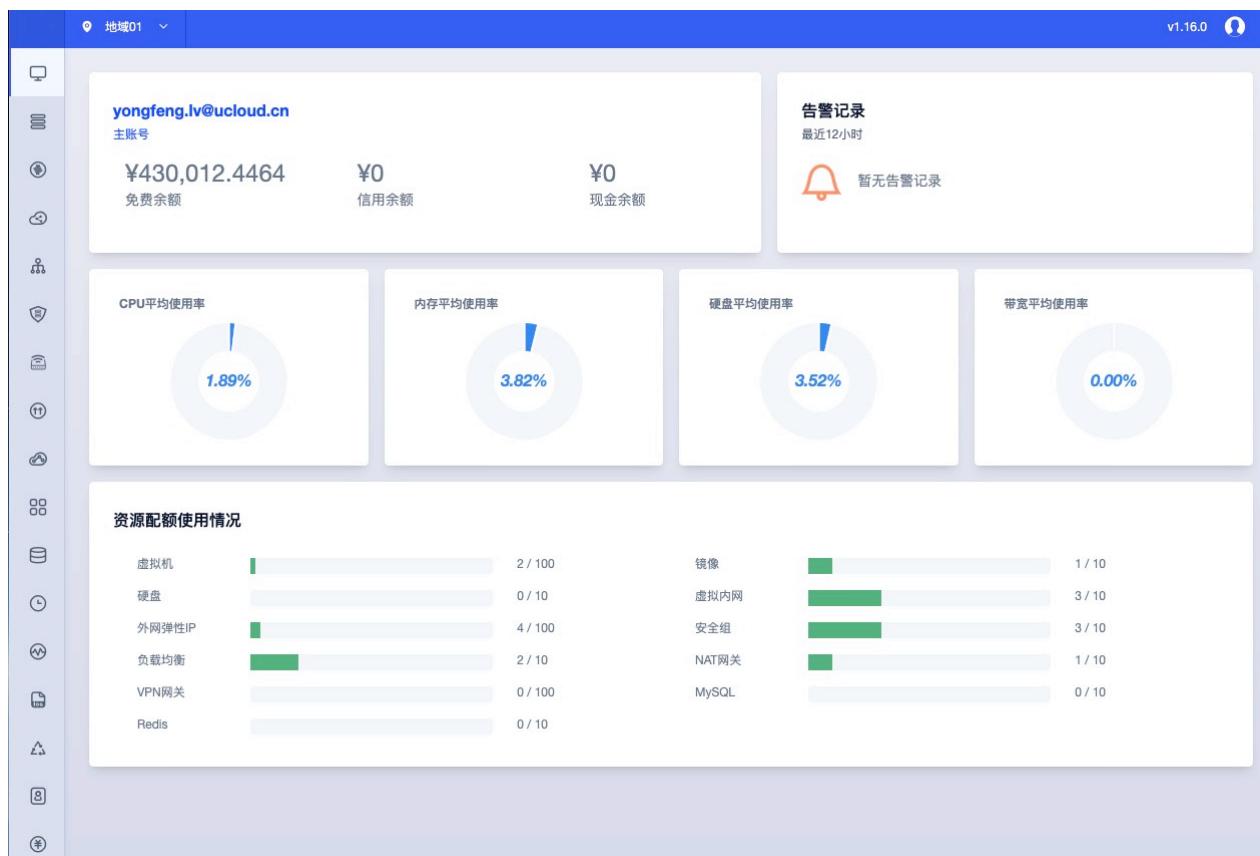


4. 通过注册的邮件和密码登录 UCloudStack 云平台，本文使用 [**UCloudStack 在线 POC 环境**] 作为示例。



云平台资源支持计量计费，在使用前需要联系平台管理员对账号进行充值，才可正常创建并使用资源。

5. 登录成功后，会为用户展示 UCloudStack 云平台的概览页面，如下图所示：



云平台用户登录控制台会默认进入概览页面，概览是当前登录账号的账户信息和资源的综合统计信息，包括登录账号信息、账户余额、免费余额、最近 12 小时的告警记录信息、资源利用率统计信息及账号配额使用状况信息等，并可对平台进行登出操作：

- 登录账号信息展示当前登录平台的账户属性及邮箱地址，若使用子账号登录平台，则展示为子账号及邮箱。
- 最近 12 小时告警记录信息展示当前账号拥有资源最近 12 小时的告警记录，方便快速查看资源健康状况。
- 资源利用率统计信息：当前账号 CPU、内存、磁盘、宽带的平均使用率，如上图 CPU 平均使用率约为 2%。
- 配额使用状况信息：当前账号各种资源的配额及占用信息，包括虚拟机、镜像、硬盘、网卡、VPC、外网IP、安全组、NAT 网关、负载均衡、VPN网关、Redis 及 MySQL 等资源配额，资源配额值可通过管理员控制台进行配置，并可通过账号信息查看当前租户的资源配额。

通过点击概览页面账户名可进入账户详情信息页面，查看当前账户的详细信息、子账号及配额相关信息。点击告警记录的可进入告警历史记录页面，查看更多告警记录。

2.2 OAuth 登录认证

平台支持第三方 OAuth 2.0 登录认证，用户可通过将企业内 OAuth 统一认证登录系统与云平台进行对接，使用企业统一登录用户即可登录并使用云平台的资源。

如 2.1 章节登录示例图所示，平台已于 OAuth 2.0 系统进行对接，并在登录页面提供第三方登录入口。企业用户可通过自有的 OAuth 统一认证平台登录跳转至云平台，同时也可通过云平台第三方登录入口通过统一用户密码认证登录云平台，如下图所示：



用户在第三方登录平台使用用户名和密码登录平台后，即可跳转至云平台概览页面，使用统一的用户认证方式管理云平台资源。

2.3 找回密码

平台支持主账号在忘记密码时通过控制台自主找回密码，找回密码时需通过邮箱进行验证，请确保管理员添加的账号为真实可用的邮箱。通过登录页面的【找回密码】功能，即可使用邮箱地址验证重新为主账号设置新密码，如下图所示：

重置密码

The screenshot shows a user interface for resetting a password. It consists of three main sections:

- A top section with a lock icon and the placeholder text "请输入密码" (Please enter password). To the right is a small eye icon for password visibility.
- A middle section with a lock icon and the placeholder text "请再次输入密码" (Please re-enter password). To the right is a small eye icon for password visibility.
- A large blue rectangular button in the center containing the text "重置密码" (Reset Password).

重置密码成功后，即可使用最新设置的密码登录云平台，进行云平台资源的使用和管理。

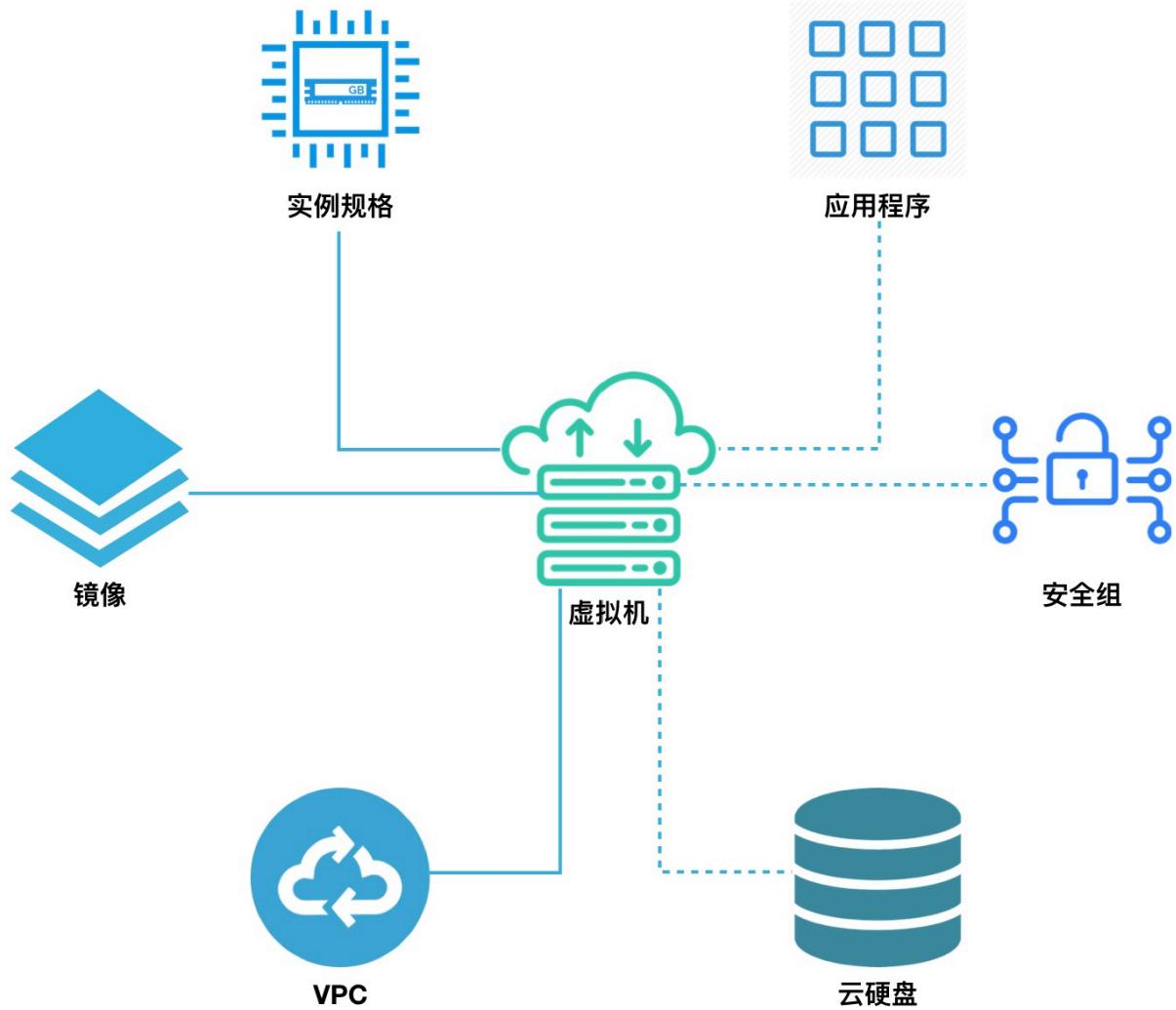
3 虚拟机

3.1 概述

虚拟机是 UCloudStack 云平台的核心服务，提供可随时扩展的计算能力服务，包括 CPU、内存、操作系统等最基础的计算组件，并与网络、磁盘、安全等服务结合提供完整的计算环境。通过与负载均衡、数据库、缓存、对象存储等服务结合共同构建 IT 架构。

- UCloudStack 云平台通过 KVM (Kernel-based Virtual Machine) 将物理服务器计算资源虚拟化，为虚拟机提供计算资源；
- 一台虚拟机的计算资源只能位于一台物理服务器上，当物理服务器负载较高或故障时，自动迁移至其它健康的物理服务器；
- 虚拟机计算能力通过虚拟 CPU (vCPU) 和虚拟内存表示，存储能力通过云存储容量和性能体现；
- 虚拟机管理程序通过控制 vCPU、内存及磁盘的 QoS，用于支持虚拟机资源隔离，保证多台虚拟机在同一台物理服务器上互不影响；

虚拟机是云平台用户部署并运行应用服务的基础环境，与物理计算机的使用方式相同，提供创建、关机、断电、开机、重置密码、重装系统、升降级等完全生命周期功能；支持 Linux、Windows 等不同的操作系统，并可通过 VNC、SSH 等方式进行访问和管理，拥有虚拟机的完全控制权限。虚拟机运行涉及资源及关联关系如下：



如图所示，实例规格、镜像、VPC 网络是运行虚拟机必须指定的基础资源，即指定虚拟机的 CPU 内存、操作系统、虚拟网卡及 IP 信息。在虚拟机基础之上，可绑定云硬盘、弹性 IP 及安全组，为虚拟机提供数据盘、公网 IP 及网络安全，保证虚拟机应用程序的数据存储和网络安全。

在虚拟化计算能力方面，平台提供 GPU 设备透传能力，支持用户在平台上创建并运行 GPU 虚拟机，让虚拟机拥有高性能计算和图形处理能力。

3.2 创建虚拟机

云平台用户可以通过指定机型、规格、镜像、云硬盘、VPC 网络、公网 IP、安全组及虚拟机相关基础信息一键创建一个或多个虚拟机，用于部署自己的应用和服务。

3.2.1 前提条件

- 在创建虚拟机前，已拥有一个可登录云平台的账号，并已为账号充值金额；
- 在创建虚拟机前，需通过控制台左上角的【地域】选择需要创建并运行的虚拟机的数据中心；
- 确认用户所指定区域及账户的配额足够；若配额不足，需向云平台管理申请资源配额；
- 若不使用系统提供的默认安全组，需要在目标地域创建一个安全组并添加能满足用户业务需求的安全规则。

3.2.2 创建操作

- 选择虚拟资源需运行的地域（数据中心）后，在左侧导航栏选择虚拟机，进入虚拟机控制台，点击“创建虚拟机”，弹出虚拟机创建向导；

基础配置

机型 * ComputeSetBBBB(x86_64) ComputeSetAAAA(aarch64)

镜像 * 基础镜像 自制镜像

UOS

UOS 20_SP1 x86_64

规格 * 1核2G 2核4G 4核8G 8核16G 16核32G 32核64G 64核128G

系统盘类型 * StorageSetAAAA(SSD) StorageSetBBBB(HDD)

系统盘容量 * 500GB 200 GB

数据盘 购买并绑定

数据盘类型 * StorageSetAAAA(SSD) StorageSetBBBB(HDD)

硬盘容量 * 8000GB 10 GB

- 选择虚拟机的机型，并确定虚拟机运行的操作系统镜像；

- 机型是运行虚拟机的宿主机的集群类型，代表不同架构、不同型号的 CPU 或硬件特征，可由管理员自定义，如 x86 机型、GPU 机型、ARM 机型等；
- 镜像即虚拟机实例运行环境的模板，可以选择基础镜像和自制镜像：
 - 基础镜像是由平台官方默认提供，包括多发行版 Centos、Ubuntu 及 Windows 等原生操作系统；
 - 自制镜像由用户通过虚拟机自行导出或自定义导入的自有镜像，可用于创建虚拟机，仅账号自身有权限查看和管理。

- 选择虚拟机的规格配置，即定义提供计算能力的 CPU 内存及 GPU 配置，规格可由平台管理员进行自定义；

- CPU 机型默认提供 1核2G、2核4G、4核8G、8核16G、16核32G 及 64核128G 等虚机规格；
- 平台提供 GPU 设备透传能力，若机型为 GPU 机型，可创建并运行拥有 GPU 能力的虚拟机；
- 针对 GPU 机型，平台支持最高配置 4 颗 GPU 芯片，为使 GPU 虚拟机发挥最佳性能，平台限制最小 CPU 内存规格为 GPU 颗数的 4 倍以上，如 1 颗 GPU 芯片最小需要 4核8G 规格，2 颗 GPU 芯片最小需要 8 核16G 规格，4 颗 GPU 芯片最小需要 16核32G 规格。

- 选择并配置虚拟机的系统盘和数据盘，可分别配置系统盘和云硬盘的容量。

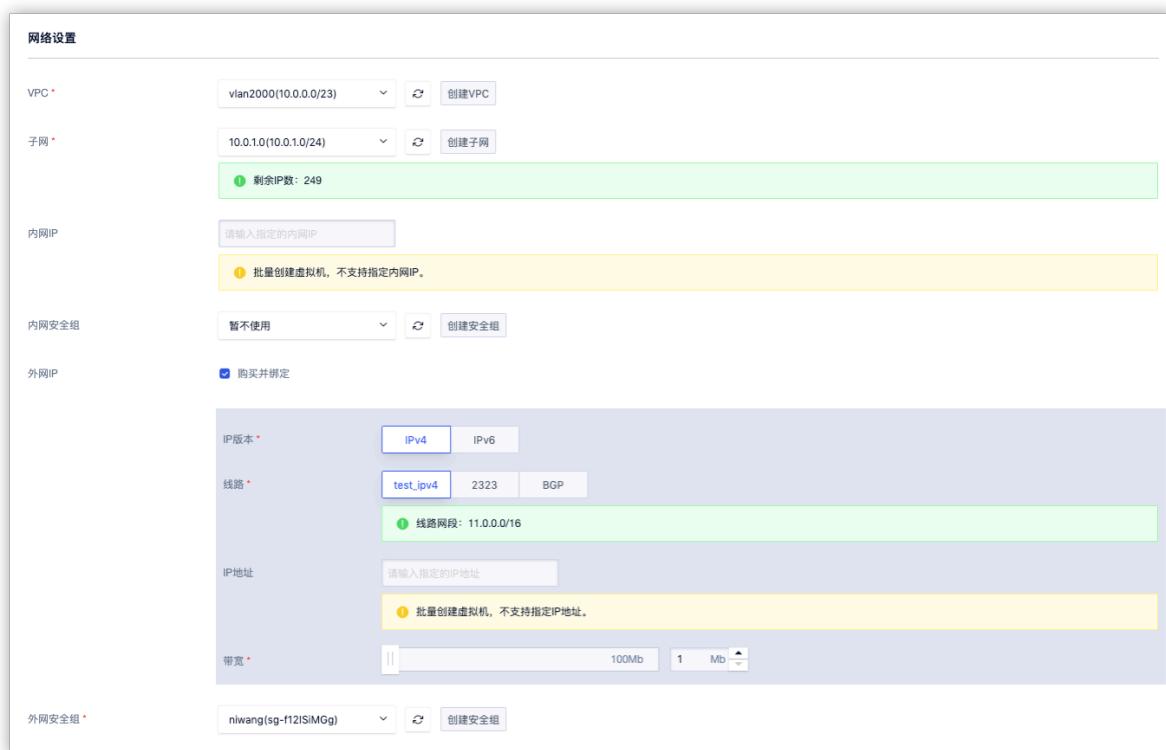
- 系统盘：运行虚拟机镜像的系统盘，创建虚拟机时必须选择系统盘类型及系统盘容量；

- 选择系统盘的磁盘类型，如 SSD 磁盘或 HDD 磁盘，磁盘类型可由管理员进行自定义；
- 配置系统盘容量，Linux 和 Windows 镜像默认系统盘均为 40GB，支持扩容系统盘容量至 500GB。

扩容系统盘是增加块设备的容量，并未对系统内的文件系统进行扩容，即系统盘扩容后需进入虚拟机内部进行文件系统的扩容(resize)操作，具体操作步骤详见：[系统盘扩容](#)。

- 数据盘：一种基于分布式存储系统为虚拟机提供持久化存储空间的弹性块设备，创建虚拟机支持同时创建一块云盘并自动绑定至虚拟机，同时会对硬盘进行自动格式化及挂载操作。
 - 默认数据盘挂载路径为 `/data`，用户也可选择虚拟机创建后再添加数据云硬盘；
 - 选择并配置数据盘类型及容量，容量范围的规格可由管理员进行自定义；
 - 平台默认规格最小支持 10GB 容量，最大支持 8000GB，步长为 10GB，即容量应为 10GB 的倍数。

5. 配置网络相关设置，包括虚拟机需要加入的 VPC 网络、子网、内网 IP 地址、内网安全组、外网 IP 及外网安全组等选项：



- VPC 网络是一个属于用户的、逻辑隔离的二层网络广播域环境。在一个 VPC 网络内，用户可以构建并管理多个三层网络，即子网（Subnet），VPC 私有网络是子网的容器，不同 VPC 间网络绝对隔离：
 - 创建虚拟机时必须选择 VPC 网络和所属子网，即选择虚拟机要加入的网络及 IP 网段；
 - 控制台已为用户计算所选子网的可用 IP 数量，创建时需指定可用 IP 数量足够的子网；
 - 平台默认会从所属子网的网段中为虚拟机自动分配 IP 地址，可通过【内网 IP】选项手动指定虚拟机的 IP 地址。
- 安全组是平台提供的虚拟防火墙，提供出入双方向流量访问控制规则，定义哪些网络或协议能访问资源：
 - 外网安全组用于控制虚拟机南北向（外网 IP）的流量，内网安全组用于虚拟机东西向（网卡间）的安全访问控制；
 - 默认必须绑定一个外网安全组，内网安全组默认为暂不绑定，可在创建虚拟机后在进行绑定；

- 系统提供默认安全组，若无法满足需求，可自行创建安全组并绑定至虚拟机。
- 外网 IP 为虚拟机提供的弹性外网出口服务，支持创建虚拟机时申请并绑定一个外网 IP 至虚拟机。平台支持 IPv4/IPv6 双栈网络，可在虚拟机创建成功后为虚拟机绑定多个外网 IP 地址，最多支持绑定 10 个 IPv4 和 10 个 IPv6 外网 IP 地址，并支持手动设置虚拟机默认出口。

平台支持在虚拟机中查看已绑定的外网 IP 地址及网络路由，虚拟机访问外网的流量直接通过虚拟网卡透传至物理网卡与外部网络通信，提升网络传输的性能。

6. 选择并配置虚拟机基础管理配置，包括虚拟机名称、登录方式及登录密码等。

管理配置

Virtual Machine Name *: host

Administrator Name *: uos

Information message: (当前显示的是UOS系统的默认用户名, 登录时请注意)

Login Method *: 密码

Administrator Password *: Please enter password

- 虚拟机名称：平台默认配置名称为 `host`，用户可自定义虚拟机名称，可通过名称进行搜索和筛选；
- 登录方式：为虚拟机设置登录凭证，即登录虚拟机的密码；
 - CentOS 的管理员为 `root`，Ubuntu 的管理员为 `ubuntu`，Windows 系统的管理员名称为 `administrator`；
 - Linux 操作系统可在虚拟机创建成功后，通过 SSH 密钥的方式进行登录及管理。

9. 选择购买数量和付费方式，如下图所示确认订单并点击“立即购买”进行虚拟机创建操作。

Purchase Quantity: 1

Payment Method: Month

Total Cost: 12 元

Buy Now

- 购买数量：按照所选配置及参数批量创建多台虚拟机，最多可批量创建 10 台虚拟机，批量创建时不支持手动设置虚拟机的 IP 地址；
- 付费方式：选择虚拟机的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式；

- 合计费用：用户选择虚拟机 CPU、内存、数据盘、外网 IP 等资源按照付费方式的费用展示；
- 立即购买：点击立即购买后，会返回虚拟机资源列表页，在列表页可查看该台主机的创建过程，通常会先显示“启动中”的状态，在1~2分钟内即可创建完成。

3.3 查看虚拟机

通过导航栏进入虚拟机控制台，可查看虚拟机资源的列表，通过列表上的虚拟机名称，可进入虚拟机详情，查看虚拟机及相关资源的详细信息。

3.3.1 虚拟机列表

虚拟机列表页可查看当前账户下已有的虚拟机资源列表，包括名称/备注、资源 ID、VPC、子网、机型、配置、IP、计费方式、创建时间、过期时间、状态及操作等，同时也可通过“自定义列表”按钮，自定义列表所需信息。

名称	虚拟机ID	VPC	子网	机型	配置	IP	计费方式	创建时间	过期时间	状态	操作
host 修改名称及备注	vm-WvcsJQGGg	vlan2000 vpc-NvYp5wMMR	10.0.1.0 subnet-1E5A5wGm	ComputeSetBBBB	0 1 2 40 0	(内)10.0.1.3 (外)192.168.179.99	月	2020-07-08	2020-08-08	运行	<button>详情</button> <button>登录</button> <button>启动</button> ...
WEB1 修改名称及备注	vm-3BScpwMg	vlan2000 vpc-NvYp5wMMR	10.0.0.0 subnet-jcMo5QGMg	ComputeSetBBBB	0 4 8 40 0	(内)10.0.0.2	月	2020-07-08	2020-08-08	运行	<button>详情</button> <button>登录</button> <button>启动</button> ...

- 主机名称：虚拟机的名称和备注，可通过列表页的编辑按钮进行修改；
- 资源 ID：虚拟机的全局唯一 ID，可通过复制按钮对 ID 进行复制操作；
- VPC/子网：虚拟机创建时所指定的 VPC 网络和子网，即虚拟机 IP 所在的 VPC 网络和子网信息；
- IP 地址：虚拟机的 IP 地址，包括内网 IP 和外网 IP (若有)，并可通过复制按钮对 IP 地址进行复制操作；
- 机型：虚拟机所运行物理机的集群类型，代表不同架构、不同型号的 CPU 或硬件特征；
- 配置：虚拟机基本配置信息，包括 CPU 内存规格、GPU 颗数、系统盘镜像、系统盘总容量及数据盘总容量；
- 计费方式：虚拟机创建时指定的付费方式，包括按时、按月、按年；
- 创建时间/过期时间：虚拟机的创建时间和计费周期内的过期时间；
- 状态：虚拟机当前的运行状态，包括启动中、运行、关机中、关机、启动中、修改配置中、重装中、删除中及迁移中和宕机迁移中等；
- 操作：对单台虚拟机的更多操作，包括详情、登录、启动、关闭、删除、断电、重启、修改告警模板、制作镜像、重置密码、重装系统、绑定外网 IP、修改安全组及修改系统配置；

默认列表每页可显示 10 条虚拟机信息，支持分页并设置每页可展示的虚拟机数量，每页最多可展示 100 条虚拟机数据，可通过搜索框对虚拟机列表进行搜索和筛选，支持模糊搜索。

为方便租户对虚拟机进行维护和操作，平台支持下载当前用户所拥有的所有虚拟机资源列表信息为 Excel 表格；同时支持对虚拟机的批量操作，包括批量启动、关闭及删除操作，可通过选中多个虚拟机，点击批量操作按钮进行批量操作，如下图所示：

虚拟机管理
虚拟机模版
镜像管理
网卡管理
硬盘管理
快照管理

创建虚拟机
启动
关机
删除

名称	虚拟机ID	VPC	子网
host 修改名称及备注	vm-u4fD4K7Mg	vlan2000 vpc-NvYp5wMMR	10.0.1.0 subnet-1E5A5wGMg
WEB1 修改名称及备注	vm-3BScpwMGg	vlan2000 vpc-NvYp5wMMR	10.0.0.0 subnet-jcMo5QGMg

3.3.2 虚拟机详情信息

在虚拟机列表上，点击虚拟机的名称或 ID 可进入当前虚拟机的概览页面查看虚拟机详情及监控信息，同时可切换到硬盘、网络及操作日志页面查看虚拟机的相关磁盘、网络、IP 地址、弹性网卡及操作日志信息，如下图概览页所示：

[虚拟机 / vm-u4fD4K7Mg](#)

概览 硬盘信息 网络 操作日志

登录 启动 关机 断电 重启 ...

基本信息

资源ID	vm-u4fD4K7Mg
资源名称	host 修改名称及备注
内网IP	10.0.1.6
VPC	vlan2000 vpc-NvYp5wMMR
子网	10.0.1.0 subnet-1E5A5wGMg
状态	运行
创建时间	2020-07-15 13:09:28
告警模版	Default

监控信息

1小时 2020-07-15 12:24:43 – 2020-07-15 13:24:43 自动刷新 OFF

CPU使用率(%)

内存使用率(%)

空间使用率(%)

网卡入带宽(Mbps)

3.3.2.1 虚拟机概览

概览页面展示基本信息、配置信息及监控图表等信息，同时可通过概览页对虚拟机进行操作及管理。

- 基本信息包括资源 ID、名称、内网 IP、VPC、子网、状态、创建时间及告警模板；

- 可点击名称右侧按钮修改虚拟机的名称和备注信息；
- 可点击告警模板右侧按钮修改虚拟机所关联的告警模板，虚拟机默认会绑定 Default 告警模板；
- 配置信息包括机型、镜像、CPU、内存、系统盘总容量和系统盘总容量，其中数据盘容量为当前虚拟机所关联所有云硬盘的容量之和；
- 监控图表：包括 CPU 使用率、内存使用率、空间使用率、网卡的出/入带宽、网卡的出/入包量、磁盘的读/写吞吐、磁盘的读/写次数、平均负载、TCP 连接数和阻塞进程数量。

用户可开启监控图表右上角的【自动刷新】，使页面每隔 30 秒自动刷新，以获取最新监控图表数据。

3.3.2.2 虚拟机硬盘

磁盘页面展示当前虚拟机的系统盘及已挂载的数据盘信息，包括每个硬盘的名称、ID、集群类型、硬盘类型、硬盘容量、挂载点、计费方式、状态、创建时间、过期时间及对单个硬盘的快照操作信息。如下图所示：

名称	资源ID	集群	硬盘类型	硬盘容量	挂载点	计费方式	状态	创建时间	过期时间	操作
3434 修改名称及备注	disk-iQTBNFnMR	StorageSetBBBB	数据盘	10GB	vdb	月	● 已绑定	2020-07-15	2020-08-15	<button>快照</button>
host 修改名称及备注	ci-u4fD4K7Mg_boot	StorageSetAAAA	系统盘	40GB	vda		● 已绑定	2020-07-15		<button>快照</button>

- 集群类型指虚拟机系统盘和数据盘所在物理机所在的集群类型，可由管理员自定义，如 SSD 或容量型等；
- 硬盘类型包括系统盘和数据盘，除系统盘外，额外绑定的云硬盘均为数据盘；
- 硬盘容量为每块硬盘的当前容量大小；
- 挂载点为硬盘在虚拟机中真实的挂载盘符，如 vdb；
- 仅数据盘支持计费方式和过期时间信息，系统盘与虚拟机的生命周期一致。

在详情页面，支持分别对系统盘和数据盘进行快照操作，快照仅捕获已写入硬盘的数据，不包含应用程序或操作系统缓存在内存中的数据，为确保快照中捕获所有应用程序的数据，建议将虚拟机关机或卸载数据盘后再进行快照。

创建快照

重要提示

- 创建快照时，请勿进行硬盘挂载，或者修改虚拟机的状态（开机），否则会导致快照创建异常。
- 快照只能捕获已写入硬盘的数据，不包含应用程序或操作系统缓存在内存中的数据。为了确保快照中捕获所有应用程序的数据，建议先暂停对硬盘的 I/O 操作后进行快照制作。（关机或者卸载硬盘）

硬盘ID *	ci-u4fD4K7Mg_boot
硬盘名称	host
快照名称 *	请输入快照名称

取消
确认

3.3.2.3 虚拟机网络

网络页面展示当前虚拟机的基本网络信息，同时可管理虚拟机的外网 IP 及弹性网卡资源。其中基本网络信息包括当前虚拟机的属 VPC、所属子网、内网 IP、外网安全组及内网安全组信息，并可通过安全组右侧的按钮更新虚拟机的外网安全组和内网安全组。如下图所示：

The screenshot shows the network configuration for a virtual machine named 'vm-XL3tALZGg'. The 'Network' tab is selected. On the left, there's a sidebar with 'Basic Information' containing fields for '所属VPC' (vpc002), '所属子网' (10.192), '内网IP' (10.0.192.6), '外网安全组' (test), and '内网安全组' (无). The main area has tabs for 'External IP' and 'Elastic Network Card'. Under 'External IP', a note says '仅支持将有默认路由的外网IP设为虚拟机默认网络出口。' (Only supports setting an external IP with a default route as the virtual machine's default network interface if it has a default route). A table lists two bound external IPs: '106.75.234.39' (BGP) and '106.75.234.30' (BGP). Both are IPv4, have a bandwidth of 1Mb or 7Mb, are set as default routes, and are bound. There are buttons to 'Bind' (已绑定) and 'Unbind' (解绑) for each row, and a 'Set as Export' button for each row.

有关虚拟机的外网 IP 和弹性网卡资源详情及管理详见：[外网IP管理](#)和[弹性网卡管理](#)。

3.3.2.4 外网 IP 管理

平台支持 IPv4/IPv6 双栈网络，每个虚拟机最多支持绑定 10 个 IPv4 和 10 个 IPv6 外网 IP 地址，默认以第一个有默认路由的 IP 地址作为虚拟机的默认网络出口；同时在虚拟机中查看已绑定的外网 IP 地址及网络路由，虚拟机访问外网的流量直接通过虚拟网卡透传至物理网卡与外部网络通信，提升网络传输的性能。

如上图所示，外网 IP 标签页可查看当前虚拟机已绑定的外网 IP 列表信息及相关管理操作，包括绑定外网 IP、解绑外网 IP、设为默认出口等。已绑定外网 IP 信息包括 IP 地址、IP 版本、出口、带宽、路由类型、状态等。

- IP 指当前已绑定外网 IP 的 IP 地址及网段名称（网段是由平台管理员自定义的外网 IP 地址池）；
- IP 版本是指当前已绑定外网 IP 的 IP 版本，包括 IPv4 和 IPv6；
- 出口指当前 IP 是否为虚拟机的默认出口，一台虚拟机最多支持两个默认出口（IPv4 和 IPv6 各一个）；
- 带宽指当前 IP 地址的带宽上限，带宽上限由申请外网 IP 地址时指定；
- 路由类型指当前 IP 地址所属网段下发路由的类型（网段路由策略由平台管理员自定义），包括默认路由和非默认路由，仅支持将有默认路由的外网 IP 设为虚拟机默认网络出口。
 - 默认路由类型指虚拟机绑定该 IP 地址时，会自动下发目标地址为 `0.0.0.0/0` 的路由到虚拟机中；
 - 非默认路由指虚拟机绑定该 IP 地址时，会下发管理员为网段配置的指定目标地址路由，如为虚拟机下发目标地址为 `10.0.0.0/24` 的路由；
 - 若绑定至虚拟机的多个外网 IP 地址均为默认路由类型，默认以第一个有默认路由的 IP 地址作为虚拟机的默认出口。

用户可通过外网 IP 管理控制台的操作项，进行外网 IP 地址的绑定、解绑及设为默认出口操作，支持批量解绑。

3.3.2.4.1 绑定外网 IP

最多支持绑定 10 个 IPv4 和 10 个 IPv6 外网 IP 地址，默认以第一个有默认路由的 IP 地址作为虚拟机的默认网络出口。



绑定成功后，可在虚拟机中查看已绑定的 IP 地址已配置在虚拟机的第二块网卡上，本章节以 `Centos` 操作系统为例，如下图所示：

```
[root@localhost ~]# [root@localhost ~]# ip a | grep eth1
: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    inet 106.75.234.39/25 brd 106.75.234.255 scope global eth1
        link layer brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff state unknown
    inet 106.75.234.30/25 brd 106.75.234.255 scope secondary eth1
        link layer brd ff:ff:ff:ff:ff:ff brd ff:ff:ff:ff:ff:ff state unknown
[root@localhost ~]#
```

3.3.2.4.2 解绑外网 IP

支持虚拟机解绑外网 IP 地址，若解绑了默认出口外网IP，则自动选择下一个有默认路由的外网 IP 作为虚拟机的默认网络出口。

解绑IP

是否确认解绑下面1个外网弹性IP？解绑后您将可以对其进行删除或重新绑定资源

资源ID *	eip-UYhr5KnMg
名称 *	343
IP *	106.75.234.39
绑定资源ID *	vm-Ls7CoF7Mg
绑定资源类型 *	虚拟机

取消 确认

3.3.2.4.3 设为默认出口

支持用户手动将一个已绑定的外网 IP 设置为虚拟机的默认网络出口，仅支持将有默认路由的外网 IP 设为虚拟机默认网络出口。用户可通过虚拟机外网 IP 管理控制台，为虚拟机绑定的 IPv4 和 IPv6 外网 IP 分别设置默认网络出口。如下图所示：

设为出口

是否将以下 IP 地址设为网络出口？虚拟机将通过新的出口 IP 对外访问。

资源ID *	eip-UYhr5KnMg
IP *	106.75.234.39

取消 确认

设为出口后，可登录虚拟机验证虚拟机访问外网的 IP 地址是否为设置的外网 IP 地址，本节以 Centos 7.4 系统设置 IPv4 默认出口为 106.75.234.39 为例，如下图所示，已绑定外网 IP 地址列表已将新 IP 地址设置为出口：

仅支持将有默认路由的外网IP设为虚拟机默认网络出口。

<input type="checkbox"/>	IP	IP版本	出口	带宽	路由类型	状态	操作
<input type="checkbox"/>	106.75.234.39 BGP	IPv4	是	1Mb	默认路由	已绑定	<button>设为出口</button> <button>解绑</button>
<input type="checkbox"/>	106.75.234.30 BGP	IPv4	否	7Mb	默认路由	已绑定	<button>设为出口</button> <button>解绑</button>

< 1 > 10 条/页 /1

登录 Centos 虚拟机，输入 `curl ifconfig.io` 查看虚拟机访问外网的出口已更换为 `106.75.234.39`，如下图输出结果所示：

```
[root@localhost ~]# ip a s | grep eth1
4: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP qlen 1000
    inet 106.75.234.39/25 brd 106.75.234.47 scope global eth1
        inet 106.75.234.30/25 brd 106.75.234.31 scope global secondary eth1
[root@localhost ~]#
[root@localhost ~]# curl ifconfig.io
106.75.234.39
[root@localhost ~]#
```

外网 IP 地址池资源由管理员自定义，支持使用私有 IP 地址段模拟公网 IP 地址，并在上层物理网络设备上做 NAT 转换访问互联网或 IDC 数据中心网络。

3.3.2.5 弹性网卡管理

平台虚拟机最多支持绑定 6 块弹性网卡，用于精细化网络管理或高可用业务等应用场景。虚拟机中可查看已绑定的弹性网卡及关联的 IP 地址等信息，在 `Linux` 操作系统中通常会以 `eth2` 开始命名。

弹性网卡

<input type="checkbox"/>	名称	资源ID	IP地址	网卡类型	VPC	子网	安全组	状态	操作
<input type="checkbox"/>	net2 修改名称及备注	nic-sU-c0F7MR	10.0.1.8	内网网卡 10.0.1.8	vlan2000 vpc-NvYp5wMMR	10.0.1.0 subnet-1E5A5wGMg	已绑定	<button>解绑</button>	
<input type="checkbox"/>	net1 修改名称及备注	nic-odTcAKnGR	10.0.1.7	内网网卡 10.0.1.7	vlan2000 vpc-NvYp5wMMR	10.0.1.0 subnet-1E5A5wGMg	已绑定	<button>解绑</button>	

< 1 > 10 条/页 /1

如上图所示，弹性网卡标签页可查看当前虚拟机已绑定的弹性网卡列表信息及解绑操作。已绑定的弹性网卡信息包括名称、ID、IP 地址、VPC、子网、安全组及状态。

- VPC/子网：指当前弹性网卡所属的 VPC 网络和子网；
- IP 地址：指当前弹性网卡从子网中分配到的 IP 地址；
- 安全组：指当前弹性网卡已绑定的安全组，若未绑定安全组，则为空。

支持在虚拟机详情中，将已绑定的弹性网卡进行解绑，解绑后可将弹性网卡绑定至其它虚拟机，通过已绑定弹性网卡列表操作项中的解绑操作可对网卡进行解绑，具体操作如下：



3.3.2.6 虚拟机操作日志

虚拟机操作日志页面展示当前虚拟机的操作日志。可提供自定义时间级别的日志展示，同时可对日志进行模糊搜索，默认提供两周内的操作日志，可通过切换日期周期查看不同时间周期的操作日志。

The screenshot shows the 'Operation Log' tab of a virtual machine's details page. It includes a search bar and date range selector (set to '不限' and '2020-07-01 16:57:49 — 2020-07-15 16:57:49'). The log table lists six operations:

操作(API)名称	资源ID	操作者	失败(码)原因	备注	状态	操作时间
UnBindEIP 解绑外网弹性IP	vm-Ls7CoF7Mg	yongfeng.lv@ucloud.cn	(空)	(无)	成功	2020-07-15 16:33:48
UpdateVMDefaultGW 设置虚拟机默认出口	vm-Ls7CoF7Mg	yongfeng.lv@ucloud.cn	(空)	(无)	成功	2020-07-15 16:18:00
BindEIP 绑定外网弹性IP	vm-Ls7CoF7Mg	yongfeng.lv@ucloud.cn	(空)	(无)	成功	2020-07-15 16:17:18
BindEIP 绑定外网弹性IP	vm-Ls7CoF7Mg	yongfeng.lv@ucloud.cn	(空)	(无)	成功	2020-07-15 16:17:14
CreateVMIstance 创建虚拟机	vm-Ls7CoF7Mg	yongfeng.lv@ucloud.cn	(空)	(无)	成功	2020-07-15 15:57:26

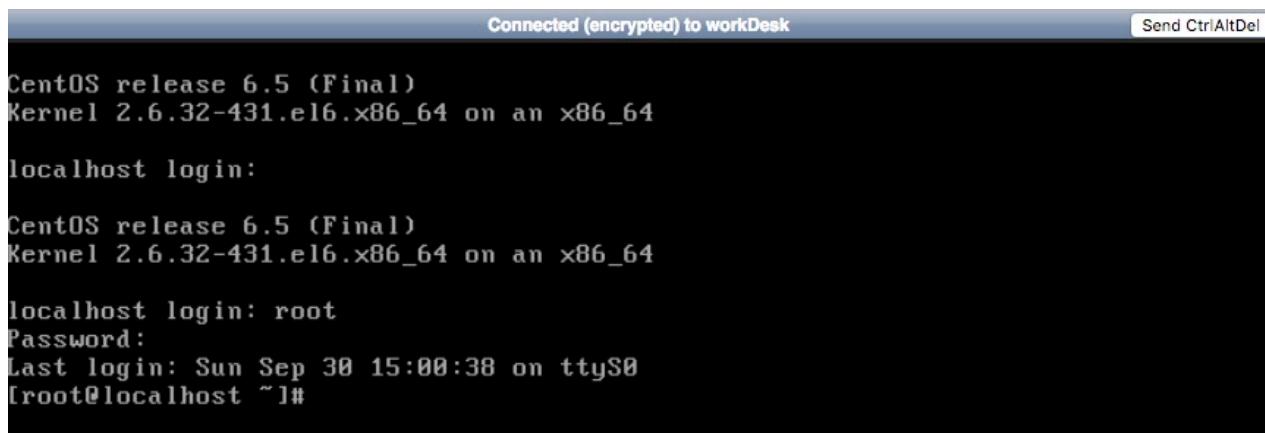
Pagination controls at the bottom right indicate page 1 of 1.

如上图所示，操作日志内容包括操作名称、资源 ID、操作者、失败原因、备注、操作状态及操作时间。

3.4 VNC 登录

VNC（Virtual Network Console）是 UCloudStack 为用户提供的一种通过 WEB 浏览器连接虚拟机的登录方式，适应于无法通过远程登录客户端（如 SecureCRT、远程桌面等）连接虚拟机的场景。通过 VNC 登录连到虚拟机，可以查看虚拟机完整启动流程，并可以像 SSH 及 远程桌面一样管理虚拟机操作系统及界面，支持发送操作管理指令，如 `CTRL+ALT+DELETE`。

用户可通过虚拟机列表或详情概览页面操作中的“登录”按钮，使用 VNC 链接登录当前虚拟机，提供如同显示器的功能，可登入虚拟机操作系统，对虚拟机进行系统级别的操作和管理。如下图所示：



Connected (encrypted) to workDesk

Send CtrlAltDel

```
CentOS release 6.5 (Final)
Kernel 2.6.32-431.el6.x86_64 on an x86_64

localhost login:

CentOS release 6.5 (Final)
Kernel 2.6.32-431.el6.x86_64 on an x86_64

localhost login: root
Password:
Last login: Sun Sep 30 15:00:38 on ttys0
[root@localhost ~]#
```

登录虚拟机的前提条件是拥有操作系统账号和密码，VNC 登录适合虚拟机没有外网 IP 地址的场景。

3.5 启动/关机/断电/重启

用户可以对虚拟机进行关机、启动、断电及重启等基本操作，且均支持多台 API 批量操作。如下图所示：



- 关机
 - 用户可使用系统命令进行关机，如 Windows 系统下的关机和 Linux 系统下的 shutdown 命令；
 - 支持用户通过控制台点击【关机】进行关机操作，关机时虚拟机的状态必须为启动状态；
 - 虚拟机关机时，状态会从运行转换为关机中，最后转换为已关机，代表关机成功；
 - 若虚拟机卡在关机中，支持对虚拟机进行断电操作；
 - 关机后，虚拟机的内存信息丢失，所有磁盘的数据将被保留；
 - 关机后可进行启动、删除、制作镜像、重装系统、修改配置、绑定外网 IP 及修改安全组等操作。
- 启动
 - 用户可通过控制台点击【启动】按钮开启虚拟机，仅在虚拟机状态为已关机时可用；
 - 虚拟机开启时，状态会从已关机转换为启动中，最后转换为运行，代表启动成功；
 - 若虚拟机卡在启动中，支持对虚拟机进行断电操作；
 - 运行的虚拟机可执行关闭、登录、删除、断电、重启、重置密码、热升级、绑定外网 IP、修改安全组及修改告警模板等操作。
- 断电
 - 断电是将虚拟机强行关机，与物理机直接断电操作相同，断电操作可能导致丢失数据甚至损坏操作系统；
 - 断电操作适用于虚拟机死机及极端测试的场景，可通过虚拟机列表操作中的“断电”按钮，对虚拟机进行强关机操作；
 - 强行关机时，虚拟机直接会进入关机状态，可再次进行启动操作。
- 重启
 - 重启是将虚拟机的操作系统进行正常的重新启动，与物理机操作系统重启操作一致；
 - 虚拟机重启时，状态会从运行转换为重启中，最后转换为运行；
 - 若虚拟机卡在重启中，支持对虚拟机进行断电操作；
 - 重启后，虚拟机的内存信息丢失，所有磁盘的数据将被保留。

3.6 制作镜像

自制镜像由云平台账户通过虚拟机自行导出，可用于创建虚拟机，仅账户自身有权限查看和管理，仅支持虚拟机关机状态下制作镜像，即在关机状态才可进行虚拟机导出为镜像操作。

用户可通过点击虚拟机列表操作中的“制作镜像”按钮进行镜像制作，需输入镜像名称及镜像描述，如下图所示：



- 镜像名称：自制镜像的名称和标识；
- 镜像描述：自制镜像的描述和备注信息，可选项；

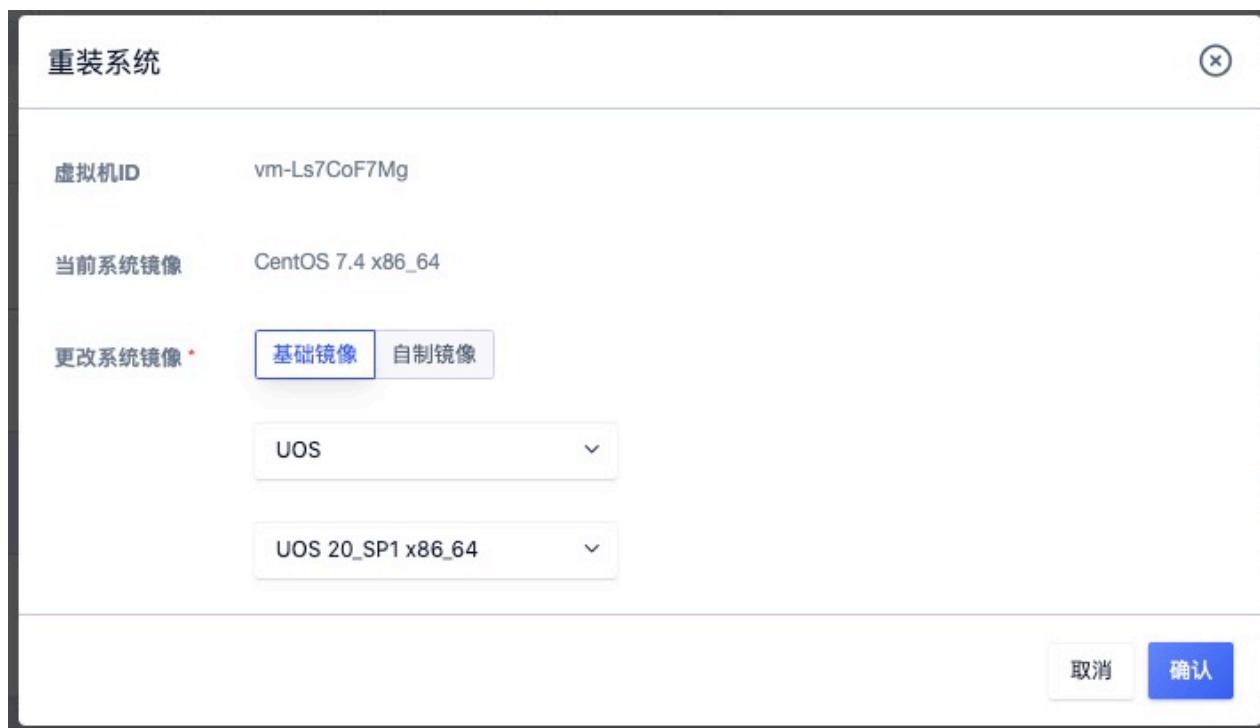
制作镜像过程中，请勿对虚拟机进行停止、启动、断电、重装系统或修改配置等操作，以免影响镜像制作过程。镜像制作成功后，会展示在虚拟机控制台——镜像管理页面，可通过页面查看镜像的制作过程，待镜像状态转换为可用时，即可使用自制镜像创建虚拟机。

通过虚拟机制作镜像时，仅导出系统盘的数据和信息，不支持数据盘。

3.7 重装系统

重装系统是重置虚拟机的操作系统，即更换虚拟机镜像，Linux 虚拟机仅支持更换 Centos 和 Ubuntu 操作系统，Windows 虚拟机仅支持更换 Windows 其它版本的操作系统，重装系统的前提是虚拟机必须为关机状态。

虚拟机关机后，通过虚拟机控制台操作中的“重装系统”按钮更换虚拟机的镜像，如下图所示：



重装系统时，虚拟机的状态自动转换为重装中，重装成功后转换为“关机”，可以通过启动操作开启虚拟机，虚拟机启动时，会使用新的镜像运行虚拟机。

注：重装系统后，虚拟机之前操作系统及数据内容将被清空，挂载的云硬盘及快照不受影响。

3.8 重置密码

重置密码是指在线修改虚拟机操作系统的登录密码，适应于忘记登录密码或想通过控制台快速修改密码的场景。

Linux 操作系统是修改 `root` 账号的密码，Windows 操作系统是修改 `administrator` 账号的密码。重置密码时虚拟机必须运行状态。用户通过点击虚拟机控制台操作中的“重置密码”按钮进行密码的重置，如下图所示：



- 虚拟机名称：当前需要修改密码的虚拟机名称和标识；
- 管理员密码/确认密码：需要修改的新密码；
- 若用户主动修改了虚拟机操作系统的管理员账号，则无法进行密码重置；

请勿在制作镜像过程中重置密码，用户也可以通过登录操作系统，使用操作系统命令或界面进行密码修改。

3.9 修改配置

修改配置即更改虚拟机的 CPU 和内存规格，支持升级和降级，适应于业务发生变化需调整虚拟机配置的场景。

修改配置前需将虚拟机进行关机，即必须在关机状态下进行配置修改操作，配置变更后，需重新启动才可生效。用户可点击虚拟机控制台资源列表操作中的“修改配置”进行虚拟机 CPU 内存的调整，如下图所示：



虚拟机降级配置，下个付费周期按新配置扣费。按小时付费的虚拟机，升级配置下个付费周期按新配置扣费；按年按月付费的虚拟机，升级配置即时生效，并按比例自动补差价。

- 虚拟机 ID 和名称：当前需要变更规格配置的虚拟机名称和全局唯一 ID 标识；
- 计费方式：当前虚拟机的付费方式；
- 目前规格：当前虚拟机变更前的 CPU 内存配置；
- 更改规格：当前虚拟机需要变更的新规格配置，支持升级或降级配置；
- 预计收费：变更配置后，系统预计需要扣除的费用；

点击确定后，虚拟机依然处于关机状态，下次启动时，会使用新变更的配置运行虚拟机。用户可在虚拟机开机后，登录操作系统查看变更后的配置。

修改配置仅对 CPU 内存生效，若虚拟机附带 GPU 能力，不支持对 GPU 颗数进行升降配。

3.10 热升级

虚拟机提供热升级能力，支持虚拟机开机状态下升级 CPU 和内存。使用热升级前，需先熟悉以下基本概念：

- 修改配置：即在虚拟机关机状态下，升级或者降级虚拟机的CPU 和内存规格；
- 热升级：即在虚拟机开机（running）状态下，支持升级虚拟机的CPU、内存；
- Base镜像：即基础镜像，用户可以通过Base镜像启动一台虚拟机，并基于该虚拟机制作一个自定义镜像。

注：目前仅支持 Base 镜像为 Centos7.4 的虚拟机热升级，不支持在线降级操作。

平台支持热升级的虚拟机，在列表上会自动显示支持热升级，如下图所示：

名称	资源ID	机型	配置	IP	过期时间	状态	操作
host 修改名称及备注	vm-CGJXP7rZg	ComputeBBBB	0 1 2 40 0	(内) 10.0.0.30	2020-04-23 13:42:09	运行	[Details] [Login] [Start] [More...]
host 修改名称及备注	vm-8j3JzC0XWg	ComputeBBBB 热升级	0 2 4 40 0	(内) 10.0.0.22 (内) 10.0.0.20	2020-04-13 15:03:51	关机	[Details] [Login] [Start] [More...]

(1) 当用户看到热升级提示后，可通过列表操作项中的“热升级”对该虚拟机进行在线配置调整，如下图：

机型	配置	IP	过期时间	状态	操作
ComputeBBBB	0 1 2 40 0	(内) 10.0.0.30	2020-04-23 13:42:09	关机	[Details] [Login] [Start] [More...]
ComputeBBBB 热升级	0 2 4 40 0	(内) 10.0.0.22 (内) 10.0.0.20	2020-04-13 15:03:51	运行	[Details] [Login] [Start] [More...]

(2) 在热升级的向导中，可以对虚拟机的 CPU 内存规格进行热升级操作，热升级后立即生效，按小时购买的虚拟机下个付费周期按新配置扣费，按年按月购买的虚拟机按比例自动补差价，如下图所示：

热升级

配置升级立即生效，按小时购买的虚拟机下个付费周期按新配置扣费，按年按月购买的虚拟机按比率自动补差价。

虚拟机ID *	vm-ytVWLK7MR
名称	host
计费方式	月
当前规格	2核4G
更改规格 *	1核2G 2核4G 4核8G 8核16G 16核32G 32核64G 64核128G
预计收费	263.76

取消 确认

若用户自定义镜像，其 Base 镜像是基于 Centos7.4 制作的，则默认允许热升级操作。

3.11 修改告警模板

修改告警模板是对虚拟机的监控数据进行告警的配置，通过告警模板定义的指标及阈值，可在虚拟机相关指标故障及超过指标阈值时，触发告警，通知相关人员进行故障处理，保证虚拟机及业务的正常运行。

用户可点击虚拟机详情概览页中告警模板右侧的按钮进行告警模板修改操作，在修改告警模板向导中选择新虚拟机告警模板，点击确定立即生效。

更改告警模版

资源ID *	vm-GgJWgoprng
资源类型 *	虚拟机
告警模版 *	请选择

取消 确定

- 资源 ID：当前需要添加或修改告警模板的虚拟机 ID；
- 资源类型：当前需要添加或修改告警模板的资源类型；
- 告警模板：需要变更的告警模板，一台虚拟机仅支持关联一个告警模板。

若系统提供的默认告警模板无法满足需求时，可前往“告警模板”页面进行添加和配置。

3.12 绑定外网 IP

绑定外网 IP 指将租户外网 IP 地址绑定至虚拟机，为虚拟机提供外部网络出口。平台支持 IPv4/IPv6 双栈网络，每个虚拟机最多支持绑定 10 个 IPv4 和 10 个 IPv6 外网 IP 地址，默认以第一个有默认路由的 IP 地址作为虚拟机的默认网络出口。

绑定外网 IP 地址后，平台会将指定的外网 IP 地址配置至虚拟机的网卡，包括外网 IP 地址所属网段的网关、子网掩码及路由相关信息，用户可在虚拟机中查看已绑定的外网 IP 地址及网络路由，虚拟机访问外网的流量直接通过虚拟网卡透传至物理网卡与外部网络通信，提升网络传输的性能。

虚拟机必须处于运行或关机状态才可进行外网 IP 绑定，可通过虚拟机管理控制台列表或虚拟机详情网络管理的操作项“绑定外网 IP”按钮，进行外网 IP 绑定操作，具体操作步骤可参考[虚拟机外网 IP 管理](#)。绑定操作需指定要绑定的外网 IP 地址，仅支持绑定 10 个 IPv4 和 10 个 IPv6 外网 IP 地址。

- 若虚拟机已绑定 10 个 IPv4 外网 IP 地址，则不可再次绑定 IPv4 外网 IP 地址；
- 若虚拟机已绑定 10 个 IPv6 外网 IP 地址，则不可再次绑定 IPv6 外网 IP 地址；
- 若虚拟机已同时绑定 10 个 IPv4 和 10 个 IPv6 外网 IP 地址，则无法再绑定任何外网 IP 地址。

外网 IP 地址绑定成功后，可通过虚拟机列表 IP 信息查看已绑定的外网 IP 地址，同时用户也可通过虚拟机详情网络管理的外网 IP 标签页查看已绑定外网 IP 地址的详情信息，并可进行设为默认出口及解绑等相关操作。

The screenshot shows a list of virtual machines. The first host has one bound external IP address: (外)106.75.234.39. The second host has two bound external IP addresses: (外)106.75.234.39 and (外)106.75.234.30. A red box highlights the second host's row, specifically the column showing its bound external IP addresses.

名称	虚拟机ID	机型	配置	IP	创建时间	过期时间	状态
host 修改名称及备注	vm-ytVWLK7MR	普通型	0 2 4 40 0	(内)10.0.192.8 (外)106.75.234.39	2020-07-15	2020-08-15	运行
host 修改名称及备注	vm-Ls7CoF7Mg	普通型	0 2 4 40 0	(外)106.75.234.30 查看详情	2020-07-15	2020-08-15	关机

仅支持绑定同一数据中心(区域)的外网 IP 地址，被绑定的外网 IP 必须处于未绑定状态。如需解绑虚拟机的外网 IP 地址，详参考：[虚拟机外网 IP 管理](#)。

3.13 修改安全组

平台用户创建的虚拟机，默认会自带两个与虚拟机生命周期一致的虚拟网卡，即内网网卡和外网网卡。

- 内网网卡：配置虚拟机创建时指定 VPC/子网的 IP 地址及相关网络信息；
- 外网网卡：配置绑定至虚拟机的所有外网 IP 地址，包括 10 个 IPv4 和 10 个 IPv6 地址；
- 弹性网卡：虚拟机绑定的弹性网卡配置弹性网卡所在 VPC/子网 的 IP 地址及安全组相关网络信息；

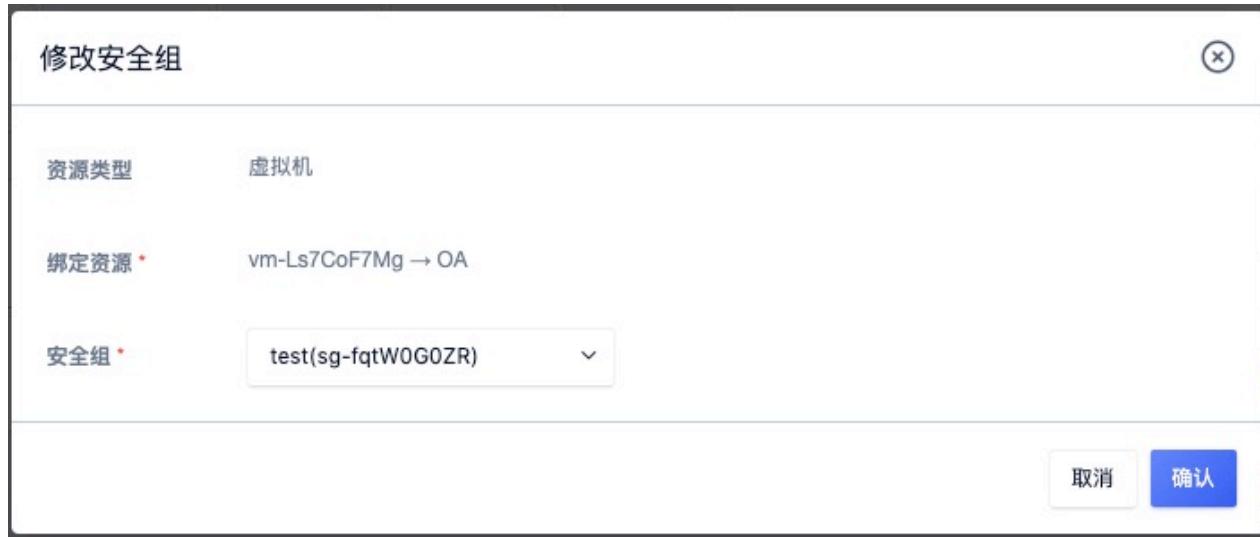
云平台安全组（软件定义的虚拟防火墙）为网卡级别，即绑定的安全组会对虚拟机中网卡流量做出入限制。平台将绑定至内网网卡的安全组定义为内网安全组；绑定至外网网卡安全组定义为外网安全组；绑定至弹性网卡的安全组为弹性网卡的所属安全组。

在创建虚拟机时可进行内网安全组和外网安全组的指定，同时在虚拟机运行后也可修改内网安全组和外网安全组。

3.13.1 修改外网安全组

修改外网安全组是指修改虚拟机外网网卡所关联的安全组，即更改绑定至外网网卡上所有外网 IP 地址的安全组。

用户可通过虚拟机列表及虚拟机详情网络页面的“修改外网安全组”按钮进行操作，如下图所示：

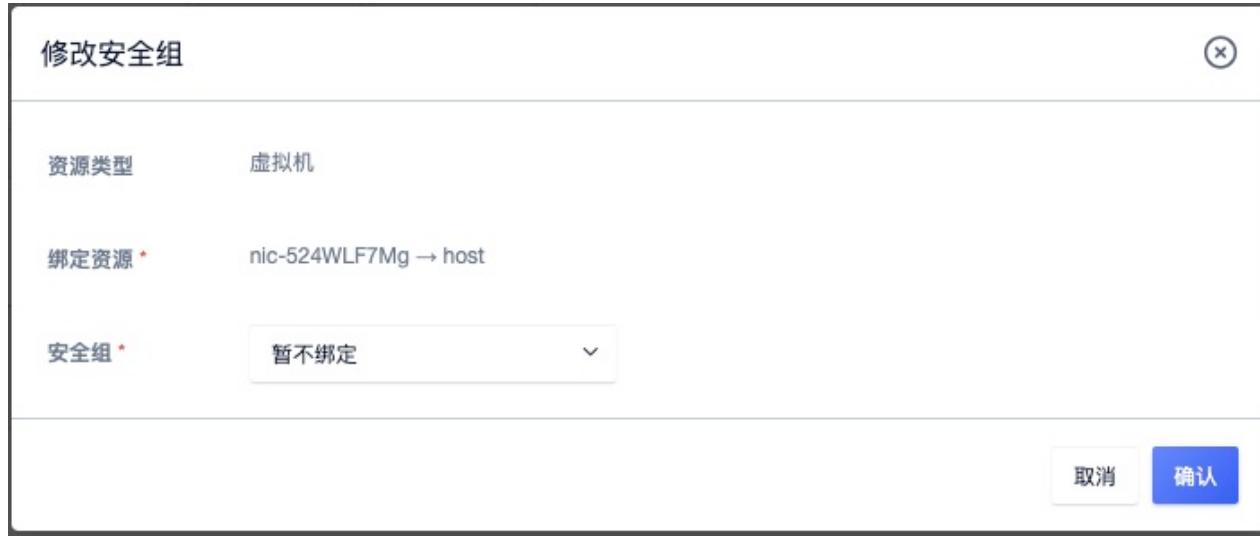


选择需修改的的外网安全组，一台虚拟机仅支持绑定一个外网安全组。修改成功后，用户可通过虚拟机详情的网络信息查看已修改的外网安全组信息。

外网安全组规则的访问限制作用于当前虚拟机所绑定的所有外网 IP。

3.13.2 修改内网安全组

修改内网安全组是指修改虚拟机内网网卡所关联的安全组，即更改虚拟机内网的安全策略，用于虚拟机与虚拟机间的流量管控。用户可通过虚拟机列表及虚拟机详情网络页面的“修改内网安全组”按钮进行操作，如下图所示：



选择需要修改的内网安全组，支持修改为“暂不绑定”用于解绑内网安全组，一台虚拟机仅支持绑定一个内网安全组。修改成功后，用户可通过虚拟机详情的网络信息查看已修改的内网安全组信息。

内网安全组和外网安全组支持绑定同一个安全组，即内外网安全组使用相同的安全组及策略。

3.14 修改名称和备注

修改虚拟机的名称和备注，在任何状态下均可进行操作。点击虚拟机列表页面虚拟机名称右侧的按钮即可进行修改，如下图所示：



3.15 删除虚拟机

平台用户可在控制台删除账户内已关机或正在运行的虚拟机资源，支持批量删除。虚拟机被删除后自动进入“回收站”，可通过回收站进行还原或彻底销毁。可通过虚拟机列表操作项中的“删除”进行操作，如下图所示：



- 删除虚拟机时会自动解绑虚拟机已绑定的外网 IP、弹性网卡、云硬盘等资源；
- 若虚拟机已添加至 NAT 网关白名单或负载均衡的服务节点中，删除虚拟机时会自动进行解绑操作；
- 支持用户在删除虚拟机时选择删除已绑定的资源，即自动解绑并删除已绑定的外网 IP、弹性网卡及云硬盘；
- 删除虚拟机时同时删除的外网 IP 和云硬盘将自动进入回收站，同时删除的弹性网卡将被彻底销毁；
- 若虚拟机过期，在允许时间内未续费成功，则虚拟机会被自动回收，关联的资源将自动解绑。

虚拟机删除后，随虚拟机创建的 2 个默认网卡、系统盘及系统盘数据将随虚拟机一起进入回收站，可进入回收站对虚拟机进行销毁或恢复操作。

随虚拟机同时进入回收站的外网 IP 及云硬盘在恢复时，不会保持原有绑定关系，需重新进行资源绑定操作。

3.16 远程登录

远程登录是指通过远程管理客户端软件通过网络远程登录并管理虚拟机，针对 Linux 和 Windows 的虚拟机分别提供不同的方式进行远程登录。远程登录的前提条件为虚拟机必须绑定外网 IP 地址，并可通过外网正常访问服务器的远程登录端口（Linux SSH 为 22、Windows 远程桌面为 3389）。

3.16.1 远程登录 Linux

为方便验证，本手册假设本地用的客户端操作系统为 Linux 或 Mac OS，即默认自带 SSH 客户端，可通过命令行直接使用 SSH 命令登录远端 SSH 服务端。具体操作步骤为：

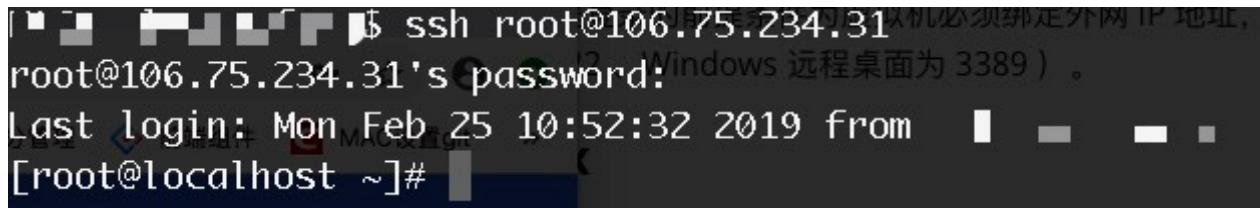
1. 为需要远程登录的虚拟机绑定外网 IP 地址且外网安全组允许 SSH 22 端口访问，如下图所示：

主机名称	资源ID	机型	配置	IP	状态	操作
cinderwindows 修改名称及备注	vm-GgJWgprmg	标准型N1	4 8 40 0	(内) 192.168.1.8	● 运行	详情 登录 启动 ...
cindertest 修改名称及备注	vm-FAdrB5rig	标准型N1	2 4 20 0	(内) 192.168.1.7 (外) 106.75.234.31	● 运行	详情 登录 启动 ...
cinder 修改名称及备注	vm-Y8uzD79ig	标准型N1	2 4 20 0	(内) 192.168.1.2	● 运行	详情 登录 启动 ...

2. 用户打开系统自带的终端（Terminal）并输入 SSH 命令登录：`ssh root@虚拟机的外网 IP 地址`，如下例：

```
# ssh root@106.75.234.31
```

3. 输入虚拟机的登录密码，即可直接登录 Linux 服务器，如下图所示即代表登录成功。



3.16.2 远程登录 Windows

为方便验证，本手册假设本地用的客户端操作系统为 Mac OS，使用微软远程桌面连接 MAC 版程序 [RDC](#) 进行登录，操作步骤同 Windows 远程桌面相同，仅需要在工具输入 Windows 的公网 IP 地址即可连接，如下图所示：



远程桌面连接的前提是虚拟机必须绑定外网 IP 地址，且绑定的外网安全组允许 3389 端口通行，若在操作系统内部修改了远程桌面的默认端口，则安全组需允许修改后的端口通行。

3.17 系统盘扩容

虚拟机默认系统盘容量为 40GB，平台支持用户对系统盘容量进行扩容，最大支持扩容至 500GB。默认 40GB 系统盘容量不能满足业务需求时，可指定所需系统盘容量进行虚拟机的创建，如下图指定 200GB 系统盘容量创建虚拟机，则创建的虚拟机系统盘块设备容量即为 200GB。

虚拟机 / 创建虚拟机

基础配置

机型 * 普通型(x86_64) 高性能(x86_64) GPU(x86_64)

镜像 * 基础镜像 自制镜像

CentOS

CentOS 7.4 x86_64

规格 * 1核2G 2核4G 4核8G 8核16G 16核32G 32核64G 64核128G

系统盘类型 * 分布式存储(HDD) 分布式存储(SSD)

系统盘容量 * 200 GB

系统盘扩容后，需要进入虚拟机内部进行文件系统的扩容。

数据盘 购买并绑定

对系统盘容量的扩容，是对系统盘块设备的容量扩容，并未对虚拟机操作系统内的文件系统进行扩容操作，即系统盘扩容后需进入虚拟机内部进行文件系统的扩容（resize）操作。

针对不同类型的的操作系统分区扩容操作有所不同，如 Windows 通常使用自带的磁盘管理工具进行扩容操作。根据不同 OS 系统盘扩容场景大致分类如下：

- Linux 系统盘分区扩容
- Windows 系统盘分区扩容

在执行系统内分区扩容及文件系统扩展前，需保证已在控制台对系统盘的存储容量进行调整。

3.17.1 Linux 系统盘分区扩容

Linux 系统通常使用 `growpart` 和 `resize2fs` 工具完成系统盘分区扩容及文件系统扩展操作。本示例以 Centos 7.4 操作系统为例，具体操作如下：

1、安装 `growpart` 文件系统扩容工具。

- Centos

```
yum install -y epel-release  
yum install -y cloud-utils
```

- Ubuntu

```
sudo apt-get install cloud-initramfs-growroot
```

2、通过 `fdisk -l` 查看系统盘容量为 200GB，运行 `df -Th` 查看系统盘分区 `/dev/vda1` 容量为 40GB，文件系统类型为 ext4。

```
[root@localhost ~]# fdisk -l  
  
磁盘 /dev/vda: 214.7 GB, 214748364800 字节, 419430400 个扇区  
Units = 扇区 of 1 * 512 = 512 bytes  
扇区大小(逻辑/物理): 512 字节 / 512 字节  
I/O 大小(最小/最佳): 512 字节 / 512 字节  
磁盘标签类型: dos  
磁盘标识符: 0x000ba442  
  
      设备 Boot      Start        End      Blocks   Id  System  
/dev/vda1  *        2048    83883775   41940864   83  Linux  
[root@localhost ~]#  
[root@localhost ~]# df -Th  
文件系统      类型      容量  已用  可用  已用% 挂载点  
devtmpfs      devtmpfs  1.9G     0  1.9G    0% /dev  
tmpfs         tmpfs    1.9G     0  1.9G    0% /dev/shm  
tmpfs         tmpfs    1.9G   8.4M  1.9G    1% /run  
tmpfs         tmpfs    1.9G     0  1.9G    0% /sys/fs/cgroup  
/dev/vda1      ext4     40G   1.4G   36G    4% /  
tmpfs         tmpfs  382M     0  382M    0% /run/user/0
```

3、运行 `growpart <DeviceName> <PartitionNumber>` 命令扩容分区并重启虚拟机，本示例 `growpart /dev/vda 1` 表示扩容系统盘的分区 1 的容量。

```
[root@localhost ~]# LANG=en_US.UTF-8
[root@localhost ~]# growpart /dev/vda 1
CHANGED: partition=1 start=2048 old: size=83881728 end=83883776 new:
size=419428319 end=419430367
[root@localhost ~]# reboot
```

4、待虚拟机重启后，扩展虚拟机系统盘的文件系统，不同文件系统类型使用不同的方式进行扩展。

- ext 类型的文件系统，可使用 `resize2fs <PartitionName>` 工具进行扩容，如下所示：

```
[root@localhost ~]# resize2fs /dev/vda1
resize2fs 1.42.9 (28-Dec-2013)
Filesystem at /dev/vda1 is mounted on /; on-line resizing required
old_desc_blocks = 5, new_desc_blocks = 25
The filesystem on /dev/vda1 is now 52428539 blocks long.
```

- 若 xff 类型的文件系统，可使用 `xfs_growfs <mountpoint>` 工具进行扩容。

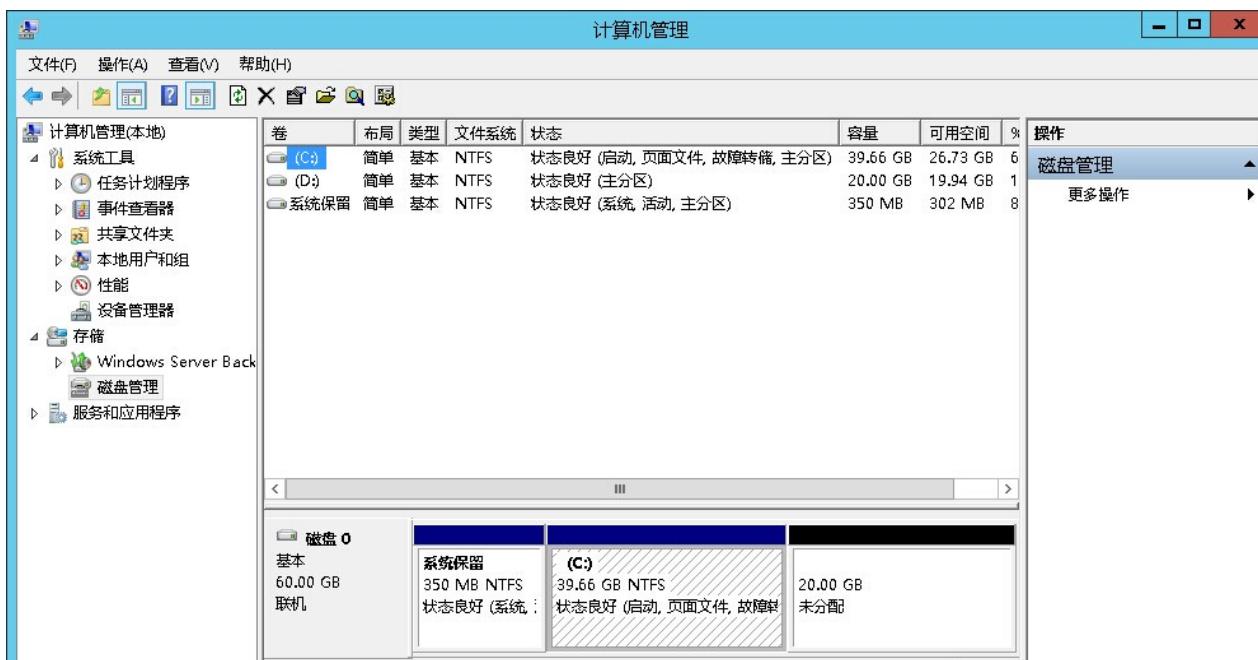
5、运行 `df -Th` 查看系统盘分区 `/dev/vda1` 容量为 200GB。

```
[root@localhost ~]# df -Th
文件系统      类型    容量  已用  可用  已用% 挂载点
/devtmpfs     devtmpfs  1.9G   0   1.9G   0% /dev
tmpfs         tmpfs    1.9G   0   1.9G   0% /dev/shm
tmpfs         tmpfs    1.9G  8.3M  1.9G   1% /run
tmpfs         tmpfs    1.9G   0   1.9G   0% /sys/fs/cgroup
/dev/vda1     ext4    197G  1.5G  187G   1% /
tmpfs         tmpfs   382M   0   382M   0% /run/user/0
```

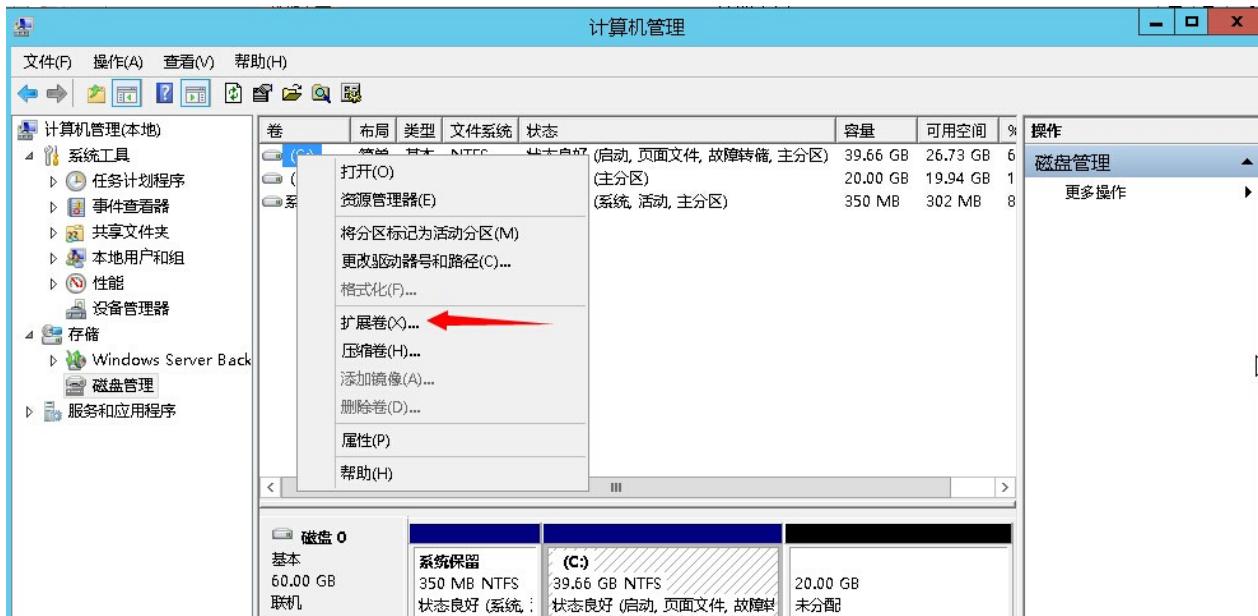
3.17.2 Windows 系统盘分区扩容

Windows 系统通常使用“管理工具——计算机管理”中的“磁盘管理”工具进行扩展卷操作。具体操作如下：

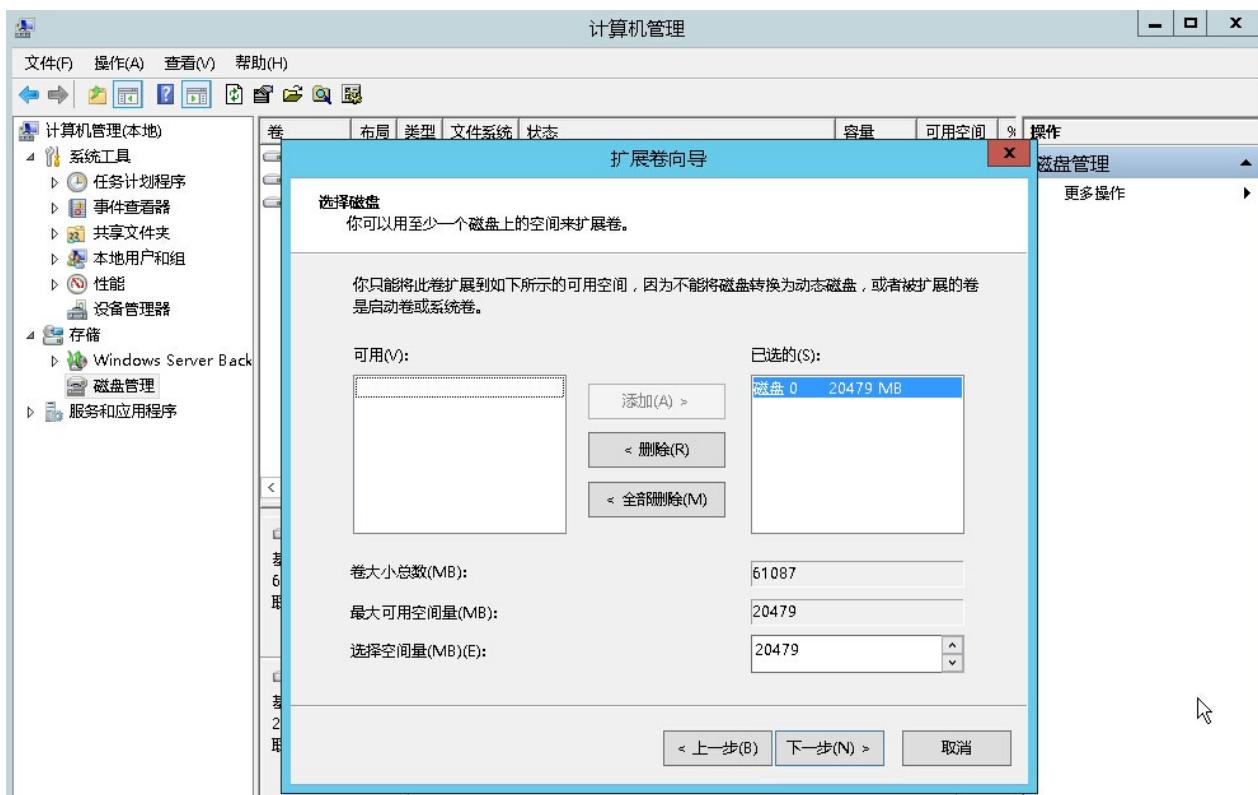
1、在磁盘管理工具中选择操作>重新扫描磁盘，用于识别新扩容的未分配空量空间，如下图 20GB 未分配空间；



2、右键点击 C 盘，选择扩展卷，对系统盘进行扩展卷操作。



3、在扩展卷向导中，使用默认配置进行扩展卷操作。



4、扩展卷操作完成后，新增系统盘容量会自动合并至 C 盘，代表系统盘文件系统扩展成功。

4 自制镜像管理

自制镜像归属于云平台用户（租户），用户从虚拟机导出的自制镜像及自定义上传导入的镜像均属于自制镜像，仅租户和平台管理员有权限查看和管理。

自制镜像可用于创建虚拟机，并支持用户下载虚拟机镜像到本地，同时镜像管理支持查看镜像、修改名称和备注、从镜像创建虚拟机、导入镜像、下载镜像及删除镜像等生命周期管理。

4.1 查看自制镜像

通过导航栏进入虚拟机控制台，切换至镜像管理页面可查看当前账户下自制镜像资源的列表及相关详细信息，包括镜像名称、资源 ID、系统类型、状态及操作项，如下图所示：

- 镜像名称/资源 ID：当前自制镜像的名称及全局唯一 ID 标识；
- 系统类型：代表当前自制镜像的操作系统类型，如 Linux、Windows、Kylin 等；

- 状态：当前自制镜像的状态，包括创建中、导入中、导入失败、可用、删除中、已删除；
 - 创建中：通过虚拟机自制镜像过程中，镜像的状态为创建中；
 - 导入中：用户通过导入镜像功能导入镜像的过程中，镜像的状态为导入中；
 - 导入失败：指用户导入镜像失败；
 - 可用：指当前镜像为可用状态，可创建虚拟机或进行下载；
 - 删除中：指当前镜像被删除中；
 - 已删除：指当前镜像已被删除，并进入回收站。
- 操作：对单个自制镜像的操作，包括从镜像创建虚拟机、下载镜像及删除镜像；

为方便租户对镜像资源进行维护和操作，平台支持对镜像进行批量删除操作，可通过选中多个自制镜像，点击批量删除按钮进行批量操作。

4.2 从镜像创建虚拟机

从镜像创建主机指通过自制或自定义导入的镜像重新创建一台虚拟机，创建的虚拟机使用自制镜像启动，虚拟机中的程序及数据保持自制镜像的创建时的状态。

用户可通过镜像管理资源列表的操作项“从镜像创建主机”进行创建，如下图所示，虚拟机创建向导自动为用户选择指定的自制镜像。

基础配置

机型 * 普通型(x86_64) 高性能(x86_64) GPU(x86_64)

镜像 * 基础镜像 自制镜像

CentOS

vpn环境

规格 * 1核2G 2核4G 4核8G 8核16G 16核32G 32核64G 64核128G

系统盘类型 * 分布式存储(HDD) 分布式存储(SSD)

系统盘容量 * 500GB 40 GB

数据盘 购买并绑定

使用自制镜像创建虚拟机的过程与基础镜像相同，可根据提示进行操作。

从镜像创建虚拟机时设置的管理员密码会覆盖原镜像操作系统中的密码，需使用新密码登录创建的虚拟机。

4.3 导入镜像

导入镜像是指租户将第三方业务虚拟机以镜像的方式迁移到平台镜像仓库，使租户可以在通过导入的镜像创建并部署业务虚拟机，是用户将业务迁移至 UCloudStack 平台的重要通道。

支持用户导入 Linux 和 Windows 发行版及自定义镜像，并支持 X86 架构和 aarch64 两种系统架构镜像的导入；云平台的镜像格式默认为 RAW，用户上传 VHD、VMDK、QCOW2、OVA、ISO 等格式的镜像时，需先将镜像转换为 RAW 格式的镜像才可导入。有关转换镜像及自定义镜像的具体操作可参考[自定义镜像指南](#)。

用户制作好自定义镜像后，可通过镜像管理控制台资源列表上方的【导入镜像】功能，进入导入镜像向导页面：

导入镜像

镜像名称 *

镜像描述

镜像地址 *

操作系统 * Linux Windows

系统架构 * x86_64 aarch64

系统平台 *

系统版本 *

镜像格式 * RAW

镜像大小 *

SHA256

- 镜像名称/描述：镜像的名称及相关描述信息；
- 镜像地址：平台导入镜像时读取并下载镜像的 URL 地址，导入镜像时必须提供；
 - 支持 HTTP、HTTPS、FTP 等协议的 URL 地址，格式包括 `https://path/file` 或 `ftp://hostname[:port]/path/file` 或 `ftp://user:password@hostname[:port]/path/file`；
 - 镜像的地址必须从云平台可达，即云平台组件可访问的 URL 地址，建议使用云平台相同外网的 IP 地址；
- 操作系统：导入镜像的操作系统类型，包括 Linux 和 Windows，需根据导入镜像 OS 类型进行选择；

- 系统架构：导入镜像的系统架构，包括 `x86_64` 和 `aarch64`，需根据导入镜像进行选择；
- 系统平台：指导导入镜像的操作系统平台；
 - Linux 操作系统的系统平台包括 Centos 和 Ubuntu；
 - Windows 操作系统的系统平台仅支持 Windows；
- 系统版本：当前需导入镜像的操作系统版本；
 - CentOS 支持 CentOS 6 和 CentOS 7 版本；
 - Ubuntu 支持 Ubuntu 14 和 Ubuntu 16 版本；
 - Windows 支持 WIN2008 和 WIN2012 版本；
- 镜像格式：当前平台仅支持导入 RAW 格式的镜像；
- 镜像大小：当前导入镜像的大小，最大不能超过 500GB；
- SHA256：用于校验文件完整性的值，默认无需指定。

镜像导入后，自制镜像列表生成一条状态为“导入中”的镜像，由于平台需要先下载镜像至镜像仓库且镜像通常较大，导入镜像的时间通常比较长。

镜像状态转换为可用时，即代表镜像导入成功，可进行虚拟机创建或进行镜像下载操作；若镜像导入过程中出现意外导致失败，则镜像的状态会转换为“导入失败”，可对失败的镜像进行删除并重新导入镜像。

导入镜像前需确保镜像地址可被访问且可读取并下载到镜像。

4.4 下载镜像

下载镜像指用户将平台自制的镜像下载至本地，用于备份或迁移。虚拟机镜像通过为 GB 级别文件，为保证下载镜像的断点续传等功能，平台以提供下载地址的方式支持镜像下载；可通过 FTP、SFTP 及相关工具进行镜像下载，以保证断点续传功能，提升镜像下载的成功率。

用户如果需要下载镜像至本地时，可通过自制镜像列表操作项中的【下载】进入镜像下载向导页面，如下图所示：



点击生成下载地址后，平台会跳转至下载地址展示向导页面，通过向导页面，用户通过复制下载地址链接，通过 HTTP、FTP 及相关下载工具下载镜像。

导出镜像



! 确认要导出镜像名为vpn环境的镜像么？

镜像ID * image-fQ06wdzMg

镜像名称 vpn环境

基础镜像 CentOS 7.4 x86_64

下载地址 http://106.75.234.4:8080/?f...

操作成功

关闭

镜像下载地址有效期为 24 小时，需在 24 小时内进行镜像下载。若镜像下载地址过期，则无法进行下载，需到平台重新生成镜像下载地址。

4.5 删除自制镜像

用户可对自制镜像进行删除操作，被删除的自制镜像会自动进入“回收站”，可进行还原和销毁操作。用户可通过自制镜像管理控制台的“删除”功能进行自制镜像的删除，删除后可到回收站中查看已删除的自制镜像。

删除镜像



! 是否删除以下 1 个镜像？镜像删除后会进入回收站，可通过回收站进行恢复和销毁。

资源ID * image-fQ06wdzMg

资源名称 * vpn环境

取消

确认

仅支持删除状态为可用或导入失败的的自制镜像；若已通过自制镜像创建虚拟机，则不可删除自制镜像，需要将虚拟机删除，才可进行自制镜像的删除。

4.6 修改名称和备注

修改自制镜像的名称和备注，在任何状态下均可进行操作。可通过点击自制镜像列表页面每个镜像名称右侧的“编辑”按钮进行修改。

5 弹性网卡

弹性网卡（Elastic Network Interface, ENI）是一种可随时附加到虚拟机的弹性网络接口，支持绑定和解绑，可在多个虚拟机间灵活迁移，为虚拟机提供高可用集群搭建能力，同时可实现精细化网络管理及廉价故障转移方案。

弹性网卡与虚拟机自带的默认网卡（一个内网网卡和一个外网网卡）均是为虚拟机提供网络传输的虚拟网络设备，同时会从所属 VPC/子网中为网卡分配 IP 地址、网关、子网掩码等网络信息。

- 默认内网网卡所属的网络即创建虚拟机时指定的 VPC 和子网；
- 每块弹性网卡在创建时均可指定所属 VPC 和子网，即可为每块弹性网卡自定义所属网络及 IP 地址。

为虚拟机绑定一块不同 VPC 的弹性网卡，虚拟机即可与不同 VPC 网络的虚拟机进行通信。

弹性网卡具有独立的生命周期，支持绑定和解绑管理，可在多个虚拟机间自由迁移；虚拟机被销毁时，弹性网卡将自动解绑，可绑定至另一台虚拟机使用。

弹性网卡具有地域（数据中心）属性，仅支持绑定相同数据中心的虚拟机。**一块弹性网卡仅支持绑定至一个虚拟机，一个虚拟机最多可绑定 6 块弹性网卡**。用户可通过平台自定义创建网卡，并对网卡进行绑定、解绑及修改安全组等相关操作。

5.1 创建弹性网卡

云平台用户可通过指定网卡名称、所属 VPC、子网创建一个弹性网卡，用于扩展虚拟机的网络接口。创建弹性网卡前需保证账户至少拥有一个 VPC 网络和子网。

通过导航栏进入虚拟机控制台，切换至网卡管理页面，点击“创建网卡”按钮进入弹性网卡创建向导弹窗，如下图：

创建网卡

名称 *	<input type="text" value="请输入网卡名称"/>
VPC *	vpc002(10.0.0.0/16) <input type="button" value="刷新"/> <input type="button" value="创建VPC"/>
子网 *	10.192(10.0.192.0/20) <input type="button" value="刷新"/> <input type="button" value="创建子网"/>
剩余IP数: 4084	
安全组 *	<input type="text" value="暂不使用"/> <input type="button" value="刷新"/> <input type="button" value="创建安全组"/>
IP	<input type="text" value="请输入网卡IP"/>
<input type="button" value="取消"/> <input type="button" value="确认"/>	

- 名称：当前需要创建弹性网卡的名称及标识；
- 所属 VPC：弹性网卡需要加入的 VPC 网络，创建时必须指定；
- 所归属子网：弹性网卡需要加入 VPC 的 IP 地址段，需选择可用 IP 数量充足的子网；
- IP 地址：当前网卡的 IP 地址，默认会从子网的 IP 地址段中自动分配 IP 地址，如需自定义 IP 地址，可在 IP 地址栏中输入指定的 IP 地址。
- 安全组：当前网卡需要绑定的安全组，用于管控进出弹性网卡的网络流量；支持暂不绑定操作，即当前网卡暂不绑定安全组。

弹性网卡绑定的安全组与虚拟机绑定的内网安全组互不影响，弹性网卡的绑定的安全组仅对关联的弹性网卡流量进行安全管控。

弹性网卡创建时状态为“创建中”，待状态转换为“未绑定”时，即代表网卡创建成功，可进行绑定虚拟机操作，同时可修改弹性网卡的安全组。

5.2 查看网卡

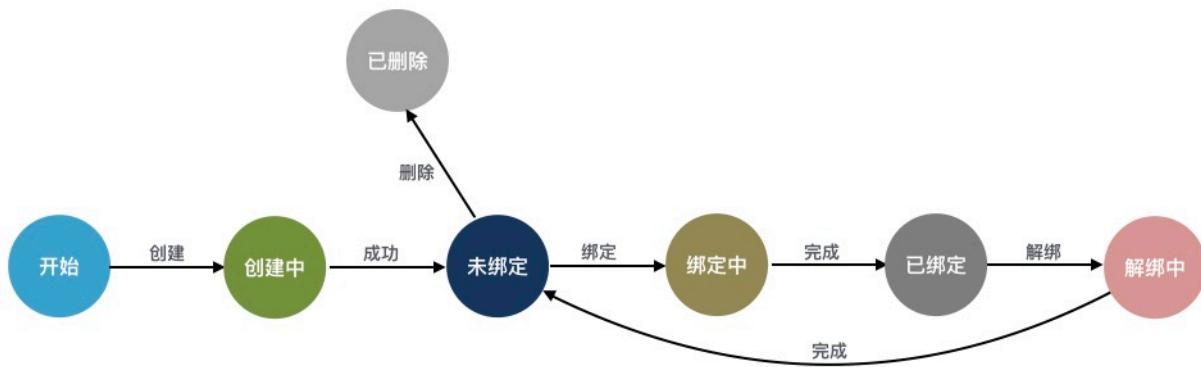
通过导航栏进入虚拟机控制台，切换至网卡管理页面可查看弹性网卡资源的列表及相关信息，包括网卡的名称、资源 ID、绑定资源、所属 VPC、所归属子网、安全组、状态、创建时间及操作项，如下图所示：

The screenshot shows the Network Card Management interface with the following details:

操作	名称	资源ID	网卡类型	绑定资源	VPC	子网	安全组	创建时间	状态	操作
<input type="checkbox"/>	nic111 修改名称及备注	nic-MU1TtYnMg	内网网卡 10.0.192.14	vm-ETbN60nMR host	vpc002 vpo-SX33TigMR	10.192 subnet-b3VqTNzGR	test sg-fqtW0G0ZR	2020-07-19	已绑定	<input type="button" value="解绑"/> <input type="button" value="删除"/> ...
<input type="checkbox"/>	2323 修改名称及备注	nic-Ea9g-a7GR	内网网卡 10.0.192.13	(无)	vpc002 vpo-SX33TigMR	10.192 subnet-b3VqTNzGR	Default sg-Ci9kUJvpm	2020-07-18	未绑定	<input type="button" value="绑定"/> <input type="button" value="解绑"/> <input type="button" value="删除"/> ...
<input type="checkbox"/>	w232 修改名称及备注	nic-a-LETYZMg	内网网卡 10.0.192.2	vm-Ls7CoF7Mg OA	vpc002 vpo-SX33TigMR	10.192 subnet-b3VqTNzGR		2020-06-24	已绑定	<input type="button" value="解绑"/> <input type="button" value="删除"/> ...

Page navigation: < 1 > 10 条/页 /1

- 名称/ID：弹性网卡的名称及全局唯一标识符；
- 网卡类型：弹性网卡的类型，目前仅支持内网网卡类型，同时会显示网卡所分配或指定的 IP 地址；
- 绑定资源：弹性网卡已绑定的虚拟机资源名称和 ID，若未指定则为空；
- VPC/子网：弹性网卡创建时指定的所属 VPC 及子网，网卡从所属 VPC 子网中分配 IP 地址及网络配置；
- 安全组：弹性网卡绑定的安全组名称或 ID，若未指定则为空，可通过修改安全组绑定安全组；
- 创建时间：当前弹性网卡的创建时间；
- 状态：弹性网卡的当前状态，包括创建中、未绑定、绑定中、已绑定、解绑中、已删除等状态，状态流转如下图所示：



列表上的操作项是指对单块弹性网卡的操作，包括绑定、解绑、修改安全组及删除等，可通过搜索框对弹性网卡列表进行搜索和筛选，支持模糊搜索。

为方便租户对弹性网卡资源的统计及维护，平台支持下载当前用户所拥有的所有弹性网卡资源列表信息为 Excel 表格；同时支持对弹性网卡进行批量解绑和批量删除操作。

5.3 绑定网卡

绑定网卡是指将一块弹性网卡绑定至一台虚拟机，用于扩展虚拟机的网络接口。

- 一块弹性网卡仅支持绑定至一个虚拟机，仅支持绑定相同数据中心且处于关机或运行状态的虚拟机；
- **X86 架构虚拟机最多可绑定 6 块弹性网卡，ARM 架构虚拟机最多支持绑定 3 块弹性网卡；**

可通过弹性网卡资源列表操作项的“绑定”按钮，进行虚拟机绑定操作，如下图所示：

绑定网卡

! x86架构虚拟机最多绑定6块网卡，ARM架构虚拟机最多绑定3块网卡

网卡ID *	nic-Ea9g-a7GR
名称 *	2323
资源 *	host(vm-ETbN60nMR)

取消 确认



绑定时需选择需要绑定网卡的虚拟机，绑定过程中弹性网卡的状态为“绑定中”，待状态变更为“已绑定”即代表绑定成功，用户也可通过虚拟机的网络信息查看已绑定的网卡资源及信息。

5.4 解绑网卡

解绑网卡是指将弹性网卡从虚拟机上分离出来，并可重新绑定至其它虚拟机，仅支持解绑已绑定状态的弹性网卡资源。用户可通过弹性网卡列表或已绑定虚拟机详情网络页面进行弹性网卡的解绑操作，如下图所示：

解绑网卡

! 是否确认解绑网卡？解绑后的网卡可以进行释放或绑定到其它资源

! 被解绑的资源需处于运行状态

资源ID *	nic-MUiTlYnMg
名称 *	nic111
绑定资源 *	虚拟机 → vm-ETbN60nMR

取消 确认

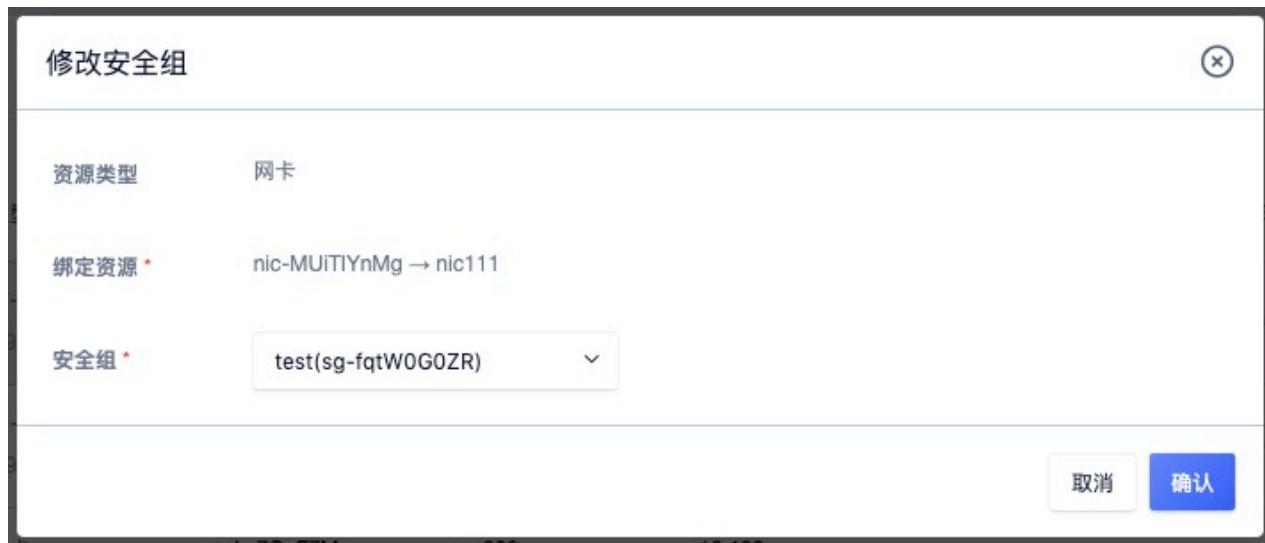


解绑时，虚拟机的状态必须处于关机或运行状态。解绑操作执行过程中，弹性网卡的状态会转换为“解绑中”，待网卡状态转换为“未绑定”，即代表解绑成功。解绑后弹性网卡的IP地址及安全组信息保持不变，可将网卡绑定至其它虚拟机。

5.5 修改安全组

支持在弹性网卡的视角修改弹性网卡的安全组，同时支持配置“暂不绑定”用于解绑安全组。

安全组作用的最小单位是网卡，若弹性网卡被绑定至虚拟机，弹性网卡的安全组策略仅对当前网卡的流量出入进行限制，不影响虚拟机默认网卡及其它弹性网卡的流量出入。用户可通过弹性网卡管理控制台列表上的“修改安全组”进行修改，如下图所示：



一块网卡仅支持绑定一个安全组，修改成功后用户可通过弹性网卡列表信息查看已修改的安全组信息。

仅当弹性网卡已绑定安全组时，才可通过“暂不绑定”解绑已绑定的安全组。

5.6 删除网卡

支持用户删除未绑定状态的弹性网卡资源，即仅支持删除“未绑定”状态的弹性网卡。删除弹性网卡后，会自动解绑与之关联的安全组。用户可通过弹性网卡列表进行弹性网卡的删除操作，支持批量删除。



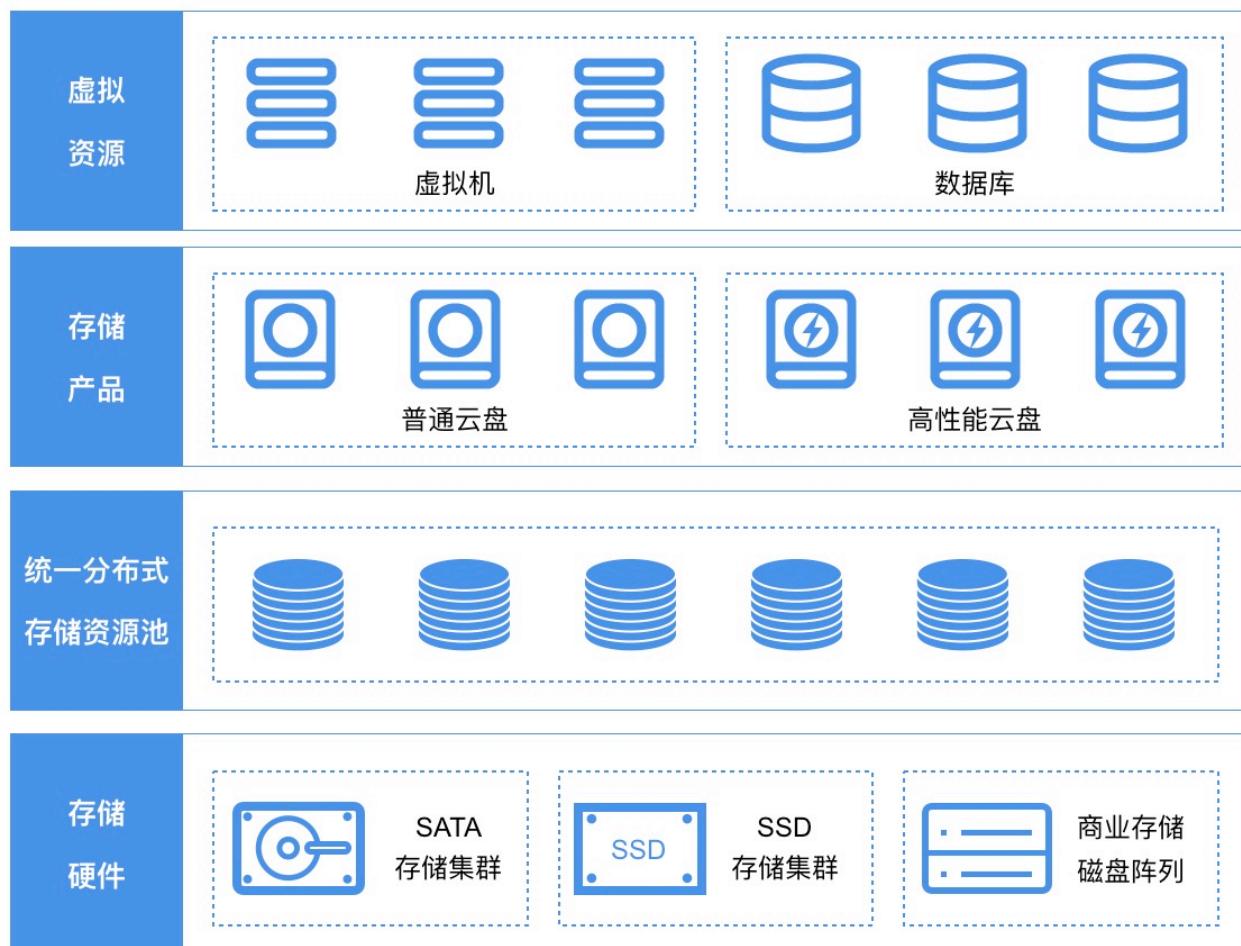
5.7 修改名称和备注

修改弹性网卡的名称和备注，在任何状态下均可进行操作。可通过弹性网卡列表页面每个网卡名称右侧的“编辑”按钮进行修改。

6 云硬盘

6.1 云硬盘概述

云硬盘是一种基于分布式存储系统为虚拟机和数据库服务提供持久化存储空间的块设备。具有独立的生命周期，支持随意绑定/解绑至多个虚拟机使用，并能够在存储空间不足时对云硬盘进行扩容，基于网络分布式访问，为云主机提供高安全、高可靠、高性能及可扩展的数据磁盘。



存储系统兼容并支持多种底层存储硬件，如通用服务器（计算存储超融合或独立通用存储服务器）和商业存储，并将底层存储硬件分别抽象不同类型集群的存储资源池，由分布式存储系统统一调度和管理。在实际应用场景中，可以将普通 SATA 接口的机械盘统一抽象为【SATA 存储集群】，将 SSD 全闪磁盘统一抽象为【SSD 存储集群】，分别由统一存储封装后提供平台用户使用。

如示意图所示，将 SATA 存储集群的资源封装为普通云盘，将 SSD 全闪存储集群的资源封装为高性能云盘。平台的虚拟机和数据库服务可根据需求挂载不同存储集群类型的磁盘，支持同时挂载多种集群类型的云硬盘。云平台管理员可通过管理员控制台自定义存储集群类型的别名，用于标识不同磁盘介质、不同品牌、不同性能或不同底层硬件的存储集群，如 EMC 存储集群、SSD 存储集群等。

通常 SSD 磁盘介质的云硬盘的性能与容量的大小成线性关系，容量越大提供的 IO 性能越高，如对 IO 性能有强烈需求，可考虑扩容 SSD 磁盘介质的云硬盘。

分布式存储底层数据通过条带化、PG 映射的方式进行数据存储，同时以多副本存储的方式保证数据安全，即写入至云平台存储集群的数据块会同时保存多份至不同服务器节点的磁盘。多副本存储的数据提供一致性保证，可能导致写入的多份数据因误操作或原如数据异常导致数据不准确；为保证数据的准确性，云平台提供硬盘快照能力，将云盘数据在某一时间点的数据文件及状态进行备份，在数据丢失或损坏时，可通过快照快速恢复数据，包括数据库数据、应用数据及文件目录数据等，可实现分钟级恢复。

云硬盘由统一存储从存储集群容量中分配，为平台虚拟资源提供块存储设备并共享整个分布式存储集群的容量及性能；同时通过块存储系统为用户提供云硬盘资源及全生命周期管理，包括云硬盘的创建、绑定、解绑、扩容、克隆、快照及删除等管理。

- 支持秒级创建云硬盘，最小支持 10G 的容量，步长为 10GB，管理员可自定义单块云硬盘的最大容量；
- 具有独立的生命周期，可自由绑定至任意虚拟机或数据库服务，解绑后可重新挂载至其它虚拟机；
- X86 架构的虚拟机最多支持绑定 6 块云硬盘，ARM 架构虚拟机最多支持绑定 3 块云硬盘；
- 支持在线和离线的方式扩容磁盘容量，磁盘存储容量扩容后需在虚拟机操作系统中进行文件系统及分区扩展；
- 为保证数据安全性及准确性，云硬盘仅支持磁盘扩容，不支持磁盘缩容。
- 支持云硬盘克隆，即将云硬盘内的数据复制成为一个新的云硬盘；
- 支持对云硬盘进行快照备份，包括虚拟机的系统盘快照及弹性云盘快照，并可从快照回滚数据至云硬盘，用于数据恢复和还原场景；
- 支持对全局及每一块云硬盘的 QoS 进行配置，可根据不同业务模式调整磁盘的性能，以平衡平台整体性能；
- 支持设置存储集群类型权限，即可以将部分存储资源设置为租户独享，满足需要独享底层存储资源的场景。

支持自动精简配置，在创建云硬盘时，仅呈现分配的逻辑虚拟容量。当用户向逻辑存储容量中写入数据时，按照存储容量分配策略从物理空间分配实际容量。如一个用户创建的云硬盘为 1TB 容量，存储系统会为用户分配并呈现 1TB 的逻辑卷，仅当用户在云硬盘中写入数据时，才会真正的分配物理磁盘容量。

6.2 创建云硬盘

在平台控制台上，用户可通过指定云硬盘的类型、容量及名称即可快速创建一块云硬盘，作为虚拟机的数据盘。创建前需确认账户的余额及硬盘配额充足。

1、通过控制台进入硬盘资源控制台，通过“创建硬盘”按钮，即可进入云硬盘创建向导页面，如下图所示，根据需求选择并配置硬盘类型、硬盘容量、硬盘名称等参数。

- 硬盘类型：即云硬盘类型，即存储集群类型，由平台管理员自定义，如 HDD 云盘或 SSD 高性能云盘；
- 硬盘容量：云硬盘分配的逻辑容量，默认最小 10GB，步长为 10GB，最大支持 8000GB，可由云平台管理员在控制台自定义容量规格；
- 云硬盘名称：需要创建的云硬盘名称；

2、选择购买数量和付费方式，如下图所示确认订单并点击“立即购买”进行云硬盘购买及创建操作：



- 购买数量：目前不支持批量创建，一次仅支持创建一块云硬盘；
- 付费方式：选择虚拟机的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式；
- 合计费用：用户选择创建云硬盘资源按照付费方式的费用展示；
- 立即购买：点击立即购买后，会返回云硬盘资源列表页，在列表页可查看云硬盘的创建过程，创建成功后，云硬盘状态显示为“未绑定”。

6.3 查看云硬盘

通过导航栏进入虚拟机控制台，切换至硬盘管理页面可查看当前账户下云硬盘资源的列表及相关详细信息，包括名称、资源 ID、集群类型、硬盘容量、绑定资源、计费方式、状态、创建时间、过期时间及操作项，如下图所示：

A screenshot of the 'Cloud Disk Management' page. At the top, there are tabs: 'Virtual Machine Management', 'Virtual Machine Template', 'Image Management', 'Network Card Management', 'Cloud Disk Management' (which is active), and 'Snapshot Management'. A yellow notification bar at the top says 'After binding the disk to the virtual machine, you need to manually mount it.' Below is a table listing four cloud disks. The columns are: Name, Resource ID, Cluster, Capacity, Bound Resource, Billing Method, Status, Creation Time, and Expiry Time. Each row includes a checkbox and three operation buttons: 'Bind', 'Unbind', and 'Delete'. The table footer shows page navigation and a '10 items per page' dropdown.

- 名称/ID：云硬盘的名称和全局唯一标识符；
- 集群类型：即云硬盘类型，即存储集群类型，由平台管理员自定义，如 HDD 云盘或 SSD 高性能云盘；
- 硬盘容量：云硬盘的容量，GB 为单位；
- 绑定资源：云硬盘已绑定的虚拟机名称和 ID，未指定则为空；
- 计费方式：云硬盘在创建时指定的计费方式，如按月、按年、按时；
- 创建时间/过期时间：云硬盘的创建时间和计费周期过期时间；
- 状态：云硬盘的当前状态，包括创建中、未绑定、绑定中、已绑定、解绑中、扩容中、被克隆中、

快照中及删除中等，其中被克隆中指当前硬盘正在克隆，快照中指当前硬盘正在快照备份中。

列表上的操作项是指对单块硬盘的操作，包括绑定、解绑、扩容、克隆、快照及删除等，可通过搜索框对硬盘列表进行搜索和筛选，支持模糊搜索。

为方便租户对硬盘资源的统计及维护，平台支持下载当前用户所拥有的所有硬盘资源列表信息为 Excel 表格；同时支持对硬盘进行批量解绑和批量删除操作。

6.4 绑定云硬盘

绑定是指将一块云硬盘挂载至一台虚拟机，为虚拟机添加数据磁盘，用于数据存储。

- 仅支持状态为“未绑定”的硬盘进行绑定，为保证数据安全，一块云硬盘同时仅支持绑定至一台虚拟机；
- 云硬盘具有地域（数据中心）属性，仅支持绑定相同数据中心且处于关机或运行状态的虚拟机；
- X86 架构虚拟机最多可绑定 6 块硬盘，ARM 架构虚拟机最多支持绑定 3 块硬盘；**

可通过硬盘管理资源列表操作项的“绑定”功能，进行硬盘绑定操作，如下图所示：



绑定时需选择绑定硬盘的虚拟机，绑定过程中硬盘的状态为“绑定中”，待状态变转换为“已绑定”即代表绑定成功。用户可通过虚拟机的硬盘信息查看已绑定云盘资源及信息，包括容量、挂载等，同时用户也可登录虚拟机操作系统中查看是否已识别到新的磁盘设备，如 Linux 操作系统用户可输入 `fdisk -l` 查看新增块设备的信息。

云硬盘绑定后，默认不进行格式化（如需）和系统挂载操作，需用户登录已挂载的虚拟机操作系统，根据需求对云盘进行格式化及挂载(`mount`)操作，有关操作系统内格式化及挂载数据盘，详见[格式化并挂载数据盘](#)。

6.5 解绑云硬盘

解绑云硬盘是指将云硬盘从虚拟机上分离出来，解绑的云硬盘可重新绑定至其它虚拟机，解绑后云硬盘的数据不会丢失，重新挂载新虚拟机后，可直接使用云硬盘上的数据。

仅支持解绑已绑定状态的硬盘资源，用户可通过硬盘列表或已绑定虚拟机详情硬盘页面进行硬盘的解绑操作，如下图所示：



解绑时，虚拟机的状态必须处于关机或运行状态。解绑操作执行过程中，云硬盘的状态会转换为“解绑中”；状态转换为“未绑定”，即代表解绑成功，可将硬盘重新绑定至其它虚拟机。

为保存数据完整性，解绑操作前建议暂停对当前硬盘所有文件系统的读写操作，并进入操作系统进行 `umount` 或脱机操作（Linux 系统需确认已 `umount` 硬盘所对应的文件系统；Windows 系统需确认至磁盘管理中进行磁盘下线操作），避免因强制解绑云硬盘导致文件系统损坏或丢失。

6.6 格式化并挂载数据盘

云硬盘成功挂载到虚拟机后，需要格式化后才可正常读写数据。本章节主要描述如何用一块新的云硬盘创建一个单分区的数据盘。Linux 的虚拟机和 Windows 的虚拟机使用云硬盘的方式不同，Linux 虚拟机格式化后，需要挂载到文件系统的一个目录中使用；Windows 的虚拟机首先需要初始化磁盘，进行分区并格式化后即可正常使用。

格式化和分区磁盘具有一定的风险，格式化后云硬盘中的数据将被清空，请慎重操作。

6.6.1 Linux 虚拟机

Linux 虚拟机挂载的云硬盘设备名是由系统默认分配的，从 `/dev/vdb` 递增排列，包括 `/dev/vdb` 到 `/dev/vdz`。本示例挂载一块 100GB 的云硬盘至 Linux 虚拟机，设备名为 `/dev/vdb`。具体操作步骤如下：

1. 创建云硬盘，并挂载至一台 Linux 的虚拟机，并通过 SSH 远程连接并登录虚拟机；
2. 使用 `fdisk -l` 命令查看虚拟机上的云硬盘，检测是否挂载成功，如下图所示挂载的数据盘为 100GB `/dev/vdb` 设备；

```
[root@localhost ~]# fdisk -l

Disk /dev/vda: 21.5 GB, 21474836480 bytes
255 heads, 63 sectors/track, 2610 cylinders
Units = cylinders of 16065 * 512 = 8225280 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00095e43

Device Boot      Start        End      Blocks   Id  System
/dev/vda1  *          1       2611    20970496   83  Linux

Disk /dev/vdb: 107.4 GB, 107374182400 bytes
16 heads, 63 sectors/track, 208050 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x00000000
```

3. 创建文件系统，使用 `mkfs.ext4 /dev/vdb` 命令进行格式化并新建一个文件系统，分区格式化可选择 `ext3`、`ext4` 等文件系统的格式，示例采用 `ext4` 格式；

```
[root@localhost ~]# mkfs.ext4 /dev/vdb
mke2fs 1.41.12 (17-May-2010)
文件系统标签=
操作系统:Linux
块大小=4096 (log=2)
分块大小=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
6553600 inodes, 26214400 blocks
1310720 blocks (5.00%) reserved for the super user
第一个数据块=0
Maximum filesystem blocks=4294967296
800 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
 32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
 4096000, 7962624, 11239424, 20480000, 23887872

正在写入inode表: 完成
Creating journal (32768 blocks): 完成
Writing superblocks and filesystem accounting information: 完成
```

4. 挂载数据盘，创建挂载点 `/data` 目录，使用 `mount /dev/vdb /data` 命令挂载新分区，并使用 `df -h` 验证云硬盘是否挂载成功；

```
[root@localhost ~]# mkdir /data
[root@localhost ~]# mount /dev/vdb /data
[root@localhost ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/vda1        20G  874M   18G   5% /
tmpfs           1.9G     0  1.9G   0% /dev/shm
/dev/vdb        99G  188M   94G   1% /data
```

5. 配置开机自动挂载，添加云硬盘的挂载信息至 `/etc/fstab`，如下：

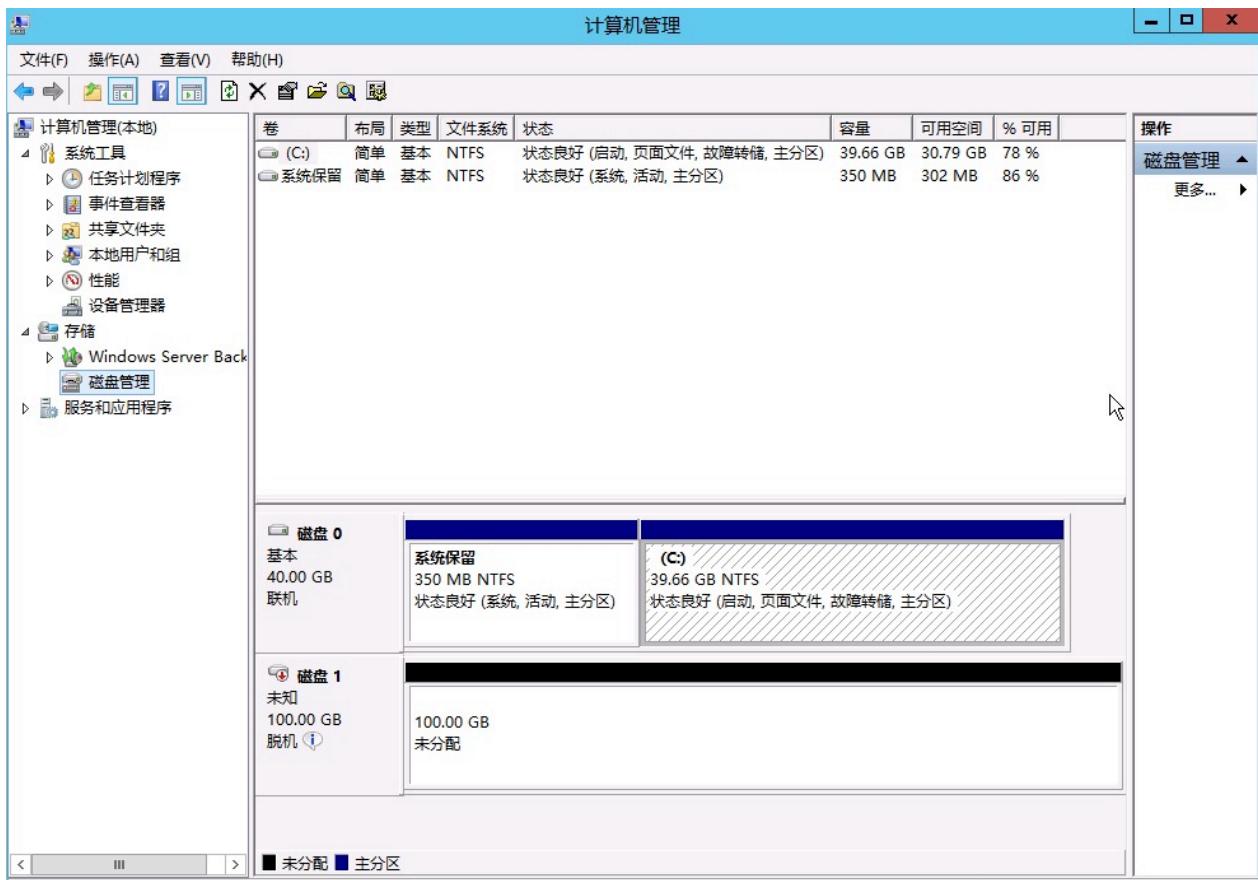
```
echo '/dev/vdb /data ext4 defaults 0 0' >> /etc/fstab
```

6. 挂载成功，即可正常使用云硬盘，若云硬盘在控制台被解绑，重新绑定至虚拟机后，需要重复执行 `mount /dev/vdb /data` 命令，或者需要重启虚拟机进行自动挂载；
7. 若云硬盘在控制台被解绑，重新绑定至其它 Linux 虚拟机后，需要按照第 4~5 步骤执行挂载操作。

6.6.2 windows 虚拟机

Windwos 虚拟机挂载云硬盘后，需要进行初始化及格式化分与等操作，才可正常使用。Windows 操作系统可进入“磁盘管理”界面进行分区与格式化操作，本章节以 Windows 2012 R2 为例进行格式化与分区操作，如下：

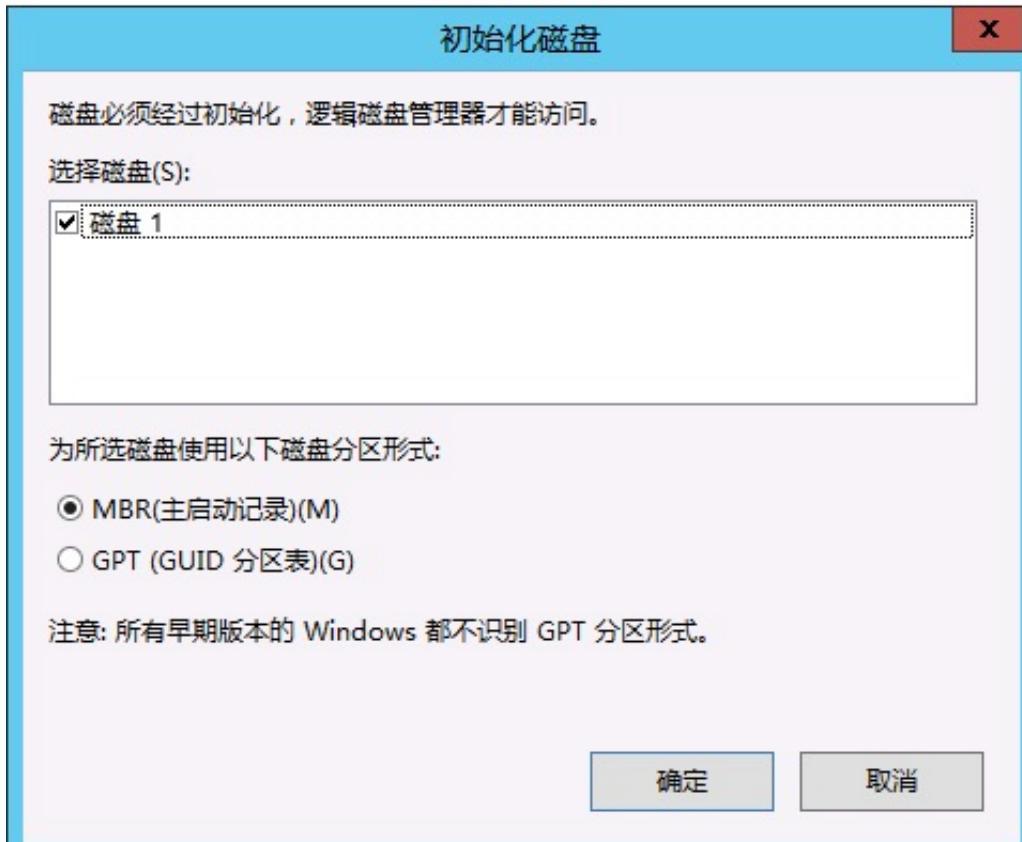
1. 创建云硬盘，并挂载至一台 windows 的虚拟机，通过 VNC 或远程桌面远程连接并登录虚拟机；
2. 点击【开始】—【管理工具】—【计算机管理】—【磁盘管理】，打开“磁盘管理”界面，查看已挂载的云硬盘，如下图所示的磁盘 1：



3. 在磁盘 1 上右键单击，选择【联机】，如下图所示：



4. 在磁盘 1 上右键单击，选择【初始化磁盘】，进入磁盘初始化向导界面，如下图所示：



5. 根据分区形式的不同，选择【GPT】或【MBR】，单击【确定】按钮；

- MBR 目前仍是最常用的分区形式，支持处理不大于 2 TB 的数据盘，仅支持分 4 个主区，如果您要将磁盘分成更多的区，需要将某个主区作为扩展区并在其中创建逻辑分区。
- GPT 是一种新的分区形式，早期版本的 Windows 不能识别这种分区形式。GPT 能处理的数据盘容量由操作系统和文件系统决定。在 Windows 操作系统里，GPT 最多可以支持 128 个主分区。

6. 磁盘分区，右键点击磁盘 1 右侧【未分配】的区域，选择【新建简单卷】，进入新建简单卷向导，如下图：



欢迎使用新建简单卷向导

此向导帮助你在磁盘上创建一个简单卷。

简单卷只能在单一磁盘上。

单击“下一步”继续。

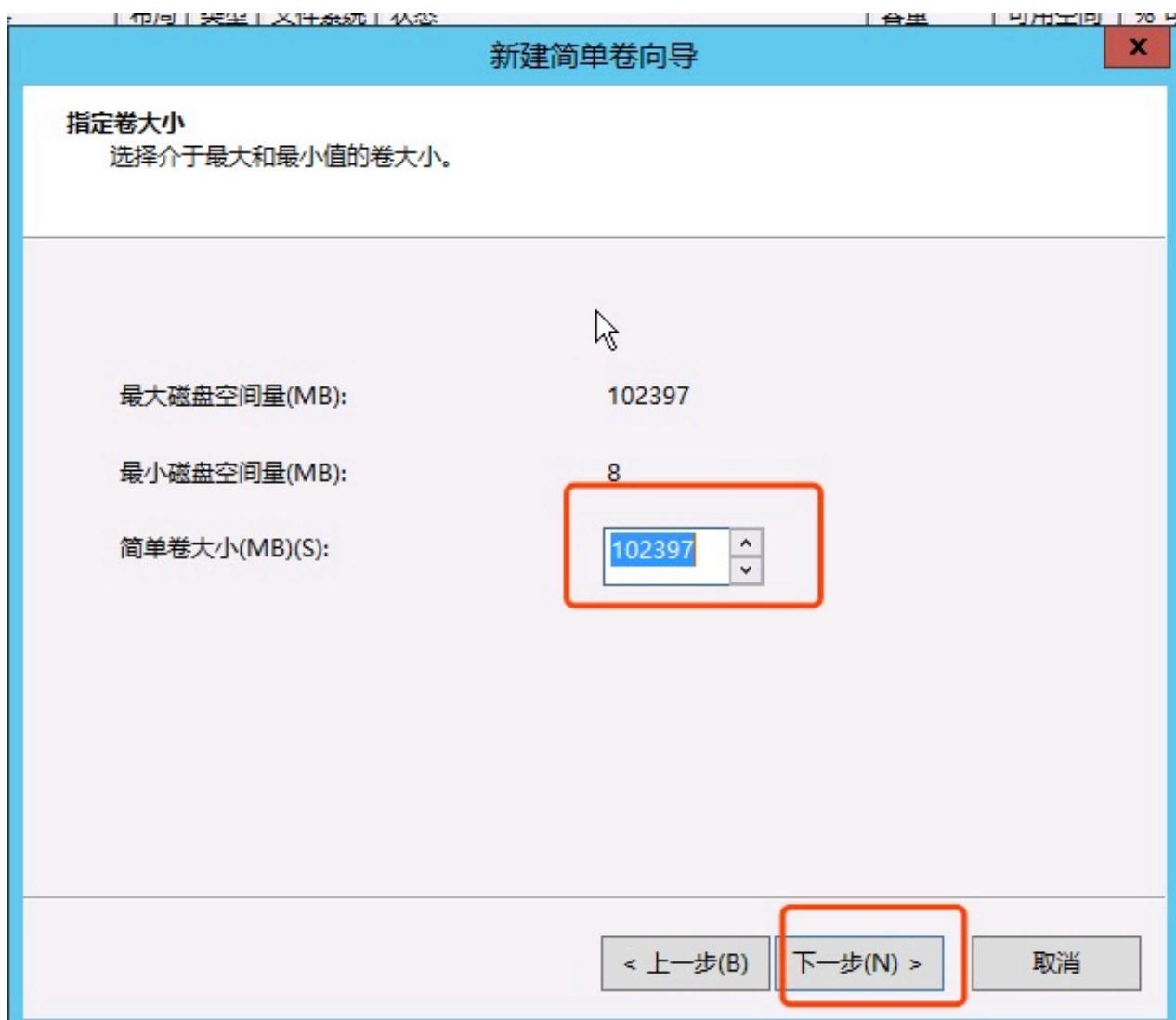


< 上一步(B)

下一步(N) >

取消

7. 点击下一步，输入分区所需的磁盘大小，若只需一个分区，使用默认值，单击下一步；



8. 分配驱动器号和路径，选择一个驱动器号（即盘符），如本示例中选择 D，单击下一步；

新建简单卷向导

X

分配驱动器号和路径

为了便于访问，可以给磁盘分区分配驱动器号或驱动器路径。

分配以下驱动器号(A):

D 

装入以下空白 NTFS 文件夹中(M):

浏览(R)...

不分配驱动器号或驱动器路径(D)

< 上一步(B)

下一步(N) >

取消

9. 格式化分区，选择格式化设置，包括文件系统、分配单元大小和卷标，确认是否 执行快速格式化 和 启用文件和文件夹压缩，这里使用默认设置，单击 下一步；



10. 点击完成，开始创建新简单卷，返回磁盘管理工具，磁盘 1 的状态良好，如下图所示：



6.7 扩容云硬盘

6.7.1 扩容云盘容量

平台支持用户扩容云硬盘的容量，适应于业务发生变化需扩容磁盘容量的场景。平台仅支持扩容磁盘容量，不支持磁盘容量的缩容。支持在线和离线两种硬盘扩容方式：

- 在线是指对运行状态虚拟机上绑定的云盘进行容量扩容；
- 离线是指对未绑定至虚拟机或关机状态虚拟机上绑定的云盘进行容量扩容。

磁盘容量扩容范围即当前硬盘类型的规格，默认为 10GB~8000GB，平台管理员可至平台管理后台全局配置中，进行磁盘规格配置。

扩容硬盘容量会对虚拟机费用产生影响，按小时付费的硬盘，扩容容量下个付费周期按新配置扣费；按年按月付费的硬盘，扩容容量即时生效，并按比例自动补差价。用户可点击云硬盘控制台操作中的“扩容”进行硬盘容量扩容操作，如下图所示：



如图所示，扩容硬盘需指定更改容量的大小，即硬盘需要扩容的容量。平台已展示当前硬盘的容量大小，由于不支持缩容，扩容时更改容量必须大于当前容量大小。

扩容过程中硬盘的状态转换为“升级中”，待状态转换为“已绑定”或“未绑定”状态即代表扩容成功。用户可通过硬盘列表或虚拟机硬盘信息查看硬盘的新容量；若硬盘已绑定虚拟机，用户也可登录虚拟机操作系统中查看绑定磁盘设备的容量，如 Linux 操作系统用户可输入 `fdisk -l` 查看新增块设备的信息。

由于 MBR 格式分区不支持大于 2TB 的磁盘容量。在扩容云硬盘时，若待扩容的硬盘采用 MBR 分区格式且需要扩容到 2TB 及以上容量时，建议重新创建并挂载一块硬盘，使用 GPT 分区方式并将数据拷贝至新硬盘中。

扩容操作仅对硬盘的块设备容量进行增加，并未对操作系统内文件系统和分区进行扩展。在容量扩容成功后，需进入挂载的虚拟机操作系统进行分区扩展或新建分区操作，详见【6.7.2 磁盘分区扩容】。

6.7.2 磁盘分区扩容

扩容硬盘容量后，需要进入操作系统对磁盘分区进行扩容，即需对文件系统进行扩容，才可使操作系统正常使用已扩容的磁盘容量。针对不同的操作系统分区扩容操作有所不同，如 Linux 通常通过 `fdisk` 或 `parted` 工具；Windows 通常使用自带的磁盘管理工具进行扩容操作。根据不同磁盘扩容场景，分区扩容大致分为如下场景：

- 裸磁盘扩容 (Linux)
- 单分区磁盘扩容 (Linux)
- 单分区磁盘扩容 (Windows)
- 多分区磁盘扩容 (Linux)
- 多分区磁盘扩容 (Windows)
- 2TB 硬盘分区扩容 (Linux)
- 2TB 硬盘分区扩容 (Windows)

6.7.2.1 裸磁盘扩容 (Linux)

裸磁盘是指未进行分区的云硬盘，即创建的云硬盘挂至主机后，直接对磁盘进行格式化进行使用，用户可通过对硬盘扩容容量后，进入操作系统对裸磁盘进行扩容操作。

裸磁盘直接格式化使用，仅适用于 Linux 系统，Windows 必须进行格式化并分区才可进行挂载使用。

本示例以 CentOS 6.5 操作系统（内核版本为 2.6.32-431.el6.x86_64）为示例环境版本，云硬盘大小为 40GB，扩容至 50GB，挂载点为 `/dev/vdb`，实际环境中需根据实际情况进行操作。

- 查看当前磁盘的信息，包括挂载点、文件系统类型及分区情况。

```
[root@localhost data]# df -Th
Filesystem      Type 1600 Sizes, Used Avail Use% Mounted on
/dev/vda1        ext4  40G  822M  37G   3% /home super user
tmpfs           tmpfs 935M    0  935M  0% /dev/shm
/dev/vdb        ext4  40G  176M  38G   1% /data
[root@localhost data]# fdisk -l
Disk /dev/vdb: 40.0 GB, 40000000000 bytes
  16 heads, 63 sectors/track, 104025 cylinders
  Units = cylinders of 1008 * 512 = 516096 bytes
  Sector size (logical/physical): 512 bytes / 512 bytes
  I/O size (minimum/optimal): 512 bytes / 512 bytes
  Disk identifier: 0x00000000
[root@localhost data]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda 252:0    0 40G  0 disk
└─vda1 252:1  0 40G  0 part /11239424, 20480000, 23887872
vdb 252:16   0 40G  0 disk /data
[root@localhost data]#
```

注：结果显示 vdb 磁盘为 ext4 分区且磁盘下无分区，为裸磁盘，可按照本文档所述方案扩容；若 vdb 下有分区，需参考单分区扩容或多分区扩容章节内容。

- 通过控制台或 API 对硬盘进行容量扩容操作，并在操作系统中查看磁盘的容量，如下图所示，扩容至50GB；

```
[root@localhost data]# fdisk -l /dev/vdb
Disk /dev/vdb: 53.7 GB, 53687091200 bytes
  16 heads, 63 sectors/track, 104025 cylinders
  Units = cylinders of 1008 * 512 = 516096 bytes
  Sector size (logical/physical): 512 bytes / 512 bytes
  I/O size (minimum/optimal): 512 bytes / 512 bytes
  Disk identifier: 0x00000000
通过云盘控制台扩容云硬盘。
[root@localhost data]#
```

- umount 磁盘，进行文件系统扩容操作，不同的文件系统扩容命令操作不同，本文分别以 ext4 及 xfs 文件系统为例进行扩容操作；
- ext4 文件系统扩容，执行 `resize2fs /dev/vdb` 进行系统磁盘扩容操作，最后重新 mount 挂载磁盘即可；

```
[root@localhost /]# resize2fs /dev/vdb
resize2fs 1.41.12 (17-May-2010)
Resizing the filesystem on /dev/vdb to 13107200 (4k) blocks.
The filesystem on /dev/vdb is now 13107200 blocks long.
```

如上图所示，扩容并挂载磁盘后，`/data` 目录所显示的容量为扩容后的 50GB。

```
[root@localhost /]# df -Th
Filesystem      Type   Size  Used Avail Use% Mounted on
/dev/vda1        ext4   40G  822M  37G  3% /dev/vdb
tmpfs           tmpfs  935M    0  935M  0% /dev/shm
/dev/vdb         ext4   50G  180M  47G  1% /data
[root@localhost /]#
```

如上图所示，扩容并挂载磁盘后，`/data` 目录所显示的容量为扩容后的 50GB。

- 若磁盘为 xfs 文件系统，则需要执行 `xfs_growfs /data/` 命令进行磁盘扩容操作

注意：xfs 文件系统的磁盘扩容，需要在操作系统中将磁盘 `mount` 后操作。

6.7.2.2 单分区扩容（Linux）

单分区磁盘是指云盘在扩容之前已被挂载过虚拟机且只划分过 1 个分区，用户可通过对硬盘扩容容量后，进入操作系统对单分区磁盘进行分区扩容操作。单分区扩容在 Linux 及 Windows 操作系统上的操作不同，本章节为 Linux 单分区扩容操作指南。

本示例以 CentOS 6.5 操作系统（内核版本为 2.6.32-431.el6.x86_64）为示例环境版本，云硬盘大小为 10G 单分区，扩容至 20GB，挂载点为 `/dev/vdb1`，实际环境中需根据实际情况进行操作。若磁盘上划分多个分区，可参考多分区扩容章节。

本操作示例默认磁盘容量小于 2TB，若磁盘容量大于 2TB 请参考《2TiB磁盘分区扩容（Linux）》章节。

- 通过 `lsblk` 查看当前磁盘的信息，包括挂载点、文件系统类型及分区情况；

```
[root@localhost mnt]# lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda    252:0   0 40G  0 disk
└─vda1  252:1   0 40G  0 part /
vdb    252:16  0 10G  0 disk
└─vdb1  252:17  0 10G  0 part /mnt
[root@localhost mnt]# df -Th
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/vda1        ext4  40G  822M  37G  3% /
tmpfs           tmpfs  935M    0  935M  0% /dev/shm
/dev/vdb1        ext4  9.9G 217M  9.2G  3% /mnt
[root@localhost mnt]#
```

注：结果显示 vdb 下只有一个 10GB 的分区，分区格式为 ext4，挂载至 /mnt 目录。

- 通过控制台或 API 对硬盘进行容量扩容操作，并在操作系统中通过 fdisk 或 lsblk 查看扩容后的磁盘容量；
- 在操作系统中 umount 磁盘，使用 `fdisk /dev/vdb` 命令删除原来的分区并创建新分区；

```

[root@localhost /]# fdisk /dev/vdb
      Disk /dev/vdb: 9.9G, 217M, 9.2G, 3% /mnt
      [root@localhost mnt]#
      WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
              switch off the mode (command 'c') and change display units to
              sectors (command 'u'). 对硬盘进行容量升级操作，并在操作系统中通过fdisk或lsblk查
      • 在操作系统中 umount 磁盘，使用 fdisk /dev/vdb 命令删除原来的分区并创建新
Command (m for help): d
Selected partition 1

Command (m for help): n
      WARNING: DOS-compatible mode is deprecated. It's strongly
              switch off the mode (command 'c') and change di
              sectors (command 'u').
      Command action
          e   extended
          p   primary partition (1-4)
p
      Selected partition 1
Partition number (1-4): 1
First cylinder (1-41610, default 1): n
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-41610, default 41610):
Using default value 41610
      primary partition (1-4)
      17:03:05
      p
Command (m for help): p
      Partition number (1-4): 1
      First cylinder (1-20805, default 1):
Disk /dev/vdb: 21.5 GB, 21474836480 bytes
      16 heads, 63 sectors/track, 41610 cylinders
      Units = cylinders of 1008 * 512 = 516096 bytes
      Sector size (logical/physical): 512 bytes / 512 bytes
      I/O size (minimum/optimal): 512 bytes / 512 bytes
      Disk identifier: 0xd62755b4
      Disk /dev/vdb: 10.7 GB, 10737418240 bytes
      16 heads, 63 sectors/track, 20805 cylinders
      Units = cylinders of 1008 * 512 = 516096 bytes
      Sector size (logical/physical): 512 bytes / 512 bytes
      I/O size (minimum/optimal): 512 bytes / 512 bytes
      Disk identifier: 0xd62755b4
      Device Boot      Start      End      Blocks   Id  System
      /dev/vdb1        1     41610    20971408+  83  Linux
      Command (m for help): wq
      The partition table has been altered!
      Calling ioctl() to re-read partition table.
      Syncing disks.
[root@localhost /]# fdisk -l
      Disk /dev/vdb: 21.5 GB, 21474836480 bytes
      16 heads, 63 sectors/track, 41610 cylinders
      Units = cylinders of 1008 * 512 = 516096 bytes
      Sector size (logical/physical): 512 bytes / 512 bytes
      I/O size (minimum/optimal): 512 bytes / 512 bytes
      Disk identifier: 0xd62755b4
      Device Boot      Start      End      Blocks   Id  System
      /dev/vdb1        1     41610    20971408+  83  Linux

```

注：删除分区不会造成磁盘内数据丢失。

- 检查文件系统并进行文件系统扩容操作，不同的文件系统扩容命令操作不同，本文分别以 ext4 及 xfs 文件系统为例进行扩容操作；
- ext4 文件系统扩容，执行 `e2fsck -f /dev/vdb1` 和 `resize2fs /dev/vdb1` 进行检查和扩容操作；

```
[root@localhost /]# e2fsck -f /dev/vdb1
e2fsck 1.41.12 (17-May-2010)
第一步：检查 inode, 块, 和大小
第二步：检查目录结构
第三步：检查目录连接性
Pass 4: Checking reference counts
第5步：检查簇概要信息
/dev/vdb1: 168/655360 files (0.6% non-contiguous), 96482/2621422 blocks
[root@localhost /]# resize2fs /dev/vdb1
resize2fs 1.41.12 (17-May-2010)
Resizing the filesystem on /dev/vdb1 to 5242852 (4k) blocks.
The filesystem on /dev/vdb1 is now 5242852 blocks long.
操作：
[root@localhost /]# mount /dev/vdb1 /mnt/
[root@localhost /]# df -Th
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/vda1        ext4   40G  894M  37G  3% /
tmpfs           tmpfs  935M    0  935M  0% /dev/shm
/dev/vdb1        ext4   20G  222M  19G  2% /mnt
[root@localhost /]#
```

如上图所示，扩容分区扩容成功后，重新 mount 分区，并查看分区大小及相关信息。

- 若磁盘为 xfs 文件系统，则先执行 `xfs_repair /dev/vdb1` 检查文件系统，如下图所示：

```
[root@10-10-33-83 ~]# lsblk
NAME  MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vdb   253:16   0  40G  0 disk
└─vdb1 253:17   0  20G  0 part
vda   253:0    0  20G  0 disk
└─vda1 253:1    0  20G  0 part /
[root@10-10-33-83 ~]# xfs_repair /dev/vdb1
Phase 1 - find and verify superblock...
Phase 2 - using internal log
  - zero log...
  - scan filesystem freespace and inode maps...
  - found root inode chunk
Phase 3 - for each AG...
  - scan and clear agi unlinked lists...
  - process known inodes and perform inode discovery...
  - agno = 0
  - agno = 1
  - agno = 2
  - agno = 3
  - process newly discovered inodes...
Phase 4 - check for duplicate blocks...
  - setting up duplicate extent list...
  - check for inodes claiming duplicate blocks...
  - agno = 0
  - agno = 1
  - agno = 2
  - agno = 3
Phase 5 - rebuild AG headers and trees...
  - reset superblock...
Phase 6 - check inode connectivity...
  - resetting contents of realtime bitmap and summary inodes
  - traversing filesystem ...
  - traversal finished ...
  - moving disconnected inodes to lost+found ...
Phase 7 - verify and correct link counts...
done
```

最后使用 `mount` 重新挂载磁盘，并执行 `xfs_growfs /mnt` 对磁盘分区进行扩容操作。

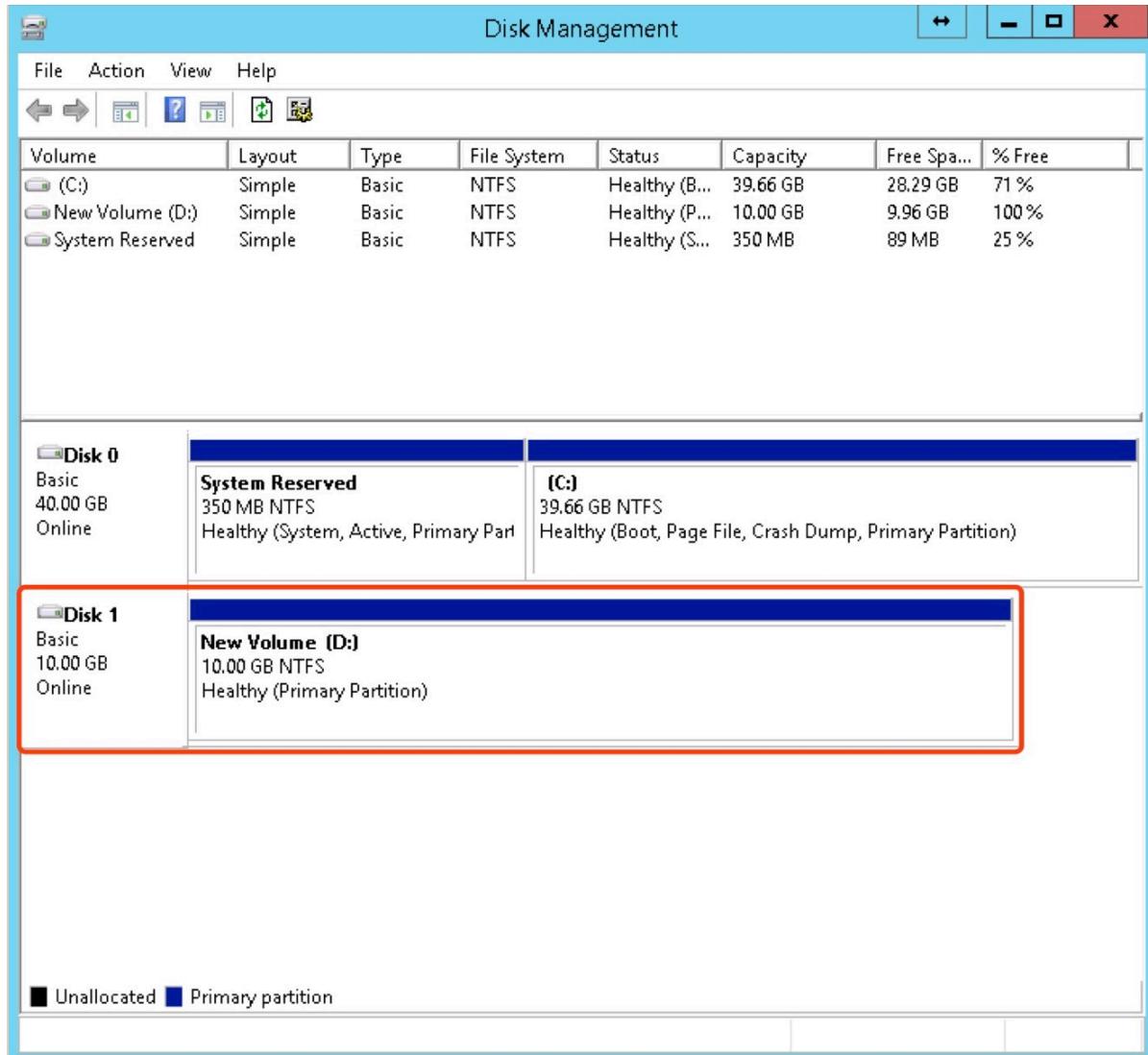
6.7.2.3 单分区扩容 (Windows)

单分区磁盘是指云盘在扩容之前已被挂载过虚拟机且只划分过1个分区，用户可通过对硬盘扩容容量后，进入操作系统对单分区磁盘进行分区扩容操作。单分区扩容在Linux及Windows操作系统上的操作不同，本章节为windows单分区扩容操作指南。

本示例以Windows Server 2012R2操作系统为示例环境版本，云硬盘大小为10GB，扩容至20GB，挂载点为Disk1，实际环境中需根据实际情况进行操作。具体操作如下：

本操作示例默认磁盘容量小于2TB，若磁盘容量大于2TB请参考《2TiB磁盘分区扩容(Windows)》章节。

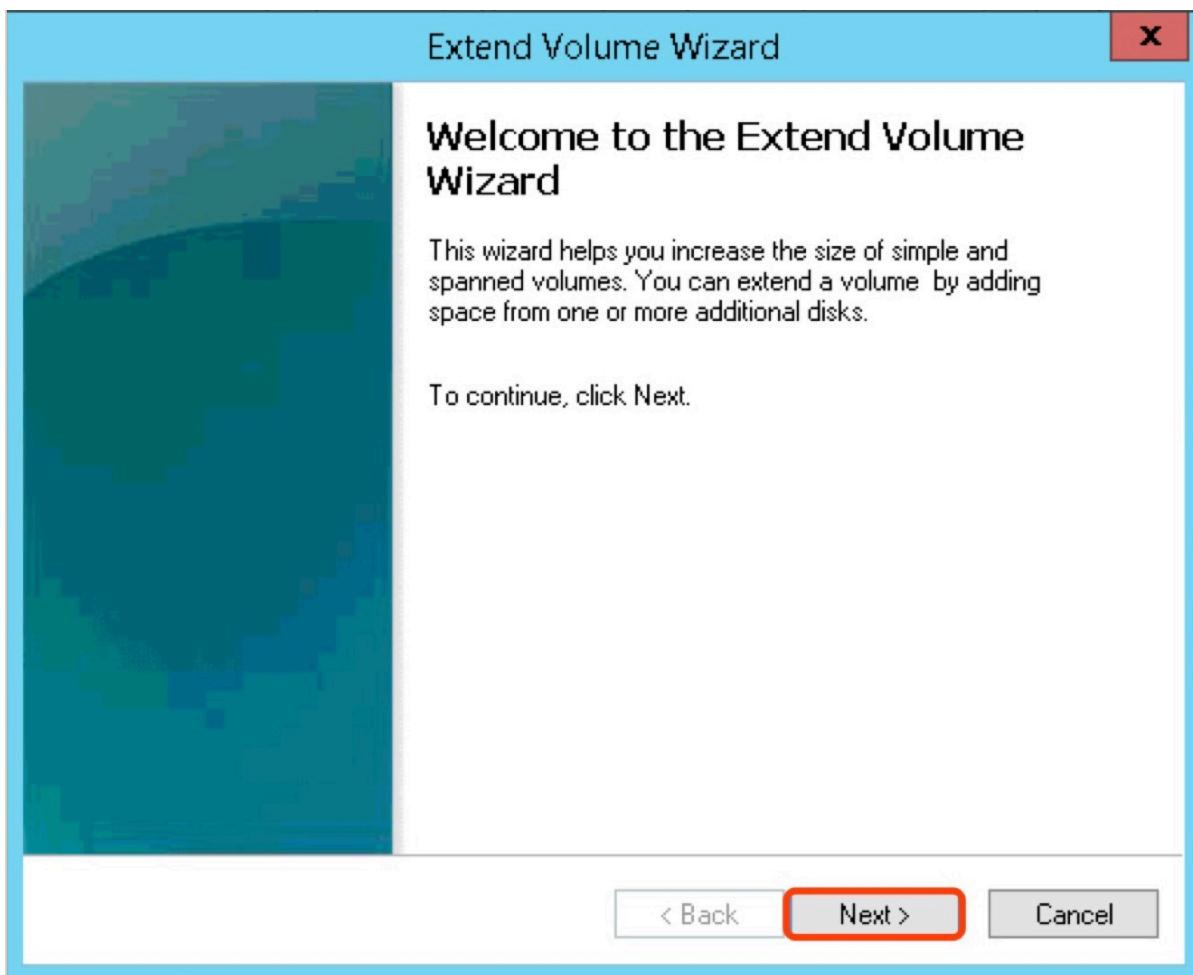
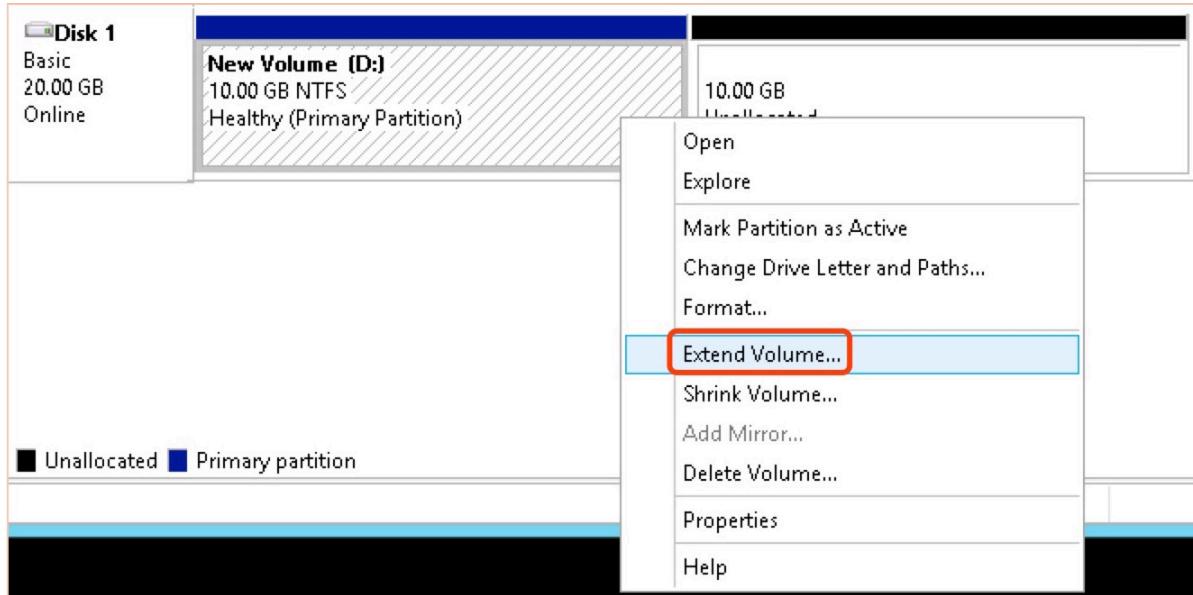
- 查看当前磁盘的分区及挂载信息，确认磁盘是当前需要扩容的磁盘，如下图所示：

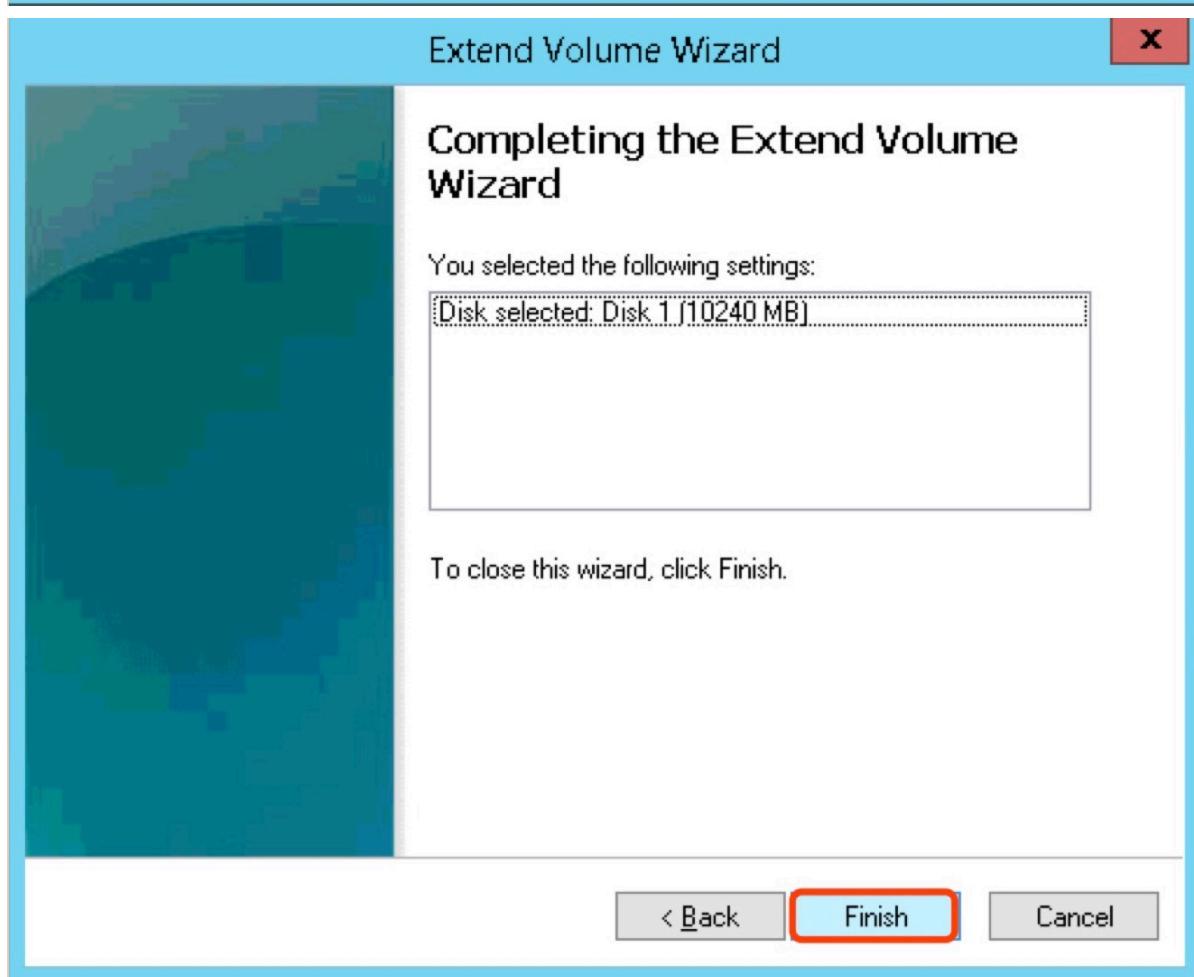
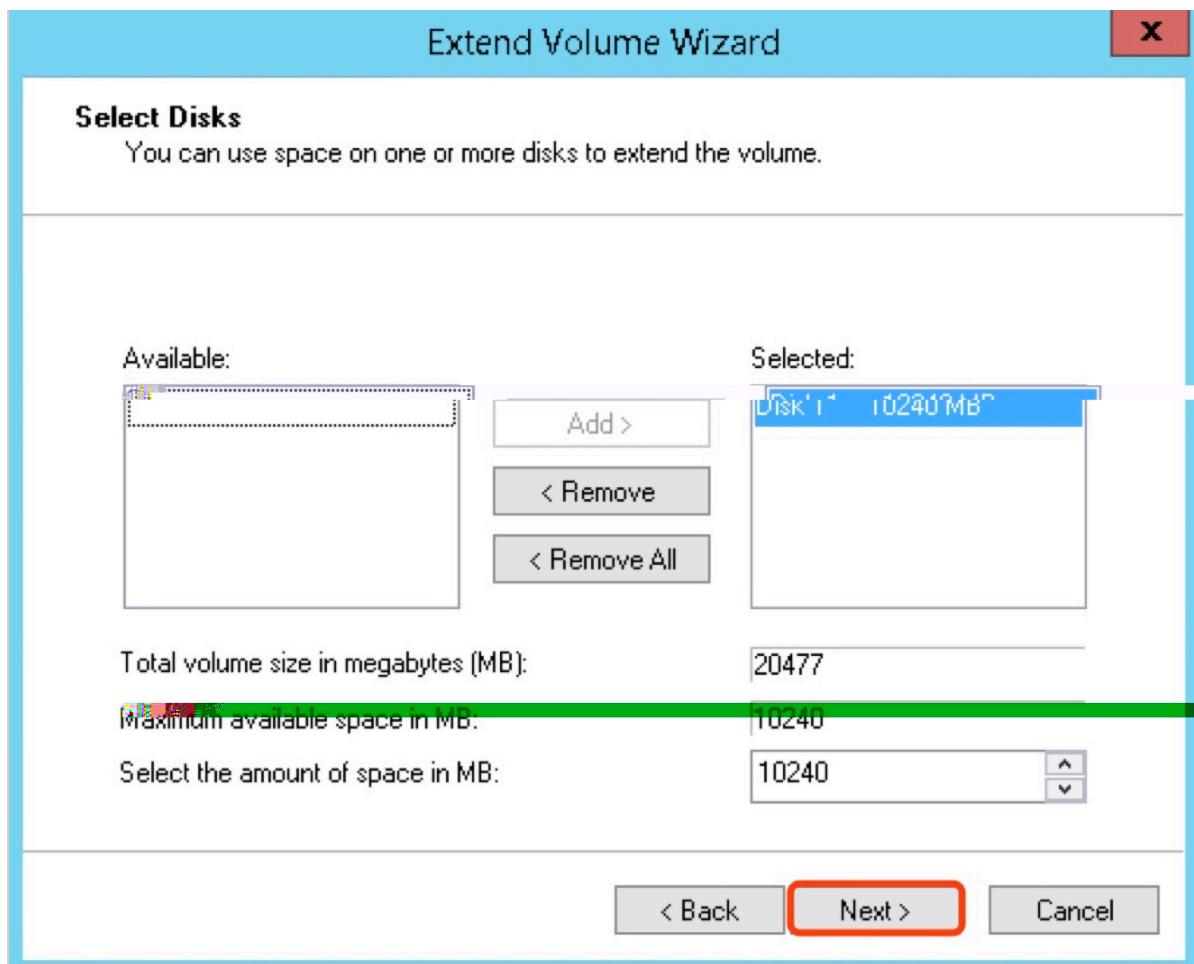


- 在操作系统中对磁盘进行脱机操作，并通过控制台及API对当前磁盘进行容量扩容操作，并通过操作系统磁盘管理工具查看扩容后的磁盘大小，如下图所示：



- 右键单击新分区D空白处，选择扩展卷(Extend Volume)，并在弹出的对话框中，对磁盘分区进行扩展操作，如以下图示：





- 分区扩展成功后，查看扩容后分区信息，如下图所示：



6.7.2.4 多分区扩容 (Linux)

多分区磁盘是指云盘在扩容之前已被挂载过虚拟机且划分过多个分区，用户可通过对硬盘扩容容量后，进入操作系统对多分区磁盘进行分区扩容操作。由于新扩容的空间是附加在虚拟云盘的末端，对于多分区的场景，只支持对排在最后的分区进行扩容操作。

多分区扩容在 Linux 及 Windows 操作系统上的操作不同，本章节为 Linux 多分区扩容操作指南。本示例以 CentOS 6.5 操作系统为示例环境版本，云硬盘大小为 20G，两个分区分别 10GB，挂载点分别为 `/dev/vdb1` 和 `/dev/vdb2`，扩容至 30GB，即将最后一个分区扩容为 20GB，实际环境中需根据实际情况进行操作。

本操作示例默认磁盘容量小于 2TB，若磁盘容量大于 2TB 请参考《2TiB磁盘分区扩容 (Linux)》章节。

- 通过 `lsblk` 及 `df` 查看当前磁盘的信息，包括挂载点、文件系统类型及分区情况；

```
[root@localhost ~]# df -Th
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/vda1        ext4  40G  823M  37G  3% /          SSH无密登录
tmpfs           tmpfs  935M    0  935M  0% /dev/shm
/dev/vdb1        ext4  9.9G  151M  9.2G  2% /mnt
/dev/vdb2        ext4  9.9G  151M  9.2G  2% /data
[root@localhost ~]# lsblk
NAME MAJ:MIN RM SIZE TYPE MOUNTPOINT
vda 252:0 0 40G disk
└─vda1 252:1 0 10G part /
vdb 252:16 0 20G disk
└─vdb1 252:17 0 10G part /mnt
└─vdb2 252:18 0 10G part /data
[root@localhost ~]#
```

结果显示 vdb 下有两个 10GB 的分区（vdb1 和 vdb2），且分别挂载至 `/mnt` 及 `/data` 目录下，扩容操作仅可对 vdb2 分区进行扩容操作，即将 vdb2 扩容为 20GB。

- 通过控制台或 API 对硬盘进行容量扩容操作，并在操作系统中通过 `fdisk` 或 `lsblk` 查看扩容后的磁盘容量；
- 在操作系统中 `umount` 磁盘，使用 `fdisk /dev/vdb` 命令删除最后一个分区（vdb2）并创建新分区；

```
[root@localhost ~]# fdisk /dev/vdb
WARNING: DOS-compatible mode is deprecated. It's strongly recommended to
switch off the mode (command 'c') and change display units to
sectors (command 'u').
Command (m for help): p
Disk /dev/vdb: 32.2 GB, 32212254720 bytes
16 heads, 63 sectors/track, 62415 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x1b0cbdbb

      Device Boot      Start        End      Blocks   Id  System
/dev/vdb1            1      20805    10485688+  83  Linux
/dev/vdb2        20806      41610    10485720  83  Linux

Command (m for help): d
Partition number (1-4): 2
[Command (m for help): n
Command action      2020-04-23
      e      extended      host
      p      primary partition (1-4)
p
Partition number (1-4): 2
[First cylinder (20806-62415, default 20806):
Using default value 20806
[Last cylinder, +cylinders or +size[K,M,G] (20806-62415, default 62415):
Using default value 62415

[Command (m for help): p
Disk /dev/vdb: 32.2 GB, 32212254720 bytes
16 heads, 63 sectors/track, 62415 cylinders
Units = cylinders of 1008 * 512 = 516096 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk identifier: 0x1b0cbdbb

      Device Boot      Start        End      Blocks   Id  System
/dev/vdb1            1      20805    10485688+  83  Linux
/dev/vdb2        20806      62415    20971440  83  Linux

Command (m for help): wq
The partition table has been altered!
```

注：删除分区不会造成磁盘内数据丢失，以上示例为删除 vdb2，即磁盘的最后一个分区。

- 检查文件系统并进行文件系统扩容操作，不同的文件系统扩容命令操作不同，本文分别以 ext4 及 xfs 文件系统为例进行扩容操作；
- ext4 文件系统扩容，执行 `e2fsck -f /dev/vdb2` 和 `resize2fs /dev/vdb2` 进行检查和扩容操作，扩容分区扩容成功后，重新 mount 分区，并查看分区大小及相关信息；

- 若磁盘为 xfs 文件系统，则先执行 `xfs_repair /dev/vdb2` 检查文件系统后，使用 `mount` 将磁盘重新挂载至 `/data` 目录，最后使用 `xfs_growfs /data` 命令对 vdb2 磁盘分区进行扩容操作。

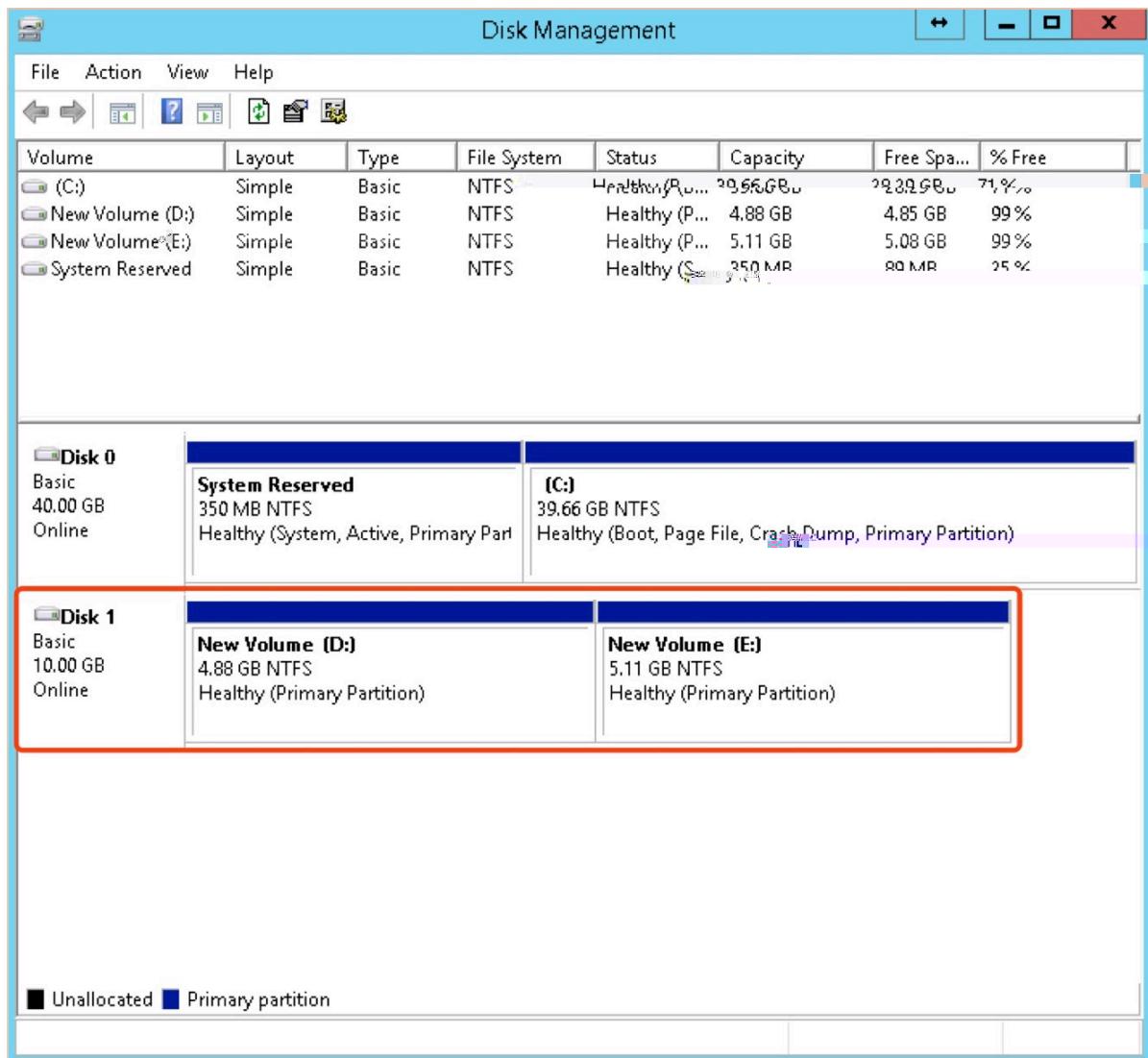
6.7.2.5 多分区扩容 (Windows)

多分区磁盘是指云盘在扩容之前已被挂载过虚拟机且划分过多个分区，用户可通过对硬盘扩容容量后，进入操作系统对多分区磁盘进行分区扩容操作。由于新扩容的空间是附加在虚拟云盘的末端，对于多分区的场景，只支持对排在最后的分区进行扩容操作。

多分区扩容在 Linux 及 Windows 操作系统上的操作不同，本章节为 Windows 多分区扩容操作指南。本示例以 Windows Server 2012R2 操作系统为示例环境版本，云硬盘大小为 10G，两个分区分别 5GB，挂载点 Disk1，扩容至 20GB，即将最后一个分区扩容为 15GB，实际环境中需根据实际情况进行操作。

本操作示例默认磁盘容量小于 2TB，若磁盘容量大于 2TB 请参考《2TiB磁盘分区扩容 (Linux)》章节。

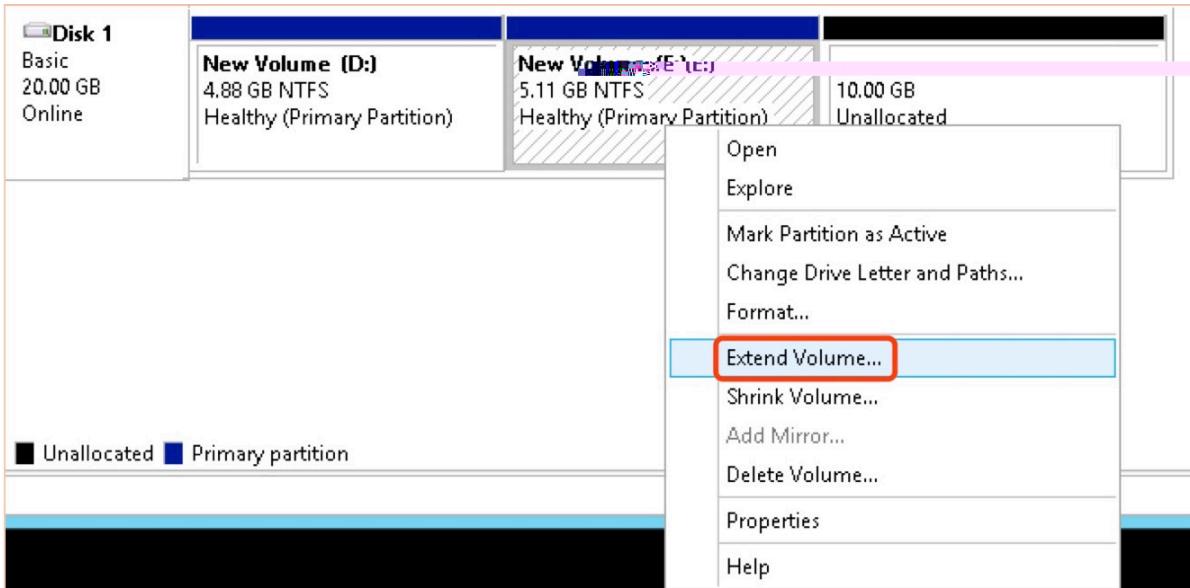
- 查看当前磁盘的分区及挂载信息，确认磁盘是当前需要扩容的磁盘，如下图所示：



- 在操作系统中对磁盘进行脱机操作，并通过控制台及 API 对当前磁盘进行容量扩容操作，并通过操作系统磁盘管理工具查看扩容后的磁盘大小，如下图所示：

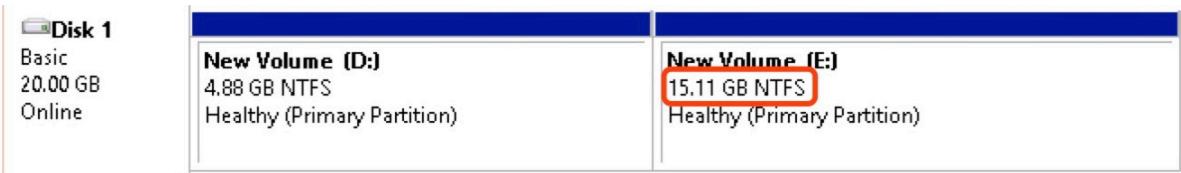
Disk 1 Basic 20.00 GB Online	New Volume (D:) 4.88 GB NTFS Healthy (Primary Partition)	New Volume (E:) 5.11 GB NTFS Healthy (Primary Partition)	10.00 GB Unallocated
--	---	---	-------------------------

- 右键点击新分区 E (最后一个分区) 空白处, 选择扩展卷 (Extend Volume) , 对分区进行扩容;



通过点击下一步及相关配置, 完成新分区的容量扩容;

- 完成扩容后, 查看扩容后分区情况, 如下图所示:



结果显示, E 盘被扩展为 15GB , 即在原来的基础之上扩容 10GB 的容量。

6.7.2.6 2TB 磁盘分区扩容 (Linux)

当一块磁盘的容量大于 2TB 时, 在 linux 下无法通过 fdisk 工具命令对对进行分区, 需通过 parted 命令进行分区及扩容操作。2TB 以上磁盘在 Linux 及 Windows 操作系统上的操作不同, 本章节为 Linux 下大于 2TB 磁盘扩容操作指南。

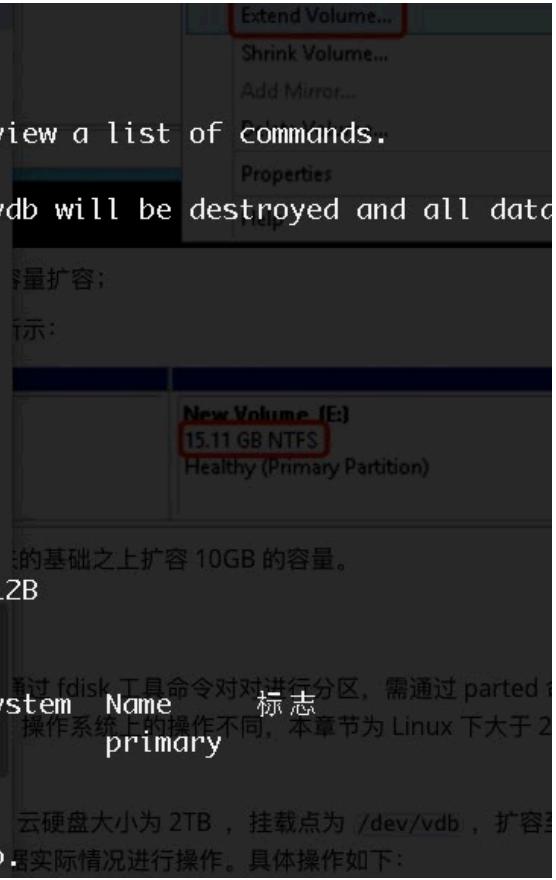
本示例以 CentOS 6.5 操作系统为示例环境版本, 云硬盘大小为 2TB , 挂载点为 `/dev/vdb` , 扩容至 2.1TB , 即将云盘及分区扩容为 100GB , 实际环境中需根据实际情况进行操作。具体操作如下:

- (1) 若磁盘为新创建, 则需要通过 parted 工具先进行分区, 具体操作如下图:

- 通过输入 `parted /dev/vdb` 进行分区操作, 其中 `mklabel gpt` 是将磁盘分区设置为 GPT 格式;

```
[root@localhost ~]# parted /dev/vdb
GNU Parted 2.1
使用 /dev/vdb
Welcome to GNU Parted! Type 'help' to view a list of commands.
(parted) mklabel gpt
警告: The existing disk label on /dev/vdb will be destroyed and all data
will be lost.
Do you want to continue? on
是/Yes/否/No? yes
(parted) mkpart primary 1 100%
(parted) align-check optimal 1
1 aligned
(parted) print
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 2147GB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Number  Start   End     Size    File system  Name
 1      1049kB 2147GB  2147GB  ntfs        New Volume (E:)

(parted) quit
信息: You may need to update /etc/fstab. 请根据实际情况进行操作。具体操作如下:
```



- 分区后，可通过 lsblk 查看磁盘分区是否成功，并通过 mkfs.ext4 /dev/vdb1 将分区进行格式化并进行挂载才可正常使用，如下图所示：

```
[root@localhost ~]# lsblk
NAME   MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda    252:0    0 40G  0 disk
└─vda1 252:1    0 40G  0 part /
vdb    252:16   0  2T  0 disk
└─vdb1 252:17   0  2T  0 part
[root@localhost ~]# mkfs.ext4 /dev/vdb1
mke2fs 1.41.12 (17-May-2010)
文件系统标签=
操作系统 :Linux
块大小=4096 (log=2)
分块大小=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
131072000 inodes, 524287488 blocks
26214374 blocks (5.00%) reserved for the super user
第一个数据块=0
Maximum filesystem blocks=4294967296
16000 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
      32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
     4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
    102400000, 214990848, 512000000

正在写入 inode表：完成
Creating journal (32768 blocks): 完成
Writing superblocks and filesystem accounting information: 完成

This filesystem will be automatically checked every 21 mounts or
180 days, whichever comes first. Use tune2fs -c or -i to override.
[root@localhost ~]#
```

- 格式化成功后，通过挂载并查看磁盘的信息，如下图所示 `/dev/vdb1` 被挂载至 `/mnt`，容量为 2TB。

```
[root@localhost ~]# mount /dev/vdb1 /mnt/
[root@localhost ~]# df -Th
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/vda1        ext4  40G   896M  37G  3% /
tmpfs           tmpfs  935M    0  935M  0% /dev/shm
/dev/vdb1        ext4  2.0T  199M  1.9T  1% /mnt
[root@localhost ~]#
```

(2) 扩容大于 2TB 磁盘的具体操作如下：

- 通过 `lsblk` 及 `df` 查看当前磁盘的信息，包括挂载点、文件系统类型及分区情况；
- 通过控制台或 API 对硬盘进行容量扩容操作，并在操作系统中通过 `fdisk` 或 `lsblk` 查看扩容后的磁盘容量，本示例中将磁盘扩容为 2.1TB，即 2100GB，如下图所示：

```
[root@localhost ~]# lsblk
NAME   MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
vda    252:0    0  40G  0 disk
└─vda1 252:1    0  40G  0 part /
vdb    252:16   0 2.1T  0 disk
└─vdb1 252:17   0   2T  0 part /mnt
[root@localhost ~]# df -Th
Filesystem      Type  Size  Used Avail Use% Mounted on
/dev/vda1        ext4  40G  896M  37G  3% /
tmpfs           tmpfs  935M    0  935M  0% /dev/shm
/dev/vdb1        ext4  2.0T 199M  1.9T  1% /mnt
[root@localhost ~]#
```

- 在操作系统中 umount 磁盘，使用 `parted /dev/vdb` 命令删除原来分区并创建新分区，同时使用 `lsblk` 命令查看 vdb1 分区信息。若为多分区则删除最后一个分区并创建新分区；

```

(parted) unit s
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 4404019200s
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number Start End Size File system Name 标志
 1 2048s 4194303966s 4194301919s ext4 test
    换一换

(parted) rm 1
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 4404019200s
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number Start End Size File system Name 标志
 1 2048s 4194303966s 405万 ext4 test
    增78例确诊病例 390万

(parted) mkpart test 2048s 100%
(parted) p
Model: Virtio Block Device (virtblk)
Disk /dev/vdb: 4404019200s
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number Start End Size File system Name 标志
 1 2048s 4404017151s 315万 ext4 test
    新冠病毒检测呈阴性 293万

(parted) q
信息： You may need to update /etc/fstab.

[root@localhost ~]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINT
vda 252:0 0 40G 0 disk
└─vda1 252:1 0 40G 0 part /
vdb 252:16 0 2.1T 0 disk
└─vdb1 252:17 0 2.1T 0 part
[root@localhost ~]#

```

如图所示，其中 `unit s` 代表将显示和操纵单位变成 `sector`；`rm 1` 是删除当前分区；`mkpart test 2048s 100%` 是创建一个名称为 `test`，起始扇区为 `2048s`，使用磁盘全部空间的新分区。
注：删除当前分区不会造成磁盘内数据丢失。

- 执行 `e2fsck -f /dev/vdb1` 命令检查文件系统，并使用 `resize2fs /dev/vdb1` 对分区进行扩容操作；

```
[root@localhost ~]# e2fsck -f /dev/vdb1
e2fsck 1.41.12 (17-May-2010)
第一步：检查 inode, 块, 和大小
第二步：检查目录结构
第三步：检查目录连接性
Pass 4: Checking reference counts
第五步：检查簇概要信息
/dev/vdb1: 169/131072000 files (1.2% non-contiguous), 8294094/524287739 blocks
[root@localhost ~]# resize2fs /dev/vdb1
resize2fs 1.41.12 (17-May-2010)
Resizing the filesystem on /dev/vdb1 to 550501888 (4k) blocks.
The filesystem on /dev/vdb1 is now 550501888 blocks long.
```

- 重新 mount 磁盘并查看磁盘情况，检查扩容是否成功

```
[root@localhost ~]# mount /dev/vdb1 /mnt/
[root@localhost ~]# df -Th
Filesystem      Type  Size  Used  Avail Use% Mounted on
/dev/vda1        ext4   40G   894M   37G   3% /
tmpfs           tmpfs  935M     0  935M   0% /dev/shm
/dev/vdb1        ext4   2.1T  264M  2.0T   1% /mnt
[root@localhost ~]# ls /mnt/
aaa
acpid
addgrupghome
groupadd
groupdel
groupmems
```

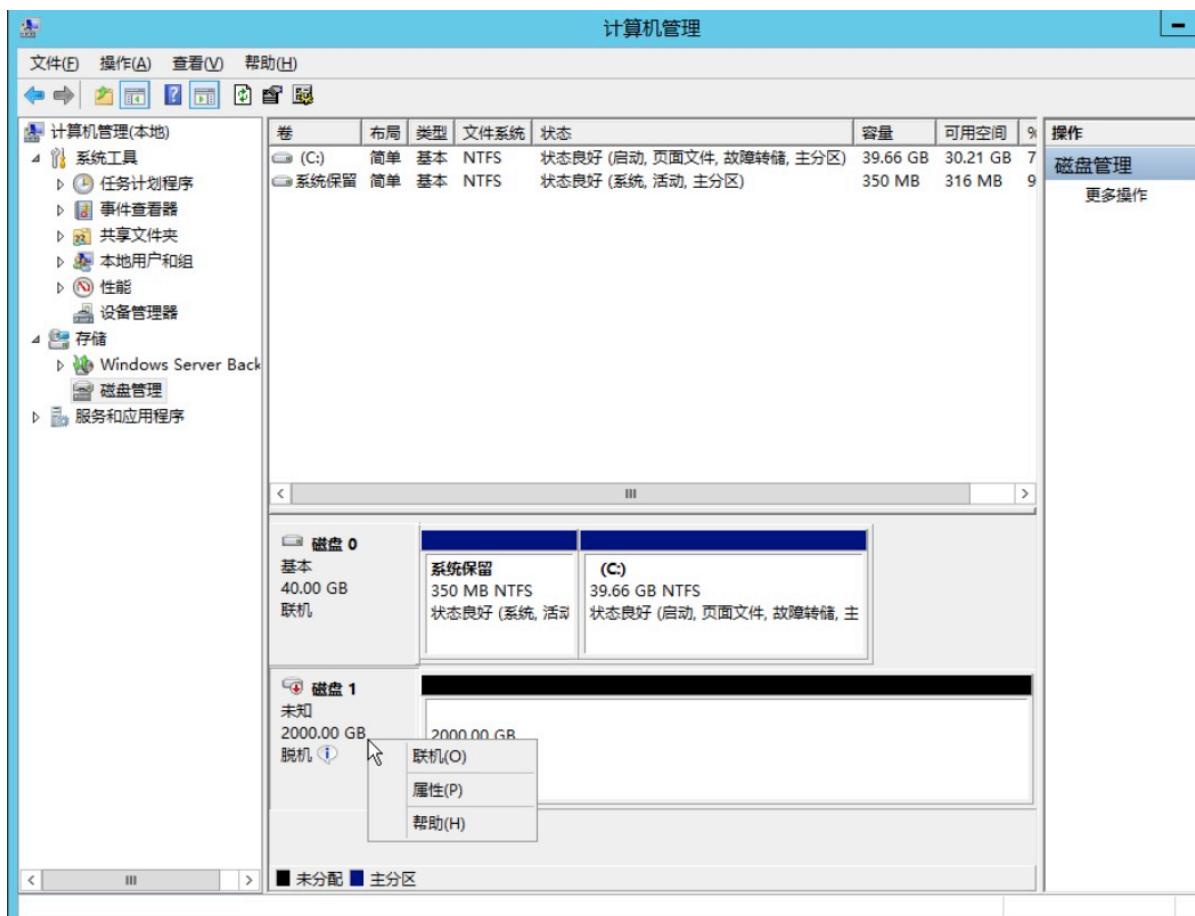
6.7.2.7 2TB 磁盘分区扩容 (Windows)

当一块磁盘的容量大于 2TB 时，在 Windows 下无法使用 MBR 分区形式，需要使用 GPT 分区表形式进行磁盘初始化，并通过磁盘管理工具进行分区及扩容操作。2TB 以上磁盘在 Linux 及 Windows 操作系统上的操作不同，本章节为 Windows 下大于 2TB 磁盘扩容操作指南。

本示例以 Windwos Server 2012R2 操作系统为示例环境版本，云硬盘大小为 2TB，挂载点为 Disk1（磁盘1），扩容至 2.1TB，即将云盘及分区扩容为 100GB，实际环境中需根据实际情况进行操作。具体操作如下：

(1) 若磁盘为新创建，则需要磁盘管理工具对磁盘进行联机并初始化操作，具体操作如下：

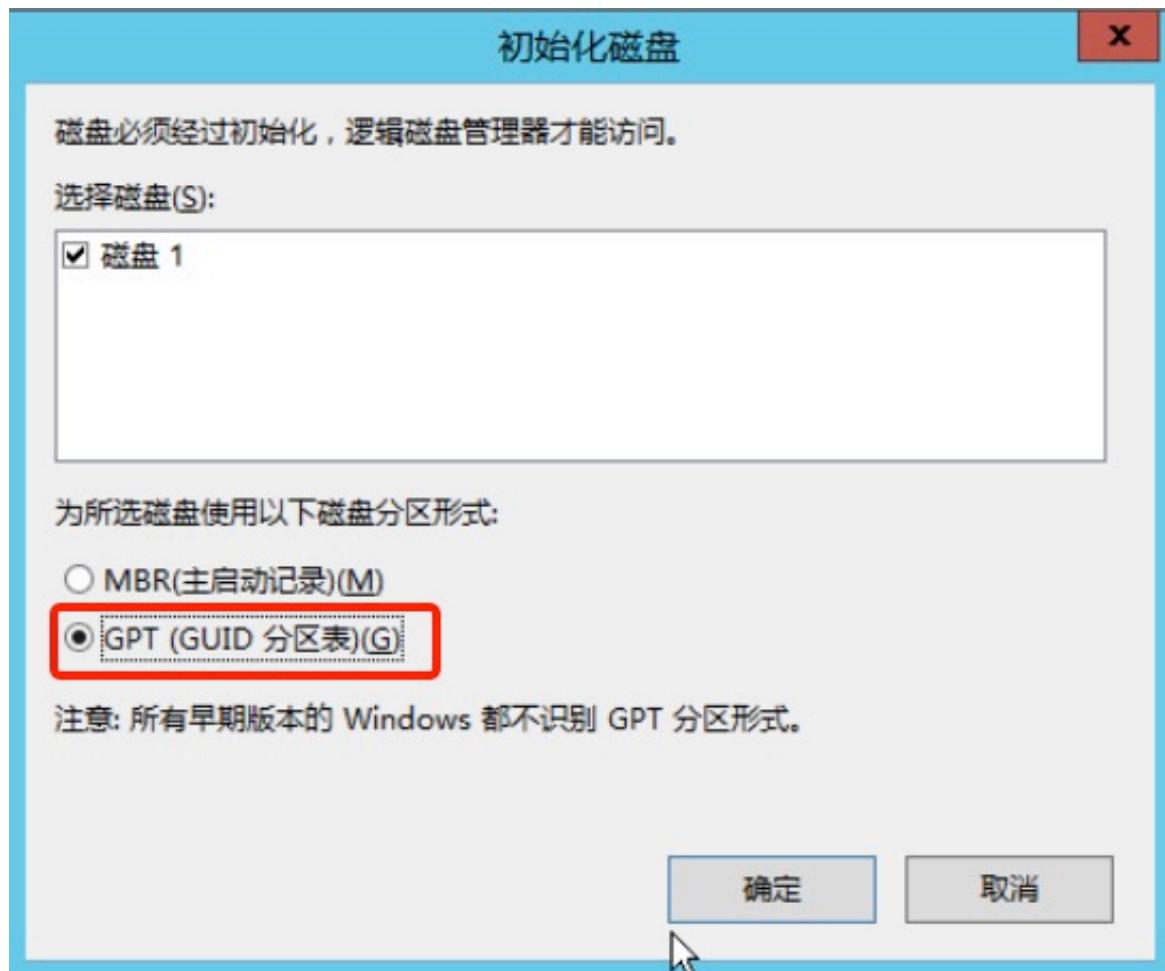
- 当在控制台创建一台 2T 的硬盘挂载至 Windows 虚拟机后，在磁盘管理工具会出现类似 磁盘1 或 Disk1 的磁盘，并且磁盘的状态为脱机；



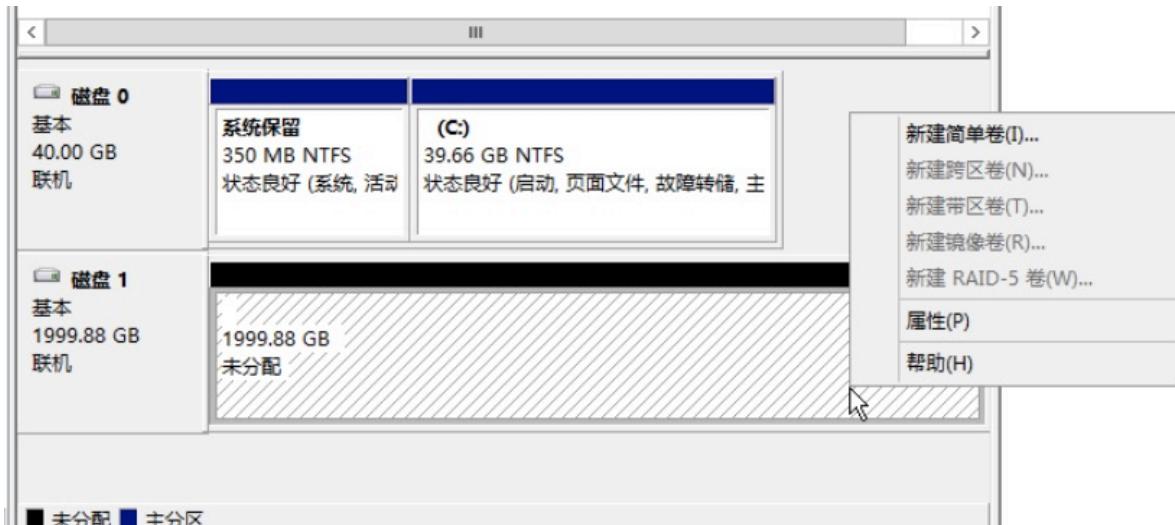
- 如上图所示，右键点击磁盘1右边空白处，单击联机，将磁盘置为联机状态；
- 磁盘联机后，磁盘状态为“没有初始化”，可点击磁盘空白处，点击初始化磁盘；



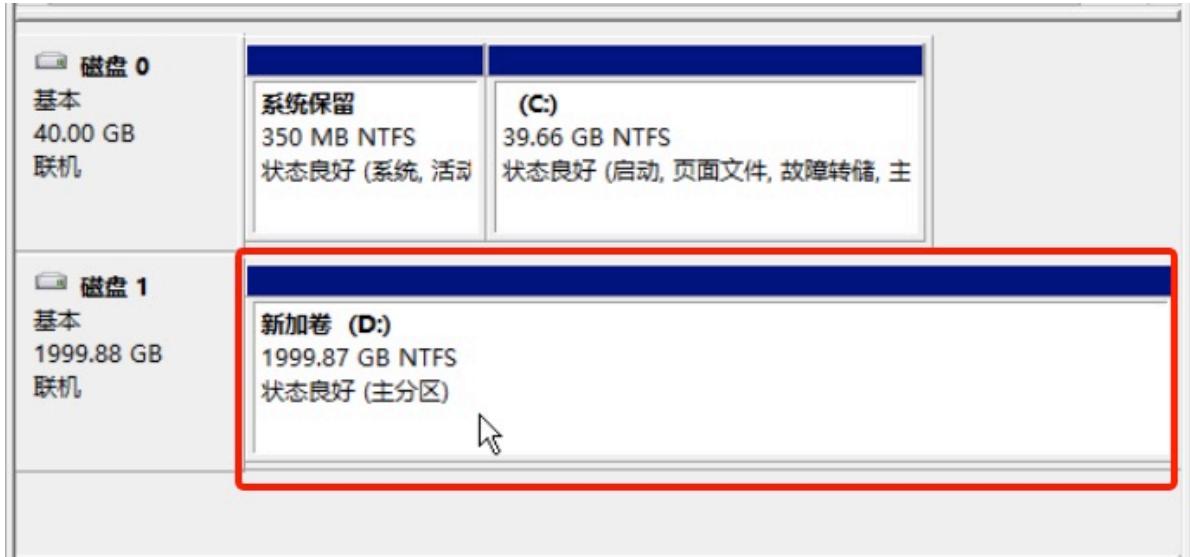
- 在初始化磁盘界面，选择“GPT (GUID分区表)”选项，进行磁盘初始化操作；



- 磁盘初始化成功后，右键点击磁盘1 未分配区域，点击单建简单卷进行分区及格式化操作；

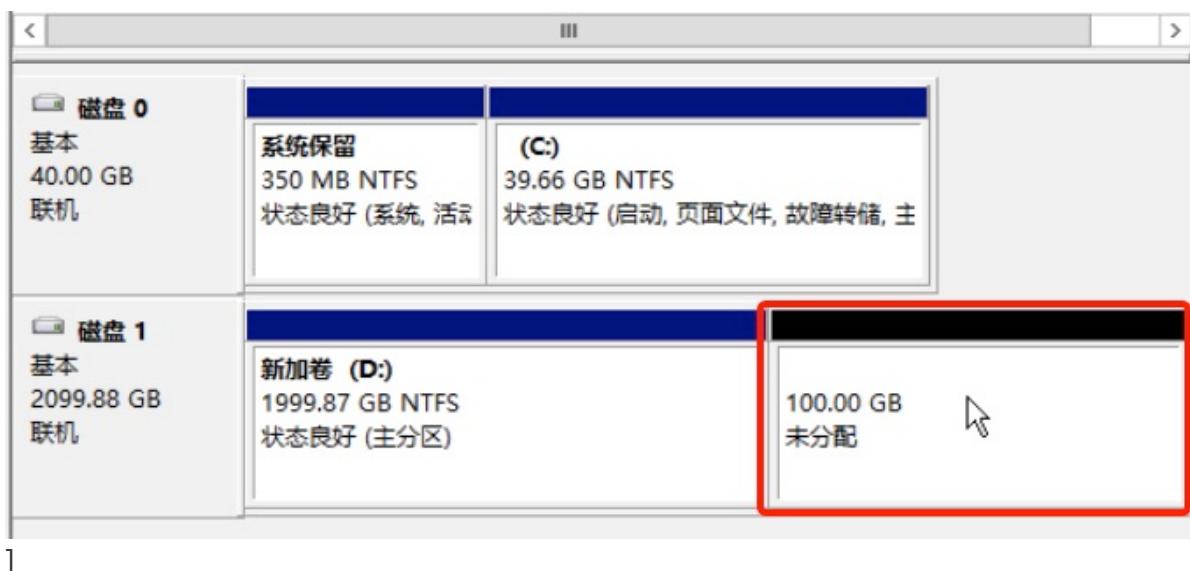


- 在新建简单卷导向中，选择卷大小、驱动器号及格式化选项后，成功创建新的分区，如下图所示：

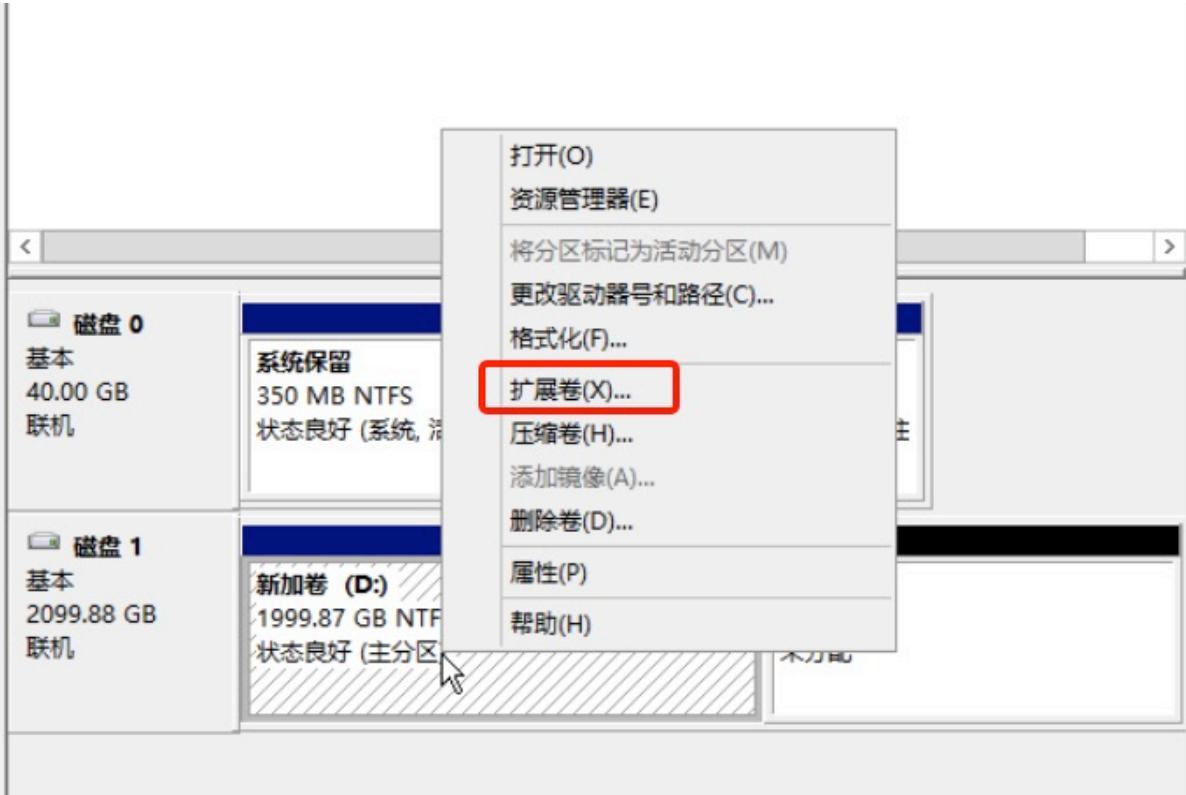


(1) 若要扩容 Windows 上 2T 的磁盘，可按如下操作进行扩容：

- 通过控制台或 API 对磁盘 1 进行扩容，扩容后可通过 Windows 操作系统的磁盘管理工具“重新扫描磁盘”查看新扩容磁盘信息，如下图所示磁盘1多出来 100GB 的未分配空间；



- Windows 扩容分区，可将多余的 100GB 单独划分一个分区，也支持将 100GB 空间扩容至已有分区中，本示例演示将 100GB 未分配的容量扩容至已有分区 D 盘中；
- 右键点击已有分区的空白处（本示例为 D 盘），单击扩展卷，通过扩展卷向导将未分配容量扩展至 D 盘中；



- 在扩展卷向导中，选择磁盘1，并输需扩展的容量，通常系统已默认选择所有未分配容量，并确认扩展卷操作



- 扩展成功后，未分配容量已成功扩容至已有分区 D 盘中，如上图所示，磁盘总容量为 2.1T；



6.8 硬盘克隆

硬盘克隆是指将云硬盘内的数据复制到一个新的云硬盘，硬盘大小和类型与原硬盘一致。仅支持克隆状态为未绑定状态的硬盘，同时在硬盘克隆过程中，源硬盘不可进行绑定、克隆、扩容等操作。

用户可通过云硬盘硬盘资源列表上的“克隆”功能，进行云硬盘克隆操作，如下图所示：



- 源硬盘名称/ID：需要进行克隆的硬盘名称和 ID；
- 源硬盘容量：需要进行克隆操作硬盘的容量，即源硬盘容量；
- 目标硬盘名称：新克隆的硬盘名称。

克隆会基于源硬盘复制出一块新的硬盘，需选择新硬盘的相关计费配置，包括购买数量、付费方式及合计费用等：

- 购买数量：按照所选配置及参数批量创建多块云硬盘，目前仅支持同时克隆一块硬盘。
- 付费方式：选择硬盘的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方

式；

- **合计费用：**用户选择创建云硬盘资源按照付费方式的费用展示；
- **确认：**点击确认购买后，会返回云硬盘资源列表页，在列表页可查看云硬盘的克隆过程，克隆成功后，云硬盘状态显示为“未绑定”。

硬盘克隆可用于硬盘数据的备份及快照等应用场景，克隆出的硬盘与源硬盘数据完全一致。

6.9 删除云硬盘

支持用户删除“未绑定”状态的云硬盘资源，被删除的云硬盘会自动进入“回收站”中，可进行还原及销毁。删除云硬盘后，通过当前云硬盘创建的快照资源会同时被销毁。

用户可通过云硬盘管理控制台的“删除”功能删除云硬盘，删除后可在回收站查看已删除的云硬盘资源。如图所示：



6.10 修改名称和备注

修改硬盘的名称和备注，在任何状态下均可进行操作。可通过硬盘列表页面每个硬盘名称右侧的“编辑”按钮进行修改。

6.11 快照管理

云平台分布式存支持磁盘快照能力，可降低因误操作、版本升级等导致的数据丢失风险，是平台保证数据安全的一个重要措施。

6.11.1 快照概述

快照是某一时间点一块云盘的数据状态文件，可以理解云硬盘某个时刻的数据备份，云硬盘的数据写入和修改不会对已创建的快照造成影响。

- **定时快照策略：**定时快照策略是指一个可周期性执行的自动创建快照的策略，快照策略与快照分离，拥有独立的生命周期；
- **快照链：**快照链是一块云硬盘所有快照的集合，一块云硬盘有且只有 1 个快照链。快照链的引入主要用于快照安全管理和快照额度管理，一条快照链最多包含 512 条快照，其中自动快照和手动快照各 256 条，由于快照采用增量机制，除了第一块快照为全量快照外，后续快照只保留前一块快照的变化数据。当用户删除中间某个快照后，只会删除该快照中未被后序快照引用的 Block，被

引用部分的 Block 将记录到后续快照。

在实际应用中，磁盘快照可降低因误操作、版本升级等导致的数据丢失风险，可大致应用于以下业务场景：

- **容灾备份**：定时为云硬盘制作快照，当系统出现问题时，可快速回退，避免数据丢失。
- **版本回退**：在业务做重大升级时，建议预先做好快照，当升级版本出现系统问题无法修复时，可通过快照恢复到历史版本。

平台支持对已绑定虚拟机的系统盘及数据盘进行快照操作，同时支持将快照回滚操作，即将快照数据回滚到关联的云硬盘，以满足数据恢复的应用场景。

6.11.2 创建快照

用户可在云硬盘列表页面，为某块云硬盘创建快照；若硬盘已挂载虚拟机，也可通过虚拟机详情页面的硬盘信息列表对硬盘进行快照操作，同时支持对虚拟机系统盘进行快照备份。为保证数据及磁盘的安全：

- 仅支持对未绑定及已绑定的硬盘进行快照操作，若硬盘在扩容或快照中，无法进行快照备份；
- 创建快照时，不可进行磁盘挂载/卸载及修改虚拟机状态（如开机或关机），否则可能会导致快照创建异常；
- 快照仅捕获已写入硬盘的数据，不包含应用程序或操作系统缓存在内存中的数据，建议在快照暂停对硬盘的 I/O 操作后进行快照制作，如关机或卸载硬盘。

在实际操作中，可通过云硬盘列表页或虚拟机详情磁盘列表操作项中的“快照”为云硬盘创建快照。如创建快照向导页面所示，用户可通过核验所需创建的硬盘信息，并输入快照名称，进行快照创建操作。



一个硬盘同时一时间仅支持创建一个快照，快照创建过程中硬盘的状态为“快照中”，待状态转换为“未绑定”或“已绑定”即代表快照创建成功，用户可通过快照列表页面查看已创建的快照状态及相关信息。

6.11.3 查看快照信息

快照创建成功后，用户可通过虚拟机控制台，切换至快照管理页面查看快照资源列表信息及相关信息，包括名称、资源 ID、磁盘、磁盘类型、状态、创建时间及操作项待，如下图所示：

名称	资源ID	硬盘ID	硬盘类型	状态	创建时间	操作
343 修改名称及备注	snap-6Y7zmPnGg	ci-ETbN60nMR_boot	系统盘	正常	2020-07-19	<button>回滚</button> <button>删除</button>
343 修改名称及备注	snap-nVZD3YnMR	disk-DT3JjYnGg	数据盘	正常	2020-07-19	<button>回滚</button> <button>删除</button>

- 资源名称/ID：代表当前快照的名称及全局唯一标识符；
- 磁盘：代表当前快照对应的磁盘，即代表该快照是由该磁盘创建；
- 磁盘类型：代表当前快照所属硬盘的属性，如数据盘或系统盘；
- 状态：代表当前快照的运行状态，包括创建中、正常、回滚中、删除中，其中回滚中代表当前快照正在进行回滚操作；
- 创建时间：当前快照的创建时间。

列表上的操作项是指对单个快照的操作，包括回滚和删除。为方便租户对快照资源的统计及维护，平台支持下载当前用户所拥有的所有快照资源列表信息为 Excel 表格，同时支持对快照进行批量删除操作。

6.11.4 回滚快照

回滚快照是将某一时刻的快照数据回滚到关联的云硬盘，应对快照数据恢复的应用场景。

- 回滚时云硬盘必须处于未绑定或绑定的虚拟机必须处于关机状态；
- 仅支持正常状态的快照进行回滚操作。

用户可通过快照资源列表操作项中的“回滚”对快照进行回滚操作，仅支持回滚快照至所属硬盘，如下图所示：

回滚硬盘

确认要回滚以下硬盘的数据吗？回滚后，此硬盘该时刻之后的数据将被清除。请谨慎操作！

硬盘ID *	disk-DT3JjYnGg
快照名称	343
创建时间	2020-07-19 17:21:01

取消 确认

点击确认后，即返回快照列表页面，快照及所属硬盘均转换为“回滚中”状态，待回滚成功后，硬盘转换为“未绑定”状态，快照转换为“正常”状态。快照回滚成功后，所属父硬盘上回滚操作前的数据将被清除，由快照中的数据覆盖，即父硬盘中的数据与当前快照上捕获的数据一致。



若快照所属硬盘处于挂载状态且挂载的虚拟机为开机状态，则无法进行数据回滚操作，如下图所示，需先关闭虚拟机或解绑硬盘。

6.11.5 删除快照

平台快照为增量快照，后续快照只保留前一块快照的变化数据，当用户删除中间某个快照后，只会删除该快照中未被后序快照引用的 Block，被引用部分的 Block 将记录到后续快照。

支持用户删除一块硬盘的任何一个快照，假设用户对一块硬盘做了 10 个快照，删除任何一个快照，都不影响快照回滚后的数据。

- 如用户删除第 1 个快照，则系统会将第 1 个快照中的数据合并至第 2 个快照中，保证通过第 2 个快照回滚的数据准确性；
- 如用户只删除了第 2 个快照，则系统会只会删除快照 2 中未被快照 3 引用的数据块，被 3 引用的数据块会被自动记录至快照 3 中，保证快照 3 快照回滚数据的准确性。



仅支持删除正常状态的快照，如上图所示，用户可通过控制台快照列表页面对某个快照进行删除操作，快照删除后将彻底销毁。

6.11.6 修改快照名称

修改快照的名称和备注，在任何状态下均可进行操作。可通过快照资源列表页面每个快照名称右侧的“编辑”按钮进行修改。

7 私有网络

7.1 VPC 简介

7.1.1 概述

UCloudStack 通过软件定义网络（SDN）对传统数据中心物理网络进行虚拟化，采用 OVS 作为虚拟交换机，VXLAN 隧道作为 OverLay 网络隔离手段，通过三层协议封装二层协议，用于定义虚拟私有网络 VPC 及不同虚拟机 IP 地址之间数据包的封装和转发。

私有网络（VPC——Virtual Private Cloud）是一个属于用户的、逻辑隔离的二层网络广播域环境。在一个私有网络内，用户可以构建并管理多个三层网络，即子网（Subnet），包括网络拓扑、IP 网段、IP 地址、网关等虚拟资源作为租户虚拟机业务的网络通信载体。

私有网络 VPC 是虚拟化网络的核心，为云平台虚拟机提供内网服务，包括网络广播域、子网（IP 网段）、IP 地址等，是所有 NVF 虚拟网络功能的基础。私有网络是子网的容器，不同私有网络之间是绝对隔离的，保证网络的隔离性和安全性。

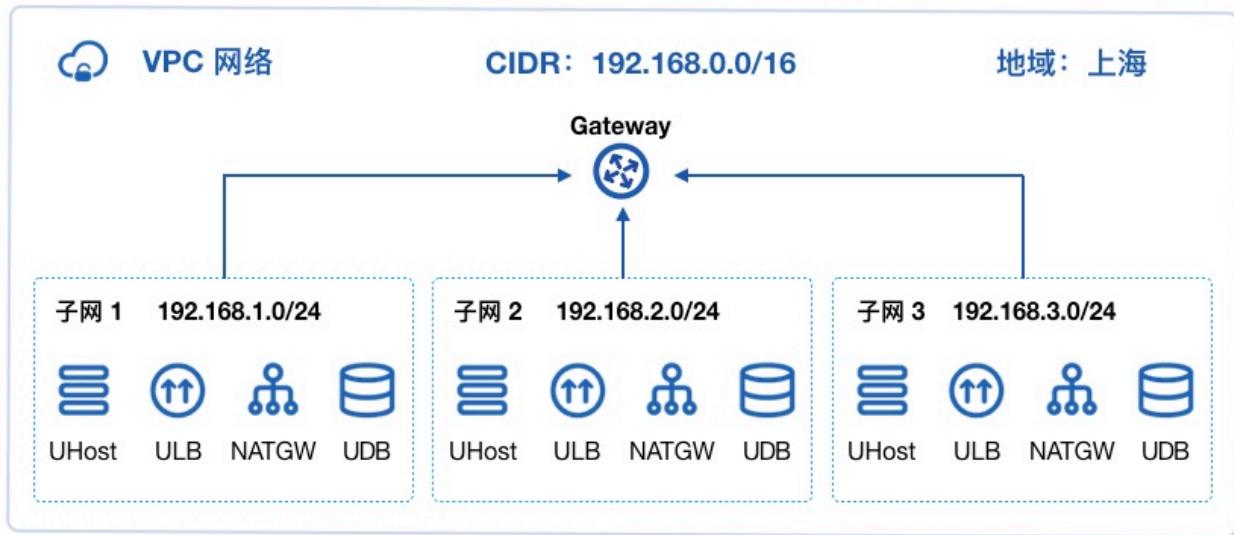
可将虚拟机、负载均衡、弹性网卡、NAT 网关等虚拟资源加入至私有网络的子网中，提供类似传统数据中心交换机的功能，支持自定义规划网络，并通过安全组对虚拟资源 VPC 间的流量进行安全防护。

可通过 IPSecVPN、专线及外网 IP 接入等方式将云平台私有网络及虚拟资源与其它云平台或 IDC 数据中心组成一个按需定制的混合云网络环境。

VPC 网络具有数据中心属性，每个 VPC 私有网络仅属于一个数据中心，数据中心间资源和网络完全隔离，资源默认内网不通。租户内和租户间 VPC 网络默认不通，从不同维度保证租户网络和资源的隔离性。

7.1.2 VPC 逻辑结构

一个 VPC 网络主要由私有网络网段和子网两部分组成，如下图所示：



(1) 私有网络网段

VPC 网络所属的 CIDR 网段，作为 VPC 隔离网络的私网网段。关于 CIDR 的相关信息，详见 [CIDR](#)。创建 VPC 网络需指定私有网段，平台管理员可通过管理控制台自定义 VPC 私有网络的网段，使租户的虚拟资源仅使用管理员定义网段的 IP 地址进行通信。平台 VPC 私有网络 CIDR 默认支持的网段范围如下表所示：

网段	掩码范围	IP 地址范围
10.0.0.0/8	8 ~ 29	10.0.0.0 - 10.255.255.255
172.16.0.0/12	12 ~ 29	172.16.0.0 - 172.31.255.255
192.168.0.0/16	16 ~ 29	192.168.0.0 - 192.168.255.255

由于 DHCP 及相关服务需占用 IP 地址，私有网络 CIDR 网段不支持 30 位掩码的私有网段。

(2) 子网

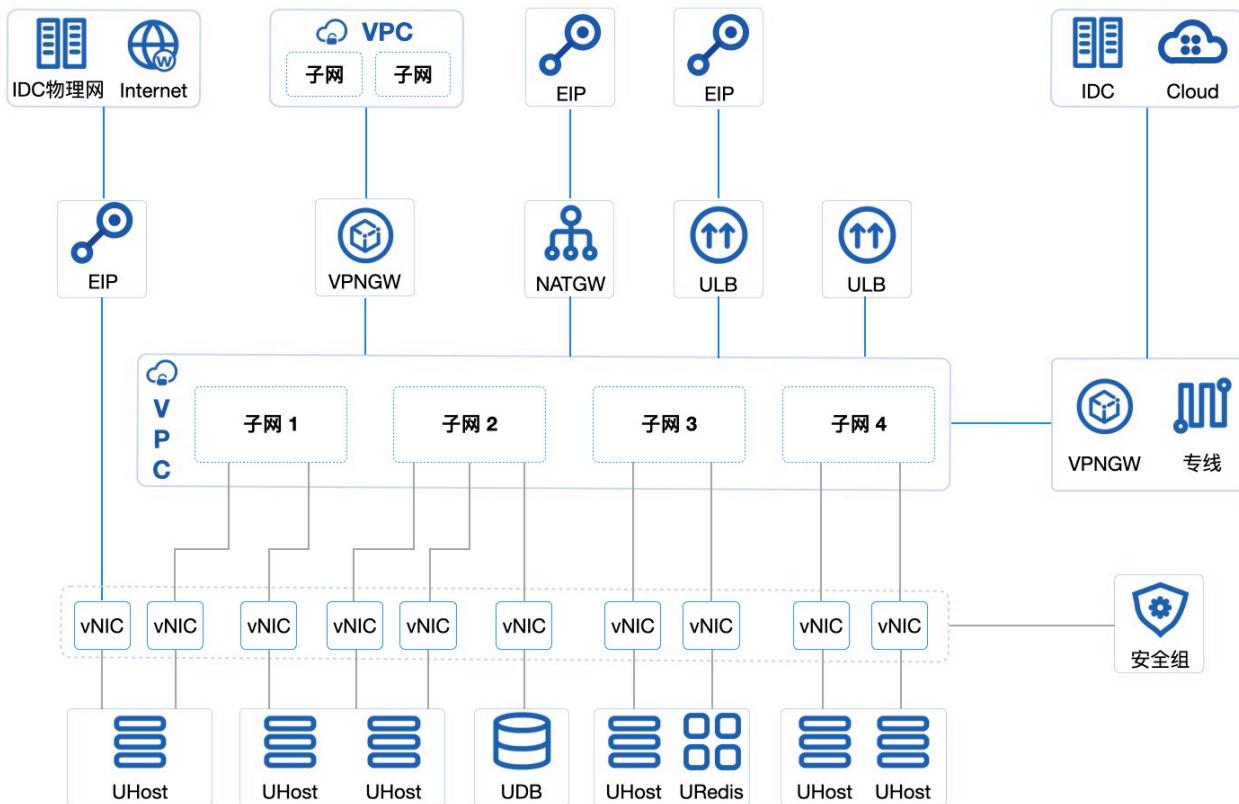
子网（Subnet）是 VPC 私有网络的基础网络地址空间，用于虚拟资源间内网连接。

- 一个私有网络至少由一个子网组成，子网的 CIDR 必须在 VPC 的 CIDR 网段内；
- 同一私有网络内子网间通过公共网关连接，资源默认内网互通，可部署虚拟机、负载均衡、NAT 网关、Redis、MySQL 及 IPSecVPN 网关等；
- 同一个 VPC 子网间默认通过公共网关进行互通；
- 子网 CIDR 网段掩码最小为 29 位，不支持 30、32 位掩码的子网网段；
- 每个子网中，使用第一个可用 IP 地址作为网关，如 192.168.1.0/24 的网关地址是 192.168.1.1。

当子网中存在虚拟资源时，不允许删除并销毁私有网络和子网资源。

7.1.3 VPC 连接

平台对常用网络设备均进行软件定义及组件抽像，通过将 VPC 网络与虚拟机、弹性网卡、外网 IP、安全组、NAT 网关、负载均衡、VPN 网关、MySQL 数据库、Redis 缓存及专线等组件连接，可快速构建和配置繁杂的网络环境及混合云场景，如下图所示：



- 虚拟机默认内网网卡（创建时自带的虚拟网卡）加入同一个 VPC 网络实现虚拟机间网络通信，并可通过安全组保证虚拟机东西向流量安全。
- 虚拟机默认外网网卡（创建时自带的虚拟网卡）可直接绑定多个外网 IP 地址实现 Internet 访问，同时可绑定与 IDC 物理网络相连的外网 IP 地址实现物理网络打通，结合安全组管控虚拟机南北向流量的同时，构建安全可靠的混合接入环境。
- 虚拟机的弹性网卡加入不同的 VPC 网络及子网，实现精细化网络管理及廉价故障转移方案，同时将安全组与弹性网卡绑定，通过安全组规则多维度保障私有网络及虚拟资源的安全。
- 虚拟机与 UDB、URedis 服务加入同一个 VPC 网络，满足业务应用和数据库、缓存服务连通场景。
- 相同 VPC 网络的虚拟机可通过 NAT 网关及外网 IP 连接，共享外网 IP 访问 Internet 或 IDC 数据中心网络，并可通过 DNAT 端口映射对外提供业务服务。
- 相同 VPC 网络的虚拟机加入至内网 ULB 后端服务节点，提供 VPC 网络内负载均衡服务。
- 相同 VPC 网络的虚拟机加入到外网 ULB 后端服务节点，结合 ULB 关联的外网 IP，提供外网负载均衡服务。
- 相同 VPC 网络的虚拟机通过 IPSecVPN 网关可与不同 VPC 网络的虚拟机进行内网互联，实现 VPC 间互通。
- 通过 IPSecVPN 网关打通不同 VPC 间的网络，使两个 VPC 间的虚拟机可直接进行内网通信。
- 采用 IPSecVPN 网关或专线将平台与本地 IDC 数据中心及第三方云平台连通，构建安全可靠的混合云环境。

外网 IP 可用于打通 IDC 数据中心的物理网络，应用于与虚拟机直接与物理机进行内网通信的场景；IPSecVPN 网关用于打通第三方云平台或 IDC 数据中心的虚拟网络，应用于不同云平台间通过 VPN 安全连接场景。

7.1.4 功能与特性

平台 VPC 网络基于租户控制台和 API 提供隔离网络环境、自定义子网、子网通信及安全防护等功能，并可结合硬件及 DPDK 等技术特性提供高性能的虚拟网络。

- 隔离的网络环境

私有网络基于 [OVS](#) (Open vSwitch) 组件，通过 [VXLAN](#) 隧道封装技术实现隔离的虚拟网络。每一个 VPC 网络对应一个 VXLAN 隧道号 (VNI)，作为全局唯一网络标识符，为租户提供一张独立且完全隔离的二层网络，可通过在私有网络中划分多个子网作为虚拟资源的通信载体，用于连通多个虚拟资源。不同的 VPC 网络间完全隔离，无法直接通信。

- 自定义子网

支持在一个 VPC 网络内进行三层网络规划，即划分一个或多个子网。提供自定义 IP 网段范围、可用 IP 网段及默认网关，可在子网中通过虚拟机部署应用程序和服务。支持在子网中增加多个弹性网卡，分别指定子网中的 IP 地址，并绑定至部署应用程序的虚拟机，用于精细化管理应用服务的网络访问。

- 子网通信

每一个子网都属于一个广播域，VPC 网络默认提供网关服务，同一个 VPC 内不同子网通过网关进行通信。

- 安全防护

云平台提供内网安全组和外网防火墙，通过协议、端口为虚拟资源提供多维度安全访问控制，同时基于虚拟网卡及虚拟实例的网络流量进行上下行的 QoS 控制，全方位提高 VPC 网络的安全性。安全组为有状态安全层，可分别设置出入方向的安全规则，用于控制并过滤进出子网 IP 的数据流量。

- 高性能虚拟网络

SDN 网络分布式部署于所有计算节点，节点间通过 20GE 冗余链路进行通信，并通过所有计算节点负载内网流量，为云平台提供高可靠及高性能的虚拟网络。

云平台在保证网络隔离、网络规模、网络通信及安全的同时，为租户和子账号提供 VPC 子网的创建、修改、删除及操作审计日志等全生命周期管理。用户创建虚拟机、NAT 网关、负载均衡、VPN 网关、MySQL 及 Redis 等虚拟资源时可指定需加入的 VPC 网络和子网，并可查询每个子网的可用 IP 数量。

VPC 网络具有数据中心属性，不同数据中心之间的虚拟资源默认内网不互通，同数据中心内不同 VPC 间默认内网不互通，同一个 VPC 的所有子网和资源默认内网互通。仅支持指定相同数据中心的虚拟资源到 VPC 网络中，且每个 VPC 网络的子网网段必须在 VPC 网络的 CIDR 网段中。

平台会通过管理员配置的 VPC 网络，为每个租户和子账号提供默认的 VPC 网络和子网资源，方便用户登录云平台快速部署业务。

7.2 创建 VPC

用户可通过指定 VPC 名称和 [CIDR](#) 网段一键添加一个 VPC 网络，用于搭建不同业务的网络环境。VPC 创建成功网段即不可修改，创建 VPC 网络需提前规划网络，如规划业务 IP 网段及 IP 地址。

通过导航栏进入“VPC 网络”资源列表页面，即可创建 VPC 网络，如下图所示：

创建VPC

VPC一旦创建成功，网段不可被修改

资源名称 *

资源描述

VPC网段 *

取消 确认

选择并配置 VPC 网络的名称及网段信息：

- VPC 名称：当前需要创建的 VPC 网络的名称标识；
- VPC 网段：VPC 网络所包含的 IP 网段，创建成功后无法修改，VPC 下所有子网共享该网段 IP 地址。

VPC 网络创建时状态为“创建中”，待状态转换为“有效”时，即代表 VPC 网络创建成功，通常可在 5 秒内完成 VPC 网络的创建，用户可通过 VPC 列表查看已创建的 VPC 资源信息。

7.3 查看私有网络

通过导航栏进入 VPC 网络控制台，可查看 VPC 网络资源的列表，并可通过列表上 VPC 名称可进入详情页面查看 VPC 网络及子网资源的详情信息。

7.3.1 私有网络列表

VPC 网络列表页可查看当前账户下 VPC 资源的列表及相关信息，包括名称、资源 ID、网段、子网数量、状态、创建时间及操作项，如下图所示：

私有网络 VPC

<input type="checkbox"/>	名称	资源ID	网段	子网数量	状态	创建时间	操作
<input type="checkbox"/>	abc 修改名称及备注	vpc-iLZhCnMR	192.168.0.0/22	0	● 有效	2020-07-22 15:16:58	详情 删除
<input type="checkbox"/>	vpc002 修改名称及备注	vpc-SX33TjgMR	10.0.0.0/16	2	● 有效	2020-05-21 12:26:15	详情 删除
<input type="checkbox"/>	vpc001 修改名称及备注	vpc-yaal9ugMg	172.16.0.0/16	2	● 有效	2020-05-20 21:29:51	详情 删除
<input type="checkbox"/>	cinder 修改名称及备注	vpc-DkYrASHWR	192.168.0.0/16	1	● 有效	2019-07-19 17:22:26	详情 删除

< 1 > 10 条/页 /1

- 名称/ID：VPC 私有网络的名称及全局唯一标识符；
- 网段：当前 VPC 网络在创建时指定的 CIDR 网段信息；
- 子网数量：当前 VPC 网络包含的子网数量；
- 状态：当前 VPC 网络的状态，一般为有效；
- 创建时间：当前 VPC 网络资源的创建时间；

列表上的操作项是可对单个 VPC 网络进行删除操作，可通过搜索框对 VPC 列表进行搜索和筛选，支持模糊搜索。

为方便租户对资源的统计及维护，平台支持下载当前用户所拥有的所有 VPC 网络资源列表信息为 Excel 表格；同时支持对 VPC 网络进行批量删除操作。

7.3.2 私有网络详情

在 VPC 网络列表上，点击 VPC 名称或 ID 可进入概览页面查看当前 VPC 网络的详情及子网信息，同时可切换至操作日志页面查看当前 VPC 网络及子网的操作日志信息，如下图概览页所示：

The screenshot shows the VPC network details page. At the top, there's a breadcrumb navigation: 私有网络 / vpc-SX33TjgMR. Below it, there are two tabs: 概览 (Overview) and 操作日志 (Operation Log). The 概览 tab is selected.

基本信息 (Basic Information):

资源ID	vpc-SX33TjgMR	编辑
资源名称	vpc002	修改名称及备注
地域	上海	
网段	10.0.0.0/16	
创建时间	2020-05-21 12:26:15	
状态	● 有效	

子网管理 (Subnet Management):

创建子网	删除	刷新			
资源名称	资源ID	网段	状态	创建时间	操作
10.192 修改名称及备注	subnet-b3VqTNzGR	10.0.192.0/20	● 有效	2020-05-25 18:57:29	删除
10.16 修改名称及备注	subnet-UwPeojgMR	10.0.16.0/20	● 有效	2020-05-21 12:26:39	删除

At the bottom right of the subnet table, there are pagination controls: < > 1 10 条/页 /1.

(1) 基本信息

VPC 网络的基本信息，包括资源 ID、资源名称、地域（数据中心）、网段、创建时间及状态。

(2) 子网管理

VPC 详情页面展示当前 VPC 网络中已创建的子网资源列表，包括名称、资源 ID、网段、状态、创建时间及对子网的操项，其中网段指当前子网的网段，包含在 VPC 网络的网段中。

子网列表上的操作项是可对单个子网进行删除操作，仅支持删除未被资源使用的子网资源。为方便租户对子网资源的维护，平台支持子网的批量删除操作。

7.4 修改名称和备注

修改 VPC 私有网络的名称和备注，在任何状态下均可进行操作。可通过 VPC 私有网络列表页面每个 VPC 名称右侧的“编辑”按钮进行修改。

7.5 删除私有网络

支持用户删除并释放未被任何资源占用 IP 地址的 VPC 网络。VPC 网络删除后会被彻底销毁，删除前须保证已清空 VPC 网络已创建的资源。删除操作如下图所示：



7.6 添加子网

添加子网是指为一个 VPC 网络添加子网，即三层网络，用于组建属于用户业务的私有网段，每一个网段是一个独立的广播域。子网的 CIDR 网段必须在 VPC 的 CIDR 网段内，同一子网内的资源默认内网互通，同一 VPC 下的所有子网默认互通。

用户可通过指定子网名称、子网 CIDR 网段为一个 VPC 网络添加一个或多个子网，用于构建内网不同的业务网络。创建子网前需保证 VPC 网络 CIDR 内有充足的 IP 网段，可通过 VPC 网络详情页面子网列表的“创建子网”进入创建向导页面，如下图所示



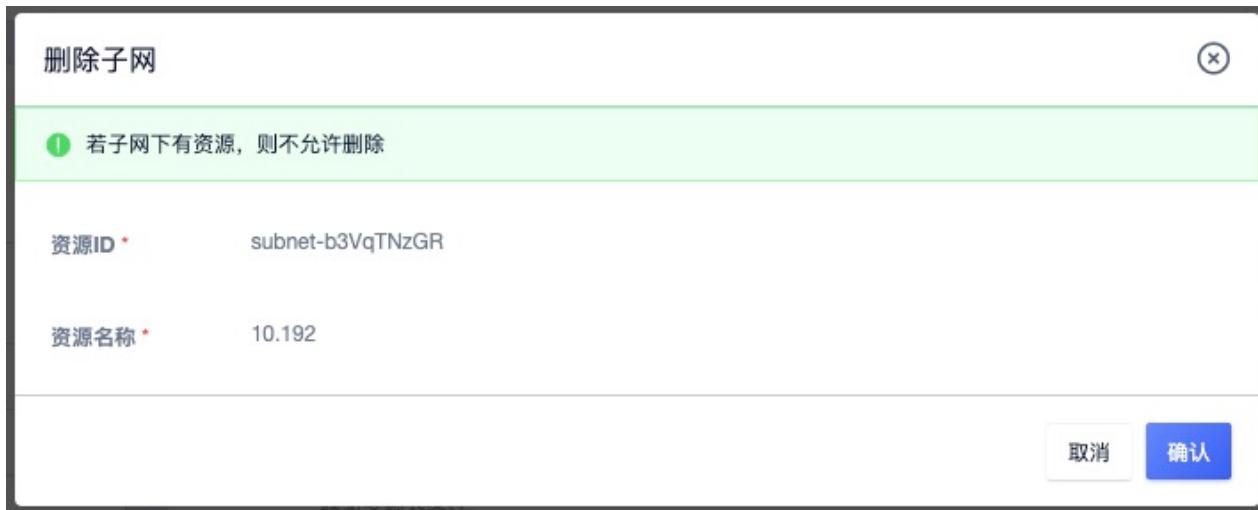
- 名称/描述：当前需要创建的子网的名称和描述信息；
- 子网网段：当前需要创建的子网的 CIDR 网段，子网网段必须在 VPC 的 CIDR 网段内，可以与 VPC CIDR 网段相同，即代表该子网包括 VPC 下所有的网络 IP 地址。

子网创建时状态为“创建中”，子网创建成功后，子网的状态转换为“有效”，可用于资源创建。

注：若子网网段的与 VPC 网段相同，则当前私有网络仅支持一个子网。

7.7 删除子网

用户可通过子网列表上的“删除”功能删除当前子网资源，被删除的子网将被直接销毁。删除子网前须保证子网内的资源已被清空，包含回收站的资源，否则不允许删除当前子网，如下图所示：



7.8 修改子网名称

修改子网的名称和备注，在任何状态下均可进行操作。可通过点击子网列表页面每个子网名称右侧的“编辑”按钮进行修改。

8 外网弹性 IP

8.1 EIP 简介

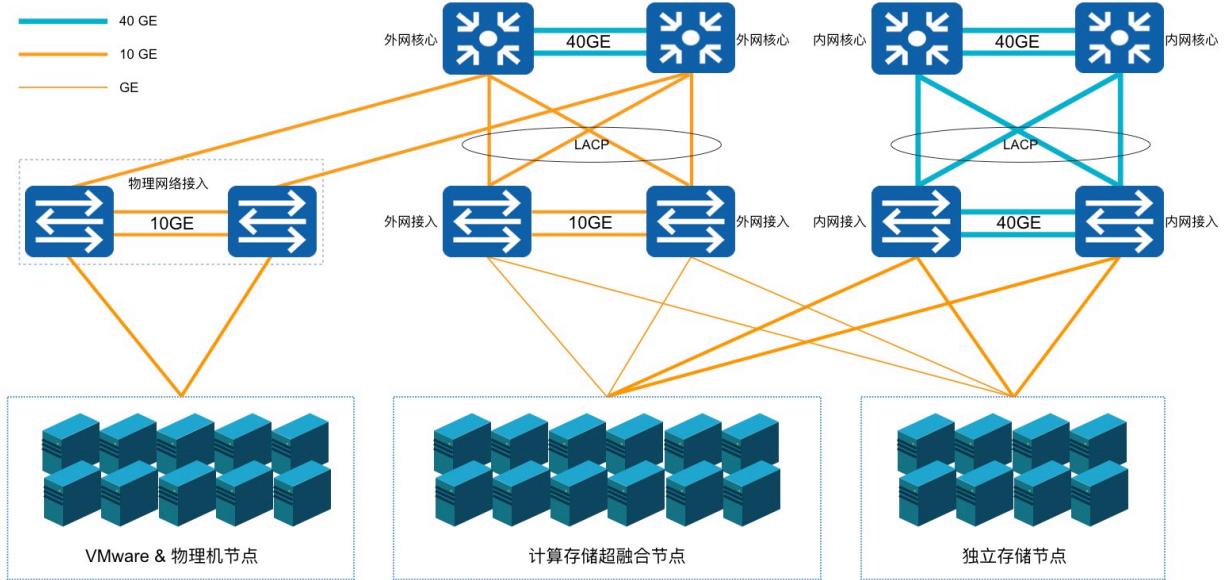
8.1.1 概述

外网弹性 IP（Elastic IP Address，简称 EIP），是平台为用户的虚拟机、NAT 网关、VPN 网关及负载均衡等虚拟资源提供的外网 IP 地址，为虚拟资源提供平台 VPC 网络外的网络访问能力，如互联网或 IDC 数据中心物理网络，同时外部网络也可通过 EIP 地址直接访问平台 VPC 网络内的虚拟资源。

EIP 资源支持独立申请和拥有，用户可通过控制台或 API 申请 IP 网段资源池中的 IP 地址，并将 EIP 绑定至虚拟机、NAT 网关、负载均衡、VPN 网关上，为业务提供外网服务通道。

8.2.2 物理架构

在私有云平台中，允许平台管理员自定义平台外网 IP 资源池，即由平台管理员自定义平台访问外网的方式，外网 IP 网段资源池在添加至云平台前，需要通过物理网络设备下发至计算节点连接的交换机端口。



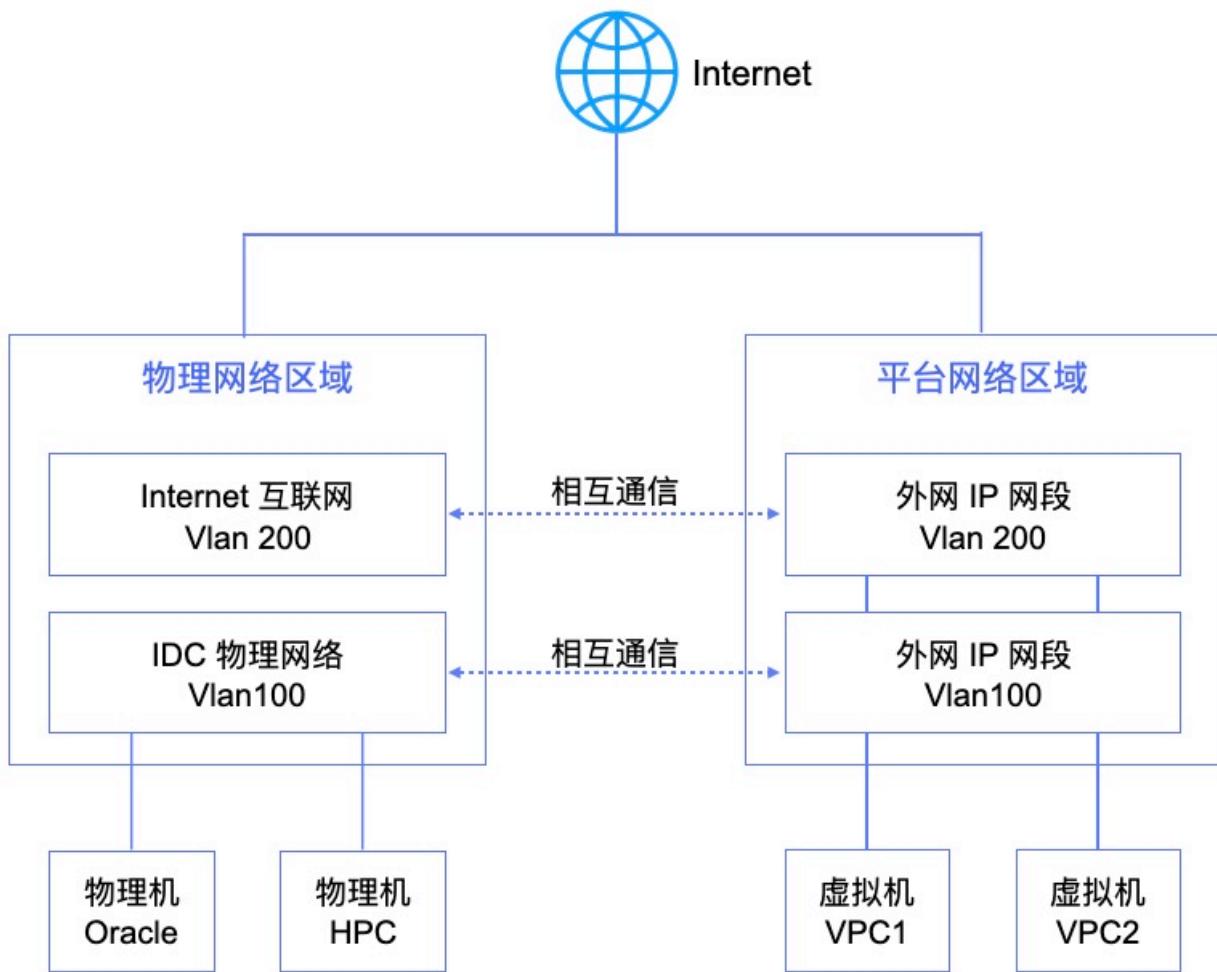
如上图物理架构示意图所示，所有计算节点需要连接网线至物理网络的外网接入交换机，并在物理网络的交互机上配置所连接端口允许透传 Vlan 的网络访问方式，使运行在计算节点上虚拟机可通过外网物理网卡直接与外部网络进行通信：

- 若通过外网 IP 访问互联网，需要物理网络设备上将自定义的外网 IP 网段配置为可直通或 NAT 到互联网；
- 若通过外网 IP 访问 IDC 数据中心的物理网络，需要在物理网络设备上将自定义的外网 IP 网段配置为可与 IDC 数据中心网络通信，如相同的 Vlan 或 Vlan 间打通等。

物理网络架构为高可用示意图，实际生产环境架构可进行调整，如内外网接入交换机可合并为一组高可用接入交换机，通过不同的 Vlan 区分内外网等。

8.2.3 逻辑架构

物理网络架构及配置确认后，在平台层面需要分别添加互联网 IP 网段和 IDC 物理网段至云平台 IP 网段资源池中，租户可申请不同网段的 EIP 地址，并将通往不同网络的 EIP 地址绑定至虚拟机默认外网网卡，使虚拟机可通过外网 IP 地址同时访问互联网和 IDC 数据中心物理网络。



如逻辑架构图所示，用户在平台中分别添加通往 Internet (Vlan200) 和通往 IDC 物理网络 (Vlan100) 的网段至云平台。网段举例如下：

- Vlan200 的网段为 106.75.236.0/25，配置下发默认路由，即虚拟机绑定网段的 EIP 将会自动下发目标地址为 0.0.0.0/0 的默认路由；
- Vlan100 的网段为 192.168.1.0/24，仅下发当前网段路由，即虚拟机绑定网段的 EIP 仅下发目标地址为 192.168.1.0/24 的指定路由。

租户可分别申请 Vlan200 和 Vlan100 的 EIP 地址，并可将两个 EIP 同时绑定至虚拟机。平台会将 EIP 地址及下发路由直接配置至虚拟机外网网卡，并通过 SDN 控制器下发流表至虚拟机所在的物理机 OVS，物理机 OVS 通过与物理机外网网卡接口及交换机进行互联，通过交换机设备与互联网或 IDC 物理网络进行通信。

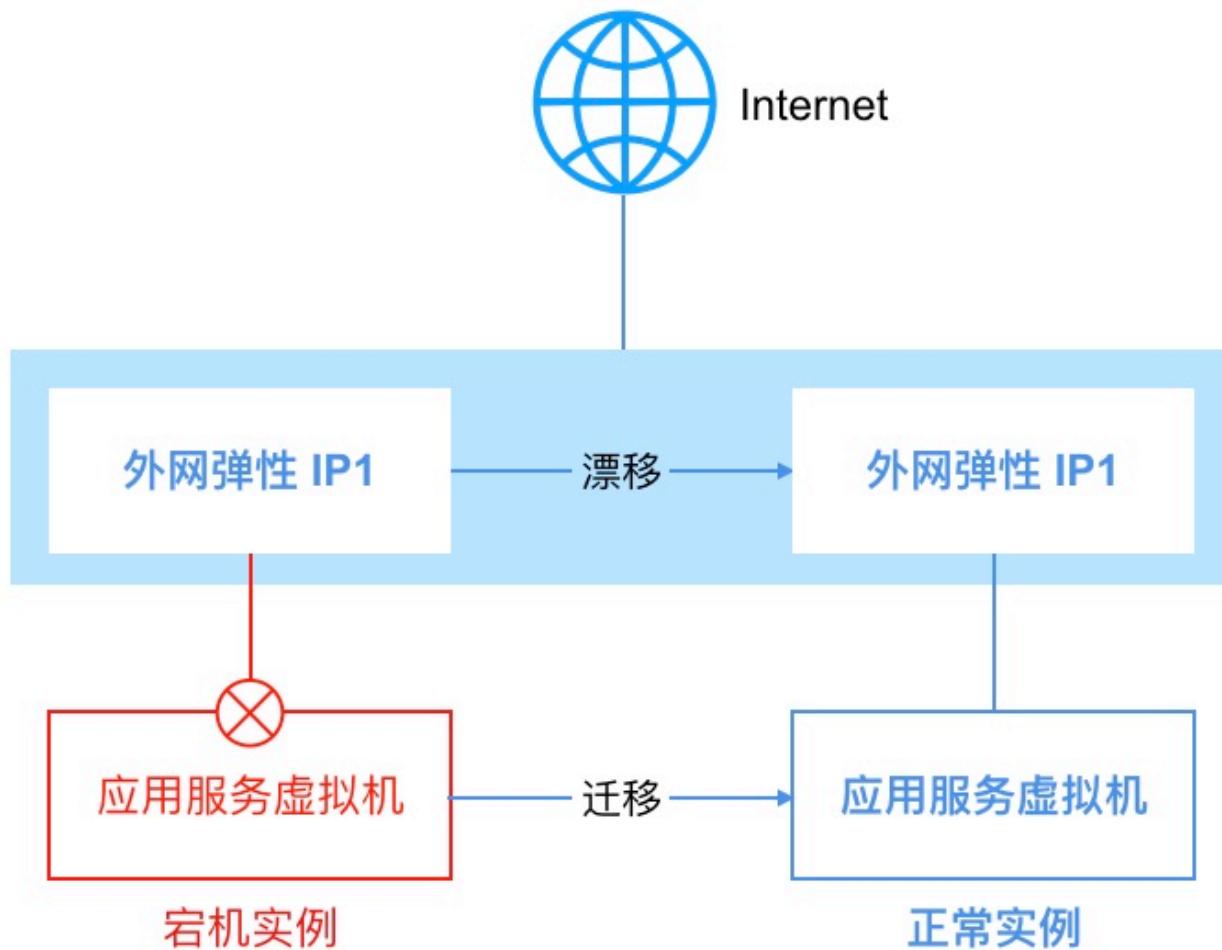
当虚拟机需要访问互联网或物理网络时，数据会通过虚拟机外网网卡直接透传至物理机的 OVS 虚拟交换机，并通过 OVS 流表将请求转发至物理机外网网卡及物理交换机，经由物理交换机的 Vlan 或路由配置将数据包转发至互联网或 IDC 物理网络区域，完成通信。

如上图 VPC1 网络的虚拟机同时绑定了 Vlan100 和 Vlan200 网段的 EIP 地址，Vlan100 EIP 为 192.168.1.2，Vlan200 EIP 为 106.75.236.2。平台会直接将两个 IP 地址直接配置至虚拟机的外网网卡，通过虚拟机操作系统可直接查看配置到外网网卡的 EIP 地址；同时自动下发两个 IP 地址所属网段需要下发的路由到虚拟机操作系统中，虚拟机的默认路由指定的下一跳为 Vlan200 互联网网段的网关，使虚拟机可通过 106.75.236.2 IP 地址与互联网进行通信，通过 192.168.1.2 与物理网络区域的 Oracle 及 HPC 高性能服务器进行内网通信。

整个通信过程直接通过虚拟机所在物理机的物理网卡进行通信，在物理网卡和物理交换机性能保障的前提下，可发挥物理网络硬件的最佳转发性能，提升虚拟机对外通信的转发能力。同时所有外网 IP 流量均可通过平台安全组在平台内进行流量管控，保证虚拟机访问平台外部网络的安全性。

8.2.4 功能特性

EIP 为浮动 IP，可随故障虚拟机恢复漂移至健康节点，继续为虚拟机或其它虚拟资源提供外网访问服务。



当一台虚拟机所在的物理主机发生故障时，智能调度系统会自动对故障主机上的虚拟机进行宕机迁移操作，即故障虚拟机会在其它健康的主机上重新拉起并提供正常业务服务。若虚拟机已绑定外网 IP，智能调度系统会同时将外网 IP 地址及相关流表信息一起漂移至虚拟迁移后所在的物理主机，并保证网络通信可达。

- 支持平台管理员自定义外网 IP 资源池，即自定义外网 IP 网段，并支持配置网段的路由策略。租户申请网段的外网 IP 绑定至虚拟资源后，下发目的路由地址的流量自动以绑定的外网 IP 为网络出口。
- 外网 IP 网段支持下发默认路由和指定路由，下发默认路由代表默认所有流量均以绑定的外网IP为出口，指定路由为管理员指定目的地址的流量以绑定的外网IP为出口。
- 提供 IPv4/IPv6 双栈能力，管理员可自定义管理 IPv4 和 IPv6 网段资源池，并支持同时绑定 IPv4/IPv6 地址到虚拟机，为虚拟机提供双栈网络通信服务。**
- 支持外网 IP 网段的权限管控，可指定所有租户或部分租户使用，未被指定的租户无权限申请并使用网段 EIP。
- EIP 具有弹性绑定的特性，支持随时绑定至虚拟机、NAT 网关、负载均衡、VPN 网关等虚拟机资

源，并可随时解绑绑定至其它资源。

- 虚拟机支持绑定 10 个外网 IPv4 和 10 个外网 IPv6 地址，以第一个有默认路由的外网 IP 作为虚拟机的默认网络出口。
- 提供外网 IP 网段获取服务，支持租户手动指定 IP 地址申请 EIP，并提供 IP 地址冲突检测，方便用户业务网络地址规划。
- 平台管理员可自定义外网 IP 网段的带宽规格，租户可在带宽规格范围内配置外网 IP 的带宽上限。

外网 IP 具有数据中心属性，仅支持绑定相同数据中心的虚拟资源。用户可通过平台自定义申请 EIP，并对 EIP 进行绑定、解绑、调整带宽等相关操作。

8.2 申请外网 IP

申请 EIP 是指租户通过控制台从管理员自定义的外网 IP 网段中申请一个 IPv4 或 IPv6 的外网 IP 地址，并将 IP 地址绑定至虚拟机、负载均衡、NAT 网关、VPN 网关、MySQL 及 Redis 等资源，为虚拟资源提供外网访问能力。

申请 EIP 时需指定 IP 版本、所属网段、IP 地址、资源名称及带宽上限等信息，可通过导航栏进入【外网 IP】资源控制台，通过“申请外网 IP”进入向导页面，如下图所示：

1. 选择并配置所申请外网 IP 基础配置及管理设置信息：

- 名称/描述：申请外网 IP 的名称和描述，申请时必须指定名称。
- 计费方式：资源的计费方式，目前仅支持带宽计费，即以带宽作为计费对象和出口上限，不限制流量。
- IP 版本：外网 IP 地址的 IP 版本，支持 IPv4 和 IPv6。
 - 选择 IPv4 时，则网段仅展示 IPv4 的网段；
 - 选择 IPv6 时，则网段仅展示 IPv6 的网段，若平台管理员未定义 IPv6 网段，则 IP 版本仅支

持 IPv4。

- 网段：所申请外网 IP 的所属网段，由平台管理员自定义，同时会展示该网段的 IP 网段，手动指定的 IP 地址必须在网段 IP 地址范围内。
- IP 地址：用户手动指定 IP 地址申请 EIP，指定的 IP 地址必须在所选网段的 IP 范围内。
- 带宽：所申请 EIP 资源的带宽出口上限，规格范围由平台管理员自定义，单位为 Mbps。

2. 选择购买数量和付费方式，确认订单金额并点击“立即购买”进行 EIP 的申请和创建。

- 购买数量：按照所选配置及参数批量创建多个 EIP 地址，当前支持批量创建 10 个 EIP；
- 付费方式：选择 EIP 的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式；
- 合计费用：用户选择 EIP 资源按照付费方式的费用展示；
- 立即购买：点击立即购买后，会返回 EIP 资源列表页，在列表页可查看 EIP 的申请过程，通常会先显示“申请中”的状态，几秒内转换为“未绑定”状态，即代表申请成功。

8.3 查看外网 IP

通过导航栏进入外网 IP 控制台，可查看外网 IP 资源列表，并可通过列表上名称和 ID 进入详情页面查看外网 IP 的详细信息及操作日志等。

8.3.1 外网 IP 列表

外网 IP 列表可查看当前账户下所有 EIP 资源的列表信息，包括名称、资源 ID、IP、IP 版本、带宽、绑定资源、路由类型、计费方式、创建时间、过期时间、状态及操作项，如下图所示：

名称	资源ID	IP	IP版本	带宽	绑定资源	路由类型	计费方式	创建时间	过期时间	状态	操作
3434 修改名称及备注	eip-La4H287MR	1.234.0.0/24 BGP	IPv4	5Mb	(无)	默认路由	月	2020-07-20	2020-08-20	未绑定	<button>详情</button> <button>绑定</button> <button>解绑</button> <button>...</button>
2323 修改名称及备注	eip-F86-o0nMg	1.32.107.0/24 BGP2	IPv4	1Mb	234343 natgw-kPdftOnMg	默认路由	月	2020-07-17	2020-08-17	已绑定	<button>详情</button> <button>绑定</button> <button>解绑</button> <button>...</button>
erera a	eip-jI0tw0kZRH	1.5.234.0/24 BGP	IPv4	5Mb	cinder natgw-vy78XXpZRH	默认路由	月	2019-08-29	2020-07-29	已绑定	<button>详情</button> <button>绑定</button> <button>解绑</button> <button>...</button>

- 名称/ID：EIP 资源的名称及全局唯一标识符。
- IP 地址：EIP 资源的 IP 地址及网段名称，若 IP 版本为 IPv6 则显示为 IPv6 地址。
- IP 版本：EIP 地址的 IP 版本，如 IPv4 或 IPv6。
- 带宽：EIP 资源申请时指定的带宽出口上限。
- 绑定资源：EIP 已绑定的资源名称和资源 ID，资源类型可以为虚拟机、NAT 网关、负载均衡及 VPN 网关。
- 路由类型：EIP 地址所属网段定义的路由类型，包括默认路由和非默认路由（指定路由或未指定路由）。
 - 默认路由绑定至虚拟资源，会自动下发目标地址为 0.0.0.0/0 的路由，即默认路由；
 - 非默认路由绑定至虚拟资源，仅会下发用户指定目标地址的路由。
- 计费方式：EIP 地址的付费方式，包括按时、按年、按月。

- 创建时间/过期时间：EIP 资源的创建时间和费用过期时间。
- 状态：EIP 资源的状态，包括申请中、未绑定、绑定中、已绑定、解绑中、修改带宽中、删除中等状态。

列表上的操作项是指对单个外网 IP 地址的操作，包括绑定、解绑、修改带宽及删除等，可通过搜索框对外网 IP 列表进行搜索和筛选，支持模糊搜索。

为方便租户对资源的统计及维护，平台支持下载当前用户所拥有的所有外网 IP 资源列表信息为 Excel 表格；同时支持对外网 IP 进行批量解绑和批量删除操作。

8.3.2 外网 IP 详情

在外网 IP 资源列表上，点击名称或 ID 可进入概览页面查看当前外网 IP 的详细信息，同时可切换至操作日志页面查看当前外网 IP 的操作日志，如概览页所示：



- 基本信息：外网 IP 地址的基本信息，包括名称、ID、IP 地址、IP 版本、带宽、绑定资源、状态、创建时间及告警模板信息。
 - 可点击名称右侧按钮修改外网 IP 的名称和备注信息；
 - 可点击告警模板右侧按钮修改外网 IP 所关联的告警模板，默认会绑定 Default 告警模板。

 仅当外网 IP 被绑定至虚拟机资源时，才可修改告警模板。

- 监控信息：当前外网 IP 地址的监控信息，包括网卡出带宽使用率、出/入带宽及出/入包量。
- 操作日志：操作日志页面展示当前外网 IP 的操作日志。可提供自定义时间级别的日志展示，同时可对日志进行模糊搜索，默认提供两周内的操作日志，可通过切换日期周期查看不同时间周期的操作日志。

8.4 绑定外网 IP

绑定外网 IP 是指将 EIP 地址绑定至虚拟机、NAT 网关、负载均衡、VPN 网关或 Redis、MySQL 服务，为虚拟资源提供外网服务能力。

- 虚拟机支持绑定 10 个 IPv4 和 10 个 IPv6 外网 IP 地址，默认以第一个有默认路由的 IP 地址作为虚拟机的默认网络出口。

- 虚拟机绑定外网 IP 地址后，系统会将外网 IP 地址及所属网段下发路由直接配置至虚拟机自带的默认外网网卡，通过虚拟机操作系统可直接查看所有绑定至虚拟机的外网 IP 地址及相关路由信息。
- NAT 网关仅支持绑定一个外网 IPv4 地址，不支持绑定 IPv6 外网 IP 地址。
- VPN 网关仅支持绑定一个外网 IPv4 地址，不支持绑定 IPv6 外网 IP 地址。
- 负载均衡仅支持绑定一个外网 IPv4 地址，不支持绑定 IPv6 外网 IP 地址。

一个外网 IP 同时仅支持绑定一个虚拟资源，仅支持未绑定状态的外网 IP 进行绑定操作，且被绑定的资源必须处于运行中、有效或关机状态。用户可通过外网 IP 资源列表操作项的“绑定”进入外网 IP 绑定向导页面，进行资源绑定操作，如下图所示：



绑定时需选择被绑定资源的类型及绑定资源对象：

- 资源类型：指被绑定对象的资源类型，支持绑定给虚拟机、负载均衡、NAT 网关、VPN 网关。
- 资源对象：指被绑定的资源对象，不同的资源类型可选的资源对象不同。
 - 虚拟机：可根据虚拟机名称及内网 IP 地址选择需绑定的虚拟机资源，不可选择至已绑定 10 个 IPv4 或 10 个 IPv6 地址的虚拟机；
 - 负载均衡：可根据名称和 ID 选择需绑定的负载均衡资源，仅支持选择未绑定外网 IP 地址且类型为外网的负载均衡实例；
 - NAT 网关：可根据名称和 ID 选择需绑定的 NAT 网关资源，仅支持选择未绑定外网 IP 地址的 NAT 网关；
 - VPN 网关：可根据名称和 ID 选择需绑定的 VPN 网关资源，仅支持选择未绑定外网 IP 地址的 VPN 网关。

绑定过程中外网 IP 地址的状态为“绑定中”，待状态变更为“已绑定”即代表绑定成功，用户也可通过被绑定资源查看绑定外网 IP 地址的信息。通常绑定会即时完成，可通过 ping 外网 IP 或相关网络工具测试绑定是否生效。

8.5 解绑外网 IP

解绑外网 IP 是指将 EIP 地址从一个虚拟资源上分离出来，并可重新绑定至其它虚拟资源。仅支持解绑已绑定状态的外网 IP 资源。用户可通过外网 IP 列表操作项进行外网 IP 的解绑操作，如下图所示：



解绑时，外网 IP 的状态转换为“解绑中”，待外网 IP 地址的状态转为换“未绑定”，即代表解绑成功，被解绑的资源网络或服务可能会受到影响。

- 虚拟机的外网 IP 地址被解绑后，不会影响虚拟机本身的内网通信。若解绑的外网 IP 地址为虚拟机默认网络出口，则系统会自动选择下一个有默认路由的外网 IP 作为虚拟机的默认网络出口。
- NAT 网关的外网 IP 地址被解绑后，会影响 NAT 网关的网络服务，所有 SNAT 及 DNAT 服务失效，即加入 NAT 网关的虚拟机无法通过 NAT 网关访问外网或对外提供服务，需重新绑定一个外网 IP 地址才可正常生效。
- 负载均衡的外网 IP 地址被解绑后，会影响负载均衡的网络服务，用户无法通过原外网 IP 地址负载访问服务节点中部署的服务。
- VPN 网关的外网 IP 地址被解绑后，会影响 VPN 网关的网络服务，IPSecVPN 两端内网无法进行通信，需重新绑定外网 IP 地址，并在对端平台或数据中心 VPN 网关处修改对端网关的 IP 地址为新绑定的 EIP 才可正常进行连接。

8.6 调整带宽

调整带宽是指对一个外网 IP 的带宽上限进行升级或降级，以适应业务对带宽的不同需求。可调整的带宽规格由云平台管理员在管理控制台上自定义，不同外网 IP 资源池支持不同的带宽规格配置。

支持在线或离线调整带宽，即可在不停止服务的情况下实时调整外网 IP 的带宽，且不会影响已绑定资源的网络通信。根据不同的付费方式，带宽调整可能会对费用及生效时间产生影响。

- 按小时付费的弹性IP，升降带宽，下个付费周期生效；
- 按年，按月付费的弹性IP，升级带宽，即时生效，并自动补差价；
- 按年，按月付费的弹性IP，直到当前付费周期的最后一天才允许降级带宽，下个付费周期生效。

用户可通过外网 IP 资源列表操作项“调整带宽”进入修改向导页面，进行带宽调整，如下图所示：

调整外网弹性IP带宽

降低外网IP带宽，下个付费周期按新配置扣费。按小时付费的外网IP，升级带宽下个付费周期按新配置扣费；按年按月付费的外网IP，升级带宽即时生效，并按比例自动补差价。

资源ID *	eip-La4H287MR
资源名称 *	3434
带宽 *	<input type="text" value="100Mb"/> Mb <input type="button" value="5"/> <input type="button" value="▲"/> <input type="button" value="▼"/>
预计收费	0

修改带宽中 EIP 状态转换为“调整带宽中”，成功后转换为“未绑定”或“已绑定”状态。在私有云环境中，外网 IP 地址可以由“内网 IP 地址”模拟，即管理员在物理网络上为云平台下发的外网 IP 网段为一个 NAT 后的内网 IP 地址段，则外网 IP 地址的真正带宽，是控制在物理网络层面。

平台的带宽调整仅作为一个 IP 地址可通信的带宽上限，如果外网 IP 地址网段是作为与 IDC 数据中心物理网络进行纯内网通信时，可将带宽规格设置为内网最大带宽，如 10000Mbps。

8.7 修改告警模板

修改告警模板是对外网 IP 的监控数据进行告警的配置，通过告警模板定义的指标及阈值，可在外网 IP 相关指标故障及超过指标阈值时，触发告警，通知相关人员进行故障处理，保证外网 IP 网络通信正常。

修改告警模版

资源ID *	eip-La4H287MR
资源类型 *	外网弹性IP
告警模版 *	Default(template-9ox841nZ4) <input type="button" value="▼"/>

用户可点击外网 IP 详情概览页中告警模板右侧的按钮进行告警模板修改操作，在修改告警模板向导中选择新外网 IP 告警模板，点击确定立即生效。

仅当外网 IP 地址被绑定至虚拟资源后，才可进行告警模板的修改。

8.8 修改外网 IP 名称

修改外网 IP 资源的名称和备注，在任何状态下均可进行操作。可通过点击外网 IP 资源列表名称右侧的“编辑”按钮进行修改。

8.9 删除外网 IP

用户可在控制台删除账户内未绑定虚拟资源的外网 IP 地址，支持批量删除。仅支持删除未绑定状态的外网 IP 资源。被删除的外网 IP 会自动进入“回收站”，可进行恢复和彻底销毁等操作。

可通过外网 IP 列表操作项中的“删除”进行操作，如下图所示：



9 安全组

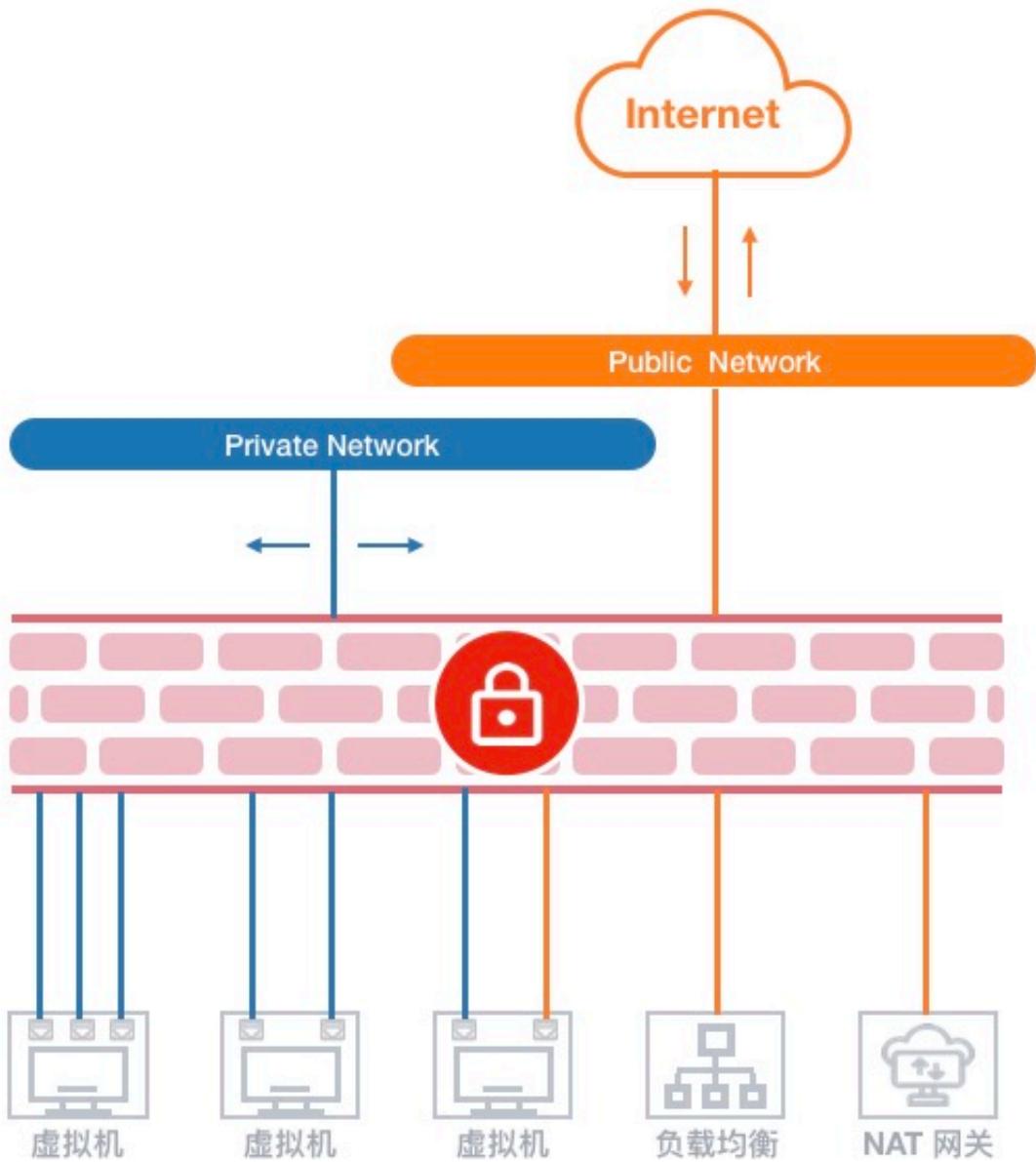
9.1 安全组简介

9.1.1 概述

安全组（Security Group）是一种类似 [IPTABLES](#) 的虚拟防火墙，提供出入双方向流量访问控制规则，定义哪些网络或协议能访问资源，用于限制虚拟资源的网络访问流量，支持 IPv4 和 IPv6 双栈限制，为云平台提供必要的安全保障。

平台安全组基于 Linux Netfilter 子系统，通过在 [OVS](#) 流表中添加流表规则实现，需开启宿主机 IPv4 和 IPv6 包转发功能。每增加一条访问控制规则会根据网卡作为匹配条件，生成一条流表规则，用于控制进入 OVS 的流量，保证虚拟资源的网络安全。

安全组仅可作用于同一个数据中心内具有相同安全需求的虚拟机、弹性网卡、负载均衡及 NAT 网关，工作原理如下图所示：



安全组具有独立的生命周期，可以将安全组与虚拟机、弹性网卡、负载均衡、NAT 网关绑定在一起，提供安全访问控制，与之绑定的虚拟资源销毁后，安全组将自动解绑。

- 安全组对虚拟机的安全防护针对的是一块网卡，即安全组是与虚拟机的默认虚拟网卡或弹性网卡绑定在一起，分别设置访问控制规则，限制每块网卡的出入网络流量；
- 如安全组原理图所示，安全组与提供外网 IP 服务的虚拟外网网卡绑定，通过添加出入站规则，对南北向（虚拟机外网）的访问流量进行过滤；
- 安全组与提供私有网络服务的虚拟网卡或弹性网卡绑定，通过添加出入站规则，控制东西向（虚拟机间及弹性网卡间）网络访问；
- 安全组与外网类型的负载均衡关联，通过添加出入站规则，可对进出外网负载均衡的外网 IP 流量进行限制和过滤，保证外网负载均衡器的流量安全；
- 安全组与 NAT 网关绑定，通过添加出入站规则，可对进入 NAT 网关的流量进行限制，保证 NAT 网关的可靠性和安全性；
- 一个安全组支持同时绑定至多个虚拟机、弹性网卡、NAT 网关及外网负载均衡实例；
- 虚拟机支持绑定一个内网安全组和一个外网安全组，分别对应虚拟机默认的内网网卡和外网网卡上，其中外网安全组对绑定至虚拟机的所有外网 IP 地址生效；
- 弹性网卡仅支持绑定一个安全组，与虚拟机默认网卡绑定的安全组相互独立，分别限制对应网卡的流量；

- 外网负载均衡和 NAT 网关实例仅支持绑定一个安全组，可更换安全组应用不同的网络访问规则。

创建虚拟机时必须指定外网安全组，支持随时修改安全组的出入站规则，新规则生成时立即生效，可根据需求调整安全组出/入方向的规则。支持安全组全生命周期管理，包括安全组创建、修改、删除及安全组规则的创建、修改、删除等生命周期管理。

9.1.2 安全组规则

安全组规则可控制允许到达安全组关联资源的入站流量及出站流量，提供双栈控制能力，支持对 IPv4/IPv6 地址的 TCP、UDP、ICMP、GRE 等协议数据包进行有效过滤和控制。

每个安全组支持配置多条规则，根据优先级对资源访问依次生效。规则为空时，安全组将默认拒绝所有流量；规则不为空时，除已生成的规则外，默认拒绝其它访问流量。

支持有状态的安全组规则，可以分别设置出入站规则，对被绑定资源的出入流量进行管控和限制。每条安全组规则由协议、端口、地址、动作、优先级及方向六个元素组成：

- 协议：支持 TCP、UDP、ICMPv4、ICMPv6 四种协议数据包过滤。
 - ALL 代表所有协议和端口，ALL TCP 代表所有 TCP 端口，ALL UDP 代表所有 UDP 端口；
 - 支持快捷协议指定，如 FTP、HTTP、HTTPS、PING、OpenVPN、PPTP、RDP、SSH 等；
 - ICMPv4 指 IPv4 版本网络的通信流量；ICMPv6 指 IPv6 版本网络的通信流量。
- 端口：源地址访问的本地虚拟资源或本地虚拟资源访问目标地址的 TCP/IP 端口。
 - TCP 和 UDP 协议的端口范围为 1~65535；
 - ICMPv4 和 ICMPv6 不支持配置端口。
- 地址：访问安全组绑定资源的网络数据包来源地址或被安全组绑定虚拟资源访问的目标地址。
 - 当规则的方向为入站规则时，地址代表访问被绑定虚拟资源的源 IP 地址段，支持 IPv4 和 IPv6 地址段；
 - 当规则的方向为出站规则时，地址代表被绑定虚拟资源访问目标 IP 地址段，支持 IPv4 和 IPv6 地址段；
 - 支持 CIDR 表示法的 IP 地址及网段，如 120.132.69.216、0.0.0.0/0 或 ::/0。
- 动作：安全组生效时，对数据包的处理策略，包括“接受”和“拒绝”两种动作。
- 优先级：安全组内规则的生效顺序，包括高、中、低三档规则。
 - 安全组按照优先级高低依次生效，优先生效优先级高的规则；
 - 同优先级的规则，优先生效精确规则。
- 方向：安全组规则所对应的流量方向，包括出站流量和入站流量。

安全组支持数据流表状态，规则允许某个请求通信的同时，返回数据流会被自动允许，不受任何规则影响。即安全组规则仅对新建连接生效，对已经建立的链接默认允许双向通信。如一条入方向规则允许任意地址通过互联网访问虚拟机外网 IP 的 80 端口，则访问虚拟机 80 端口的返回数据流（出站流量）会被自动允许，无需为该请求添加出方向允许规则。

注：通常建议设置简洁的安全组规则，可有效减少网络故障。

9.2 安全组管理

9.2.1 创建安全组

系统默认提供的安全组无法满足需求时，可指定安全组名称并添加相关安全组规则，快速创建一个属于用户独立的安全组，可关联或绑定至相关资源，为相关资源提供内网或外网的访问控制，保证网络访问的安全性。

用户可通过导航栏进入【安全组】资源控制台，通过“**创建安全组**”可进入安全组创建向导页面，如下图所示：

协议类型	端口	地址	动作	优先级	方向
TCP	80	0.0.0.0/0	接受	高	入
TCP	22	0.0.0.0/0	接受	高	入
TCP	53	::/0	接受	高	入

可根据向导页面的提示，选择并配置安全组名称，并根据需求配置安全组规则，包括协议类型、端口、地址、动作、优先级及方向等。

其中安全组名称指当前需要创建的安全组的名称标识。添加规则指增加安全组相应的入和出的流量规则，可批量增加多条，也可在安全组创建后在进行规则的添加。

- 协议：一条规则仅支持一种协议，可选择 ALL 或 ALL TCP、ALL UDP 等。
- 端口：端口可指定单个端口号或端口范围，端口范围的格式如 56-60。
- 地址：地址栏支持输入 IPv4 和 IPv6 地址，支持批量输入多个 IP 地址，多个地址间用逗号进行分隔。
- 动作：规则的协议、端口、地址及方向相同时，不支持同时配置接受和拒绝两种动作。
- 方向：规则的流量方向，包括入站和出站，一条规则仅支持选择一个方向。

点击确定后，自动返回至安全组列表页面，在列表页面可查看新建安全组的创建过程，待安全组的状态由“创建中”转换为“有效”时，即代表创建成功。

9.2.2 查看安全组

通过导航栏进入安全组资源控制台，可查看当前账户安全组资源列表，并可通过列表上安全组名称进入详情页面查看安全组基本信息、安全组规则及已绑定的资源等信息。

9.2.2.1 安全组列表

安全组列表页面可查看当前账户下安全组资源列表及相关信息，包括名称、ID、规则数量、绑定资源数量、创建时间、状态及操作项等，如下图所示：

The screenshot shows a table with columns: 名称 (Name), 资源ID (Resource ID), 规则数量 (Rule Count), 绑定资源数量 (Bound Resource Count), 创建时间 (Creation Time), 状态 (Status), and 操作 (Operations). The status column uses green dots to indicate '有效' (Effective). The operations column includes '详情' (Details), '编辑安全组' (Edit Security Group), and '删除' (Delete) buttons.

<input type="checkbox"/>	名称	资源ID	规则数量	绑定资源数量	创建时间	状态	操作
<input type="checkbox"/>	dff232323 修改名称及备注	sg-lkSj7gVGg	4	0	2020-07-23	● 有效	详情 编辑安全组 删除
<input type="checkbox"/>	test 修改名称及备注	sg-fqtW0G0ZR	4	2	2019-10-25	● 有效	详情 编辑安全组 删除
<input type="checkbox"/>	Default Default	sg-Ci9vkUvpm	8	4	2019-06-18	● 有效	详情 编辑安全组 删除

< 1 > 10 条/页

- 名称/ID：安全组的名称及全局唯一标识符；
- 规则数量：安全组已添加的安全组规则数量，以数字表示；
- 绑定资源数量：安全组已绑定的资源数量，以数字表示，未绑定时显示为 0；
- 创建时间：安全组的创建时间；
- 状态：安全组的运行状态，包括有效、创建中、删除中等；

列表上的操作项是可对单个安全组进行删除操作，支持安全组批量删除操作，可通过搜索框对安全组列表进行搜索和筛选，支持模糊搜索。

9.2.2.2 安全组详情

在安全组资源列表上，点击安全组名称可查看当前安全组的详情及安全组规则信息，同时可切换至资源页面查看当前安全组已绑定的资源信息，如下图概览页所示：

The screenshot shows two main sections: '基本信息' (Basic Information) and '安全组规则' (Security Group Rules).

基本信息:

资源ID	sg-fqtW0G0ZR
资源名称	test
规则数量	4
绑定资源数量	2
创建时间	2019-10-25 23:16:31

安全组规则:

<input type="checkbox"/>	协议类型	端口	地址	动作	优先级	方向	操作
<input type="checkbox"/>	ICMPv4	/	0.0.0.0/0	接受	高	出	编辑 删除
<input type="checkbox"/>	ICMPv4	/	0.0.0.0/0	接受	高	入	编辑 删除
<input type="checkbox"/>	ALL	/	0.0.0.0/0	接受	高	出	编辑 删除
<input type="checkbox"/>	ALL	/	0.0.0.0/0	接受	高	入	编辑 删除

< 1 > 10 条/页

- 基本信息：当前安全组的基本信息，包括名称、ID、规则数量、已绑定资源数量及创建时间等信息。
- 安全组规则管理：当前安全组的访问控制规则管理，包括添加、查看、编辑、删除等，详见[安全组规则管理](#)。
- 已绑定资源：当前安全组已绑定资源的列表信息，详见[已绑定资源](#)。

9.2.2.3 已绑定资源

已绑定资源指安全组已绑定资源的列表信息，可通过列表信息查看当前安全组已经绑定或关联的虚拟资源信息。用户可通过安全组详情页面进入“资源”子页面，查看已绑定的资源信息。

资源名称	资源ID	资源类型
OA	vm-Ls7CoF7Mg	虚拟机
234343	natgw-kPdft0nMg	NAT网关

10 条/页

如上图列表图所示，已绑定资源的列表信息包括资源名称、资源类型、资源ID等信息，其中资源类型包括虚拟机、弹性网卡、NAT 网关、负载均衡等。

9.2.3 修改安全组名称

修改安全组资源的名称和备注，在任何状态下均可进行操作。可通过点击安全组资源列表页面每个安全组名称右侧的“编辑”按钮进行修改。

9.2.4 删除安全组

支持用户删除未被任何资源绑定的安全组资源。安全组删除后，会被彻底销毁，删除前需保证安全组未被任何资源绑定或关联。可通过安全组列表页面操作项中的“删除”进行安全组的删除，如下图所示：



9.3 安全组规则管理

9.3.1 新建规则

为已绑定资源提供网络安全访问控制的主要手段是制定合理的安全组规则，每个安全组支持配置多条规则，根据优先级对资源访问依次生效。规则为空时，安全组将默认拒绝所有流量；规则不为空时，除已生成的规则外，默认拒绝其它访问流量。

用户可指定规则的协议类型、端口、地址、动作、优先级、方向等信息进行规则的添加，通过安全组详情页面的“新建规则”即可进入新建规则向导页面，具体操作与[创建安全组](#)中的添加规则相同，可根据具体业务网络安全控制需求，新建安全组规则。

9.3.2 查看规则

通过安全组详情页面的规则列表可查看当前安全组已生成的规则信息，并可通过列表的操作项对已有规则进行编辑和删除等操作。规则列表信息包括协议类型、端口、地址、动作、优先级、方向及操作项等，如下图所示：

协议类型	端口	地址	动作	优先级	方向	操作
TCP	22	0.0.0.0/0	接受	高	入	<button>编辑</button> <button>删除</button>
TCP	53	::/0	接受	高	入	<button>编辑</button> <button>删除</button>
TCP	56-60	0.0.0.0/0	接受	高	入	<button>编辑</button> <button>删除</button>
TCP	80	0.0.0.0/0	接受	高	入	<button>编辑</button> <button>删除</button>

Page: 1 / 1 | 10 条/页

9.3.3 编辑规则

已有安全组规则不能满足业务需求时，可通过安全组规则列表操作项中的“编辑”进行修改及变更操作，修改项与新建规则时指定的参数相同，可根据实际情况修改指定参数。

- 当协议类型为 ALL 或 ICMPv4/ICMPv6 时，端口不可选择并显示为“/”；
 - 地址支持 IP 地址和 CIDR IP 网段格式，若需指定所有 IP 地址可配置为 0.0.0.0/0 或 ::/0。
- 规则编辑后即时生效，同时会对已绑定的资源网络访问产生影响，请慎重操作。

9.3.4 删除规则

已有安全组规则需被删除时，可通过安全组规则列表操作项中的“删除”操作，删除的规则会被即时销毁。为避免影响业务，建议删除前确认安全组规则是否有必要删除。删除安全组规则后，安全组信息中的规则数量会重新统计，显示最新的规则数量。

10 负载均衡

10.1 负载均衡简介

10.1.1 概述

负载均衡（Load Balance）是由多台服务器以对称的方式组成一个服务器集合，每台服务器都具有等价的地位，均可单独对外提供服务而无须其它服务器的辅助。平台负载均衡服务（简称 ULB—UCloudStack Load Balance）是基于 TCP/UDP/HTTP/HTTPS 协议将网络访问流量在多台虚拟机间自动分配的控制服务，类似于传统物理网络的硬件负载均衡器。

通过平台负载均衡服务提供的虚拟服务地址，将相同数据中心、相同 VPC 网络的虚拟机添加至负载均衡转发后端，并将加入的虚拟机构建为一个高性能、高可用、高可靠的应用服务器池，根据负载均衡的转发规则，将来自客户端的请求均衡分发给服务器池中最优的虚拟机进行处理。

支持内外网两种访问入口类型，分别提供 VPC 内网和 EIP 外网的负载访问分发，适应多种网络架构及高并发的负载应用场景。提供四层和七层协议的转发能力及多种负载均衡算法，支持会话保及健康检查等特性，可自动隔离异常状态虚拟机，同时提供 **SSL Offloading** 及 SSL 证书管理能力，有效提高整体业务的可用性及服务能力。

ULB 支持收集并展示负载流量各种网络指标的监控数据，并可根据告警模板进行监控报警及通知，保证业务的正常运行。当前负载均衡为接入的虚拟机服务池提供基于 NAT 代理的请求分发方式，在 NAT 代理模式下，所有业务的请求和返回数据都必须经过负载均衡，类似 LVS 的 NAT 工作模式。

10.1.2 应用场景

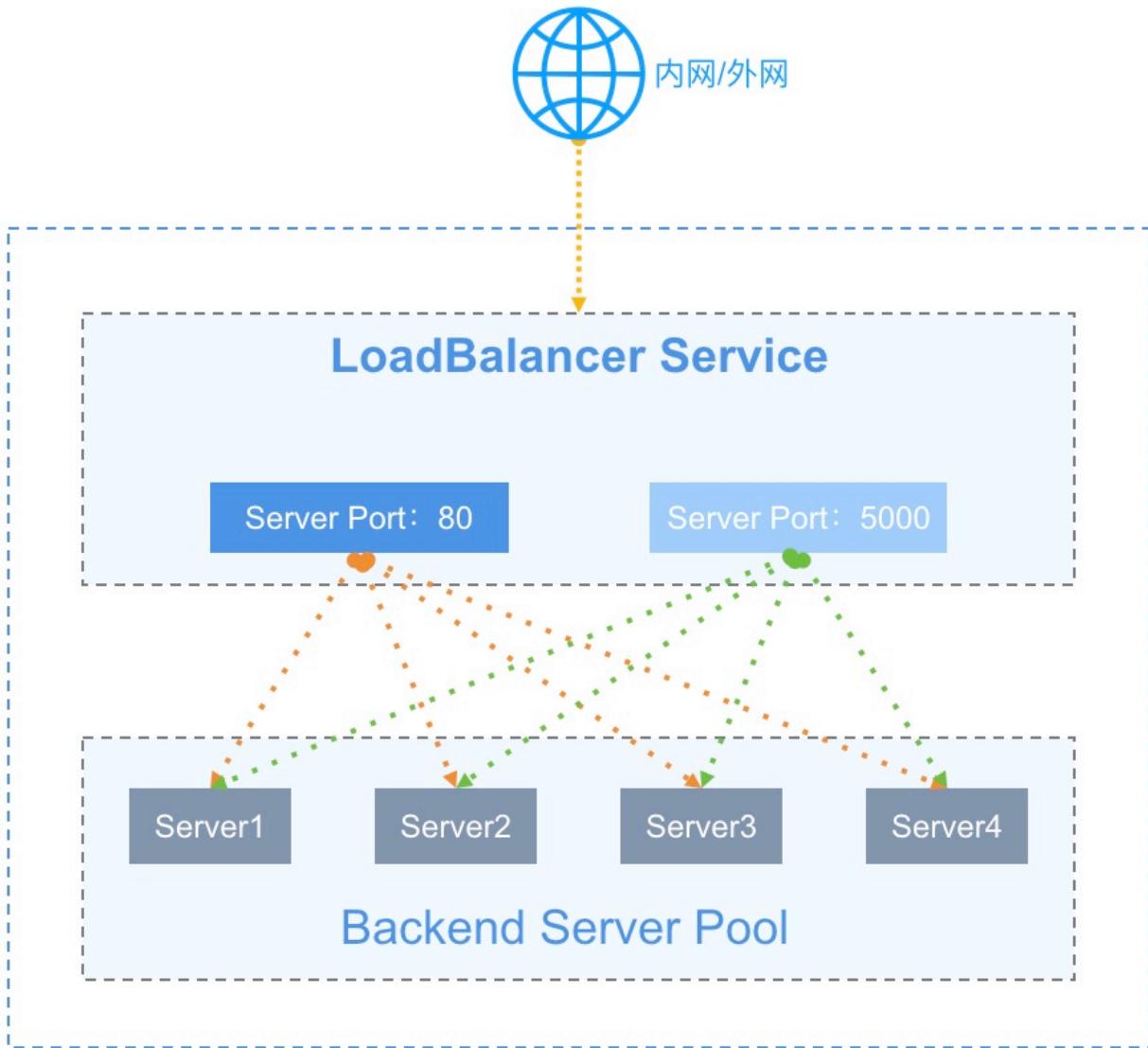
平台提供外网和内网两种类型的负载均衡服务，分别对应外网服务和内网服务两种场景。用户可根据业务需求，选择创建对外公开或对内私有的负载均衡实例，平台会根据负载均衡类型分别分配外网 IP 地址或 VPC 私有网络的 IP 地址，即负载均衡的服务访问地址。

- 外网类型的负载均衡使用场景：
 - 部署在平台的业务服务需要构建高可用虚拟机集群，且需对互联网提供统一访问入口。
 - 部署在平台的业务服务需要构建高可用虚拟机集群，且需对 IDC 数据中心提供统一访问入口。
- 内网负载均衡使用场景：
 - 部署在平台的业务服务需要构建高可用虚拟机集群，且仅需对 VPC 内网提供统一访问入口。
 - 部署在 VPC 私有网络的虚拟机集群需要对其他用户或服务屏蔽真实 IP 地址，对客户端提供透明化服务。

用户也可将负载均衡服务分配的 IP 地址与自有域名绑定在一起，通过域名访问后端应用服务。

10.1.3 架构原理

一个提供服务的负载均衡，主要由 LB 实例（LoadBalancer）、虚拟服务器（VServer）、后端服务器（Backend Real Server）三部分组成。如架构图所示：



- LoadBalancer (LB) : 负载均衡实例为主备高可用集群架构，可实现负载均衡器故障自动切换，提高接入负载均衡服务的可用性。同时结合内外网 IP 地址，根据 VServer 配置的监听器，将虚拟机加入到 Backend 成为 Real Server，以实现业务的流量均衡与服务容错。
- Virtual Server (VServer) : 监听器，每个监听器是一组负载均衡的监听端口配置，包含协议、端口、负载算法、会话保持、连接空闲超时及健康检查等配置项，用于分发和处理访问 LB 的请求。
- Backend Server Pool : 后端一组虚拟机服务器池，实际处理请求的真实服务器 (RealServer)，即真实部署业务的虚拟机实例。
- 外网 IP (EIP) : 外网弹性 IP 地址，绑定至外网类型的 LB 实例上，对互联网或 IDC 数据中心提供业务负载均衡访问入口。
- 内网 IP (Private IP) : 内网 IP 地址，内网类型 LB 实例提供服务的访问地址，通常是由创建内网负载均衡器时指定的 VPC 自动分配。

负载均衡器用于承载 VServer 及访问入口，VServer 负责访问入口地址的端口监听及请求分发。当负载均衡器接受到来自客户端的请求后，会通过一系列负载均衡算法，将访问请求路由分发到后端虚拟机服务器池进行请求处理，同时由 VServer 将处理结果返回给客户端。

- 通过加权轮询、最小连接数及基于源地址的负载均衡调度策略，进行业务请求流量转发，满足多场景业务负载需求，如加权轮询是按照后端服务器的权重进行请求转发，权重越大转发的请求越多。
- 通过会话保持机制，在请求会话的生命周期内，会将来自同一个客户端的会话转发至同一个虚拟机

进行处理，适用于 TCP 长连接等应用场景。

- 通过健康检查机制，监控 RealServer 的运行状况及业务可用性，确保只将流量分发至业务健康的虚拟机。当后端虚拟机业务不可访问时，调度器会停止向虚拟机分发负载流量；待虚拟机业务恢复正常后，会将虚拟机重新加入至 VServer 后端并分发流量至虚拟机。

负载均衡器的工作模式为 **NAT** 请求代理，请求和返回均由负载均衡器进行转发和处理，即后端 RealServer 虚拟机处理请求后，会将请求返回给负载均衡，由负载均衡将结果返回给客户端。

10.1.4 功能特性

平台负载均衡服务提供四层和七层转发能力，支持内网和外网两种网络入口，在多种负载调度算法基础之上支持健康检查、会话保持、连接空闲超时、内容转发及 **SSL Offloading** 和 SSL 证书管理等功能，保证后端应用服务的可用性和可靠性。

- 支持内网和外网两种类型负载均衡器，满足 VPC 内网、IDC 数据中心及互联网服务负载均衡应用场景。
- 提供四层和七层业务负载分发能力，支持基于 TCP、UDP、HTTP 及 HTTPS 协议的监听及请求转发。
- 支持加权轮询、最小连接数和基于源地址的的负载调度算法，满足不同场景的流量负载业务。
 - 加权轮询：基于权重的轮询调度，负载均衡器接收到新的访问请求后，根据用户指定的权重，按照权重概率分发流量至各后端虚拟机，进行业务处理；
 - 最小连接数：基于后端服务器最小连接数进行调度，负载均衡器接收到新的访问请求后，会实时统计后端服务器池的连接数，选择连接数最低的虚拟机建立新的连接并进行业务处理；
 - 源地址：基于客户端源 IP 地址的调度策略，采用哈希算法将来源于相同 IP 地址的访问请求均转发至一台后端虚拟机进行处理。
- 提供会话保持功能，在会话生命周期内，保证同一个客户端的请求转发至同一台后端服务节点上。四层和七层分别采用不同的方式进行会话保持。
 - 针对 UDP 协议，基于 IP 地址保证会话保持，将来自同一 IP 地址的访问请求转发到同一台后端虚拟机进行处理，支持关闭会话 UDP 协议的会话保持；
 - 针对 HTTP 和 HTTPS 协议，提供 Cookie 植入的方式进行会话保持，支持自动生成 KEY 和自定义 KEY。自动生成 KEY 是由平台自动生成 Key 进行植入，自定义 Key 是由用户自定义 Key 进行植入。
- 支持 TCP、HTTP 及 HTTPS 协议的连接空闲超时配置，自动中断在超时时间内一直无访问请求的连接。
 - 客户端向 LB 地址发送的请求，在平台会维护两个连接，一个由客户端到 LB，一个由 LB 到后端虚拟机；
 - 连接空闲超时是指由客户端到 LB 的连接空闲超时，若在超时周期内没有发送或接收任何数据，将自动中断从客户端到 LB 的连接；
 - 默认连接空闲超时周期为 60 秒，即在建立连接后的 60 秒内一直没有新的数据请求，将自动中断连接。
- 健康检查：支持端口检查和 HTTP 检查，根据规则对后端业务服务器进行业务健康检查，可自动检测并隔离服务不可用的虚拟机，待虚拟机业务恢复正常后，会将虚拟机重新加入至 VServer 后端并分发流量至虚拟机。
 - 端口检查：针对四层和七层负载均衡，支持按 IP 地址 + 端口的方式探测后端服务节点的健康状况，及时剔除不健康的节点；
 - HTTP 检查：针对七层负载均衡，支持按 URL 路径和请求 HOST 头中携带的域名进行健康检

查，筛选健康节点。

- 内容转发：针对七层 HTTP 和 HTTPS 协议的负载均衡，支持基于域名和 URL 路径的流量分发及健康检查能力，可将请求按照域名及路径转发至不同的后端服务节点，提供更加精准的业务负载均衡功能。
- SSL 证书：针对 HTTPS 协议，提供统一的证书管理服务和 **SSL offloading** 能力，并支持 HTTPS 证书的单向和双向认证。SSL 证书部署至负载均衡，仅在负载均衡上进行解密认证处理，无需上传证书到后端业务服务器，降低后端服务器的性能开销。
- 获取客户端真实 IP：HTTP 监听器支持附加 HTTP header 字段，通过 X-Forwarded-For 和 X-Real-IP 获取客户端真实 IP 地址。
- 获取监听器协议：HTTP 监听器支持附加 HTTP header 字段，通过 X-Forwarded-Proto 获取监听器的协议。
- 附加 HTTP HOST：HTTP 监听器支持附加 HTTP header 字段，通过 Host 附加 HOST 域名至 HTTP 请求中，用于适配需要检测 HTTP 头 HOST 字段的业务。
- 监控数据：负载均衡级别提供每秒连接数、每秒出/入流量、每秒出/入包数量的监控及告警；VServer 级别提供连接数、HTTP 2XX、HTTP 3XX、HTTP 4XX、HTTP 5XX 等监控数据及告警。
- 安全控制：通过安全组对外网负载均衡的访问进行安全管控，仅允许安全组规则内的流量透传负载均衡到达后端真实服务器，保证业务负载的安全性。

负载均衡为用户提供业务级别的高可用方案，可以将业务应用同时部署至多个虚拟机中，通过负载均衡和 DNS 域名的方案设置流量均衡转发，实现多业务级别的流量负载均衡。当大并发流量通过负载均衡访问虚拟机业务时，可通过最小连接数、加权轮询等算法，将请求转发给后端最健壮的虚拟机进行处理，请通过负载均衡将请求结果返回给客户端，保证业务可用性和可靠性。

用户可通过智能 DNS 服务，将两个数据中心的负载均衡实例同时绑定至一个域名，使用 DNS 实现跨数据中心的业务容灾方案。

10.1.5 负载均衡隔离性

- 资源隔离
 - 负载均衡具有数据中心属性，不同数据中心间负载均衡资源物理隔离；
 - 负载均衡资源在租户间相互隔离，租户可查看并管理账号及子账号下所有负载均衡资源；
 - 一个租户内的负载均衡资源，仅支持绑定租户内同数据中心的 VPC 子网资源；
 - 一个租户内的负载均衡资源，仅支持绑定租户内同数据中心的外网 IP 资源；
 - 一个租户内的负载均衡资源，仅支持绑定租户内同数据中心的安全组资源。
- 网络隔离
 - 不同数据中心间负载均衡资源网络相互物理隔离；
 - 同数据中心负载均衡网络采用 VPC 进行隔离，不同 VPC 的负载均衡资源无法相互通信；
 - 负载均衡绑定的外网 IP 网络隔离取决于用户物理网络的配置，如不同的 Vlan 等。

10.2 负载均衡管理

10.2.1 使用流程

在使用负载均衡服务前，需根据业务需求规划负载均衡的网络类型及监听类型，并根据业务需求在平台部署并配置好业务虚拟机，具体流程如下：

- 根据业务需求和规划，在平台创建并部署多台业务虚拟机，并保证业务在单台虚拟机的可用性；
- 根据业务需求，选择负载均衡的网络入口类型及所属 VPC，在云平台部署高可用负载均衡实例；
- 在已创建的负载均衡实例中，根据需求配置监听器 VServer，包括服务的协议、端口、负载均衡算法、证书、会话保持及健康检查等参数；
- 为已配置的 VServer 添加服务节点来确定负载均衡入口请求路由的目标，即将第 1 步部署的业务虚拟机实例添加至 VServer 的服务节点；
- 负载均衡会对添加至 VServer 的服务节点立即进行业务健康检查，并及时剔除不健康的服务节点；
- 通过负载均衡服务提供的统一入口 IP 地址访问业务服务。

10.2.2 创建负载均衡

用户在平台创建负载均衡需指定所属集群类型、网络类型、VPC 网络、子网、外网 IP 及安全组等信息，可通过导航栏进入【负载均衡】资源控制台，通过“创建负载均衡”进入向导页面，如下图所示：

The screenshot shows the 'Create Load Balancer' wizard page. The first step, 'Basic Configuration', is selected. The configuration fields are as follows:

- Machine Type ***: High-performance (x86_64) is selected.
- Network Type ***: External network is selected.
- VPC ***: vpc002 (10.0.0.0/16) is selected.
- Subnet ***: 10.192 (10.0.192.0/20) is selected. A note indicates there are 4082 remaining IP addresses.
- External IP ***: 2323 (120.132.107.202) is selected. A note specifies it only supports IPv4 version and has a default gateway.
- Security Group ***: dff232323 (sg-lkSj7gVGg) is selected.

The second step, 'Management Information', is shown below:

- Instance Name ***: An empty input field.
- Remarks**: An empty input field.

本文以创建外网类型的负载均衡进行描述，内网类型的负载均衡无需指定外网 IP 和安全组信息。

1. 选择并配置负载均衡器的基础配置及网络信息：

- 机型：负载均衡实例所在宿主机的集群类型，由平台管理员自定义（如 x86 机型）。
- 网络类型：负载均衡实例网络入口的类型，可选择内网和外网。内网类型提供所属 VPC 的网络入口地址，外网类型以绑定的外网 IP 地址为负载均衡的网络入口地址。
- VPC 网络：负载均衡所服务的 VPC 网络，仅支持将相同 VPC 网络的虚拟机加入到负载均衡服务节点中提供负载均衡服务，同时负载均衡实例本身会运行在所指定的 VPC 网络中。
- 子网：负载均衡实例所在子网，系统将自动根据所选子网分配内网 IP 地址作为内网负载均衡的入

口地址，通常建议选择可用 IP 数量充足的子网。

- 外网 IP：当网络类型为外网时，可配置负载均衡实例自动绑定的外网 IP 地址，仅支持绑定 IPv4 且有默认路由的外网 IP 地址作为负载均衡的入口地址。
- 安全组：当网络类型为外网时，可配置负载均衡自动绑定的外网安全组，用于外网访问负载均衡的安全控制。
- 实例名称/备注：负载均衡实例的名称及备注信息。

2. 选择购买数量和付费方式，确认订单金额并点击“立即购买”进行负载均衡实例的创建。

- 购买数量：按照所选配置及参数批量创建多个负载均衡实例，一次仅支持创建 1 个负载均衡实例；
- 付费方式：选择负载均衡的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式；
- 合计费用：用户选择负载均衡资源按照付费方式的费用展示；

确认订单无误后点击立即购买，点击立即购买后，会返回负载均衡资源列表页，在列表页可查看资源的创建过程，通常会先显示“创建中”的状态，分钟内转换为“有效”状态，即代表创建成功。

10.2.3 查看负载均衡

通过导航栏进入负载均衡控制台，可查看负载均衡资源列表，并可通过列表上名称和 ID 进入详情页面查看负载均衡的概览及监控信息，同时可切换至 VServer 标签页对负载均衡的 VServer 进行管理。

10.2.3.1 负载均衡列表

负载均衡列表可查看当前账户下所有负载均衡资源信息，包括名称、资源 ID、IP、VPC、子网、VServer 数量、创建时间、过期时间、计费方式、状态及操作项，如下图所示：

The screenshot shows the 'Load Balancer' management interface. At the top, there are tabs for 'Load Balancer' (selected), 'SSL Certificate', and a search bar. Below the tabs is a toolbar with buttons for 'Create Load Balancer' and 'Delete Load Balancer'. The main area is a table listing load balancers:

名称	资源ID	IP	VPC	子网	VServer数量	创建时间	过期时间	计费方式	状态	操作
niwang 修改名称及备注	lb-5SsLxd4MR	(内) 10.0.192.22	vpc002 vpc-SX33TjgMR	10.192 subnet-b3VqT...	0 管理	2020-07-27	2020-08-27	月	● 有效	[详情] [删除] [...]
lb001 修改名称及备注	lb-IRu29DVMR	(外) 106.75.234.74	vpc002 vpc-SX33TjgMR	10.192 subnet-b3VqT...	0 管理	2020-07-27	2020-08-27	月	● 有效	[详情] [删除] [...]

At the bottom right of the table, there are navigation buttons for page numbers and a dropdown for '10 条/页'.

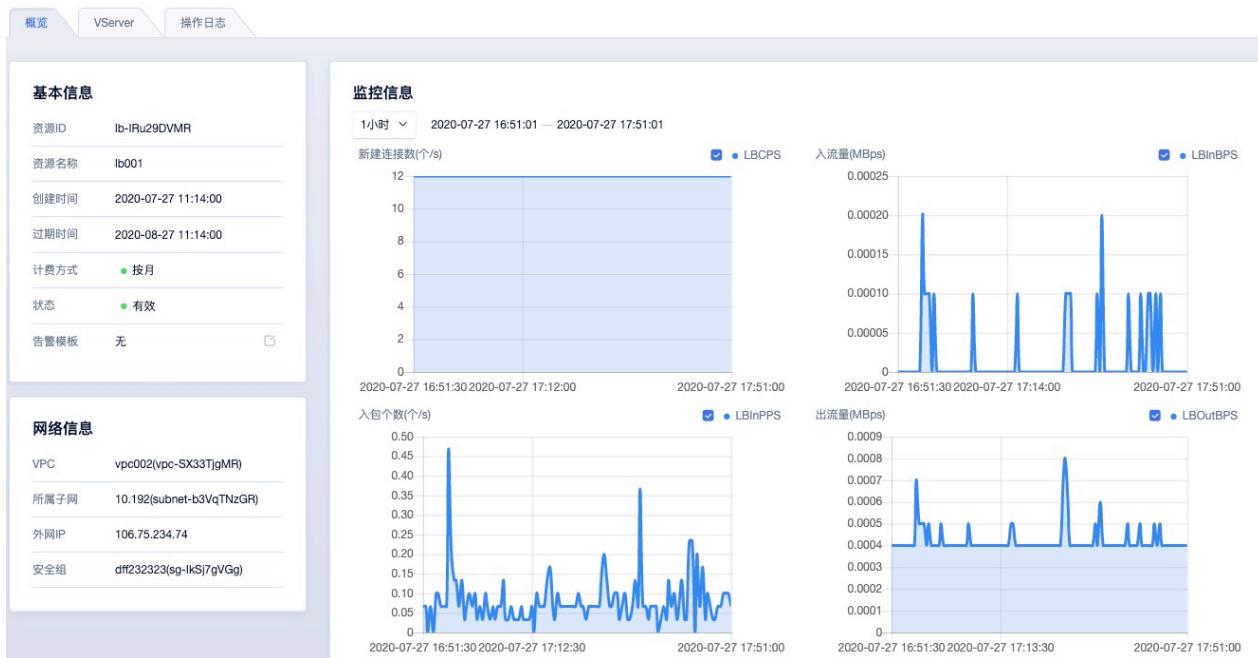
- 名称/ID：负载均衡的名称及全局唯一标识符。
- IP 地址：负载均衡对外提供服务的访问地址，网络类型为内网时为所属子网自动分配的 IP 地址，网络类型为外网时为所绑定的外网 IP 地址。
- VServer 数量：负载均衡实例上已创建的监听器 VServer 数量。
- 创建时间/过期时间：负载均衡的创建时间及费用过期时间。
- 计费方式：负载均衡创建时指定的计费方式。
- 状态：负载均衡的运行状态，包括创建中、有效、删除中等。

列表上操作项是指对单个负载均衡实例的操作，包括删除、修改告警模板、修改安全组等，可通过搜索框对负载均衡资源列表进行搜索和筛选，支持模糊搜索。

为方便租户对资源的统计及维护，平台支持下载当前用户所拥有的所有负载均衡资源列表信息为 Excel 表格；同时支持对负载均衡进行批量删除操作。

10.2.3.2 负载均衡详情

在负载均衡资源列表上，点击“名称”可进入概览页面查看当前负载均衡实例的详细信息，同时可切换至 VServer 页面对当前负载均衡的 VServer 监听器进行管理，如概览页所示：



(1) 基本信息

负载均衡器的基本信息，包括资源 ID、名称、创建时间、过期时间、计费方式、状态及告警模板信息，可点击告警模板右侧按钮修改负载均衡所关联的告警模板。

(2) 网络信息

负载均衡的网络入口相关信息，包括 VPC 网络、子网及内网 IP 地址，若负载均衡为外网类型，会展示外网 IP 地址及所绑定的安全组信息。

(3) 监控信息

负载均衡实例相关的监控图表及信息，包括新建连接数、出/入流量及出/入包数量，支持查看 1 小时、6 小时、12 小时、1 天及自定义时间的监控数据。

(4) VServer 管理

当前负载均衡的监听器生命周期管理，包括 VServer 的添加、查看、修改、删除操作管理，同时还可对 VServer 的后端服务节点及七层内容转发规则进行管理，详见 [VServer 管理](#)。

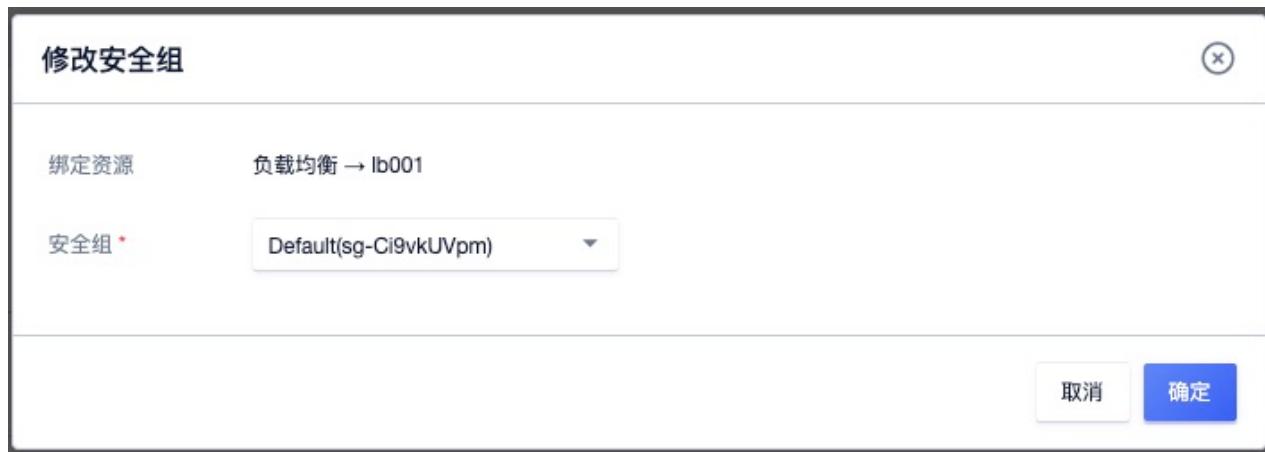
10.2.4 修改告警模板

修改告警模板是对负载均衡器的监控数据进行告警的配置，通过告警模板定义的指标及阈值，可在负载均衡相关指标故障及超过指标阈值时，触发告警，通知相关人员进行故障处理，保证负载均衡及业务的网络通信。

用户可通过负载均衡列表或详情概览页的操作项进行告警模板修改操作，在修改告警模板向导中选择新负载均衡告警模板进行修改。

10.2.5 修改安全组

支持在负载均衡的视角修改安全组，仅当负载均衡实例的网络类型为外网时才可修改负载均衡的安全组。可通过负载均衡列表操作项中的“修改安全组”进行修改操作，如下图所示：



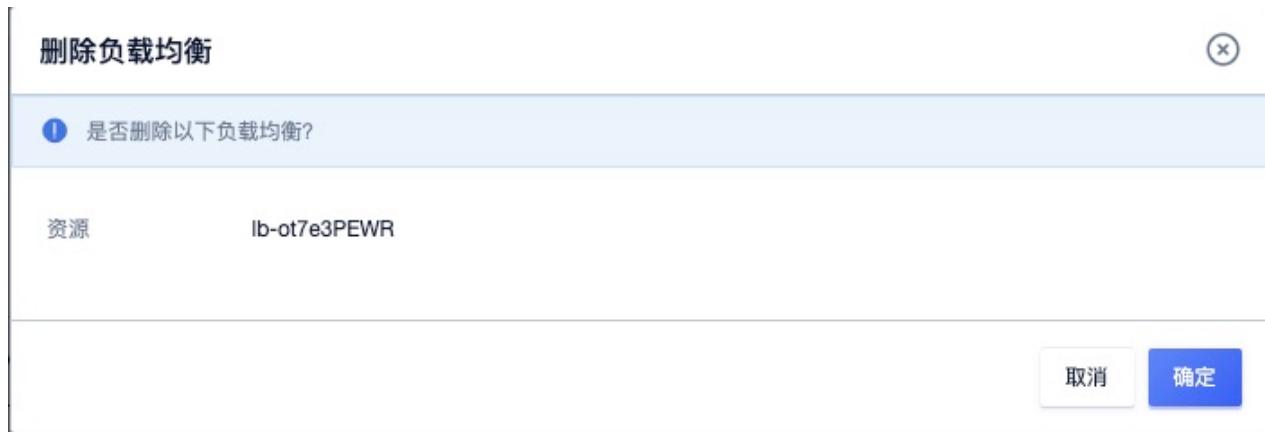
一个负载均衡仅支持绑定一个安全组，修改成功后外网负载均衡会以新的安全组策略对进出流量进行限制，用户可通过负载均衡详情网络信息查看已绑定的安全组信息。

10.2.6 修改名称和备注

修改负载均衡资源的名称和备注，在任何状态下均可进行操作。可通过点击负载均衡资源列表页面每个负载均衡名称右侧的“编辑”按钮进行修改。

10.2.7 删除负载均衡

用户可通过控制台或 API 的方式删除不需要的负载均衡实例，删除负载均衡时会自动解绑已关联的外网 IP、后端服务节点及绑定的 SSL 证书，并清除负载均衡已创建的 VServer 监听器及内容转发规则策略。



负载均衡实例删除即被直接销毁，删除前需确保负载均衡无业务流量请求，否则可能影响业务的正常访问。

10.3 VServer 管理

VServer 即负载均衡的监听器，主要承载负载均衡业务网络的四层和七层监听，通过负载均衡 IP 地址的请求仅能访问被监听的协议和端口，并根据调度算法定义的转发策略将请求流量分发至后端服务节点。

用户可对监听器进行添加、修改、删除、查看管理，同时可对 VServer 的后端服务节点及七层内容转发规则进行管理。针对每一个 VServer 监听器，用户可对监听协议、端口、负载均衡算法、会话保持及健康检查进行配置，若协议为 HTTP 或 HTTPS，可进行七层内容转发或 SSL 证书的配置和管理。一个负载均衡支持多个 VServer 监听器，每个监听器对应一个应用负载均衡服务。

10.3.1 添加 VServer

添加 VServer 是指为一个负载均衡器添加监听器，用于对负载均衡的 IP 地址进行服务监听，使用户可通过负载均衡的 IP 地址进行业务负载访问。支持用户根据应用需求，分别创建 TCP、UDP、HTTP、HTTPS 协议的监听器，如为负载均衡器添加一个 `HTTP:80` 的 VServer 监听器，基于负载均衡提供高可用 WEB 服务。

- TCP 监听器：基于 TCP 协议的监听器，即仅监听 TCP 的端口，适用于注重可靠性，对数据准确性要求高，如文件传输 FTP、发送或接收邮件 SMTP&POP3、远程登录 22/3389 等。
- UDP 监听器：基于 UDP 协议的监听器，关注实时性而相对不注重可靠性的场景，如 DNS 应用等。
- HTTP 监听器：基于 HTTP 协议及内容转发策略的监听器，适用于 WEB 服务及应用服务。
- HTTPS 监听器：基于 HTTPS 及证书加密的监听器，适用于加密传输的应用服务。

10.3.1.1 添加 TCP 监听器

用户为负载均衡实例创建一个基于 TCP 协议的监听器，提供注重可靠性的负载均衡服务，本文以创建 `TCP:23` (Telnet) 服务为例进行创建。用户可通过负载均衡详情页面 VServer 左侧导航栏的【添加】进入 VServer 监听器的创建向导页面，如下图所示：



根据向导页面配置 VServer 监听器，包括协议、端口、负载均衡算法、连接空闲超时及健康检查：

- 监听协议：负载均衡业务的网络协议，支持 TCP、UDP、HTTP、HTTPS，本示例中选择 TCP。
- 端口：负载均衡业务对外或对内提供服务时用来接收请求的应用端口，端口范围为 `1~65535`，本示例使用 23 端口，用于提供高可用的 Telnet 服务。

323、9102、9103、9104、9105、60909、60910 等端口被占用，在任何协议下均不可使用。

- 负载均衡算法：负载均衡分发请求到后端 RealServer 的调度计算策略，支持加权轮询、最小连接数和源地址三种算法。
- 连接空闲超时：客户端至负载均衡的连接空闲超时限制，范围为 1~86400 秒。默认值为 60 秒，即在 60 秒内客户端对负载均衡一直无访问请求，平台会自动中断连接。
- 健康检查：根据规则对后端服务节点进行健壮性检查，可自动检测并隔离服务不可用的后端服务节点。TCP 协议仅支持端口检查，即通过 IP:端口的方式检测业务的可用性。

创建过程中 VServer 的资源状态为“创建中”，待状态更新为“运行”即代表创建成功，用户可通过 VServer 列表及详情查看已添加的 TCP 监听器，并可查看 VServer 下所有服务节点的健康状态。

10.3.1.2 添加 UDP 监听器

用户为负载均衡实例创建一个基于 UDP 协议的监听器，提供基于 UDP 协议的负载均衡业务服务，本文以创建 UDP:53 (DNS) 服务为例进行创建。用户可通过负载均衡详情页面 VServer 左侧导航栏的【添加】进入 VServer 监听器的创建向导页面，如下图所示：



根据向导页面配置 VServer 监听器，包括协议、端口、负载均衡算法、会话保持及健康检查：

- 监听协议：负载均衡业务的网络协议，支持 TCP、UDP、HTTP、HTTPS，本示例中选择 UDP。
- 端口：负载均衡业务对外或对内提供服务时用来接收请求的应用端口，端口范围为 1~65535，本示例使用 53 端口，用于提供高可用的 DNS 服务。

323、9102、9103、9104、9105、60909、60910 等端口被占用，在任何协议下均不可使用。

- 负载均衡算法：负载均衡分发请求到后端 RealServer 的调度计算策略，支持加权轮询和源地址三种算法。

- 会话保持：针对 UDP 协议，基于 IP 地址保证会话保持，将来自同一 IP 地址的访问请求转发到同 一台后端虚拟机进行处理，可选择开启或关闭 UDP 协议的会话保持功能。
- 健康检查：根据规则对后端服务节点进行健壮性检查，可自动检测并隔离服务不可用的后端服务节 点。UDP 协议仅支持端口检查，即通过 IP:端口的方式检测业务的可用性。

创建过程中 VServer 的资源状态为“创建中”，待状态更新为“运行”即代表创建成功，用户可通过 VServer 列表及详情查看已添加的 UDP 监听器，并可查看 VServer 下所有服务节点的健康状态。

10.3.1.3 添加 HTTP 监听器

用户为负载均衡实例创建一个基于 HTTP 协议的监听器，提供基于 HTTP 协议的负载均衡业务服务，本文以创建 `HTTP:80` (WEB) 服务为例进行创建。用户可通过负载均衡详情页面 VServer 左侧导航栏的【添加】进入 VServer 监听器的创建向导页面，如下图所示：

创建 VServer	
LB	lb-IRu29DVMR
协议 *	HTTP
端口 *	80
负载均衡算法 *	hash
会话保持 *	关闭 自动生成KEY 自定义KEY
会话保持KEY *	testabc
连接空闲超时 *	60 S
健康检查 *	端口检查 HTTP检查
HTTP检查域名	
HTTP检查路径 *	/
<input type="button" value="取消"/> <input type="button" value="确认"/>	

根据向导页面配置 VServer 监听器，包括协议、端口、负载均衡算法、会话保持、连接空闲超时及健康 检查：

- 监听协议：负载均衡业务的网络协议，支持 TCP、UDP、HTTP、HTTPS，本示例中选择 HTTP。
- 端口：负载均衡业务对外或对内提供服务时用来接收请求的应用端口，端口范围为 `1~65535`，本 示例使用 80 端口，用于提供基于 HTTP 协议的高可用 WEB 服务。

323、9102、9103、9104、9105、60909、60910 等端口被占用，在任何协议下均不可使 用。

- 负载均衡算法：负载均衡分发请求到后端 RealServer 的调度计算策略，支持加权轮询、最小连接数和基于源地址三种算法。
- 会话保持：针对 HTTP 和 HTTPS 协议，提供 Cookie 植入的方式进行会话保持，支持自动生成KEY 和自定义 KEY。选择自动生成 KEY 则由平台自动生成 Key 进行植入，选择自定义 Key 时需输入 KEY 值（只能输入数字、字母及_字符）。
- 连接空闲超时：客户端至负载均衡的连接空闲超时限制，范围为 1~86400 秒。默认值为 60 秒，即在 60 秒内客户端对负载均衡一直无访问请求，平台会自动中断连接。
- 健康检查：根据规则对后端服务节点进行健壮性检查，可自动检测并隔离服务不可用的后端服务节点。HTTP 协议端检查和 HTTP 检查两种方式，其中 HTTP 检查支持按 URL 路径和请求 HOST 头中携带的域名进行健康检查，筛选健康节点。
 - HTTP 健康检查路径：默认为 /，可输入 Linux 格式的路径，只能使用字母、数字、和-/.%? #& 这些字符，必须以 / 开头，例如 /data；
 - HTTP 健康域名：检查时校验请求的 HOST 字段中的域名，可输入标准域名用于校验请求 host 字段中携带的域名。

HTTP 健康检查中的域名作用：某些应用服务器会对请求中的 host 字段做校验，即要求请求头中必须存在 host 字段。若在健康检查中配置了域名，则负载均衡会将域名配置到 host 字段中，并在健康检查时携带域名对后端服务节点进行检查，若健康检查请求被服务节点拒绝，则健康检查失败，即代表服务节点状态为异常；若应用服务器需要校验请求的 host 字段，则需要配置相关域名，确保健康检查正常工作。

创建过程中 VServer 的资源状态为“创建中”，待状态更新为“运行”即代表创建成功，用户可通过 VServer 列表及详情查看已添加的 HTTP 监听器，并可查看 VServer 下所有服务节点的健康状态。

10.3.1.4 添加 HTTPS 监听器

用户为负载均衡实例创建一个基于 HTTP 协议的监听器，提供基于 HTTPS 协议的负载均衡业务服务，本文以创建基于 SSL 证书加密的 HTTPS:443 (WEB) 服务为例进行创建。用户可通过负载均衡详情页面 VServer 左侧导航栏的【添加】进入 VServer 监听器的创建向导页面，如下图所示：

创建 VServer

LB lb-IRu29DVMR

协议 * HTTPS

端口 * 443

SSL解析模式 ⑦ * 双向认证

服务器证书 ⑦ * 请选择资源 新建服务器证书

客户端证书 ⑦ * 请选择资源 新建客户端证书

负载均衡算法 * 最小连接数

会话保持 * 关闭 自动生成KEY 自定义KEY

会话保持KEY * httpstest

连接空闲超时 * 60 S

健康检查 * 端口检查 HTTP检查

HTTP检查域名

HTTP检查路径 * /

取消 确认

This screenshot shows the 'Create VServer' configuration dialog. The dialog has a title bar '创建 VServer' and a close button. It contains several configuration fields:

- LB: lb-IRu29DVMR
- 协议: HTTPS (selected)
- 端口: 443
- SSL解析模式: 双向认证 (Mutual Authentication)
- 服务器证书: 请选择资源 (Select Resource) | 新建服务器证书 (Create Server Certificate)
- 客户端证书: 请选择资源 (Select Resource) | 新建客户端证书 (Create Client Certificate)
- 负载均衡算法: 最小连接数 (Min Connections)
- 会话保持: 关闭 (Off) | 自动生成KEY (Auto-generate KEY) | 自定义KEY (Custom KEY) (selected)
- 会话保持KEY: httpstest
- 连接空闲超时: 60 S
- 健康检查: 端口检查 (Port Check) | HTTP检查 (HTTP Check) (selected)
- HTTP检查域名: (empty)
- HTTP检查路径: /

At the bottom right are '取消' (Cancel) and '确认' (Confirm) buttons.

根据向导页面配置 VServer 监听器，包括协议、端口、SSL 解析模式、服务器证书、客户端证书、负载均衡算法、会话保持、连接空闲超时及健康检查：

- 监听协议：负载均衡业务的网络协议，支持 TCP、UDP、HTTP、HTTPS，本示例中选择 HTTPS。
- 端口：负载均衡业务对外或对内提供服务时用来接收请求的应用端口，端口范围为 1~65535，本示例使用 443 端口，用于提供基于 HTTPS 协议且使用 SSL 证书加密认证的高安全、高可用 WEB 服务。

323、9102、9103、9104、9105、60909、60910 等端口被占用，在任何协议下均不可使用。
- SSL 解析模式：HTTPS 协议的 SSL 证书认证的解析模式，支持单向认证和双向认证，通常选择单向认证。
 - 单向认证：由网站服务端提供 SSL 证书并进行身份验证，保证 HTTPS 网站的数据安全性，任何访问网站的用户无需拥有 CA 证书即可随时访问网站；

- 双向认证：网站服务端和用户双方均需提供 SSL 证书，只有提供 CA 证书的客户端才允许访问网站。
- 服务器证书：用户证明服务器的身份，HTTPS 检查服务器发送的证书是否是由自己信赖的中心签发。
 - 部署并配置于负载均衡服务器中，为负载均衡后端服务节点的网站提供 SSL 服务器证书及验证。
 - 在创建时需提前上传服务器证书到平台，可通过新建服务器证书进行上传，详见 [SSL 证书管理](#)。
- 客户端证书：客户端CA公钥证书用于验证客户端证书的签发者，HTTPS 双向认证中需验证客户端提供的证书，才可成功建立连接。
 - 网站服务器用 CA 证书验证客户端证书的签名，如果没有通过验证，则拒绝连接；
 - 在创建时需提前上传客户端证书到平台，可通过新建客户端证书进行上传，详见 [SSL 证书管理](#)。
- 负载均衡算法：负载均衡分发请求到后端 RealServer 的调度计算策略，支持加权轮询、最小连接数和基于源地址三种算法。
- 会话保持：针对 HTTP 和 HTTPS 协议，提供 Cookie 植入的方式进行会话保持，支持自动生成KEY 和自定义 KEY。选择自动生成 KEY 则由平台自动生成 Key 进行植入，选择自定义 Key 时需输入 KEY 值（只能输入数字、字母及_字符）。
- 连接空闲超时：客户端至负载均衡的连接空闲超时限制，范围为 1~86400 秒。默认值为 60 秒，即在 60 秒内客户端对负载均衡一直无访问请求，平台会自动中断连接。
- 健康检查：根据规则对后端服务节点进行健壮性检查，可自动检测并隔离服务不可用的后端服务节点。HTTP 协议端检查和 HTTP 检查两种方式，其中 HTTP 检查支持按 URL 路径和请求 HOST 头中携带的域名进行健康检查，筛选健康节点。
 - HTTP 健康检查路径：默认为 /，可输入 Linux 格式的路径，只能使用字母、数字、和-/.%? #& 这些字符，必须以 / 开头，例如 /data；
 - HTTP 健康域名：检查时校验请求的 HOST 字段中的域名，可输入标准域名用于校验请求 host 字段中携带的域名。

创建过程中 VServer 的资源状态为“创建中”，待状态更新为“运行”即代表创建成功，用户可通过 VServer 列表及详情查看已添加的 HTTPS 监听器，并可查看 VServer 下所有服务节点的健康状态。

VServer 监听器配置完成后，需添加业务虚拟机至监听器的服务节点中才可正常提供服务。HTTP 和 HTTPS 协议的监听器可根据需求配置内容转发规则，根据请求的域名和 URL 进行精准的请求分发。

10.3.2 查看 VServer

通过负载均衡详情页面进入 VServer 资源控制台，可查看当前负载均衡实例中已拥有 VServer 列表信息及所属服务节点的健康状况，并可通过列表名称切换 VServer 在右侧概览中查看 VServer 的基本信息及监控信息，同时可切换至服务节点和内容转发标签页进行服务节点和内容转发规则的管理。

10.3.2.1 VServer 列表

VServer 列表页面可查看当前负载均衡实例中已拥有的 VServer 资源列表，包括协议端口和状态，如下图所示：

	协议端口	状态
<input checked="" type="radio"/>	HTTP:22	●
<input type="radio"/>	HTTP:30	●

- 协议端口：VServer 监听器协议和端口，是负载均衡处理请求的入口依据；
- 状态：VServer 监听器的服务状态，包括绿色、黄色和红色；
 - 绿色：VServer 中添加的所有服务节点的健康状态均为正常；
 - 黄色：VServer 中添加的部分服务节点异常；
 - 红色：VServer 中添加的所有服务节点健康状态为异常，即代表 VServer 停止工作；若未添加任何服务节点，VServer 的默认状态为全部异常。

在列表页可对 VServer 进行添加、修改及删除操作，通过点击 VServer 可在右侧查看当前 VServer 的详细信息，点击状态按钮可显示状态描述。

10.3.2.2 VServer 详情

通过 VServer 资源列表的“协议端口”可在右侧查看 VServer 详情页面，可查看当前 VServer 资源的详细信息，如下图所示，详情页面分为基本信息、VServer 监控信息、服务节点管理及内容转发信息：

The screenshot shows the VServer configuration interface. On the left, there's a sidebar with buttons for '添加' (Add), '修改' (Modify), and '删除' (Delete). Below that is a table with columns '协议端口' (Protocol Port) and '状态' (Status). It lists two entries: 'HTTP:22' (status green dot) and 'HTTP:30' (status red dot). At the bottom of this sidebar are buttons for '10条/页' (10 items/page) and a search bar.

The main content area has tabs: '概览' (Overview), '服务节点' (Service Nodes), and '内容转发' (Content Forwarding). The '概览' tab is selected. It displays basic information in a table:

资源ID	vs-1ecwgypWR	负载算法	加权轮询	连接空闲超时	60s
协议端口	HTTP: 22	健康检查	端口检查	告警模板	无
运行状态	正常	会话保持	自动生成KEY		
VS状态	运行				
创建时间	2020-01-15 17:28:39				

Below this is a section titled '监控信息' (Monitoring Information) with a time range from '2020-01-15 16:41:56' to '2020-01-15 17:41:56'. It includes four charts for '每秒网卡连接数(个/s)' (Connections per second) and 'HTTP 2XX(个/s)', 'HTTP 3XX(个/s)', and 'HTTP 4XX(个/s)'. Each chart shows a single data point: '尚未获得有效数据, 请稍后重新查看' (No effective data obtained, please check again later).

(1) 基本信息

VServer 的基本信息，包括 ID、协议端口、负载均衡算法、会话保持、会话保持 Key、连接空闲超时、健康检查方式、运行状态、VS 状态、告警模板及创建时间等信息。若 VServer 监听协议为 HTTP/HTTPS，可查看 HTTP 健康检查路径、HTTP 检查域名、SSL 解析模式、服务器证书及客户端证书等信息。

- 会话保持：会话保持的开关和类型。UDP 协议值为开启或关闭，HTTP/HTTPS 协议值为关闭、自动生成 KEY 或自定义 KEY。
- 运行状态：VServer 监听器的服务状态，包括全部异常、部分异常、全部正常。
- VS 状态：VServer 监听器资源的状态，包括可用、更新中、已删除。
- 告警模板：VServer 绑定的监控告警模板，若未绑定则展示为无。
- 服务器证书/客户端证书：HTTPS 监听器 SSL 证书名称，可通过查看证书查询证书的内容。

(2) 监控信息

VServer 实例相关监控图表及信息，包括新建连接数、HTTP 2XX、HTTP 3XX、HTTP 4XX、HTTP 5XX，支持查看 1 小时、6 小时、12 小时、1 天及自定义时间的监控数据。

(3) 服务节点和内容转发

- 服务节点：VServer 的服务节点生命周期管理，包括服务节点的添加、查看、修改、启用、禁用及删除等，详见[服务节点管理](#)。
- 内容转发规则：当前 VServer 配置的内容转发规则生命周期管理，包括转发规则的添加、查看、修改及删除，详见[内容转发规则管理](#)。

10.3.3 修改 VServer

用户通过控制台修改 VServer 监听器配置，如修改监听器的负载均衡算法、会话保持、连接空闲超时及健康检查配置信息，若协议为 HTTPS 可更换监听器的 SSL 解析模式及 SSL 证书。可通过 VServer 列表上的“修改”按钮进行修改操作，如修改向导所示：

修改 VServer

LBID	lb-AecOLLYZR
VSID	vs-toraLLYWg
协议	HTTP
端口	30
负载均衡算法	加权轮询
会话保持 *	<input type="button" value="关闭"/> <input type="button" value="自动生成KEY"/> <input type="button" value="自定义KEY"/>
会话保持KEY *	<input type="text"/>
连接空闲超时 *	60 S
健康检查 *	<input type="button" value="端口检查"/> <input type="button" value="HTTP检查"/>
HTTP检查域名	<input type="text"/>
HTTP检查路径 *	/
<input type="button" value="取消"/> <input type="button" value="确定"/>	

修改配置的参数设置与创建 VServer 时一致，不支持修改 VServer 的协议和端口。修改过程中 VS 状态由“运行”变更为“更新中”，更新成功后流转为“运行”，即代表更新成功，可通过详情页面查看新修改的配置。修改成功后，平台会立即根据新配置重新对服务节点进行健康检查，同时会根据新修改的调度算法分发请求。

修改 VServer 的调度算法、会话保持、连接空闲超时，仅对新连接生效，不影响已建立连接的服务。

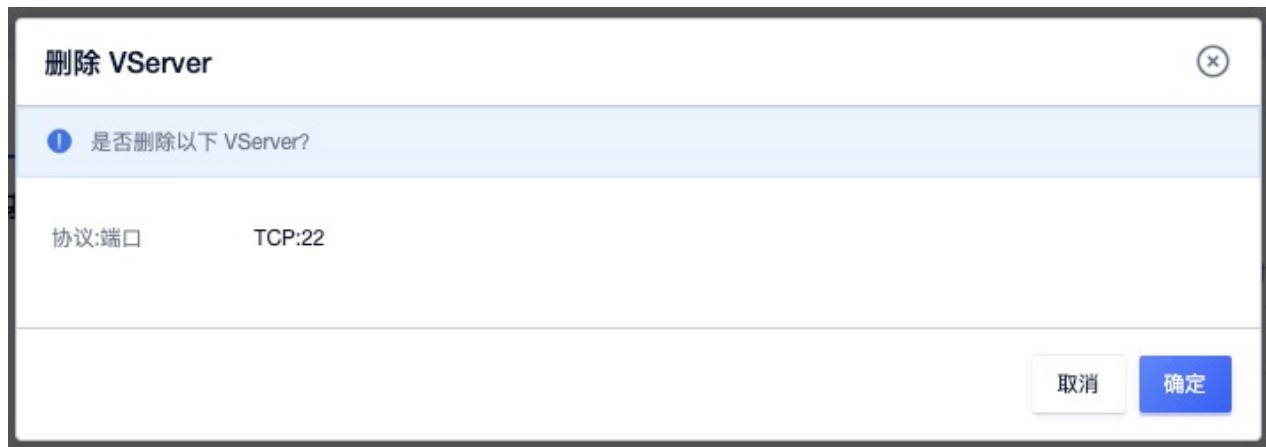
10.3.4 修改告警模板

修改告警模板是对 VServer 的监控数据进行告警的配置，通过告警模板定义的指标及阈值，可在 VServer 相关指标故障及超过指标阈值时，触发告警，通知相关人员进行故障处理，保证负载均衡及业务的网络通信。

用户可通过 VServer 详情概览页的操作项进行告警模板修改操作，在修改向导页面中选择新告警模板进行修改。VServer 和 负载均衡器可共用一个负载均衡监控告警模板，即在负载均衡的告警模板中即可定义 LB 实例的指标告警策略，同时可定义 VServer 的监控指标告警，可根据需求自定义告警模板的规则。

10.3.5 删除 VServer

用户可通过控制台或 API 的方式删除 VServer 资源，删除时会自动清除 VServer 下已创建的内容转发规则策略，同时会自动解绑已关联的 SSL 证书，仅当 VServer 中不存在后端 RealServer 资源时才可进行删除操作。



VServer 删除后不可恢复，在删除时需检查并确认是否有必要删除 VServer 资源，控制台 VServer 标签页可查看删除过程，待被删除的 VServer 资源被清空时，代表删除成功。

10.4 服务节点管理

服务节点指负载均衡架构中的后端真实服务器，即 RealServer，用于提供真正业务并处理业务请求的服务池，一般是由多台虚拟机集群构成。

- 添加服务节点需要在 VServer 监听器创建完成后才可进行添加。
- 服务节点添加后，负载均衡即通过健康检查 Check 服务节点的业务是否正常。
- 若业务节点无法正常处理 VServer 发送的请求，平台会提示服务节点状态为无效，需检测服务节点中部署的业务状况。
- 若业务节点可正常处理 Check 请求，即服务节点状态为有效，则代表负载均衡可正常工作。

10.4.1 添加服务节点

添加服务节点前，需确保服务节点上业务正常运行且可进行正常访问。可通过 VServer 详情页面进入“服务节点”资源控制台，点击“添加服务节点”进行后端 RealServer 的添加。添加服务节点时，仅可选择与负载均衡实例在相同 数据中心且 VPC 网络相同的虚拟机。如下图所示：

添加服务节点



① RServer 服务节点由云主机的 IP 地址和端口组成

VServer vs-toraLLYWg

虚拟机 * 请选择

端口 * 30

权重 * 1

取消

确定

- 虚拟机：即需要添加至负载均衡当前 VServer 服务节点的虚拟机，支持指定服务节点暴露的端口及权重。
- 端口：后端服务节点暴露的服务端口，如 VServer 监听 80，服务节点监听 8080 端口，则在端口处输入 8080 即可，负载均衡会将到达 VServer 80 端口的请求分发至服务节点的 8080 端口。
- 权重：后端服务节点的权重，范围为 1~100。数字越大即代表权重越高，负载均衡会优先将请求分发至权重较高的服务节点，默认值为 1。

支持添加同一个虚拟机的多个端口到 VServer 的服务节点，即将 VServer 监听器端口的请求分别转发至同一个服务节点的多个端口上，满足不同应用场景的负载分发需求。

添加服务节点后，可在服务节点资源列表页面查看添加服务节点过程，待服务节点的状态为“有效”或“无效”时，即代表添加服务节点成功。若服务节点状态为无效，则需要检测服务节点中业务的运行状态，服务状态“有效”的前提是通过虚拟机的网络地址及健康检查方式可正常访问业务。

负载均衡服务的服务模式为 NAT 请求代理模式，若添加虚拟机至提供外网的负载均衡后端，无需在后端服务节点上配置环回服务地址即可通过外网直接访问至服务节点。

10.4.2 查看服务节点

通过 VServer 详情页面的“服务节点”标签页，可查看 VServer 监听器后端已添加的服务节点资源列表信息，包括服务节点 ID、资源ID、内网 IP、端口、权重、节点模式、节点状态及操作项，如下图所示：

服务节点	资源ID	内网IP	节点模式	端口	权重	节点状态	操作
rs-jfVMWsEWg	vm-M3SUIWLWR	10.0.0.4	启用	30	1	• 无效	<button>启用</button> <button>禁用</button> <button>删除</button> <button>...</button>

- 服务节点：当前服务节点的全局 RS 唯一标识符。

- 资源ID：当前服务节点已绑定的虚拟机名称和 ID。
- IP/端口：当前服务节点的内网 IP 地址及配置的服务端口。
- 权重：当前服务节点配置的转发权重。
- 节点模式：当前服务节点的启用和禁用模式。
- 状态：当前服务节点的业务负载状态，包括有效、无效。
 - 有效：指当前服务节点中的业务服务正常运行且可通过网络进行访问，即服务节点为健康；
 - 无效：指当前服务节点中的业务服务未正常运行或无法通过网络进行访问，即代表服务节点不健康。

列表上操作项是指对单个服务节点的操作，包括启用、禁用、删除及修改等，支持服务节点的批量启用、批量禁用及批量删除操作。

10.4.3 启用/禁用

用户对添加至负载均衡 VServer 的服务节点进行启用和禁用操作，支持批量启用和禁用。

- 禁用：禁用服务节点，禁用后负载均衡将停止向该服务节点分发请求，并停止对其健康检查；
- 启用：启用服务节点，启用后负载均衡将对其进行健康检查，若健康检查通过则根据调度算法，分发新的请求至该服务节点；
- 仅当节点模式为启用时才可进行禁用操作；
- 仅当节点模式为禁用时，才可进行启用操作。

10.4.4 修改服务节点

用户可对负载均衡 VServer 服务节点的服务端口及权重进行修改，如下图所示：

修改服务节点

RSERVER 服务节点由云主机的 IP 地址和端口组成

RSERVER	rs-jfVMWsEWg
虚拟机	dfdfdf(vm-M3SUIWLWR)
端口 *	30
权重 *	1

取消 确定

修改端口和权重不会影响已建立的业务连接，仅对负载均衡新分发请求生效。点击确定后，即返回至服务节点列表页面，节点状态由“有效”或“无效”流转为“更新中”，待修改成功后，重新流转回“有效”或“无效”，有效则代表健康检查成功，服务节点可正常提供服务。

10.4.5 删除服务节点

如需对一个服务节点的业务进行变更或从负载均衡后端服务节点下线，可通过删除服务节点功能进行下线操作，下线后不影响虚拟机本身的运行和使用。用户可通过服务节点列表操作项中的“删除”进行服务节点的删除，删除后可重新添加至负载均衡实例。



若负载均衡 VServer 的监听协议为 HTTP/HTTPS 且已配置内容转发规则，则删除服务节点时，会自动解绑内容转发规则。

10.5 内容转发规则管理

平台支持为 HTTP 监听器添加转发规则，支持为域名+ URL 路径的请求分发至不同的服务节点，满足精准负载分发业务需求。仅当负载均衡的 VServer 监听协议为 HTTP 或 HTTPS 时，才可进行内容转发规则的配置，包括内容转发规则的添加、查看、修改及删除。

10.5.1 添加内容转发规则

用户可通过 VServer 详情页面进入“内容转发”资源标签页，点击“添加内容转发”进行内容转发规则的添加。平台会自动生成一条默认内容转发规则，即代表所有请求默认转发至所有已添加的服务节点。

内容转发规则中的服务节点，仅可从当前 VServer 已存在的服务节点中进行选择，支持为一个域名添加多个 URL 路径，如下图所示：

添加内容转发

① 域名支持泛域名，* 必须在第一个字符，比如 *.text.com 或 *abc.test.com; URL 长度限制为1~30，只能使用字母、数字和-.%?#&这些字符，且必须以/开头。

域名	test.com	操作	
添加 *			
URL路径	服务节点	操作状态	操作
/abc	已选择 1 项	未操作	删除
/test	已选择 1 项	未操作	删除
添加URL			

[取消](#) [确定](#)

- 域名：内容转发规则匹配的域名，代表请求该域名时及 URL 时，将请求转发至 URL 配置的服务节点。
 - 域名值可以为空，代表无域名请求，仅匹配路径，即通过 IP 地址+ URL 路径的方式；
 - 支持泛域名，如 *.test.com 或 *abc.test.com；
- URL 路径：内容转发规则匹配的 URL 路径，URL 必须属于一个域名；
 - URL 长度限制为 1~30 个字母、数字和 -/.%?#& 这些字符，且必须以 / 开头；
 - URL 可以为 /，代表请求该域名的根目录时，转发请求至匹配的服务节点；
- 服务节点：当前内容转发规则所对应的服务节点，即当请求匹配 域名+路径 时，将请求转发发配
 置的服务节点，转发规则中的服务节点必须为 VServer 中已添加的服务节点。

点击确定后，返回内容转发规则的列表，可查看创建内容转发规则的过程，待添加的内容转发规则状态由“创建中”流转为“有效”时，即代表创建成功。

10.5.2 查看内容转发规则

通过 VServer 详情页面的“内容转发”标签进入内容转发规则管理控制台，可查看当前 VServer 监听器已添加的内容转发规则列表，同时可对内容转发规则进行添加、修改及删除操作。

内容转发规则列表页面可查看当前 VServer 已添加的内容转发规则信息，包括域名、URL 路径、转发节点、节点数量、规则状态及操作项，如下图所示：

The screenshot shows a table with columns: 域名 (Domain), URL路径 (URL Path), 转发节点 (Forwarding Node), 节点数量 (Node Count), 状态 (Status), and 操作 (Operations). There are four rows of data:

域名	URL路径	转发节点	节点数量	状态	操作
test.com	/test	dfdfdf(10.0.0.4):30	1	● 有效	<button>修改</button> <button>删除</button>
	/abc	dfdfdf(10.0.0.4):30	1	● 有效	<button>修改</button> <button>删除</button>
-	/	dfdfdf(10.0.0.4):30	1	● 有效	<button>修改</button> <button>删除</button>

At the bottom right, there are navigation buttons: < > 1 /1, and a dropdown for '10条/页'.

- 域名：内容转发规则匹配的域名，代表请求该域名时及 URL 时，将请求转发至 URL 配置的服务节点。
- URL 路径：内容转发规则匹配的 URL 路径，URL 必须属于一个域名。
- 转发节点：匹配当前内容转发规则时，请求分发的服务节点。
- 节点数量：当前转发规则已添加的服务节点数量。
- 状态：当前转发规则的状态，包括创建中、有效和删除中。

列表上操作项是指对域名或单条转发规则的修改及删除操作。点击域名右侧的修改和删除，即修改和删除整个域名及包括的所有转发规则；点击单条 URL 规则的修改和删除，即仅对单条规则进行删除和修改操作。

默认转发规则仅支持查看，不支持修改和删除，默认转发规则的节点数量即 VServer 中所包含的所有服务节点数量。

10.5.3 修改内容转发规则

用户可对一个域名或所包含的 URL 规则进行修改，包括域名、URL 路径、转发的服务节点，如下图所示：

修改内容转发

① 域名支持泛域名，* 必须在第一个字符，比如 *.text.com 或 *abc.text.com; URL 长度限制为1~30，只能使用字母、数字和-/.%?#&这些字符，且必须以/开头。

域名	URL路径	服务节点	操作状态	操作
test.com	/test	已选择 1 项	未操作	<button>删除</button>
	/abc	已选择 1 项	未操作	<button>删除</button>

添加URL

取消 **确定**

修改内容转发规则仅对新负载分发请求生效，不影响已建立并在处理的业务请求。点击确定后，即返回至内容转发规则列表页面，内容转发规则由“有效”流转为“更新中”，待修改成功后，重新流转回“有效”，则代表新的匹配规则请求会直接分发到规则所配置的服务节点。

10.5.4 删除内容转发规则

用户可通过控制台或 API 的方式删除不需要的内容转发规则，删除内容转发规则会自动解绑已关联的后端服务节点。内容转发规则被删后，即直接销毁，在删除前需确保负载均衡转发规则无业务流量的负载请求，否则可能影响业务的正常访问。如下图所示，删除域名时即直接删除该域名下所包括的所有 URL 规则信息：

删除内容转发

① 是否删除以下内容转发规则？删除后可能影响负载均衡业务访问。

名称	节点数量	操作状态
test.com:/test	1	未操作
test.com:/abc	1	未操作

取消 **确定**

10.6 SSL 证书管理

负载均衡支持 HTTPS 负载转发及 SSL 证书装载能力，确保用户业务受到加密保护并得到权威机构的身份认证。针对 HTTPS 协议的服务器证书和客户端证书，平台提供统一的证书管理服务，包括证书的上传、绑定、删除操作。

证书无需上传到服务节点，解密处理在负载均衡上进行，降低后端服务器的CPU开销，即 HTTPS 协议的监听器仅实现客户端至负载均衡器的 HTTPS 请求和 SSL 加解密，负载均衡至后端服务节点依然采用 HTTP 协议转发请求。

在上传和创建证书前需确认需要上传的证书类型，包括服务器证书和客户端证书，并按照证书格式要求上传或输入证书内容至平台。

- 服务器证书：用户证明服务器的身份，HTTPS 检查服务器发送的证书是否是由自己信赖的中心签发。部署并配置于负载均衡服务器中，为负载均衡后端服务节点的网站提供 SSL 服务器证书及验证。单向认证和双向认证均需要上传服务器证书和私钥内容。
- 客户端证书：客户端CA公钥证书用于验证客户端证书的签发者，HTTPS 双向认证中需验证客户端提供的证书，才可成功建立连接。网站服务器用 CA 证书验证客户端证书的签名，如果没有通过验证，则拒绝连接。仅在双向认证时需要上传客户端证书并绑定到 VServer 监听器。

证书具有地址（数据中心）属性，仅支持关联相同数据中心的负载均衡资源，若一个证书需要在多个数据中心同时使用，需要在多个数据中心同时创建并上传证书。

10.6.1 证书格式要求

负载均衡 SSL 证书支持用户上传 `.crt` 和 `.pem` 格式的证书文件，当 SSL 证书被 VServer 监听器关联时，平台会自动读取文件中的证书内容并装载至负载均衡 VServer 监听器中，使用户 HTTPS 应用通过 SSL 证书进行加解密。

证书文件格式支持 Linux 环境下 PEM 或 CRT，不支持其他格式的证书，需进行证书格式转换才可上传。用户也可通过直接输入证书内容创建证书，在上传证书或输入证书内容前，需确保证书、证书链及私钥内容符合证书的格式要求。

10.6.1.1 Root CA 机构颁发的证书

若证书是 Root CA 机构颁发的唯一证书，则无需额外的证书，配置的站点即可被浏览器等访问设备认为可信。证书内容格式要求如下：

- 以 `-----BEGIN CERTIFICATE-----` 开头，以 `-----END CERTIFICATE-----` 结尾。
- 每行 64 个字符，最后一行长度可以不足 64 个字符。
- 证书内容不能包含空格。

Root CA 机构颁发的证书格式规范如下，可参考以下文本内容和证书示例：

```
-----BEGIN CERTIFICATE-----  
用户证书(BASE64编码)  
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----  
MIIFFnDCCBISgAwIBAgIQD1pxAmxfzY+R4k4Ua1cVWDANBgkqhkiG9w0BAQsFADBy
```

```
MQSwCQYDVQQGEwJDTjE1MCMGA1UEChMcVHJ1c3RBC21hIFR1Y2hub2xvz211cywg
SW5jLjEdMBSGA1UECxMURG9tYwluIFZhbG1kYXR1ZCBTU0wxHTAbBgNVBAMTFFRy
dXN0QXNpYSBUTFMgU1NBIEAMB4XDTE5MDQyMzAwMDAwMFoXDTIwMDQyMjEyMDAw
MFowHDEaMBgGA1UEAwRKi51Y2xvdWRzdGFjay5jb20wggEiMA0GCSqGSIb3DQE
AQUAA4IBDwAwggEKAoIBAQC2SDT5pJEQhRhQQ98vzuAvK1zUFMD1p1E3YyJGDISY
SINH38QTtvqwbZgmVku6v2R1GrBz0imfevo0/sjxefwhmiGYd1ytG9dm8D3fvzox
piST9hoIyj0FRstBLGXuxwSa2LdjvSePaFfxaN3UZLYY6MIHkdqxFZLhM4ANSLnr
PI6cRUZBU29V3A2znkVExb5dwKA3SGFVwfqjfzXqC+NTy1Lkb7H304Bxspz1kdi
n+/av/vSovVM7zg57AOtxjksNZBDjdz+Ud3wqat104vEG4tqqAnsIyJeaMueFti0
cjIMwLVsFsmV1eVSBiYWGO8U/YRFv+dNg4XG2MqYUFsRAgMBAAGjggKCMIIcfjAf
BgNVHSMEGDAwBR/05nzoECOMQBWViKot8ye3coBijAdBgNVHQ4EFgQUJYEWLiy
YgqKaGaT8thKWAAnuwfEwLQYDVR0RBCYwJIIRKi51Y2xvdWRzdGFjay5jb22CD3vj
bG91ZHN0YWNrLmNvbTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR01BBYwFAYIKwYBBQUH
AwEGCCsGAQUFBwMCMEwGA1UdIARFMEMwNwYJYIZIAYb9bAECMCowKAYIKwYBBQUH
AgEWGh0dHBzoi8vd3d3LmRpZ1jZXJ0LmNvbS9DUFMwCAYGZ4EMAQIBMH0GCCSG
AQUFBwEBBHEwbzAhBgrBqEFBQcwAYYVaHR0cDovL29jc3AuZGNvY3NwLmNuMEoG
CCSGAQUFBzACHj5odHRwOi8vY2FjZXJ0cy5kawdpdGFsY2VydHzhbG1kYXRpB24u
Y29tL1RydXN0QXNpYVRMU1JTQUNBLmNyddAJBgnVHRMEAjaAMIIBAYKKwYBBAHw
eQIEAgSB9QSB8gDwAHYA7ku9t3XOYLrhQmkfq+GeZqMPf1+wctiDAMR7ixqo/cSA
AAFqSaRkyQAABAMARzBFAiEAuovTHM3SEWQRyktGXvtm1hLhd7gxhPNzdrzkjFX
rWMCIAPideB1BqUSUcpRME6NXIXJD70661dwusqgPkoiPtLAHYAh3w/5118+IXD
mV+9827/v01HVjb/SrvgbwTq/16ggw8AAAFqSaR14wAABAMARzBFAiBiIp059m6u
bm1muQ8cL7wzoDkHiyE+UloEKZXidpqcfQIhAPIRdaJfh/5IZHFq31oJvd/Tz3g
pTQ6RpHe0BsesSefMA0GCSqGSIb3DQEBCWUA4IBAQARanWOjbAI7Rv6QPChPewL
Mqryk+t01terdxYZay6tr3Ea8voqss7Ydvtdkr1/k4k87H5AwCQT60/yu4N5j7M
vkzmqo3tvQTTzVFo0SavgARY12xuu0jhG3LGFI0a43cgfMYMcZ0DiylhYUM48GWZ
/axza5uangnIQxBwv+4KXGUfp1jujv8wfBepeh+tqPgS8qcq6e0+sdkUN7yHca/
O24DiQajtMXG5nR6qHdZhRLCFRXRghYdvVKrkOVFogYqwa4dviyup/6EFdkuMwDs
7rxJ1jL8qp9Lrw2shN1F+USKh1PRaNBtzDELf54zVgAIaEfUriqtER8ZWBwgP4
-----END CERTIFICATE-----
```

10.6.1.2 中级机构颁发的证书

若证书是通过中级 CA 机构颁发的证书，则拿到的证书文件包含多份证书，需要人为将服务器证书与中间证书合并在一起填写或上传，俗称证书链。

证书链的拼接规则为：用户证书放第一份，中间证书放第二份，中间不可有空行；每行 64 个字符且证书内容不能包含空格，最后一行长度可以不足 64 个字符，格式规范及证书示例如下所示：

```
-----BEGIN CERTIFICATE-----
用户证书(BASE64编码)
-----END CERTIFICATE-----
!!!中间不可有空行!!!
-----BEGIN CERTIFICATE-----
中级签发机构证书(BASE64编码)
-----END CERTIFICATE-----
```

```
-----BEGIN CERTIFICATE-----
MIIFnDCCBISgAwIBAgIQD1pxAmxfzY+R4k4Ua1cVWDANBgkqhkiG9w0BAQsFADBy
```

MQswCQYDVQQGEwJDTjE1MCMGA1UEChMcVHJ1c3RBC21hIFR1Y2hub2xvz211cywg
SW5jLjEdMBSGA1UECxMURG9tYwluIFZhbG1kYXR1ZCBTU0wxHTAbBgNVBAMTFFRy
dXN0QXNpYSBUTFMgU1NBIEAMB4XDTE5MDQyMzAwMDAwMFoXDTIwMDQyMjEyMDAw
MFowHDEaMBgGA1UEAwRKi51Y2xvdWRzdGFjay5jb20wggEiMA0GCSqGSIB3DQEBr
AQUAA4IBDwAwggEKAoIBAQc2SDT5pJEQhRhQQ98vzuAvK1zUFMD1p1E3YyJGDISY
SINH38QtqvwbZgmVku6v2R1GrBz0imfevo0/sjxefwhmiGYd1ytG9dm8D3fvzox
piST9hoIyj0FRstBLGXuxwSa2LdjvSePaFFxaN3UZLYY6MIHkdqxFzLhM4ANSLNr
PI6cRUZBU29V3A2znkVEbx5dwKA3SGFVwfqjfzxqc+NTy1Lkb7H304Bxspz1kdi
n+/av/vsovVM7zg57AotxjksnzBDjdz+ud3wqat104vEG4tqqAnsIyJeaMueFti0
cjimwLVsfsmV1eVSBiYWGO8U/YRFv+dNg4XG2MqYUFsRAgMBAAGjggKCMIIcfjAf
BgnVHSMEGDAwBR/05nzoEcOMBWViKot8ye3coBijAdBgNVHQ4EFgQUJYEWLiyn
YgqKaGaT8thKWAnuwFEwlQYDVR0RBCYwJIIRKi51Y2xvdWRzdGFjay5jb22CD3Vj
bG91ZHN0YWNrLmNvbTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR01BBYwFAYIKwYBBQUH
AwEGCCsGAQUFBwMCMEwGA1UdIARFMEMwNwYJYIZIAyB9bAECMCowKAYIKwYBBQUH
AgEWHGh0dHBzoi8vd3d3LmRpZ21jZXJ0LmNvbS9DUFMwCAYGZ4EMAQIBMH0GCCSG
AQUFBwEBBHEwbzAhBgrBqEFBQcwAYYVaHR0cDovL29jc3AuZGNvY3NwLmNuMEoG
CCSGAQUBZACHj5odHRwOi8vY2FjZXJ0cy5kawdpdGFsY2VydHzhbG1kYXRpb24u
Y29tL1RydXN0QXNpYVRMU1JTQUNBLmNyddAJBgnVHRMEAjaAMIIBAYKKwYBBAHw
eQIEAgSB9QSB8gDwAHYA7ku9t3XOYLrhQmkfq+GeZqMPf1+wctiDAMR7ixqo/cSA
AAFqSaRkyQAABAMARzBFAiEAuovTHM3SEWQRYktGXvtm1hLhd7gxhPNzdrzkjFX
rwMCIApideB1BqUSUcpRME6NXIXJD70661dwusqgPkoiPtLAHYAh3w/5118+IXD
mV+9827/v01hvjb/SrvgbwTq/16ggw8AAAFqSar14wAABAMARzBFAiBiIp059m6u
bm1muQ8cL7wzodKhiyE+UloEKZXiDpqcfQihAPIRdaJfh/5IZHFq31oJvd/Tz3g
pTQ6RpHe0BsesSefMA0GCSqGSIB3DQEBCwUA4IBAQARanwoJbAI7Rv6QPChPewL
Mqryk+t01terdxYZay6tr3Ea8voqss7Ydvtdkr1/k4k87H5AwCQT60/yu4N5j7M
vkzmqo3tvQTTzVFo0SavgARY12xuu0jhG3LGFI0a43cgfMYMcZ0DiylhYUM48GWz
/axza5uangnIQxBwv+4KXGUfp1jujv8wfBepeh+tqPgS8qcq6e0+sdkUN7yHCA/
024DiQajtMXG5nR6qhdzhRLCFRXRghYdvVKrkOVFogYqwa4dviyup/6EFDkuMwDs
7xrxJ1jL8qp9Lrw2shN1F+USKh1PRaNBtzDELf54zVgAIaEfUriqteR8ZWBwgP4

-----END CERTIFICATE-----

-----BEGIN CERTIFICATE-----

MIIErjCCA5agAwIBAgIQBYAmfwby1vM0jhwYw17uLjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGa1UEChMMRG1naUN1cnQgSw5jMRkwFwYDVQQLEXB3
d3cuZG1naWn1cnQuY29tMSAwHgYDVQQDEXdEawdpQ2VydCBhbG9iYwggUm9vdCBD
QTAeFw0xNzEyMDgxMjI4MjzaFw0yNzEyMDgxMjI4MjzaMHIXCzAJBgnVBAYTAkNO
MSUwIwYDVQQKExxUcnVzdEFzaWegvGVjaG5vbG9naWvzLCBjbmmMuMR0wGwYDVQQL
EXREb21haw4gVmFsawRhdGvkIFNTTDEDMBSGA1UEAxMUVHJ1c3RBC21hIFRMUyBS
U0EgQ0EwgEiMA0GCSqGSIB3DQEBAQUAA4IBDwAwggEKAoIBAQcgWa9X+ph+wAm8
Yh1Fk1MjkBQ5QwBOOKVazR/ofCh+F6f93u7vZHGUU/1vvGGUQnbzJhR1UV2epJa
e+m7cxnXIKdd0/vs9btAgwJSzGFvwoqXeaCqFop71wPmxjjUwLT70+qvX4hdYfo
JcjeTz5QKtg8zQwxak9x4JT9Co0moVdvhEBAiD3Dwr5ffgOHdwwGxdJwvBvktnoA
zjdTLXDbSVC5jz0u8oq9B1TDv7jA1sB5F8azgvSzDOQeFrwaOTbKWSEInEhnchK
ZTD1dz6ab1k1xGEI5PZWAnVAbA/ofH33ktymaTDse6xrdnw97pdkimCrak6CEbfe
3dxw60v5AgMBAAGjggFPMIIBSzAdBgNVHQ4EFgQUf9oz86BHDjEAV1YijrfMnt3k
AYowHwYDVR0jBBgwFoAU95QNVbRTLtm8KPiGxvD17I90VUwDgYDVR0PAQH/BAQD
AgGGMB0GA1UDJQQWMBQGCCsGAQUFBwMBBgrBqEFBQcDAjASBgNVHRMBAf8ECDAG
AQH/AgEAMDGCCsGAQUFBwEBBCgWjAkBgrBqEFBQcWAYYyAHR0cDovL29jc3Au
ZG1naWn1cnQuY29tMEIGA1UdHwQ7MDkwN6A1oDOGMwh0dHA6Ly9jcmwzLmRpZ21j
ZXJ0LmNvbS9EawdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwTAYDVR0gBEUwQZA3Bglg

```
hkgBhv1sAQIwKjAoBggrBgEFBQCCARYcaHR0cHM6Ly93d3cuZGlnawN1cnQuY29t
L0NQUZAIBgZngQwBAgEwDQYJKoZIhvcNAQELBQADggEBAK3dvoj5d1v4MzK2i233
1DYvyJ3s1FY2X2HKTGte8nb6i5/fsDIImMYihAkp6VaNY/en8WZ5qcrQPVLuJrJ
DSXT04NnMeZoQDUoj/NHAMdfCBB/h1bZ50GK6sf1h5Yx/5wR4f3TUoPgGlnU7EuP
ISLNdMRiDrXntcImDAiRvhk5GJuH4YCE6XEntqaNIgGkRwxKSgnU3Id3iuFbw9F
UQ9Qqtb1GX91AJ7i4153TikGgYCdwykBURD8gSve80Ac06IfZOYt/TEwiilIvi1c
qnuu1wpsF1LdQNIdfbw3TSe0BhQa7ifbvIfvPwHYou3rkg1ZeMo6XRu9B4n5VYJY
RmE=
-----END CERTIFICATE-----
```

10.6.1.3 RSA 私钥

在上传服务器证书时，需要用户同时上传证书的私钥内容。

- 以 -----BEGIN RSA PRIVATE KEY----- 开头，以 -----END RSA PRIVATE KEY----- 结尾。
- 每行 64 个字符，最后一行长度可以不足 64 个字符。
- 证书内容不能包含空格。

证书 RSA 私钥内容的格式规范如下，可参考以下文本内容和证书示例：

```
-----BEGIN RSA PRIVATE KEY-----
证书私钥(BASE64编码)
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAtkg0+aSREIUYUEPfL87gLytc1BTA9adRN2MiRgyEmEiDR9/E
E7valm2YJ1ZFor9kdRqwc9IjH3rztp7I8xn8B5ohmHdcrrVxzVA931waMaykk/Ya
CMozhubLQsx17svkmti3Y1Unj2hx8wj1GS2GOjCB5Hasvws4TOADUiZazyOnEVG
VQVNvVdwNs55FRG8eXccgN0hhvvn6o3816gvju8pSym+x990AcBKwzSg4p/v21f7
0ql1T0840ewDrcY5EjcwQ43c/lhd8Kmk9TuLxbuLaqqj7CMiXmjLnhbYtHI4jMC1
bBbj1dx1ugYmfhjvFP2ERb/nTYOFxtjkMFBbEQIDAQABAOIBAAbLqdftu+/A+nR
jHJ1lOCFthR1Aq2V04gMVNSGNJD78r/61wtvGctxmKVgEa4qGraOB5VRPRXPCEV
Z3fjk5Nv+1uoDACzHMRsa+4Vz6YostnmSKGvwhxzn306T0GHz+Ca+d1Gjs9CPVcv
aQG4UHacxNEJ7byD03LUW++C2jeEjg2LVLjt+jRwfIAwmk8xjm/jyOn5kcj2kvz6
w/yHbmwAac2mfA42CQN78o1bvEH1HH1cvDRHZ482pN1fp8wBGgCFWHBGeMpLoq9R
YXEt+Sj84o80mTeR2Dgswpw577uzLGFpYfuWKpc/XGzszbFKx5L9ctGQrr4lsq+
F2stok0cgYEA5JyQ5S7qPf8YcczQfxb1vues1DL56zt1/kuduQ4L9i2as+5LkiN+
7gVK8InhvYi8dRAqZxqXLqu5dxEWbkcnFbenjoQyPCfYI51ZE2+cZriLt03I0YKP
nc9NwSE+gRR9kxbgGSIANJmGC5TxOU99hR7Nx6wUMAfatCaSmP5RbUCgYEazB67
M0wzeVD8Eq/DhEE5N0o3hpyhiMy++A/LC81AjFAi61dc70zMYMuJfh+eTNK89z6H
1z3xBaQMLhAy8pu5uI9Logm/xWaPNZ034xx4fwftBnEGFtBglfbNphouz3Df5vk
XvxhjdkEkwevcLoZWhfNZIJnenn1EV26Tk1DGW0CgYBYCKaPasqPRy2NnRZosig0
npBJnxu5zsE/ogGxFdyrvxJs2YXGZ97YH7ek+kLpzs7rwwbiv02ai8udmwfNPZ8i
cm+YRPXnTlygEMxJfMBYmhZKfQrjcyLs3ui055nfN5nHK2Toq1b7amdBDID71c17
Nsp9ap13iyLh6CSSIV95xQKBgCHmKKhiPYA0VuizkAdy5BGunbIZasps9pQz60c1
16z12Jaak7Catib1toNhtP6FMSSJg33Xp60MLwpcUwyG2brOb+j5w6CZcdgQtba5
ioZASJmcfdidry81wY6jmQ/Z/hG/ScijhSYmHD/20sgh3/u1scMbdRv+CnDr4/kF
E90xAoGBAK0mCJyyKNkwSDog7fbBwYJKQ1BBZ61h1gVpc7recSreNPRFWTd61+cw
eCxXqbSJw4oYYF4IoBX1fcfFd82engRkwmkDykGMwpomnJoZqjFhmVtDb81xRQL
```

```
pscHorV4f1p0cSwg6b3jq0N6+PN85XI9XIFImXXHJqqKSFBBSPrf
```

```
-----END RSA PRIVATE KEY-----
```

若 RSA 私钥内容已进行加密，如私钥以 -----BEGIN PRIVATE KEY----- 或 -----BEGIN ENCRYPTED PRIVATE KEY----- 开头，以 -----END PRIVATE KEY----- 或 -----END ENCRYPTED PRIVATE KEY----- 结尾，需对证书私钥内容进行转换。在 Linux 系统中操作如下所示：

```
openssl rsa -in old_server_key.pem -out new_server_key.pem
```

10.6.1.4 客户端证书

客户端证书格式要求和 Root CA 机构颁发的证书要求一致，以 -----BEGIN CERTIFICATE----- 开始，以 -----END CERTIFICATE----- 结尾，每行64字符，最后一行可以不足64字符。如下规范所示：

```
-----BEGIN CERTIFICATE-----  
客户端CA证书(BASE64编码)  
-----END CERTIFICATE-----
```

10.6.2 创建 SSL 证书

用户上传 SSL 证书用于部署 HTTPS 协议的负载均衡业务，支持上传服务器证书和客户端证书。上传证书时需检测 SSL 证书的格式及有效性，若 SSL 证书内容不符合格式规范，则无法成功生成 SSL 证书。

10.6.2.1 创建服务器证书

支持本地上传证书文件和手动输入证书内容两种方式创建服务器证书，用户可通过负载均衡控制台切换至 SSL 证书标签页，进入 SSL 证书管理控制台，通过创建 SSL 证书进入上传证书向导页面，选择服务器证书进行创建。

(1) 本地上传证书文件的方式创建如下图所示：

创建 SSL 证书

证书名称 *

证书类型 ⑦ *

服务器证书

证书内容 *

本地上传 手动输入

用户证书 ⑦ *

上传证书 支持 .crt 和 .pem 格式的文件

你还未上传任何内容

证书私钥 ⑦ *

上传证书 支持 .key 格式的文件

你还未上传任何内容

取消 确认

本地上传时需要上传用户证书文件和证书私钥文件，其中用户证书文件仅支持 crt 和 pem 格式的文件，证书私钥仅支持上传 .key 格式的文件。

- 用户证书：用户的授权证书内容，包括公钥和签名等信息，支持证书链，一般为 .crt 和 .pem 格式的文件。
- 证书私钥：加密证书的私钥内容，一般为 .key 格式的文件。

点击上传证书，即可将本地已生成的证书文件读取到平台，并通过确认进行证书创建，创建过程中，平台会检测证书内容的合法性。

(2) 手动输入证书内容创建如下图所示：

创建 SSL 证书

证书名称 *

证书类型 ⑦ *

服务器证书

证书内容 *

本地上传 手动输入

用户证书 ⑦ *

```
-----BEGIN CERTIFICATE-----  
用户证书(BASE64编码)  
-----END CERTIFICATE-----  
!!!中间不可有空行!!!  
-----BEGIN CERTIFICATE-----  
中级签发机构证书(BASE64编码)
```

证书私钥 ⑦ *

```
-----BEGIN RSA PRIVATE KEY-----  
证书私钥(BASE64编码)  
-----END RSA PRIVATE KEY-----
```

取消 确认

手动输入证书同样需要输入用户证书和证书私钥的文本内容，需参考文本框中的格式规范输入证书内容和私钥内容，通过确认进行证书创建，创建过程中，平台会检测证书内容的合法性。

10.6.2.2 创建客户端证书

支持本地上传证书文件和手动输入证书内容两种方式创建客户端证书，用户可通过负载均衡控制台切换至 SSL 证书标签页，进入 SSL 证书管理控制台，通过创建 SSL 证书进入上传证书向导页面，选择客户端证书进行创建。

(1) 本地上传证书文件的方式创建如下图所示：



本地上传时需要上传客户端 CA 公钥证书文件，仅支持 `crt` 和 `pem` 格式的文件。点击上传证书，即可将本地已生成的证书文件读取到平台，并通过确认进行证书创建，创建过程中，平台会检测证书内容的合法性。

(2) 手动输入证书内容创建如下图所示：



手动输入证书同样需要输入 CA 客户端证书的文本内容，需参考文本框中的格式规范输入证书内容和私钥内容，通过确认进行证书创建，创建过程中，平台会检测证书内容的合法性。

10.6.3 查看 SSL 证书

通过导航栏进入负载均衡控制台，切换至 SSL 证书标签页可查看 SSL 证书的资源列表，并可通过列表上名称和 ID 进入详情页面查看证书的详细信息及已绑定资源信息。

10.6.3.1 SSL 证书列表

SSL 证书列表可查看当前账户下所有 SSL 证书的资源列表信息，包括名称、资源 ID、证书类型、域名、MD5 值、创建时间、证书过期时间及操作项，如下图所示：

名称	资源ID	证书类型	域名	MD5值	创建时间	过期时间	操作
ca 修改名称及备注	crt-N1hg3cVGR	客户端证书	主域名: *.ucloudstack.com 备域名: *.ucloudstack.com ucloudstack.com	bc6a14645f513dd0b6eec98f2a04ab3d	2020-07-28	已过期	详情 查看证书 ...
test 修改名称及备注	crt-wQdDpc4GR	服务器证书	主域名: *.ucloudstack.com 备域名: *.ucloudstack.com ucloudstack.com	bc6a14645f513dd0b6eec98f2a04ab3d	2020-07-28	已过期	详情 查看证书 ...

- 名称/ID：SSL 证书的名称及全局唯一标识符。
- 证书类型：SSL 证书的类型，包括服务器证书和客户端证书，仅在 VServer 监听器的 SSL 解析模式为双向认证时才需上传客户端证书。
- 域名：SSL 证书的主域名和备用域名信息，分别对应证书的 CommonName 和 Subject Alternative Name 字段信息，代表该证书可进行加解密服务的域名。
- MD5 值：SSL 证书的 MD5 较验值，用于验证 SSL 证书的准确性。
- 创建时间：SSL 证书在平台的创建时间。
- 证书过期时间：SSL 证书本身的过期时间，若证书已过期，需要重新为域名申请或制作新的证书，否则 HTTPS 协议访问会被认为不可信，即 HTTPS 失效。

列表上的操作项是指对单个证书的操作，包括查看证书和删除证书，可通过搜索框对证书列表进行搜索和筛选，支持模糊搜索。为方便租户对资源的维护，同时支持对 SSL 证书进行批量删除操作。

10.6.3.2 SSL 证书详情

在证书资源列表上，点击名称或 ID 可进入概览页面查看当前证书的详信细信及已绑定的资源信息，如概览所示：

基本信息
资源ID: crt-N1hg3cVGR
资源名称: ca
证书类型: 客户端证书
主域名: *.ucloudstack.com
备域名: *.ucloudstack.com ucloudstack.com
MD5值: bc6a14645f513dd0b6eec9...
证书内容: 查看证书
创建时间: 2020-07-28 15:38:49
过期时间: 已过期

关联资源			
负载均衡	LBID	VServerID	协议端口
lb001	lb-IRu29DVMR	vs-Av1Dp5VGg	HTTPS:443

(1) 基本信息

SSL 证书的基本信息，包括资源 ID、名称、证书类型、主域名、备域名、MD5 值、证书内容、创建时间及证书的过期时间。用户可通过资源列表上或基本信息中的【查看证书】按钮查询当前证书的内容，如下图所示：



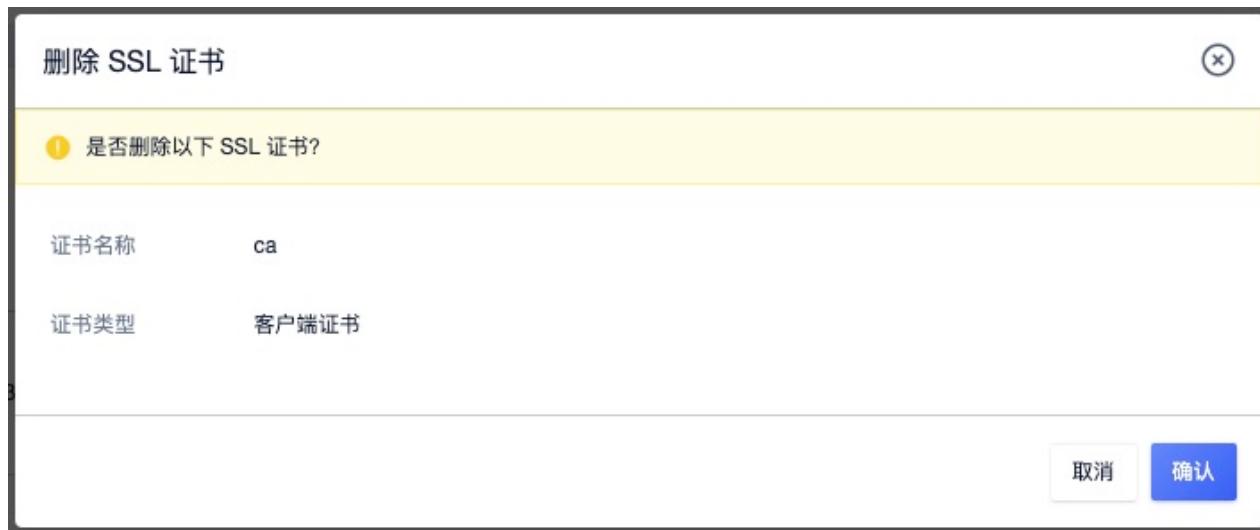
若证书已过期，可通过点击已过期查看证书内容本身的具体过期时间。

(2) 关联资源

通过已关联资源信息列表，可查看当前 SSL 证书已被关联的负载均衡及 VServer 信息，包括负载均衡名称、LBID、VServerID、VServer 的协议端口，如概览页所示，证书已关联 1 个资源（HTTPS:443）。

10.6.4 删除 SSL 证书

用户删除 SSL 证书，仅允许删除未被使用的的 SSL 证书。若一个 SSL 证书已关联一个负载均衡的 VServer，则不可进行删除。



证书被删除后即在平台彻底销毁，不可进行恢复，可重新进行上传并关联负载均衡进行使用。

11 NAT 网关

11.1 NAT 网关简介

11.1.1 概述

NAT 网关（NAT Gateway）是一种类似 [NAT](#) 网络地址转换协议的 VPC 网关，为云平台资源提供 SNAT 和 DNAT 代理，支持互联网地址转换能力，并支持普通和白名单两种资源网络出口模式。

用户可通过 NAT 网关让 VPC 子网中未绑定外网 IP 的虚拟机访问外网，同时可配置端口转发规则使虚拟机、数据库 MySQL 及 Redis 服务对外提供服务。作为一个虚拟网关设备，需要绑定外网 IP 作为 NAT 网关的默认统一出口，支持普通和白名单两种网络出口模式。

- 普通模式下，NAT 网关指定子网中所有未绑定外网 IP 的云资源，均可通过 NAT 网关访问互联网或 IDC 数据中心的物理网络。
- 白名单模式下，NAT 网关指定子网中且在白名单中定义的云资源，才可通过 NAT 网关访问互联网或 IDC 数据中心的物理网络。

同时网关提供 DNAT 能力，支持配置基于 TCP 和 UDP 两种协议的端口转发，将 VPC 内的云资源内网端口映射到 NAT 网关所绑定的外网 IP，对互联网或 IDC 数据中心网络提供服务。NAT 网关具有地域（数据中心）属性，仅支持相同数据中心下同 VPC 虚拟资源的 SNAT 和 DNAT 转发服务，

虚拟机通过 NAT 网关可访问的网络取决于绑定的外网 IP 所属网段在物理网络上的配置，若所绑定的外网 IP 可通向互联网，则虚拟机可通过 NAT 网关访问互联网；若所绑定的外网 IP 可通向 IDC 数据中心的物理网络，则虚拟机通过 NAT 网关访问 IDC 数据中心的物理网络。

11.1.2 应用场景

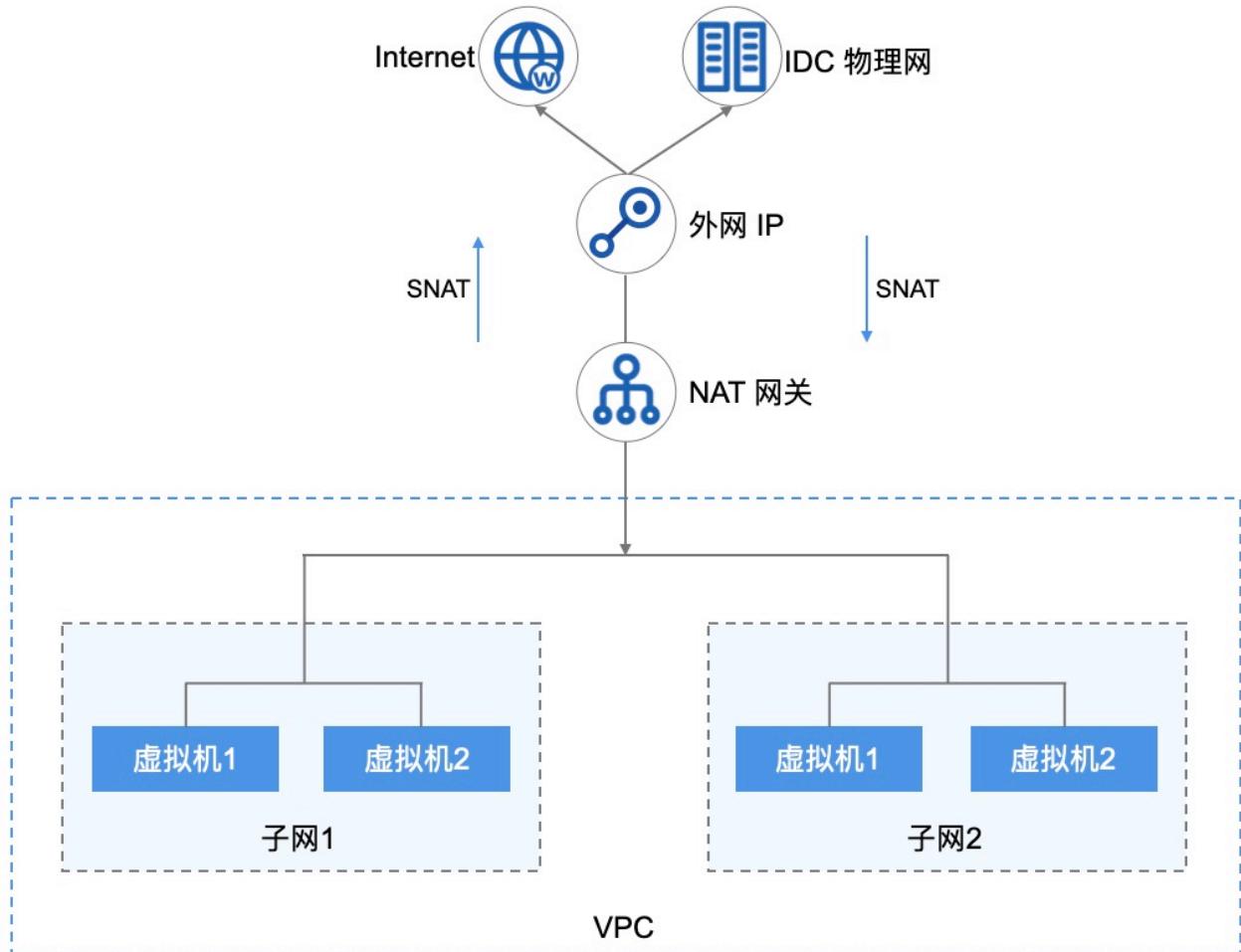
用户在平台使用虚拟机部署应用服务时，有访问外网或通过外网访问虚拟机的应用场景，通常我们会在每一台虚拟机上绑定一个外网 IP 用于和互联网或 IDC 数据中心网络进行通信。真实环境和案例中，可能无法分配足够的公网 IP，即使公网 IP 足够也无需在每一台需要访问外网的虚拟机上绑定外网 IP 地址。

- 共享 EIP：通过 SNAT 代理，使多台 VPC 内网虚拟机共享 1 个外网 IP 地址访问互联网或 IDC 数据中心的物理网络。
- 屏蔽真实 IP：通过 SNAT 代理，多台 VPC 内网虚拟机使用代理 IP 地址通信，自动屏蔽真实 IP 内网地址。
- VPC 内网虚拟机提供外网服务：通过 DNAT 代理，配置 IP 及端口转发，对互联网或 IDC 数据中心的网络提供业务服务。

11.1.3 架构原理

平台产品服务底层资源统一，NAT 网关实例为主备高可用集群架构，可实现 NAT 网关故障自动切换，提高 SNAT 和 DNAT 服务的可用性。同时结合外网 IP 地址，根据 NAT 配置为租户虚拟资源提供 SNAT 和 DNAT 代理。

在产品层面，租户通过申请一个 NAT 网关，指定 NAT 网关可允许通信的子网，通过绑定【外网 IP】使多子网下虚拟机与互联网或 IDC 数据中心物理网进行通信，具体逻辑架构图如下：



- 平台支持同 VPC 多子网虚拟机使用 NAT 网关访问互联网或 IDC 数据中心网络。
- 当多个子网中未绑定外网 IP 的虚拟机关联 NAT 网关时，平台将自动在虚拟机中下发访问外网的路由。
- 虚拟机通过下发的路由，将访问外网的数据通过 NAT 网关透传至已绑定的【外网 IP】。
- 透传至外网 IP 的数据通过平台 OVS 及物理网卡将数据包发送至物理交换机，完成数据 SNAT 的通信。
- 当外网需要访问 VPC 中的虚拟机或 MySQL 服务时，可通过 NAT 网关端口转发，使互联网或 IDC 物理网通过 NAT 网关已绑定的 IP+端口访问 VPC 内网服务。

NAT 网关 SNAT 功能支持白名单模式，即仅支持多子网中已添加至白名单的虚拟机通过 NAT 网关提供 SNAT 地址转换服务。

11.1.4 功能特性

云平台提供 NAT 网关全生命周期管理，包括 NAT 网关的增删改查、模式设置、DNAT 端口转发及资源绑定等。

- **多子网绑定**

NAT 网关服务的核心价值是为平台虚拟机提供 SNAT 和 DNAT 的功能，节省 IP 地址的同时提升部署效率。一个 VPC 支持多个子网，NAT 网关可为指定的多个子网同时提供地址转换服务，使【多个子网】中的虚拟机均通过 NAT 网关与外网或 IDC 物理网进行通信。

- 用户可将一个 VPC 中的一个子网绑定至 NAT 网关，也可将一个 VPC 中的部分子网绑定至 NAT 网关。
- 支持用户将一个 VPC 中的所有子网绑定至 NAT 网关，同时支持用户移除部分子网。

- 指定子网后，子网下未绑定外网 IP 且在白名单中的虚拟机可通过 NAT 网关与外界通信。

- **SNAT 能力**

NAT 网关支持 SNAT (Source Network Address Translation 源地址转换)，即 VPC 子网 IP 地址转换为外网 IP 地址进行网络访问。通过 SNAT 功能，关联 NAT 网关的虚拟机可在不绑定外网 IP 的情况下，与外网通信。

- 在虚拟机未绑定外网 IP 地址的情况下，NAT 绑定的外网 IP 将作为所有关联虚拟机的默认网络出口，共享外网 IP 地址访问互联网信息和服务。
- 若虚拟机已添加 NAT 网关白名单在绑定外网 IP 时，默认会将虚拟机从 NAT 网关白名单移除，以虚拟机绑定的外网 IP 地址为虚拟机的默认出口。

- **出口模式：NAT 网关支持多种网络出口模式，包括普通模式和白名单模式。**

- 普通模式下 NAT 网关指定子网中所有未绑定外网 IP 的虚拟机，均可通过 NAT 网关访问外网或 IDC 数据中心的网络。
- 白名单模式下 NAT 网关指定子网中且在白名单中定义的云资源，才可通过 NAT 网关访问外网或 IDC 数据中心的网络。
- 支持修改出口模式，从普通模式切换到白名单模式，则白名单生效。若从白名单模式切换到普通模式，则白名单失效，网关所关联的子网中的虚拟机均可通过 NAT 网关与外界通信。

- **DNAT 能力**

NAT 网关支持 DNAT (Destination Network Address Translation 目的地地址转换)，也称为端口转发或端口映射，即将外网 IP 地址转换为 VPC 子网的 IP 地址提供网络服务。

- 支持 TCP 和 UDP 两种协议的端口转发，支持对端口转发规则进行生命周期管理。
- 支持批量进行多端口转发规则配置，即支持映射端口段，如 TCP:1024~TCP:1030。
- NAT 网关绑定外网 IP 时，端口转发规则为 VPC 子网内的虚拟机提供互联网外网服务，可通过外网访问子网内的虚拟机服务。

- **监控告警**

平台支持对 NAT 网关进行监控数据的收集和展示，通过监控数据展示每一个 NAT 网关的指标数据，同时支持为每一个监控指标设置阈值告警及通知策略。支持的监控指标包括网络出/带宽、网络出/包量及连接数。

支持查看一个 NAT 网关多时间维度的监控数据，包括 1 小时、6 小时、12 小时、1 天、7 天、15 天及自定义时间的监控数据。默认查询数据成为 1 小时的数据，最多可查看 1 个月的监控数据。

- **NAT 网关安全**

NAT 网关的网络访问控制可以关联安全组给予安全保障，通过安全组的规则可控制到达 NAT 网关所绑定外网 IP 的入站流量及出站流量，支持 TCP、UDP、ICMP、GRE 等协议数据包的过滤和控制。

安全组及安全组的规则支持对已关联安全组的 NAT 网关的流量进行限制，仅允许安全组规则内的流量透传安全组到达目的地。

- **NAT 网关高可用**

NAT 网关实例支持高可用架构，即至少由 2 个虚拟机实例构建，支持双机热备。当一个 NAT 网关的实例发生故障时，支持自动在线切换到另一个虚拟机实例，保证 NAT 代理业务正常。同时基于外网 IP 地址的漂移特性，支持在物理机宕机时，保证 SNAT 网关出口及 DNAT 入口的可用性。

- **NAT 网关隔离性**

- 资源隔离

- NAT 网关具有数据中心属性，不同数据中心间 NAT 网关资源物理隔离；

- NAT 网关资源在租户间相互隔离，租户可查看并管理账号及子账号下所有 NAT 网关资源；
 - 一个租户内的 NAT 网关资源，仅支持绑定租户内同数据中心的 VPC 子网资源；
 - 一个租户内的 NAT 网关资源，仅支持绑定租户内同数据中心的外网 IP 资源；
 - 一个租户内的 NAT 网关资源，仅支持绑定租户内同数据中心的安全组资源。
- 网络隔离
 - 不同数据中心间 NAT 网关资源网络相互物理隔离；
 - 同数据中心 NAT 网关网络采用 VPC 进行隔离，不同 VPC 的 NAT 网关资源无法相互通信；
 - NAT 网关绑定的外网 IP 网络隔离取决于用户物理网络的配置，如不同的 Vlan 等。

11.2 使用流程

在使用 NAT 网关服务前，需根据业务需求规划 NAT 网关的 VPC 网络及外网 IP 网络，并根据业务需求将多台虚拟机绑定至 NAT 网关。具体流程如下：

1. 租户根据需求创建 VPC 和子网，并在多个子网中创建虚拟机；
2. 租户根据需求创建 外网 IP 地址，并通过 API 或控制台指定网络类型、关联子网及绑定的出口 IP 地址，创建一个 NAT 网关；
3. 若 NAT 网关的网络出口模式为默认，则关联子网中所有未绑定公网 IP 的虚拟机可通过 NAT 网关访问外网；
4. 若 NAT 网关的网络出口模式为白名单，则关联子网中所有未绑定公网 IP 且添加至白名单列表中的虚拟机可通过 NAT 网关访问外网；
5. 租户可通过 NAT 网关的端口转发功能，配置需要通过外网访问 VPC 网络中未绑定公网 IP 的虚拟机及服务。

11.3 创建 NAT 网关

用户在平台创建 NAT 网关需指定机型、VPC 网络、子网、外网 IP、安全组及 NAT 网关名称和备注信息。可通过导航栏进入【NAT 网关】资源控制台，通过“创建 NAT 网关”进入创建向导页面，如下图所示：

基础配置

机型 * 高性能(x86_64) GPU(x86_64) 普通型(x86_64)

NATGW名称 * 请输入资源名称

NATGW备注 请输入资源描述

网络设置

VPC * vpc002(10.0.0.0/16)

子网 * 10.192(10.0.192.0/20)

剩余IP数: 4082

外网IP * 2323(120.132.107.202)

仅支持 IPv4 版本且有默认路由的外网 IP

外网安全组 * dff232323(sg-1kSj7gVGg)

1. 选择并配置 NAT 网关基础配置及网络设置信息：

- 机型：NAT 网关实例所在宿主机的集群类型，由平台管理员自定义（如 x86 机型）。
- 名称/备注：NAT 网关的名称及备注信息。
- VPC 网络：NAT 网关所服务的 VPC 网络，即 NAT 网关仅为所选择的 VPC 内资源提供 SNAT 和 DNAT 服务，同时在白名单模式下，仅支持添加相同 VPC 网络的虚拟机进入白名单通过 NAT 网关访问外网。
- 子网：NAT 网关实例所在子网，通常建议选择可用 IP 数量充足的子网。
- 外网 IP：NAT 网关地址所使用的外网 IP 地址，VPC 网络内绑定的资源均通过 NAT 网关所绑定的外网 IP 地址访问互联网或 IDC 物理网络，仅支持绑定有默认路由的外网 IP 地址。
- 安全组：NAT 网关的外网 IP 地址所使用的安全组，控制可进入 NAT 网关的流量。

2. 选择并配置以上信息后，可选择购买数量和付费方式，确认订单金额并点击“立即购买”进行 NAT 网关创建：

- 购买数量：按照所选配置及参数批量创建 NAT 网关实例，一次仅支持创建 1 个 NAT 网关实例。
- 付费方式：选择 NAT 网关的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式。
- 合计费用：用户选择 NAT 网关资源按照付费方式的费用展示。

确认订单无误后点击立即购买，点击立即购买后，会返回 NAT 网关资源列表页，在列表页可查看 NAT 网关的创建过程，通常会先显示“创建中”的状态，创建成功后转换为“运行”。

允许在一个 VPC 下创建多个 NAT 网关，将 VPC 下的虚拟机分批添加至多个 NAT 网关中，实现 NAT 网关分流，应对大批量虚拟机共享外网 IP 地址访问外网的场景。

11.4 查看 NAT 网关

通过导航栏进入 NAT 网关资源控制台，可查看 NAT 网关资源列表，并可通过列表上名称和 ID 进入详情页面查看 NAT 网关的概览及监控信息，同时可切换至白名单标签页对 NAT 网关的白名单进行管理。

11.4.1 NAT 网关列表

NAT 网关列表可查看当前账户下所有 NAT 网关的资源信息，包括名称、资源 ID、VPC、子网、安全组、外网 IP、创建时间、过期时间、计费方式、状态及操作项，如下图所示：

The screenshot shows a table of NAT gateway resources. Each row contains the following columns: Name, Resource ID, VPC, Subnet, Security Group, External IP, Creation Time, Expiration Time, Billing Method, Status, and Operations. Row 1 (2323) has values: vpc002, vpc-SX33TjgMR, 10.192, subnet-b3VqTNzGR, sg-ikSj7gVGg, 120.132.107.202, 2020-07-28, 2020-08-28, Month, Running, with buttons for Details, Delete, and More. Row 2 (NATGW001) has values: vpc002, vpc-SX33TjgMR, 10.192, subnet-b3VqTNzGR, Default, sg-C0vkuVpm, 106.75.234.74, 2020-07-28, 2020-08-28, Month, Running, with similar buttons. At the bottom right, there are navigation icons, a page size selector (10 items per page), and a total count of 1 item.

- 名称/ID：NAT 网关的名称及全局唯一标识符。
- 外网 IP：NAT 网关所绑定的外网 IP 地址，加入至白名单的虚拟机均通过该 IP 地址访问外网。
- 状态：NAT 网关的运行状态，包括创建中、运行、删除中等。
- 创建时间/过期时间：指当前 NAT 网关的创建时间和费用过期时间。
- 计费方式：指当前 NAT 网关创建时指定的计费方式。

列表上操作项是指对单个 NAT 网关实例的操作，包括删除及修改安全组等，可通过搜索框对 NAT 网关资源列表进行搜索和筛选，支持模糊搜索。

为方便租户对资源的统计及维护，平台支持下载当前用户所拥有的所有 NAT 网关资源列表信息为 Excel 表格；同时支持对 NAT 网关进行批量删除操作。

11.4.2 NAT 网关详情

在 NAT 网关资源列表上，点击“名称”可进入概览页面查看当前 NAT 网关实例的详细信息，同时可切换至白名单页面对当前 NAT 网关的白名单进行管理，如概览页所示：

The screenshot shows the detailed overview of a specific NAT gateway. On the left, the 'Basic Information' panel displays details like Resource ID (natgw-PnGCMp4Mg), Name (2323), VPC (vpc002), Subnet (10.192), Security Group (df232323), IP (120.132.107.202), Status (Running), Billing Type (Month), Creation Time (2020-07-28 17:39:20), and Expiration Time (2020-08-28 17:39:20). On the right, there are three monitoring charts: 1. 'Network Card Inbound Bandwidth (Mbps)' vs. Time (2020-07-28 17:09:00 to 2020-07-28 18:08:55). 2. 'Network Card Outbound Bandwidth (Mbps)' vs. Time (2020-07-28 17:09:00 to 2020-07-28 17:57:00). 3. 'Connection Number' vs. Time (2020-07-28 17:25:00 to 2020-07-28 17:41:00). A top navigation bar includes tabs for Overview, White List, and Operation Log, along with a refresh button and a switch for automatic refresh.

(1) 基本信息

NAT 网关的基本信息，包括名称、ID、VPC 网络、子网、外网 IP、安全组、状态、计费方式、创建时间、过期时间及告警模板信息，可点击告警模板右侧按钮修改 NAT 网关所关联的告警模板。

(2) 监控信息

NAT 网关实例相关的监控图表及信息，包括网卡入/出带宽、网卡入/出包量及连接数，支持查看 1 小时、6 小时、12 小时、1 天及自定义时间的监控数据。

(3) 白名单管理

NAT 网关绑定白名单管理，即可通过 NAT 网关访问外网的虚拟资源管理，包括白名单资源的添加、查看及移除操作等，详见[白名单管理](#)。

11.5 修改告警模板

修改告警模板是对 NAT 网关的监控数据进行告警的配置，通过告警模板定义的指标及阈值，可在 NAT 网关相关指标故障及超过指标阈值时，触发告警，通知相关人员进行故障处理，保证 NAT 网关及业务的网络通信。

用户可通过 NAT 网关详情概览页的操作项进行告警模板修改操作，在修改告警模板向导中选择新 NAT 网关告警模板进行修改。

11.6 删除 NAT 网关

用户可通过控制台或 API 的方式删除不需要的 NAT 网关实例，删除时会自动解绑已绑定的外网 IP 地址，并清除 NAT 网关已添加的白名单资源及路由策略等。



NAT 网关被删除后即直接销毁，请在删除前确保 NAT 网关无业务流量访问外网请求，否则可能影响业务访问。

11.7 修改名称和备注

修改 NAT 网关资源的名称和备注，在任何状态下均可进行操作。可通过点击 NAT 网关资源列表页面每个 NAT 网关名称右侧的“编辑”按钮进行修改。

11.8 修改安全组

绑定至 NAT 网关的安全组策略作用于 NAT 网关出口的外网 IP，用于限制通过 NAT 网关出口流量。支持修改 NAT 网关的安全组，用户可通过 NAT 网关列表操作项中的“修改安全组”进行修改操作，如下图所示：



一个 NAT 网关仅支持绑定一个安全组，修改成功安全组即时生效，平台会以新的安全组策略对进出 NAT 网关的流量进行限制，用户可通过 NAT 网关列表及详细信息查看已修改的安全组信息。

11.9 白名单管理

白名单是指通过 NAT 网关绑定的外网 IP 地址访问互联网或 IDC 数据中心网络的虚拟机资源集合，支持一台或多台虚拟机资源。若一台虚拟机已被添加至一个 NAT 网关白名单，则不允许在添加至其它 NAT 网关白名单中。

白名单仅支持 SNAT 功能，不对 DNAT 端口转发能力进行限制，即添加至白名单的虚拟机可通过 NAT 网关访问外网或 IDC 物理网；无论虚拟机是否添加至白名单，均可通过添加 DNAT 端口转发规则，使外网通过 NAT 网关的外网 IP 访问虚拟机部署的业务服务。

11.9.1 添加白名单

NAT 网关白名单仅支持添加未绑定外网 IP 地址的虚拟机资源，添加白名单前需确保虚拟机和 NAT 网关在同一个 VPC 网络中且状态必须为运行状态。用户可通过 NAT 网关详情页面“白名单”控制台中的“添加白名单”进入白名单添加向导页面，如下图所示：

添加白名单

白名单仅支持添加同VPC且未绑定外网弹性IP的虚拟机资源

NAT网关ID *	natgw-PnGCMp4Mg
名称	2323
IP	120.132.107.202
绑定资源类型	虚拟机
资源 *	已选择 1 项

取消 **确认**

在向导页面选择需要添加至 NAT 网关白名单，仅支持添加与 NAT 网关相同 VPC 且未绑定网 IP 地址的虚拟机资源。添加过程中，白名单虚拟机资源的状态为“绑定中”，待虚拟机的状态转换为“已绑定”时，即代表绑定成功。

同时 NAT 网关会自动下发 NAT 网关外网 IP 所属网段配置的路由到白名单的虚拟机中，使虚拟机可通过 NAT 网关访问互联网或 IDC 数据中心网络，可在虚拟机中查看与互联网的联通性。

可通过 netstat -rn 命令在 Linux 虚拟机中查看 NAT 网关自动下发的路由信息。

11.9.2 查看白名单

用户通过 NAT 网关详情页面的“白名单列表”可查看已添加至当前网关的虚拟机列表和信息，包括 NAT 网关、资源 ID、资源名称、内网 IP、状态、创建时间及操作项，如下图所示：

NAT网关 / natgw-PnGCMp4Mg

白名单						
操作		NAT网关ID	资源ID	资源名称	内网IP	状态
<input type="checkbox"/>	添加白名单	natgw-PnGCMp4Mg	vm-ETbN60nMR	host	10.0.192.12	已绑定
<input type="button" value="移除白名单"/> 1 10 条/页 /1						

- 资源名称/ID：已添加至 NAT 网关白名单的虚拟机的名称和全局唯一标识符。
- 内网 IP：已添加至 NAT 网关白名单的虚拟机内网 IP 地址。
- 创建时间：当前虚拟机绑定至 NAT 网关白名单的时间。
- 状态：当前白名单资源的状态，包括绑定中、已绑定、解绑中。

列表上操作项是指对单条白名单资源的移除操作，为方便租户对资源的统计及维护，平台支持下载当前 NAT 网关所添加的所有白名单资源列表信息为 Excel 表格，同时支持对 NAT 网关白名单资源进行批量移除操作。

11.9.3 移除白名单

移除白名单指将一个虚拟机从 NAT 网关白名单解绑，可通过白名单资源列表操作项中的“移除白名单”功能进行虚拟机解绑操作。具体解绑操作如下图所示：

The screenshot shows a modal dialog titled "移除白名单" (Remove White List). It contains the following fields:

NAT网关ID *	natgw-PnGCMp4Mg
资源ID *	vm-ETbN60nMR
资源名称	host
内网IP *	10.0.192.12
状态	● 已绑定

At the bottom right of the dialog are two buttons: "取消" (Cancel) and "确认" (Confirm).

解绑过程中，白名单虚拟机状态为“解绑中”，待列表上解绑的资源被清除即代表解绑成功。解绑后不影响虚拟机本身的正常运行，自动下发的路由将清除，即不可通过 NAT 网关访问外网，可通过重新加入白名单或绑定外网 IP 地址访问外网。

12 IPSecVPN 服务

12.1 产品简介

12.1.1 背景

用户在使用云平台部署并管理应用服务时，会有部分业务部署于 IDC 数据中心环境的内网或第三方公/私有云平台上，如 Web 服务部署于公有云平台，应用和数据库等应用部署于私有云，构建公有云和私有云混合部署环境。

在混合云的应用场景中，可以可通过专线的方式将两端网络的内网直接打通，且较好的保证网络可靠性和性能。但由于专线成本较高，仅适用于部分对网络时延要求较高的业务，为节省成本并与第三方平台建立点对点的网络通信，云平台提供 VPN 网关-IPsecVPN 连接的服务能力，允许平台侧 VPC 子网的资源直接与第三方平台内网的主机进行通信，同时也可为平台不同 VPC 网络间提供连接服务。

12.1.2 概述

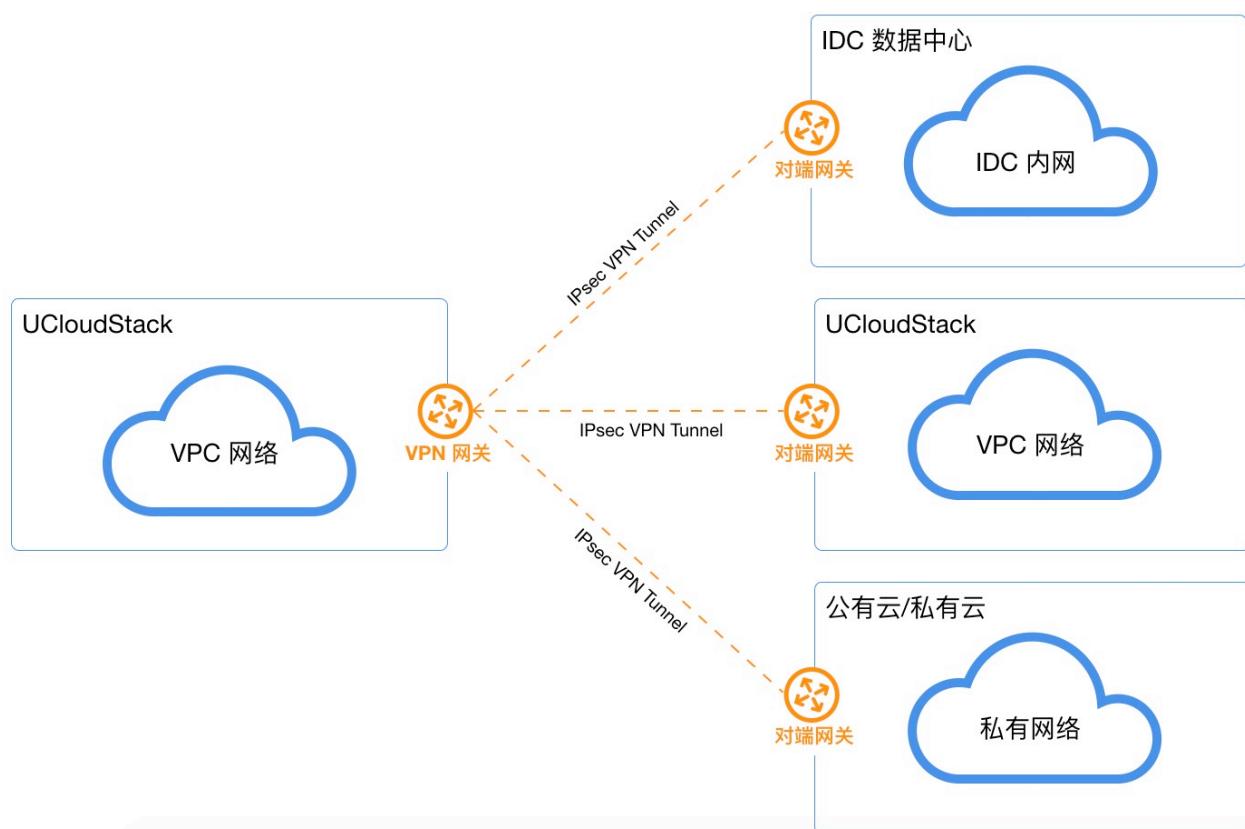
IPsec VPN 是一种采用 IPsec 协议加密的隧道技术，由 Internet Engineering Task Force (IETF) 定义的安全标准框架，在互联网上为两个私有网络提供安全通道，通过加密保证连接的安全。有关 IPsec 可参考 [RFC2409](#) (IKE—Internet Key Exchange 因特网密钥交换协议) 和 [RFC4301](#) (IPsec 架构)。

云平台 IPsecVPN 服务是基于 Internet 的网络连接服务，采用 IPsec (Internet Protocol Security) 安全加密通道实现企业数据中心、办公网络与平台 VPC 私有网络的安全可靠连接，同时也可使用 VPN 网关在 VPC 之间建立加密内网连接。网关服务为可容灾的高可用架构，同时支持用户选择多种加密及认证算法，并提供 VPN 连接健康检测及连接日志，保证隧道连接的可靠性、安全性及管理便捷性。

通过 IPsecVPN 服务，用户可将本地数据中心、企业分支机构与私有云平台的 VPC 私有网络通过加密通道进行连接，也可将用于不同 VPC 之间的加密连接。对端设备或系统仅需支持 IPsec 的 IKEv1 或 IKEv2，即可通过配置与平台的 VPN 网关进行互连，如通用网络设备或配置 IPsecVPN 的服务器。

12.1.3 逻辑架构

VPN 网关 IPsecVPN 服务由 VPN 网关、对端网关及 VPN 隧道连接三部分组成。



- **VPN 网关**

平台侧 VPC 网络建立 IPsecVPN 连接的出口网关，通过关联 VPC 和外网 IP 与对端网关的 IPsecVPN 进行连接，用于平台私有网络和外部网络（如 IDC、公有云、私有云）之间建立安全可靠的加密网络通信。

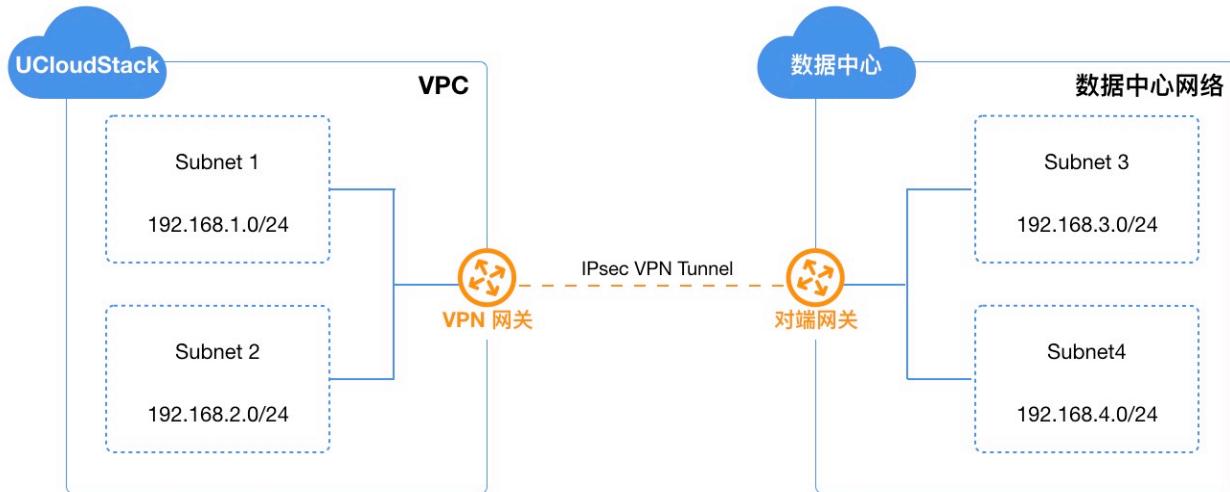
- **对端网关**

运行于外部网络端 IPsecVPN 网关的公网 IP 地址，即与私有云平台 VPN 网关进行隧道连接的网关 IP 地址，支持 NAT 转发的网关地址。

- **VPN 隧道**

连接 VPN 网关和对端网关的加密隧道，结合相应的加密认证算法及策略，为平台 VPC 私有网络和外部私有网络建立加密通信的隧道连接。

一个 VPN 网关有且必须关联 1 个 VPC 网络和 1 个外网 IP 地址，与对端网关相对应，通过 VPN 隧道进行连接。IPsecVPN 支持点到多点的连接特性，使得 VPN 网关与对端网关可以为一对一或一对多的连接关系，即一个 VPN 网关可以同时与多个对端网关建立隧道。VPN 隧道支持平台多个 VPC 子网与对端网络的多个网段通过隧道进行加密通信，平台 VPC 子网的网段与对端网络的网络不可重叠（本端与对端子网重叠会影响网络的正常通信）。



如上图案例所示，在云平台中的 VPC 网络已拥有 2 个子网，分别为 subnet1（192.168.1.0/24）和 subnet2（192.168.2.0/24）。在远端 IDC 数据中心下有 2 个内网网段，分别为 subnet3（192.168.3.0/24）和 subnet4（192.168.4.0/24）。

- 私有云平台 VPN 网关绑定 VPC 子网，并使用外网 IP 地址作为网络出口及远端数据中心的对端网关。
- 远端数据中心的平台的网关绑定数据中心子网，并使用另一个公网 IP 地址作为网络出口及私有云平台的对端网关。
- 两端 VPN 网关分别建立 IPsecVPN 隧道，使用相同的预共享密钥及加密认证策略，经过第一阶段的 IKE 认证及第二阶段的 IPsec 认证，建立 VPN 连接通道。
- 两端网络的子网分别通过 VPN 隧道与对端网络的子网进行通信，打通跨数据中心、跨云平台的内网，构建混合云环境。

IPsecVPN 通道在 Internet 网络中构建并运行，公网的带宽、网络阻塞、网络抖动会直接影响 VPN 网络通信的质量。

12.1.4 VPN 隧道建立

在建立 IPsecVPN 安全通道时，需要先在两个网关间建立 SA（Security Association 安全联盟）。SA 是 IPsec 的基础，是通信网关间对连接条件的约定，如网络认证协议（AH、ESP）、协议封装模式、加密算法（DES、3DES 和 AES）、认证算法、协商模式（主模式和野蛮模式）、共享密钥及密钥生存周期等。**SA 安全联盟的建立需要在两端网关上均约定并配置相同的条件，以确保 SA 可以对两端网关进行双向数据流通信保护。**

标准 IPsecVPN 建立 SA 的方式有手工配置和 IKE 自动协商两种，**私有云平台 VPN 网关服务使用 IKE 协议来建立 SA**。IKE 协议建立在由 ISAKMP（Internet Security Association and Key Management Protocol，互联网安全联盟和密钥管理协议）定义的框架上，具有一套自保护机制，可在不安全的网络上安全地认证身份、交换及密钥分发，为 IPsec 提供自动协商交换密钥并建立 SA 服务。

- 身份认证：支持预共享密钥（pre-shared-key）认证，确认通信两端的身份，并在密钥产生之后对身份数据进行加密传送，实现对身份数据的安全保护。

- 交换及密钥分发：DH（Diffie-Hellman，交换及密钥分发）算法是一种公共密钥算法，通信两端在不传输密钥的情况下通过交换一些数据，计算出共享的密钥。

IKE 通过两个阶段为 IPsec 进行密钥协商并建立 SA：

1. 第一阶段：通信两端彼此间建立一个已通过身份认证和安全保护的通道，即建立一个 IKE SA，作用是为两端之间彼此验证身份，并协商出 IKE SA，保护第二阶段中 IPsec SA 协商过程。支持 IKE V1 和 V2 版本，其中 V1 版本支持主模式（Main Mode）和野蛮模式（Aggressive Mode）两种 IKE 交换方法。
2. 第二阶段：用第一阶段建立的 IKE SA 为 IPsec 协商安全服务，即为 IPsec 协商具体的 SA，建立用于最终的 IP 数据安全传输的 IPsec SA。

IKE 为 IPsec 协商建立 SA，并将建立的参数及生成的密钥交给 IPsec，IPsec 使用 IKE 协议建立的 SA 对最终 IP 报文加密或认证处理。通过 IKE 协议可为 IPsecVPN 提供端与端之间的动态认证及密钥分发，通过自动建立 IPsec 参数，降低手工配置参数的复杂度；同时由于 IKE 协议中每次 SA 的建立均需运行 DH 交换过程，可有效保证每个 SA 所使用密钥的互不相关，增加 VPN 通道的安全性。

VPN 隧道成功建立连接后，将自动为所属 VPC 关联的本端子网下发到对端子网的路由，使本端子网访问远端私有网络的请求通过 VPN 网关及隧道进行转发，完成整个链路的打通。

12.1.5 VPN 隧道参数

IPsecVPN 隧道 SA 协商建立需要配置相应的参数信息，包括隧道的基本信息、预共享密钥、IKE 策略及 IPsec 策略配置信息。两端的 VPN 在建立的过程中，需保证预共享密钥、IKE 策略及 IPsec 策略配置一致，IKE 策略指定 IPSec 隧道在协商阶段的加密和认证算法，IPSec 策略指定 IPSec 在数据传输阶段所使用的协议及加密认证算法。具体参数信息如下表所示：

(1) 基本信息

- **名称/备注**：VPN 隧道连接的名称和备注。
- **VPN 网关**：VPN 隧道挂载的 VPN 网关，即隧道运行在云平台端的所属 VPN 网关。
- **对端网关**：VPN 隧道挂载的对端网关，即对端网关的互联网出口 IP 地址，如 IDC 数据中心的 VPN 网关。
- **本端网段**：VPN 网关所在 VPC 网络内需要和对端网络（如 IDC 数据中心）互通的子网，如 192.168.1.0/24。本端网段用于第二阶段协商，不可与对端网段重叠。
- **对端网段**：IDC 数据中心或第三方云平台中需要与本端网段 VPN 通信的子网，如 192.168.2.0/24。对端网段用于第二阶段协商，不可与本端网段重叠。

(2) 预共享密钥

- **Pre Shared Key**：IPsecVPN 连接的秘钥，用于 VPN 连接的协商，在 VPN 连接协商过程中，需保证本端与对端的密钥一致。

(3) IKE 策略

- **版本**：IKE 密钥交换协议的版本，支持 V1 和 V2。V2 版对 SA 的协商过程进行简化且更加适应多网段场景，推荐选择 V2 版本。
- **认证算法**：为 IKE 协商过程中的报文提供认证，支持 md5、sha1 和 sha2-256 三种认证算法。
- **加密算法**：为 IKE 协商过程中的报文提供加密保护，支持 3des、aes128、aes192、aes256 四种加密算法。
- **协商模式**：IKE v1 的协商模式，支持主模式（main）和野蛮模式（aggressive）。

- 主模式在 IKE 协商时需经过 SA 交换、密钥交换、身份验证三个双向交换阶段（6 个消息），而野蛮模式仅需要经过 SA 生成/密钥交换和身份验证两次交换阶段（3 个消息）。
- 由于野蛮模式密钥交换与身份认证一起进行无法提供身份保护，因此主模式的协商过程安全性更高，协商成功后信息传输安全性一致。
- 主模式适用于两端设备的公网 IP 固定的场景，野蛮模式适用于需要 NAT 穿越及 IP 地址不固定的场景。
- **DH 组**：指定 IKE 交换密钥时使用的 Diffie-Hellman 算法，密钥交换的安全性及交换时间随 DH 组的扩大而增加，支持 1、2、5、14、24。
 - 1：采用 768-bit 模指数（Modular Exponential, MODP）算法的 DH 组。
 - 2：采用 1024-bit MODP 算法的 DH 组。
 - 5：采用 1536-bit MODP 算法的 DH 组。
 - 14：采用 2048-bit MODP 算法的 DH 组。
 - 24：带 256 位的素数阶子群的 2048-bit MODP 算法 DH 组。
- **本端标识**：VPN 网关的标识，用于 IKE 第一阶段协商。支持 IP 地址和 FQDN（全称域名）。
- **对端标识**：对端网关的标识，用于 IKE 第一阶段协商。支持 IP 地址和 FQDN（全称域名）
- **生存周期**：第一阶段 SA 的生存时间，在超过生存周期后，SA 将被重新协商，如 86400 秒。

(4) IPSec 策略

- **安全传输协议**：IPSec 支持 AH 和 ESP 两种安全协议，AH 只支持数据的认证保护，ESP 支持认证和加密，推荐使用 ESP 协议。
- **IPSec 认证算法**：为第二阶段用户数据提供的认证保护功能，支持 md5 和 sha1 两种认证算法。
- **IPSec 加密算法**：为第二阶段用户数据提供的加密保护功能，支持 3des、aes128、aes192 和 aes256 四种加密算法，使用 AH 安全协议时不可用。
- **PFS DH 组**：PFS（Perfect Forward Secrecy，完善的前向安全性）特性是一种安全特性，指一个密钥被破解，并不影响其他密钥的安全性。PFS 特性为第二阶段协商的 Diffie-Hellman 密钥交换算法，支持的 DH 组为支持 1、2、5、14、24 与关闭（Disable），Disable 适用于不支持 PFS 的客户端。
- **生存周期**：第二阶段 SA 的生存时间，在超过生存周期后，SA 将被重新协商，如 86400 秒。

12.1.6 应用场景

VPN 网关 IPsecVPN 服务是基于 Internet 的网络连接服务，通过 IPsec 安全加密通道实现企业数据中心、办公网络与平台 VPC 私有网络的安全可靠连接，同时用户也可使用 VPN 网关在 VPC 之间建立加密内网连接。网关服务为可容灾的高可用架构，同时支持用户选择多种加密及认证算法，并提供 VPN 连接健康检测及连接日志，可满足不同的应用场景。

- VPC 到本地数据中心的连接：通过 IPsecVPN 服务将本地数据中心的内网主机和 VPC 网络的虚拟资源进行连接，构建混合云服务模式。
- VPC 到公有云 VPC 的连接：通过 IPsecVPN 服务将第三方公有云 VPC 私有网络和私有云 VPC 网络的虚拟资源进行连接，构建多云混合服务模式。
- VPC 到第三方私有云内网的连接：通过 IPsecVPN 服务将第三方私有云的 VPC 私有网络和 UCloudStack VPC 网络的虚拟资源进行连接，构建多云混合服务模式。
- VPC 到 VPC 的连接：通过 IPsecVPN 服务将 VPC 与另一个 VPC 网络进行连接，实现 VPC 打通的场景。

12.2 使用流程

使用 VPN 网关 IPsec 服务前，需要明确场景并根据不同场景部署 VPN 及连接：

- 租户根据需要创建本端 VPC 网络及子网，并在子网中部署虚拟机。
- 租户根据需求指定 VPN 网关所在的 VPC 网络外网 IP 地址、安全组等参数创建高可用 VPN 网关。
- 租户根据对端网关的 IP 地址创建对端网关。
- 租户根据需求指定 VPN 隧道基本参数、预共享密钥、IKE 策略及 IPsec 策略部署 IPsec VPN 隧道。
- 用户使用一致的 VPN 隧道参数对远端网关设备的 VPN 进行配置。（远端网关设备指 IDC 数据中心的 VPN 路由设备、不同于本端 VPC 的 VPN 网关或第三方云平台的 VPN 网关等）
- 根据需求配置 VPC 私有网络中需要通信主机的路由，若可以自动下发路由，则无需配置路由。
- 测试网络连通性，如本端 VPC 子网中虚拟机 ping 远端私有网络中的 IP 地址，验证通信是否正常。

通常情况下，IKE 协议采用 UDP 的 500 和 4500 端口进行通信，IPsec 的 AH 和 ESP 协议分别使用 51 或 50 号协议来工作，因此为保障 IKE 和 IPsec 的正常运行，需要确保应用 IKE 和 IPsec 配置的网关设备或防火墙已开放以上端口和协议的流量。

IPSecVPN 服务是基于互联网的加密通信服务，在使用 IPSecVPN 前需确认两端网关均有固定或 NAT 后的互联网 IP 地址。

12.3 VPN 网关

用户根据网络规划需求创建 VPN 网关，用于和对端网关建立 IPSecVPN 隧道连接，提供安全加密的 VPN 专属网络通道。

12.3.1 创建 VPN 网关

创建 VPN 网关时需指定机型、VPC 网络、子网、外网 IP、安全组及 VPN 网关名称和备注信息，可通过导航栏 "IPSecVPN" 进入【VPN 网关】资源控制台，通过“创建 VPN 网关”进入创建向导页面，如下图所示：

基础配置

机型 * GPU(x86_64) 普通型(x86_64) 高性能(x86_64)

VPN名称 * 请输入资源名称

VPN备注 请输入资源描述

网络设置

所属VPC * vpc002(10.0.0.0/16)

子网 * 10.192(10.0.192.0/20)

剩余IP数: 4082

外网IP * 3434(106.75.234.74)

仅支持 IPv4 版本且有默认路由的外网 IP

1. 选择并配置 VPN 网关基础配置及网络设置信息：

- 机型：VPN 网关实例所在宿主机的集群类型，由平台管理员自定义（如 x86 机型）。
- 名称/备注：VPN 网关的名称及备注信息。
- VPC 网络：VPN 网关所服务的 VPC 网络，即 VPN 网关仅为所选择的 VPC 内资源提供 IPSecVPN 通信服务，仅支持添加相同 VPC 网络的子网到关联隧道的本端网关。
- 子网：VPN 网关实例所在子网，通常建议选择可用 IP 数量充足的子网。
- 外网 IP：VPN 网关所使用的外网 IP 地址，即对端网关建立 IPSecVPN 隧道的本端网关地址，仅支持绑定相同数据中心且有默认路由的外网 IP 地址。

2. 选择并配置以上信息后，可选择购买数量和付费方式，确认订单金额并点击“立即购买”进行 VPN 网关创建：

- 购买数量：按照所选配置及参数批量创建 VPN 网关实例，一次仅支持创建 1 个 VPN 网关实例。
- 付费方式：选择 VPN 网关的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式。
- 合计费用：用户选择 VPN 网关资源按照付费方式的费用展示。

确认订单无误后点击立即购买，点击立即购买后，会返回 VPN 网关资源列表页，在列表页可查看 VPN 网关的创建过程，通常会先显示“创建中”的状态，创建成功后转换为“运行”。

允许在一个 VPC 下创建多个 VPN 网关，将 VPC 子网分别与不同的对端网关建立隧道，实现同 VPC 下不同子网与对端不同子网建立隧道的通信场景。

12.3.2 查看 VPN 网关

通过导航栏进入 VPN 网关资源控制台，可查看 VPN 网关资源列表，并可通过列表上名称和 ID 进入详情页面查看 VPN 网关的概览及监控信息。

12.3.2.1 VPN 网关列表

VPN 网关列表可查看当前账户下所有 VPN 网关的资源信息，包括名称、资源 ID、VPC、子网、外网 IP、隧道数量、创建时间、过期时间、计费方式、状态及操作项，如下图所示：

The screenshot shows a list of VPN gateways. Each entry includes columns for Name, Resource ID, Associated VPC, Subnet, External IP, Tunnel Count, Billing Method, Creation Time, Expiry Time, Status, and Operations. The '2323' entry has a status of 'Running'. The 'VPN网关' entry also has a status of 'Running'. The interface includes a search bar and pagination controls.

名称	资源ID	所属VPC	子网	外网IP	隧道数量	计费方式	创建时间	过期时间	状态	操作
2323 修改名称及备注	ipsvpn-CD8g0T4GR	vpc-SX33TjgMR	subnet-b3VqTNzGR	106.75.234.74	0	月	2020-07-29	2020-08-29	运行	<button>详情</button> <button>删除</button>
VPN网关 修改名称及备注	ipsvpn-0RcXum4Mg	vpc-SX33TjgMR	subnet-b3VqTNzGR	106.75.234.78	1	月	2020-07-24	2020-08-24	运行	<button>详情</button> <button>删除</button>

- 名称/ID：VPN 网关的名称及全局唯一标识符。
- VPC 网络：VPN 网关所服务的 VPC 网络，即 VPN 网关仅为所选择的 VPC 内资源提供 IPSecVPN 通信服务，仅支持添加相同 VPC 网络的子网到关联隧道的本端网关。
- 子网：VPN 网关实例所在子网。
- 外网 IP：VPN 网关所使用的外网 IP 地址，即对端网关建立 IPSecVPN 隧道的本端网关地址。以远端数据中心或云平台与当前网关建立隧道时必须指定该 IP 地址或 SNAT 后的地址作为对端网关 IP 地址。
- 隧道数量：当前 VPN 网关上已创建的隧道数量。
- 状态：VPN 网关的运行状态，包括创建中、运行、删除中等。

列表上操作项是指对单个 VPN 网关实例的删除操作，可通过搜索框对负载均衡资源列表进行搜索和筛选，支持模糊搜索。

为方便租户对资源的统计及维护，平台支持下载当前用户所拥有的所有 VPN 网关资源列表信息为 Excel 表格；同时支持对 VPN 网关进行批量删除操作。

12.3.2.2 VPN 网关详情

在 VPN 网关资源列表上，点击“名称”可进入概览页面查看当前 VPN 网关实例的详细信息，如概览页所示：



(1) 基本信息

VPN 网关的基本信息，包括名称、ID、VPC 网络、子网、外网 IP、隧道数量、计费方式、状态、创建时间、过期时间及告警模板信息，可点击告警模板右侧按钮修改 VPN 网关所关联的告警模板。

(2) 监控信息

VPN 网关实例相关的监控图表及信息，包括网卡入/出带宽、网卡入/出包量及 VPN 网关的出带宽使用率，支持查看 1 小时、6 小时、12 小时、1 天及自定义时间的监控数据。

12.3.3 修改名称和备注

修改 VPN 网关资源的名称和备注，在任何状态下均可进行操作。可通过点击 VPN 网关资源列表页面每个 VPN 网关名称右侧的“编辑”按钮进行修改。

12.3.4 修改告警模板

修改告警模板是对 VPN 网关的监控数据进行告警的配置，通过告警模板定义的指标及阈值，可在 VPN 网关相关指标故障及超过指标阈值时，触发告警，通知相关人员进行故障处理，保证 VPN 网关及业务的网络通信。

用户可通过 VPN 网关网关详情概览页的操作项进行告警模板修改操作，在修改告警模板向导中选择新 VPN 网关告警模板进行修改。

12.3.5 删除 VPN 网关

用户可通过控制台或 API 的方式删除不需要的 VPN 网关实例，删除时会自动解绑已绑定的外网 IP 地址。仅支持删除未关联任何 VPN 隧道的网关，删除前需将 VPN 网关已关联的隧道连接进行删除。



VPN 网关被删除后即直接销毁，请在删除前确保 VPN 网关无业务流量访问请求，否则可能影响业务访问。

12.4 对端网关

运行于外部网络端 IPsecVPN 网关的公网 IP 地址，即与私有云平台 VPN 网关进行隧道连接的网关。对端网关可以认为是与当前平台建立 VPN 连接的第三方私有云平台、IDC 数据中心及公有云平台的 VPN 网关 IP 地址。

12.4.1 创建对端网关

创建对端网关需指定对端网关的公网 IP 地址。由于 **IPSecVPN** 服务是基于互联网的加密通信服务，在使用前需确认两端网关均有固定或 NAT 后的互联网 IP 地址。用户在输入正确定的 IP 地址后即可创建对端网关，用于创建隧道连接。



若远端网络 VPN 网关使用的是内网地址，需提供内网地址被 SNAT 后的固定公网 IP 地址。若远端网络 SNAT 后的地址为非固定公网 IP 地址，如 IP 地址池，则将对端网关录入为 **0.0.0.0**，即代表和任意的对端网关 IP 地址建立隧道连接，在认证算法、密钥、本端子网和对端子网都一致的情况下，连接即可建立，使两端网络透传 NAT 进行 IPSecVPN 通信。

12.4.2 查看对端网关

在 VPN 网关资源控制台可切换至对端网关查看当前账户下所有对端网关的资源信息，包括名称、ID、公网 IP 地址、隧道数量、创建时间及操作项，如下图所示：

名称	资源ID	公网IP	隧道数量	创建时间	操作
gongyou 修改名称及备注	ipsvpn_remote-wwwFrZ4Gg	113.31.115.114	0	2020-07-25	<button>删除</button>
0.0.0.0 修改名称及备注	ipsvpn_remote-OvHrAWVG...	0.0.0.0	1	2020-07-24	<button>删除</button>
对端网关1 修改名称及备注	ipsvpn_remote-tJFB_m4GR	183.60.22.171	0	2020-07-24	<button>删除</button>

- 公网 IP 地址：指对端网关的公网 IP 地址，指定对端网关创建的隧道将以该 IP 地址为对端 IP 地址发起 VPN 连接请求，需确保该 IP 地址为正确定的远端 VPN 网关 IP 地址。
- 隧道数量：当前对端网关上已创建的隧道数量。

列表上操作项是指对单个对端网关实例的删除操作，可通过搜索框对对端网关资源列表进行搜索和筛选，支持模糊搜索。

为方便租户对资源的统计及维护，平台支持下载当前用户所拥有的所有对端网关资源列表信息为 Excel 表格；同时支持对对端网关进行批量删除操作。

12.4.3 修改名称和备注

修改对端网关资源的名称和备注，在任何状态下均可进行操作。可通过点击对端网关资源列表页面每个对端网关名称右侧的“编辑”按钮进行修改。

12.4.4 删除对端网关

用户可通过控制台或 API 的方式删除不需要的对端网关实例，仅支持删除未关联任何 VPN 隧道的对端网关，删除前需将对端网关已关联的隧道连接进行删除。

删除REMOTEGW

是否删除以下对端网关？若对端网关已关联隧道，则不可删除。

资源ID * ipsvpn_remote-wwwFrZ4Gg

资源名称 * gongyou

取消 确认

对端网关被删除后即直接销毁，请在删除前确保对端网关无业务流量访问请求，否则可能影响业务访问。

12.5 VPN 隧道

连接 VPN 网关和对端网关的加密隧道，结合相应的加密认证算法及策略，为平台 VPC 私有网络和外部私有网络建立加密通信的隧道连接，**单个 VPN 网关或对端网关最多可创建 20 条 VPN 隧道**。在使用 VPN 隧道与远端网关进行连接时，需要具备一些前提条件：

- 远端数据中心或云平台的网关设备需支持 IKEv1 和 IKEv2 版本的协议，如华为、华三、山石、深信服、Cisco ASA、Juniper 等品牌的路由器或防火墙设置，也可以为使用 Linux 系统搭建的 IPsecVPN 服务器。
- 远端数据中心、云平台的网关或 IPsecVPN 服务器必须配置有固定或经过 SNAT 转换的公网 IP 地址。
- 远端数据中心和本端云平台必须在网络上放通 UDP 500、UDP 4500、UDP 50 及 UDP 51 端口，保障 IKE 和 IPsec 的正常通信。
- 云平台需要和远端数据中心打通 VPN 的网段不可重复且不可重叠。

12.5.1 VPN 隧道配置流程

1. 在本端云平台创建 VPN 网关和对端网关；
2. 在本端云平台使用已创建的 VPN 网关和对端网关创建 VPN 隧道；
3. 配置远端数据中心、第三方云平台或公有云平台上的 VPN 网关及相关隧道配置；
4. 等待两端网关进行 SA 协商并建立 VPN 连接；
5. 在本端云平台上创建一台与 VPN 网关相同 VPC 且被指定本端网段的虚拟机，通过虚拟机 Ping 远端网络内网的一台主机，验证网络的连通性。

12.5.2 创建 VPN 隧道

用户创建 VPN 隧道用于连接 VPN 网关和对端网关，并支持配置 IKE 及 IPsec 策略。创建时需指定 VPN 隧道的基本配置、预共享密钥、IKE 策略及 IPsec 策略，通常用户仅需指定基本配置及预共享密钥，即可快速创建。

可通过 IPsecVPN 资源控制台进入 【VPN 隧道】 标签页，进行 VPN 隧道的创建操作，创建隧道向导页面的基本配如下图所示：

基本配置

隧道名称 *	vpntest
隧道备注	vpntest
VPN网关 *	2323(eip-vaGHBo4Gg) <input type="button" value="刷新"/> <input type="button" value="创建VPN网关"/>
对端网关 *	2323(0.0.0.0) <input type="button" value="刷新"/> <input type="button" value="创建对端网关"/>
归属VPC	Default
本端网段 *	已选择 1 项
对端网段 *	192.168.45.0/24
预共享密钥 *	fdlsfjd232

IKE 高级选项

IPSec 高级选项

1. 选择亲配置 VPN 隧道的基本配置及预共享密钥信息：

- **名称/备注**: VPN 隧道连接的名称和备注。
- **VPN 网关**: VPN 隧道挂载的 VPN 网关，即隧道运行在云平台端的所属 VPN 网关，也可称为本地网关。
- **对端网关**: VPN 隧道挂载的对端网关，即对端网关的互联网出口 IP 地址，如 IDC 数据中心的 VPN 网关。
- **本端网段**: VPN 网关所在 VPC 网络内需要和对端网络（如 IDC 数据中心）互通的子网，如 192.168.1.0/24。本端网段用于第二阶段协商，不可与对端网段重叠，仅可选择 VPN 网关归属 VPC 包含的子网网段。
- **对端网段**: IDC 数据中心或第三方云平台中需要与本端网段 VPN 通信的子网，如 192.168.2.0/24。对端网段用于第二阶段协商，不可与本端网段重叠，支持配置多个网段，每个网段间用逗号进行分隔，最多支持 20 个对端网段。
- **预共享密钥**: IPsecVPN 连接的秘钥，用于 VPN 连接的协商，在 VPN 连接协商过程中，**需保证本端与对端的密钥一致**。由a-z, A-Z, 数字, 特殊字符组成，但是不能包含'?'和空格，长度为128 个字符。

注意：在对端建立隧道配置时，由于从对端网关设备的角度出发，在配置网段时需将本端网段和对端网段调换进行配置。

2. 根据需求配置用于 VPN 隧道连接协商一阶段的 IKE 策略及二阶段的 IPSec 策略。**在建立连接时，需保证两端的 IKE 策略必须保持一致（本端和对端标识在对端配置相反）**。通常选择默认值即可创建隧道，只需要在对端建立隧道配置时，使用相同的配置参数即可将两条隧道通过两端网关进行连接。

IKE 高级选项 ^

IKE版本	IKE V2	IKE V1	
IKE认证算法	sha1	▼	
IKE加密算法	aes128	▼	
DH组	2	▼	
本端标识	自动识别	IP Address	全称域名
对端标识	自动识别	IP Address	全称域名
生存周期	86400	s	

IPSec 高级选项 ^

安全传输协议	ESP	AH
IPsec认证算法	sha1	▼
IPsec加密算法	aes128	▼
PFS DH组	2	▼
生存周期	86400	s

IKE 策略：

- 版本：** IKE 密钥交换协议的版本，支持 V1 和 V2。V2 版对 SA 的协商过程进行简化且更加适应多网段场景，推荐选择 V2 版本。若对端 VPN 设备仅支持 V1，则必须选择 V1 版本进行创建。
- 认证算法：** 为 IKE 协商过程中的报文提供认证，支持 md5、sha1 和 sha2-256 三种认证算法，默认认为 sha1。
- 加密算法：** 为 IKE 协商过程中的报文提供加密保护，支持 3des、aes128、aes192、aes256 四种加密算法，默认算法为 aes128。
- 协商模式：** IKE v1 的协商模式，支持主模式 (main) 和野蛮模式 (aggressive)。
 - 主模式在 IKE 协商时需经过 SA 交换、密钥交换、身份验证三个双向交换阶段（6 个消息），而野蛮模式仅需要经过 SA 生成/密钥交换和身份验证两次交换阶段（3 个消息）。
 - 由于野蛮模式密钥交换与身份验证一起进行无法提供身份保护，因此主模式的协商过程安全性更高，协商成功后信息传输安全性一致。
 - 主模式适用于两端设备的公网 IP 固定的场景，野蛮模式适用于需要 NAT 穿越及 IP 地址不固定的场景。
- DH 组：** 指定 IKE 交换密钥时使用的 Diffie-Hellman 算法，密钥交换的安全性及交换时间随 DH 组的扩大而增加，支持 1、2、5、14、24，默认值为 2，值越大所占用的计算性能越高。

- 1: 采用 768-bit 模指数 (Modular Exponential, MODP) 算法的 DH 组。
 - 2: 采用 1024-bit MODP 算法的 DH 组。
 - 5: 采用 1536-bit MODP 算法的 DH 组。
 - 14: 采用 2048-bit MODP 算法的 DH 组。
 - 24: 带 256 位的素数阶子群的 2048-bit MODP 算法 DH 组。
- **本端标识:** VPN 网关的标识, 用于 IKE 第一阶段协商, 支持 IP 地址和 FQDN (全称域名), 默认为 VPN 网关的外网 IP 地址。
 - **对端标识:** 对端网关的标识, 用于 IKE 第一阶段协商。支持 IP 地址和 FQDN (全称域名), 默认为对端网关的 IP 地址。若对端为 NAT 透传模式 (对端网关的 IP 地址为 0.0.0.0) , 需要将标识 IP 修订为真正的对端网关 IP 地址, 即在对端 VPN 网关设备中配置的本端网关 IP 地址。
 - **生存周期:** 第一阶段 SA 的生存时间, 在超过生存周期后, SA 将被重新协商, 取值范围为 3600~86400 , 默认值为 86400 秒。

注意: 在对端建立隧道配置时, 由于从对端网关设备的角度出发, 在配置标识时需将本端标识和对端标识调换进行配置。

IPSec 策略

- **安全传输协议:** IPSec 支持 AH 和 ESP 两种安全协议, AH 只支持数据的认证保护, ESP 支持认证和加密, 推荐使用 ESP 协议。
- **IPSec 认证算法:** 为第二阶段用户数据提供的认证保护功能, 支持 md5 和 sha1 两种算法, 默认为 sha1。
- **IPSec 加密算法:** 为第二阶段用户数据提供的加密保护功能, 支持 3des、aes128、aes192 和 aes256 四种加密算法, 默认为 aes128 , 使用 AH 安全协议时不可用。
- **PFS DH 组:** PFS (Perfect Forward Secrecy, 完善的前向安全性) 特性是一种安全特性, 指一个密钥被破解, 并不影响其他密钥的安全性。PFS 特性为第二阶段协商的 Diffie-Hellman 密钥交换算法, 支持的 DH 组为支持 1、2、5、14、24 与关闭 (Disable) , 默认值为 2 , Disable 适用于不支持 PFS 的客户端。
- **生存周期:** 第二阶段 SA 的生存时间, 在超过生存周期后, SA 将被重新协商, 取值范围为 3600~86400 , 默认值为 86400 秒。

3. 选择并配置以上信息后, 点击“立即创建”进行 IPSecVPN 隧道的创建, 可返回至隧道列表页面查看隧道的创建过程及 VPN 连接过程。

创建过程中, VPN 隧道的资源状态为“创建中”, 待隧道创建成功后, 资源状态流转为“运行”。创建成功后平台会根据隧道所配置的参数与对端网关进行 VPN 连接, 即进行 IPSecVPN 两个 SA 的阶段协商, VPN 隧道的连接状态为“连接中”, 待连接状态流转为“已连接”后, 证明 VPN 隧道已连接成功。若 VPN 隧道连接失败, 则会进行重试, 3 次重试依然失败, 则显示阶段 1 失败或阶段 2 失败, 系统会在连接失败后, 每隔 12 秒重新进行连接尝试。

VPN 隧道的连接状态处在已连接时, 平台会根据隧道配置的对端网段, 在关联的本端 VPC 子网中包含虚拟机里自动下发到对端网段的网络路由, 保证网络连通性。

12.5.2 查看 VPN 隧道

VPN 隧道创建成功后, 用户可通过导航栏进入【VPN 网关】控制台, 切换至 VPN 隧道标签页可查看隧道的资源列表, 并可通过列表上名称和 ID 进入详情页面查看 VPN 隧道的详细配置信息及监控信息。

12.5.2.1 VPN 隧道列表

VPN 隧道列表可查看当前账户下所有隧道的资源列表信息，包括名称、资源 ID、VPN 网关、对端网关、创建时间、资源状态、连接状态及操作项，如下图所示：

名称	资源ID	VPN网关	对端网关	创建时间	资源状态	连接状态	操作
修改名称及备注	ipvpn_tunnel-MQcK-cVMR	ipvpn-VMvrumVMR	ipvpn_remote-q1Qs_j4MR	2020-07-28	运行	阶段1失败	详情 下载配置 ...
修改名称及备注	ipvpn_tunnel-kJvrbcVGR	ipvpn-VMvrumVMR	ipvpn_remote-71hfkZVMR	2020-07-28	运行	已连接	详情 下载配置 ...
修改名称及备注	ipvpn_tunnel-8tK1JHVGR	ipvpn-VMvrumVMR	ipvpn_remote-khhR0NVMg	2020-07-26	运行	已连接	详情 下载配置 ...

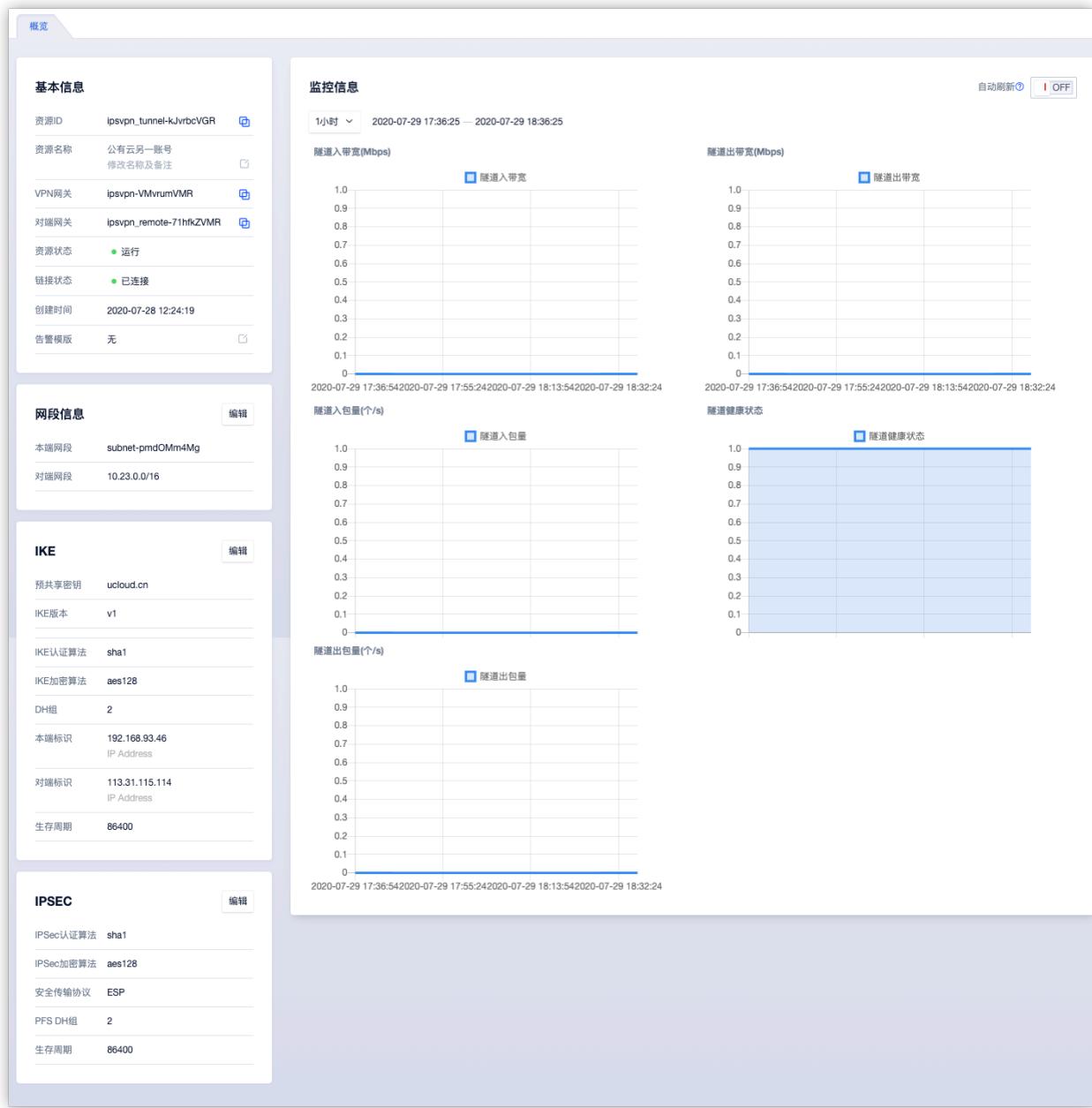
- 名称/ID：VPN 隧道的名称及全局唯一标识符。
- VPN 网关：VPN 隧道所关联的 VPN 网关名称及 IP 地址。
- 对端网关：VPN 隧道所关联的对端网关名称及 IP 地址。
- 创建时间：VPN 隧道的创建时间。
- 资源状态：VPN 隧道的资源运行状态，包括创建中、运行、删除中等。
- 连接状态：VPN 隧道的连接状态，包括连接中、已连接、阶段 1 失败及阶段 2 失败。
 - 阶段 1 失败代表 VPN 隧道在协商第一阶段 IKE SA 时失败，需要检查两端隧道的 VPN 网关 IP、对端网关 IP、对端网段、本端网段、预共享密钥及 IKE 配置参数是否一致；
 - 阶段 2 失败通常代表第 1 阶段的 IKE SA 已协商成功，但第 1 阶段的 IPSec SA 协商失败，需要检查两端隧道的第二阶段的 IPSec 配置参数是否一致。

列表上操作项是指对单个隧道的操作，包括下载隧道配置及删除操作，可通过搜索框对隧道资源列表进行搜索和筛选，支持模糊搜索。

为方便租户对资源的统计及维护，平台支持下载当前用户所拥有的所有隧道资源列表信息为 Excel 表格；同时支持对隧道进行批量删除操作。

12.5.2.2 VPN 隧道详情

在 VPN 隧道资源列表上，点击“名称”或 ID 可进入概览页面查看当前 VPN 隧道的详细配置信息和监控信息：



(1) 基本信息

VPN 隧道基本信息，包括资源 ID、名称、VPN 网关、对端网关、资源状态、连接状态、创建时间及告警模板信息，可点击告警模板右侧按钮修改负载均衡所关联的告警模板。

(2) 网段信息

VPN 隧道已配置的网段匹配信息，包括本端网段和对端网段，仅展示网段间可通过 VPN 隧道建立的连接进行通信。可通过编辑按钮对本端和对端网段进行修改，详见[修改隧道网段策略](#)。

(3) IKE 配置信息

VPN 隧道的 IKE 配置信息，包括预共享密钥、IKE 版本、协商模式、IKE 认证算法、IKE 加密算法、DH 组、本端标识、对端标识及生存周期等信息。可通过编辑按钮对 IKE 配置信息进行修改，详见[修改 IKE 策略](#)。

(4) IPsec 配置信息

VPN 隧道的 IPsec 配置信息，包括安全传输协议、IPsec 认证算法、IPsec 加密算法、PFS DH 组及生存周期等信息。可通过编辑按钮对 IPsec 配置信息进行修改，详见[修改 IPsec 策略](#)。

(5) 监控信息

负载均衡实例相关的监控图表及信息，包括隧道出/入带宽、隧道出/入包量及隧道健康状态，支持查看1小时、6小时、12小时、1天及自定义时间的监控数据。

用户也可直接通过隧道健康状态的监控图表查看隧道的连接状态，若图表数据全为1代表已连接，为0代表连接中或连接失败。

12.5.3 下载 VPN 隧道配置

支持用户下载隧道的配置信息至本地，可参照下载的配置文件进行远端数据中心或云平台的VPN隧道配置。下载的配置文件为 `.conf` 格式，包括整个 VPN 隧道 VPN 网关、对端网关、本端网段、对端网关、预共享密钥及 IKE 和 IPsec 的策略相关配置信息。

可通过隧道列表上的【下载隧道配置】按钮进行配置文件的下载，点击后会直在本地下载一个 `.conf` 的文件，在文件中会列举当前隧道的相关配置：

```
conn ipvpn_tunnel-MQCK-CVMR
    keyingtries=3
    authby=psk
    auto=start
    type=tunnel
    pfs=no

    keyexchange=ikev2

    # IPsecProtocol

    esp=aes128-sha1-modp1024!

    ike=aes128-sha1-modp1024!
    ikelifetime=86400s
    lifetime=86400s
    left=192.168.93.46
    leftid=192.168.93.46
    leftsubnet=172.16.1.0/24
    leftnexthop=%defaultroute
    right=106.75.234.78
    rightid=106.75.234.78
    rightsubnet=10.0.192.0/20
    rightnexthop=%defaultroute
    dpdaction=hold
    dpddelay=8s
    dpdtimeout=13s
```

- `keyexchange` 代表当前隧道使用的 IKE 版本为 V2。
- IKE 及 esp 分别代表 IKE 策略和 IPsec 策略的认证及加密算法。
- `left` 和 `right` 分别代表 VPN 网关和对端网关的外网 IP 地址，示例配置文件中 VPN 网关使用的是内网地址，通过 SNAT 与对端网关 106.75.234.78 进行通信。

- leftid 和 rightid 代表 IKE 配置项中的本端标识和对端标识。
- leftsubnet 和 rightsubnet 分别代表本端网段和对端网段。

如果用户需要根据此配置文件进行远端数据中心或云平台的 VPN 配置，从对端网关设备的角度出发，本端网关和本端网段指自己的网关设备和网段，对端网关和对端网段指私有平台的 VPN 网关及 VPC 子网，故在配置对端网关时需要分别将将 VPN 网关&对端网关、本端网段&对端网关、本端标识&对端标识进行对调。

12.5.4 修改隧道网段策略

用户可根据业务需求对隧道的网段策略进行修改，如增加本端网段或减少对端网段。通过隧道详情概览页面的网段信息可进行网段策略的修改，如下图所示：



支持自定义修改本端网段和对端网段，本端网段和对端网段不允许重复且不允许重叠。

- 本端网段仅允许选择 VPN 网关所属 VPC 内包含的子网网段。
- 支持输入多个对端网段，每行一个网段，必须符合网段的输入规范。
- 同一个隧道内最多支持 20 个对端网段。

确认修改后，平台会自动对隧道进行重新连接，即隧道的连接状态为连接中，待状态流转至已连接，代表配置修改成功，此时平台会自动下发对端网段为目标的路由至关联子网的虚拟机中，使虚拟机可以和对端网段进行通信。

在同一个 VPC 下，本端网段和对端网段的对应规则仅允许存在一条，即两个相同 VPC 的 VPN 网段关联的隧道不可有相同的网段策略，否则可能会影响路由下发导致网络中断。

12.5.5 修改 IKE 策略配置

当网络配置发生变更或隧道连接状态为阶段 1 失败时，可通过校验并修改 IKE 策略配置，重新进行连接。通过隧道详情概览页面的 IKE 可进行 IKE 策略的修改，如下图所示：

修改 IKE

预共享密钥 *

IKE版本

IKE V2 IKE V1

协商模式

主模式 野蛮模式

IKE认证算法

sha1

IKE加密算法

aes128

DH组

2

本端标识

自动识别 IP Address 全称域名

本端IP Adress *

192.168.93.46

对端标识

自动识别 IP Address 全称域名

对端IP Adress *

113.31.115.114

生存周期

86400 s

取消 确认

支持修改预共享密钥 及 IKE 策略的所有配置参数，两端隧道的预共享密钥、IKE 版本、协商模式（IKEv1）、认证算法、加密算法、DH 组、本端标识、对端标识必须保持一致，生存周期可以不一致。

在本端标识处通常建议使用本端网关和对端网关的 IP 地址，若对端网关使用的是 0.0.0.0 时，通常建议配置对端网关的内网 IP 地址，只要两端配置的标识是一致的就可以正常连接。

确认修改后，平台会自动对隧道进行重新连接，即隧道的连接状态为连接中，待状态流转至已连接，代表 IKE 策略修改成功。

12.5.6 修改 IPSec 策略配置

当网络配置发生变更或隧道连接状态为阶段 2 失败时，可通过校验并修改 IPSec 策略配置，重新进行连接。通过隧道详情概览页面的 IPSec 可进行 IPSec 策略的修改，如下图所示：

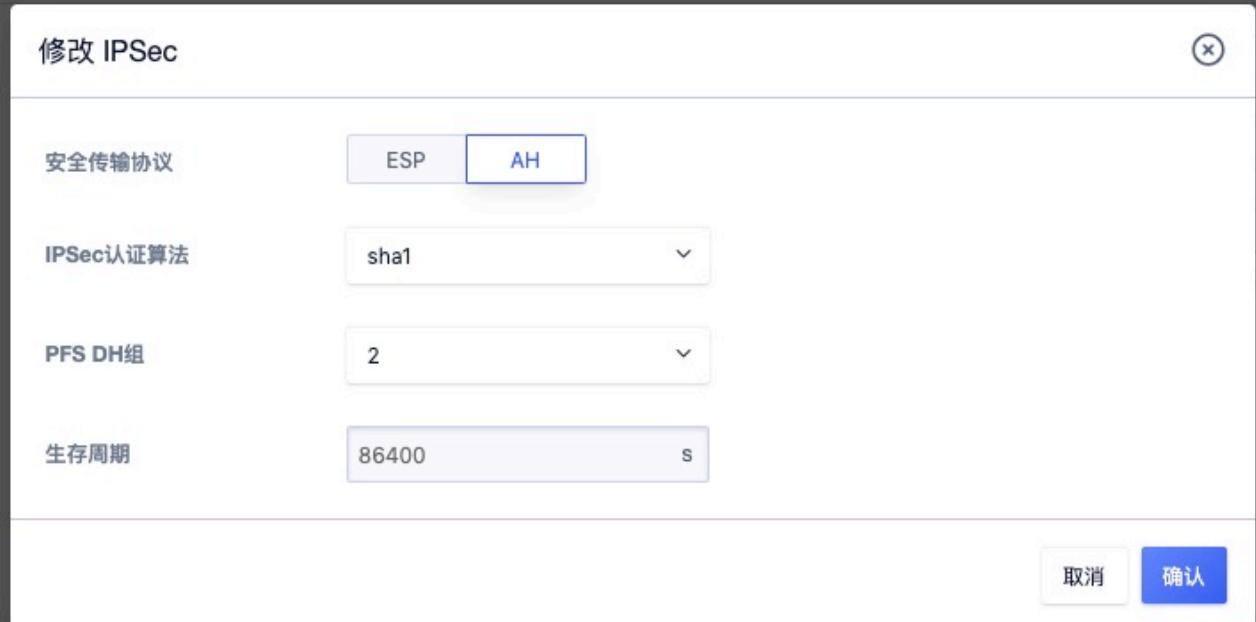
修改 IPSec

安全传输协议 ESP AH

IPSec认证算法 sha1

PFS DH组 2

生存周期 86400 s



支持修改 IPSec 策略的所有配置参数，两端隧道的安全传输协议、认证算法、加密算法及 PFS DH 组必须保持一致，生存周期可以不一致。

确认修改后，平台会自动对隧道进行重新连接，即隧道的连接状态为连接中，待状态流转至已连接，代表 IPSec 策略修改成功。

12.5.7 修改名称和备注

修改 VPN 隧道资源的名称和备注，在任何状态下均可进行操作。可通过点击 VPN 隧道资源列表页面每个 VPN 隧道名称右侧的“编辑”按钮进行修改。

12.5.8 修改告警模板

修改告警模板是对 VPN 隧道的监控数据进行告警的配置，通过告警模板定义的指标及阈值，可在 VPN 隧道相关指标故障及超过指标阈值时，触发告警，通知相关人员进行故障处理，保证 VPN 网关及业务的网络通信。

用户可通过 VPN 隧道详情概览页的操作项进行告警模板修改操作，在修改告警模板向导中选择新 VPN 隧道告警模板进行修改。

12.5.9 删 除 VPN 隧道

用户可通过控制台或 API 的方式删除不需要的 VPN 隧道，删除后 VPN 隧道会自动中断，同时会清除已配置在本端子网虚拟机中的路由。



VPN 隧道被删除后即直接销毁，请在删除前确保 VPN 隧道无业务流量访问请求，否则可能影响业务访问。

12.6 VPN 管理员指南

在私有云平台端 VPN 网关和隧道创建成功后，还需要管理员配置远端 VPN 设备或网络平台，实现远端数据中心或云平台的内网与本端私有云平台的 VPC 子网互联互通。

远端 VPN 设备或网络平台即本端 UCloudStack 私有云平台标记的对端网关，可以是物理硬件或和软件系统，如路由器、防火墙、VPN 设备或使用 `OpenSwan` 和 `StrongSwan` 搭建在 Linux 系统上的 VPN 服务器系统；同样也可以是其它云平台的 VPN 服务，如 UCloud 公有云 VPN 网关服务或阿里云的 IPsecVPN 连接等。

为演示方便，本文主要通过以下几种示例环境与 UCloudStack IPsecVPN 网关建立连接：

- UCloud 公有云 IPsecVPN
- Cisco 防火墙配置
- StrongSwan 配置
- VPC 到 VPC 的 VPN 连接

12.6.1 UCloud 公有云 IPsecVPN

通过在 UCloud 公有云和 UCloudStack 之间建立 IPsecVPN 连接，实现私有云和公有云混合构建及数据传输。

UCloud 公有云 IPsecVPN 目前仅支持 IKEv1，本文描述在私有云和 UCloud 公有云间建立基于 IKEv1 版本的 IPsecVPN 连接。

12.6.1.1 前提条件

在建立 IPsecVPN 连接进行通信前，需确认两端要建立 IPsecVPN 连接的网络拓扑关系及配置参数信息。

网络配置和配置参数	UCloudStack 私有云	UCloud 公有云
VPN 网关公网 IP 地址	106.75.234.78	113.31.115.114
VPC 网段	10.0.192.0/20	10.23.0.0/16、10.25.0.0/16
客户虚拟机 IP	10.0.192.32	10.23.228.173
预共享密钥	ucloud.1231	ucloud.1231
IKE 版本	V1——协商模式为主模式	V1——协商模式为主模式
IKE 策略	认证 SHA1、加密 AES128、DH 组 2	认证 SHA1、加密 AES128、DH 组 2
IPSec 安全传输协议	ESP	ESP
IPSec 策略	认证 SHA1、加密 AES128、PFS DH 2	认证 SHA1、加密 AES128、PFS DH 2

本文假设已在 UCloudStack 私有云上部署 VPN 网关和对端网关，并已通过以上配置参数创建 VPN 隧道，等待 UCloud 公有云配置好 VPN 隧道后，即可进行 VPN 连接。

12.6.1.2 配置公有云网关

UCloud 公有云 IPSecVPN 服务与 UCloudStack VPN 服务的配置过程相同，均需创建 VPN 网关、客户网关，并建立配置 VPN 隧道进行 VPN 连接。

确保配置前已创建 VPC 网络的子网为 10.23.0.0/16 和 10.25.0.0/16，并已在 VPC 内创建云主机 10.23.228.173。

1. 使用 113.31.115.114 外网 IP 地址创建 VPN 网关，如下图所示：



2. 使用 UCloudStack 侧 VPN 网关的公网 IP 地址创建客户网关，本示例假设 UCloudStack 环境 VPN 网关的出口 IP 为固定公网 IP 地址，如下图所示：

<input type="checkbox"/>	客户网关名称	客户网关ID	业务组	客户网关IP	隧道个数	创建时间	操作
<input type="checkbox"/>	UCloudStack侧网关 修改名称及备注	remotevpngw-05bkfbs3	未分组	106.75.234.78	1 [?]	2020-07-25	修改业务组 删除
<input type="checkbox"/>	dfdf 修改名称及备注	remotevpngw-cuiwhxfo	未分组	0.0.0.0	1 [?]	2020-07-24	修改业务组 删除
<input type="checkbox"/>	修改名称及备注	remotevpngw-0xeeks355	未分组	■ ■ ■ ■ ■	0	2020-07-24	修改业务组 删除
<input type="checkbox"/>	修改名称及备注	remotevpngw-e3csvgtj	未分组	■ ■ ■ ■ ■	0	2020-06-15	修改业务组 删除
<input type="checkbox"/>	修改名称及备注	remotevpngw-0gb51gbi	未分组	■ ■ ■ ■ ■	0	2020-06-15	修改业务组 删除

注意：如果 UCloudStack 侧 VPN 网关使用的公网 IP 地址为 SNAT 后的地址池，即 VPN 网关的出口非固定公网 IP，则需要将对端网关创建为 0.0.0.0，使 UCloud 公有云可以通过任意地址连接 UCloudStack 侧的 VPN 网关并建立 VPN 连接。

3. 使用已创建的 VPN 网关和客户网关，采用前提条件中的 IKE 和 IPSec 策略创建 VPN 隧道，如下图所示：

IKE		IKE 编辑
版本	IKE V1	
加密算法	aes128	
认证算法	sha1	
协商模式	野蛮模式	
预共享秘钥	uccloud.1231	
DH组	2	
本地ID类型	113.31.115.114 IP Address	
对端ID类型	106.75.234.78 IP Address	
SA超时(时间)	86400	

IPSec		IPSec 编辑
归属VPC	uvnet-zklyzhkl	
本地网段	10.23.0.0/16 subnet-w0fp1uxl 10.25.0.0/16 subnet-ht0dqjrp	
对端网段	10.0.192.0/20	
加密算法	aes128	
认证算法	sha1	
PFS DH组	2	
安全协议	ESP	
SA超时(时间)	3600	
SA超时(流量)	暂无	

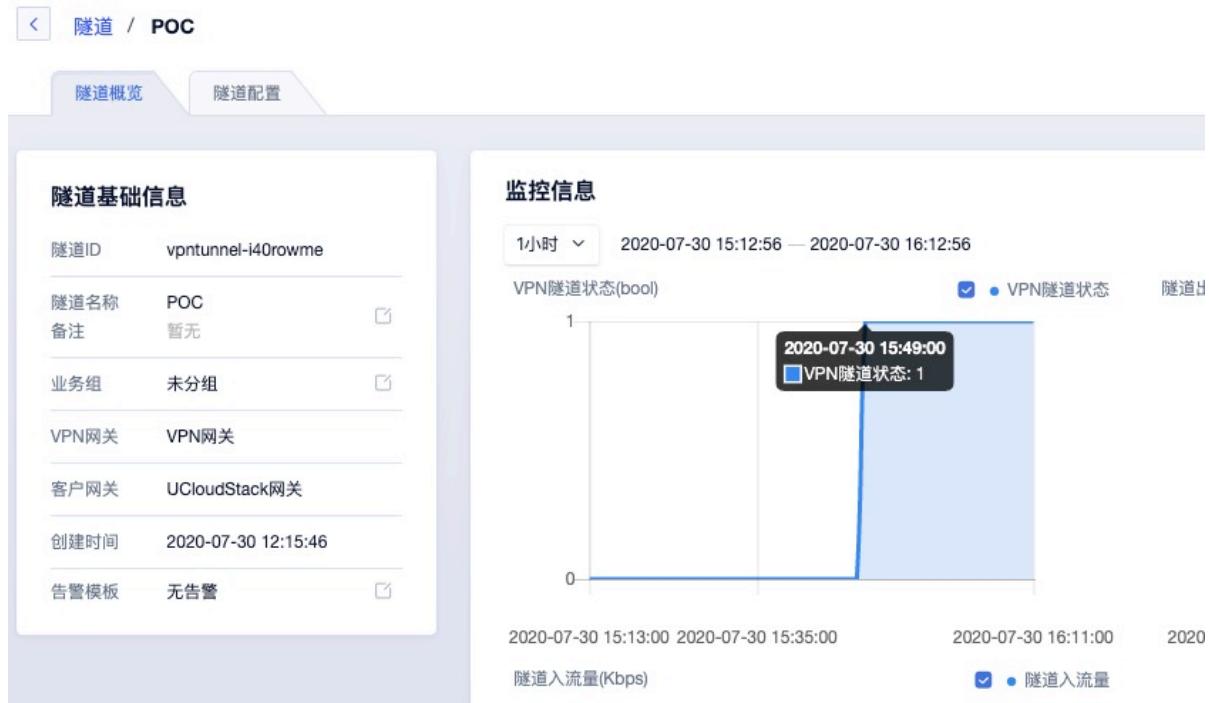
- 本地网段和对端网段与 UCloudStack 平台侧隧道正好相反，UCloudStack 平台侧隧道配置的

本端网段为 10.0.192.0/20，对端网段为 10.23.0.0/16 和 10.25.0.0/16。

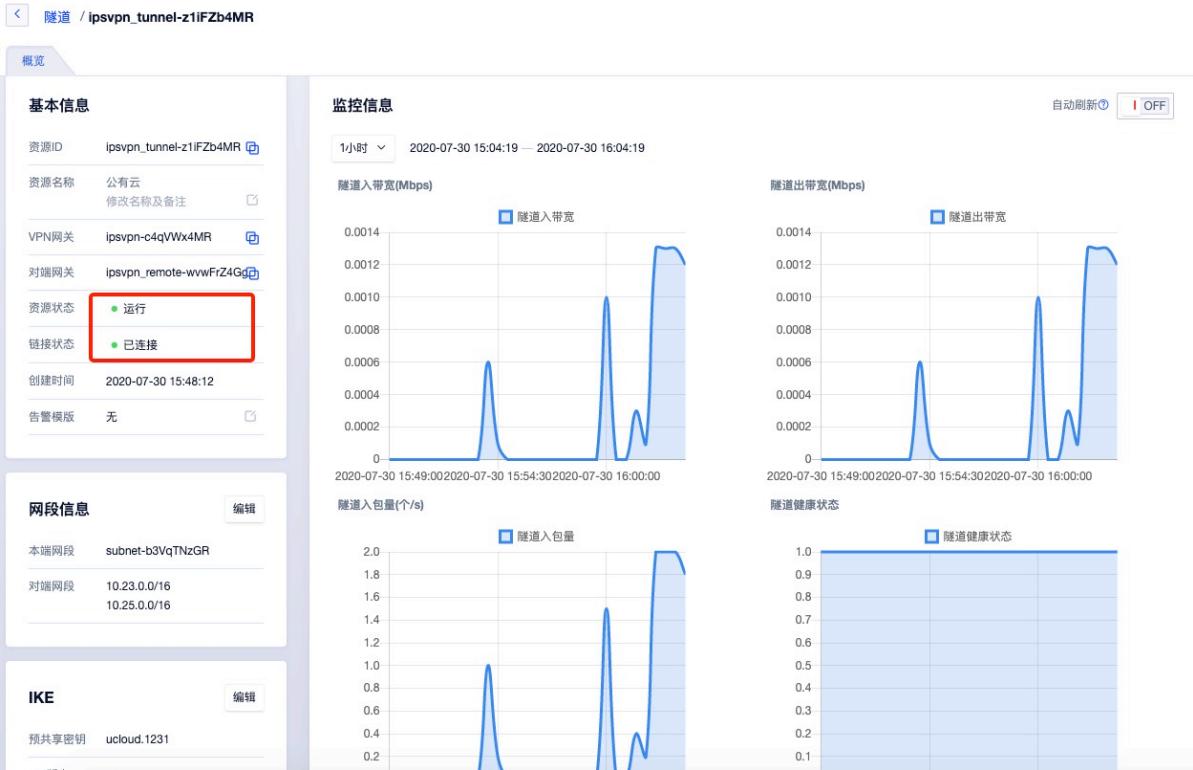
- 本端 ID 和对端 ID 即对应 UCloudStack 平台侧的本端标识和对端标识，如图所示与 UCloudStack 侧的配置正好相反，UCloudStack 侧配置的本端标识为 106.75.234.78，对端标识为 113.31.115.114。
- IKE 策略的版本、加密算法、认证算法、预共享密钥、DH 组 均与 UCloudStack 侧保持一致。
- IPSec 策略安全协议、加密算法、认证算法、PFS DH 组与 UCloudStack 侧保持一致。

4. 分别查看 UCloudStack 侧和 UCloud 公有云侧的 VPN 隧道连接状态，等待隧道自动连接。

UCloudStack 侧可通过列表上连接状态直接查看隧道是否已连接，UCloud 公有云侧需进入隧道详情页面查看"VPN 隧道状态"的监控，如下图所示：



5. 在 UCloud 公有云的隧道监控中查看 VPN 隧道状态已变为 1，代表 VPN 已连接，同时在 UCloudStack 中隧道的连接状态流转为“已连接”，如下图所示：



12.6.1.3 配置验证

在已连接状态时，UCloudStack 侧会自动下发对端网段为目标地址的路由至本端网段内的虚拟机中，可登入提前准备的本端虚拟机查看相关网络及路由配置信息。

如下图所示，本端虚拟机的 IP 地址为 10.0.192.32，下发的路由为 10.23.0.0/16 及 10.25.0.0/16，即代表虚拟机可与 UCloud 公有云侧的两个网段进行通信。

```
[root@localhost ~]# ip a |grep eth0
4: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast
    inet 10.0.192.32/20 scope global eth0
[root@localhost ~]# ip route
10.0.0.0/16 via 10.0.192.1 dev eth0
10.0.192.0/20 dev eth0 proto kernel scope link src 10.0.192.32
10.23.0.0/16 via 10.0.192.35 dev eth0
10.25.0.0/16 via 10.0.192.35 dev eth0
172.16.1.0/24 via 10.0.192.33 dev eth0
[root@localhost ~]# _
```

可通过 ping 命令检测与 UCloud 公有云虚拟机的网络连通性，如下图代表两端内网的虚拟机网络互通。

```
[root@localhost ~]# ip route
10.0.0.0/16 via 10.0.192.1 dev eth0
10.0.192.0/20 dev eth0 proto kernel scope link src 10.0.192.32
10.23.0.0/16 via 10.0.192.35 dev eth0
10.25.0.0/16 via 10.0.192.35 dev eth0
172.16.1.0/24 via 10.0.192.33 dev eth0
[root@localhost ~]#
[root@localhost ~]# ping 10.23.228.173
PING 10.23.228.173 (10.23.228.173) 56(84) bytes of data.
64 bytes from 10.23.228.173: icmp_seq=1 ttl=61 time=13.1 ms
64 bytes from 10.23.228.173: icmp_seq=2 ttl=61 time=3.35 ms
64 bytes from 10.23.228.173: icmp_seq=3 ttl=61 time=3.30 ms
64 bytes from 10.23.228.173: icmp_seq=4 ttl=61 time=3.33 ms
64 bytes from 10.23.228.173: icmp_seq=5 ttl=61 time=3.12 ms
64 bytes from 10.23.228.173: icmp_seq=6 ttl=61 time=4.21 ms
64 bytes from 10.23.228.173: icmp_seq=7 ttl=61 time=3.18 ms
64 bytes from 10.23.228.173: icmp_seq=8 ttl=61 time=3.18 ms
64 bytes from 10.23.228.173: icmp_seq=9 ttl=61 time=3.42 ms
64 bytes from 10.23.228.173: icmp_seq=10 ttl=61 time=3.47 ms
64 bytes from 10.23.228.173: icmp_seq=11 ttl=61 time=3.27 ms
64 bytes from 10.23.228.173: icmp_seq=12 ttl=61 time=3.43 ms
64 bytes from 10.23.228.173: icmp_seq=13 ttl=61 time=16.0 ms
64 bytes from 10.23.228.173: icmp_seq=14 ttl=61 time=3.39 ms
64 bytes from 10.23.228.173: icmp_seq=15 ttl=61 time=3.59 ms
```

根据以上的配置过程，即可通过 IPSecVPN 的方式将 UCloudStack 和与 UCloud 公有云内网打通。

12.6.2 Cisco 防火墙配置

通过在 IDC 数据中心的 Cisco 防火墙与 UCloudStack 之间建立 IPSecVPN 连接，实现私有云和 IDC 数据中心网络互通和数据交互。

Cisco 防火墙支持 IKEv1 和 IKEv2，本文仅介绍私有云平台和 Cisco 防火墙建立基于 IKEv2 的 IPSecVPN 连接。

12.6.2.1 前提条件

在建立 IPSecVPN 连接进行通信前，需确认两端要建立 IPSecVPN 连接的网络拓扑关系及配置参数信息。

网络配置和配置参数	UCloudStack 私有云	Cisco 防火墙
VPN 网关公网 IP 地址	106.75.234.78	1.1.1.1
VPC 网段/本地网段	10.0.192.0/24	192.168.1.0/24
客户虚拟机 IP	10.0.192.32	192.168.1.2
预共享密钥	ucloud.1231	ucloud.1231
IKE 版本	V2	V2
IKE 策略	认证 SHA1、加密 AES128、DH 组 2	认证 SHA1、加密 AES128、DH 组 2
IPSec 安全传输协议	ESP	ESP
IPSec 策略	认证 SHA1、加密 AES128、PFS DH 2	认证 SHA1、加密 AES128、PFS DH 2

本文假设已在 UCloudStack 私有云上部署 VPN 网关和对端网关，并已通过以上配置参数创建 VPN 隧道，等待数据中心的 Cisco 防火墙配置好 VPN 隧道后，即可进行 VPN 连接。

12.6.2.2 配置防火墙

1. 配置 IKE 第一阶段算法。

```
crypto ikev2 proposal test
encryption aes-cbc-128
integrity sha1
group 2
```

2. 配置 IKEv2 策略并应用至 proposal。

```
crypto ikev2 policy ipsecpro64_v2
proposal test
```

3. 配置预共享密钥。

```
crypto ikev2 keyring ipsecpro64_v2
peer vpngw
address 106.75.234.78
pre-shared-key 0 ucloud.1231
```

4. 配置身份认证。

```
crypto ikev2 profile ipsecpro64_v2
match identity remote address 106.75.234.78 255.255.255.255
identity local address 192.168.1.1
authentication remote pre-share
authentication local pre-share
keyring local ipsecpro64_v2
```

5. 配置 IPSec 安全协议。

```
crypto ipsec transform-set ipsecpro64_v2 esp-aes esp-sha-hmac
mode tunnel
```

6. 配置 ACL，定义需要 VPN 保护并透传的数据流，即本端网段和对端网段。若有两个网段，则需要分别对两个网段添加 ACL 策略，以确保 VPN 可透传网段流量。

```
access-list 200 permit ip 192.168.1.0 0.0.0.255 10.0.192.0/24 0.0.0.255
```

7. 配置 IPSec 策略并应用 IPSec 策略

```
crypto map ipsecpro64_v2 10 ipsec-isakmp
set peer 106.75.234.78
set transform-set ipsecpro64_v2
set ikev2-profile ipsecpro64_v2
match address 200

interface g0/1
crypto map ipsecpro64_v2
```

interface g0/1 代表防火墙网关公网 IP 地址的接口，即防火墙的公网接口。

8. 配置静态路由

```
ip route 10.0.192.0 255.255.255.0 106.75.234.78
```

12.6.2.3 配置验证

通过 IDC 数据中心防火墙下 192.168.1.0/24 网段的主机 Ping 云平台的虚拟机 10.0.192.32，测试连通性。

12.6.3 StrongSwan 配置

通过在任意有公网 IP 地址的 Linux 主机上安装并配置 StrongSwan 与 UCloudStack 之间建立 IPSecVPN 连接，实现私有云和安装 IPSec 软件的主机对接，使相同网段的客户主机通过 IPSec 主机与 UCloudStack 平台虚拟机进行通信。

12.6.3.1 前提条件

在建立 IPSecVPN 连接进行通信前，需确认两端要建立 IPSecVPN 连接的网络拓扑关系及配置参数信息。

网络配置和配置参数	UCloudStack 私有云	IDC 侧 StrongSwan
VPN 网关公网 IP 地址	106.75.234.78	113.31.113.78 (内网 10.23.228.173)
VPC 网段/本地网段	10.0.192.0/20	10.23.0.0/16
客户虚拟机 IP	10.0.192.32	10.23.112.177
预共享密钥	ucloud.1231	ucloud.1231
IKE 版本	V2	V2
IKE 策略	认证 SHA1、加密 AES128、DH 组 5	认证 SHA1、加密 AES128、DH 组 5
IPSec 安全传输协议	ESP	ESP
IPSec 策略	认证 SHA1、加密 AES128、 PFS DH 5	认证 SHA1、加密 AES128、PFS DH 5

本文假设已在 UCloudStack 私有云上部署 VPN 网关和对端网关，并已通过以上配置参数创建 VPN 隧道，等待数据中心的 StrongSwan 配置好 VPN 隧道后，即可进行 VPN 连接。

12.6.3.2 配置 StrongSwan

本节介绍安装配置 StrongSwan 软件，安装环境为 Centos 7.4。

1. 安装 StrongSwan

```
yum install strongswan  
strongswan version
```

2. 开启操作系统数据转发配置并进行相关网络配置

```

echo 'net.ipv4.ip_forward = 1' >> /etc/sysctl.conf
echo 'net.ipv4.conf.default.rp_filter = 0' >> /etc/sysctl.conf
echo 'net.ipv4.conf.all.accept_redirects = 0' >> /etc/sysctl.conf
echo 'net.ipv4.conf.all.send_redirects = 0' >> /etc/sysctl.conf
echo 0 > /proc/sys/net/ipv4/conf/lo/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth0/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/eth1/rp_filter
echo 0 > /proc/sys/net/ipv4/conf/all/rp_filter
sysctl -a | egrep "ipv4.*(accept|send)_redirects" | awk -F "=" '{print$1="0"}' >> /etc/sysctl.conf

sysctl -p      //执行命令，生效转发配置命令

```

3. 配置 StrongSwan 参数

```

vi /etc/strongswan/ipsec.conf          //编辑ipsec.conf文件

conn test                           //定义连接名称为 test
authby=psk
type=tunnel                         //开启隧道模式
keyexchange=ikev2                   // ike密钥交换方式为版本2
auto=start
leftid=113.31.113.78                //本端标识ID
left=10.23.228.173                  //本地IP, nat场景选择真实的主机地址
leftsubnet=10.23.0.0/16              //本地子网
rightid=106.75.234.78               //远端标识ID
right=106.75.234.78                 //远端VPN网关IP
rightsubnet=10.0.192.0/20            //远端子网
ike=aes128-sha1-modp1024           //按照对端配置定义ike阶段算法和group
esp=aes128-sha1-modp1024           //按照对端配置定义ipsec阶段算法和group
ikelifetime=86400s                  // ike阶段生命周期
lifetime=86400s                     //二阶段生命周期
dpdaction=restart
dpddelay=8s
dpdtimeout=13s

```

本文搭建 StrongSwan 的主机是通过 NAT 网关模式，即使用 NAT 网关的 IP 地址访问互联网，或真实的搭建环境中 StrongSwan 主机有真实的公网 IP 地址，则 left 的值为真实公网 IP 地址。

4. 配置 ipsec.secrets 文件，定义预共享密钥

```

vi /etc/strongswan/ipsec.secrets

113.31.113.78 106.75.234.78 : PSK ucloud.1231

```

5. 启动 StrongSwan 并加入开机启动

```
systemctl enable strongswan  
systemctl start strongswan
```

12.6.3.3 配置验证

- 通过 `strongswan statusall` 命令查询 strongswan 的连接状态，若出现类似 `ESTABLISHED 6 minutes ago` 的信息，证明已连接成功，如下所示：

```
[root@10-23-228-173 ~]# strongswan statusall  
Status of IKE charon daemon (strongSwan 5.7.2, Linux 3.10.0-  
957.27.2.el7.x86_64, x86_64):  
  uptime: 6 minutes, since Jul 30 19:13:57 2020  
  malloc: sbrk 2666496, mmap 0, used 609168, free 2057328  
  worker threads: 11 of 16 idle, 5/0/0/0 working, job queue: 0/0/0/0,  
  scheduled: 5  
  loaded plugins: charon pkcs11 tpm aesni aes des rc2 sha2 sha1 md4 md5 mgf1  
    random nonce x509 revocation constraints acert pubkey pkcs1 pkcs7 pkcs8 pkcs12  
    pgp dnskey sshkey pem openssl gcrypt fips-prf gmp curve25519 chapoly xcbc cmac  
    hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default farp stroke  
    vici updown eap-identity eap-sim eap-aka eap-aka-3gpp eap-aka-3gpp2 eap-md5  
    eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-tls eap-ttls eap-peap xauth-  
    generic xauth-eap xauth-pam xauth-noauth dhcp led duplcheck unity counters  
Listening IP addresses:  
  10.23.228.173  
Connections:  
  test: 10.23.228.173...106.75.234.78  IKEV2, dpddelay=8s  
  test: local: [113.31.113.78] uses pre-shared key authentication  
  test: remote: [106.75.234.78] uses pre-shared key authentication  
  test: child: 10.23.0.0/16 === 10.0.192.0/20 TUNNEL,  
dpdaction=restart  
Security Associations (1 up, 0 connecting):  
  test[1]: ESTABLISHED 6 minutes ago,  
  10.23.228.173[113.31.113.78]...106.75.234.78[106.75.234.78]  
    test[1]: IKEV2 SPIs: 8285787a9e1b8ae2_i* 22543e6225ea8e59_r, pre-  
    shared key reauthentication in 23 hours  
    test[1]: IKE proposal:  
    AES_CBC_128/HMAC_SHA1_96/PRF_HMAC_SHA1/MODP_1024  
      test{1}: INSTALLED, TUNNEL, reqid 1, ESP in UDP SPIs: c22520e2_i  
c30646c8_o  
      test{1}: AES_CBC_128/HMAC_SHA1_96, 35364 bytes_i (421 pkts, 1s ago),  
35364 bytes_o (421 pkts, 1s ago), rekeying in 23 hours  
      test{1}: 10.23.0.0/16 === 10.0.192.0/20
```

- 在 IDC 数据中心 StrongSwan 下 `10.23.0.0/16` 网段的主机内添加到达 UCloudStack 侧网段的路由，使两端主机可以互相通信。

```
ip route add 10.0.192.0/20 via 10.23.228.173
```

3. 通过 IDC 数据中心 StrongSwan 下 10.23.0.0/16 网段的主机 Ping 云平台的虚拟机 10.0.192.32，测试连通性。

```
[root@docs1 docs]#  
[root@docs1 docs]# ip route  
default via 10.23.0.1 dev eth0  
10.0.192.0/20 via 10.23.228.173 dev eth0  
10.23.0.0/16 dev eth0 proto kernel scope link src 10.23.112.177  
[root@docs1 docs]#  
[root@docs1 docs]# ping 10.0.192.32  
PING 10.0.192.32 (10.0.192.32) 56(84) bytes of data.  
64 bytes from 10.0.192.32: icmp_seq=1 ttl=61 time=12.0 ms  
64 bytes from 10.0.192.32: icmp_seq=2 ttl=61 time=3.77 ms  
64 bytes from 10.0.192.32: icmp_seq=3 ttl=61 time=3.28 ms  
64 bytes from 10.0.192.32: icmp_seq=4 ttl=61 time=3.22 ms  
64 bytes from 10.0.192.32: icmp_seq=5 ttl=61 time=3.37 ms  
64 bytes from 10.0.192.32: icmp_seq=6 ttl=61 time=3.30 ms  
64 bytes from 10.0.192.32: icmp_seq=7 ttl=61 time=3.59 ms  
64 bytes from 10.0.192.32: icmp_seq=8 ttl=61 time=3.02 ms  
64 bytes from 10.0.192.32: icmp_seq=9 ttl=61 time=3.50 ms
```

12.6.4 VPC 到 VPC 的 VPN 连接

通过 VPN 网关将 UCloudStack 平台建立 VPC 到 VPC 的 VPN 连接，实现两个 VPC 内虚拟机互问及数据传输入。

平台 IPSecVPN 支持 IKEv1 和 IKEv2，本文描述在两个 VPC 网络间建立基于 IKEv2 版本的 IPSecVPN 连接。

12.6.4.1 前提条件

本操作以同一个账号下的两个 VPC 网络为例，在建立 IPSecVPN 连接进行通信前，需确认两端要建立 IPSecVPN 连接的网络拓扑关系及配置参数信息。

网络配置和配置参数	UCloudStack 私有云 VPC1	UCloudStack 私有云 VPC2
VPN 网关公网 IP 地址	106.75.234.78	106.75.234.74
VPC 网段	10.0.192.0/20	192.168.0.0/16
客户虚拟机 IP	10.0.192.32	192.168.0.16
预共享密钥	ucloud.1231	ucloud.1231
IKE 版本	V2	V2
IKE 策略	认证 SHA1、加密 AES128、DH 组 2	认证 SHA1、加密 AES128、DH 组 2
IPSec 安全传输协议	ESP	ESP
IPSec 策略	认证 SHA1、加密 AES128、PFS DH 2	认证 SHA1、加密 AES128、PFS DH 2

12.6.4.2 配置 VPN 网关和隧道

本操作需要在两个 VPC 内分别创建 VPC 网关，并针对两个 VPC 的网关分别创建对应的对端网关和隧道，即需要创建 VPN 网关-VPC1、VPN 网关-VPC2、对端网关1、对端网关 2、VPN 隧道 1、VPN 隧道 2，并使 VPN 隧道 1 和 隧道 2 建立连接。

- 分别在 VPC1 和 VPC2 中创建 VPN 网关，并确认两个网关地址分别为 `106.75.234.78` 和 `106.75.234.74`，如下图所示；

名称	资源ID	所属VPC	子网	外网IP	隧道数量	创建时间	状态	操作
VPN网关-VPC2 修改名称及备注	ipsvpn-9jIKma4GR	vpc-DkYrASHWR	subnet-vkYr0INWRz	106.75.234.74	0	2020-07-31	运行	<button>详情</button> <button>删除</button>
VPN网关-VPC1 修改名称及备注	ipsvpn-c4qVWx4MR	vpc-SX33TjgMR	subnet-b3VqTNzGR	106.75.234.78	0	2020-07-30	运行	<button>详情</button> <button>删除</button>

- 分别针对两个 VPN 网关创建对应的对端网关，VPN 网关-VPC1 的对端网关 IP 为 `106.75.234.74`，VPN 网关-VPC2 的对端网关 IP 为 `106.75.234.78`，如下图所示：

VPN网关	对端网关	隧道																					
<div style="display: flex; justify-content: space-between;"><button>创建对端网关</button><button>删除</button><input type="text"/> 搜索重置刷新</div> <table border="1" style="width: 100%; border-collapse: collapse;"><thead><tr><th><input type="checkbox"/></th><th>名称</th><th>资源ID</th><th>公网IP</th><th>隧道数量</th><th>创建时间</th><th>操作</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td>对端网关2 修改名称及备注</td><td>ipsvpn_remote-t1iTZ-4Mg</td><td>106.75.234.78</td><td>0</td><td>2020-07-31</td><td><button>删除</button></td></tr><tr><td><input type="checkbox"/></td><td>对端网关1 修改名称及备注</td><td>ipsvpn_remote-s_8hW-4Gg</td><td>106.75.234.74</td><td>0</td><td>2020-07-31</td><td><button>删除</button></td></tr></tbody></table> <div style="text-align: right; margin-top: 10px;">上一页 1 下一页 10 条/页 /1</div>			<input type="checkbox"/>	名称	资源ID	公网IP	隧道数量	创建时间	操作	<input type="checkbox"/>	对端网关2 修改名称及备注	ipsvpn_remote-t1iTZ-4Mg	106.75.234.78	0	2020-07-31	<button>删除</button>	<input type="checkbox"/>	对端网关1 修改名称及备注	ipsvpn_remote-s_8hW-4Gg	106.75.234.74	0	2020-07-31	<button>删除</button>
<input type="checkbox"/>	名称	资源ID	公网IP	隧道数量	创建时间	操作																	
<input type="checkbox"/>	对端网关2 修改名称及备注	ipsvpn_remote-t1iTZ-4Mg	106.75.234.78	0	2020-07-31	<button>删除</button>																	
<input type="checkbox"/>	对端网关1 修改名称及备注	ipsvpn_remote-s_8hW-4Gg	106.75.234.74	0	2020-07-31	<button>删除</button>																	

3. 使用 VPN 网关-VPC1 和 对端网关 1 结合前提条件中的网段信息及参数配置创建 VPN 隧道 1，如
下图所示：

基本信息

资源ID ipsvpn_tunnel-9gnwZaVMg [编辑](#)

资源名称 VPN隧道1
修改名称及备注 [编辑](#)

VPN网关 ipsvpn-c4qVWx4MR [编辑](#)

对端网关 ipsvpn_remote-s_BhW-4Gg [编辑](#)

资源状态 ● 运行

链接状态 ● 已连接

创建时间 2020-07-31 01:15:08

告警模版 无 [编辑](#)

监控信息

1小时 [分钟](#) 2020-07-31 00:17:57 — 2020-07-31 01:17:57

隧道入带宽(Mbps)

隧道入带宽

隧道出带宽(Mbps)

隧道出带宽

网段信息

编辑

本端网段 subnet-b3VqTNzGR

对端网段 192.168.0.0/16

IKE

编辑

预共享密钥 ucloud.1231

IKE版本 v2

IKE认证算法 sha1

IKE加密算法 aes128

DH组 2

本端标识 Auto
自动识别

对端标识 Auto
自动识别

生存周期 86400

IPSEC

编辑

IPSec认证算法 sha1

IPSec加密算法 aes128

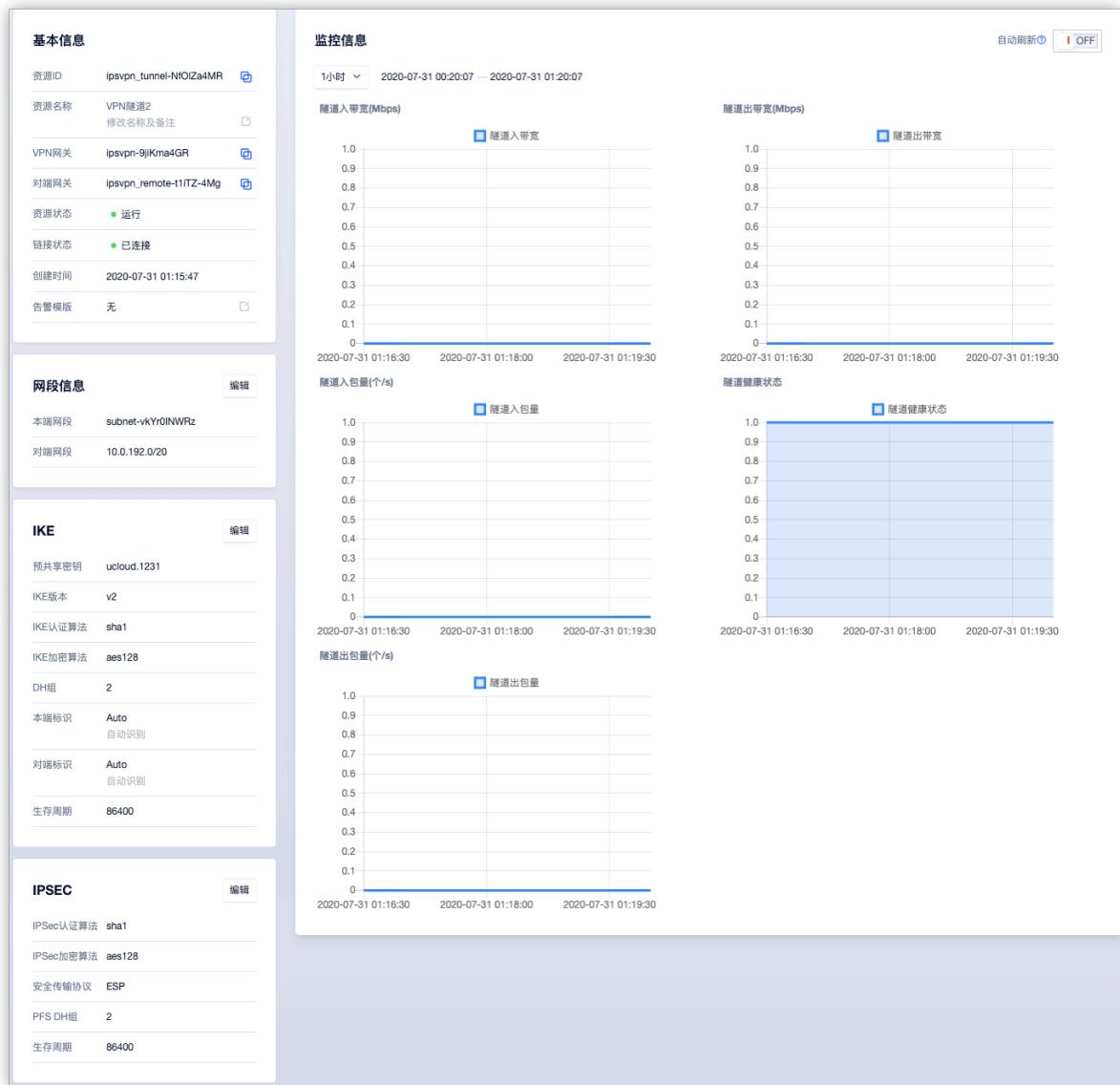
安全传输协议 ESP

PFS DH组 2

生存周期 86400

自动刷新 OFF

4. 使用 VPN 网关-VPC2 和 对端网关 2 结合前提条件中的网段信息及参数配置创建 VPN 隧道 2，需确保网段信息与 隧道1 匹配，同时保证 IKE 策略、IPSec 策略与隧道 1 保持一致才可正常建立连接，如下图所示：



如图所示，隧道 2 的对端网段为隧道的本端网段，IKE 及 IPsec 策略配置均和隧道 1 一致，均使用 IKEv2 版本，IKE 策略均为：认证 SHA1、加密 AES128、DH 组 2，IPsec 策略均为：认证 SHA1、加密 AES128、PFS DH 2。

5. 查看两个隧道的连接状态，等待隧道连接成功后，即可进行连通性验证，如下图所示两个隧道均已连接，且已向所选择了子网的虚拟机中下发路由，如下图所示：

<input type="checkbox"/>	名称	资源ID	VPN网关	对端网关	创建时间	资源状态	连接状态	操作
<input type="checkbox"/>	VPN隧道2 编辑 修改名称及备注	ipvpn_tunnel-NfOjZa4MR	ipvpn-9jiKma4GR	ipvpn_remote-t1iTZ-4Mg	2020-07-31	● 运行	● 已连接	详情 下载配置 ...
<input type="checkbox"/>	VPN隧道1 编辑 修改名称及备注	ipvpn_tunnel-9gnwZaVlg	ipvpn-c4qVWx4MR	ipvpn_remote-s_8hW-4Gg	2020-07-31	● 运行	● 已连接	详情 下载配置 ...

12.6.4.3 配置连接验证

在已连接状态时，平台会分别对两个隧道所关联的本端子网虚拟机中下发对端网段为目标地址的路由，可登入个 VPC 的客户虚拟机中查看相关网络及路由配置信息：

```

VPC1 客户虚拟机
[root@localhost ~]# ip a |grep eth0
1: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast
    link 10.0.192.32/20 brd 10.0.192.255 scope global eth0
[root@localhost ~]# ip route
10.0.0.0/16 via 10.0.192.1 dev eth0
10.0.192.0/20 dev eth0 proto kernel scope link src 10.0.192.32
192.168.0.0/16 via 10.0.192.35 dev eth0
[root@localhost ~]# ping 192.168.0.16
PING 192.168.0.16 (192.168.0.16) 56(84) bytes of data.
64 bytes from 192.168.0.16: icmp_seq=1 ttl=62 time=0.985 ms
64 bytes from 192.168.0.16: icmp_seq=2 ttl=62 time=1.34 ms
64 bytes from 192.168.0.16: icmp_seq=3 ttl=62 time=2.54 ms
64 bytes from 192.168.0.16: icmp_seq=4 ttl=62 time=0.870 ms
64 bytes from 192.168.0.16: icmp_seq=5 ttl=62 time=1.23 ms
64 bytes from 192.168.0.16: icmp_seq=6 ttl=62 time=1.25 ms
64 bytes from 192.168.0.16: icmp_seq=7 ttl=62 time=0.993 ms
64 bytes from 192.168.0.16: icmp_seq=8 ttl=62 time=1.09 ms
64 bytes from 192.168.0.16: icmp_seq=9 ttl=62 time=1.82 ms
64 bytes from 192.168.0.16: icmp_seq=10 ttl=62 time=1.29 ms
64 bytes from 192.168.0.16: icmp_seq=11 ttl=62 time=1.54 ms
64 bytes from 192.168.0.16: icmp_seq=12 ttl=62 time=0.988 ms
64 bytes from 192.168.0.16: icmp_seq=13 ttl=62 time=1.15 ms
64 bytes from 192.168.0.16: icmp_seq=14 ttl=62 time=0.966 ms
64 bytes from 192.168.0.16: icmp_seq=15 ttl=62 time=0.986 ms
64 bytes from 192.168.0.16: icmp_seq=16 ttl=62 time=1.16 ms
64 bytes from 192.168.0.16: icmp_seq=17 ttl=62 time=1.05 ms
64 bytes from 192.168.0.16: icmp_seq=18 ttl=62 time=0.869 ms
64 bytes from 192.168.0.16: icmp_seq=19 ttl=62 time=1.12 ms
64 bytes from 192.168.0.16: icmp_seq=20 ttl=62 time=1.86 ms
64 bytes from 192.168.0.16: icmp_seq=21 ttl=62 time=0.984 ms
64 bytes from 192.168.0.16: icmp_seq=22 ttl=62 time=1.17 ms
64 bytes from 192.168.0.16: icmp_seq=23 ttl=62 time=1.14 ms
64 bytes from 192.168.0.16: icmp_seq=24 ttl=62 time=1.23 ms
64 bytes from 192.168.0.16: icmp_seq=25 ttl=62 time=1.11 ms
^C
--- 192.168.0.16 ping statistics ---
25 packets transmitted, 25 received, 0% packet loss, time 24033ms
rtt min/avg/max/mdev = 0.869/1.193/2.547/0.348 ms
[root@localhost ~]# 

VPC2 客户虚拟机
[root@localhost ~]# ip a |grep eth0
4: eth0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pfifo_fast state UP qlen 1
    link 192.168.0.16/20 brd 192.168.0.255 scope global eth0
[root@localhost ~]# ip route
10.0.192.0/20 via 192.168.0.17 dev eth0
192.168.0.0/16 dev eth0 proto kernel scope link src 192.168.0.16
[root@localhost ~]#
[root@localhost ~]# ping 10.0.192.32
PING 10.0.192.32 (10.0.192.32) 56(84) bytes of data.
64 bytes from 10.0.192.32: icmp_seq=1 ttl=62 time=2.73 ms
64 bytes from 10.0.192.32: icmp_seq=2 ttl=62 time=1.03 ms
64 bytes from 10.0.192.32: icmp_seq=3 ttl=62 time=1.18 ms
64 bytes from 10.0.192.32: icmp_seq=4 ttl=62 time=0.998 ms
64 bytes from 10.0.192.32: icmp_seq=5 ttl=62 time=3.57 ms
64 bytes from 10.0.192.32: icmp_seq=6 ttl=62 time=3.52 ms
64 bytes from 10.0.192.32: icmp_seq=7 ttl=62 time=4.88 ms
64 bytes from 10.0.192.32: icmp_seq=8 ttl=62 time=3.24 ms
64 bytes from 10.0.192.32: icmp_seq=9 ttl=62 time=1.38 ms
64 bytes from 10.0.192.32: icmp_seq=10 ttl=62 time=1.85 ms
64 bytes from 10.0.192.32: icmp_seq=11 ttl=62 time=2.87 ms
64 bytes from 10.0.192.32: icmp_seq=12 ttl=62 time=2.29 ms
64 bytes from 10.0.192.32: icmp_seq=13 ttl=62 time=6.18 ms
64 bytes from 10.0.192.32: icmp_seq=14 ttl=62 time=1.35 ms
64 bytes from 10.0.192.32: icmp_seq=15 ttl=62 time=0.975 ms
64 bytes from 10.0.192.32: icmp_seq=16 ttl=62 time=2.18 ms
64 bytes from 10.0.192.32: icmp_seq=17 ttl=62 time=2.42 ms
64 bytes from 10.0.192.32: icmp_seq=18 ttl=62 time=1.29 ms
64 bytes from 10.0.192.32: icmp_seq=19 ttl=62 time=4.61 ms
64 bytes from 10.0.192.32: icmp_seq=20 ttl=62 time=1.33 ms
64 bytes from 10.0.192.32: icmp_seq=21 ttl=62 time=1.23 ms
64 bytes from 10.0.192.32: icmp_seq=22 ttl=62 time=1.52 ms
64 bytes from 10.0.192.32: icmp_seq=23 ttl=62 time=4.68 ms
64 bytes from 10.0.192.32: icmp_seq=24 ttl=62 time=7.28 ms
64 bytes from 10.0.192.32: icmp_seq=25 ttl=62 time=1.36 ms
64 bytes from 10.0.192.32: icmp_seq=26 ttl=62 time=1.11 ms
^C
--- 10.0.192.32 ping statistics ---
26 packets transmitted, 26 received, 0% packet loss, time 25039ms
rtt min/avg/max/mdev = 0.975/2.578/7.289/1.690 ms
[root@localhost ~]# 

```

- VPC1 的客户虚拟机 IP 地址为 `10.0.192.32`，下发的目标路由为 `192.168.0.0/16`
- VPC2 的客户虚拟机 IP 地址为 `192.168.0.16`，下发的目标路由为 `10.0.192.0/20`

如上图所示通过 Ping 命令检测到不同 VPC 虚拟机可相互通信，代表 VPC1 和 VPC2 在 VPN 网关中指定的子网已通过 IPSecVPN 打通网络。

12.7 常见问题

1. 是否可以通过 VPN 网关绑定的外网 IP 访问互联网或外网 IP 通向的其它外网？

不可以，通过 VPN 网关建立的 VPN 隧道，仅可透传隧道内指定的本端网段和对端网段的流量，不提供互联网访问能力。

2. 远端数据中心通过平台的 IPSecVPN 服务打通 VPC 网络的前提条件是什么？

远端数据中心或平台必须具有固定公网 IP 或通过 NAT 提供公网 IP 的网关设备，且网关设备必须支持 IKEv1 或 IKEv2 协议的 IPSecVPN，在建立 VPN 隧道时两端需要互通的网段不可重复且不可重叠。

3. 每个 VPN 网关可以建立多少个 VPN 隧道连接？

每个 VPN 网关最多可支持 20 个 VPN 隧道连接。

4. 每个 VPN 隧道支持多少个本端网段和对端网段？

每个 VPN 隧道支持配置 20 个本端网段和 20 个对端网段。

5. 可以在一个 VPC 内创建两个 VPN 网关用于构建不同流量透传的隧道吗？

可以，平台支持在一个 VPC 内创建多个 VPN 网关，但相同 VPC 网关上建立隧道的本端网段和对端网段匹配规则不可相同，否则可能导致影响路由下发及网络通信。

6. VPN 隧道连接状态为“阶段 1 失败”，应该如何处理？

阶段 1 失败，通常是因为两端 VPN 隧道在建立连接协商 IKE SA 时的配置参数不一致导致，可能原因及解决方案如下：

- (1) 预共享密钥不一致：两端设置一致的共享密钥。
- (2) IKE 版本不一致及协商模式不一致：两端设置一致的 IKE 版本，若 IKE 版本为 V1，则需保证两端配置的协商模式一致。
- (3) 本端标识和对端标识不一致：两端设置一致的本端标识和对端标识，并且保证两端的本端标识和对端标识位置对调，如左侧的本端标识和对端标识分别为 192.168.1.1 & 172.16.1.1，则右侧的本端标识和对端标识分别为 172.16.1.1 & 192.168.1.1。
- (4) 加密/认证算法/DH 组不一致：两端设置一致的加密算法、认证算法及一致的 DH 组。
- (5) 对端网关未响应：确认与对端网关的网络是否异常，若对端网关的公网 IP 为 NAT 地址，需确保对端网关的公网 IP 地址为固定 IP 地址。若对端网关公网 IP 地址为非固定 IP 地址，则建立隧道时需要使用 IP 地址为 0.0.0.0 的对端网关。

7. VPN 隧道连接状态为“阶段 2 失败”，应该如何处理？

阶段 1 失败，通常是因为两端 VPN 隧道在建立连接协商 IPSec SA 时的配置参数不一致导致，可能原因及解决方案如下：

- (1) 本端网段和对端网段不一致：两端配置一致的本端网段和对端网段，并且保证两端的本端网段和对端网段位置对调，如左侧的本端网段和对端网段分别为 192.168.1.0/24 & 172.16.0.0/16，则右侧的本端网段和对端网段分别为 172.16.0.0/16 & 192.168.1.0/24。（StrongSwan 报错 received INVALID_ID_INFORMATION error notify）
- (2) IPSec 参数的安全传输协议不一致：两端设置一致的安全传输协议，如 ESP 或 AH。
- (3) IPSec 参数的加密/认证算法及 DH 组不一致：两端设置一致的 IPSec 加密算法、认证算法及 DH 组。

8. VPN 隧道连接状态一直为“连接中”，应该如何处理？

连接中代表 VPN 隧道正在初始化并准备连接对端网关和隧道，若一直卡在连接中，可能需要检测两端网关的网络通信，并确保两端网络已放通 UDP 4500、UDP 500、UDP 50 及 UDP51 等端口。

若有一端环境存在 NAT 透传，通常需要 NAT 端主动发起请求，才可正常建立连接。

9. 两端 VPN 隧道连接状态为“已连接”，VPC 内的虚拟机无法与对端网段内的主机进行通信，如何处理？

平台侧会自动下发路由至 VPC 内的虚拟机，需检查 VPC 虚拟机路由配置，若本端虚拟机路由正常，需要检测是否为对端网关下的内网主机下发路由。

13 弹性伸缩

13.1 产品简介

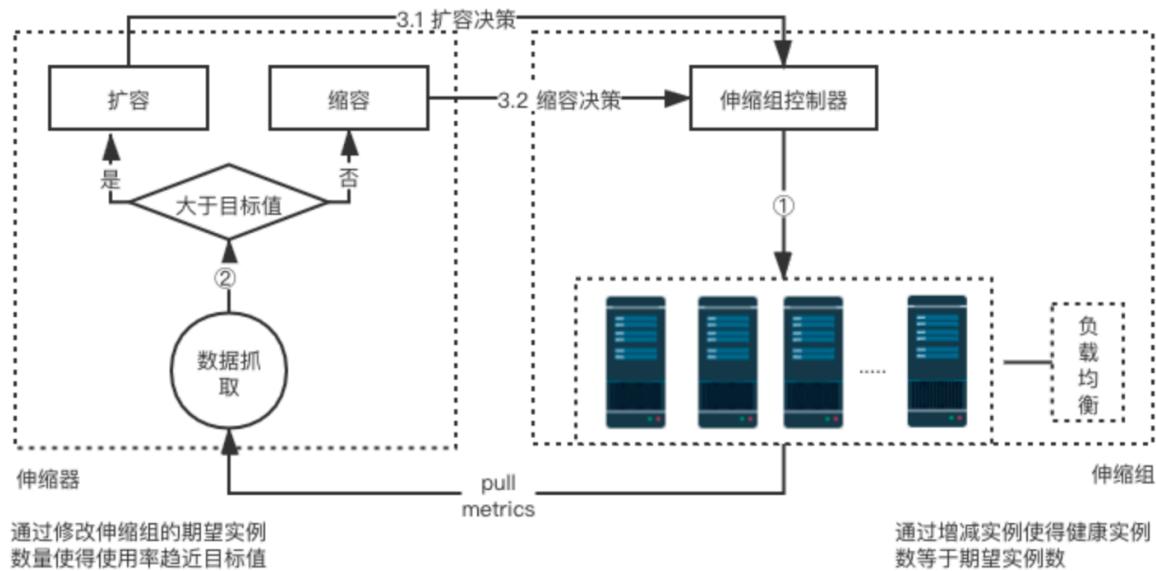
13.1.1 概述

弹性伸缩（Auto Scaling）是指在业务需求增长时自动增加计算资源（虚拟机）以保证计算能力，在业务需求下降时自动减少计算资源以节省成本；同时可结合负载均衡及健康检查机制，满足请求量波动和业务量稳定的场景。

用户可通过弹性伸缩服务，定制弹性伸缩组及伸缩策略，在伸缩组内资源量达到策略定义的阈值后，根据定制的虚拟机模板自动增减虚拟机数量，提升业务部署及运维的效率。

13.1.2 逻辑架构

弹性伸缩从逻辑架构上可分为三部分，分别为伸缩组、伸缩器及虚拟机模板。



- 伸缩组：负责将组内的实例数量维持在“期望”的水位，添加/缩减虚拟机的动作均由伸缩组进行操作，支持“自动伸缩”和“固定数量”两种模式维护伸缩组内的实例数量。
- 伸缩器：即伸缩策略，用于定义伸缩组内虚拟机伸缩的规则，可为伸缩组定义根据 CPU 使用率的阈值触发伸缩动作，支持定义伸缩组最小及最大实例数量，并可配置是否允许缩容。
- 虚拟机模板：用户根据需求自定义虚拟机模板，用于弹性伸缩时自动创建虚拟机的模板，同时支持通过虚拟机模板手动创建虚拟机。

伸缩组定义好伸缩模式后，伸缩组的实例“期望”值由伸缩策略接管并动态修改，最终由伸缩组负责虚拟机的动态扩容和缩容，新增虚拟机实例时会根据虚拟机模板创建新的虚拟机实例。

13.1.3 伸缩组工作流程

伸缩组内的虚拟机实例可定义预热时间，指为虚拟机创建成功后需要一定的时间拉起应用程序以承接业务流量。因此在伸缩组发起创建虚拟机的请求后，在虚拟机创建成功并处于运行中状态时，伸缩组中虚拟机的状态为“启动中”，代表虚拟机在预热中，待超过预热时间后，会自动转换为“运行”，代表虚拟机为健康状态。

伸缩组每 15 秒 获取一次被其控制的所有虚拟机状态，判断是否需要添加或删除实例。若伸缩组开启了负载均衡，则由负载均衡判断伸缩组内的实例是否健康，若不健康具体流程如下：

- 健康实例等于期望值
 - 伸缩组会自动将不健康（基于三个周期健康检测的判断）的实例移出伸缩组，并执行删除虚拟机操作。
- 健康实例大于期望值
 - 选择将最晚创建的健康虚拟机实例移出伸缩组，并执行删除虚拟机操作，同时将不健康的实例移出伸缩组并执行删除操作。
- 健康实例小于期望值

伸缩组会自动以虚拟机模板发起创建实例操作，并将实例数量维持在期望值，同时会将不健康的实例移出伸缩组并执行删除操作。

13.1.4 伸缩器工作流程

伸缩器会根据伸缩策略中设置的最小和最大实例值，每 15 秒采集一次伸缩组中健康实例的 CPU 监控数据，用于判断是否需要扩容或缩容伸缩组中的实例。

- 扩容

若伸缩组中健康实例的 CPU 平均使用率大于伸缩策略定义的阈值，则会触发伸缩组进行扩容实例操作。

- 缩容

通常伸缩组中健康实例的 CPU 平均使用率小于伸缩策略定义的阈值，则会触发伸缩组进行缩容实例操作。为避免频繁的缩容导致伸缩组内集群服务震荡，缩容时会获取伸缩组过去 10 分钟内所有健康实例的 CPU 监控数据平均值，用于判断是否需要缩容伸缩组中的实例。

13.1.5 功能特性

弹性伸缩通过伸缩组、伸缩策略及虚拟机模板共同维护集群内虚拟机的实例数量，同时可结合负载均衡对伸缩组内虚拟机实例的业务健康进行检测并及时剔除处于不健康状态的虚拟机实例，保证整体集群业务的可用性和可靠性。

- 支持定义虚拟机模板，用于伸缩组自动创建虚拟机的模板，同时支持通过虚拟机模板手动创建虚拟机。
- 支持伸缩组预热时间，使虚拟机创建成功后有时间拉起应用程序以承接业务流量。
- 支持自动伸缩和固定数量两种伸缩模式，适应多种自动伸缩场景。
 - 自动伸缩模式依据伸缩器的伸缩策略维护伸缩组中的实例数量；
 - 固定数量模式依据用户指定的实例数量维护伸缩组中的实例。
- 支持按照伸缩组中健康实例的平均 CPU 使用率作为自动伸缩模式中是否需要扩缩容的依据。
- 支持设置伸缩策略的最大实例数量，避免因 CPU 使用率过高，无限制扩容伸缩组内实例数量，如集群虚拟机被攻击等。
- 支持设置伸缩策略的最小实例数量，避免因 CPU 使用率过低而导致伸缩组中实例数量为 0，导致业务中断或服务停止等问题。
- 支持设置伸缩策略的缩容策略，即限制一个伸缩组内的实例只允许扩容，不允许缩容。
- 支持用户查看伸缩组的伸缩日志和已添加至伸缩组的实例信息，用于查看自动伸缩组所有执行动作及原因，方便用户对伸缩组集群业务进行维护。
- 支持用户启用或禁用一个伸缩组，伸缩组禁用后即为不可用状态，将不会在触发伸缩策略执行实例伸缩和健康检查，禁用伸缩组不影响伸缩组中已存在实例的正常运行。
- 提供伸缩组中所有实例的平均 CPU 使用率监控数据，并可通过告警模板对监控数据进行告警配置，在使用率过高而触发扩缩容时，为用户发送告警邮件。

支持弹性伸缩与负载均衡进行关联，通过将伸缩组中的实例添加至负载均衡的监听器中，为伸缩组中的虚拟机业务提供负载均衡服务，同时通过监听器的健康检查机制，判断伸缩组中所有实例的业务健康状况，自动剔除业务不健康的实例并新增健康实例到业务集群。

14 MySQL 服务

提供自服务模式的MySQL数据库，采用主备高可用架构，结合异步半同步数据复制机制，为用户提供MySQL服务集群的全生命周期管理，包括一键部署、主备自动切换、配置变更、配置文件修改、重置密码、备份恢复、监控告警及审计日志等，使用户在通过平台轻松使用MySQL。

15 Redis 服务

提供自服务模式的Redis缓存，采用主备高可用架构为用户提供Redis服务集群的全生命周期管理，包括一键部署、主备自动切换、配置变更、配置文件修改、重置密码、备份恢复、监控告警及审计日志等，使用户在通过平台轻松使用Redis服务。

16 定时器

16.1 产品简介

16.1.1 概述

定时器（Scheduler）是平台为用户提供自动化任务功能，可用于定期执行一系列任务的，如自动开关虚拟机、创建快照、创建MySQL及Redis备份等。可在指定的周期重复执行，也可仅执行一次，且每个任务支持多个资源批量操作。

16.1.2 功能特性

- 支持定时创建快照，即实现硬盘的自动快照，同时支持为多个硬盘批量创建定时快照任务。
- 支持单次和重复执行定时任务，重复执行支持每天、每周、每月的指定时间执行任务。
- 每天支持单小时或每个小时进行定时任务的执行操作。
- 每周支持星期一至星期日单小时或每个小时进行定时任务的执行操作。
- 每月支持每一天单小时或每个小时进行定时任务的执行操作。
- 平台会保存定时器执行的任务列表及执行结果记录，支持用户在定时器中查看每个任务的执行记录。

17 监控告警

监控告警是UCloudStack平台全线产品的运维监控及告警服务，提供全线资源实时监控数据及图表信息，可根据监控数据批量为资源设置告警策略，并在资源故障或监控指标超过告警阈值时，以短信、邮件及电话的方式给予通知及预警；同时监控告警服务还为用户提供历史资源告警记录，让用户实时、精准掌控业务和各云产品的健康状况，全方位保障业务的可靠性和安全性。

监控告警服务提供监控图表、告警模板、通知组及告警记录四大架构功能，整体架构功能均以监控数据为基准：

- 云平台通过智能化数据采集系统，对虚拟机、云硬盘、弹性网卡、EIP、负载均衡、NAT网关、弹性伸缩、MySQL、Redis、VPN网关等资源指定的监控指标数据进行完整挖掘；
- 将采集来的监控数据存储至数据库中，并根据指定规则对数据进行检索及统计，通过指定的时间维

度及数据粒度以图形化的方式显示监控图表；

- 基于已有的监控数据，用户可通过配置告警模板，为指定的监控指标指定告警阈值及告警设置，可通过设置告警重复频次，判定区分不同等级的告警及通知；
- 为告警模板配置通知组，指定在发生告警时通知事件的通知人及通知方式；
- 在告警期间或故障结束后，可通过告警记录查询历史告警记录信息，以判断故障的发生时间和发生频率。

17.1 监控图表

监控图表指平台将智能化采集的资源运行数据，根据指定的资源及指标等筛选规则进行检索并统计，通过指定的数据粒度及时间维度以图形化的方式显示监控图表。通过监控图表，用户可以直观的查看并了解平台上已运行虚拟资源的性能、容量及网络状态等状态，及时了解资源的健康状况及故障节点。

平台为用户构建的虚拟机、弹性 EIP、负载均衡、NAT 网关、弹性伸缩、MySQL、Redis、VPN 网关分别提供多种监控指标的实时和历史监控图表，并可根据监控指标项配置相关告警模板，用于阈值超标时给予告警及通知。

- 虚拟机监控图表：通过虚拟机详情页面的监控信息栏可查看单台虚拟机的监控信息，包括网卡出/入带宽、网卡出/入包量、磁盘读/写吞吐、磁盘读/写次数、平均负载、空间使用率、内存使用率、CPU 使用率；
- 弹性 EIP 监控图表：通过 EIP 详情页面的监控信息可查看单个 EIP 资源的监控信息，包括网卡出带宽使用率、入带宽、出带宽、入包量、出包量；
- 负载均衡监控图表：通过负载均衡详情页面的监控信息可分别查看负载均衡实例和VServer监听器的监控信息，监控图表包括LB每秒连接数、LB每秒网卡出/入流量、LB每秒网卡出包数量、VServer 连接数、HTTP 2XX、HTTP 3XX、HTTP 4XX、HTTP 5XX；
- NAT 网关监控图表：通过 NAT 网关详情页面的监控信息可查看单个 NAT 网关的监控信息，包括网卡入带宽、网卡出带宽、连接数、网卡入包量、网卡出包量。
- MySQL 服务监控图表：通过 MySQL 服务详情页面的监控信息可查看单个 MySQL 服务的监控信息，包括CPU使用率、内存使用率、磁盘使用率、TPS、网卡出/入带宽、表锁、QPS、DeletePS、InsertPS、全表扫描、SelectPS、UpdatePS、连接数、慢查询、线程活跃数、连接线程数等。
- Redis 服务监控图表：通过 Redis 服务详情页面的监控信息可查看单个 Redis 服务的监控信息，包括内存使用量、内存使用率、连接数量、QPS、RedisKeys、RedisExpiredKeys、RedisEvictedKeys、命中数量、未命中数量、命中率、网卡出/入带宽等。
- VPN 网关监控图表：通过 VPN 网关服务详情页面的监控信息可查看单个网关的监控信息，包括网关出/入带宽、网关出带宽使用率、网关出/入包量。
- VPN 隧道监控图表：通过 VPN 隧道服务详情页面的监控信息可查看单个隧道的监控信息，包括隧道出/入带宽、隧道出/入包量及隧道健康状态。

监控图表可根据时间维度展示实时监控数据，同时支持查看 1 小时、6 小时、12 小时、1 天及自定义时间的监控数据及图表信息。

17.2 告警模板

告警模板是 UCloudStack 平台监控告警服务为用户提供的一种批量设置资源告警的功能，通过预先定义模板中的告警规则及通知规则，将模板中定义的规则应用到虚拟资源；若虚拟资源的监控指标数据达到或超过告警规则中设定的阈值及条件，则根据通知规则中定义的通知方式发送告警通知到指定的通知联人。

根据不同的资源类型，可定制不同监控指标及阈值的告警规则，并可选择将监控指标应用至关联资源的单个网卡或磁盘设备，满足多种应用场景下的监控报警需求。

- 告警模板是由多条告警规则及关联资源构成的；
- 一个告警模板仅支持绑定一种类型资源，包括虚拟机、外网弹性 IP、NAT 网关、负载均衡、Redis、MySQL 及 VPN 网关等；
- 每个告警模板可包含多条告警规则，每条告警规则包含监控对象、设备名称、对比方式、告警阈值、探测周期、触发周期、收敛策略及通知组；
- 每个告警模板仅支持绑定一个通知组，每个通知组可包含多个通知人，支持短信和邮件的通知方式。

17.2.1 创建告警模板

用户可指定资源类型、模板名称及备注快速创建一个告警模板，在告警规则管理中创建配置适用于业务需求的告警规则，最后将告警模板关联至虚拟资源，完成监控告警的配置。用户可通过控制台导航栏“监控”进入监控告警配置控制台，通过“告警模板”页面的“创建”按钮进入告警模板创建向导页面，如下图所示：

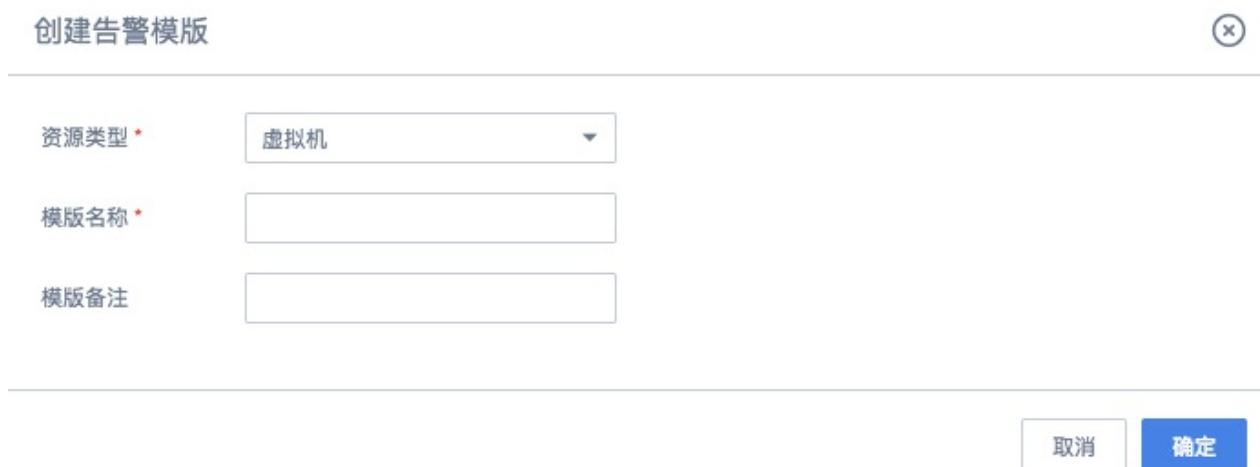
创建告警模版

资源类型 * 虚拟机

模版名称 *

模版备注

取消 确定



- 资源类型：告警模板需绑定资源的类型，包括虚拟机、外网弹性 IP、NAT 网关、负载均衡、Redis、MySQL 及 VPN 网关等，一个告警模板仅支持一种资源类型；
- 模板名称/备注：告警模板的名称标识及全局唯一标识符；

点击确定后，向导页面即返回告警模板列表，通过告警模板列表即可查看已创建的资源列表及信息。

17.2.2 查看告警模板

用户可通过导航栏进入告警模板资源控制台查看告警模板的资源列表，同时可通过点击列表上告警模板的名称进入模板详情页面，用于查看告警模板的详细信息、告警规则管理及绑定资源的管理。

17.2.2.1 告警模板列表

告警模板列表页面可查看当前账号下已拥有的模板列表，包括名称、ID、资源类型、绑定资源数量及操作项，如下图所示：

模版名	模版ID	资源类型	绑定资源数量	操作
test 修改名称及备注	template-sikpiUjmR	弹性IP	0	详情 查看资源 删除
34 修改名称及备注	template-WlY5m8jg	负载均衡	0	详情 查看资源 删除
hostvm db	template-ERPre-siR	虚拟机	0	详情 查看资源 删除

- 名称/ID：当前告警模板的名称和全局唯一标识符；
- 资源类型：当前告警模板创建时所指定的资源类型；
- 绑定资源数量：当前告警模板已关联的资源数量；
- 操作：对单个告警模板的操作项，包括详情、查看资源及删除；
- 可通过搜索框对资源列表进行搜索和筛选，支持模糊搜索。

17.2.2.2 告警模板详情

通过告警模板列表的“名称”进入模板详情页面，可查看当前告警模板的详情信息，如下图所示，详情页面分为基本信息、告警规则管理及资源绑定管理：

The screenshot shows the 'Alarming Template / hostvm' detail page. On the left, there's a sidebar with tabs for 'Rules' and 'Resources'. The main area has two sections: 'Basic Information' and 'Rules Management'.

Basic Information:

Template Name	hostvm
Template ID	template-ERPre-siR
Resource Type	Virtual Machine
Bound Resource Count	0

Rules Management:

Monitoring Object	Device Name	Comparison Method	Warning Threshold	Probe Period(s)	Trigger Period(次)	Recovery Strategy	Notification Target	Operations
磁盘写带宽	giygu	>=	3434(MBps)	30	3	Continuous alarm	notify-group-NtvuSAjmR xzd	Update Delete
CPU usage rate	无	>=	90(%)	30	3	Continuous alarm	notify-group-s9f4GM_ir user	Update Delete

- 基本信息：当前告警模板的基本信息，包括名称、ID、资源类型、已绑定的资源数量等信息，其中已绑定的资源数量若为空时，显示为“0”；
- 告警规则管理：当前告警模板的告警规则管理，包括告警规则的创建、查看、更新、删除等，具体管理操作详见：[告警规则管理](#)；
- 资源绑定管理：当前告警模板关联资源的管理，即告警模板中的规则可生效的资源，包括绑定资源、已绑定资源查看及解绑资源，具体管理操作详见：[绑定资源管理](#)。

17.2.3 查看资源

查看资源指查看当前告警模板已绑定资源的信息，点击后可进入[绑定资源管理](#)。

17.2.4 删除告警模板

仅当告警模板中未绑定任何资源时才可进行删除操作，被成功删除的告警模板将直接被销毁。用户可通过监控告警模板资源控制台中的“删除”进行模板的删除操作，如下图所示：

删除告警模版



！ 是否确定删除告警模版？告警模版下有绑定资源不可删除。

告警模版名称 * 34

告警模版ID * template-WIY5m8jig

取消

确定

删除告警模板操作被确认后，系统自动返回至告警模板列表页面，在列表页面可查看删除过程，待该资源被清空时即成功删除。

17.2.5 告警规则管理

告警规则是告警模板的核心，每个告警模板均由 1 条或多条告警规则组成。被绑定至告警模板的资源监控指标数据会根据告警规则中定义的阈值触发相关告警策略，并通过告警规则中的通知方式进行告警信息的通知，以便快速入处理告警或故障。

17.2.5.1 创建规则

用户可通过告警模板详情页面的“创建”功能进行告警规则的创建，创建告警规则时需指定监控对象、设备名称、对比方式、告警阈值、探测周期、触发周期、收敛策略及通知组等参数，如图所示：

创建告警规则

（）

监控对象 *	CPU使用率(%)
对比方式 *	>=
告警阈值 *	80
探测周期⑦ *	30
触发次数 *	3
收敛策略⑦ *	连续告警
通知组 *	Default

（ ）

- 监控对象：即监控指标，仅可选择告警模板资源类型所包含的监控指标，一条告警规则仅支持一个监控指标：

- 对比方式：指监控指标的实际数据与告警阈值的比较方式，代表当前告警规则的告警逻辑，包括 `>=` 或 `<=`：
 - 当选择 `>=` 时，即代表监控数据大于或等于阈值时触发一次告警周期；
 - 当选择 `<=` 时，即代表监控数据小于或等于阈值时触发一次告警周期；
- 告警阈值：指监控指标数据的临界值，与监控指标数据进行对比，符合对比方式即触发一次告警周期，如 CPU 使用率的告警阈值为 80，对比方式为大于等于，即 CPU 使用率大于等于 80% 即触发一次告警周期；
- 探测周期：对监控指标的数据检测的最小周期，即每隔多长时间收集一次监控数据，默认值为 30s；
- 触发周期：监控数据达到阈值条件的连续周期，即监控指标数据连续 N 次符合阈值条件即触发一次告警周期；若触发周期为 1 次，即代表触发一次告警周期就进行告警；
- 收敛策略：发生告警后发送通知给通知组的频率，可选择连续告警、指数递增、单次告警：
 - 连续告警：即每次到达触发周期即发送告警通知；
 - 指数递增：即以 2^N 时间递增告警延迟；
 - 单次告警：触发告警周期后，仅告警并通知一次，告警恢复后重新激活；
- 通知组：即触发告警周期且需要发送通知时，发送告警通知的方式及联系人。

选择并配置完成后，点击确定可返回告警模板详情页面，通过告警规则列表可查看已创建成功的告警规则。

17.2.5.2 查看规则

可通过告警模板详情页面查看当前模板包含的规则列表，列表信息包括监控对象、设备名称、对比方式、告警阈值、探测周期、触发周期、收敛策略、通知对象及操作项，如下图所示：



The screenshot shows a table with the following data:

监控对象	设备名称	对比方式	告警阈值	探测周期(s)	触发周期(次)	收敛策略	通知对象	操作
磁盘写吞吐	giygu	<code>>=</code>	3434(MBps)	30	3	连续告警	notify-group-NtvuSAjmRxzd	<button>更新</button> <button>删除</button>
CPU使用率	无	<code>>=</code>	90(%)	30	3	连续告警	notify-group-s9f4GM_JRuser	<button>更新</button> <button>删除</button>

Page navigation: 10条/页 1 / 1

其中操作项是指对单条通知规则的操作，包括更新及删除，分别指对单条告警规则的修改和删除。

17.2.5.3 更新规则

更新规则是指对单条告警规则的修改，修改项的选择与配置与创建告警规则相同，可参考 [创建规则](#)。

17.2.5.4 删除规则

删除告警规则指对单条告警规则的删除。规则被删除后即直接销毁，可重新添加该监控指标的告警规则。

17.2.6 查看绑定资源

通过告警模板详情的资源标签，进入告警模板资源绑定管理页面，可查看已绑定资源的列表及信息，包括绑定资源的 ID、类型、地址、可用区等，如下图所示：

The screenshot shows a web-based management interface for resource binding. At the top, there's a header with a back arrow, the text '告警模板 / Default', and tabs for '规则' (Rules) and '资源' (Resources). The '资源' tab is selected. Below the tabs is a search bar with placeholder text '请输入搜索内容' (Please enter search content). The main area displays a table of bound resources:

地域	可用区	资源ID	资源类型
上海	可用区A	vm-ZsslvyEZR	虚拟机
上海	可用区A	vm-jj2ApEEWR	虚拟机
上海	可用区A	vm-RRO40STZg	虚拟机

At the bottom right of the table, there are navigation buttons for '上一页' (Previous page), '下一页' (Next page), and '10条/页' (10 items per page), along with a refresh icon.

17.3 通知组管理

通知组是指监控报警发送告警通知的方式及联系人信息，通过对用户邮箱电话信息的收集，将不同资源告警通过邮件或短信的方式通知给通知人，以便划分全责，精细化处理告警通知。

- 通知组是一组通知人的组合，可以包含一个或多个联系人；
- 同一个联系人，可以加入多个通知组；
- 通知方式包括邮件通知、短信和邮件通知。

在使用监控告警模板时，需要先创建一个通知组，添加相关联系人信息，并设置通知组的通知方式，以便关联告警模板，通知组具体管理详见下文。

17.3.1 创建通知组

用户可通过控制台导航栏“监控”进入监控告警配置控制台，切换至“通知组”页面进行通知组管理页面的“创建”按钮进入通知组的创建向导页面，如下图所示指定通知组名称及通知方式进行创建操作：

The screenshot shows a modal dialog box titled '创建通知组' (Create Notification Group). It contains two input fields: '通知组名称 *' (Notification Group Name *) with the value 'test' and '通知方式 *' (Notification Method *) with the value '短信和邮件通知' (SMS and Email Notification). At the bottom right of the dialog are two buttons: '取消' (Cancel) and '确定' (Confirm).

- 通知组名称：当前需要创建的通知组名称及标识；
- 通知方式：当前需要创建的通知组通知方式，即触发告警通知时通过什么渠道通知用户，包括邮件通知和短信通知等方式；

点击确定后，进入通知组列表页面，可查看已创建的通知组信息，并对通知组进行相关操作及管理。

17.3.2 查看通知组

用户可通过监控告警控制台进入通知组页面查看通知组列表信息，同时可通过点击列表上通知组的 ID 进入详情页面，用于查看通知组的详细信息及通知人的管理。

17.3.2.1 通知组列表

通知组列表页面可查看当前账号下已拥有的通知组列表，列表信息包括 ID、名称、通知方式及对单个通知组的操作项，如下图所示：

通知组ID	名称	通知方式	操作
notify-group-C7skK0Cmg	111	短信和邮件通知	详情 更新 删除
notify-group-NtvuSAjmR	xzd	短信和邮件通知	详情 更新 删除
notify-group-s9f4GM_lR	user	邮件通知	详情 更新 删除
notify-group-7BgDdfsR	messagedb	邮件通知	详情 更新 删除

- 名称/ID：通知组的名称标识及全局唯一标识符；
- 通知方式：当前通知组的通知方式；
- 操作：对单个通知组的操作项，包括详情、更新、删除等。

17.3.2.2 通知组详情

通过通知组列表的 ID 进入通知组详情页面，可查看当前通知组的基本信息，并可通过通知人管理进行通知联系人的管理，如下图所示：

基本信息				
通知组ID	notify-group-C7skK0Cmg			
通知组名称	111			
通知方式	短信和邮件通知			
创建				
通知人ID	通知人名称	手机	邮箱	操作
contact-SeqREUjmR	帐篷	187387	lwer.zha@uc.com	更新 删除
contact-hTTeY8jiR	w	3186725	lver@asdfb.comq	更新 删除

- 基本信息：当前通知组的基本信息，包括通知组 ID、名称及通知方式；
- 通知人管理：当前通知组的通知联系人管理，包括通知人的创建、查看、更新及删除，详见[通知人管理](#)。

17.3.3 更新通知组

更新通知组是指对单个通知组的修改，修改项的选择与配置与创建通知组相同，可参考[创建通知人](#)。

17.3.4 删除通知组

删除通知组前需确认通知组未被绑定至任何一个告警规则中，若已被添加至一个告警规则，则无法删除。被成功删除的通知组即被销毁，需用户确认才可成功删除。用户可通过通知组控制台列表操作项中的“删除”进行通知组删除，如下图所示：

删除通知组



！ 是否确定删除通知组？通知组下有绑定告警规则不可删除。

通知组名称 * notify-group-C7skK0Cmg

通知组ID * 111

取消

确定

17.3.5 通知人管理

通知人是指告警规则发送通知的具体联系人，包括联系人姓名、手机、邮箱等信息。每个通知组可添加1个或多个通知人，根据通知组通知方式的不同，在资源发生告警时会发送邮件或短信至所有通知人。

17.3.5.1 添加通知人

用户可通过通知组详情页面的“创建”功能进行通知人的添加，创建通知人时需指定通知人姓名、电话、邮箱等参数，如下图所示：

创建通知人



通知人名称 *

通知人邮箱 *

通知人电话 *

取消

确定

- 通知人名称：指当前需要创建的联系人姓名或昵称；
- 通知人邮箱：指当前需要创建的联系人邮箱地址；
- 通知人电话：指当前需要创建的联系人手机号码。

点击确定后，即可成功创建一个通知联系人，可通过通知组详情的通知人列表查看联系人信息。

17.3.5.2 更新通知人信息

更新通知人信息是指对单个通知人的信息进行修改，修改项的配置与创建通知人规则相同，可参考[创建通知人](#)。

17.3.5.3 删除通知人

删除通知人指对单个通知人进行删除，通知人删除后即直接销毁，可重新添加联系人信息。

17.4 告警记录

告警记录是指当前账户所有告警记录及信息，通过告警记录可查看 1 小时、6 小时、12 小时、1 天、7 天、15 天及自定义时间周期的历史告警信息：

ID	指标名称	资源ID	资源类型	地域	可用区	告警时间	恢复时间	阈值	当前值
recover-message-EVyoU8jmR	CPU使用率	vm-Y_1NGUCiR	虚拟机	上海	上海一	解除告警	2019-03-11 17:09:37	4%	2%
recover-message-UlsoU8CiR	CPU使用率	vm-E9s8ihCiR	虚拟机	上海	上海一	解除告警	2019-03-11 17:09:37	4%	2%
alarm-message-CN8QyUCiR	CPU使用率	vm-E9s8ihCiR	虚拟机	上海	上海一	2019-03-11 16:57:39	告警	1%	3%
alarm-message-SiBwsUjmg	CPU使用率	vm-Y_1NGUCiR	虚拟机	上海	上海一	2019-03-11 16:57:38	告警	1%	2%

如上图所示，告警记录列表信息包括告警的 ID、指标名称、资源ID、资源类型、地域、可用区、告警时间、恢复时间、阈值及当前值：

- 告警 ID：指当前告警记录的全局唯一标识符；
- 指标名称：触发当前告警记录的资源监控指标项，即数据来源；
- 资源类型/资源：触发当前告警记录的资源类型及资源；
- 地域/可用区：触发当前告警记录的资源所在地域和可用区；
- 告警时间：即当前告警记录的告警触发时间：
 - 当前值达到阈值条件时，则展示具体告警时间；
 - 当前值未达到阈值条件，即告警恢复后，告警时间展示“解除告警”；
- 恢复时间：即当前告警记录资源监控指标数据恢复正常的时间：
 - 当前值达到阈值条件，即告警中时，显示为“告警”；
 - 当告警恢复后，则展示资源监控指标数据恢复正常的时间；
- 阈值：触发当前告警记录的资源告警规则中设置的阈值；
- 当前值：即触发告警或恢复告警时当前告警记录监控指标的数据值。

18 操作日志

操作日志是指用户在控制台或 API 对资源进行的操作行为及登录登出平台的审计信息。操作日志会记录用户在 UCloudStack 平台中的所有资源操作，提供操作记录查询及筛选，通过操作日志可实现安全分析、资源变更追踪以及合规性审计。操作日志根据资源类型不同在控制台可分为资源操作日志及全局操作日志：

- 资源操作日志：用户通过每种资源控制台的详情页面，查看每一个资源实例的操作日志；
- 全局操作日志：租户通过操作日志资源控制台，查看平台内属于自己的所有资源操作日志及平台登录登出审计日志等。

租户可通过操作日志控制台或 API 查看 7 天内、14 天内、1 个月内及 1 年内自定义时间的操作审计日志，操作日志包括资源的操作、用户登录审计及资源续费操作等信息。

操作日志不记录用户在虚拟机内部进行的操作。

18.1 资源操作日志

资源操作日志是指用户通过资源控制台详情的操作日志控制台查看单个资源实例的操作日志，同时也可
通过 API 查询单个资源实例的操作日志信息。资源操作日志支持查看 7 天内、14 天内、1 个月内及 1
年内自定义时间的日志信息，具体信息包括操作时间、操作（API）名称、操作者、失败（码）原因、
备注及状态：

- 操作时间：指当前资源操作日志的操作触发时间，可通过操作时间进行排序；
- 操作（API）名称：当前操作日志的操作名称或 API 名称，即指具体的操作，如创建虚拟机、绑定
弹性 IP 等；
- 操作者：指当前操作项的操作者邮箱，可由操作邮箱追溯操作联系人；
- 状态：当前操作项的操作结果状态，可为成功或失败；若为失败时，则会在失败（码）原因处显示
失败原因或失败码；
- 失败（码）原因：当前操作项操作失败后的失败原因及失败代码：
 - 若操作成功，则失败原因为空；
 - 若操作失败，则失败原因为具体的操作原因或失败码；
- 备注：当前操作项的操作备注，如自动续费时备注系统自动续费。

UCloudStack 平台资源操作日志可支持单独查看日志的资源包括虚拟机、负载均衡（包括负载均衡实
例及 VServer）、私有网络、弹性 IP 及 NAT 网关等，具体信息如下：

- 虚拟机操作日志：

操作时间	操作(API)名称	操作者	失败(码)原因	备注	状态
2019-03-11 11:24:46	AllocateVMVNCSession 申请VNC会话	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 11:16:49	AllocateVMVNCSession 申请VNC会话	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 11:16:10	CreateVMinstance 创建主机	admin@ucloud.cn	(空)	(无)	成功

- 负载均衡实例操作日志：

操作时间	操作(API)名称	操作者	失败(码)原因	备注	状态
2019-03-07 16:36:53	CreateLBInstance 创建负载均衡	admin@ucloud.cn	(空)	(无)	成功

- 负载均衡 VServer 监听器操作日志：

[负载均衡](#) / 001 / 001

概览 服务节点 操作日志

7天内 ▾ 2019-03-04 18:01:01 — 2019-03-11 18:01:01

操作时间	操作(API)名称	操作者	失败(码)原因	备注	状态
2019-03-07 16:50:10	AddRealServer 添加服务节点	admin@ucloud.cn	(空)	(无)	● 成功
2019-03-07 16:37:41	AddRealServer 添加服务节点	admin@ucloud.cn	(空)	(无)	● 成功
2019-03-07 16:37:25	CreateVServer 创建VServer	admin@ucloud.cn	(空)	(无)	● 成功

- 私有网络操作日志：

[私有网络](#) / testddd

概览 操作日志

一个月内 ▾ 2019-02-11 18:02:29 — 2019-03-11 18:02:29

操作时间	操作(API)名称	操作者	失败(码)原因	备注	状态
2019-02-25 14:48:56	CreateNIC 创建弹性网卡	admin@ucloud.cn	(空)	(无)	● 成功
2019-02-25 14:40:47	CreateNIC 创建弹性网卡	admin@ucloud.cn	(空)	(无)	● 成功

- 弹性 IP 操作日志：

[外网弹性IP](#) / cinder-nat

概览 操作日志

7天内 ▾ 2019-03-04 18:04:02 — 2019-03-11 18:04:02

操作时间	操作(API)名称	操作者	失败(码)原因	备注	状态
2019-03-07 17:08:28	BindEIP 弹性IP绑定资源	admin@ucloud.cn	(空)	(无)	● 成功
2019-03-07 17:07:42	UnBindEIP 弹性IP解绑资源	admin@ucloud.cn	(空)	(无)	● 成功
2019-03-07 10:58:10	AllocateEIP 申请弹性IP	admin@ucloud.cn	(空)	(无)	● 成功

- NAT 网关操作日志：

[NAT网关](#) / 002

概览 绑定资源 操作日志

7天内 ▾ 2019-03-04 18:06:22 — 2019-03-11 18:06:22

操作时间	操作(API)名称	操作者	失败(码)原因	备注	状态
2019-03-07 16:57:38	BindNATGWVM NAT网关绑定虚拟机	admin@ucloud.cn	8504 vm is already bind	(无)	● 失败
2019-03-07 16:57:27	BindNATGWVM NAT网关绑定虚拟机	admin@ucloud.cn	(空)	(无)	● 成功
2019-03-07 16:57:21	BindNATGWVM NAT网关绑定虚拟机	admin@ucloud.cn	(空)	(无)	● 成功
2019-03-07 16:56:07	CreateNATGW 创建NAT网关	admin@ucloud.cn	(空)	(无)	● 成功

如上资源操作日志示例图所示，资源操作日志支持搜索筛选功能，可通过搜索框对操作日志进行搜索和筛选，支持模糊搜索。

18.2 全局操作日志

全局操作日志是指租户通过操作日志控制台查看整个平台属于用户所有的资源操作日志及平台登录登出审计日志等，同时用户也可通过 API 查询租户内所有资源的操作日志及审计信息。

全局操作日志支持查看 7 天内、14 天内、1 个月内及 1 年内自定义时间的日志信息，具体信息包括操作时间、资源 ID、操作 (API) 名称、操作者、失败 (码) 原因、备注及状态，其中资源 ID 指一条操作日志信息对应的资源全局唯一标识符，如下图所示：

The screenshot shows the 'Operation Log' section of a cloud provider's management console. At the top, there are filters for 'Resource Type' (All) and 'Status' (Unlimited). Below that, a date range selector shows '7 days' from '2019-03-04 18:16:59' to '2019-03-11 18:16:59'. A search bar and a refresh button are also present. The main area displays a table of log entries with columns: Operation Time, Resource ID, Operation (API) Name, Operator, Failure (Code) Reason, Remarks, and Status. The table lists various operations such as resource renewal, disk creation, and alarm template binding, with status indicators (green for success, red for failure) and failure reasons like 'Resource expiration, system automatic续费' or 'Params Name is not valid'.

操作时间	资源ID	操作(API)名称	操作者	失败(码)原因	备注	状态
2019-03-11 18:08:01	disk-upsW_8jmg	RenewResource 资源续费	admin@ucloud.cn	(空)	资源过期, 系统自动续费	成功
2019-03-11 17:38:01	disk-upsW_8jmg	CreateDisk CreateDisk	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 17:37:54		CreateDisk CreateDisk	admin@ucloud.cn	140 Params Name is not valid	(无)	失败
2019-03-11 17:30:07	natgw-NwtyaVCig	RenewResource 资源续费	admin@ucloud.cn	(空)	资源过期, 系统自动续费	成功
2019-03-11 17:16:15	200000237	LogoutToken 登出	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 17:10:55	vm-Y_1NGUcIR	BindAlarmTemplate 绑定告警模板	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 17:10:55	template-ERPre-siR	BindAlarmTemplate 绑定告警模板	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 17:10:53	template-rule-jfz-0UCmR	UpdateAlarmTemplateRule 更新告警模板规则	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 17:09:23	vm-Y_1NGUcIR	BindAlarmTemplate 绑定告警模板	admin@ucloud.cn	(空)	(无)	成功
2019-03-11 17:09:23	template-ERPre-siR	BindAlarmTemplate 绑定告警模板	admin@ucloud.cn	(空)	(无)	成功

At the bottom, there is a pagination bar showing page 1 of 62.

全局操作日志支持根据资源类型及状态进行日志的筛选，同时支持日志的搜索检索：

- 资源类型包括所有、虚拟机、磁盘、安全组、账户、监控、服务节点、VServer、负载均衡、弹性 IP、VPC、子网、镜像、NAT 网关、Redis、MySQL 服务等，其中：
 - 所有是指不限资源类型，默认展示所有资源类型的操作审计日志信息；
 - 账户是指筛选出有关账户登录登出、修改密码等相关日志信息；
- 状态包括成功、失败及不限，其中不限是指展示所有状态的日志信息；
- 可通过搜索框对操作日志进行搜索和筛选，支持模糊搜索。

19 回收站

19.1 回收站概述

回收站是指资源删除或欠费自动释放的暂时保留区，用户删除的资源包括虚拟机、磁盘、EIP、自制镜像等资源，会在删除后自动进入回收站中。

进入回收站中的资源会默认保留一个时间，平台默认保留时间为 360000 秒，可通过云平台管理员进行自定义保留时间的设置。保留期间可对资源进行恢复、续费及销毁操作，保留时间到期后，资源会被彻底销毁，不可恢复。

19.2 查看回收站资源

云平台资源被用户手动删除及费用过期时，会自动进入回收站暂时留存。在留存期间可到回收站控制台查看已进入回收站的资源列表，如下图所示：

The screenshot shows the 'Recycle Bin' section of the Cloud Platform control panel. At the top, there are two tabs: '恢复资源' (Restore Resources) and '销毁资源' (Delete Resources). Below the tabs is a search bar and some filter options. The main area displays a table of deleted resources with the following columns: Name, Resource ID, Resource Type, Expiry Time, Delete Time, Auto-Self-Destruction,预定销毁时间 (Scheduled Deletion Time), and Operations. Two entries are listed:

名称	资源ID	资源类型	过期时间	删除时间	是否自动销毁	预定销毁时间	操作
host	vm-u4fD4K7Mg	虚拟机	2020-08-15 13:09:28	2020-07-31 11:29:41	是	2020-08-04 15:29:41	<button>恢复</button> <button>续费</button> <button>销毁</button>
WEB1	vm-3BScpwMGg	虚拟机	2020-08-08 15:26:54	2020-07-31 11:29:39	是	2020-08-04 15:29:39	<button>恢复</button> <button>续费</button> <button>销毁</button>

At the bottom right, there are navigation buttons for page 1 of 1, and a footer indicating 10 items per page.

通过回收站资源列表可查看当前账户下已被删除或释放的留存资源信息，包括资源 ID、资源名称、资源类型、过期时间、删除时间、是否自动销毁、销毁时间及操作项：

- 资源名称/ID：当前留存资源的名称及全局唯一标识符；
- 资源类型：当前留存资源的资源类型，包括虚拟机、硬盘、外网 IP、自制镜像等；
- 过期时间：指当前资源的费用过期时间，仅当资源类型为需计费的资源时有效，如虚拟机、磁盘、外网 IP；
- 删除时间：指当前留存资源被手动删除或费用过期进入回收站的时间；
- 是否自动销毁：指当前留存资源是否会在留存期间自动销毁，可通过云平台管理控制台设置保留期后是否自动销毁资源：
 - 若云平台全局配置为回收站资源自动销毁，则到达保留期后，将自动销毁资源；
 - 若云平台全局配置为回收站资源不自动销毁，则资源将永久留存在回收站，可通过手动恢复或销毁资源；
- 销毁时间：指当前留存资源将被自动销毁的时间，仅当云平台全局配置为回收站资源自动销毁时有效。

列表上操作项是指对单个资源的操作，包括恢复、续费及立即续费等操作，其中续费操作仅在资源类型为需计费的资源时有效，可通过搜索框对资源列表进行搜索和筛选，支持模糊搜索。

为方便租户对回收站资源的维护，支持对进入回收站的资源进行批量操作，包括批量恢复资源和批量销毁。

19.3 恢复资源

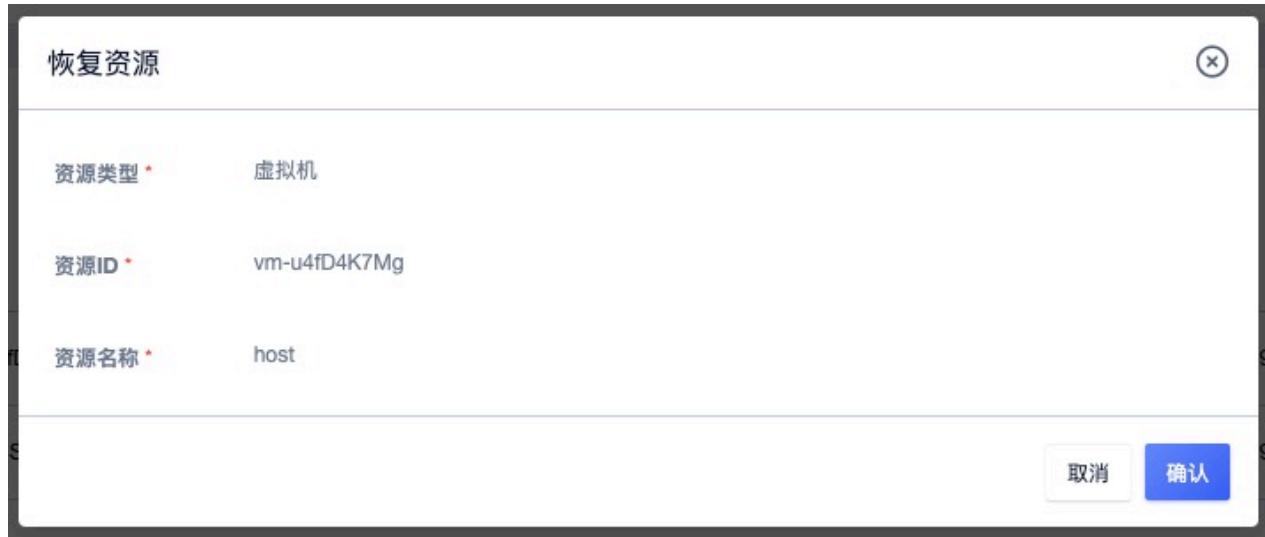
恢复资源是指手动恢复被误删而进入回收站的资源。

- 若资源被用户手动删除且无欠费的情况下，可直接通过恢复资源操作进行恢复；
- 若资源因账户欠费而自动进入回收站，则恢复资源时，需联系云平台管理员对账号进行充值后，通

过“续费”操作对资源进行续费后，在进行资源恢复；

- 若全局未开启资源自动续费且账户余额充足，资源过期后会自动进入回收站，恢复资源时，需要先通过“续费”操作对资源进行续费后，在进行资源恢复。

用户可通过回收站留存资源列表的“恢复”操作项进行资源的恢复，若资源费用已过期，需要先进行续费才可进行恢复操作。具体恢复操作如下图所示：



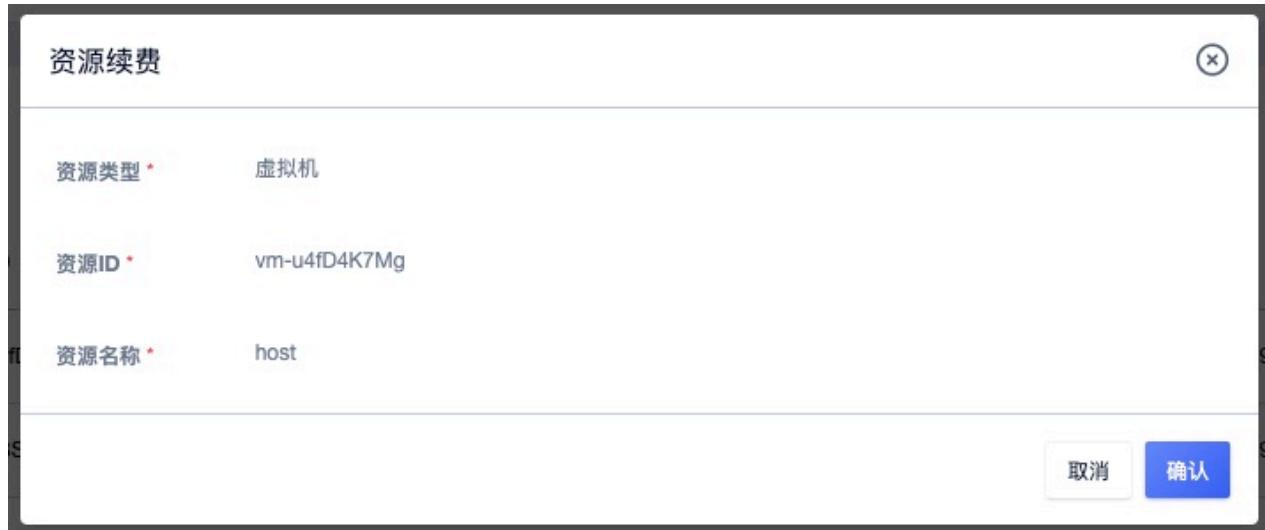
点击确定后，当前资源会自动恢复至被删除前的资源列表，可通过相关资源列表进行查看。若资源为欠费状态，则界面会提示用户，资源已欠费，需要先进行充值或续费，才可进行资源恢复。

19.4 续费资源

续费资源是指对资源的费用周期进行续费，仅支持需计费的资源进行“续费”操作。因欠费或费用到期自动进入回收站的资源被成功续费后，才可进行恢复操作。资源续费的周期根据计费方式会有所区别：

- 资源按小时计费时：一次续费操作可续费 1 小时，N 次续费操作即续费 N 小时；
- 资源按月计费时：一资续费操作可续费 1 个月，N 次续费操作即续费 N 个月；
- 资源按年计费时：一资续费操作可续费 1 年，N 次续费操作即续费 N 年的费用周期。

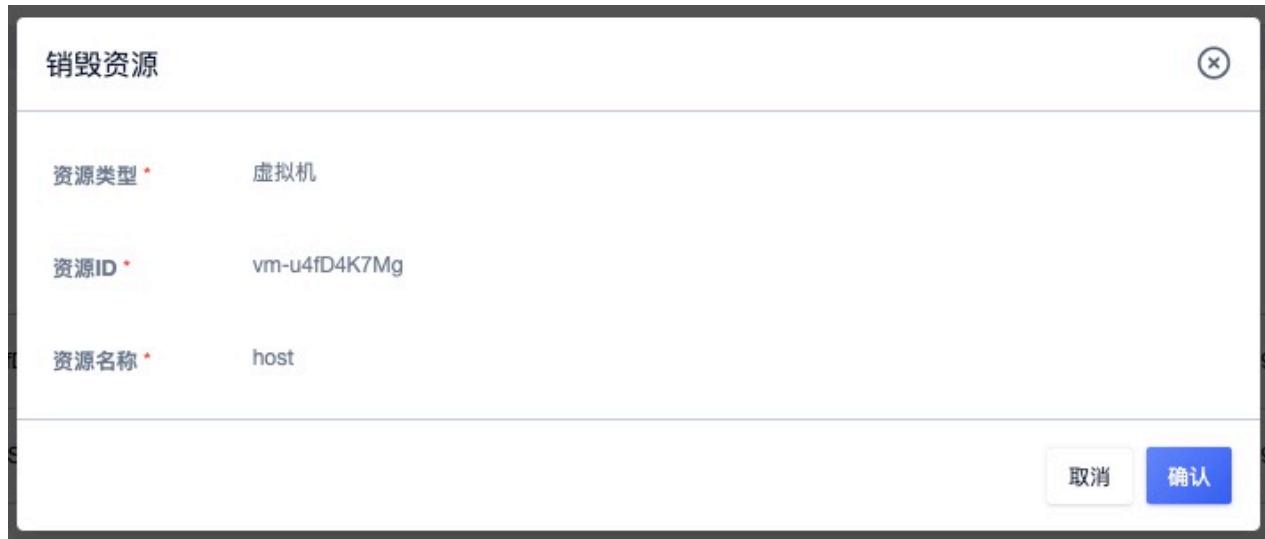
用户可通过回收站留存资源列表的“续费”操作项进行资源续费操作，若账户已欠费，需先联系管理员对账户进行充值后在进行续费操作。具体续费操作如下图所示：



点击确定后，返回至回收站留存资源列表，在列表页可查看被续费资源的过期时间被延长一个计费周期。

19.5 销毁资源

销毁资源是指手动销毁留存在回收站的资源，资源被销毁后无法恢复，需确认是否有必要销毁资源。具体操作如下图所示：



点击确定后，该资源将从留存资源列表清空，无法恢复，请慎重操作。

20 账号管理

账号管理是平台基于多租户为用户提供的用户身份管理与资源访问控制服务。通过账号管理服务，可管理账号及子账号并配置账号的安全认证，同时通过子账号管理集管理租户内的用户（子账号），控制并管理子账号对资源的访问和操作权限，适用于企业多用户协同、按需资源分配的场景，从而降低企业信息安全风险。

- 支持多租户模式，可同时创建多个租户并共享整个云平台的资源；多租户间通过认证及权限实现资源访问控制，通过 VPC 网络实现多租户间的网络隔离；
- 账号管理服务提供主账号及子账号的管理，支持查看账号的基本信息且可对账号的登录密码及登录授权进行配置及管理；
- 在主账号控制台中，可进行子账号全生命周期的管理，包括子账号的添加、查看、冻结及资源权限管理；

账号根据角色不同，分为云平台管理员、租户管理员和普通成员：

- 云平台管理员：指整个云平台的管理员，可管理整个云平台的物理管理、虚拟资源管理、平台运维及运营等相关，可登录并管理云平台管理控制台及租户控制台，是整个云平台的超级管理员，有关平台管理员的详情介绍及使用指南可参考【UCloudStack 管理员手册】；
- 租户管理员：指一个主账号，即通过平台自助注册或平台管理员创建的租户账号：
 - 通过租户管理员，可创建并使用配额内的虚拟资源，并可通过子账号管理添加属于主账号的子账号，实现企业级精细化权限控制；
 - 租户管理员支持充值，平台管理员通过管理控制台的租户管理中，可对租户进行充值及管理；

- 普通成员：子账号，即租户管理员通过用户控制台子账号管理创建的普通账号；
 - 通过主账号权限配置及管理，子账号可独立登录云平台，进行权限范围内的资源管理及操作；
 - 所有子账号共享主账号（租户管理员）的账户余额、免费余额及信用余额；
 - 所有子账号共享主账号（租户管理员）的资源配额；
 - 所有子账号间默认相互隔离，主账号可查看并管理所有子账号创建的资源。

20.1 账号信息

账号信息可以查看账号或子账号的基本信息，包括账户 ID、角色 ID、账户邮箱、现金余额、赠送余额及创建时间等信息。可通过用户控制台导航栏“账户”进入账户控制台进行查看，如下图所示：



- 账号 ID / 角色 ID：当前登录平台账号的 ID 及角色 ID。
- 账户邮箱：当前登录平台账户的邮箱地址。
- 现金余额：指通过支付宝、微信、银行及新浪支付充值的金额。
- 赠送余额：指优惠券及其它渠道赠送的余额，一般由平台管理员进行充值。
- 免费余额：指优惠券及其它渠道赠送的余额，一般由平台管理员进行充值。
- 创建时间：指当前账户的注册时间或创建时间。

20.2 账户安全

账户安全是指平台为用户账户安全提供的登录保护，可通过账户安全修改登录密码，同时可开通二次身份认证授权服务，保证登录账号的安全。

对于 API 用户，账户安全为开发者提供 API 公钥和私钥信息，可通过复制密钥信息用于操作 API 指令，可参考 API 开发者手册。

20.2.1 修改登录密码

平台支持用户修改账号登录密码，可通过账号控制台【账号安全】登录密码的“修改”进行密码修改。

The screenshot shows a modal dialog titled "修改登录密码". Inside, there is a field labeled "账户邮箱" with the value "yongfeng.lv@ucloud.cn". Below it are three input fields: "当前登录密码 *", "输入新密码 *", and "确认新密码 *", all with placeholder text "请输入密码". At the bottom right are two buttons: "取消" (Cancel) and "确认" (Confirm).

修改密码必须使用旧密码，若忘记旧密码，可联系管理员进行修改。

20.2.2 开通登录保护

平台提供免费的基于 TOTP (Time-Based One-Time Password Algorithm) 登录二次认证服务，开通本服务后，用户每次登录控制台均需通过授权认证。为了降低用户账号密码泄漏造成的风险，建议您开通账号登录二次认证。开通登录保护的前提条件如下：

- 开通对象为独立主账号或子账号；
- 移动设备上安装有 Google Authenticator 或其他基于 TOTP 技术的令牌工具；
- 推荐使用 Google Authenticator；

20.2.2.1 开通步骤

1. 登录控制台并进入账号控制台，点击账号安全“开通”按钮；
2. 检查移动设备上是否安装 Google Authenticator：
 - 页面提供IOS和Android用户工具下载地址，若您未安装 Google Authenticator 可通过扫码下载；
 - 安卓手机用户也可以通过手机品牌商提供的应用商店搜索和下载 Google Authenticator；
3. 点击下一步后，打开 Google Authenticator 工具，扫码获取授权码，也可手动输入密钥获取授权码；
4. 在页面方框内输入获取到的授权码，完成绑定，如下图所示：

开通登录保护



① 选择方案 →

② 授权 →

③ 完成

选择获取方式

扫码获取

手动获取

⑦ 如需帮助 [点击这里](#)

- ① 打开Authenticator，进入“开始设置-扫描条形码”扫码绑定后，在页面输入工具中提供的授权码



请输入授权码

上一步

20.2.2.2 关闭登录保护

1. 登录控制台并进入账号控制台，点击账号安全“关闭”按钮；
2. 按照页面提示获取并输入授权码即可关闭二次认证功能。

20.2.2.3 功能应用

二次认证服务开通后，账号密码登录平台时会要求输入验证码，系统判断验证码有效后，即可成功登录平台。

UCLOUD 专业云计算服务商

Google身份认证

请输入已绑定Authenticator提供的身份验证码

如需帮助，请联系技术支持

20.2.2.4 登录保护 FAQ

Q: Google Authoriticator 怎么下载?

A: 账号绑定页面提供 ISO 和 Android 工具下载链接，可选择通过移动设备扫码下载。若使用的是基于 Android 系统的移动设备，可通过移动设备本身提供的应用下载市场搜索和下载 Google 身份认证器。

Q: Google Authoriticator 无法扫描获取授权码怎么办?

A: 可切换至手动获取，手动输入账号密钥绑定并获取授权码。

Q: 是否可以用其他工具绑定账号?

A: 若使用的是 Google 身份认证方式，可以用基于 TOTP 算法的其他动态令牌工具绑定账号，如 FortiToken、微信小程序“二次验证码”等。为安全起见，推荐使用谷歌官方“Google Authoriticator”。

Q: 同一个账号是否支持绑定多个终端工具?

A: 支持。您只需要使用多个终端绑定同一账号（扫码或输入密钥）即可。建议您在绑定工具时妥善保存系统提供的密钥，方便后续添加绑定新的终端

20.2.3 API 密钥

通过账户安全租户可查看属于当前账号的 API 密钥，用于管理并使用 API 接口，如处图所示：



可通过点击复制按钮进行公私密钥的信息复制，以方便 API 指令的调用。

20.3 子账号管理

子账号管理是指通过租户管理员进行子账号的生命周期及权限管理，包括添加账户、查看账户、冻结账户及资源权限管理等。子账号对应某一个操作实体，如操作人员或应用程序，可通过创建新的子账号并授权相关资源访问管理权限启用一个子账号。

子账号登录云平台时，不可进行子账号管理

20.3.1 添加账户

用户通过账户资源控制台的“添加账户”，指定子账号的邮箱、密码及确认密码，即可快带为主账号创建一个子账号，如下图所示：

The screenshot shows a modal dialog titled '添加子账号'. It contains three input fields: '账户邮箱 *' with placeholder '请填写有效的邮箱', '账户密码 *' with placeholder '请输入密码', and '确认密码 *' with placeholder '请输入密码'. At the bottom right are two buttons: '取消' (Cancel) and a blue '确认' (Confirm) button.

- 邮箱：新建子账号的电子邮件地址，必须实际有效的邮箱地址；
- 密码/确认密码：新建子账号的登录密码，密码须包含有大小写字母、数字、符号中的两种，密码长度为 6-20 个字符。

点击确定后，即返回子账号列表页面，可查看当前主账号已拥有的子账号信息。

20.3.2 查看账户

用户通过账户控制台可查看子账号列表信息，同时可通过点击子账号 ID 或 邮箱地址进入子账号详情页面，用于查看子账号的基本信息及资源权限管理。

20.3.2.1 子账号列表

子账号列表页面可查看当前主账号下已拥有的所有子账号列表（包含主账号本身），列表信息包括 ID、邮箱、角色、状态、创建时间及操作项，如下图所示：

The screenshot shows a table of sub-account details. The columns are: 角色ID, 角色, 账户ID, 邮箱, 状态, 创建时间, and 操作 (Operations). The table contains three rows of data:

角色ID	角色	账户ID	邮箱	状态	创建时间	操作
200000257	子账号	200000246	cinder.lv1@ucloud.cn	使用中	2020-06-28	<button>详情</button> <button>冻结</button>
200000256	子账号	200000246	cinder.lv@ucloud.cn	使用中	2020-06-28	<button>详情</button> <button>冻结</button>
200000252	主账号	200000246	yongfeng.lv@ucloud.cn	使用中	2020-06-22	<button>详情</button>

At the bottom right, there are navigation icons (back, forward, search), a page size selector ('10 条/页'), and a total count indicator ('/1').

- ID：当前账号在云平台全局的唯一标识符；
- 邮箱：当前账号的登录邮箱地址；
- 角色：当前账号的角色，包括管理员和普通成员，主账号为租户管理员，子账号为普通成员；

- 状态：当前账号的状态，包括使用中、冻结中：
 - 使用中的用户可登录控制台，并可使用并管理资源；
 - 冻结中的用户无法登录控制台，并禁使使用并管理资源；
- 创建时间：当前账号的创建时间；
- 操作项：对单个账号的操作项，包括冻结和解冻。

20.3.2.2 子账号详情

通过子账号列表的“ID”或邮箱地址可进入账号的详情页面，可查看当前账号的详细信息，如下图所示，详情页面分为基本信息及资源权限管理：

The screenshot shows the 'Overview' tab selected in the Cloud Account Detail interface. On the left, there's a sidebar with 'Basic Information' and 'Account Security' sections. The 'Basic Information' section contains fields for Role ID (200000257), Role (Sub-account), Account ID (200000246), Account Email (cinder.lv1@ucloud.cn), Phone Number, Cash Balance (0.0000 CNY), Gift Balance (0.0000 CNY), Credit Balance (0.0000 CNY), and Creation Time (2020-06-28 10:31:12). The 'Account Security' section lists Public Key and Private Key. On the right, under 'Permission Management', there's a tree view with collapsed categories: MySQL, NAT Gateway, Redis, Recycle Station, External IP, Security Groups, Operation Log, Monitoring, Virtual Internal Network, Virtual Machine, Billing, Load Balancing, Accounts, and Images.

- 基本信息：当前子账号的基本信息，包括 ID、角色、账户邮箱及创建时间；
- 资源权限管理：当前子账号的资源访问及管理的权限控制，可控制的资源包括 NAT 网关、MySQL、Redis、回收站、安全组、外网 IP、操作日志、监控、VPC、虚拟机、计费、负载均衡、账户及镜像等，具体权限管理详见：[权限管理](#)。

20.3.3 冻结账户

冻结账户是指将一个子账号进行锁定，被成功冻结的用户，将不允许登录控制台，且禁止控制并管理相关资源。仅支持状态为“使用中”的账号进行冻结操作，用户可点击子账号列表操作项中的“冻结”进入冻结账户向导页面：



如上图所示，冻结账户需要主账户进行确认。成功锁定子账号后，账号的状态变更为冻结中，在冻结中状态的子账号支持解冻操作。

不支持对主账号进行冻结和解冻操作，需平台管理员在管理员控制台进行全租户的冻结和解冻操作。

20.3.4 解冻账户

解冻账户是指解冻一个已冻结的账号，被成功解冻的用户，可登录管理控制台且可进行相关资源使用和管理。仅支持状态为“冻结中”的账号进行解冻操作，用户可点击子账号列表操作项中的“解冻”进入解冻账户向导页面：



如上图所示，解冻一个已锁定的账号需要主账户进行确认。成功解锁的子账号状态将变更为“使用中”，在使用中状态的子账号支持冻结操作。

20.3.5 权限管理

子账号权限管理是指租户管理员对每个子账号对云平台资源的控制及管理配置，通过权限管理可以为子账号开启或关闭云平台资源及生命周期管理的功能，实现企业精细化权限管控及资源合理分配的场景。

子账号权限管理可管控的资源包括 NAT 网关、MySQL、Redis、回收站、安全组、外网 IP、操作日志、监控、VPC、虚拟机、计费、负载均衡、账户及镜像等等，对于不同的虚拟资源，分别提供不同的权限管控项，如下图所示：

权限管理

- ✓ MySQL
- ✓ NAT网关

创建NAT网关	ON	删除NAT网关	ON	获取NAT网关	ON
获取NAT网关价格	ON	添加NAT网关规则	ON	删除NAT网关规则	ON
获取NAT网关规则	ON	获取NAT网关配置	ON		
- ✓ Redis
- ✓ 回收站
- ✓ 外网IP
- ✓ 安全组
- ✓ 操作日志
- ✓ 监控
- ✓ 虚拟内网
- ✓ 虚拟机
- ✓ 计费
- ✓ 负载均衡

如权限管理示意图所示，根据不同的资源可为子账号开启或关闭不同的管理权限。为子账号开启一个资源的功能开关，子账号登录控制台后，即可使用当前功能；若为子账号关闭一个资源的功能开关，子账号登录控制台后，即显示该功能“权限不足”，如下图所示：

The screenshot shows a user interface for managing virtual machines. At the top, there are tabs for 'Virtual Machine Management', 'Virtual Machine Template', and 'Network Card Management'. Below the tabs, there are buttons for 'Create Virtual Machine', 'Start', 'Stop', and 'Delete'. On the right side, there are icons for 'Customize Headers', 'Search', and other navigation functions. The main area displays a table with columns: 'Name', 'Model', 'Configuration', 'IP', 'Status', and 'Operations'. A red warning box is overlaid on the table, containing a red exclamation mark icon and the text '权限不足' (Insufficient Permissions). At the bottom right, there are page navigation buttons and a '10 items/page' dropdown.

权限管理的配置即时生效，在变更子账号资源权限时需谨慎操作。

20.4 查看配额

配额（quota）是一个租户（包含子账号）针对每种虚拟资源在一个地域下可创建的数量限制。通过限制每个账户拥有的资源配额，可有效共享并合理分配云平台物理资源，提升资源利用率的同时，满足云平台上每一个账户的资源需求。

云平台全局提供每种资源在每个数据中心的默认配额，即每个租户创建时默认提供的资源配置模板，可通过云平台管理员分别自定义每个租户的资源配置。租户管理员及所拥有的子账号不可自定义修改资源配置数量，仅提供查看配额。

子账号和租户管理员（主账号）共享资源配置，即每种资源配置为主账号和所包含的所有子账号可创建的资源数量之和。如租户对于云硬盘的配额为 10，则租户及所有子账号可创建的云硬盘数量上限不可超过 10 个。

租户和子账号可通过账号管理控制台“配额”配额控制台查看当前账号拥有的资源配置列表，并根据地域分别展示配额信息，如下图所示：

产品类型	地域	配额	更新时间
VPN隧道	全部	10	2020-07-20 17:54:48
对端网关	全部	10	2020-06-08 15:56:19
VPN网关	全部	100	2020-06-30 16:50:54
MySQL	全部	10	2020-06-12 19:12:54
Redis	地域01	10	2020-06-12 19:12:54
Redis	全部	10	2020-06-12 19:12:54
NAT网关	全部	10	2020-06-12 19:12:54
安全组	全部	10	2020-06-12 19:12:54
负载均衡	全部	10	2020-06-12 19:12:54
外网弹性IP	全部	100	2020-06-28 11:10:01
网卡	全部	10	2020-06-12 19:12:54
硬盘	全部	10	2020-06-12 19:12:54
VPC	全部	10	2020-06-12 19:12:54
镜像	全部	10	2020-06-12 19:12:54

- 产品类型：当前配额信息的资源类型，平台支持的资源配置包括虚拟机、镜像、VPC、硬盘、弹性网卡、外网 IP、负载均衡、安全组、NAT 网关、Redis、MySQL、VPN 网关、VPN 隧道。
- 地域：当前配额信息的地域信息，代表一个地域可创建的资源配置，支持某个地域或全部地域；
- 数量：当前配额项在一个地域或全部地域可创建的资源数量；
- 更新时间：当前配额项的修改更新时间。

子账号与主账号的配额信息及数量一致，若主账号和子账号创建的资源数量超过配额，则平台自动禁止主账号和子账号创建当前资源。

21 计费管理

计费管理为用户资源分配和使用提供计量计费服务，需计费的资源均支持按时、按年、按月三种计费方式，支持资源的计费、扣费、续费、过期回收及退费等订单管理操作，同时基于账户提供充值、扣费、退费等交易管理。子账号共享主账号的账户余额，通过子账号创建的资源可直接通过共享余额进行扣费，并可通过主账号或子账号查看账户的交易流水及订单明细。

平台资源计费均为预付费模式，即无论按时、按年、按月付费，在资源创建时都需保证账户余额可满足一个计费周期的扣费，下一个计费周期开始前即进行扣费。

- 按时计费：一小时为一个计费周期，资源按照每小时的单价进行预扣费；
- 按月计费：一个月（非自然月）为一个计费周期，资源按照每个月的单价进行预扣费；
- 按年计费：一年（顺延年）为一个计费周期，资源按照每年的单进行预扣费；

按年按月购买的资源支持随时升降级配置并在升级配置后自动补齐差价。

账户余额不足下一个计费周期时，资源即会自动进入回收站，需要对资源账号及资源进行续费操作后，才可恢复使用；对于 NAT 网关和负载均衡资源，账户余额不足下一个计费周期时，资源会自动进行删除。

云平台管理员在全局开启“资源自动续费”且账户余额充足时，则资源在下一个计费周期会进行自动续费操作；若云平台管理员在全局关闭“资源自动续费”且账户余额充足时，则资源在下一个计费周期会自动进入回收站，需在回收站对资源进行续费操作，并恢复资源。

资源在创建时，所有计费资源的计费计价均会通过资源计价器按照计费方式进行展示，用于确认订单的费用。每个计费周期内的资源均支持释放和删除，当资源在回收站被成功销毁时，将按照计费周期所剩余额进行退费。当账户余额不足时，可通过云平台管理员进行充值。

21.1 资源计价器

资源计价器为用户提供资源付费方式的选择，并展示付费模式下所有资源的费用信息及资源的“购买”确认按钮，如下图示例所示：



- 计价器中付费方式支持用户选择时、月、年，分别代表按时计费、按月计费、按年计费，其中选择月和年时，可以选择购买的月份数量和年份数量。
 - 月份可选择 1~11，分别代表 1 个月或 11 个月；
 - 年份可选择 1~5，分别代表 1 年或 5 年；
- 合计费用指当前订单中所有计费资源一个计费周期的费用合计，如一个虚拟机订单中，包括指定的 CPU 内存、云盘(若有)、EIP(若有)等资源按照付费方式的费用合计。

点击立即购买后，即从账号余额扣除合计费用金额，并产生一个新购订单及一笔扣费的交易流水；若账号余额不足一个计费周期时，无法点击立即购买，需要先对账号进行充值，才可进行购买和创建资源操作。

21.2 订单管理

订单管理是平台为用户提供的订单查询及统计服务，通过订单管理可以查看平台账号及子账号所有订单记录，支持查看1天、3天、7天、14天、1个月及自定义时间的历史订单记录。对资源进行创建、续费或变更配置时，会分别产生新购、续费及升级等类型订单，如下图所示：

订单号	资源ID	地域	订单类型	订单金额(元)	创建时间
order-r8EkBT4GR	ipsvpn-4yEzfT4Gg	地域01	新购	560.0000	2020-07-29 16:42:28
order-lLozBo4GR	eip-nQokfT4GR	地域01	新购	50.0000	2020-07-29 16:42:21
order-i-QhNoVMg	eip-C_7HmiGMR	地域01	续费	50.0000	2020-07-29 13:19:54
order-l9c2NTVGg	eip-0FUSmmMGR	地域01	续费	50.0000	2020-07-29 13:19:41
order-ZmA5K7Mg	eip-UlmAck7Mg	地域01	新购	50.0000	2020-07-15 14:57:50
order-Z7qTcFnMg	eip-MMmqo5K7GR	地域01	新购	50.0000	2020-07-15 14:57:46
order-wH95dK7Mg	eip-PIr5OFnGg	地域01	新购	50.0000	2020-07-15 14:21:09
order-cITBNF7Gg	disk-IQTBNFnMR	地域01	新购	4.0000	2020-07-15 13:50:21
order--SBv4FnMg	vm-u4fd4K7Mg	地域01	新购	148.0000	2020-07-15 13:09:28
order-33qV4KnGR	vm-VVcsJQGGg	地域01	升级	308.4840	2020-07-15 13:08:01

- 订单号：指当前订单的全局唯一标识符；
- 资源 ID：产生当前订单的资源标识符；
- 地域：当前订单资源所在的区域；
- 订单类型：当前订单的类型，包括新购、续费及升级三种类型；
 - 新购是指用户新创建的计费资源，包括虚拟机、云硬盘、弹性 IP、NAT 网关及负载均衡等；
 - 续费是指预付费资源每一个计费周期续费时产生的订单，包括手动续费和系统自动续费；
 - 升级是指按月按年计费的资源变更配置时产生的续费订单，如升级带宽、升级虚拟机配置等；
- 订单金额：当前订单金额，即订单在新购所付的费用或升级时补的差价；
- 创建时间：当前订单记录的生成时间，如图上所示，一个按时计费的资源，每小时产生一条续费订单。

主账号与所有子账号的订单管理及数据相同，可通过一个账号查看所有订单记录。

21.3 交易管理

交易管理是平台为用户提供的账号金额相关的收支明细，包括扣费、充值、退费及统计服务。通过交易管理可查看平台账号及子账号所有交易流水记录，支持查看1天、3天、7天、14天、1个月及自定义时间的历史交易记录，如下图：

The screenshot shows a table of transaction history. At the top left, there is a dropdown menu set to "一个月内" (One month) with the date range "2019-02-19 15:58:19 — 2019-03-19 15:58:19". On the far right, there is a refresh icon. The table has columns: 交易单号 (Transaction ID), 交易类型 (Transaction Type), 支出(元) (Spending), 收入(元) (Income), 账户余额(元) (Account Balance), 免费余额(元) (Free Balance), and 交易时间 (Time). The data shows various transactions including account top-ups and deductions, with dates ranging from March 19, 2019, to March 19, 2019.

交易单号	交易类型	支出(元)	收入(元)	账户余额(元)	免费余额(元)	交易时间
trade-vdm1lp3mg	免费账户充值	0.00	100.00	0.00	91968.66	2019-03-19 15:57:18
trans-YRyZltqmgz	扣费	1600.00	0.00	0.00	91868.66	2019-03-19 15:50:00
trans-2v1ZStqmRz	扣费	250.00	0.00	0.00	93468.66	2019-03-19 15:49:55
trans-n2kj4t3mgz	扣费	8.00	0.00	0.00	93718.66	2019-03-19 15:46:22
trans-HIN94pqmRz	扣费	14.43	0.00	0.00	93726.66	2019-03-19 15:45:57
trans-jOgw4tqmRz	扣费	264.00	0.00	0.00	93741.09	2019-03-19 15:44:10
trans-ErPs4p3mgz	扣费	13.88	0.00	0.00	94005.09	2019-03-19 15:43:27
trans-5carkt3igz	扣费	0.02	0.00	0.00	94018.97	2019-03-19 14:18:45
trans-4m6Ygtqgz	扣费	0.02	0.00	0.00	94018.99	2019-03-19 13:57:39
trans-U9Nlq53iRz	扣费	0.28	0.00	0.00	94019.01	2019-03-19 13:25:03

[<] [1] [2] [3] [4] [5] [>] [10条/页] [1 / 10]

- 交易单号：当前交易记录在全局唯一的 ID 标识符，一般扣费以 `trans` 开头，充值以 `trade` 作为开头；
- 交易类型：当前交易记录的类型，根据平台对资源的不同操作，分别包括充值和扣费：
 - 充值指平台管理员通过后台为租户进行的充值操作；
 - 扣费指系统针对每个资源的计费方式，在每个计费周期自动从账号余进行的扣费操作，如按小时计费的虚拟机，每小时按照单价进行一次扣费；
- 支出：当前交易记录所扣费的金额，仅当交易类型为扣费时有效，充值类型显示为 `0.00`；
- 收入：当前交易记录进账的金融，仅当交易类型为充值时有效，扣费类型显示为 `0.00`；
- 免费余额：当前账户在当前交易记录发生后的当前余额；
- 交易时间：当前交易记录发生时间。

主账号与所有子账号的交易流水记录相同，可通过一个账号查看租户的整体收支记录。