UCLOUD优刻得

中国第一家公有云科创版上市公司

股票代码：688158

UCloudStack 2.10

私有云用户操作手册

文档更新：2023 年 10 月 26 日

版权信息

关于文档

优得刻科技股份有限公司在编写本文档时已尽最大努力保证其内容准确可靠，但优得刻科技股份有限公司不对本文本中的遗漏、不准确或错误导致的损失和损害承担责任。

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。

目录

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。

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。

(1) 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。

(2) 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、高可用 VIP 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。

(3) 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。

(4) 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；
- **高可用 VIP**：提供高可用 VIP 服务，HAvip 是归属于 VPC 内某个子网内的可漂移内网 IP，用户可将 VIP 与高可用服务结合，以便在服务出现故障时进行服务入口的漂移，以实现服务的高可用。
- **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；
- **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 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。

- **应用商店**：支持管理员指定租户安装应用，实例归属指定租户所有，目前只有终端检测响应平台 EDR、数据库审计 UDAS 两款应用，只支持安装部署。
- **文件存储**：支持管理员指定租户在控制台创建文件存储实例，在虚拟机实例中安装文件存储客户端，使用标准挂载命令挂载创建的文件系统，就可以在多个实例间共享文件。
- **对象存储**：对象存储服务 OSS（Object Storage Service），兼容亚马逊云的 S3 API（接口协议），仅需在 UCloudStack 平台上创建对象存储实例，便可以在任何应用、任何时间、任何地点通过存储和访问任意类型的数据。对象存储为云原生设计，即使在高负载的情况下也可以高效利用 CPU 和内存资源，适合私有云场景。
- **隔离组**：隔离组是一种针对虚拟机资源的简单编排策略，支持组内或组之间的实例分散到不同物理机上，用以保障业务的高可用。
- **组播**：作为一种与单播（Unicast）和广播（Broadcast）并列的通信方式，组播（Multicast）技术能够有效地解决单点发送、多点接收的问题，从而实现了网络中点到多点的高效数据传送，可以为企业节约网络带宽、降低网络负载，在 ucloudstack 平台创建组播产品，支持 VPC 内组播通信。

(5) 统一云管平台

- 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。

(6) 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额及产品价格；
- 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、节点资源、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、高可用 VIP、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。

(7) 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。

1.4 应用场景

- **虚拟化&云化**

通过将业务系统和内部应用部署至 UCloudStack 平台，可为用户提供一套集虚拟化、分布式存储、SDN 网络为一体的私有云平台。平台支持多数据中心管理，可将业务部署至多个数据中心构建灾备云或边缘计算，同时支持与公有云无缝打通，灵活调用公有云能力，帮助政企快速构建安全可靠的业务架构。

- **业务快速交付**

平台服务所见即所得，可通过自服务云管理平台一键部署并管理业务交付所需的基础设施和中件间，包括在线扩容、负载分发、数据库缓存及监控日志等应用基础环境服务能力；同时平台支持镜像导入导出，可方便快捷将业务系统迁移至云平台，并可对所有业务系统的资源进行统一管理。

- **超融合一体机**

平台提供一体机交付模式，多款机型应用不同业务场景，集成 UCloudStack 私有云平台，出厂预装开箱即用，服务模块热插拔可按需部署，提供虚拟化、网络、存储、数据库、缓存及云管等一系列云服务能力；同时可通过与 IDC 数据中心互联，构建混合云解决方案。

- **政企专有云**

UCloudStack 提供租户控制台和管理员控制台，支持多租户、账户注册、计量计费等功能特性，同时为云平台管理者提供运营运维管理功能，包括资源管理、租户管理、价格配置、资源规格配置、部署升级及监控日志等服务，为政企提供行业专有云解决方案。

UCloudStack 轻量级私有云属于 IaaS+PaaS 复合型产品，并可按需搭载大数据、安全屋、AI 等公有云产品，适用于全行业客户需要云化且私有部署的业务

应用上云场景，典型行业如下：

- **政府、央企、军工、交通、制造型企业**

对外承担公共服务职责，内外部业务应用系统和商用软件需要快速交付、资源共享、智能调度及统一管理等上云需求的行业客户。

- **泛互联网行业，如 B2B 电商、大数据、教育等企业**

需要构建行业专属云，结合自有 SaaS 业务为其用户提供整体解决方案的行业客户。

- **人工智能和科研实验室行业**

需要大量可快速交付且私有化部署的虚拟化环境，用于科研项目和训练系统的快速部署和管理的行业客户。

2 账号注册与登录

2.1 注册登录

本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：

- 账号名称：注册账号的名称，仅支持中英文字符，长度在 5-50 字符之间；
- 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：允许进行密码复杂度的修改，密码须包含有大写字母、小写

字母、数字、特殊符号（除空格）中的两种或以上，密码长度为 6-30 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“私有云平台激活账户”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。

2.2 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。

2.3 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。

在平台成功对接 OAuthy 认证后，在登录页面会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。

3 概览页

3.1 概览页

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，概览页展示的是当前登录账号的资源综合统计信息，包括当前账号最近 12 小时的告警记录信息、资源状态信息、系统信息、虚拟机 CPU 使用率 Top5 数据、虚拟机内存使用率 Top5 数据、虚拟机磁盘总读吞吐 Top3 数据、虚拟机磁盘总写吞吐 Top3 数据、资源配额使用情况，其中资源状态信息包括虚拟机、硬盘和外网 IP 的总数量、非稳定状态数量及已过期资源列表，并可对平台进行登出操作：

- 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。
- 资源状态信息信息：当前账号下虚拟机、硬盘和外网 IP 的总数量、非稳定状态数量及已过期资源列表。
- 系统信息：云平台的系统信息，包括系统 ntp 服务、计费功能、资源自动续费功能、资源是否可删除。
- 虚拟机 CPU 使用率 Top5:当前账号下 CPU 使用率前 5 的虚拟机。
- 虚拟机内存使用率 Top5:当前账号下内存使用率前 5 的虚拟机。
- 虚拟机磁盘总读吞吐 Top3:当前账号下磁盘总读吞吐前 3 的虚拟机。

- 虚拟机磁盘总写吞吐 Top3:当前账号下磁盘总写吞吐前 3 的虚拟机。
- 资源配额使用情况：当前账号各种资源的配额及占用信息，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。
- 通过点击概览页面的告警记录可进入告警历史记录页面，查看更多告警记录。点击资源 ID 可进入资源详情页，查看资源详情信息。点击配额使用情况“查看更多”按钮，可进入配额信息页面，查看更多资源配额信息。

3.2 导航栏

在控制台的上方导航栏，可为用户展示平台 logo、地域切换、费用中心、账号和组织及账号信息展示等按钮入口。

- **平台 logo**：平台管理员自定义的 logo 图标，可在管理员控制台中进行自定义配置。
- **地域切换**：平台支持多地域统一管理，通过地域切换按钮可进行不同地域的管理，在不同的产品服务页面，切换地域按钮将会仅展示和操作当前地域的资源和管理。
- **费用中心**:通过费用中心可进入租户计量计费管理模块,包括订单管理、交易管理及账单管理。
- **账号和组织**：通地账号和组织可进入账号及子账号授权管理模块，包括当前登录账号信息及账号安全配置，并可进行配额信息的查看；同时结合人员管理、角色管理、项目组管理可进行精细化子账号资源级权限授权管理。
- **账号信息**：点击右上角的账户名称，可展示账号信息模块，查看当前账号的邮箱地址、账号级别、账号余额等信息，并可通过查看 API 密钥、修改登录邮箱、简/EN、文档中心进行账号的管理；同时可查看当前平台的版本号。如下图如下示：

- 查看 API 密钥：通过该入口可查看当前账号的 API 密钥。
- 修改登录邮箱：修改当前登录账号的登录邮箱地址。
- 简/EN 切换：支持中英双语平台，可通过按钮进行中文和英语的切换。
- 文档中心：进入平台提供的在线操作手册。

4 计算服务

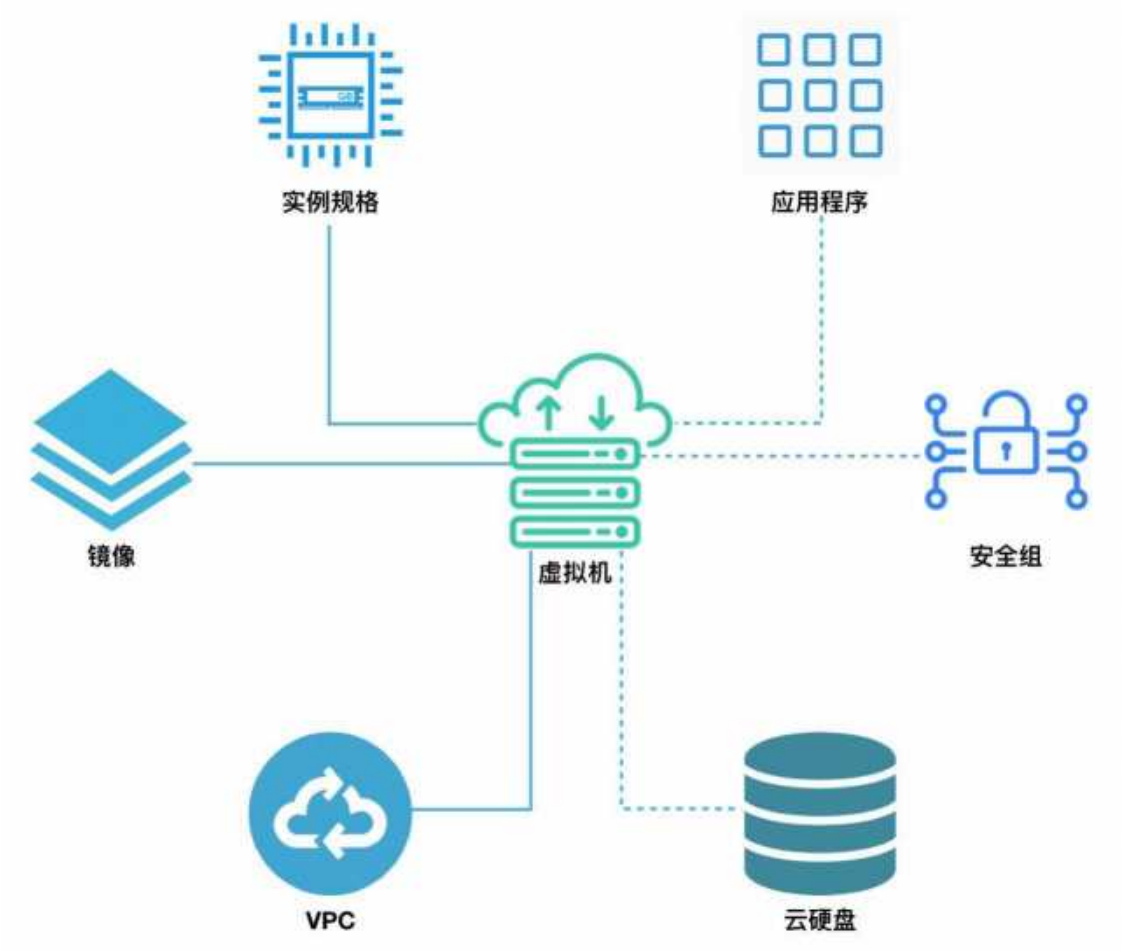
4.1 虚拟机

4.1.1 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、磁盘等服务结合提供完整的计算环境。

- 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 及网络防火墙，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。支持透传的设备包括 NVIDIA 的 K80、P40、V100、2080、2080Ti、T4 及华为 Atlas300 等。

4.1.2 创建虚拟机

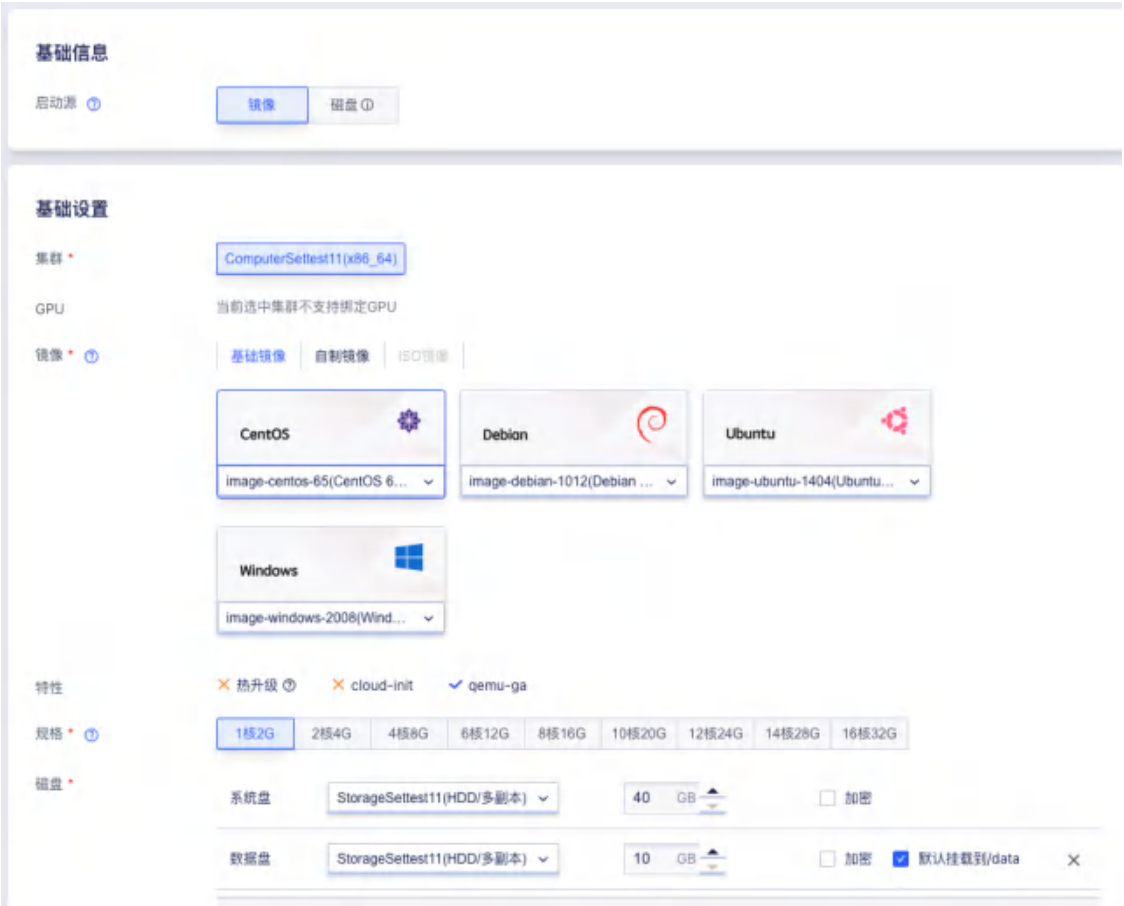
云平台用户可以通过指定机型、规格、镜像、云硬盘、VPC 网络、公网 IP、安全组、USB、DNS、及虚拟机相关基础信息一键创建多台虚拟机，用于部署自己的应用和服务。

4.1.2.1 前提条件

- 在创建虚拟机前，已拥有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；
- 确认已创建所需要的 VPC、子网、安全组以及安全组规则，满足在目标地域中的网络划分以及业务需求的安全规则。

4.1.2.2 创建操作

(1) 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；



(2) 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节点的集群类型，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，通过 ARM 机型创建的实例为 ARM 版虚拟机实例，已适配国产芯片、服务器及操作系统，并可运行国产化操作系统，如 UOS 或银河麒麟。

- 镜像即虚拟机实例运行环境的模板，可以选择基础镜像、自制镜像和 ISO 镜像。

  - 基础镜像是由平台官方默认提供，包括多发行版 Centos、Ubuntu、Debian 及 Windows 等原生操作系统，同时基础镜像的默认时区为上海。

  - 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。

  - ISO 镜像目前平台未默认提供，需要用户通过本地或者 URL 进行上传使用。

(3) 查看镜像特性：镜像特性包括热升级、cloud-init、qemu-ga 及是否加密。

(4) 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 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，支持选择 GPU 类型，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。

(5) 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，并选择是否对磁盘加密。

- 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 加密系统盘创建时默认增加 1G 空间，系统盘最大支持 2T，支持扩容系统盘容量至 2T，步长为 1GB，即容量应为 1GB 的倍数。

  注意：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。
  - 数据盘挂载路径可选择默认为/data（windows 系统除外），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 32000GB，步长为 1GB，即容量应为 1GB 的倍数。
- 磁盘加密：系统盘、数据盘密码输入，设置密码后，对应的硬盘将会被加密。
  - 目前不支持修改任一资源的密钥。

- 磁盘一旦被加密，除非格式化，否则无法去除加密。
- 用户自己制作的加密数据盘，创建的虚拟机，无法使用平台的加密机制，因为无法感知数据盘是否加密。

注意：加密属性继承，由加密资源产生的新资源自动被加密。如快照、自制镜像、克隆磁盘，都会继承加密属性。

(6) 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。若手动指定的 IP 地址已被使用，则会弹出占用提示。
- 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；
- 外网安全组和内网安全组默认为暂不绑定，可在创建虚拟机后再进行绑定；
- 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 50 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。若手动设置的外网 IP 地址已被占用，则弹出占用提示。支持通过标签筛选外网线路资源。
  - 镜像特性不支持 qemu-ga 时，创建虚拟机不可申请直通 EIP，可以在虚拟机创建完成后绑定 NATEIP，绑定 NATEIP 需要开启 VPC 网关；

  注：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。

(7) 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、登录密码（可选择随机生成）、项目组和标签等。

- 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，可选择随机生成；
  - CentOS 的管理员为 root，Ubuntu 的管理员为 ubuntu，Debian 的管理员为 root，Windows 系统的管理员名称为 administrator；
- 标签：选择已创建的标签键值对绑定虚拟机资源。

注：创建虚拟机选择的镜像既无 cloud-init 特性也无 qemu-ga 特性时，管理员名称、登录方式、管理员密码不展示。

(8) 配置高级设置，包括主机名、USB、DNS、CPU 启动模式，高可用模式，隔离组，自定义数据。

- 主机名：表示操作系统内部的计算机名，批量创建时会在当前填写主机名添加有序后缀，新的主机名会在实例重启后生效；

  注：Windows 系统，长度为 2~15 个字符。Linux 系统，长度为 2~63 个字符。在批量创建时，Windows 最大支持 12 字符，Linux 最大支持 60 位字符。

- USB：支持 USB 透传功能，物理机 USB 设备可直接透传至该物理机上所运行的云主机，USB 设备包含以下两种模式：
  - 直通：将 USB 设备加载到此物理机上的云主机，迁移云主机时需要卸载此 USB 设备；
  - 转发：将 USB 设备加载到此物理机所在计算集群内的云主机，迁移云主机时不需要卸载此 USB 设备；
- DNS：支持自定义 DNS，最多支持两个 ip，多个 ip 请换行；
- CPU 启动模式：虚拟机启动时 CPU 使用的模式，分为默认和直通，其中直通模式在线迁移需要 2 个物理机的 CPU 型号完全一致；

- 高可用模式：该策略可触发云主机自动重启，提高云主机可用性。高可用为永不停止的虚拟机进行保活，为无的不进行保活；
- 隔离组：隔离组是一种针对虚拟机资源的简单编排策略，支持组内或组之间的实例分散到不同物理机上，用以保障业务的高可用。
- 自定义数据：即自定义初始化脚本，经过 base64 编码，最大 1M，可在初次启动和每次开机/重装/重启时执行。选择的镜像支持 cloud-init 时，支持输入。

(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。

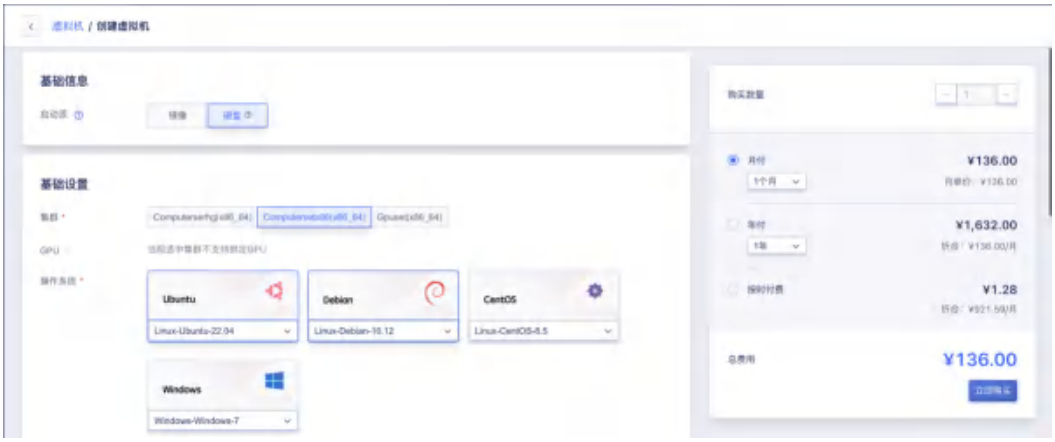
- 购买数量：按照所选配置及参数批量创建多台虚拟机，最多可批量创建 10 台虚拟机，批量创建时不支持手动设置虚拟机的 IP 地址；
- 付费方式：选择虚拟机的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式；
- 合计费用：用户选择虚拟机 CPU、内存、数据盘、外网 IP、GPU 等资源按照付费方式的费用展示；
- 立即购买：点击立即购买后，会返回虚拟机资源列表页，在列表页可查看该台主机的创建过程，通常会先显示“启动中”的状态，在 1~2 分钟内

即可创建完成。

4.1.2.3 从磁盘创建虚拟机

云平台允许用户基于已有的磁盘镜像创建自己的虚拟机实例。这项功能为用户提供了灵活、快速、可定制化的虚拟机创建方式。

首先，用户可以通过云平台的云硬盘服务创建自己需要的磁盘。可以选择不同的容量等配置选项，确保满足个性化需求，用户可以将已有的云硬盘用作虚拟机的系统盘。



接下来，用户可以创建虚拟机，选择启动源为磁盘，根据磁盘中挂载的操作系统，选择相应的集群与操作系统，可选 Ubuntu、Debian、CentOS、Windows。

根据需求选择虚拟机所支持的特性以及规格，然后系统盘需要选择“已有云硬盘”，通过这种方式，用户可以快速创建具有个性化配置的虚拟机实例，并根

据需要灵活调整存储容量和性能。用户可以通过远程登录工具连接到虚拟机，安装和配置所需的软件和应用程序，满足自己的业务需求。

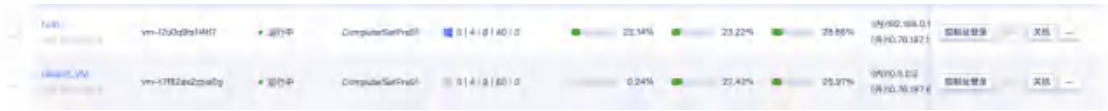
总之，从磁盘创建虚拟机是云平台提供的一项便捷而灵活的功能，它使用户能够快速搭建自己的虚拟机环境，并提供了强大的存储管理和定制化能力。

4.1.3 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。

4.1.3.1 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、资源 ID、状态、VPC、子网、集群与特性、配置、CPU 使用率、内存使用率、磁盘使用率、IP 地址、项目组、高可用级别、计费方式、创建时间、过期时间、标签及操作等，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；
- 状态：虚拟机当前的运行状态，包括启动中、运行、关机中、关机、重启中、修改配置中、重装中、删除中、断电中和销毁中等，在管理员侧还有迁移中和宕机迁移中等状态；
- 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；

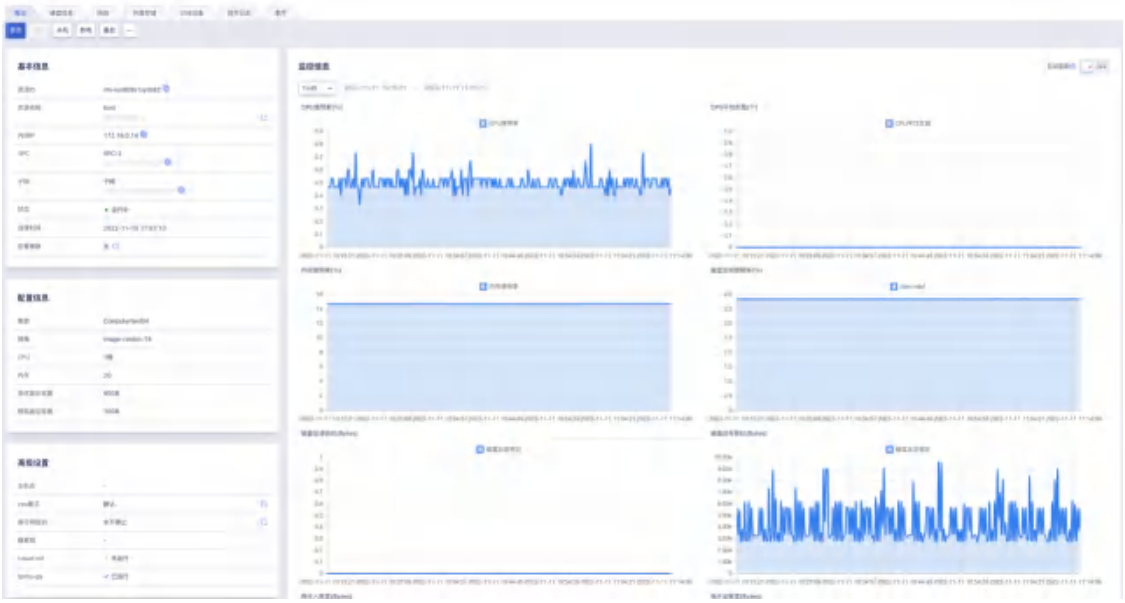
- 集群与特性：虚拟机所运行物理机的集群类型，代表不同架构、不同型号的 CPU 或硬件特征；
- 配置：虚拟机基本配置信息，包括 CPU 内存规格、GPU 颗数、系统盘镜像、系统盘总容量及数据盘总容量；
- 计费方式：虚拟机创建时指定的付费方式，包括按时、按月、按年；
- 创建时间/过期时间：虚拟机的创建时间和计费周期内的过期时间；
- CPU 使用率、内存使用率、磁盘使用率：在列表页展示三种监控数据；
- 高可用级别：虚拟机保活策略，该策略可触发云主机自动重启,提高云主机可用性；
- 标签：虚拟机绑定的标签键值；
- 操作：对单台虚拟机的更多操作，包括详情、登录、启动、关机、删除、断电、重启、续费、修改告警模板、制作镜像、重置密码、重装系统、热升级、绑定外网 IP、修改外网安全组、修改内网安全组、修改配置、绑定 USB、修改标签、修改自定义数据及获取 VNC 信息等。

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，CPU 和内存支持按照使用率进行正序，倒序查看。

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，关机，断电，删除，开启虚拟机保活，关闭虚拟机保活，修改告警模版操作，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：

4.1.3.2 虚拟机详情信息

在虚拟机列表上，点击虚拟机的名称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、操作日志，同时可切换到 USB 设备，硬盘信息、网络，外置存储页面查看虚拟机相关的磁盘、外置存储盘，USB 设备，网络、IP 地址及弹性网卡信息，如下图概览页所示：



4.1.3.2.1 虚拟机概览

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

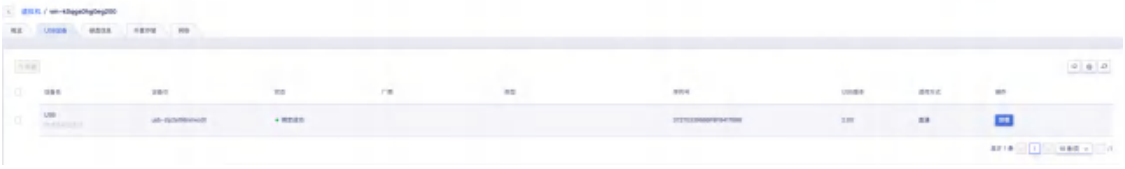
- 基本信息包括资源 ID、名称、内网 IP、VPC、子网、状态、创建时间及告警模板。
  - 可点击名称右侧按钮修改虚拟机的名称和备注信息；
  - 可点击告警模板右侧按钮修改虚拟机所关联的告警模板，虚拟机默认会不绑定告警模板；
- 配置信息包括机型、镜像、CPU、内存、系统盘总容量和系统盘总容量，其中数据盘容量为当前虚拟机所关联所有云硬盘的容量之和；

- 高级设置包括主机名，cpu 模式，高可用级别，隔离组，cloud-init，qemu-ga，点击高可用级别修改按钮可变更高可用级别，点击 cpu 模式修改按钮可以变更 cpu 模式；
- 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。

4.1.3.2.2 USB 设备

USB 设备页面展示虚拟机绑定的 USB 设备，包括那个 USB 设备名、设备 ID、状态、厂商、类型、序列号、USB 版本、透传方式及卸载 USB 设备的操作。如下图所示：



4.1.3.2.3 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和共享盘信息，包括每个硬盘的名称、ID、集群架构、集群、是否加密、硬盘类型、硬盘容量、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：

- 集群架构是指虚拟机系统盘或数据盘所属物理机所在的集群架构，包括 HDD、SSD、NVME 等，代表集群的磁盘介质类型；
- 集群指虚拟机系统盘或数据盘所属物理机所在的集群，可由管理员自定义，如容量型或性能型等；
- 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；
- 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；
- 是否加密表示虚拟机硬盘加密状态。

在虚拟机硬盘管理列表的操作项中，支持对虚拟机的系统盘和数据盘进行扩容、续费及快照操作，支持数据盘的续费、绑定、解绑操作，系统盘与虚拟机生命周期一致，支持共享盘的挂载、扩容、续费操作。数据盘支持解绑绑定。

4.1.3.2.3.1 硬盘快照

支持对系统盘和数据盘分别进行快照操作，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。具体操作如下图所示：

4.1.3.2.3.2 硬盘扩容

支持对系统盘和数据盘分别进行扩容操作，扩容云硬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，即系统盘和数据盘扩容后需进入虚拟机内部进行文件系统的扩容（resize）操作，系统盘具体操作步骤详见【系统盘扩容】章节内容介绍。

扩容会按照新容量进行收费，按小时付费的硬盘，升级容量下个付费周期按新配置扣费；按年按月付费的硬盘，升级容量即时生效，并按比例自动补差价。

4.1.3.2.3.3 数据盘续费

支持在虚拟机中对已挂载至虚拟机的数据盘直接进行续费操作，续费时会按照续费时长收取费用，如下图所示：

云盘续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

云盘续费的时长与资源的计费方式相匹配，当数据盘的计费方式为【小时】，则续费时长指定为 1 小时；当数据盘的计费方式为【按月】，则续费时长可选择 1 至 11 月；当数据盘的计费方式为【按年】，则数据盘的续费时长为 1 至 5 年。

4.1.3.2.4 虚拟机网络

网络页面展示当前虚拟机的基本网络信息及高级设置信息，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。高级设置包括 DNS 和网卡 mac，点击修改按钮可以修改 DNS 和网卡 mac 地址，网卡 mac 地址需要关机后才能修改，如下图所示：

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。

4.1.3.2.5 虚拟机外网 IP

平台支持 IPv4/IPv6 双栈网络，每个虚拟机最多支持绑定 50 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（包括外网弹性网卡的 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。

外网 IP 信息包括虚拟机及绑定的外网弹性网卡 IP，仅支持将有默认路由的外网 IP 设为虚拟机默认网络出口。可通过列表信息查看已绑定外网 IP 的详细信息及相关管理操作，如图所示已绑定外网 IP 信息包括 IP 地址、IP 版本、IP 类型、出口、带宽、路由类型、绑定时间及状态。

- 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；
- IP 类型是指当前已绑定外网 IP 的 IP 类型，包括直通和 NAT；
- 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。

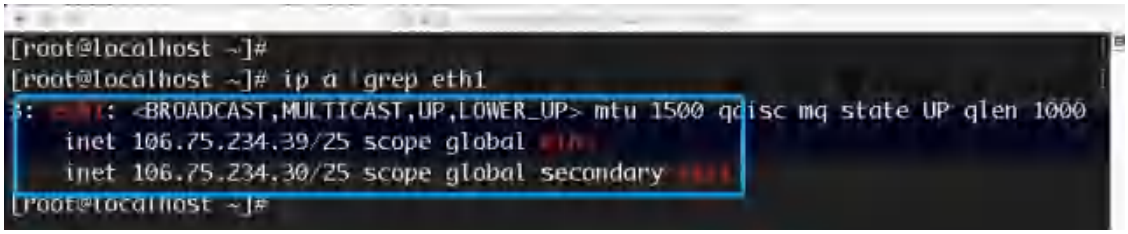
用户可通过外网 IP 管理控制台的操作项，进行外网 IP 地址的绑定、解绑及设为默认出口操作，并支持批量解绑。

注意：绑定至虚拟机的外网弹性网卡的 IP 地址同时会展示至外网 IP 列表，支持设为出口操作但不支持解绑，可通过解绑弹性网卡进行弹性网卡外网 IP 的解绑和释放。

4.1.3.2.5.1 绑定外网 IP

最多支持绑定 50 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：



虚拟机镜像未安装 qemu-ga 时，仅支持绑定 NAT 类型的外网 IP。

4.1.3.2.5.2 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。

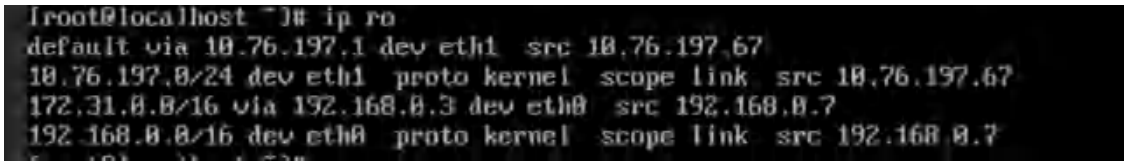
绑定至虚拟机的外网弹性网卡 IP 不支持解绑操作，如需解绑弹性网卡的 IP 地址，可直接解绑弹性网卡。

4.1.3.2.5.3 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 10.76.197.67 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：

登录 Centos 虚拟机，输入 ip ro 查看虚拟机访问外网的出口已更换为 10.76.197.67，如下图输出结果所示：



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。

4.1.3.2.6 虚拟机弹性网卡

x86 架构虚拟机最多支持绑定 6 块弹性网卡，ARM 架构虚拟机最多支持绑定 3 块网卡，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。

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，支持批量解绑操作。已绑定的弹性网卡信息包括名称、ID、网卡类型、所属网络、IP 地址、安全组及状态信息。

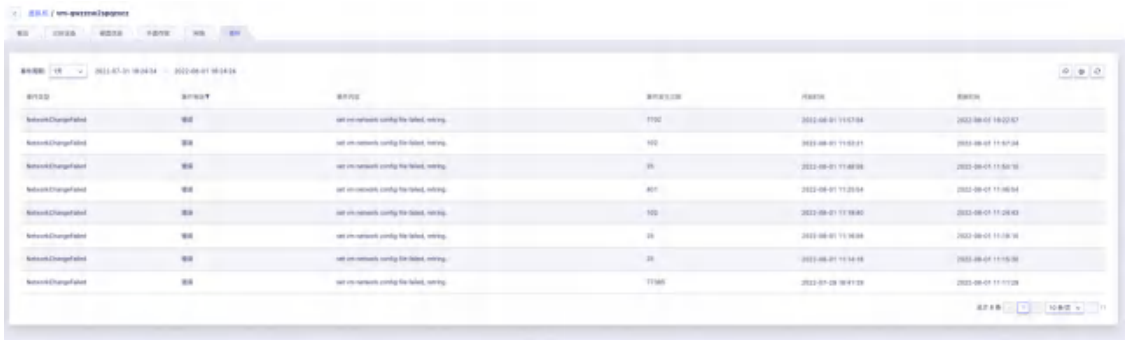
- 网卡类型：指当前绑定至虚拟机的弹性网卡类型，包括内网网卡和外网网卡。
  - 内网类型的弹性网卡仅可从关联的 VPC 子网中自动或手动分配 IP 地址。
  - 外网类型的弹性网卡仅可从关联的外网网段中自动或手动分配 IP 地址，且分配的 IP 地址与弹性网卡生命周期一致，仅支持随弹性网卡销毁而释放。
- 所属网络：弹性网卡的 IP 地址所属网络，内网类型的所属网络为弹性网卡所在的 VPC 网络和子网信息；外网类型的所属网络为弹性网卡所属外网网段信息。
- IP 地址：指当前弹性网卡的 IP 地址，内网类型的网卡 IP 为 VPC 子网分配的内网 IP 地址，外网类型的网卡 IP 为所属外网网段分配的外网 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。平台安全组为作用于网卡，即每块弹性网卡均可指定属于自己的安全组，分别对所关联的网卡进行流量控制。

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：

注意：虚拟机镜像未安装 qemu-ga 时，不支持绑定弹性网卡。

4.1.4 虚拟机事件

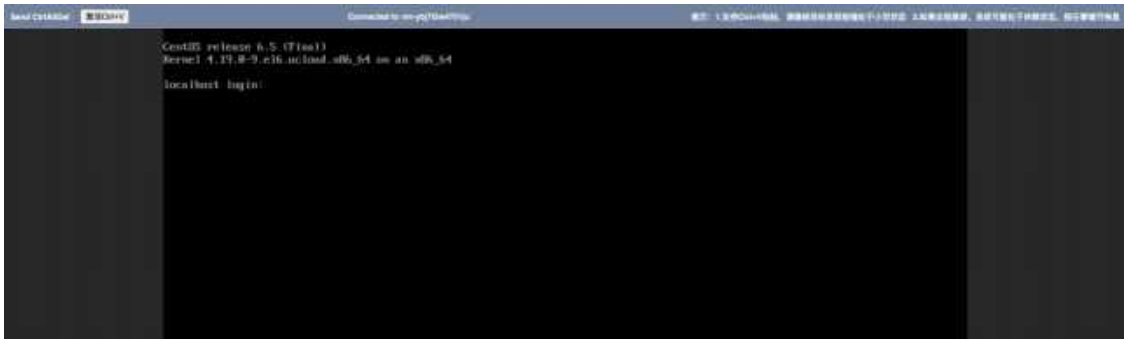
支持用户查看虚拟机操作相关的资源事件，内容包括事件类型、事件等级、事件内容、事件发生次数、开始时间和更新时间。如下图所示：



4.1.5 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“控制台登录”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：



注意：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。

4.1.6 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：

4.1.6.1 关机

- 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运行状态；
- 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、挂载云硬盘、重制密码、修改标签等操作。

4.1.6.2 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。

4.1.6.3 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，对虚拟机进行强行关机操作；

- 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。

4.1.6.4 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。

4.1.7 制作镜像

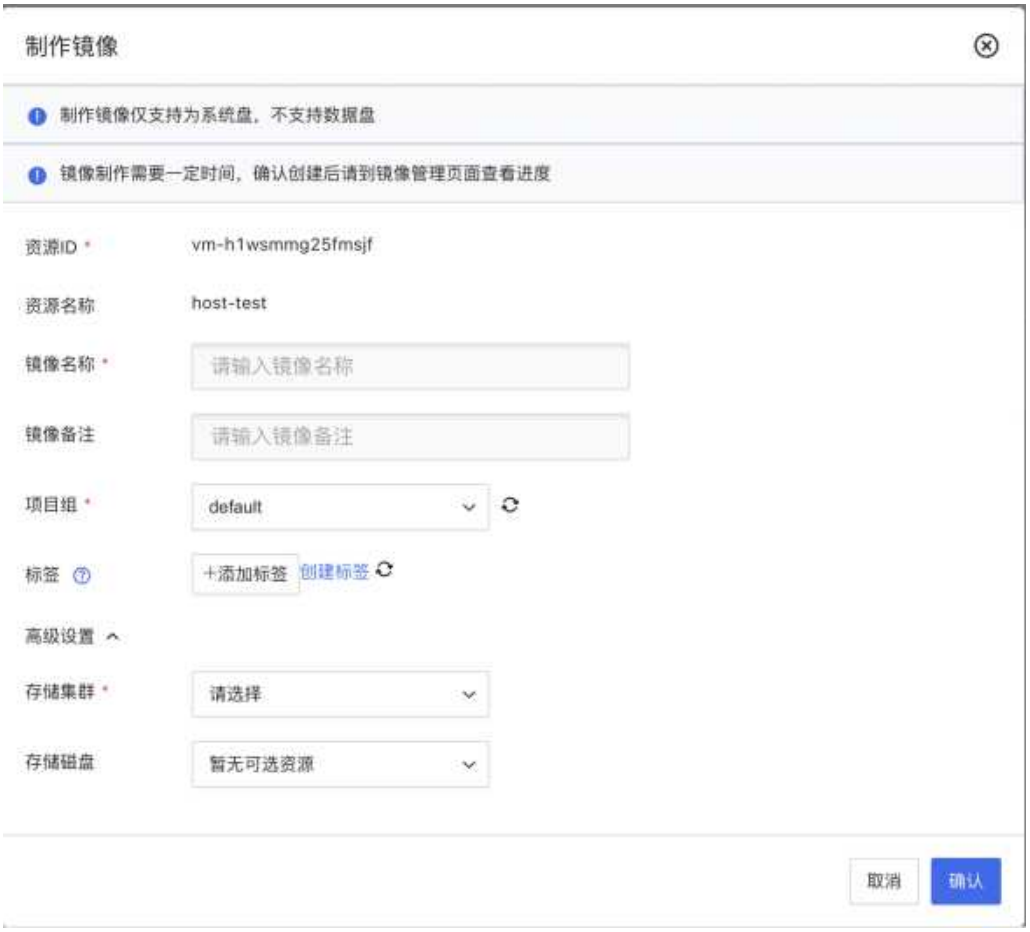
自制镜像由云平台账户通过虚拟机自行导出，可用于创建虚拟机，仅账户自身有权限查看和管理，仅支持虚拟机关机状态下制作镜像，即在关机状态才可进行虚拟机导出为镜像操作。

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；

从虚拟机制作镜像支持选择存储集群和外置存储的磁盘制作，不支持加密盘和共享盘，可在高级设置中选择，如下图所示：



在制作镜像过程中，用于制作镜像的磁盘与虚拟机绑定，并在虚拟机详情中临时中间盘列表展示，如下图所示：

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。

注意：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；加密系统盘创建的镜像为加密镜像。

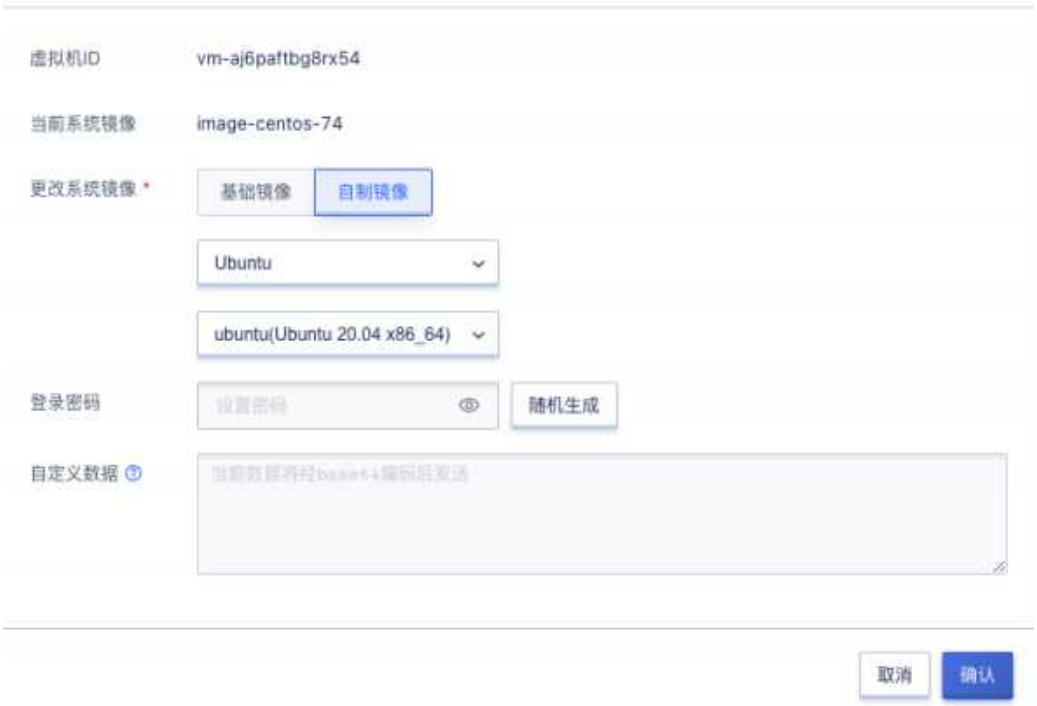
4.1.8 重装系统

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，可以在重装时进行密码重置操作：

重装系统将会自动清除虚拟机已创建的系统盘快照，可通过制作镜像对虚拟机系统盘数据进行备份。在重装系统过程中，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。

重装系统时若选择的镜像有 Cloud-init 特性，则支持输入自定义数据，如下图所示：



重装系统时若选择的镜像既无 cloud-init 特性也无 qemu-ga 特性，则不支持密码重置，重装后的登录密码为镜像密码，如下图所示：

注意：重装系统后，虚拟机之前操作系统及数据内容将被清空，挂载的云硬盘数据盘及快照不受影响，并且重装系统不影响磁盘的加密属性。

4.1.9 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 或 ubuntu 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；

虚拟机既无 cloud-init 特性也无 qemu-ga 特性时，不可操作重置密码。

注意：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。

4.1.10 修改配置（升降级）

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。

注意：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。

4.1.11 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：

（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：

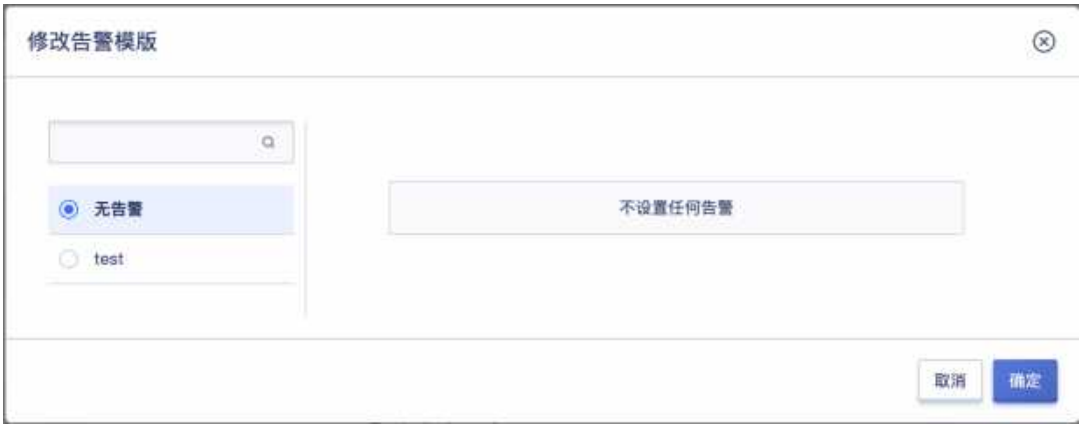
（2）在热升级的向导中，可以对虚拟机的 CPU 内存规格进行热升级操作，热升级后立即生效，按小时购买的虚拟机下个付费周期按新配置扣费，按年按月购买的虚拟机按比例自动补差价，如下图所示：

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。

4.1.12 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。



- 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。

4.1.13 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 50 个 IPv4 和 10 个 IPv6 外网 IP 地址，同时也可将外网弹性网卡绑定至虚拟机提供外网通信能力，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。

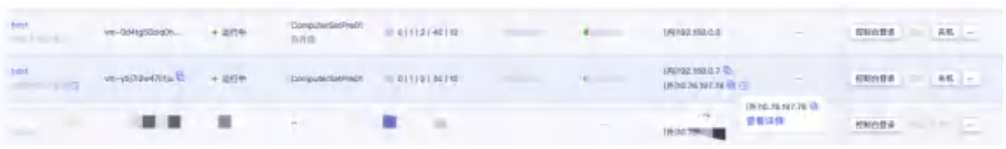
每台虚拟机创建时会自带两张默认网卡，分别为内网网卡和外网网卡，以 Linux 操作系统为例，内网网卡一般为为 eth0，外网网卡一般为 eth1，默认绑定的外网 IP 均会被配置在虚拟机的 eth1，即 50 个外网 IP 均会被绑定至外网网卡，并共用虚拟机的外网安全组；在虚拟机绑定外网弹性网卡时，会在虚拟机中直接增加一张弹性网卡，并自动配置外网弹性网卡配置 IP 地址及安全组策略。

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 50 个 IPv4 和 10 个 IPv6 外网 IP 地址。

- 若虚拟机已绑定 50 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 50 个 IPv4 和 10 个 IPv6 外网 IP 地址，则无法再绑定外网 IP 地址，可继续增加外网弹性网卡。

注意：虚拟机镜像未安装 qemu-ga 时，仅支持绑定 NAT 类型的外网 IP。

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，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。



仅支持绑定同一数据中心的外网 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。

4.1.14 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，同时也可在虚拟机上绑定弹性网卡资源。

- 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 50 个 IPv4 和 10 个 IPv6 地址；
- 弹性网卡：配置弹性网卡所属网络所分配的 IP 地址及安全组，若弹性网卡为内网类型则所属网络为 VPC 和子网，若弹性网卡为外网类型则所属网络为外网网段。

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。平台将绑定至虚拟机内网网卡的安全组定义为内网安全组；绑定至虚拟机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。

内网安全组用于虚拟机东西向（网卡间）的安全访问控制；外网安全组用于控制虚拟机南北向（外网 IP）的流量。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。

4.1.14.1 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请网络页面的“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。

注意：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。

4.1.14.2 修改内网安全组

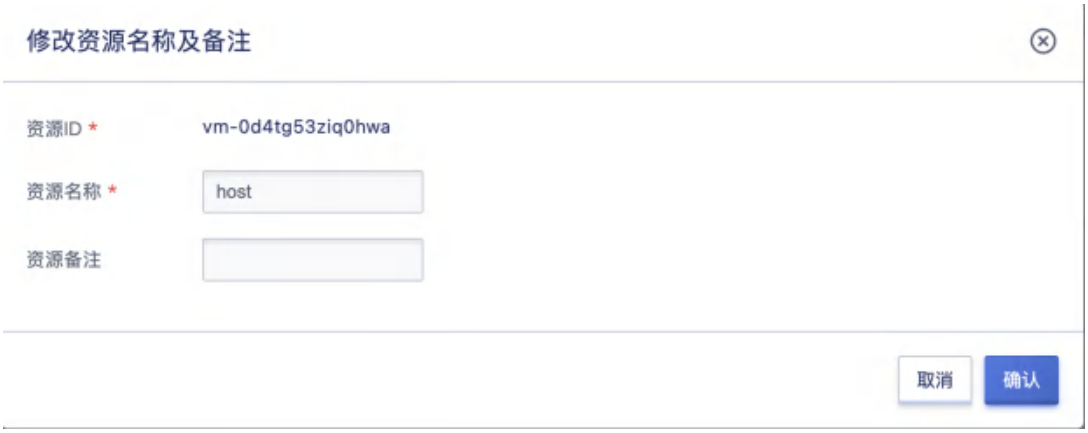
修改内网安全组是指修改虚拟机内网网卡所关联的安全组，即更改虚拟机内网的安全策略，用于虚拟机与虚拟机间的流量管控。用户可通过虚拟机列表及虚拟机详请网络页面的“修改内网安全组”按钮进行操作，如下图所示：

选择需要修改的内网安全组，支持修改为“无安全组”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。

注：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。

4.1.15 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：



4.1.16 虚拟机续费

支持用户手动对虚拟机进行续费，续费操作只针对资源本身，不对资源额外关联的资源进行续费，如外网 IP、云硬盘、外网弹性网卡等。额外关联的资源到期后，会自动解绑，为保证业务正常使用，需及时对相关资源进行续费操作，如下图所示：

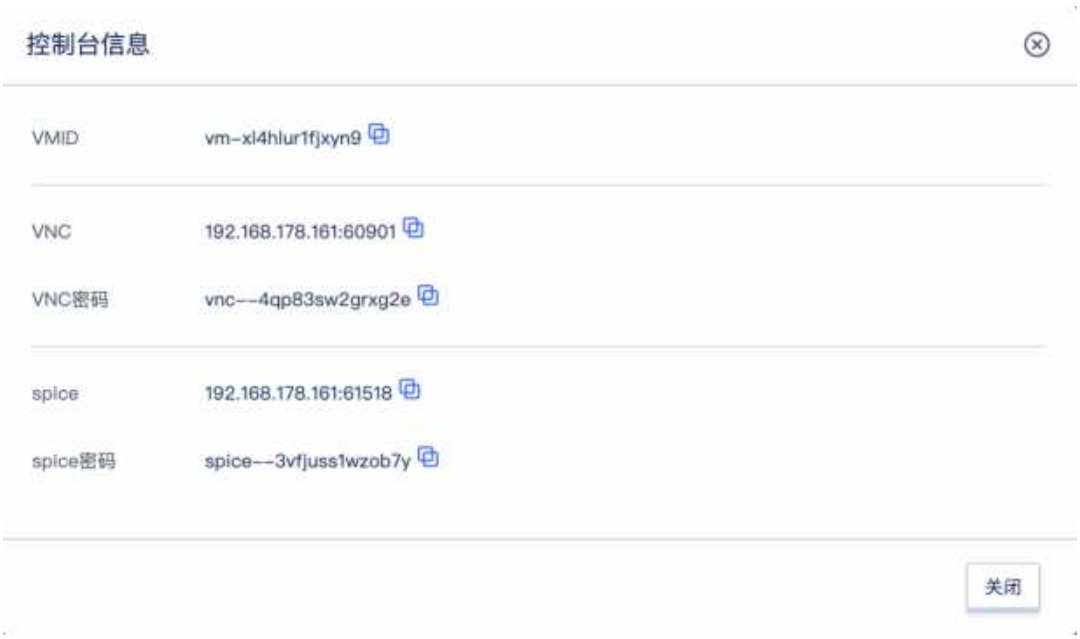
虚拟机续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

虚拟机续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当虚拟机的计费方式为【小时】，则续费时长可选择 1 至 24 小时；当虚拟机的计费方式为【按月】，则续费时长可选择 1 至 11 月；当虚拟机的计费方式为【按年】，则虚拟机的续费时长为 1 至 5 年。

4.1.17 获取 VNC 登录信息

支持用户获取虚拟机的 VNC 登录信息，适用于使用 VNC 客户端连接虚拟机的场景。如桌面云场景中，桌面云服务商的桌面终端通常会以 VNC、Spice 及 RDP 等协议连接平台提供的桌面虚拟机，其中 VNC 和 Spice 协议基本作为桌面服务商的通用协议。

用户可通过 API 接口或虚拟机控制台操作项中的【获取 VNC 信息】查看虚拟机的 VNC 登录信息，包括虚拟机 ID、VNCIP 地址、VNC 端口及 VNC 客户端登录密码，如下图所示：



- VNCIP 地址：当前云平台外网 IP 地址池中分配的地址，可访问外网 IP 地址的网络均可使用 VNCIP:端口和密码通过 VNC 客户端连接虚拟机，如 VNCView 客户端软件。
- VNC 端口：VNC 登录时使用的端口，为保证安全平台会在每次获取 VNC

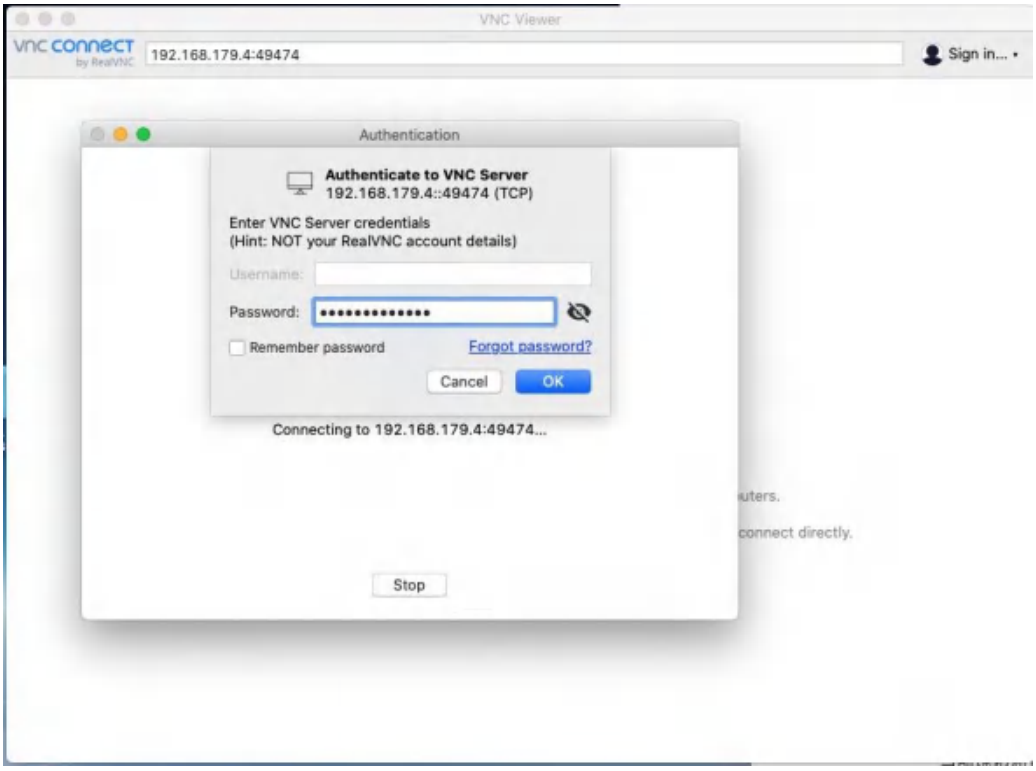
信息时更换一个未被使用的端口。

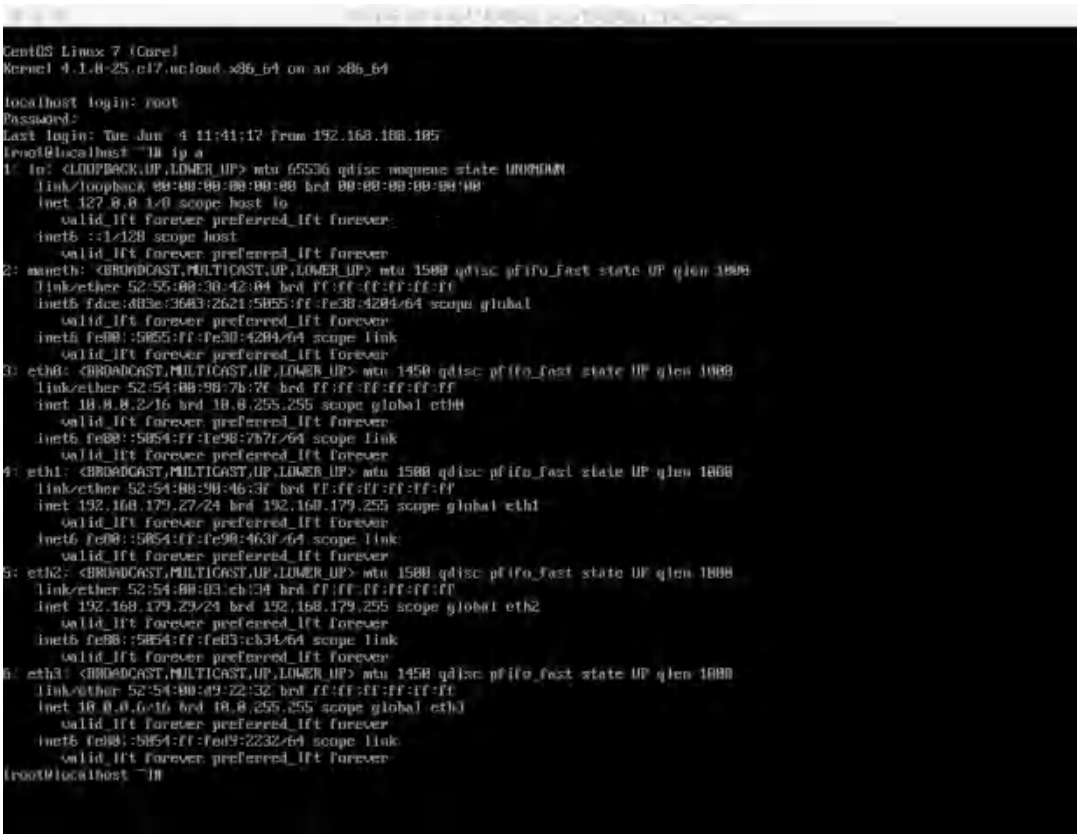
- VNC 密码：VNC 登录时使用的密码，每一次查看均会根据算法随机提供新的 VNC 登录密码，为保证虚拟机 VNC 登录安全性（场景举例：用户首次使用 VNC 登录虚拟机后，通过虚拟机操作系统的登录密码进入到桌面或命令行，则下一次登录 VNC 会自动进入至桌面和命令行，对用户的虚拟机带来不可避免的安全隐患）

为确保 VNC 连接的安全性，每一次调用 API 或通过界面所获取的 VNC 登录信息有效期为 300 秒，如果 300 秒内用户未使用 IP 和端口进行连接，则信息直接失效，需要重新获取新的登录信息；同时用户使用 VNC 客户端登录虚拟机后，300 秒内无任何操作将会自动断开连接。

注意：用户在使用云平台时，至少会提供的一段可访问到云平台的外网 IP 网段，VNC IP 地址即为该网段中分配的 IP 地址，以确保网络可达。

用户可在网络可达平台的环境中，使用诸如 VNCView 客户端登录平台虚拟机，如下图所示：





4.1.18 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。

注意：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。

4.1.19 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）。

4.1.19.1 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：

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@10.76.197.78
```

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。

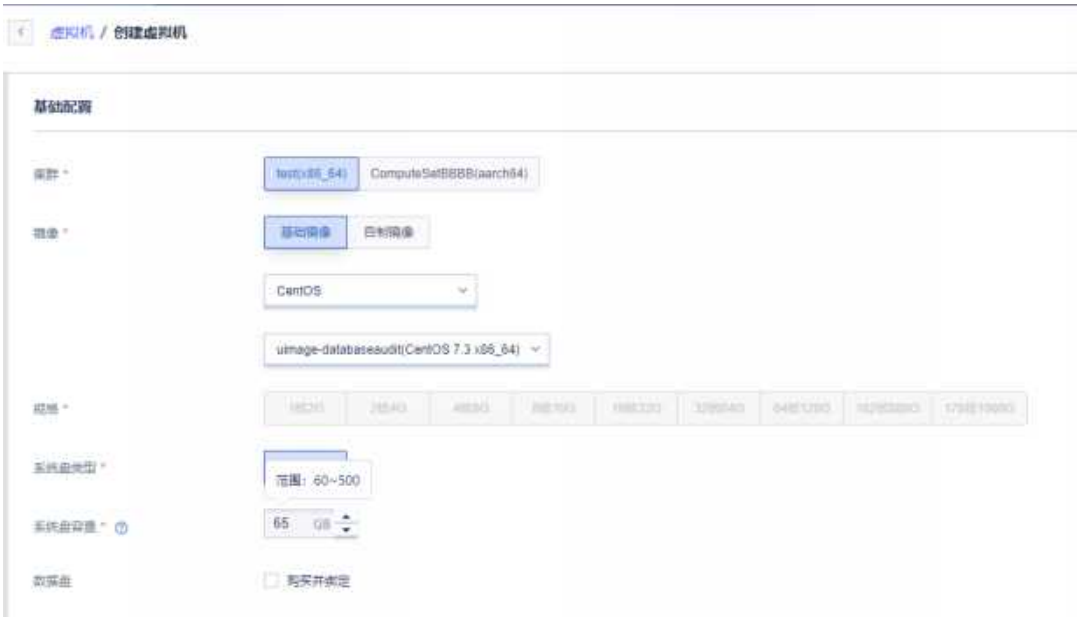
4.1.19.2 远程登录 Windows

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：

注：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。

4.1.20 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 2000GB。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。



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。

4.1.20.1 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
```

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><PartionNumber> 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 xfs 类型的文件系统，可使用 xfs_growfs<mountpoint>工具进行扩容。

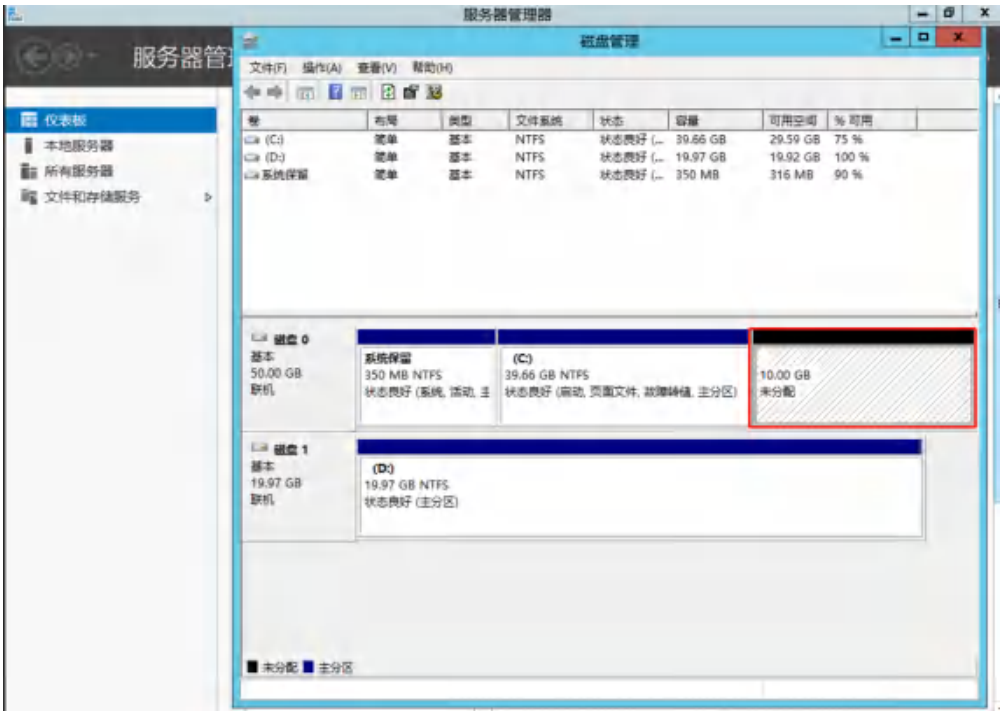
5、运行 df -Th 查看系统盘分区/dev/vda1 容量为 200GB 。


```
[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
```

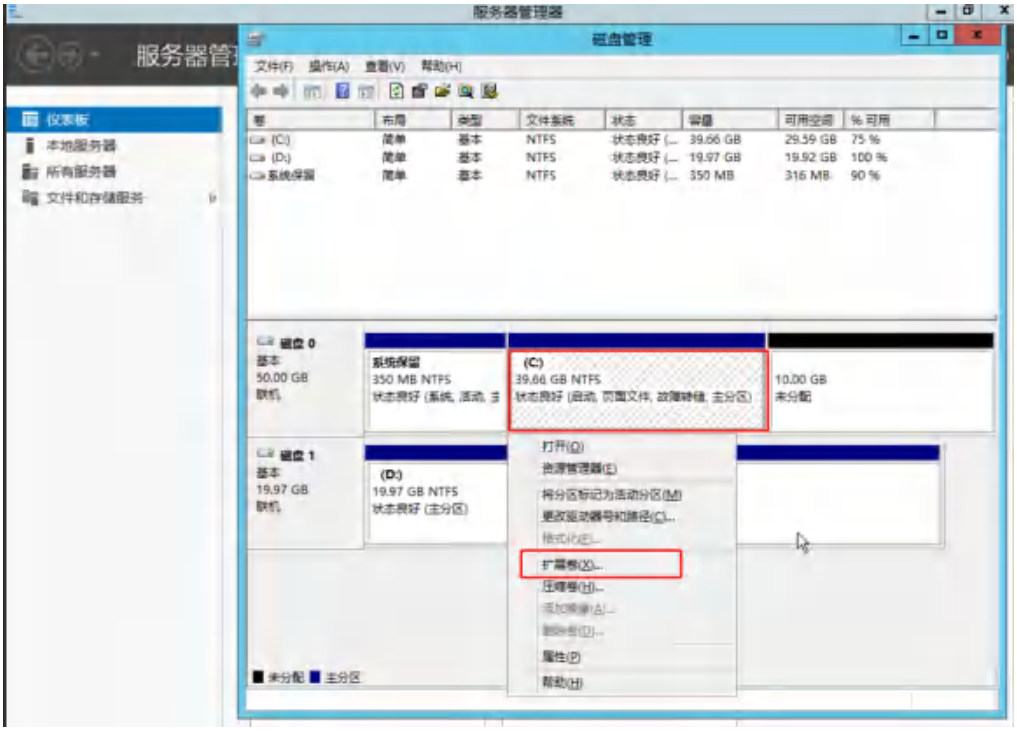
4.1.20.2 Windows 系统盘分区扩容

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：

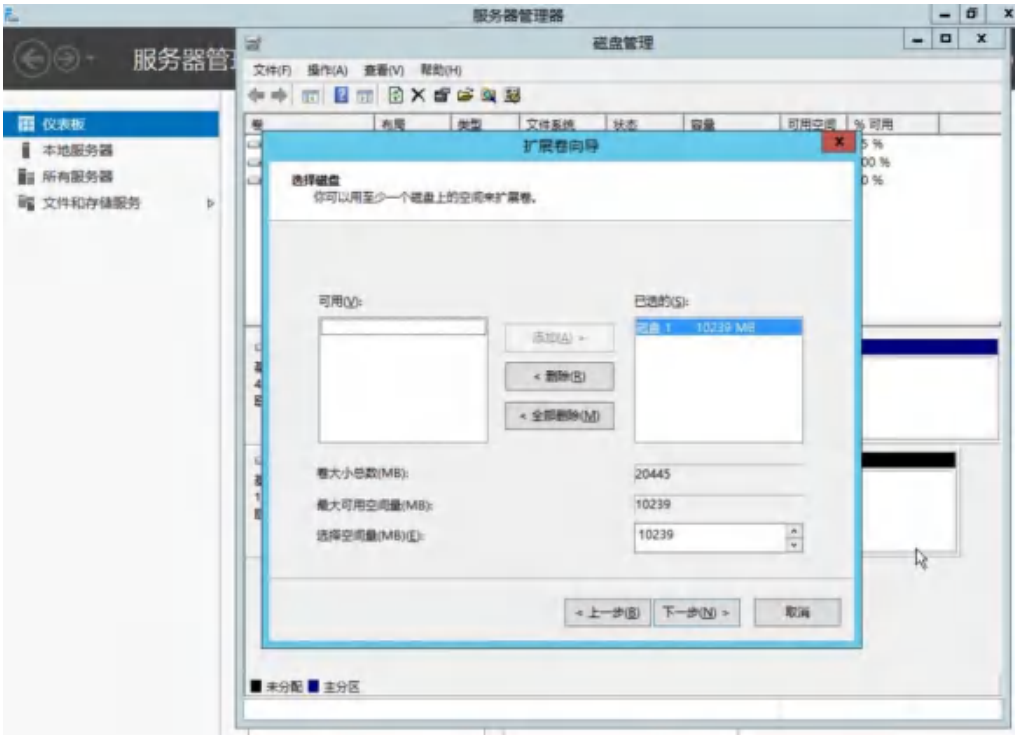
1、在磁盘管理工具中选择操作>重新扫描磁盘，用于识别新扩容的未分配空量空间，如下图 磁盘 0 中有 10GB 未分配空间；



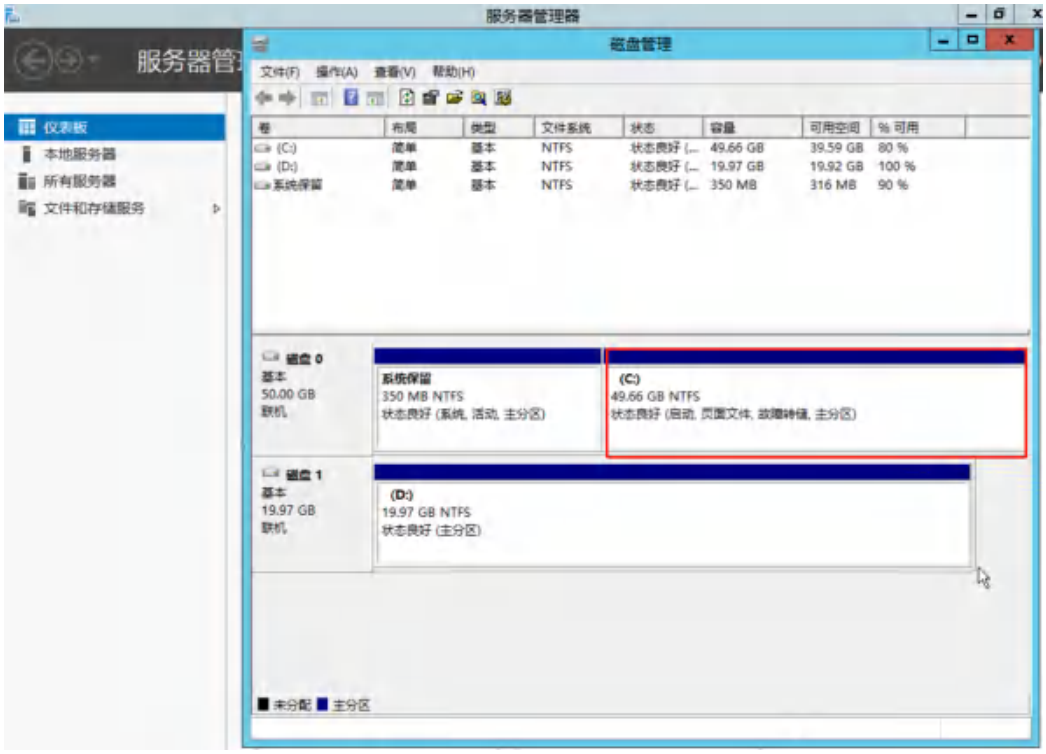
2、右键点击 C 盘，选择扩展卷，对磁盘 0 进行扩展卷操作。



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 磁盘 0 文件系统扩展成功。



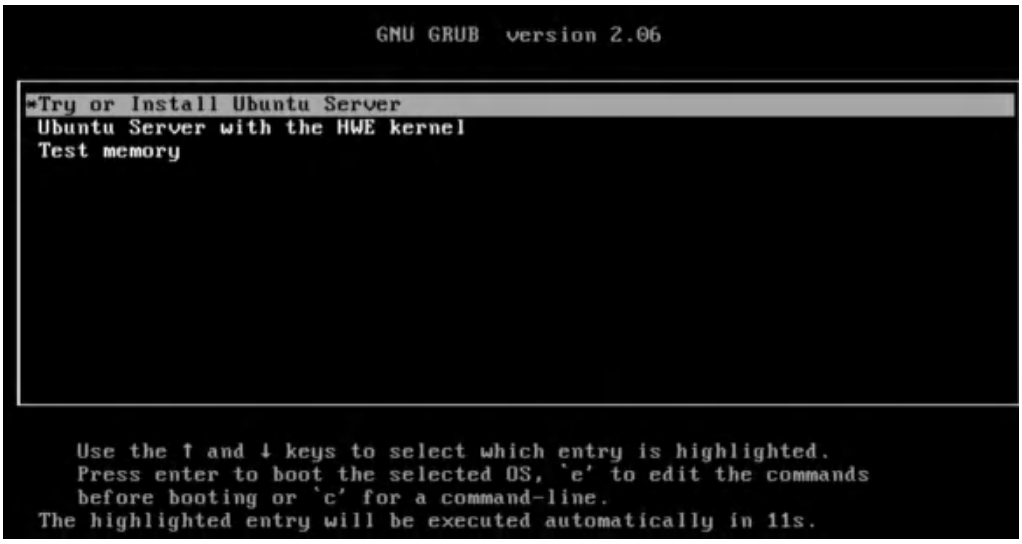
4.1.21 虚拟机 ISO 镜像

虚拟机支持用户从 ISO 镜像创建虚拟机。在虚拟机详细信息-硬盘信息-cdrom 盘中，支持虚拟机挂载、卸载 ISO 镜像、设置 ISO 镜像为引导项、取消设置 ISO 镜像为引导项。

4.1.21.1 从 ISO 镜像创建虚拟机

1.从 ISO 镜像创建虚拟机，在创建虚拟机页面上选择镜像类型为 ISO 的镜像，配置相应的虚拟机配置，然后单击创建。

2.登录控制台选择安装。

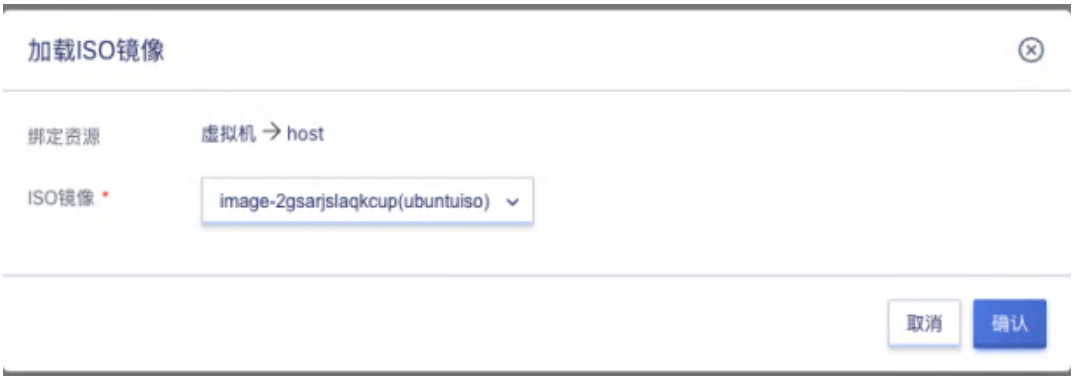


3.安装完成后取消从 ISO 引导。

4.关机然后重启虚拟机。

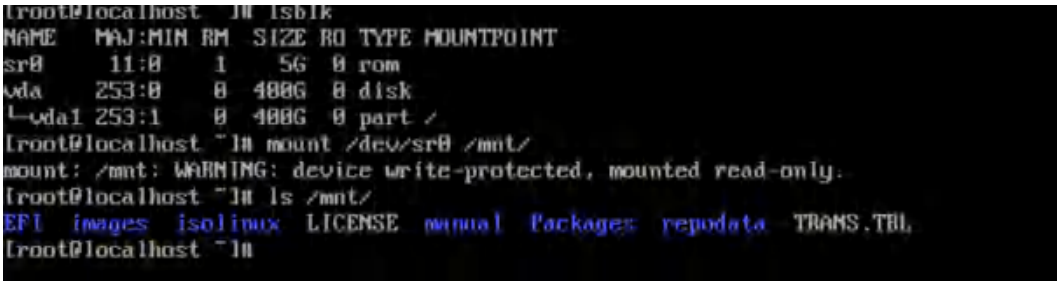
4.1.21.2 将 ISO 镜像挂载使用

1.在虚拟机详情，硬盘信息内，点击加载 ISO 镜像



2.绑定成功后，如下图所示。

3.登录到虚拟机并将/dev/sr0 挂载到/mnt 目录以查看 ISO 映像文件。

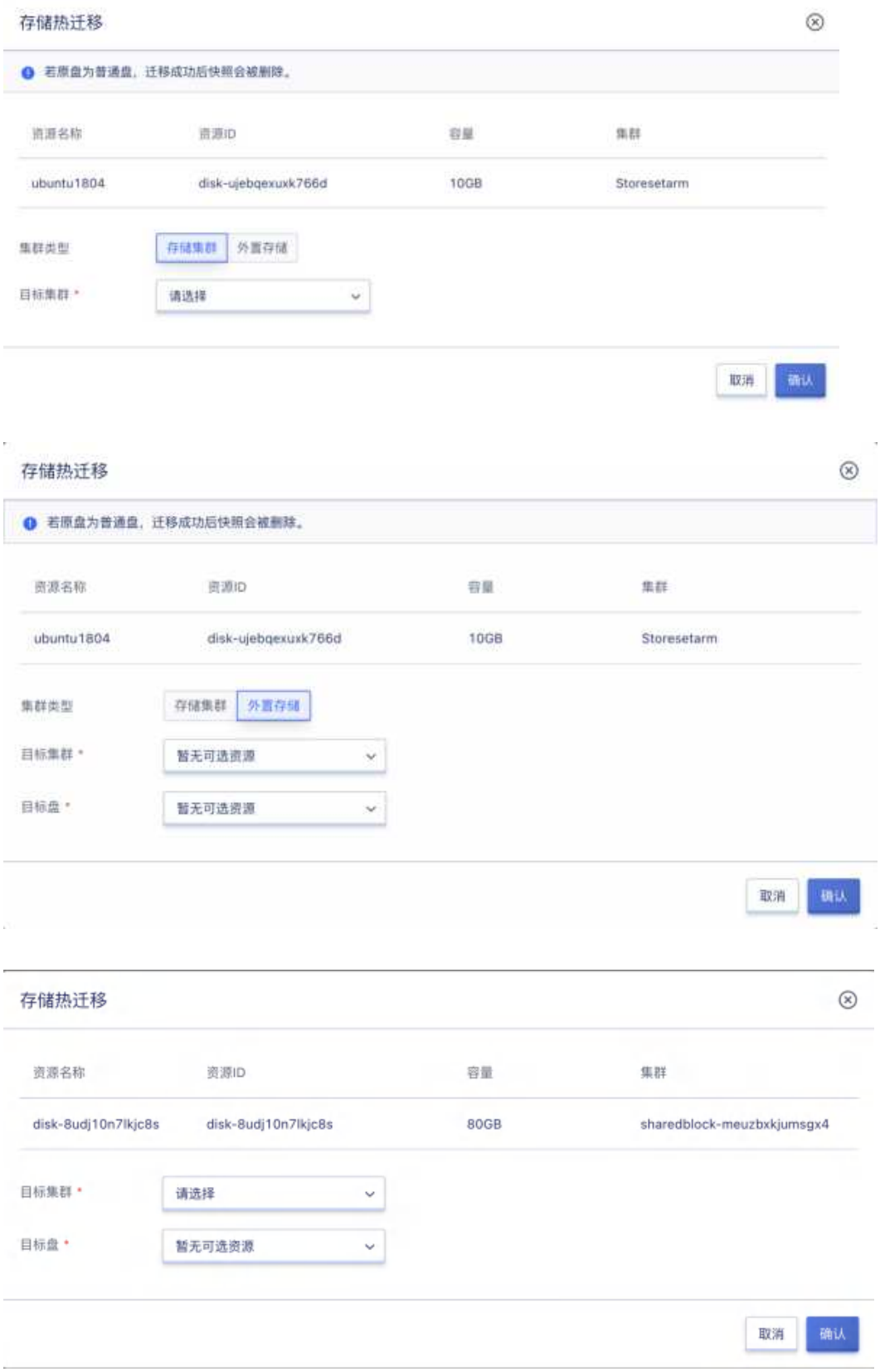


4.1.22 虚拟机存储热迁移

虚拟机存储热迁移为用户提供一种在不停机的情况下，底层存储动态更换的能力。支持虚拟机系统盘、数据盘及外置存储盘进行存储热迁移操作。

- 支持 ceph->ceph、ceph->iscsi、iscsi->ceph 的迁移场景；
- 加密盘及共享盘不支持存储热迁移；

用户可点击虚拟机详情-硬盘信息，操作磁盘的 “存储热迁移” 按钮，选择目标集群、目标盘进行存储热迁移操作。



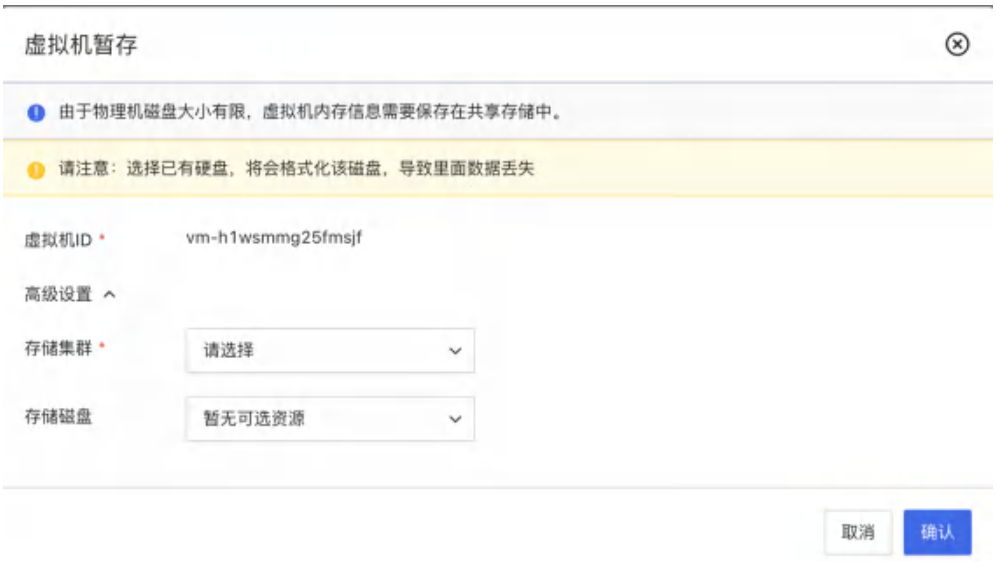
磁盘操作存储热迁移后，磁盘及磁盘所在虚拟机状态为“磁盘迁移中”。

4.1.23 虚拟机暂存

磁盘操作存储热迁移后，磁盘及磁盘所在虚拟机状态为“磁盘迁移中”

4.1.23.1 操作暂存

虚拟机支持指定存储集群和外置存储的磁盘操作暂存，不支持加密盘和共享盘，可在高级设置中选择，如下图所示：



暂存过程中，虚拟机状态为“**暂存中**”，用于暂存的磁盘与虚拟机绑定，并在虚拟机详情中临时中间盘列表展示，如下图所示：

4.1.23.2 暂存恢复

支持对状态为“**暂存**”的虚拟机操作恢复暂存，如下图所示：

4.1.23.3 暂存断电

支持对状态为“**暂存**”的虚拟机操作断电，如下图所示：

4.2 镜像管理

自制镜像以及 ISO 镜像归属于云平台租户，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，平台管理员、租户及有权限的子账号均有权限查看和管理。

自制镜像和 ISO 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。

4.2.1 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以及 ISO 镜像资源的列表及相关详细信息，包括镜像名称、资源 ID、状态、是否加密、特性支持、系统类型、操作系统及操作项，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；
- 状态：当前自制镜像的状态，包括制作中、上传中、可用、失败，删除中、已删除；
  - 制作中：通过虚拟机自制镜像过程中，镜像的状态为制作中；
  - 上传中：用户通过导入镜像功能导入镜像的过程中，镜像的状态为上传中，上传支持查看进度；
  - 失败：指用户上传镜像失败；
  - 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。
- 是否加密：表示当前镜像的加密状态；
- 特性支持：指当前自制镜像的特性支持项，如热升级、cloud-init、qemu-ga；

- 系统类型：代表当前自制镜像的操作系统类型，如 Linux、Windows、Kylin 等；
- 操作系统：指当前自制镜像的基础操作系统发行版，如 CentOS 7.4 x86_64；
- 项目组：指当前自制镜像所在的项目组信息；
- 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，中断上传及删除镜像；

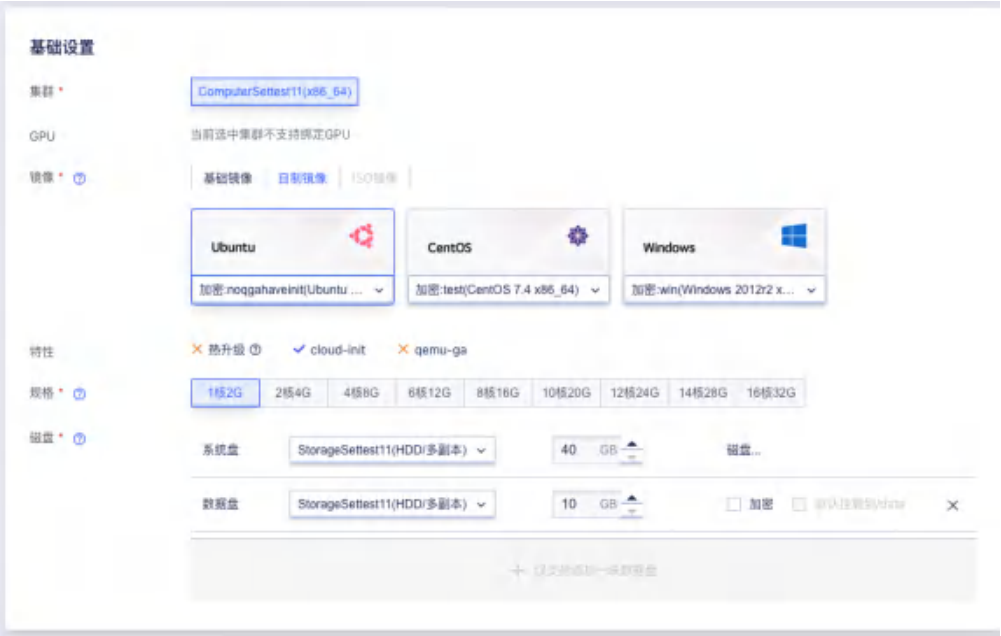
为方便租户对镜像资源进行维护和操作，平台支持下载当前用户所拥有的所有自制镜像资源列表信息为 Excel 表格，同时支持对自制镜像进行批量删除操作，可通过选中多个自制镜像，点击批量删除按钮进行批量操作。

平台支持用户导入自定义镜像，列表上为用户提供自行制作镜像文档，可通过查看文档阅读镜像制作及格式转换的操作步骤，方便镜像导入和业务迁移。

4.2.2 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“创建虚拟机”进行创建，点击后会跳转至虚拟机创建界面，如下图所示，虚拟机创建界面将根据用户选择的自制镜像或者 ISO 镜像展示目前平台所具备的镜像版本。



使用自制镜像和 ISO 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。

注：已加密镜像创建虚拟机暂不支持修改密钥。

4.2.3 导入镜像

导入镜像是指租户或平台管理员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，上传 ISO 格式镜像在 ISO 镜像管理界面上传，用户上传 VHD、VMDK、QCOW2、OVA、ISO 等格式的镜像时，需先将镜像转换为 QCOW2 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制镜像列表上展示的【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
请务必根据文档在镜像中安装初始化工具，否则镜像导入平台后会无法正常启动和管理虚拟机。
镜像名称 *
镜像备注
导入方法 *
本地文件
URL
本地文件指选择当前浏览器选择的本地文件进行上传
镜像文件 *
选择文件
请选择.qcow2文件
操作系统 *
Linux
Windows
系统架构 *
x86_64
aarch64
引导方式 *
BIOS
UEFI
系统平台 *
CentOS
系统版本 *
8.5
agent支持
cloud-init
qemu-ga
项目组 *
default
标签
+添加标签
取消
确认

- 镜像名称/描述：镜像的名称及相关描述信息；
- 导入方法：用户可以自行选择本地文件或者是 URL 导入 QCOW2 格式和 ISO 格式的镜像文件；
- 镜像文件：在选择导入方法为本地文件时，可以选择当前浏览器选择的本地文件进行上传；
- 镜像地址：在选择导入方法为 URL 时，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，平台会从提供的 URL 地址自动下载镜像并自动导入至镜像仓库，用于创建虚拟机。

- 当前仅支持 HTTP、HTTPS 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 地址或外网 IP 地址可通信的地址。

- 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；
- 引导方式：导入镜像的引导方式，支持 BIOS,UEFI;
- 系统平台：指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 x86_64 架构支持 6.5~6.10 及 7.0~7.9 版本；
  - CentOS aarch64 架构支持 7.6~7.9 版本；
  - Ubuntu x86_64 架构支持 14.04 和 20.10 版本；
  - Ubuntu aarch64 架构支持 16.04 和 18.04 版本；
  - Windows server 支持 2008 至 2019 版本；
  - Windows 支持 7 至 10 版本。
- agent 支持：仅在自制镜像导入时出现，当前导入镜像支持的特性，包括 cloud-init、qemu-ga；
- 标签：支持导入的镜像选择绑定标签。

镜像导入后，自制镜像列表生成一条状态为 “上传中” 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。导入过程中点击“取消上传”，可以中断上传。

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“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。

4.2.4 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。

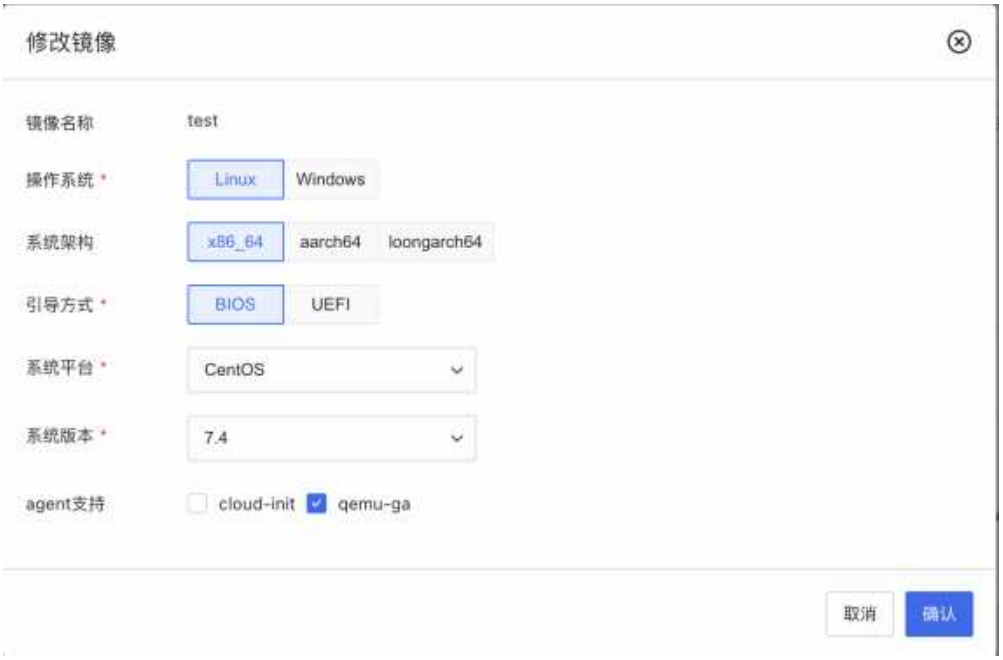
用户如果需要下载镜像至本地时，可通过自制镜像列表操作项中的【下载】进入镜像下载向导页面，如下图所示：

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。

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。

4.2.5 修改镜像

支持用户对自制镜像和 ISO 镜像操作修改，修改项包括操作系统、系统架构、引导方式、系统平台、系统版本和 agent 支持，如下图所示：



4.2.6 镜像上传列表

用户通过导入本地文件上传镜像时，在导入镜像弹框展示上传镜像进度条，如下图所示：

关闭导入镜像弹框会中断镜像上传。

4.2.6.1 断点上传

通过本地文件上传的镜像支持断点上传，如下图所示：

关闭上传列表弹框会中断镜像上传。

4.2.6.2 删除上传镜像进度

支持用户在上传列表删除镜像进度，即取消镜像上传，镜像状态变为“**上传失败**”。

4.2.7 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。

仅支持删除状态为可用或导入失败的的自制镜像；

4.2.8 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。

4.3 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，分为内网网卡和外网网卡两种类型，同时均会从所属网络中分配 IP 地址、网关、子网掩码及路由相关网络信息。

- 内网类型的弹性网卡所属网络为 VPC 和子网，同时从 VPC 中自动或手动分配 IP 地址。
- 外网类型的弹性网卡所属网络为外网网段，同时会从外网网段中自动或

手动分配 IP 地址，且分配的 IP 地址与弹性网卡生命周期一致，仅支持随弹性网卡销毁而释放。

- 当网卡类型为外网时，网卡会根据所选外网 IP 的带宽规格进行计费，用户可根据业务需要，选择适合的付费方式和购买时长。

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，x86 架构虚拟机最多支持绑定 6 块弹性网卡，ARM 架构虚拟机最多支持绑定 3 块网卡。

外网弹性网卡被绑定至虚拟机后，不影响虚拟机默认网络出口策略，包含虚拟机上弹性网卡绑定的外网 IP 在内，以第一个有默认路由的 IP 作为虚拟机的默认网络出口，用户可设置某一个有默认路由的外网 IP 为虚拟机默认网络出口。

每块弹性网卡仅支持分配一个 IP 地址，并可根据需要绑定一个安全组，用于控制进出弹性网卡的流量，实现精细化网络安全管控；如无需对弹性网卡的流量进行管控，可将弹性网卡的安全组置空。

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，对于外网弹性网卡还可进行【调整带宽】操作，用于调整外网弹性网卡上的外网 IP 地址的带宽上限。

4.3.1 创建弹性网卡

云平台用户可通过 API 接口或控制台创建一块弹性网卡，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 网络和子网或外网网段。通过导航栏进入虚拟机控制台，切换至【弹性网卡】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，如下分别是创建内网类型和外网类型的示意图：

- 名称：当前需要创建弹性网卡的名称及标识；
- 网卡类型：弹性网卡的类型，包括内网网卡和外网网卡，分别从 VPC 和外网网段中分配 IP 地址。
- 所属网络：弹性网卡的所属网络，创建时必须指定。
  - 内网类型的弹性网卡所属网络为 VPC 和子网，同时从 VPC 中自动或手动分配 IP 地址，创建时需指定可用 IP 数量充足的子网。
  - 外网类型的弹性网卡所属网络为外网网段，同时会从外网网段中自动或手动分配 IP 地址，创建时需指定可用 IP 数量充足的外网网段，并配置外网 IP 地址的带宽上限。
- IP 地址：当前网卡的 IP 地址，默认会从所属网络的 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。

若手动指定的 IP 地址已被使用，则会弹出占用提示。

- 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/外网安全组互不影响，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。

创建外网弹性网卡时，会根据外网 IP 的带宽规格进行计费，用户可根据需要选择适合的付费方式和购买时长。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。

4.3.2 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、状态、网卡类型、所属网络、IP 地址、绑定资源、安全组、项目组、创建时间及操作项等，如下图所示：

- 名称/资源 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，包括内网网卡和外网网卡两种类型，分别对应 VPC 网络和外网网络。
- 所属网络：弹性网卡的所属网络，内网类型时所属网络为指定的 VPC 和子网，外网类型时所属网络为指定的外网网络和网段。
- IP 地址：当前弹性网卡从所属网络中分配的 IP 地址，同时也是绑定至虚拟机后弹性网卡上所配置的 IP 地址；若弹性网卡为外网类型，在 IP 地

址后会展示该 IP 地址的带宽上限。

- 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。
- 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。
- 项目组：当前弹性网卡的项目组信息。
- 状态：弹性网卡的当前状态，包括创建中、未绑定、已绑定、删除中等状态。

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、调整带宽及删除等，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。

4.3.3 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：

绑定时需选择需要绑定网卡的虚拟机，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。绑定成功后，虚拟机的操作系统中即会增加一块网卡，并配置弹性网卡上所分配的 IP 地址及相关信息，同时会在操作系统中下发所属网络的路由信息。

场景举例：一个虚拟机默认无默认网络出口，为虚拟机绑定一个外网类型且有默认路由的弹性网卡后，由于该网卡上的外网 IP 成为虚拟机第一个有默认路由的外网 IP ，系统会自动在虚拟机中下发默认路由，虚拟机中的所有请求默认将以弹性网卡作为默认网络出口。

4.3.4 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：

解绑时，虚拟机的状态必须处于关机或运行状态。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。

解绑成功后，虚拟机的操作系统中原有的弹性网卡信息将会自动被清除，若解绑前弹性网卡为当前虚拟机的默认网络出口，解绑后虚拟机将会从虚拟机已绑定的外网 IP 中自动选择一个有默认路由的外网 IP 作为虚拟机的默认网络出口。

4.3.5 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“无安全组”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“无安全组“解绑已绑定的安全组。

4.3.6 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。

4.3.7 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。

4.3.8 调整带宽

支持用户调整外网弹性网卡的 IP 带宽，可通过弹性网卡列表操作项中的【调整带宽】进行操作，如下图所示：

仅支持外网类型的弹性网卡进行带宽调整操作，同时会根据 IP 带宽进行计费，需确保账户余额充足。

4.4 隔离组

4.4.1 概述

隔离组是一种针对虚拟机资源的简单编排策略，支持组内或组之间的实例分散到不同物理机上，用以保障业务的高可用。节点隔离组，支持设置虚拟机和节点的亲和，反亲和策略，是管理员独有的隔离组策略。

4.4.2 创建隔离组

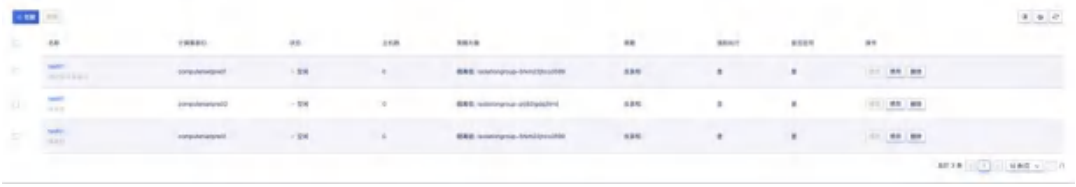
在平台控制台上，用户可通过指定名称、集群、策略对象及是否强制执行创建隔离组,隔离组默认启用，如下图所示：

- 名称：隔离组的名称。
- 备注：隔离组的备注信息。
- 集群：隔离组所属的计算集群。
- 策略对象类型：虚拟机组。
- 策略对象：目前隔离组支持指定隔离策略对象为组内或组间，组内隔离即同组内虚拟机根据策略调度，组间即为两组隔离组之间的虚拟机根据策略调度。
- 策略：目前隔离组支持亲和以及反亲和策略。
- 强制执行：强制执行开启后，如果节点不能满足虚拟机调度策略，虚拟机实例将会一直处于调度中状态，直到调度策略条件满足。

- 是否启用：是否启用隔离组，默认启用。

4.4.3 查看隔离组

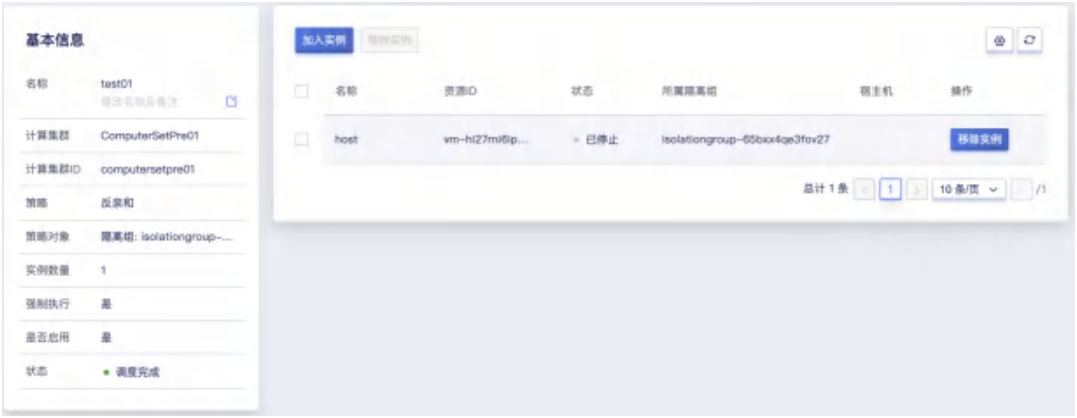
通过导航栏进入隔离组页面可查看当前账户下隔离组资源的列表及相关详细信息，包括隔离组名称、资源 ID、计算集群 ID、状态、主机数、策略对象、策略、是否强制执行、是否启用、创建时间及操作项，如下图所示：



- 隔离组名称：当前隔离组名称。
- 资源 ID：隔离组唯一 ID 标识。
- 计算集群 ID：隔离组所属计算集群的 ID（隔离组的调度隔离粒度在一个集群 ID 下打散）。
- 状态：隔离组的状态，包括完成（隔离组内除关机断电外的所有虚拟机调度完成），调度中（隔离组内有虚拟机未调度完成），删除中。
- 主机数：隔离组下虚拟机数量。
- 策略对象：目前隔离组支持指定隔离策略对象为组内或组间，组内隔离即同组内虚拟机互斥调度，组间即为两组隔离组之间的虚拟机成组互斥调度。
- 策略：目前隔离组支持亲和以及反亲和策略。
- 是否强制执行：强制执行开启后，如果节点不能满足虚拟机调度策略，虚拟机实例将会一直处于调度中状态，直到调度策略条件满足。
- 启用：是否启用隔离组。
- 创建时间：隔离组的创建时间。
- 操作项：对隔离组的修改，禁用，删除。

4.4.4 查看隔离组详情

通过隔离组名称进入隔离组详情页面可查看当前隔离组下的基本信息和实例信息，如下图所示：



（1）基本信息

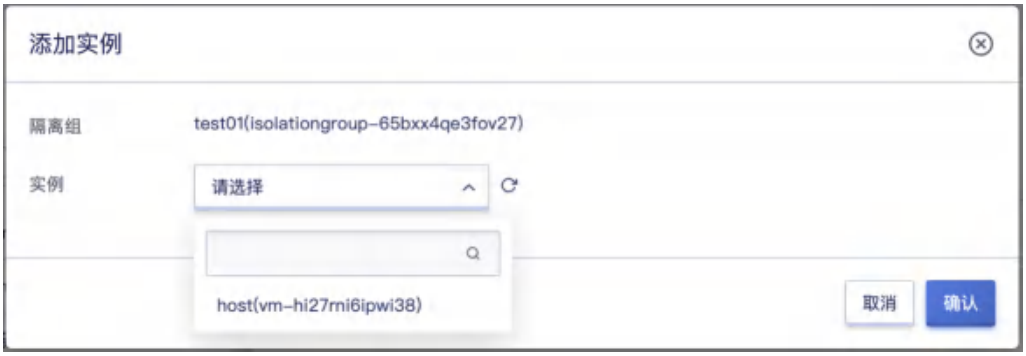
隔离组的基本信息，包括名称、计算集群、计算集群 ID、策略、策略对象、实例数量、强制执行、是否启用、状态。

（2）实例信息

隔离组详情页展示当前隔离组下的实例列表，包括名称、资源 ID、状态、所属隔离组、节点及操作。

4.4.5 加入实例

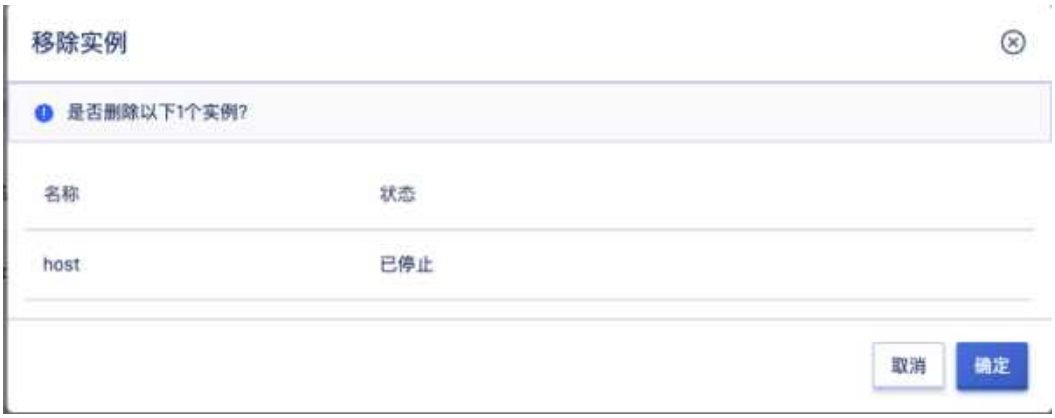
支持将关机/断电状态下且与隔离组所属计算集群一致的的虚拟机加入隔离组，如下图所示：



- 隔离组：隔离组名称和 ID。
- 实例：可加入的实例。

4.4.6 移除实例

支持将隔离组下的实例移除，如下图所示：



- 名称：实例名称。
- 状态：实例电源状态。

4.4.7 启用隔离组

隔离组为禁用状态且已绑定策略对象时，可操作启用隔离组。

4.4.8 禁用隔离组

隔离组为启用状态时，可操作禁用隔离组。禁用隔离组时，隔离组内实例会被移除，且不允许操作加入实例。

4.4.9 修改隔离组

隔离组状态为禁用时，可操作修改隔离组内容。支持修改策略对象和是否强制执行，如下图所示：

4.4.10 删除隔离组

支持用户操作删除隔离组，隔离组状态为空闲时，可操作删除。隔离组状态为调度中/调度完成，需先操作禁用隔离组，然后操作删除。如下图所示：

4.4.11 节点隔离组

4.4.11.1 创建节点隔离组

管理员支持创建节点隔离组，策略对象类型为节点组，支持亲和，反亲和策略。创建节点组启用强制执行可能会导致虚拟机无法调度。

4.4.11.2 加入和移除实例

管理员支持在节点隔离组中加入/移除虚拟机实例，管理员支持为租户创建虚拟机时选择节点隔离组。处于关机或断电状态的虚拟机实例可以加入到隔离组中。

4.4.11.3 加入和移除目的节点

管理员支持将处于可用状态的节点加入到目的节点组中或者从节点组中移除目的节点。

4.5 裸金属

4.5.1 产品概述

裸金属为用户提供统一纳管存量裸金属能力的服务，用户在控制台即可对已纳管的裸金属进行电源管理、访问远程控制台和查看硬件监控等基础运维操作。

4.5.2 使用流程

在使用裸金属服务前，必须提前准备好裸金属设备，并根据需求将裸金属服务器的 IPMI 网络及业务网络与平台网络进行打通，在通过平台录入设备信息，将设备添加给租户管理。裸金属服务的使用流程分为【平台管理员流程】和【租户流程】两大部分，具体如下：

1. 硬件环境装备

准备好硬件环境，配置物理网络交换机及服务器 IPMI 网络，使平台物理网络与 IPMI 网络可互相通信。

2. 为租户添加裸金属

由【平台管理员】为租户添加裸金属信息，包括服务器的名称、IPMI IP、IPMI User、IPMI PassWord、机架位置、标签及租户邮箱，支持批量导入裸金属信息。

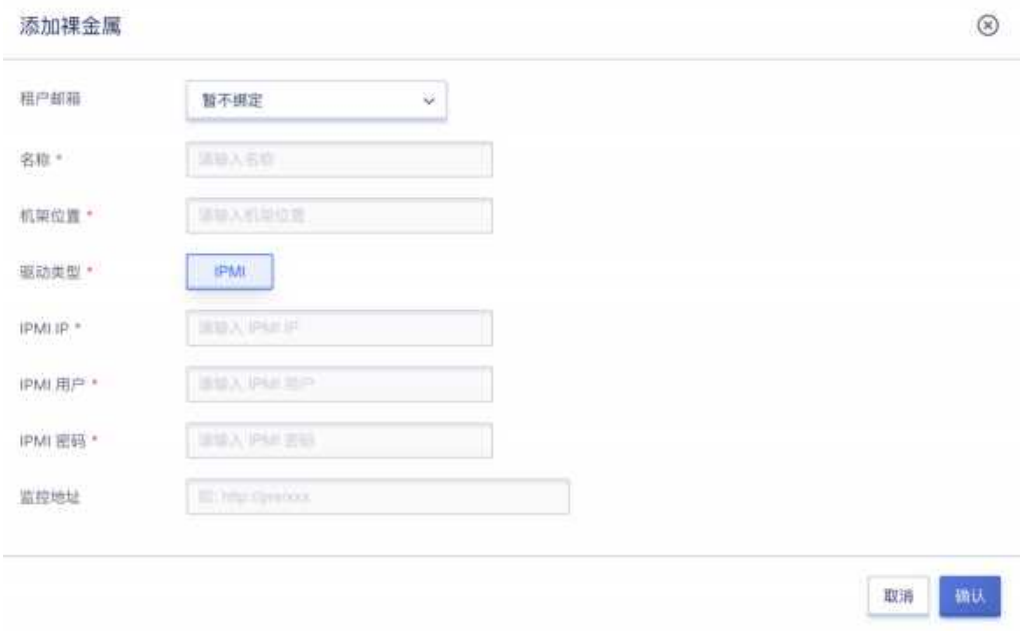
3. 裸金属管理

由【平台租户】对已申请的裸金属进行生命周期管理，支持开启、关机、重启、准备控制台、控制台登录、释放控制台、装机、重装、强制关机及关机并重新开机。

平台租户在使用裸金属服务的前提是裸金属准备好并添加给租户，租户在控制台即可对已纳管的裸金属进行电源管理、访问远程控制台和查看硬件监控等基础运维操作。

4.5.3 添加裸金属

在平台已提供裸金属服务时，租户的主账号和子账号可在平台上直接单独添加或批量导入裸金属进行管理。用户可登录控制台，通过控制台导航栏【裸金属】中的添加裸金属操作进入向导页面，如下图所示：



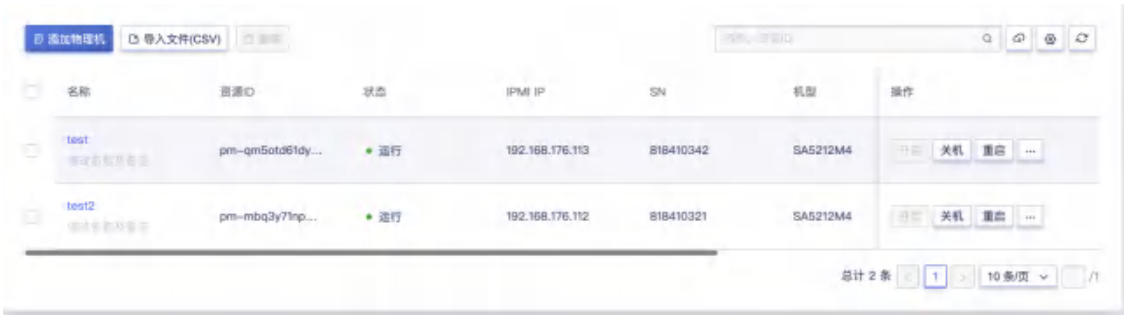
- 租户邮箱：裸金属仅可通过租户管理员添加，指定所需用户。
- 名称：指裸金属在平台的名称标识，添加时必须指定。
- 机架位置：裸金属所处的机架位置，添加时必须指定。驱动类型：默认 IPMI。
- IPMI IP：指裸金属的 IPMI IP 地址，添加时必须指定，IP 地址必须从平台可达
- IPMI 用户：裸金属的 IPMI 用户名，添加时必须指定。
- IPMI 密码：裸金属的 IPMI 密码，添加时必须指定。
- 标签：裸金属的标签。
- 监控地址：支持添加纳管的物理机的 node_exporter 地址获取监控信息。

租户添加提交后列表将生成一条【资源准备中】的裸金属信息，待添加成功

后，会置为【运行】状态，此时租户可对裸金属进行管理。

4.5.4 查看裸金属

租户的管理员可通过裸金属列表及详情查看账号下已添加的裸金属信息及当前状态，如下图所示：



- 名称/资源 ID：裸金属的名称和全局资源唯一标识符。
- SN：裸金属的整机序列号。
- IPMI IP：裸金属的 IP 地址。
- 机型：裸金属的机型。
- 机架位置：裸金属所处的机架位置。
- 电源：裸金属的电源状态，如开启、关机中、关机等。
- KVM 状态：裸金属控制台的状态，如未准备、准备中、就绪等。
- 创建时间：裸金属的添加时间。
- 状态：当前裸金属的资源状态，如运行、资源准备中等，裸金属首次添加时，状态为纳管。

列表上的操作项中可对单台裸金属进行开启、关机、重启、VNC 登录、准备控制台、控制台登录、释放控制台、强制关机、关机并重新开机、更新裸金属及删除等操作，支持批量删除裸金属，其中删除后租户可重新进行添加。

租户也可通过访问列表上裸金属的名称进入裸金属的详情页面，查看裸金属的详细信息，包括基本信息和配置信息：

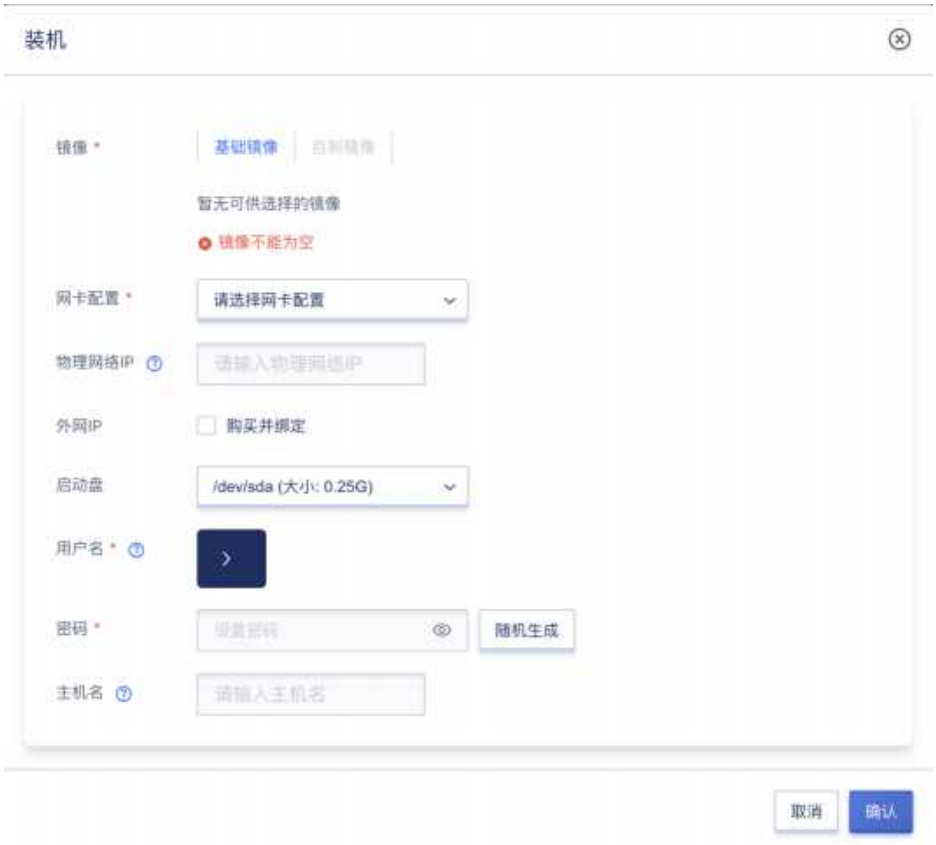
- 基本信息包括：裸金属的名称、ID、IPMI IP、SN 序列号及电源状态。
- 配置信息包括：裸金属的 CPU 信息、内存信息及 PCIE 信息等。

4.5.5 分配裸金属

租户管理员可对已上架裸金属进行分配操作，如下图所示：

4.5.6 裸金属装机

租户、管理员可对已上架裸金属进行装机操作，如下图所示：



装机所用的镜像格式为 qcow2，需要支持 cloud-init 特性。

4.5.7 裸金属开机/关机

平台支持租户对已添加的裸金属进行关机、开启、重启、强制关机、关机并重新开机操作，用于维护和管理裸金属的生命周期。电源状态为开启时，才可执行关机、重启、强制关机、关机并重新开机操作；电源状态为关闭时，才可执行开启操作。

裸金属开启过程中，裸金属的电源状态为开机中，待开机成功后流转为开启；当用户触发关机时，裸金属的状态为关机中，待关机成功后流转为关闭。

4.5.8 裸金属控制台操作

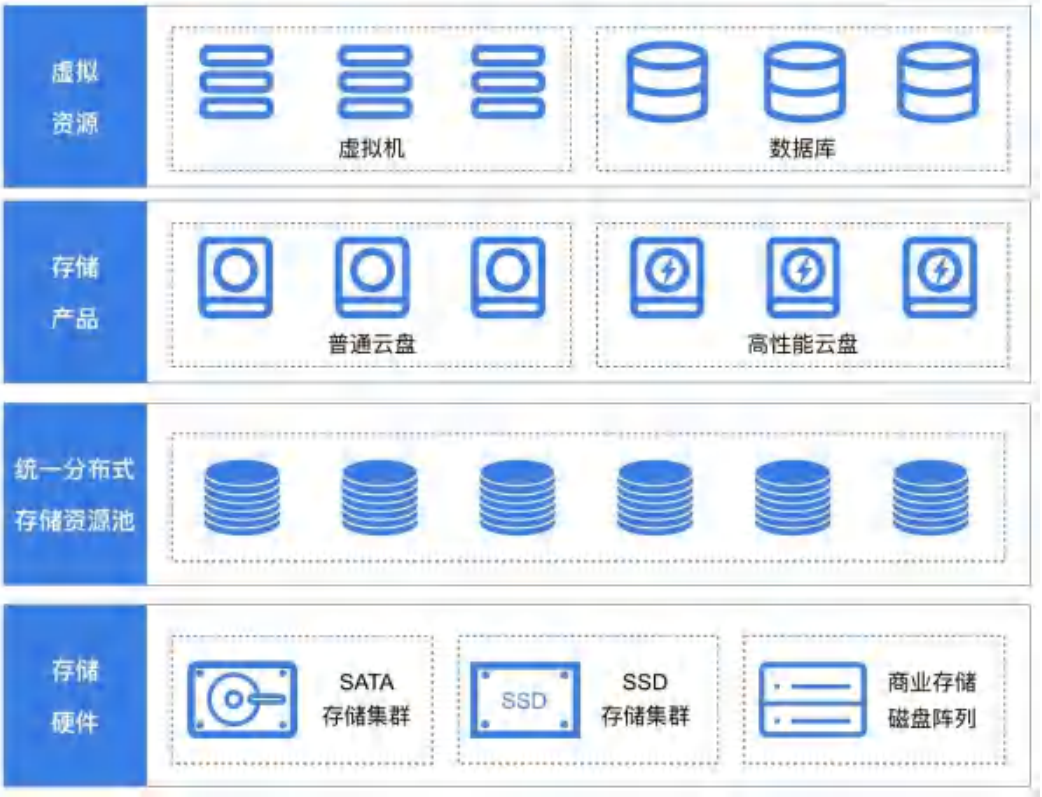
租户可在控制台对已纳管的裸金属进行电源管理、访问远程控制台和查看硬件监控等基础运维操作。裸金属 KVM 状态为未准备时，需执行准备控制台操作，执行完毕后，KVM 状态流转为就绪；裸金属 KVM 状态为就绪时，支持控制台登录和释放控制台。

5 存储服务

5.1 云硬盘

5.1.1 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像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像为【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始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 1GB，可自定义控制单块云硬盘的最大容量，最大支持 32000GB；
- 具有独立的生命周期，可自由绑定至任意虚拟机，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 25 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；
- 支持从快照创建云硬盘，创建的硬盘大小与快照的原始硬盘大小相等，从快照创建云硬盘，该云硬盘只能与快照所对应的原始云硬盘归属同一存储集群，可以用系统盘快照创建的云硬盘创建虚拟机；
- 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。

5.1.2 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、硬盘密钥等参数。

- 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 1GB，最大支持 32000GB，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；
- 硬盘密钥：输入密钥后该硬盘将加密；

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：选择需要创建的云硬盘数量，一次最多支持批量创建 10 块相同规格的云硬盘。
- 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”。

5.1.3 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、状态、集群类型、硬盘容量、绑定资源、计费方式、创建时间、过期时间、项目组及操作项，如下图所示：

- 名称/ID：云硬盘的名称和全局唯一标识符；
- 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、正在被克隆中、及删除中等，其中正在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。
- 是否加密：磁盘的加密状态；
- 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；
- 项目组：当前云硬盘的项目组信息；

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。

5.1.4 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 25 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。

5.1.5 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。

注：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。

5.1.6 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。

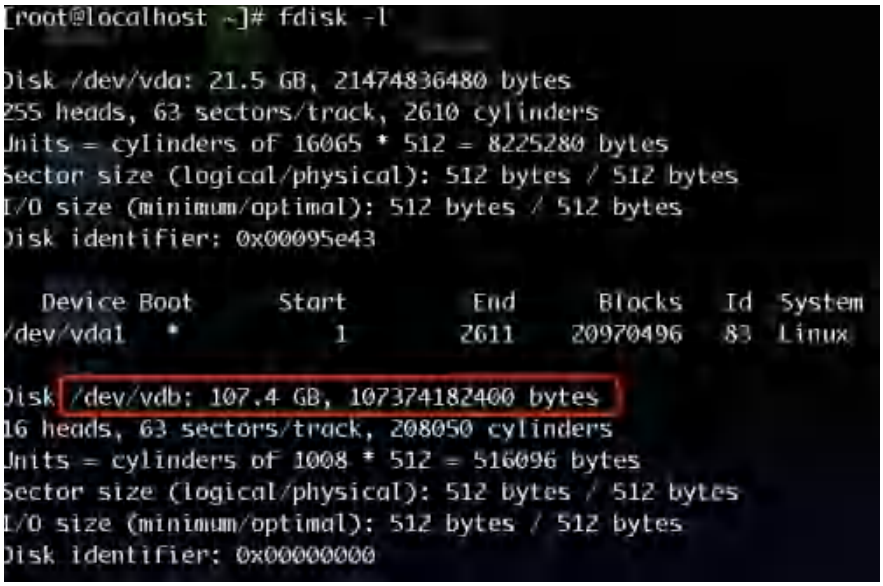
格式化和分区磁盘具有一定的风险，格式化后云硬盘中的数据将被清空，请慎重操作。

5.1.6.1 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；



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；

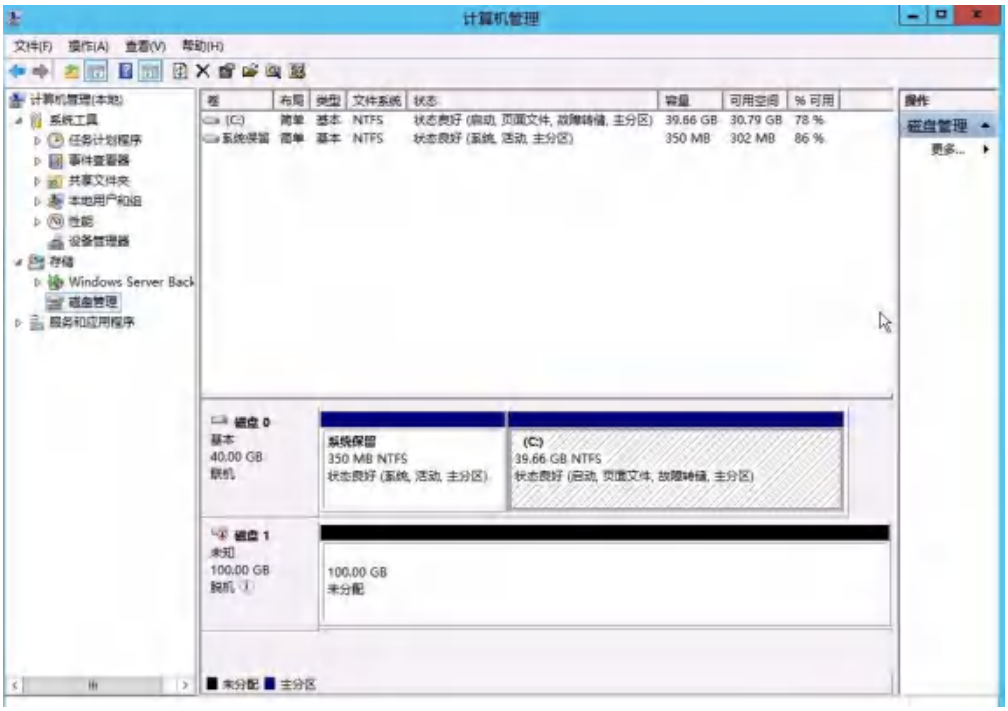
7. 若云硬盘在控制台被解绑，重新绑定至其它 Linux 虚拟机后，需要按照第 4~5 步骤执行挂载操作。

5.1.6.2 Windows 虚拟机

Windwos 虚拟机挂载云硬盘后，需要进行初始化和格式化分区操作，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：

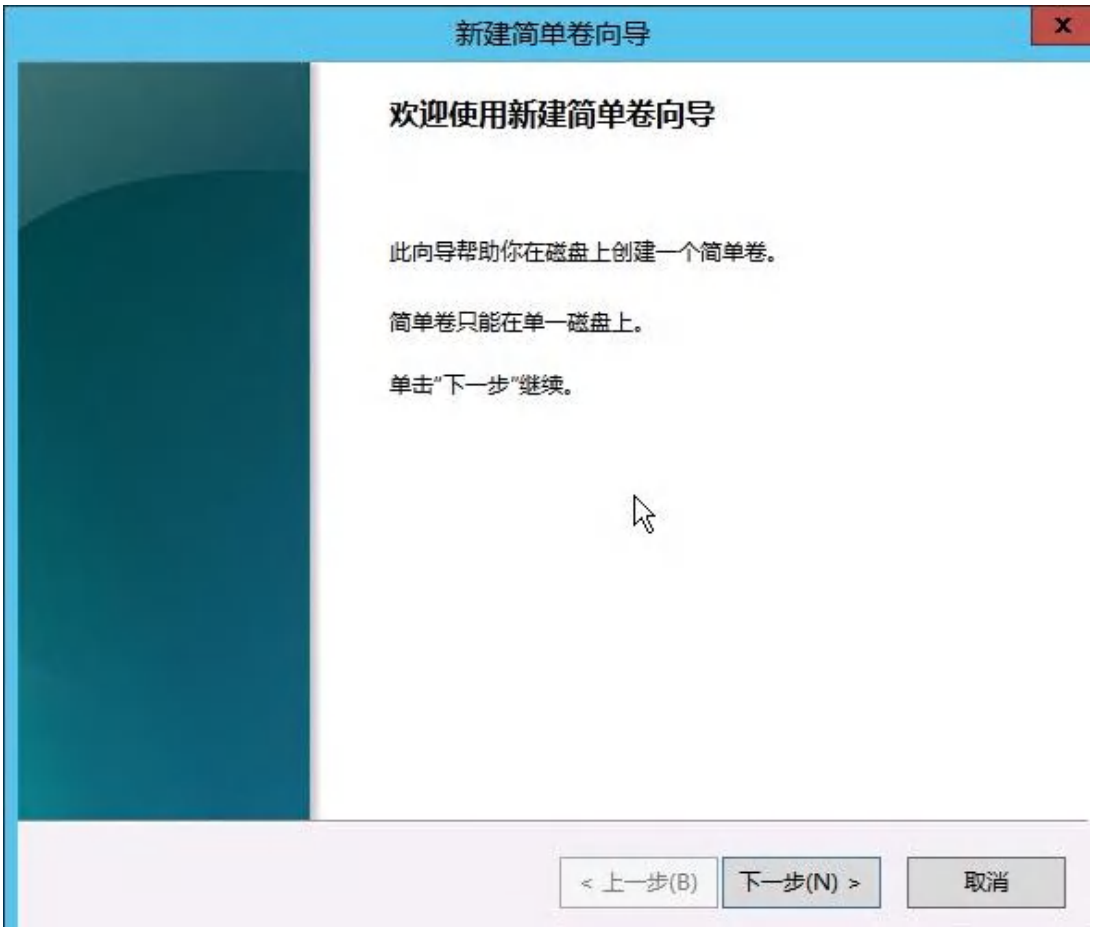
5. 根据分区形式的不同，选择【GPT】或【MBR】，单击【确定】按钮；

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。

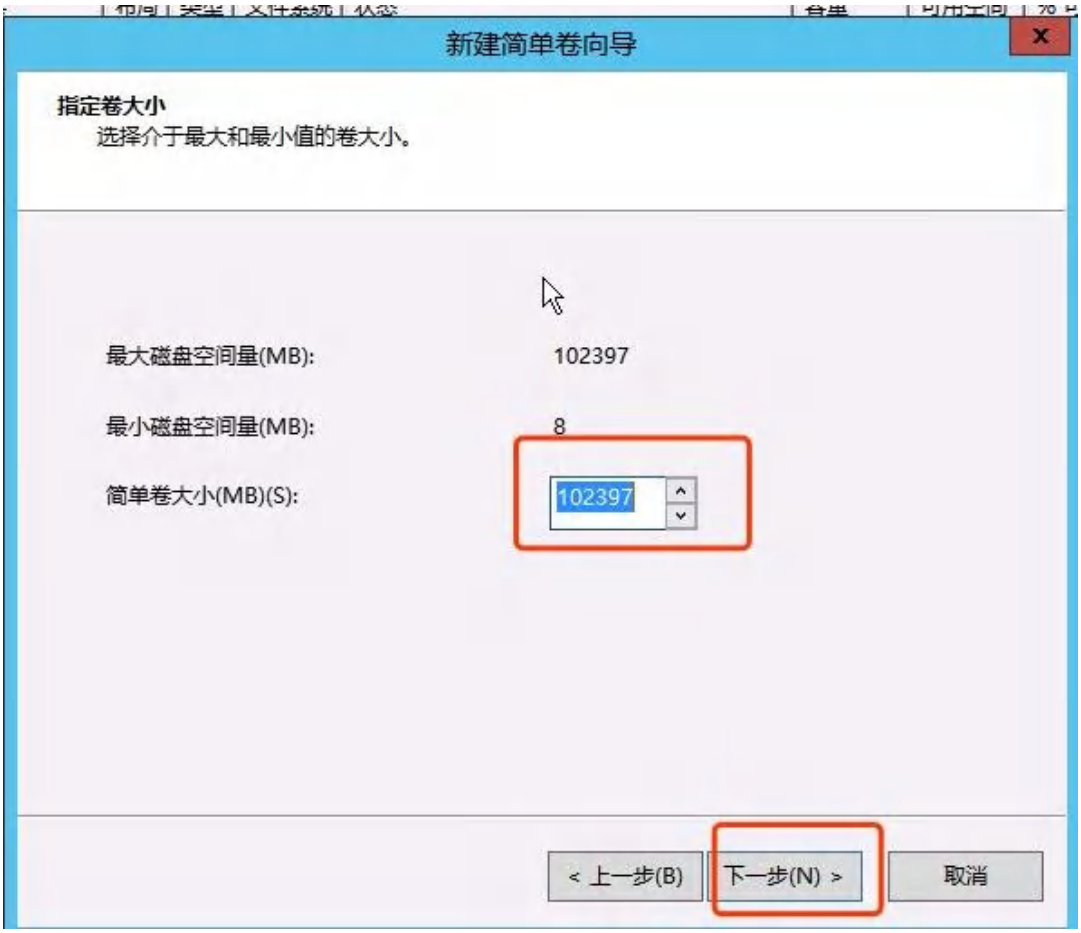
GPT 是一种新的分区形式，早期版本的 Windows 不能识别这种分区形式。GPT 能处理的数据盘容量由操作系统和文件系统决定。在 Windows 操作系统

里，GPT 最多可以支持 128 个主分区。

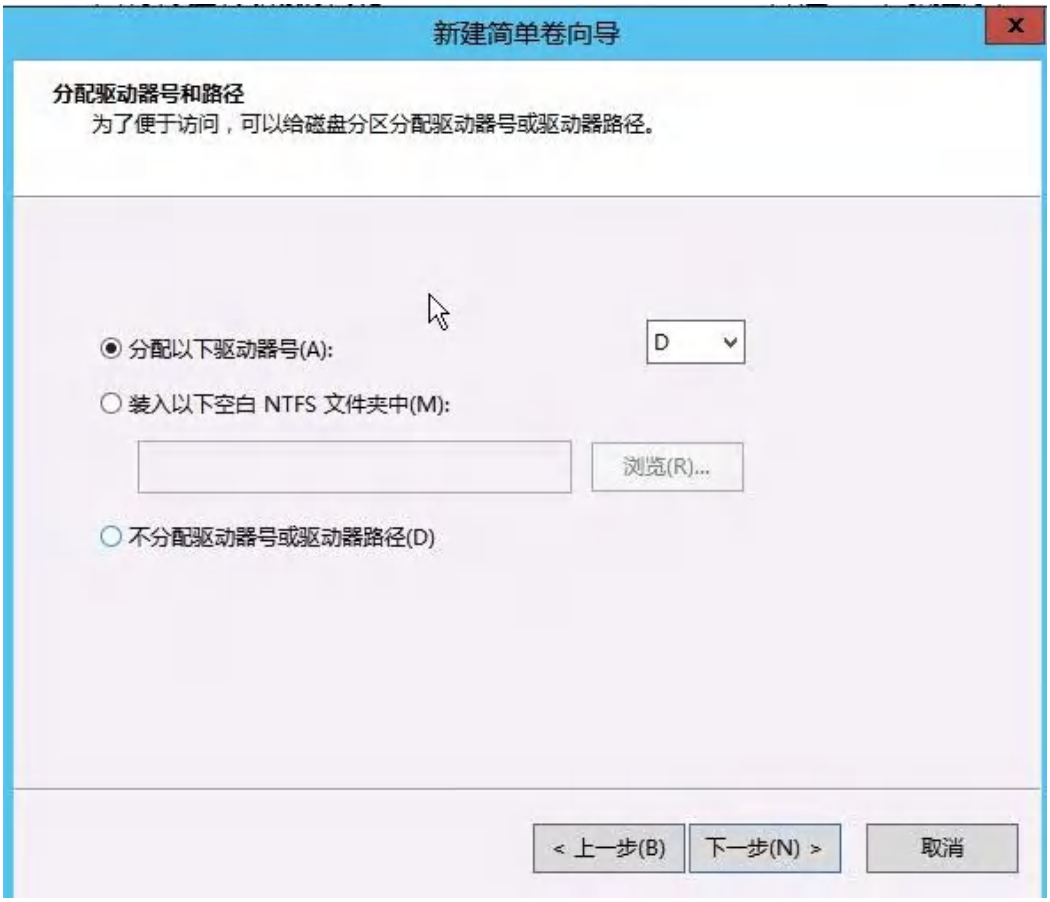
6. 磁盘分区，右键点击磁盘 1 右侧【未分配】的区域，选择【新建简单卷】，进入新建简单卷向导，如下图：



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；



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：

5.1.7 扩容云硬盘

5.1.7.1 扩容云硬盘容量

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~32000GB ，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。

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。

注意：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【磁盘分区扩容】。

5.1.7.2 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）

5.1.7.2.1 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。

1. 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   Size  Used Avail Use% Mounted on
/dev/vda1      ext4    40G  822M   37G   3% /
tmpfs          tmpfs  935M     0  935M   0% /dev/shm
/dev/vdb       ext4    40G  176M   38G   1% /data
[root@localhost data]#
[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 /
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。

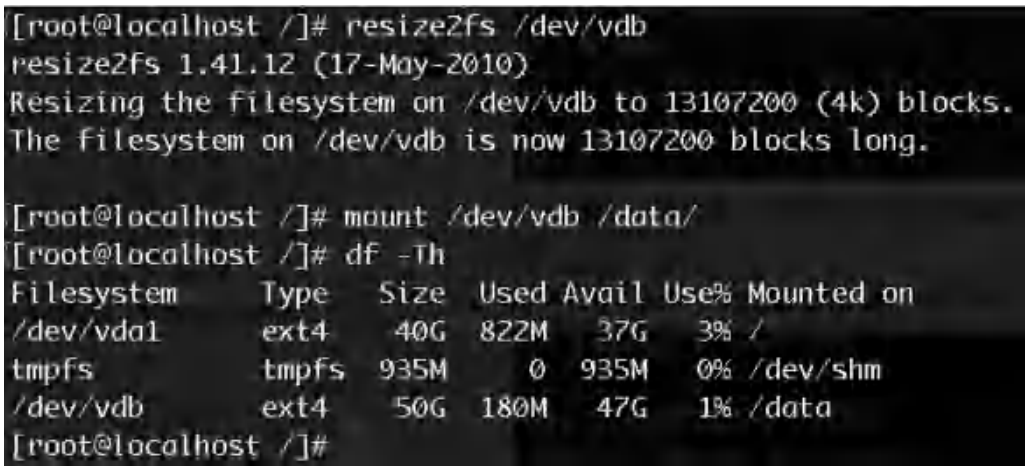
2. 通过控制台或 API 对硬盘进行容量扩容操作，并在操作系统中查看磁盘的容量，如下图所示，扩容至 50GB；

```
[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
```

3. 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；

4. 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；



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。

5. 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。

5.1.7.2.2 单分区扩容（Linux）

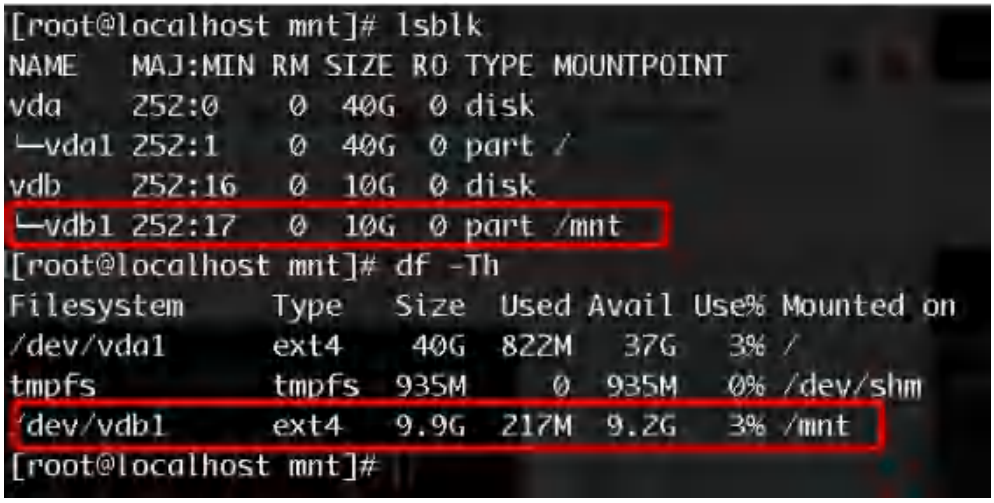
单分区磁盘是指云盘在扩容之前已被挂载过虚拟机且只划分过 1 个分区，用户可通过对硬盘扩容容量后，进入操作系统对单分区磁盘进行分区扩容操作。单分区扩容在 Linux 及 Windows 操作系统上的操作不同，本章节为 Linux 单分区扩容操作指南。

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。

注意：本操作示例默认磁盘容量小于 2TB，若磁盘容量大于 2TB 请参考章节。

1. 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；



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。

2. 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；

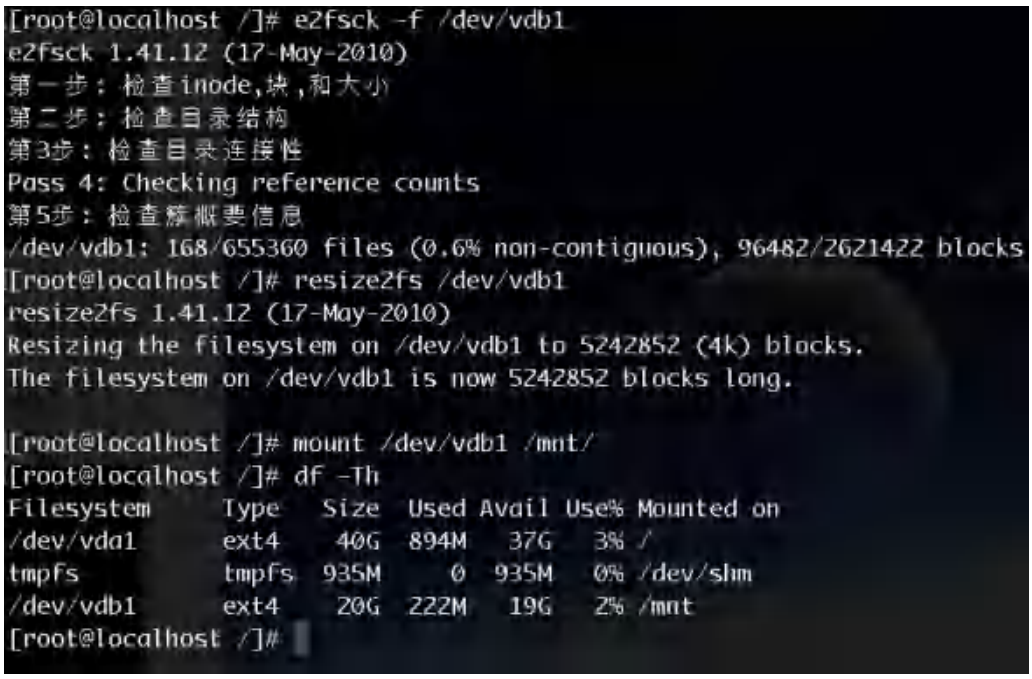
3. 在操作系统中 umount 磁盘，使用 fdisk/dev/vdb 命令删除原来的分区并创建新分区；


```
[root@localhost /]# fdisk /dev/vdb

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): d
Selected partition 1

Command (m for help): n
Command action
   e   extended
   p   primary partition (1-4)
p
Partition number (1-4): 1
First cylinder (1-41610, default 1):
Using default value 1
Last cylinder, +cylinders or +size{K,M,G} (1-41610, default 41610):
Using default value 41610

Command (m for help): p

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

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

Calling ioctl() to re-read partition table.
Syncing disks.
[root@localhost /]#
```

注：删除分区不会造成磁盘内数据丢失。

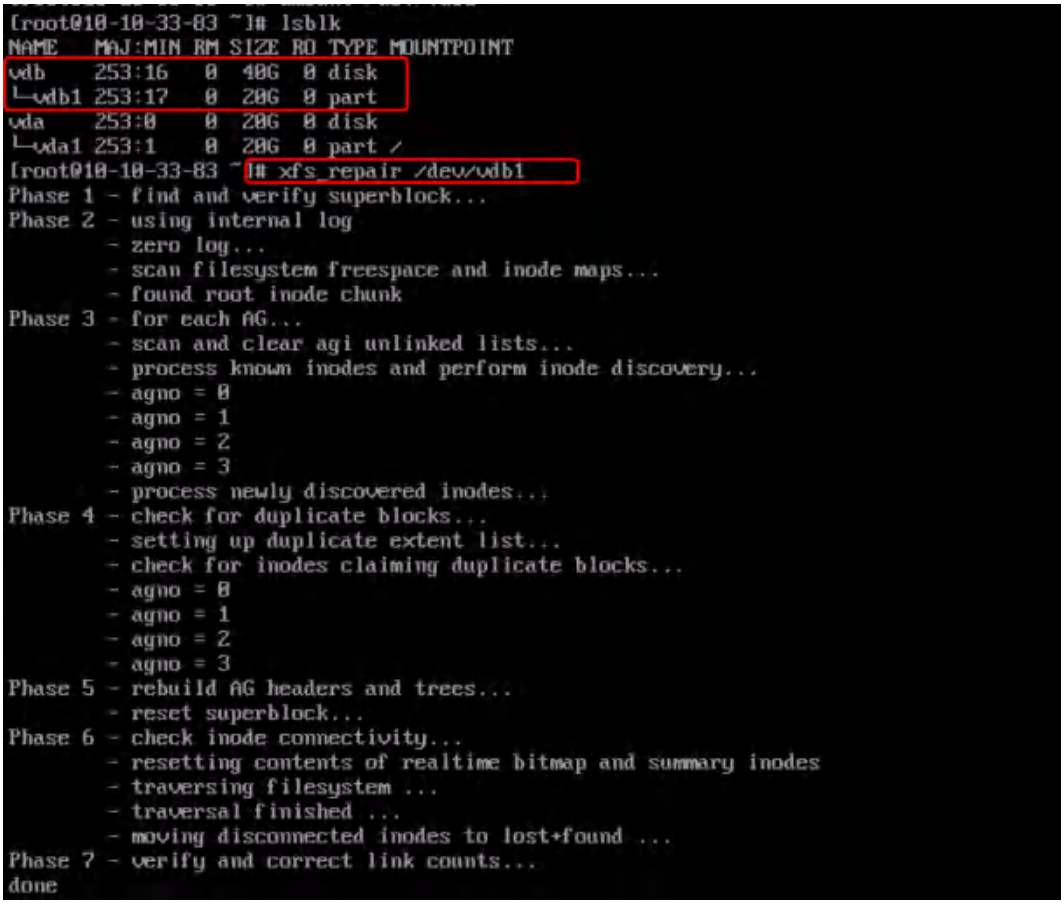
4. 检查文件系统并进行文件系统扩容操作，不同的文件系统扩容命令操作不同，本文分别以 ext4 及 xfs 文件系统为例进行扩容操作；

5. 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；



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。

6. 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：



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。

5.1.7.2.3 单分区扩容（Windows）

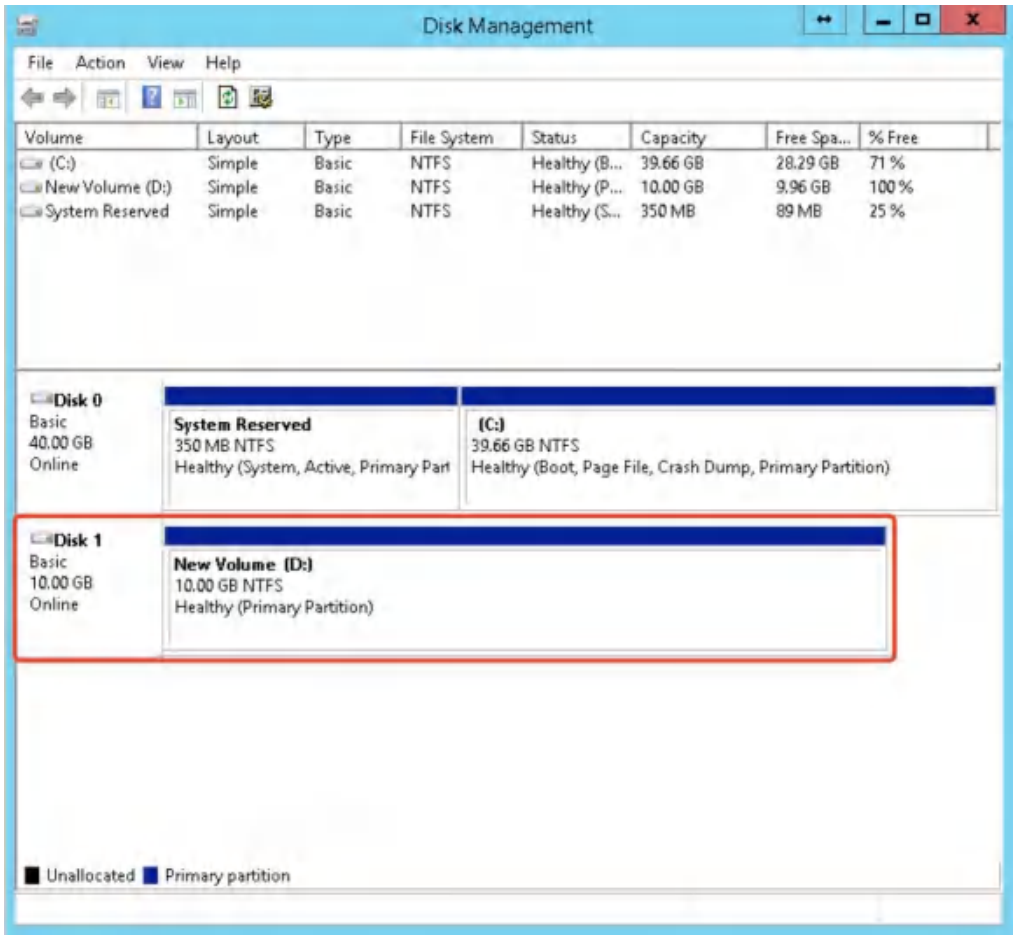
单分区磁盘是指云盘在扩容之前已被挂载过虚拟机且只划分过 1 个分区，用户可通过对硬盘扩容容量后，进入操作系统对单分区磁盘进行分区扩容操作。单分区扩容在 Linux 及 Windows 操作系统上的操作不同，本章节为 windows 单分区扩容操作指南。

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：

注意：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。

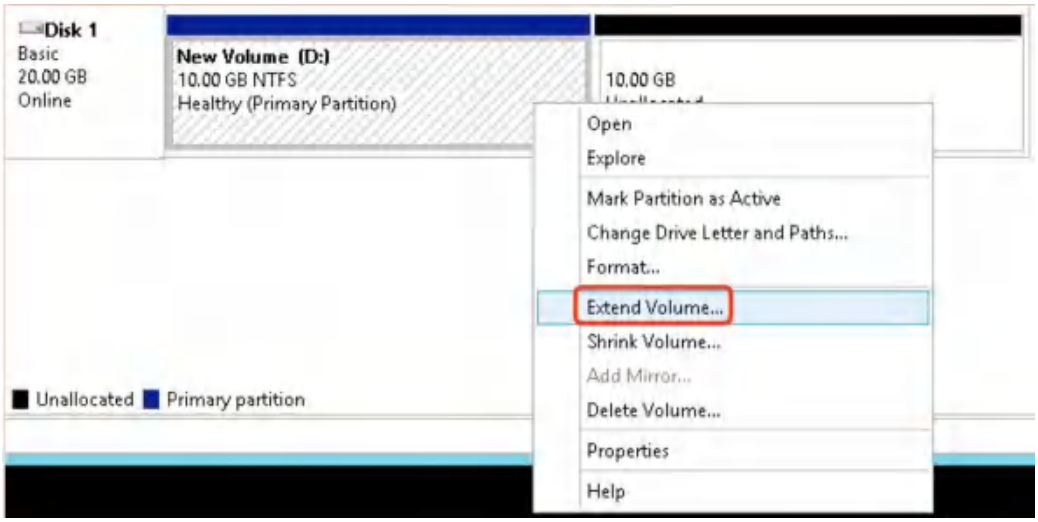
1. 查看当前磁盘的分区及挂载信息，确认磁盘是当前需要扩容的磁盘，如

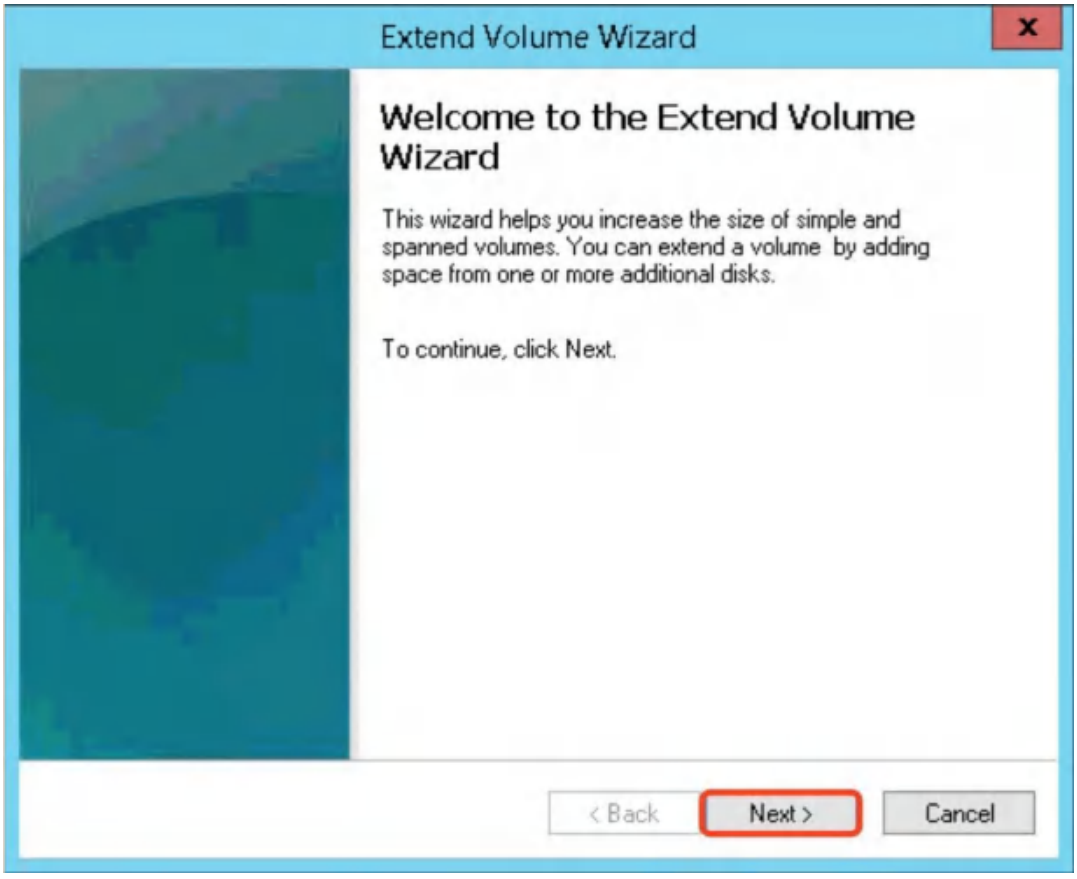
下图所示：

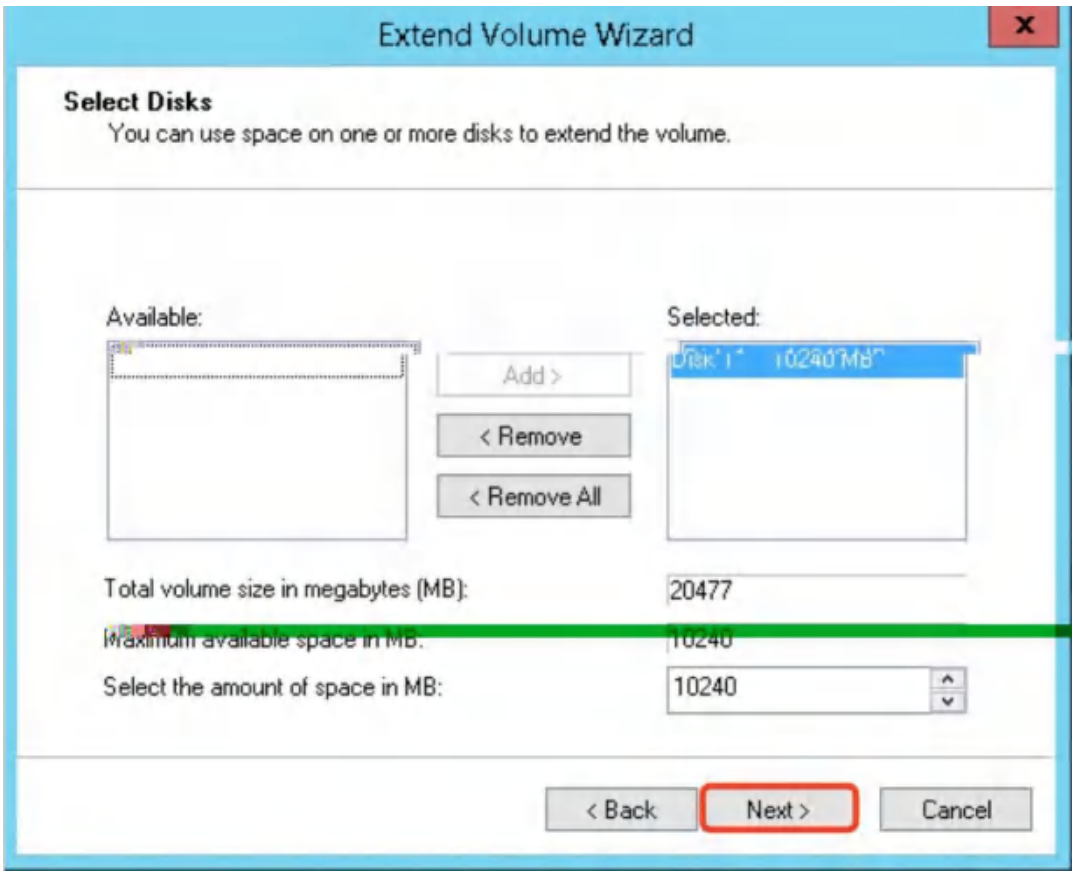


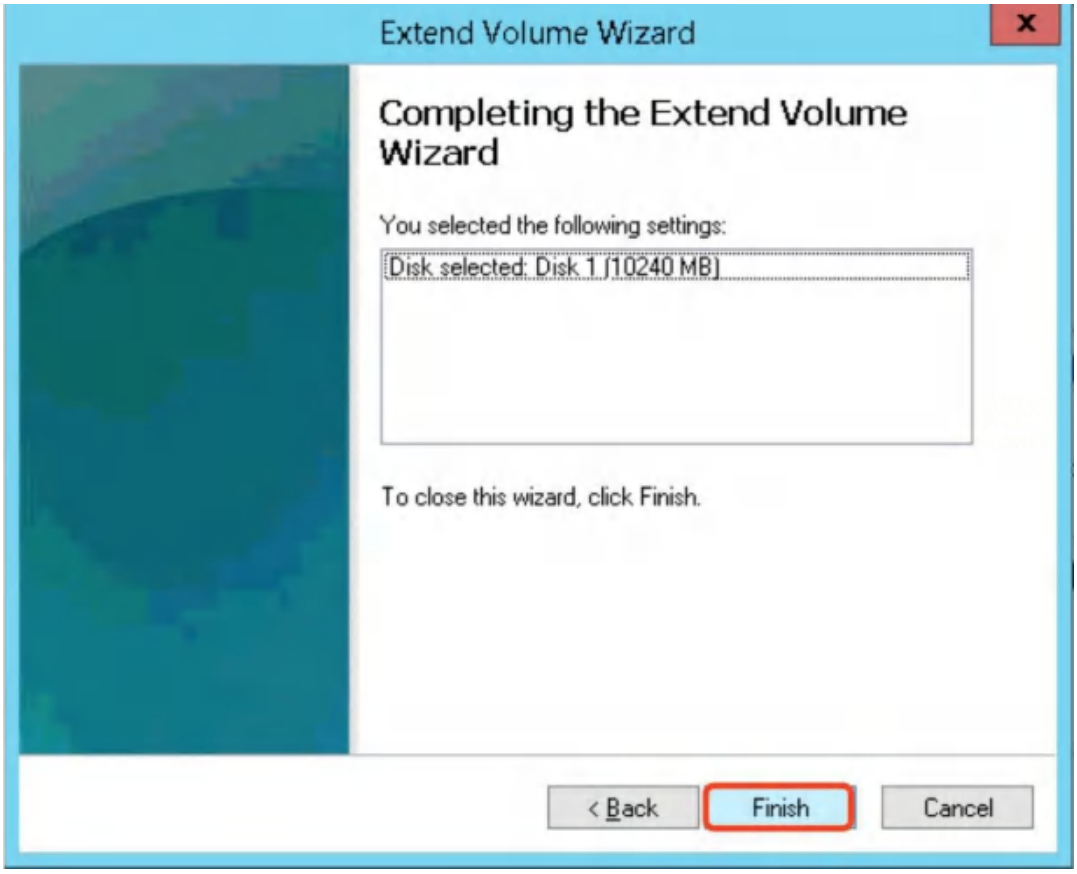
2. 在操作系统中对磁盘进行脱机操作，并通过控制台及 API 对当前磁盘进行容量扩容操作，并通过操作系统磁盘管理工具查看扩容后的磁盘大小，如下图所示：

3. 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：









4. 分区扩展成功后，查看扩容后分区信息，如下图所示：

5.1.7.2.4 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。

注意：本操作示例默认磁盘容量小于 2TB，若磁盘容量大于 2TB 请参考章节。

1. 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；

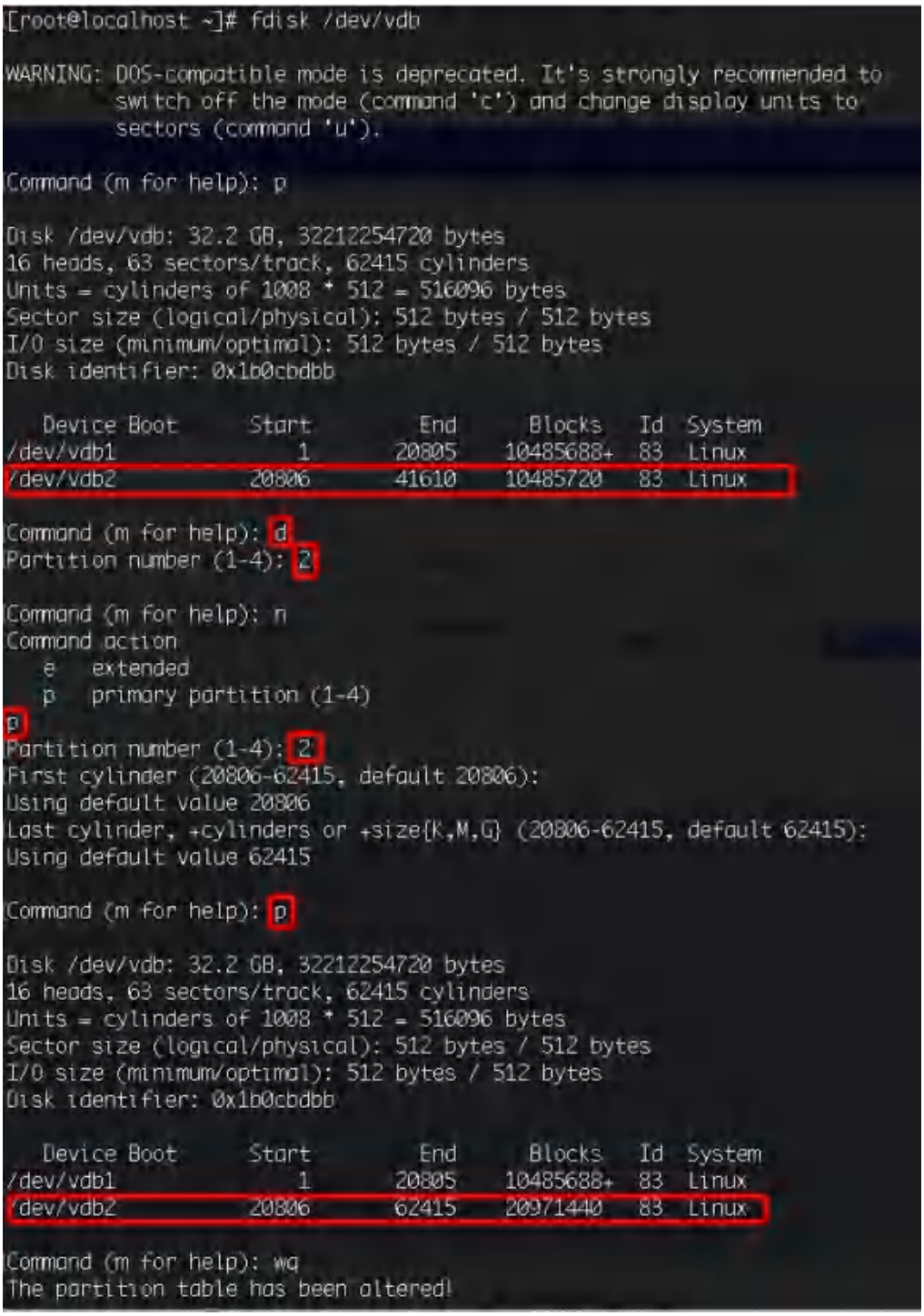
```
[root@localhost ~]# df -Th
Filesystem     Type   Size  Used Avail Use% Mounted on
/dev/vda1      ext4    40G  823M   37G   3% /
tmpfs          tmpfs  935M     0  935M   0% /dev/shm
/dev/vdb1      ext4   9.9G  151M  9.2G   2% /mnt
/dev/vdb2      ext4   9.9G  151M  9.2G   2% /data
[root@localhost ~]#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

2. 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；

3. 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；



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。

4. 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；

5. 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；

6. 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。

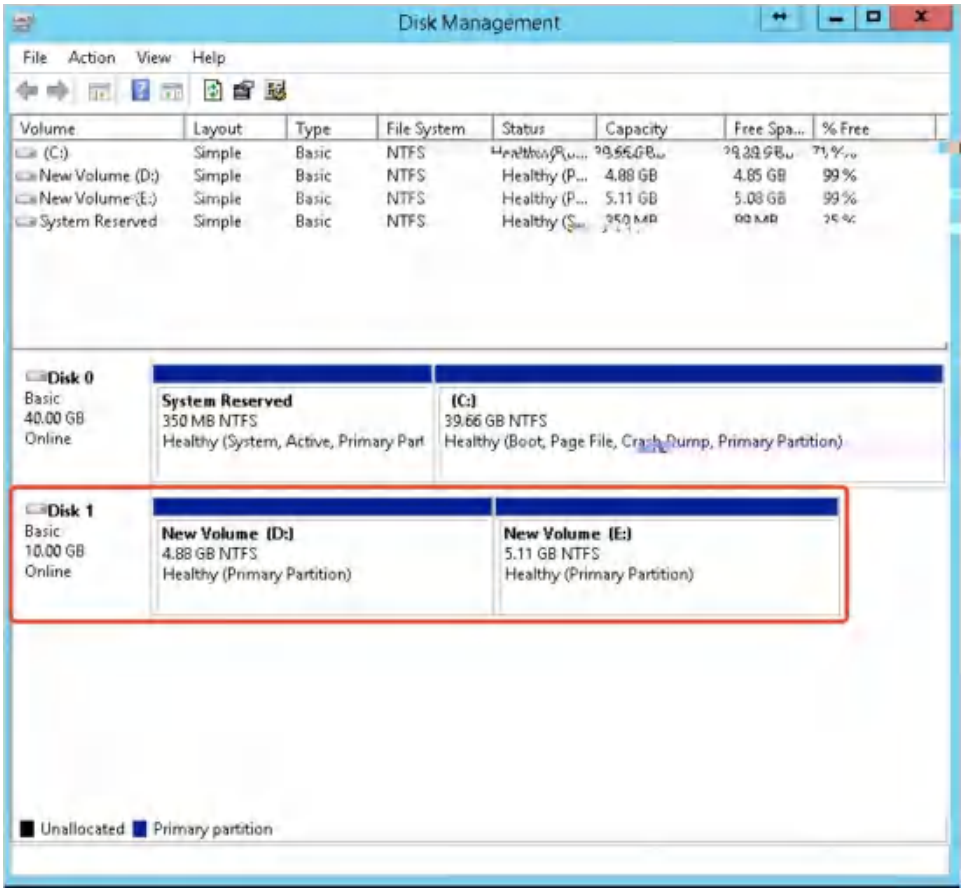
5.1.7.2.5 多分区扩容（Windows）

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。

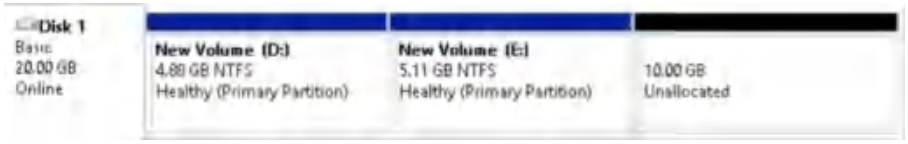
多分区扩容在 Linux 及 Windows 操作系统上的操作不同，本章节为 Windows 多分区扩容操作指南。本示例以 Windows Server 2012R2 操作系统为示例环境版本，云硬盘大小为 10G，两个分区分别 5GB，挂载点 Disk1，扩容至 20GB，即将最后一个分区扩容为 15GB，实际环境中需根据实际情况进行操作。

注意：本操作示例默认磁盘容量小于 2TB，若磁盘容量大于 2TB 请参考章节。

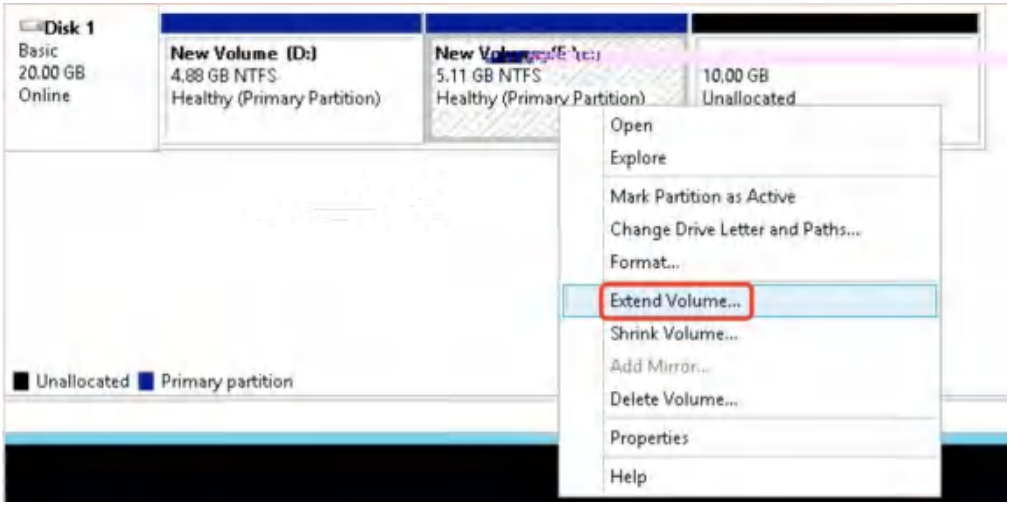
1. 查看当前磁盘的分区及挂载信息，确认磁盘是当前需要扩容的磁盘，如下图所示：



2. 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：



3. 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；

4. 完成扩容后，查看扩容后分区情况，如下图所示：

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

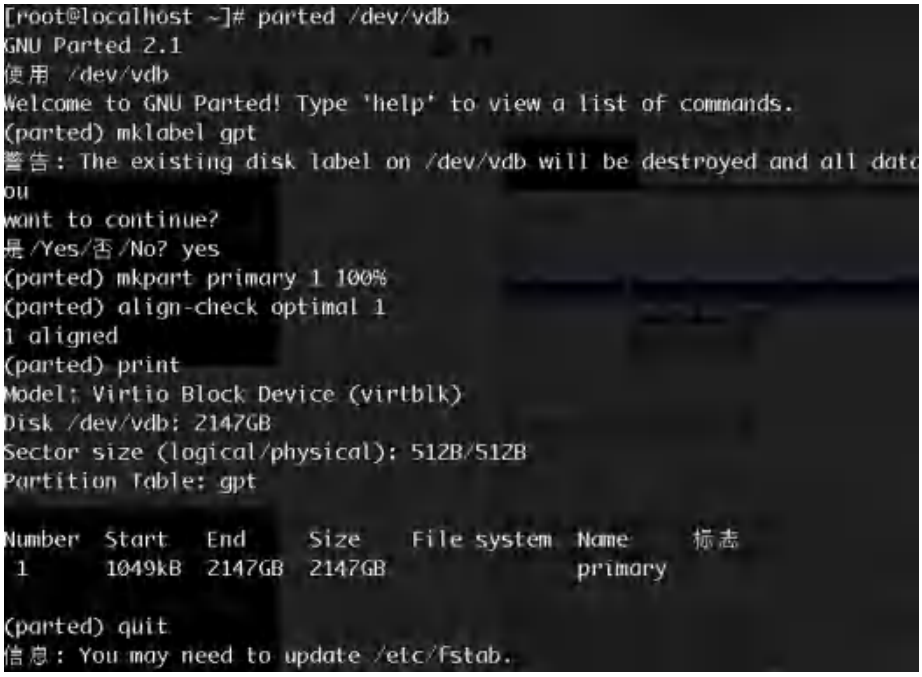
5.1.7.2.6 2TB 磁盘分区扩容（Linux）

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。

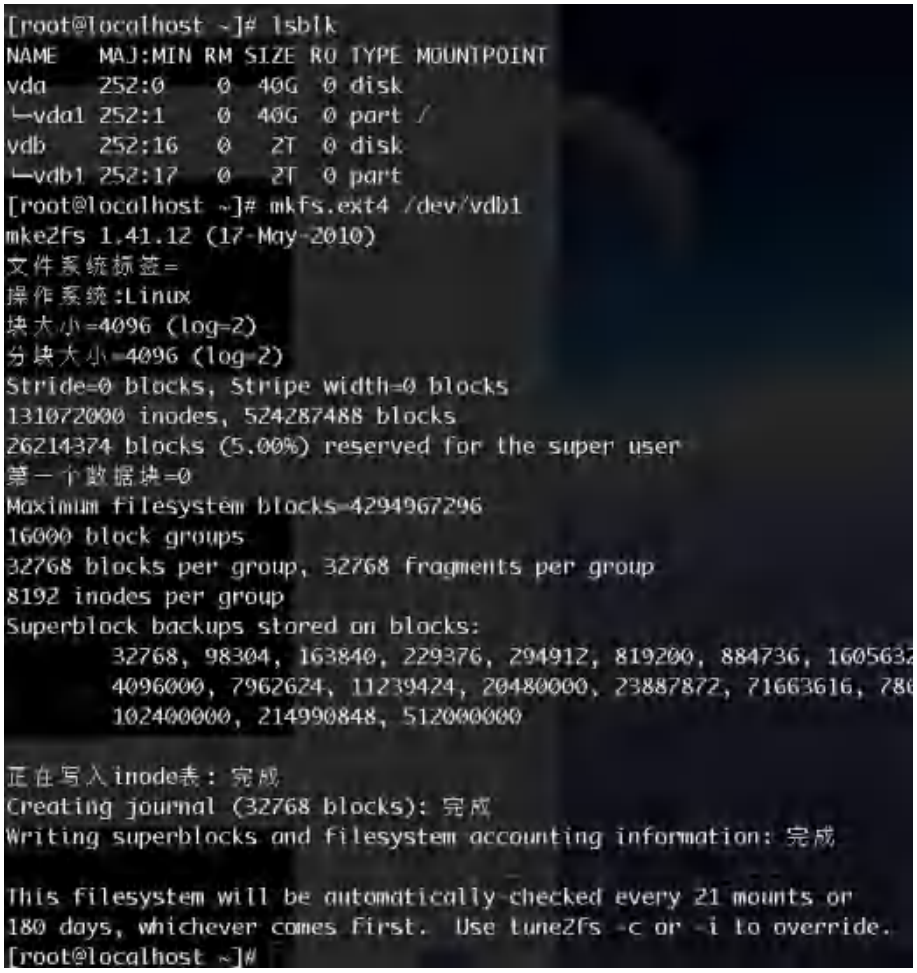
本示例以 CentOS 6.5 操作系统为示例环境版本，云硬盘大小为 2TB，挂载点为/dev/vdb，扩容至 2.1TB，即将云盘及分区扩容为 100GB，实际环境中需根据实际情况进行操作。具体操作如下：

（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：

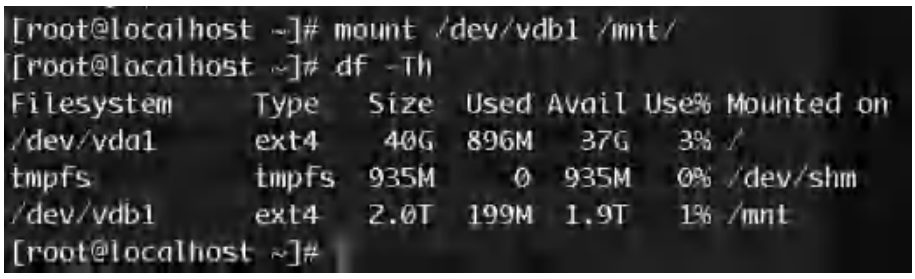
- 通过输入 parted/dev/vdb 进行分区操作，其中 mklabel gpt 是将磁盘分区设置为 GPT 格式；



- 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：



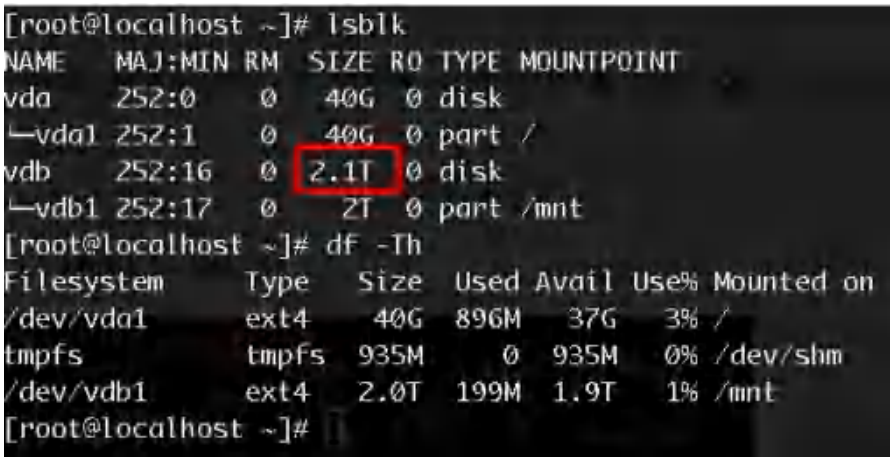
- 格式化成功后，通过挂载并查看磁盘的信息，如下图所示/dev/vdb1 被挂载至/mnt，容量为 2TB。



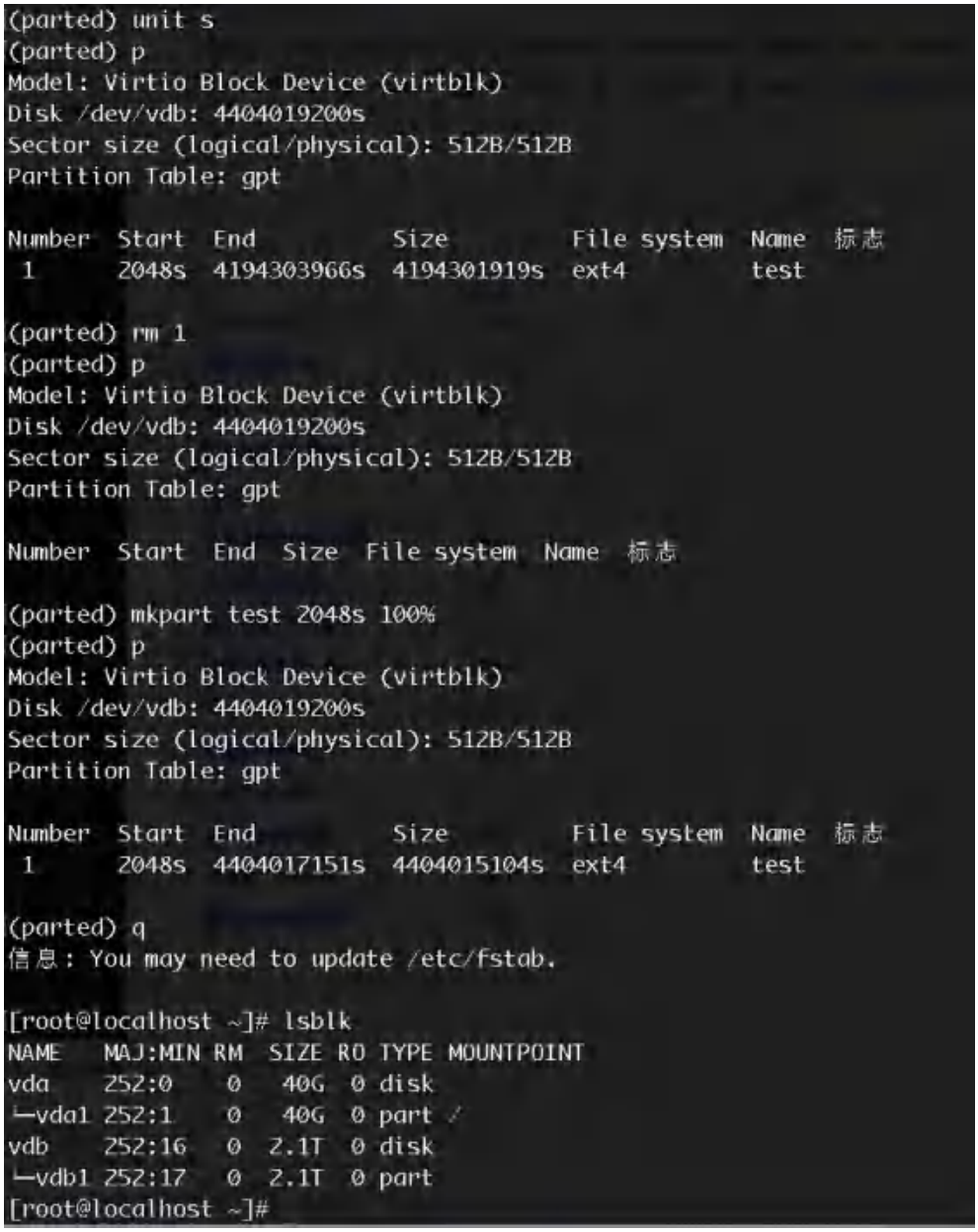
（2）扩容大于 2TB 磁盘的具体操作如下：

- 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：

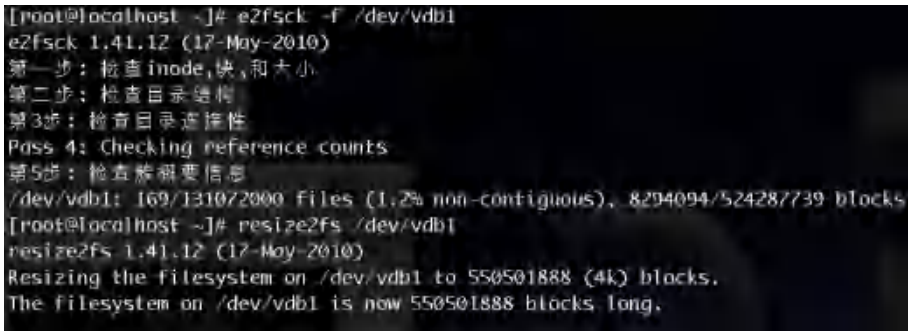


- 在操作系统中 umount 磁盘，使用 parted/dev/vdb 命令删除原来分区并创建新分区，同时使用 lsblk 命令查看 vdb1 分区信息。若为多分区则删除最后一个分区并创建新分区；



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；



- 重新 mount 磁盘并查看磁盘情况，检查扩容是否成功

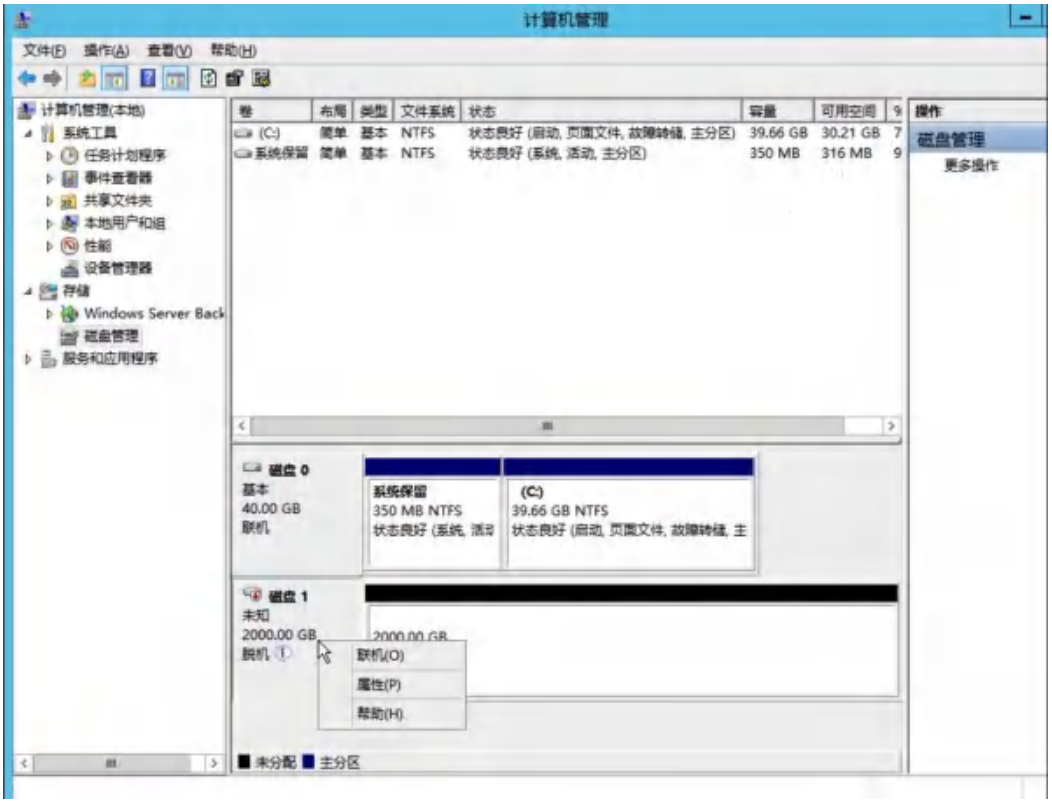
5.1.7.2.7 2TB 磁盘分区扩容（Windows）

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：

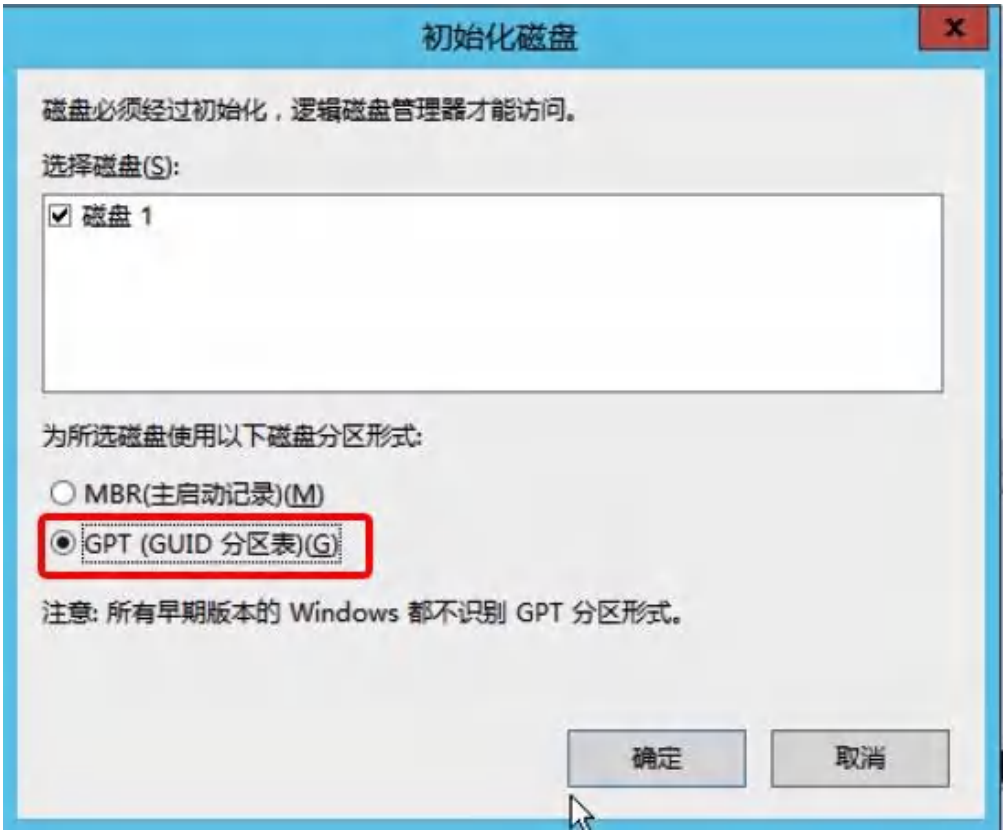
（1）若磁盘为新创建，则需要磁盘管理工具对磁盘进行联机并初始化操作，具体操作如下：

- 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；



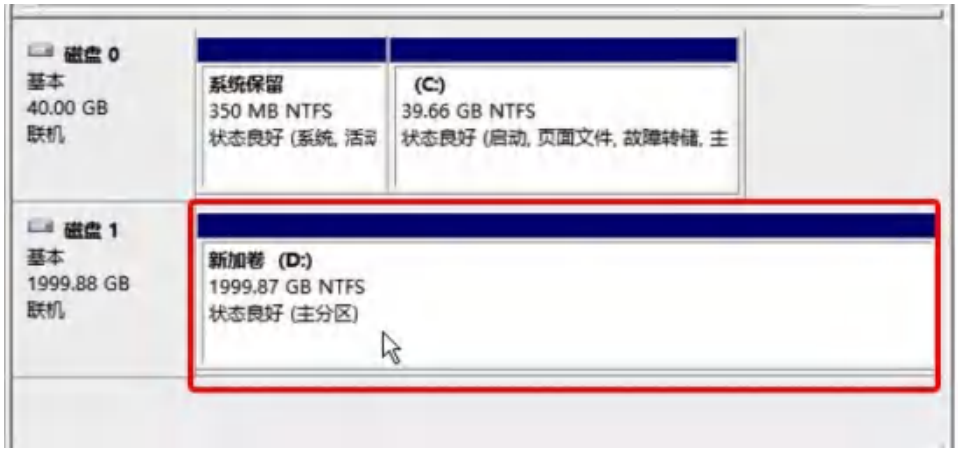
- 如上图所示，右键点击磁盘 1 右边空白处，单击联机，将磁盘置为联机状态；
- 磁盘联机后，磁盘状态为“没有初始化”，可点击磁盘空白处，点击初始化磁盘；

- 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；

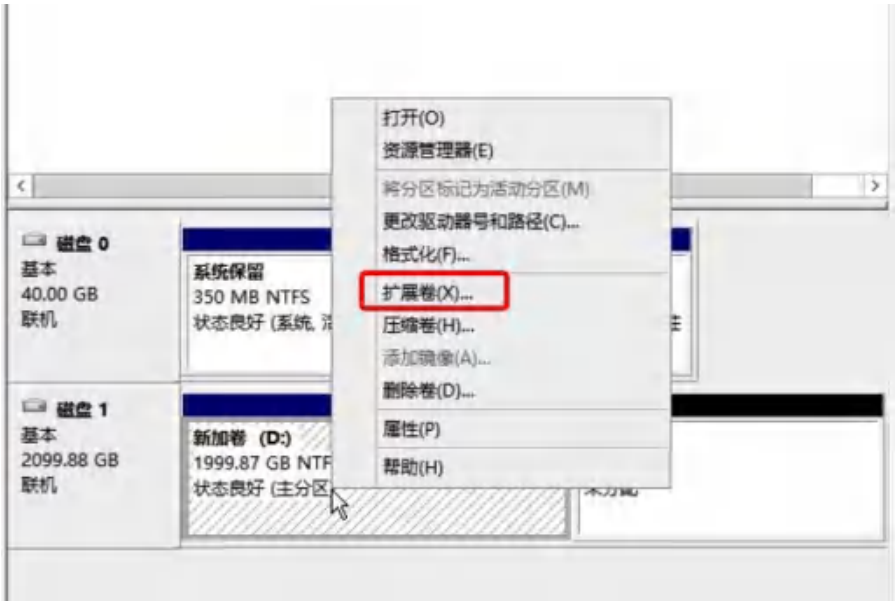
- 在新建简单卷导向中，选择卷大小、驱动器号及格式化选项后，成功创建新的分区，如下图所示：



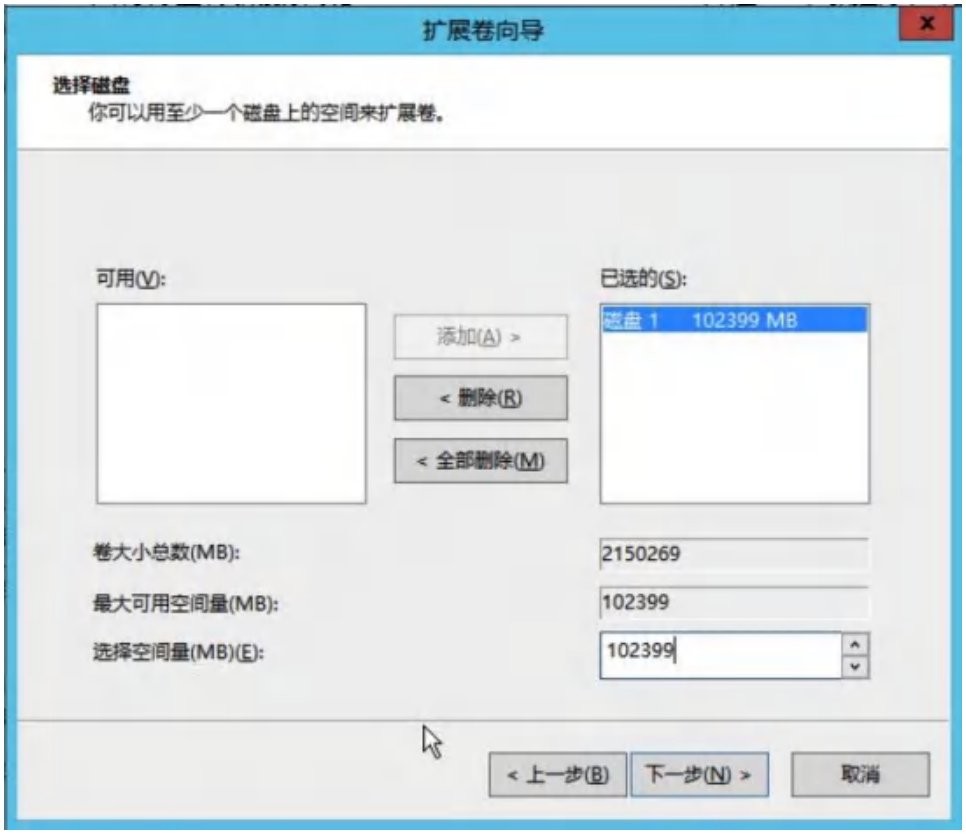
（2）若要扩容 Windows 上 2T 的磁盘，可按如下操作进行扩容：

- 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；

5.1.8 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，克隆云硬盘继承加密属性。

5.1.9 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：

5.1.10 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。

5.1.11 续费云硬盘

支持用户手动对云硬盘进行续费，续费操作只针对资源本身，不对资源额外关联的虚拟机资源进行续费。额外关联的资源到期后，会自动解绑，为保证业务正常使用，需及时对相关资源进行续费操作。

云硬盘续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

云硬盘续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当云硬盘的计费方式为【小时】，则续费时长指定为 1 小时；当云硬盘的计费方式为【按月】，则续费时长可选择 1 至 11 月；当云硬盘的计费方式为【按年】，则云硬盘的续费时长为 1 至 5 年。

5.2 快照管理

云平台分布式存储支持磁盘快照能力，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。

5.2.1 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。

支持定时快照策略，即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。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。

5.2.2 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，快照创建过程中快照的状态为“创建中”，待状态转换为“正常”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。

5.2.3 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、是否加密、创建时间及操作项，如下图所示：

- 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、恢复中、删除中，

其中恢复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。

5.2.4 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：

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“恢复中”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。

5.2.5 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。

5.2.6 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。

5.2.7 创建云硬盘

支持从快照创建云硬盘，创建的硬盘大小与快照的原始硬盘大小相等，继承加密属性，从快照创建云硬盘，该云硬盘只能与快照所对应的原始云硬盘归属同一存储集群，可以用系统盘快照创建的云硬盘创建虚拟机。

在实际操作中，可通过快照列表页或云硬盘详情快照列表操作项中的“创建云硬盘”从快照创建云硬盘。如创建云硬盘向导页面所示，用户可通过核验所需创建的关联硬盘信息，快照信息，并输入云硬盘名称，进行云硬盘创建操作。

5.3 共享硬盘

共享云硬盘是一种支持多个云服务器并发读写访问的数据块级存储设备，具备多挂载点、高并发性、高性能、高可靠性等特点。主要应用于需要支持集群、HA（High Available，指高可用集群）能力的关键企业应用场景，多个云服务器可同时访问一个共享云硬盘。

5.3.1 创建共享硬盘

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

打开云硬盘，共享硬盘页面，点击“创建”按钮，打开创建页面如下：

- 硬盘类型：即共享硬盘类型，即存储集群类型，由平台管理员自定义，

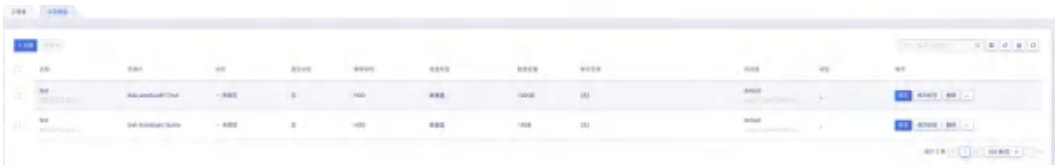
如 HDD 云盘或 SSD 高性能云盘；

- 硬盘容量：共享硬盘分配的逻辑容量，默认最小 10GB，步长为 1GB，最大支持 32000GB，可由云平台管理员在控制台自定义容量规格；
- 硬盘名称：需要创建的共享硬盘名称；
- 硬盘备注：添加必要的备注说明信息；
- 硬盘密钥：输入密钥后该硬盘将加密；
- 项目组：创建时所绑定的项目组；
- 标签：绑定标签用于资源管理；

设置以上信息后，点击“确认”按钮，成功创建共享硬盘。

5.3.2 查看共享硬盘列表

打开云硬盘，共享硬盘页面，查看共享硬盘列表，显示如下：

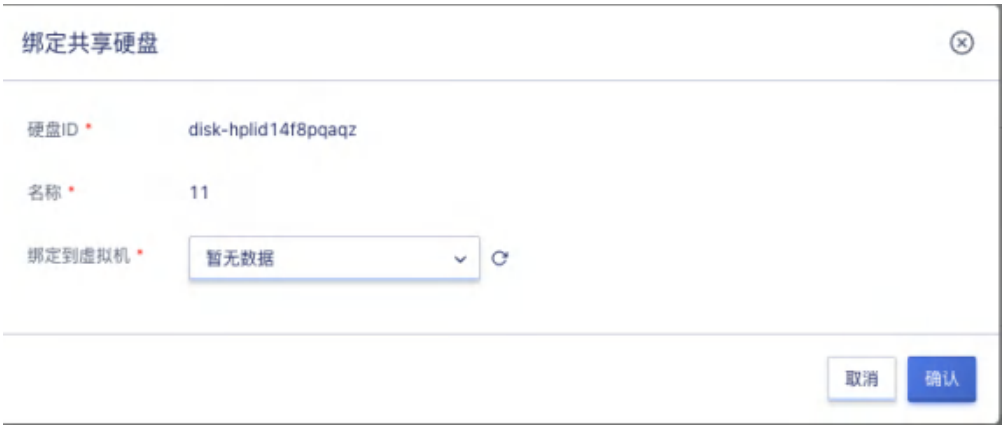


- 名称/ID：共享硬盘的名称和全局唯一标识符；
- 状态：共享硬盘的当前状态，包括创建中、未绑定、共享中、已共享、解绑中、正在被克隆中及删除中等，其中正在被克隆中指当前硬盘正在克隆。
- 是否加密：磁盘的加密状态；
- 集群架构：即共享硬盘类型，即存储集群类型，由平台管理员自定义，如 HDD 云盘或 SSD 高性能云盘；
- 硬盘类型：共享硬盘类型都为数据盘
- 硬盘容量：共享硬盘的容量，GB 为单位；
- 绑定资源：共享硬盘已绑定的虚拟机名称和 ID，未指定则为空；

- 计费方式：共享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；
- 项目组：当前共享硬盘的项目组信息；
- 标签：当前共享硬盘的标签信息；

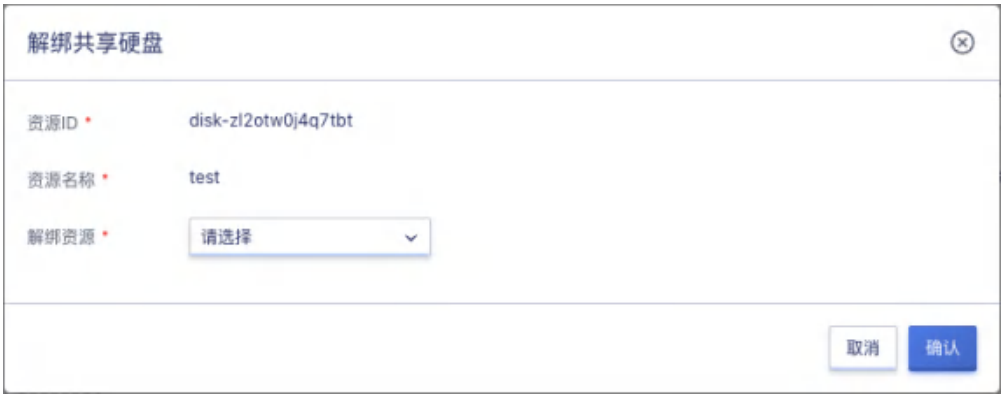
5.3.3 绑定共享硬盘

点击绑定按钮，打开绑定共享硬盘页面，选择虚拟机，点击确认。



5.3.4 解绑共享硬盘

点击解绑按钮，打开解绑共享硬盘页面，选择虚拟机，点击确认。



5.3.5 修改共享硬盘标签

点击修改标签按钮，打开修改标签页面，选择标签，点击确定。

5.3.6 扩容共享硬盘

点击扩容按钮，打开扩容硬盘，修改容量后，点击确认。

5.3.7 克隆共享硬盘

点击克隆按钮，打开克隆共享硬盘，设置目标硬盘名称，项目组，标签等信息，点击确认。

5.3.8 共享硬盘续费

点击续费按钮，打开续费页面，选择续费方式及时长，点击确认。

5.3.9 删除共享硬盘

点击删除按钮，点击确认后，删除共享硬盘。

5.4 外置存储

5.4.1 概述

云平台默认提供分布式存储作为虚拟化的后端存储，为云平台用户提供高可用、高性能、高可靠及高安全的存储服务。同时云平台虚拟化支持对接商业存储设备，如 IPSAN 等存储阵列，为云平台虚拟机提供集群中高性能块存储服务，同时可利旧企业用户的集中存储设备，整体节省信息化转型的总拥有成本。

外置存储服务是云平台为企业用户提供的商业存储服务，通过 ISCSI 协议，FC 协议对接商业存储，将商业存储作为虚拟化后端存储池，提供存储池管理及

逻辑卷分配，可直接作为虚拟机的系统盘及数据盘进行使用，即只要支持 ISCSI 协议和 FC 协议的存储设备均可作为平台虚拟化的后端存储，适应多种应用场景。

平台支持存储设备的对接和管理，并支持将存储设备中的 LUN 分配给租户，由租户将 LUN 分配或挂载至虚拟机的系统盘或数据盘，进行数据的读写，具体功能特性如下：

- 支持存储设备资源池的录入管理，并支持一键扫描 ISCSI 设备中已创建的 LUN 存储卷信息。
- 支持扫描云平台接入的 FC-SAN 设备中已创建的 LUN 存储卷信息。
- 支持将已扫描的 LUN 存储卷分配给平台租户，使租户有权限使用磁盘作为虚拟机的系统盘或数据盘。
- 支持租户将有权限的 LUN 存储卷信息作为虚拟机的系统盘，使虚拟机直接运行直商业存储中，提升性能。
- 支持租户将有权限的 LUN 存储卷信息作为虚拟机的数据盘。
- 支持将存储卷重新分配给平台其它租户。

基于以上功能特性，平台可支持直接使用商业存储设备作为虚拟化的后端存储，为虚拟机提供传统商业存储设备的存储空间，同时不影响商业存储中的其它 LUN 为其它业务提供存储服务。

平台基于 ISCSI 协议，FC 协议对接商业存储，在对接中需要将存储设备的 LUN 映射到平台计算节点，使平台计算节点上运行的虚拟机可直接使用映射的 LUN；同时为保证虚拟机的高可用，需要将 LUN 同时映射到一个集群内的所有计算节点，即所有计算节点均可挂载并使用映射的存储卷，以保证宕机迁移时可在每个计算节点挂载该存储卷信息。

- 当虚拟机所在的计算节点故障时，平台会自动触发虚拟机宕机迁移，即将虚拟机迁移至计算集群内正常的计算节点上，使虚拟机可正常提供服务。

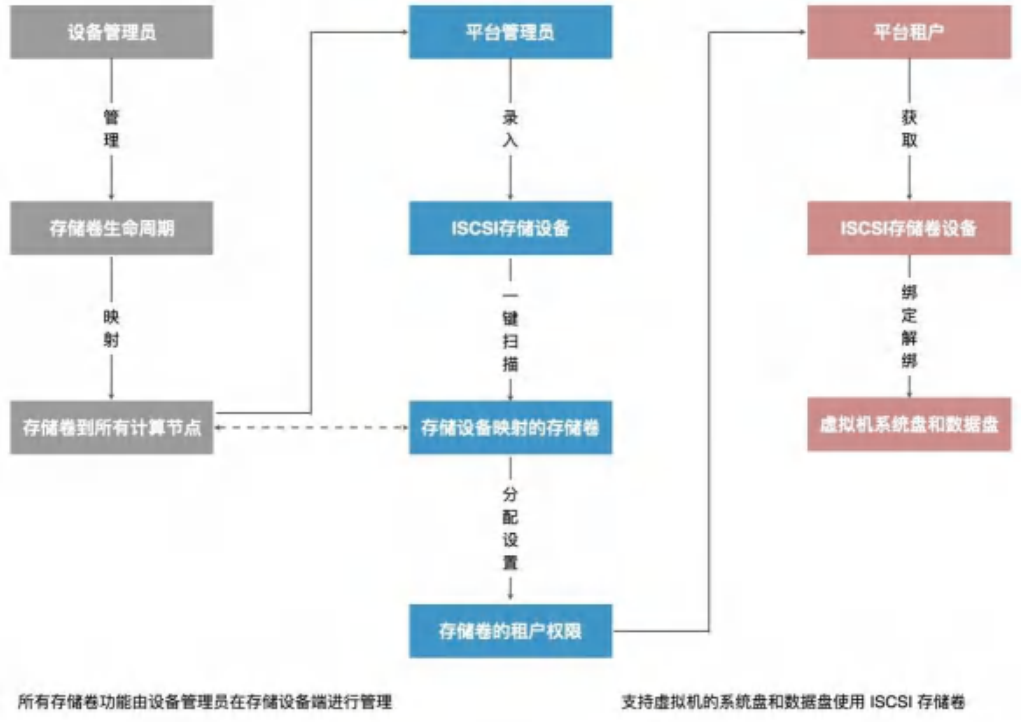
- 虚拟机使用的 LUN 存储卷已被映射到集群内所有计算节点，当虚拟机在集群内迁移至新节点后，可直接使用已映射的 LUN 存储启动虚拟机的系统盘或数据盘，并正常挂载至虚拟机，保证虚拟机迁移后业务正常。

平台仅将商业存储的 LUN 作为存储卷进行使用，不对存储卷本身进行管理，如 LUN 的创建、映射、扩容、快照、备份、回滚、克隆等。

5.4.2 使用流程

在使用外置存储前，需要平台管理者或存储设备管理者，将外置存储与平台的计算节点网络打通，使计算节点可与存储设备间直接内网可互相通信。

物理存储设备及网络准备好后，即可与平台进行对接并使用平台提供的外置存储服务，整个对接过程需要存储设备管理员、平台管理员及平台租户三个角色进行操作，其中与平台相关的为平台管理员和平台租户的操作，如下图流程所示：



1. 存储设备管理员管理存储卷

所有存储卷的管理均由存储设备管理员自行在商业存储的管理系统上进行操作，包括存储卷（Lun）的创建和映射，同时包括存储卷的扩容、快照、备份

及删除等相关生命周期管理。

2. 存储设备管理员映射存储卷至集群计算节点

创建好的 Lun，由存储设备管理员在存储设备上映射到所有计算节点（如果新增计算节点，需再次进行映射），同时也可进行多路径映射。

3. 平台管理员录入并管理存储设备

存储卷 LUN 映射成功后，由【平台管理员】在管理控制台“外置存储集群”中进行 ISCSI 存储池或存储设备的录入，录入时需要指定存储设备的 ISCSI 地址，如 172.18.12.8:8080。

4. 平台管理员扫描已映射的 LUN 信息

录入的存储设备后，由【平台管理员】在存储设备中一键扫描 ISCSI 存储设备中已被映射至集群节点上的存储卷设备及信息；FC-SAN 存储设备接入计算集群后，通过扫描获取已被映射至集群节点上的存储卷设备及信息。

5. 平台管理员为租户分配 LUN 设备

由【平台管理员】将扫描成功的 LUN 存储卷设备指定给租户，一个存储卷同一时间仅支持分配给一个租户，分配后租户在外置存储设备中即可查询已分配的存储卷设备，并可进行创建虚拟机或挂载虚拟机。

6. 平台租户使用 LUN 存储卷设备

平台租户通过控制台外置存储可直接查询已分配的存储卷，并在创建虚拟机时指定系统盘类型为外置存储，或者也可直接将 LUN 存储卷直接挂载给已有虚拟机，作为虚拟机的数据盘进行使用。

平台租户使用外置存储服务的前提是存储卷已映射并分配给租户，租户只需要简单的绑定即可便捷的使用平台提供的外置存储设备，并可进行弹性绑定和解绑。

5.4.3 查看外置存储设备

在平台已提供外置存储服务并已分配存储卷 LUN 设备给租户时，租户的主

账号和子账号可在平台上直接查询有权限的存储卷设备，并可将存储卷设备挂载至虚拟机进行数据存储。管理员分配存储卷如下图所示：

用户可登录控制台，通过控制台导航栏【存储】进入【外置存储盘】资源控制台，通过外置存储列表查看已有权限的 LUN 存储卷信息，包括名称、资源 ID、类型、容量大小、状态、集群、LUNID、挂载资源及操作项，如图所示：

- 名称/资源 ID：当前存储卷的名称及全局唯一标识符。
- 类型：存储卷的类型，包括系统盘和数据盘，当创建虚拟机选择外置存储卷作为系统盘时类型为系统盘；当存储卷绑定给虚拟机时类型为数据盘。
- 容量大小：存储卷的容量大小，由存储设备管理员创建时指定的大小。
- 状态：存储卷的状态，包括未绑定、已绑定。
- 集群：存储卷的所属存储池集群。
- LUNID：当前存储卷在商业存储中的 LUNID。
- 挂载资源：当前存储卷已挂载的虚拟机名称和 ID。

列表上的操作项是指对存储卷的绑定和解绑操作，支持批量解绑操作，同时列表上支持对存储卷设备进行搜索，支持模糊搜索。

5.4.4 外置存储作为系统盘

平台支持将一块 LUN 存储卷设备作为虚拟机的系统盘，当租户被分配外置存储卷时，会自动在外置存储卷列表中获取到有权限的 LUN 设备，同时创建虚拟机时系统盘类型可选择有权限的存储卷的存储池集群。

用户只需要创建虚拟机时选择系统盘类型为平台管理员录入的【存储池名称】，并选择存储池中有权限的存储卷设备作为虚拟机的系统盘，即可将一台虚拟机的系统盘直接运行在外置存储卷设备上。

作为虚拟机系统盘的外置存储 LUN 设备与虚拟机的生命周期一致，不支持解绑操作。

5.4.5 外置存储作为数据盘

平台支持将一块 LUN 存储卷设备作为虚拟机的数据盘，当租户被分配外置存储卷时，会自动在外置存储卷列表中获取到有权限的 LUN 设备，LUN 存储卷作为数据盘的使用方式与平台默认的云硬盘一致，只需要简单的绑定操作即可。

用户只需要在外置存储设备列表上将 LUN 设备直接绑定至虚拟机，即可将一块 LUN 存储卷作为虚拟机的数据盘进行使用，仅支持绑定状态为【未绑定】状态的存储卷设备，同时平台支持用户随时将存储卷从虚拟机上解绑。

5.4.6 解绑外置存储

平台支持将已挂载至虚拟机 LUN 存储卷进行解绑，重新绑定至其它虚拟机。仅支持解绑状态为【已绑定】状态的存储卷，解绑操作不影响虚拟机系统盘的正常访问，同时不影响存储卷设备中的数据。

5.4.7 设为共享硬盘

平台支持将外置存储盘设置为共享硬盘使用，该操作过程不可逆。

5.5 对象存储

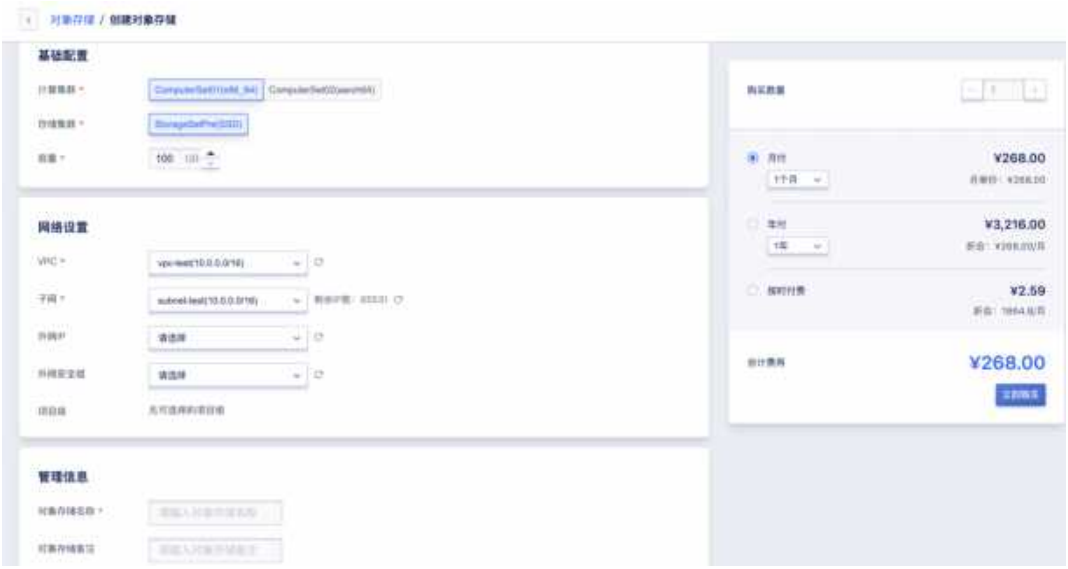
5.5.1 对象存储概述

对象存储服务 OSS（Object Storage Service），兼容亚马逊云的 S3 API（接口协议），仅需在 UCloudStack 平台上创建对象存储实例，便可以在任何应用、任何时间、任何地点通过存储和访问任意类型的数据。对象存储为云原生设计，即使在高负载的情况下也可以高效利用 CPU 和内存资源，适合私有云场景。

5.5.2 创建对象存储

云平台用户可以通过指定计算集群、存储集群、容量、VPC、子网、外网 IP、外网安全组、项目组、对象存储名称等相关基础信息创建对象存储。

可通过导航栏进入【对象存储】资源控制台，通过“创建”进入向导页面，如下图所示：



1. 选择并配置对象存储的基础配置、网络设置及管理配置信息：

   - 名称/备注：申请对象存储的名称和备注，申请时必须指定名称；
   - 容量：支持的容量范围为 100~1024 GB；
   - 创建对象存储时必须选择 VPC 网络和所属子网，即选择要加入的网络及 IP 网段；
   - 外网 IP 为对象存储提供外网访问服务，支持创建对象存储时申请并绑定一个外网 IP 作为外网访问地址。平台支持 IPv4/IPv6 双栈网络，也可在对象存储创建成功后为对象存储绑定多个外网 IP 地址，最多支持绑定 50 个 IPv4 和 10 个 IPv6 外网 IP 地址。

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”进行对象存储的创建：

   - 购买数量：默认支持创建 1 个对象存储；
   - 付费方式：选择对象存储的计费方式，支持按月、按年、按时三种方式，可根据需求选择合适的付费方式；
   - 合计费用：用户选择对象存储资源按照付费方式的费用展示；
   - 立即购买：点击立即购买后，会返回对象存储资源列表页，在列表页可查看对象存储的创建过程，通常会先显示“初始化”的状态，几秒内转换

为“可用”状态，即代表创建成功。

5.5.2.1 通过内网配置对象存储

用户可通过对象存储列表的内网地址配置对象存储服务：

```
wget -c https://dl.min.io/client/mc/release/linux-amd64/mc
chmod+x mc
./mc alias set 名称 http://内网 ip:9000 admin 密码
```

5.5.2.2 通过外网配置对象存储

用户可通过对象存储列表的外网地址配置对象存储服务：

```
wget -c https://dl.min.io/client/mc/release/linux-amd64/mc
chmod+x mc
./mc alias set 名称 http://外网 ip:9000 admin 密码
```

5.5.3 对象存储列表

通过导航栏进入对象存储控制台，可查看对象存储资源列表。

对象存储列表可查看当前账户下所有对象存储资源的列表信息，包括名称、资源 ID、状态、存储容量、域名、VPC、子网、计费方式、项目组、创建时间、过期时间及操作项，如下图所示：

- 名称：对象存储资源的名称；
- 资源 ID：对象存储的资源 ID 作为全局唯一标识符；
- 状态：对象存储资源的状态，包括初始化、可用、删除中等状态；
- 存储容量：对象存储的内存容量，容量范围为 100~1024 GB；

- 域名：可通过内网/外网访问地址配置对象存储服务；
- VPC/子网：对象存储创建时所指定的 VPC 网络和子网，即对象存储内网 IP 所在的 VPC 网络和子网信息；
- 计费方式：对象存储的付费方式，包括按时、按年、按月；
- 项目组：对象存储创建时所绑定的项目组；
- 创建时间/过期时间：对象存储资源的创建时间和费用过期时间；
- 操作：列表上的操作项是对单个对象存储的操作，包括扩容、绑定、解绑、续费及删除。

5.5.4 扩容对象存储容量

平台支持用户扩容对象存储的容量，适应于业务发生变化需扩容对象存储容量的场景。平台仅支持扩容对象存储容量，不支持对象存储容量的缩容。

对象存储容量扩容范围即当前硬盘类型的规格，默认为 100GB~1024 GB。

扩容对象存储容量会对费用产生影响，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。用户可点击对象存储控制台操作中的“扩容”进行容量扩容操作，如下图所示：

如图所示，**更改容量**，即对象存储需要扩容的容量。平台已展示当前对象存储的容量大小，由于不支持缩容，扩容时更改容量必须大于当前容量大小。用户可通过对象存储列表查看新容量。

5.5.5 绑定外网 IP

绑定外网 IP 是指将 EIP 地址绑定至对象存储，用户可通过外网访问地址使用对象存储服务。

用户可通过对象存储资源列表操作项的“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的弹性 IP，绑定成功后，对象存储列表的访问地址会新增外网访问地址。

5.5.6 解绑外网 IP

解绑外网 IP 是指将 EIP 地址从一个对象存储资源上分离出来，并可重新绑定至其它虚拟资源。仅支持解绑已绑定对象存储的外网 IP 资源，用户可通过对象存储资源列表操作项的“解绑”进入外网 IP 解绑向导页面，进行资源解绑操作，如下图所示：

5.5.7 对象存储续费

支持用户手动对对象存储进行续费。对象存储续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

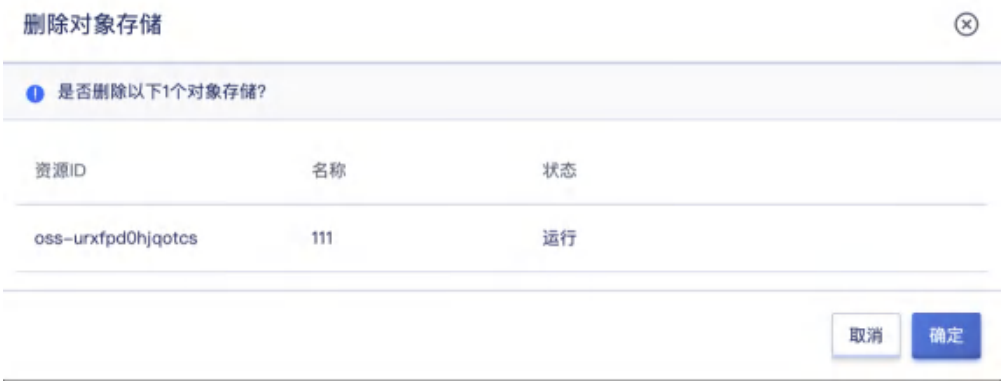
对象存储续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当对象存储的计费方式为【小时】，则续费时长指定为 1 小时；当对象存储的计费方式为【按月】，则续费时长可选择 1 至 11 月；当对象存储的计费方式为【按年】，则续费时长为 1 至 5 年。可通过对象存储列表操作项中的“续费”进行操作，如下图所示：

5.5.8 重置密码

支持用户重置对象存储密码，可通过对象存储列表操作项中的“重置密码”操作，如下图所示：

5.5.9 删除对象存储

用户可在控制台删除账户内对象存储，支持对对象存储进行批量删除操作。可通过对象存储列表操作项中的“删除”进行操作，如下图所示：



用户可通过命令行工具在 client 端重新设置密码

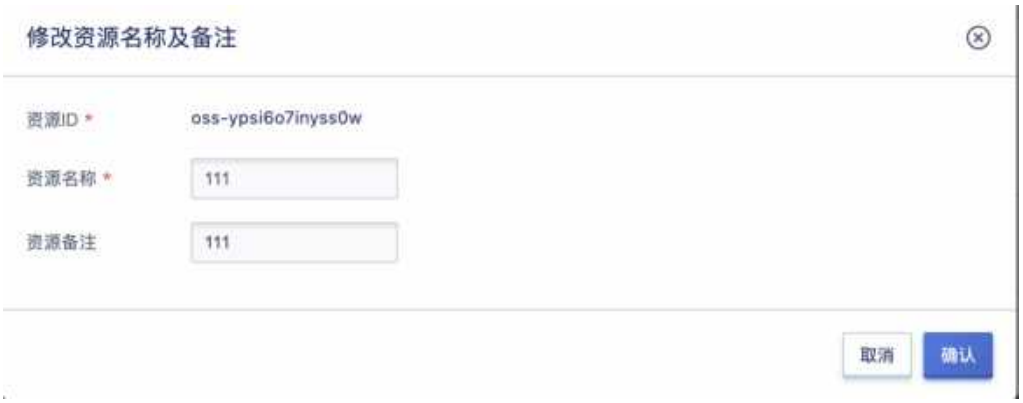
./mc alias set 名称 http://外网 ip:9000 admin 新密码

5.5.10 搜索对象存储

用户可通过搜索框对对象存储列表进行搜索和筛选，支持从名称、备注、资源 ID、域名进行模糊搜索，如下图所示：

5.5.11 修改对象存储名称与备注

修改对象存储的名称和备注。可通过点击对象存储列表名称右侧的“编辑”按钮进行修改，如下图所示：



5.5.12 对象存储监控页面

用户可通过点击对象存储列表操作项中的“名称”，进入对象存储的监控页面，还可以通过操作项中的“修改告警模版”，对监控数据进行告警

5.5.13 外网对象存储绑定/解绑安全组

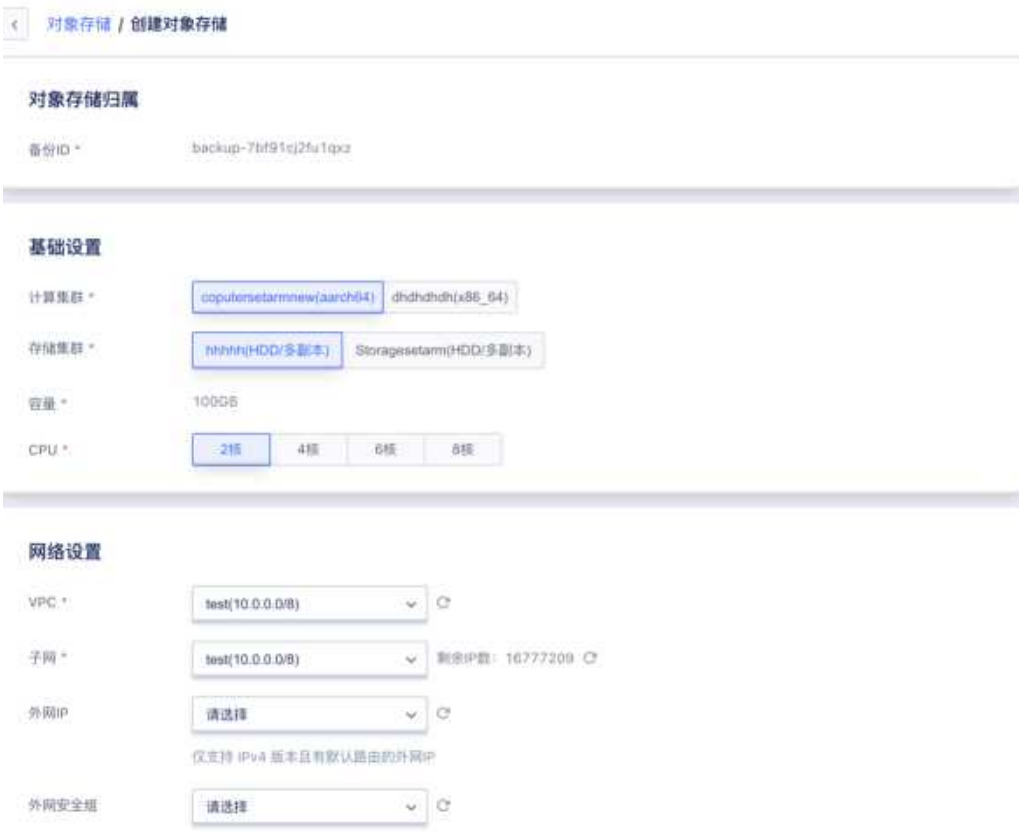
用户可通过点击对象存储列表操作项中的“修改外网安全组”对外网做网络安全策略

5.5.14 修改 IP 地址

支持用户修改对象存储的内网 IP 地址。

5.5.15 从备份创建

用户可以通过备份创建对象存储。



5.5.16 桶管理

5.5.16.1 桶列表

用户点击对象存储列表页的“**桶管理**”操作按钮，即可进入桶管理页面。如下图所示：

桶列表中每行表示一个存储桶，显示信息包括：

- 名称：存储桶的名称；
- 访问类型：私有、公共读、公共读写；
- 创建时间：桶的创建时间，格式：YYYY-MM-DD；
- 操作：支持文件管理和删除桶的操作。

5.5.16.2 桶详情

在桶列表信息页面，选择某个桶，点击桶名称即可进入桶详情页。如下图所示：

“概览”分页中显示的基本信息包括：

- 名称：存储桶的名称；
- 访问类型：值为私有、公共读、公共读写，默认创建桶时为私有，用户根据需要进行选择；

- 多版本：是否开启，默认不开启；
- 对象锁定：是否开启，默认不开启，如开启，对象不能写入，只能读。并且开启后无法关闭。

“文件管理”分页信息，如下图所示：

显示信息包括以下内容：

- 上传文件：用户可以在页面上传文件
- 创建目录：可以创建文件目录
- 上传列表：支持把没有上传成功的文件记录下来，重新上传
- 清空当前桶：清空存储桶中的所有文件、历史版本、文件碎片、删除后数据不可恢复和访问
- 文件名：用户上传至对象存储中的文件名；
- 文件大小：上传文件的大小；
- 更新时间：文件上传时间；
- 操作：历史版本、下载和删除文件操作；

“删除标记”分页信息，如下图所示：

显示信息包括以下内容：

- 文件名：对象名称；
- 更新时间：展示更新时间；
- 操作：查看历史版本。

“生命周期”分页信息，如下图所示：

显示信息包括以下内容：

- ID：生命周期规则的唯一标识符；
- 规则范围：生命周期规则的范围，包括整个存储桶和指定前缀。存储桶是对象存储中用于存储文件和数据的容器，前缀是对象在存储桶中的路径前缀；
- 过期类型：生命周期规则的过期类型，未开启多版本时，类型为当前版本；开启多版本时，类型为当前版本/非当前版本；
- 过期天数：生命周期规则的过期天数；

- 操作：支持编辑和删除生命周期规则。

5.5.16.3 桶的相关操作

桶的相关操作包括：

- 创建存储桶
- 开启对象锁定
- 删除存储桶
- 删除文件
- 恢复历史文件（多版本控制）
- 文件管理
- 删除标记
- 生命周期

5.5.16.3.1 创建存储桶

在桶管理页面，点击“创建存储桶”按钮，弹出创建存储桶窗口，如下图所示：

用户需要填写以下信息：

- 存储桶名称：填写存储桶名称；
- 访问类型：私有、公共读和公共读写，选这一个，默认为私有；
- 是否开启多版本：默认不开启，开启后会出现是否开启对象锁定选项；
- 是否开启对象锁定：用户选择开启或关闭（对象锁定依赖多版本功能，开启后无法关闭），默认为关闭；
- 对象锁定天数：对象锁定开启后会出现设置锁定天数的选项，锁定功能不开启则不需要设置。

填写完成后，点击“确定”按钮，即可完成添加存储桶操作。

5.5.16.3.2 开启对象锁定

对象锁定功能一旦开启，该桶只能上传文件，对对象进行多次查询和读取，不能进行写操作，也不能删除，适应于一次写多次读，以及安全、防护有要求的场景。

开启对象锁定只能在创建桶时进行，桶创建以后无法开启锁定功能操作，并且对象锁定依赖多版本功能，开启后无法关闭。

进入创建存储桶页面，在“是否开启对象锁定”项中，用户点击开启（ON），弹出“对象锁定天数”设置项，用户输入锁定周期（周期可以是天、月、年维度），原则上周期不设上限。如下如图所示：

点击对话框“确定”按钮，开启对象锁定操作完成。

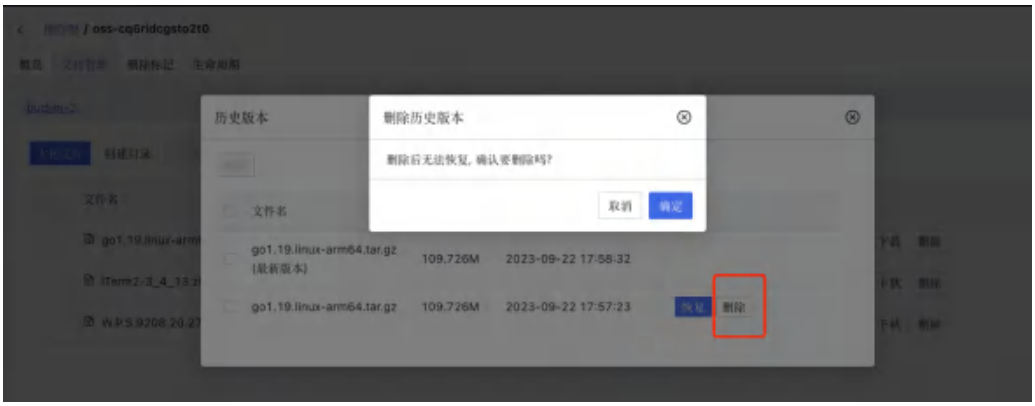
5.5.16.3.3 删除存储桶

勾选列表中的一个或多个多选按钮，点击菜单上方的“删除”按钮，或点击列表右侧的“删除”按钮，弹出删除存储桶确认对话框，点击“确定”按钮，即可完成删除存储桶操作。如下图所示：

5.5.16.3.4 删除文件

在桶的“文件管理”分页，勾选列表中的一个或多个多选按钮，点击菜单上方的“删除”按钮，或点击列表右侧的“删除”按钮，弹出删除该桶下文件确认对话框，点击“确定”按钮，即可完成删除文件操作。如下图所示：

点击“确定”按钮，即可完成删除文件操作。 如开启多版本功能，可以在文件管理页面，删除其历史版本文件。如下图所示：

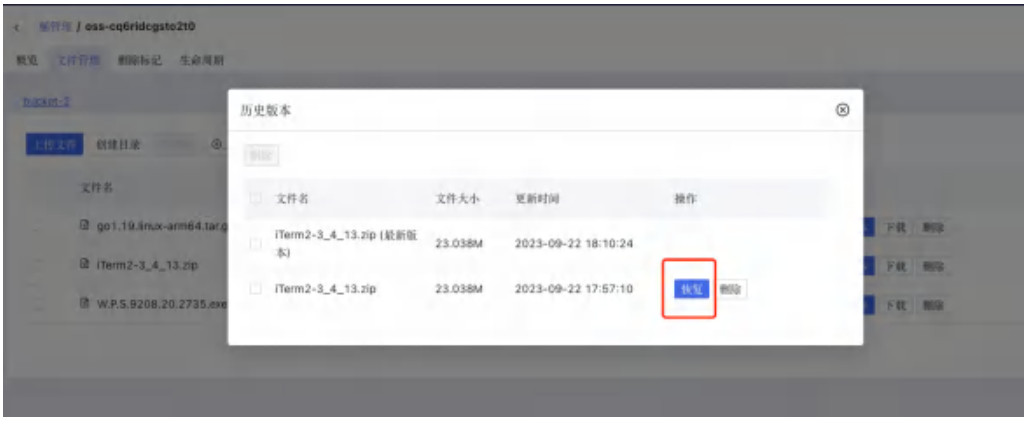


点击确认，即可完成文件历史版本数据的删除操作。 删除历史数据，对该桶文件的最新数据没有任何影响。

5.5.16.3.5 恢复历史文件（多版本控制）

多版本控制默认是关闭的，用户需要手动开启，方可进行历史文件的恢复操作。 在存储桶概览页，“基本信息”页面下开启多版本功能。如下图所示：

文件管理页面信息。如下图所示：



在文件列表中，针对某文件一行，点击右侧的“恢复”按钮。如下图所示：

点击按钮后，该历史文件恢复为当前最新版本文件（之前最新的文件已变为历史文件）。

5.5.16.3.6 文件管理

在“文件管理”分页，点击列表操作栏下的“上传文件”按钮，可以上传对象文件。如下图所示：

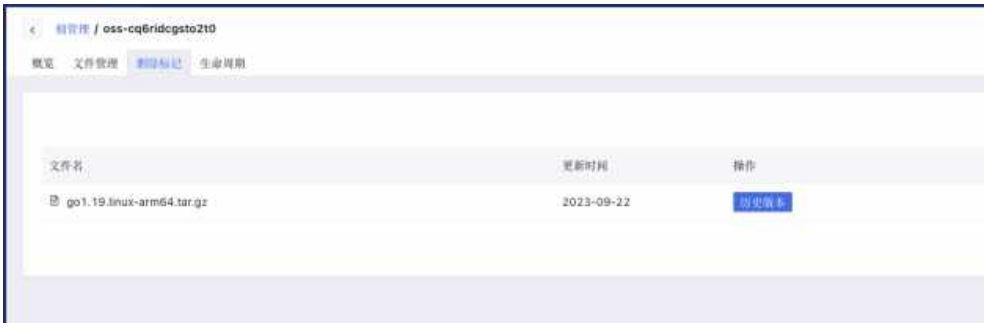
点击列表操作栏下的“创建目录”按钮，可以在文件管理页创建目录。如下图所示：

点击列表操作栏下的“上传列表”按钮，可以在文件管理页中没有上传成功的文件继续上传。如下图所示：

点击列表操作栏下的“清空当前桶”按钮，可以把存储桶中的所有文件、历史版本、文件碎片、删除后数据不可恢复和访问。如下图所示：

5.5.16.3.7 删除标记

在“删除标记”分页，会展示已删除对象的历史版本。如下图所示：



5.5.16.3.8 生命周期

支持用户为桶设置生命周期，生命周期扫描程序根据系统判断和负载情况自动启动，处理过期对象可能存在一定延迟。

生命周期规则列表页，如下图所示：

支持租户**创建生命周期规则**，未开多版本时支持设置整个存储桶/指定前缀，过期类型为当前版本的过期天数，如下图所示：

支持租户**创建生命周期规则**，开启多版本支持设置整个存储桶/指定前缀，过期类型为当前版本/非当前版本的过期天数，如下图所示：

支持租户**编辑生命周期规则**，如下图所示：

支持租户**删除生命周期规则**，如下图所示：

5.5.17 令牌管理

令牌管理可以根据用户的需求灵活的开放存储空间和文件管理权限。

一个令牌由一对特殊的公私钥组成。其中包括了：允许操作的存储空间列表、允许操作的文件前缀列表、操作权限和令牌过期时间等属性。

用户可以按需申请不同令牌来完成不同权限的管控。

5.5.17.1 令牌管理列表

在桶管理页面点击左侧菜单“令牌管理”，即可进入存储桶令牌管理列表。如下图所示：

每行表示一个令牌，令牌管理列表中显示的信息包括：

- 名称：令牌名称；
- 公钥：公钥；
- 私钥：私钥；
- 权限：令牌的操作权限有上传、下载、删除、文件列表；
- 桶名称：桶名称；
- 授权的文件前缀：允许操作的文件前缀列表；
- IP 白名单：允许操作的客户端 ip；
- IP 黑名单：不需要操作的客户端 ip；
- 过期时间：令牌的过期时间，格式：YYYY-MM-DD；
- 操作：支持对令牌修改和删除操作。

5.5.17.2 令牌管理相关操作

存储用户相关操作包括：

- 创建令牌
- 修改令牌信息

- 删除和批量删除令牌

5.5.17.2.1 创建令牌

点击管理菜单左上角“创建”按钮，弹出创建令牌对话框。如下图所示：

用户需要填写以下信息：

- 令牌名称：用户输入令牌名称；
- 过期时间：令牌的过期时间，格式：YYYY-MM-DD；
- 授权的存储空间：桶名称；
- IP 白名单：允许操作的客户端 ip；
- IP 黑名单：不需要操作的客户端 ip；
- 授权的文件前缀：允许操作的文件前缀列表；
- 令牌权限：令牌的操作权限有上传、下载、删除、文件列表。

填写完成后，点击“确定”按钮，即可完成对象存储令牌的创建。

5.5.17.2.2 修改令牌

点击操作栏“修改”按钮，弹出修改令牌对话框。如下图所示：

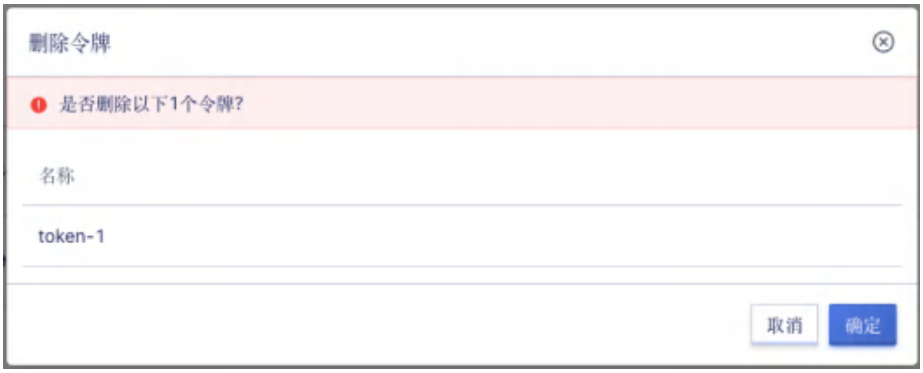
用户需要填写以下信息：

- 过期时间：令牌的过期时间，格式：YYYY-MM-DD；
- 授权的存储空间：桶名称；
- IP 白名单：允许操作的客户端 ip；
- IP 黑名单：不需要操作的客户端 ip；
- 授权的文件前缀：允许操作的文件前缀列表；
- 令牌权限：令牌的操作权限有上传、下载、删除、文件列表；

填写完成后，点击“确定”按钮，即可完成对象存储令牌的更新。

5.5.17.2.3 删除令牌

点击操作栏“删除”按钮，弹出删除令牌对话框。如下图所示：



点击“确定”按钮，即可完成对象存储令牌的删除。

5.5.18 MinIO Client 常用命令

mc version	输出 mc 版本
mc ls play	列出所有 https://play.min.io 上的存储桶
mc mb play/mybucket	创建一个名叫"mybucket"的存储桶
mc cat play/mybucket/myobject.txt	显示 myobject.txt 文件的内容
mc cp myobject.txt play/mybucket	拷贝一个文本文件到对象存储
mc rm play/mybucket/myobject.txt	删除一个对象
mc find s3/bucket --name "*.jpg" --watch --exec "mc cp {} play/bucket"	持续从 s3 存储桶中查找所有 jpeg 图像，并复制到 minio "play/bucket"存储桶

5.6 文件存储

5.6.1 文件存储概述

文件存储是云平台提供的 NFS 文件服务器，可以与虚拟机实例和本地服务器搭配使用。文件存储提供了标准的 NFS 文件访问协议，协议版本为 NFSv4，支持 POSIX 文件接口。

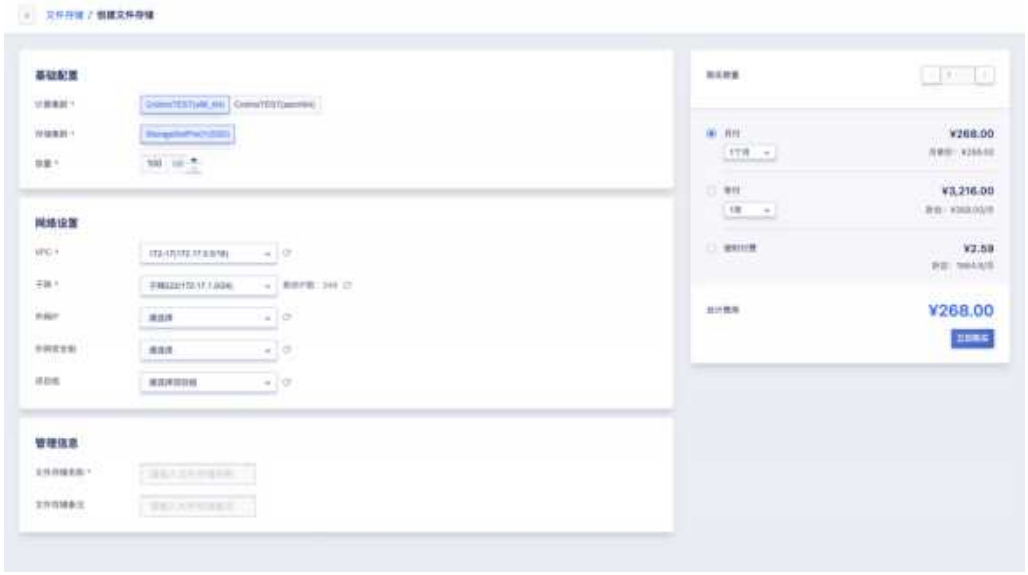
用户在控制台创建文件存储实例后，只需在虚拟机实例中安装文件存储客户端，使用标准挂载命令挂载创建的文件系统，就可以轻松地在多个实例间共

享文件。

5.6.2 创建文件存储

云平台用户可以通过指定计算集群、存储集群、容量、VPC、子网、外网IP、外网安全组、项目组、文件存储名称等相关基础信息创建文件存储。

可通过导航栏进入【文件存储】资源控制台，通过“创建”进入向导页面，如下图所示：



1. 选择并配置文件存储的基础配置、网络设置及管理配置信息：

   - 名称/备注：申请文件存储的名称和备注，申请时必须指定名称；
   - 容量：支持的容量范围为 100~1024 GB；
   - 创建文件存储时必须选择 VPC 网络和所属子网，即选择要加入的网络及 IP 网段；
   - 外网 IP 为文件存储提供外网挂载服务，支持创建文件存储时申请并绑定一个外网 IP 作为外网挂载地址。平台支持 IPv4/IPv6 双栈网络，也可在文件存储创建成功后为文件存储绑定多个外网 IP 地址，最多支持绑定 50 个 IPv4 和 10 个 IPv6 外网 IP 地址。

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”进行文件存储的

创建：

- 购买数量：默认支持创建 1 个文件存储；
- 付费方式：选择文件存储的计费方式，支持按月、按年、按时三种方式，可根据需求选择合适的付费方式；
- 合计费用：用户选择文件存储资源按照付费方式的费用展示；
- 立即购买：点击立即购买后，会返回文件存储资源列表页，在列表页可查看文件存储的创建过程，通常会先显示“初始化”的状态，几秒内转换为“可用”状态，即代表创建成功。

5.6.2.1 通过内网挂载文件存储

用户可通过文件存储列表的内网挂载地址挂载文件存储服务：

```
# mkdir /datanfs
# yum install-y nfs-utils
# mount-t nfs4 10.0.0.28://datanfs
```

5.6.2.2 通过外网挂载文件存储

用户可通过文件存储列表的外网挂载地址挂载文件存储服务：

```
# mkdir/datanfs
# yum install-y nfs-utils
# mount-t nfs4 192.168.179.179://datanfs
```

5.6.3 文件存储列表

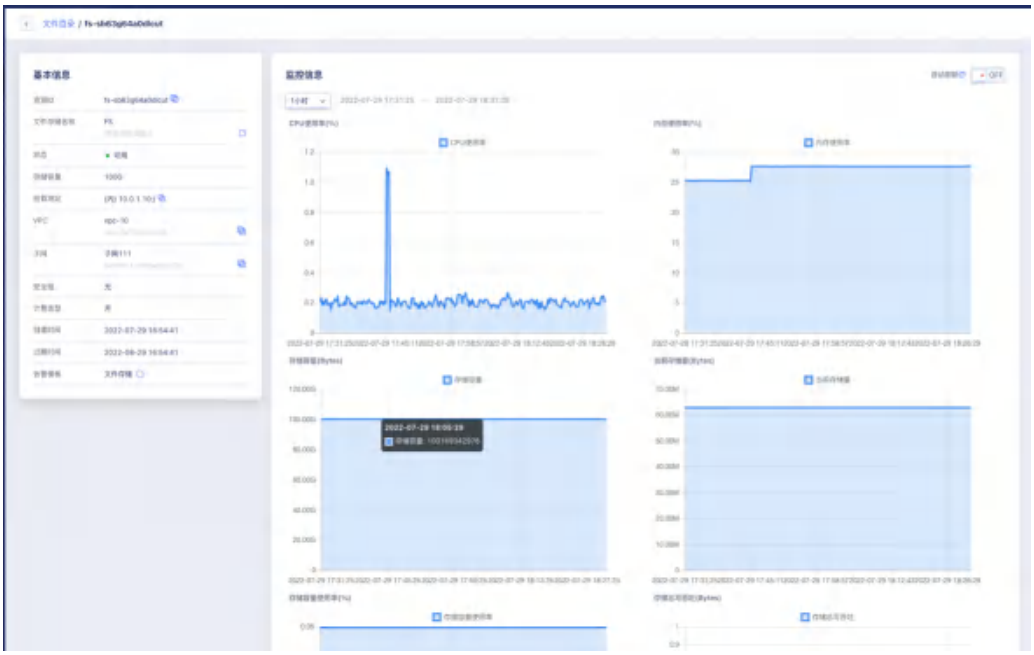
通过导航栏进入文件存储控制台，可查看文件存储资源列表。

文件存储列表可查看当前账户下所有文件存储资源的列表信息，包括名称、资源 ID、状态、存储容量、挂载地址、VPC、子网、计费方式、项目组、创建时间、过期时间及操作项，如下图所示：

- 名称：文件存储资源的名称；
- 资源 ID：文件存储的资源 ID 作为全局唯一标识符；
- 状态：文件存储资源的状态，包括初始化、可用、删除中等状态；
- 存储容量：文件存储的内存容量，容量范围为 100~1024 GB；
- 挂载地址：可通过内网/外网挂载地址挂载文件存储服务；
- VPC/子网：文件存储创建时所指定的 VPC 网络和子网，即文件存储内网 IP 所在的 VPC 网络和子网信息；
- 计费方式：文件存储的付费方式，包括按时、按年、按月；
- 项目组：文件存储创建时所绑定的项目组；
- 创建时间/过期时间：文件存储资源的创建时间和费用过期时间；
- 操作：列表上的操作项是对单个文件存储的操作，包括扩容、绑定、解绑、续费及删除。

5.6.4 查看文件存储详情

用户可通过点击列表的名称进入文件存储详情页，查看基本信息和监控信息，基本信息包括资源 ID、文件存储名称、状态、存储容量、挂载地址、VPC、子网、安全组、计费类型创建时间及过期时间，监控信息包括 CPU 使用率、内存使用率、存储容量、当前存储量、存储容量使用率、存储总写吞吐及存储总读吞吐，如下图所示：



5.6.5 文件存储扩容

平台支持用户扩容文件存储的容量，适应于业务发生变化需扩容文件存储容量的场景。平台仅支持扩容文件存储容量，不支持文件存储容量的缩容。

文件存储容量扩容范围即当前硬盘类型的规格，默认为 100GB~1024 GB。

扩容文件存储容量会对费用产生影响，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。用户可点击文件存储控制台操作中的“扩容”进行容量扩容操作，如下图所示：

如图所示，更改容量，即文件存储需要扩容的容量。平台已展示当前文件存储的容量大小，由于不支持缩容，扩容时更改容量必须大于当前容量大小。用户可通过文件存储列表查看新容量。

5.6.6 绑定外网 IP

绑定外网 IP 是指将 EIP 地址绑定至文件存储，用户可通过外网挂载地址使用文件存储服务。

用户可通过文件存储资源列表操作项的“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的弹性 IP，绑定成功后，文件存储列表的挂载地址会新增外网挂载地址。

5.6.7 解绑外网 IP

解绑外网 IP 是指将 EIP 地址从一个文件存储资源上分离出来，并可重新绑定至其它虚拟资源。仅支持解绑已绑定文件存储的外网 IP 资源，用户可通过文件存储资源列表操作项的“解绑”进入外网 IP 解绑向导页面，进行资源解绑操作，如下图所示：

5.6.8 文件存储续费

支持用户手动对文件存储进行续费。文件存储续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

文件存储续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当文件存储的计费方式为【小时】，则续费时长可指定为 1 小时；当文件存储的计费方式为【按月】，则续费时长可选择 1 至 11 月；当文件存储的计费方式为【按年】，则续费时长为 1 至 5 年。可通过文件存储列表操作项中的“续费”进行操作，如下图所示：

5.6.9 修改文件存储告警模板

用户可在控制台修改文件存储的告警模板。可通过文件存储列表操作项中的“修改告警模板”按钮进行操作，如下图所示：

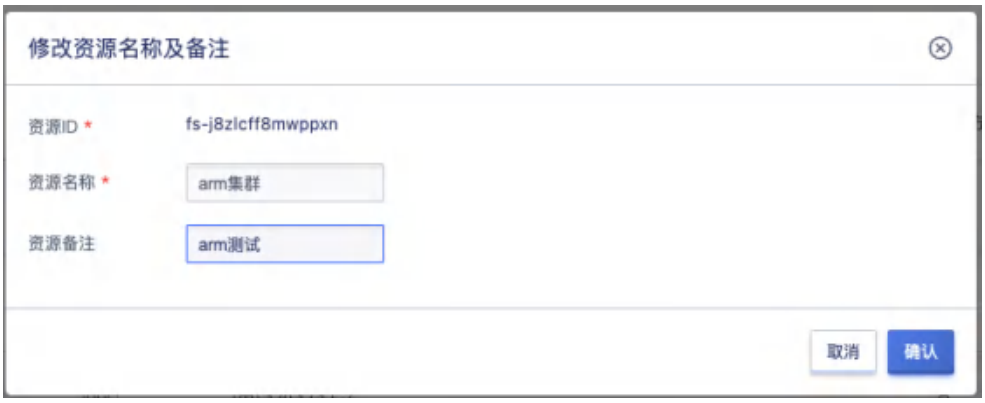
5.6.10 搜索文件存储

用户可通过搜索框对文件存储列表进行搜索和筛选，支持从名称、备注、

资源 ID、挂载地址进行模糊搜索，如下图所示：

5.6.11 修改文件存储名称与备注

修改文件存储的名称和备注。可通过点击文件存储列表名称右侧的“编辑”按钮进行修改，如下图所示：

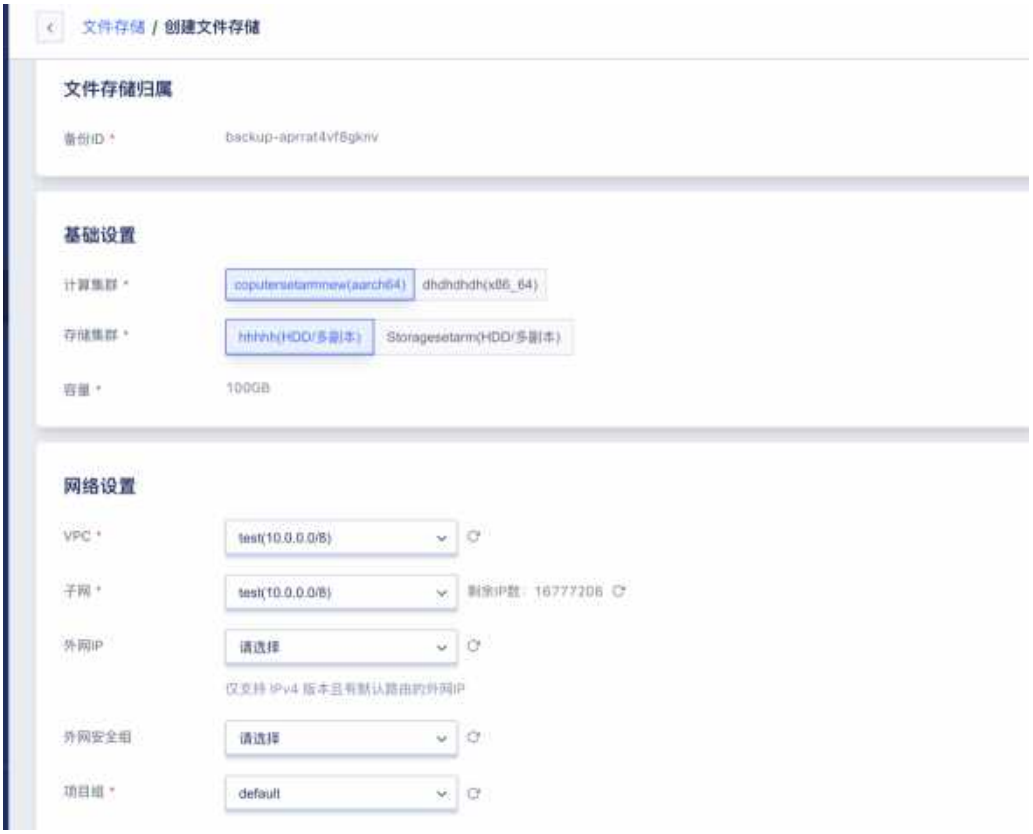


5.6.12 修改 IP

支持用户修改文件存储的内网 IP 地址。

5.6.13 从备份创建

支持用户从备份创建新实例。



5.6.14 删除文件存储

用户可在控制台删除账户内文件存储，支持对文件存储进行批量删除操作。可通过文件存储列表操作项中的“删除”进行操作，如下图所示：

5.6.15 文件管理

支持用户查看文件存储中的文件，并进行管理操作，页面如下图所示：

在“文件管理”分页，点击列表操作栏下的“上传文件”按钮，可以从本地上传文件，如下图所示：

点击列表操作栏下的“创建目录”按钮，可以在文件管理页创建目录，如下图所示：

点击文件列表的“删除”按钮，可删除对应的文件，也支持批量删除，如下图所示：

6 网络服务

6.1 VPC 网络

6.1.1 VPC 网络简介

6.1.1.1 VPC 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 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 NFV 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。

提示：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。

6.1.1.2 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（10.0.0.0/8 网段需在系统管理-全局配置-产品策略中自行配置）：

网段	掩码范围	IP 地址范围	默认配置/可配置项
10.0.0.0/8	8 ~ 29	10.0.0.0 - 10.255.255.255	可配置项
10.0.0.0/16	16 ~ 29	10.0.0.0 - 10.10.255.255	默认配置
172.16.0.0/16～ 172.29.0.0/16	16 ~ 29	172.16.0.0 - 172.29.255.255	可配置项
192.168.0.0/16	16 ~ 29	192.168.0.0 - 192.168.255.255	默认配置

注意：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

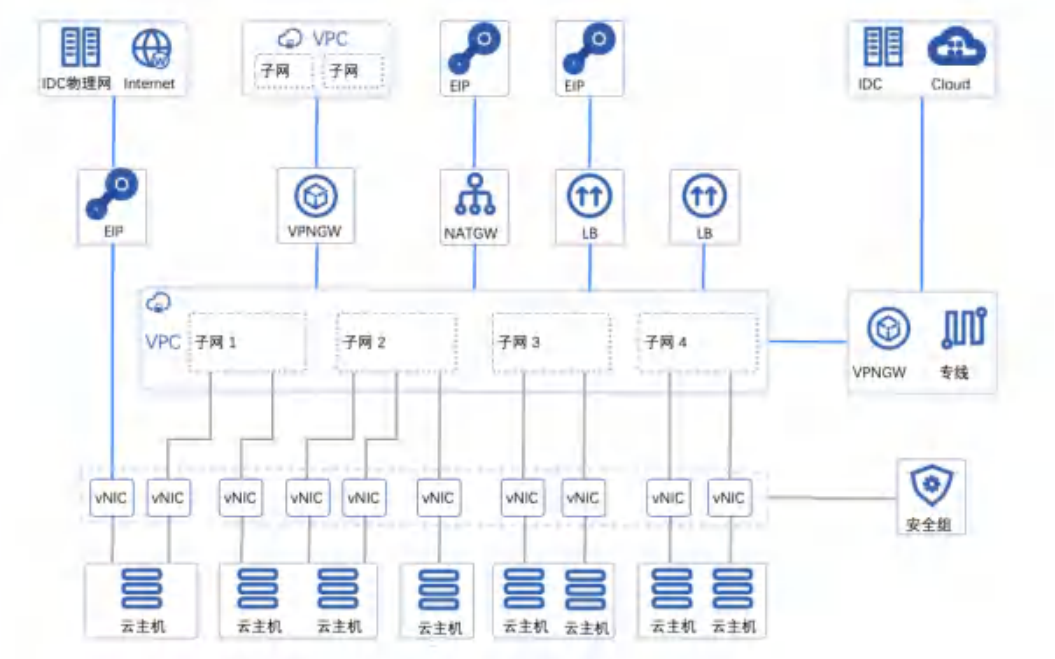
网连接。

- 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 网段拔码最小为 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。

6.1.1.3 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。
- 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 LB 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 LB 后端服务节点，结合 LB 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。

6.1.1.4 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。

6.1.2 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：

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。
- 项目组：VPC 网段所属的项目组，可用于 VPC 网络的分组及权限控制。

VPC 网络创建时状态为“创建中”，待状态转换为“可用”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。

6.1.3 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。

6.1.3.1 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：

- 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，一般为可用；
- 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。

6.1.3.2 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：

（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。

（3）子网路由管理

子网路由页面展示当前子网下的路由规则列表，包括目的地址、下一跳类型、下一跳、备注及对路由规则的操作，其中下一跳类型指虚拟机、vip 和自定义类型。

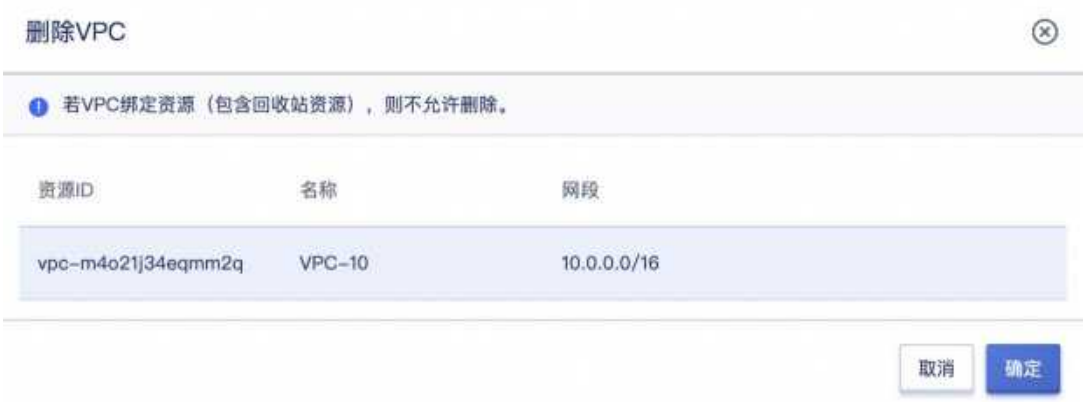
路由列表上的操作项是可对单个路由进行删除操作，平台支持路由的批量创建与删除操作。

6.1.4 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。

6.1.5 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：



6.1.6 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“可用”，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。

6.1.7 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：

6.1.8 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。

6.1.9 添加子网路由

路由策略用于控制子网出流量的走向，用户从子网详情页上的“路由策略”按钮，进入路由列表，可通过目的地址、下一跳类型、下一跳及备注创建路由策略。

- 目的端口

目的端即为您要转发到的目标网段，目的网段描述仅支持网段格式，如果您希望目的端为单个 IP，可设置掩码为 32（例如 172.16.1.1/32）。

- 下一跳类型：

下一跳类型	说明
Local	不可编辑，提供 VPC 互通能力
NAT 网关	NAT 网关，不可编辑，NATGW 下发的路由
IPSecVPN	IPSecVPN，不可编辑，IPSecVPN 下发的路由
公共服务	公共服务，不可编辑
VIP	VIP，可编辑，VIP
虚拟机	虚拟机，可编辑，虚拟机资源
自定义	自定义，可编辑，自定义地址

- 下一跳

指定具体跳转到的下一跳实例，如网关或云服务器 IP 等。

- 备注

可自行添加路由条目的描述信息，便于资源管理。

6.1.10 修改子网路由

用户可通过路由列表上的“修改”功能修改当前的路由策略

6.1.11 删除子网路由

用户可通过路由列表上的“删除”功能删除当前的路由策略。

6.1.12 子网网络拓扑

用户可通过子网拓扑页面查看子网使用情况，下图为缩略状态。

用户可通过右侧列表按钮，查看子网详细使用情况，如下图所示。

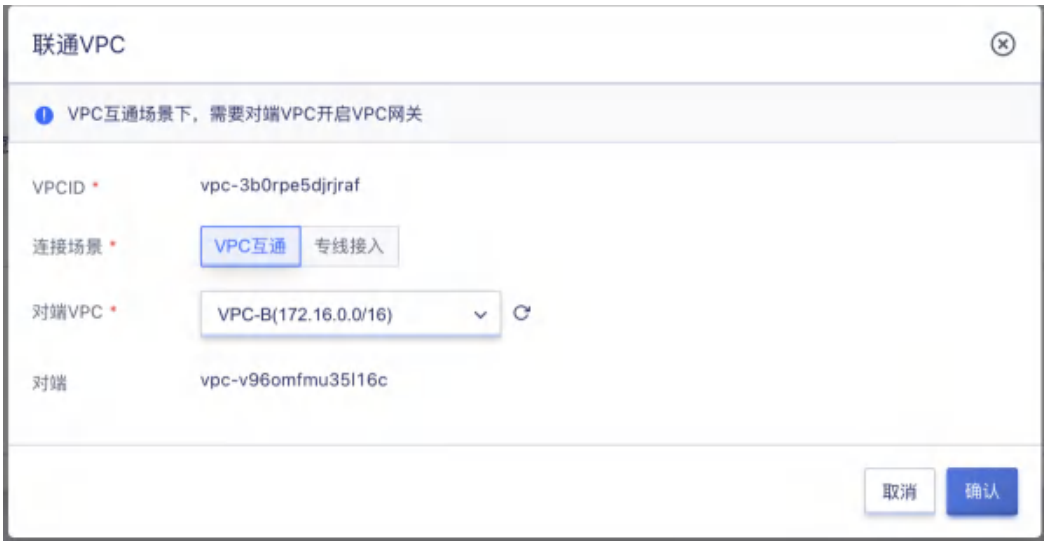
6.2 VPC 网络互通

网络互通功能用于实现同租户两个 VPC 之间的网络互通，租户可以通过网络互通功能将两个 VPC 之间建立连接，如此就可以使用私有 IP 地址在两个 VPC 之间进行通信，就像两个 VPC 在同一个网络中一样。

6.2.1 联通网络

（1）联通网络的前提是开启 VPC 网关，如下图所示：

（2）联通页面如下：



- VPCID：当前 VPC 的 ID。
- 连接场景：“VPC 互通”可以直接使用，用于同租户不同 VPC 之间的互联；“专线接入”需要在管理侧创建专线才可使用。
- 对端 VPC：与当前 VPC 建立连接的 VPC，也需要开启 VPC 网关。

6.2.2 查看列表

通过 VPC 网络互通列表可查看 VPC 已互通的 VPC 列表及信息，如下图：

6.2.3 断开网络

用户可以通过操作列的“断开”按钮单独断开连接，**也可以通过选中后批量断开连接。**

6.2.4 约束与限制

- 配置网络互通时，两端 VPC 的网段（CIDR）不能重叠，否则可能会造成路由冲突，导致配置不生效。
- 两个 VPC 之间不能同时建立多个 VPC 连接。
- VPC 中存在连接时，VPC 网关不能关闭。

6.3 安全组

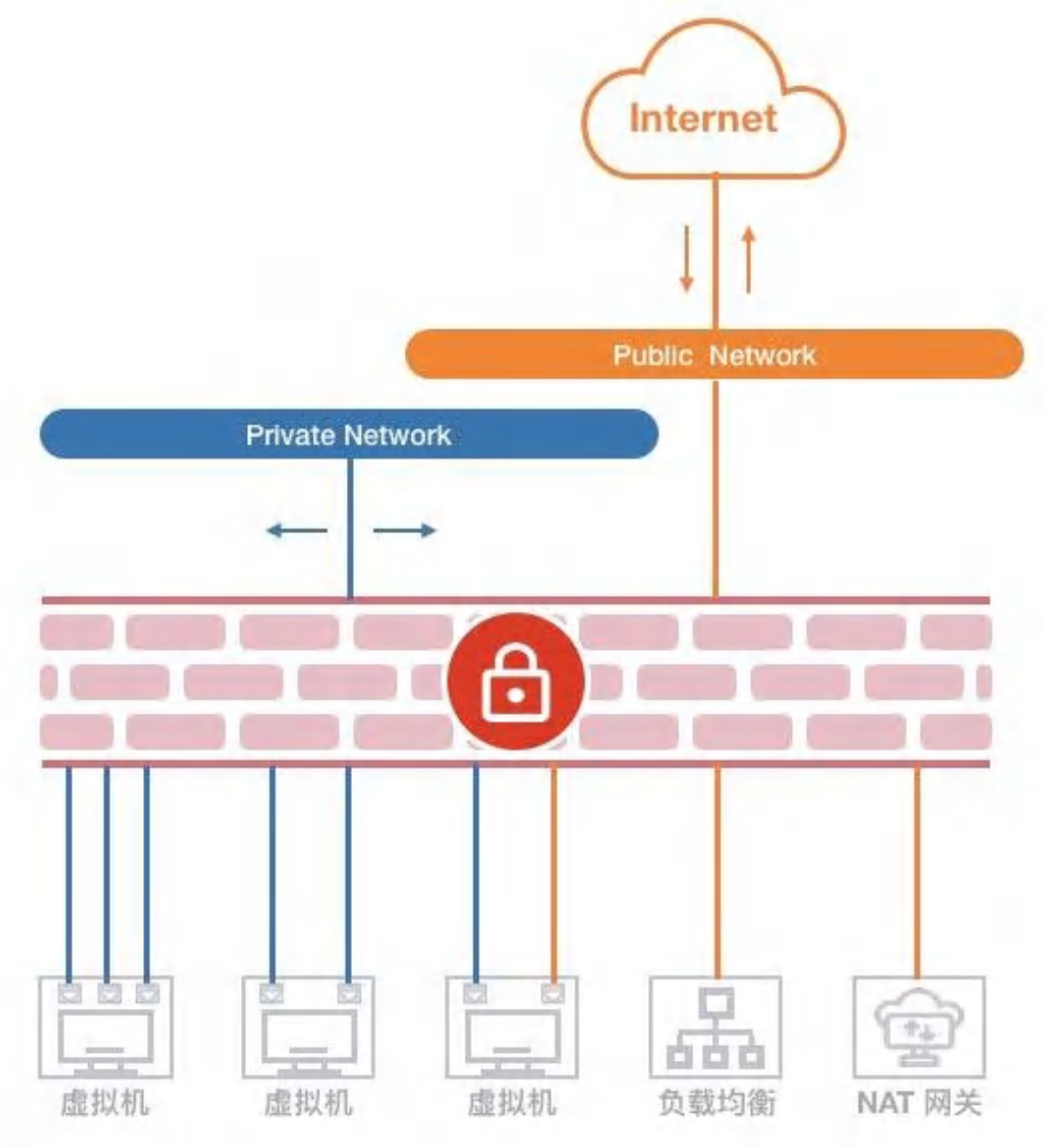
6.3.1 安全组简介

6.3.1.1 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，需开启计算节点 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。

创建虚拟机时支持指定外网安全组，允许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。

6.3.1.2 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、UPD、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、动作的规则，优先生效先添加的规则；同优先级，不同动作的规则，默认生效拒绝规则。
- 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。

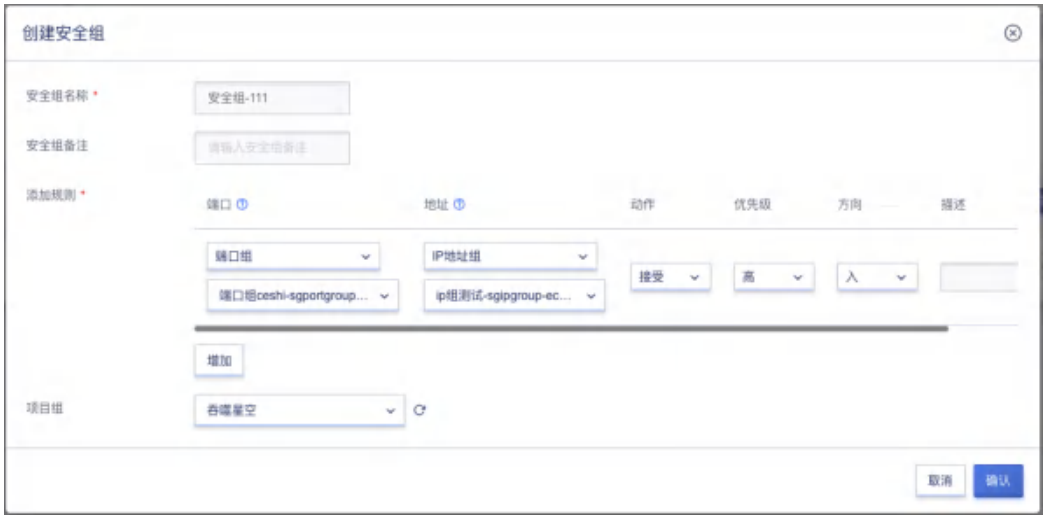
注：通常建议设置简洁的安全组规则，可有效减少网络故障。

6.3.2 安全组管理

6.3.2.1 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：



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、方向及描述等。

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：端口支持选择自定义端口或端口组，端口组列表展示当前租户下创建的端口组，可到端口组页面进行创建操作。
- 地址：地址栏支持选择自定义 IP 或 IP 地址组，IP 地址组列表展示当前租户下创建的 IP 组，可到 IP 组页面进行创建操作。
- 动作：规则的协议、端口、地址及方向相同时，若同时配置接受和拒绝两种动作，默认生效拒绝。
- 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。
- 描述：指当前安全组规则的描述。

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“可用”时，即代表创建成功。

6.3.2.2 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。

6.3.2.3 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：

- 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，包括可用、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。

6.3.2.4 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：

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。

已绑定资源：当前安全组已绑定资源的列表信息，详见。

6.3.2.5 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。

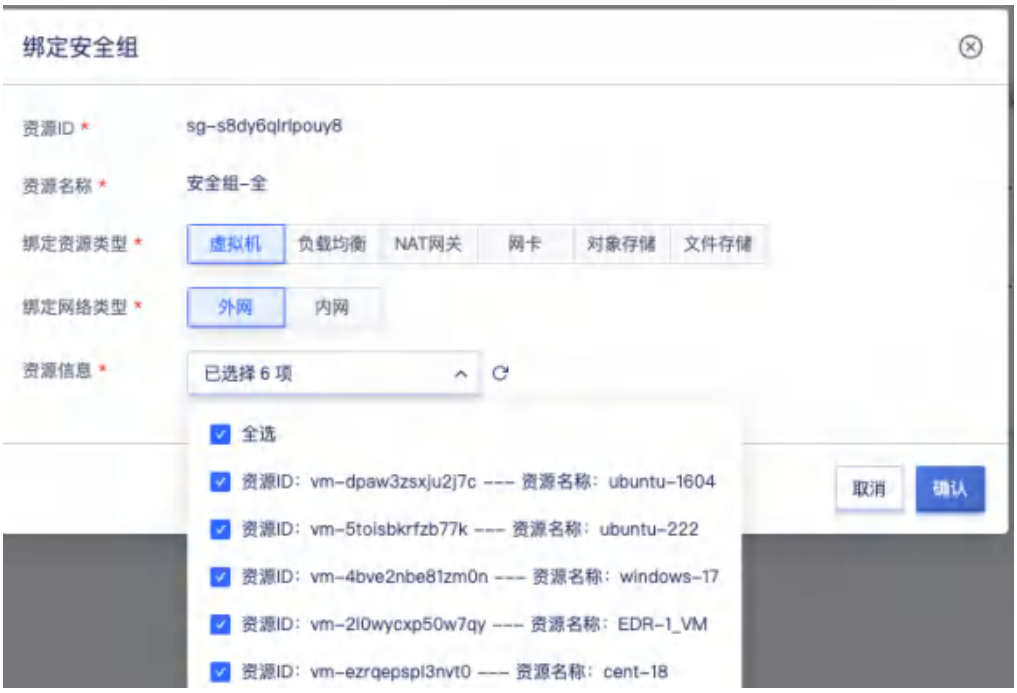
如上图列表图所示，已绑定资源的列表信息包括资源名称、资源类型、资源 ID 等信息，其中资源类型包括虚拟机、弹性网卡、NAT 网关、负载均衡等。

6.3.2.6 批量绑定虚拟资源

支持用户批量绑定安全组至虚拟资源，已绑定的资源可在安全组的详情页

“资源”子页面进行查看。用户可通过安全组列表操作栏的“绑定”按钮进入绑定安全组向导页。

1、支持虚拟机绑定内网和外网安全组，如下图所示：



- 资源 ID：安全组的全局唯一标识符；
- 资源名称：安全组的名称；
- 绑定资源类型：安全组支持绑定的资源类型，包括虚拟机、负载均衡、NAT 网关、网卡、对象存储及文件存储；
- 绑定网络类型：安全组支持绑定虚拟机的网络类型，包括外网和内网；
- 资源信息：资源信息列表展示虚拟机资源列表，可多选。

2、支持负载均衡绑定安全组，如下图所示：

- 资源 ID：安全组的全局唯一标识符；
- 资源名称：安全组的名称；
- 绑定资源类型：安全组支持绑定的资源类型，包括虚拟机、负载均衡、NAT 网关、网卡、对象存储及文件存储；
- 资源信息：资源信息列表展示负载均衡资源列表，可多选。

3、支持 nat 网关绑定安全组，如下图所示：

- 资源 ID：安全组的全局唯一标识符；
- 资源名称：安全组的名称；
- 绑定资源类型：安全组支持绑定的资源类型，包括虚拟机、负载均衡、NAT 网关、网卡、对象存储及文件存储；

- 资源信息：资源信息列表展示 NAT 网关资源列表，可多选。

4、支持网卡绑定安全组，如下图所示：

- 资源 ID：安全组的全局唯一标识符；
- 资源名称：安全组的名称；
- 绑定资源类型：安全组支持绑定的资源类型，包括虚拟机、负载均衡、NAT 网关、网卡、对象存储及文件存储；
- 资源信息：资源信息列表展示网卡资源列表，可多选。

5、支持对象存储绑定安全组，如下图所示：

- 资源 ID：安全组的全局唯一标识符；

- 资源名称：安全组的名称；
- 绑定资源类型：安全组支持绑定的资源类型，包括虚拟机、负载均衡、NAT 网关、网卡、对象存储及文件存储；
- 资源信息：资源信息列表展示对象存储资源列表，可多选。

6、支持文件存储绑定安全组，如下图所示：

- 资源 ID：安全组的全局唯一标识符；
- 资源名称：安全组的名称；
- 绑定资源类型：安全组支持绑定的资源类型，包括虚拟机、负载均衡、NAT 网关、网卡、对象存储及文件存储；
- 资源信息：资源信息列表展示文件存储资源列表，可多选。

6.3.2.7 批量解绑资源

支持用户批量解绑安全组，可通过安全组列表操作栏的“解绑”按钮进入解绑安全组向导页，如下图所示：

- 资源 ID：安全组的全局唯一标识符；
- 资源名称：安全组的名称；
- 解绑资源：展示支持解绑的资源列表，可多选。

6.3.2.8 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。

6.3.2.9 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：

6.3.3 安全组规则管理

6.3.3.1 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、方向及描述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。

6.3.3.2 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、描述、创建时间及操作项等，如下图所示：

6.3.3.3 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。

6.3.3.4 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。

6.3.4 IP 组管理

6.3.4.1 创建 IP 组

可根据向导页面的提示，创建并配置 IP 组，包括 IP 组名称、IP 地址、IP 组备注及项目组等。

其中 IP 组名称指当前需要创建的 IP 组的名称标识，IP 地址可增加多条，如下图所示：

- IP 组名称：IP 组的名称；
- IP 地址：地址栏支持批量输入多个 IP 地址，多个 IP 地址换行输入，IP 支持以下格式:
  - 单个 IP:10.0.0.1 或 FF05::B5
  - 网段:10.0.1.0/24
  - 连续地址段:10.0.0.1-10.0.0.100
- IP 组备注：当前 IP 组的备注；
- 项目组：可绑定当前租户下创建的项目组。

点击确定后，自动返回至 IP 组列表页面，IP 组的状态为“可用”时，即代表创建成功。

6.3.4.2 查看 IP 组

用户查看已创建的 IP 组信息，包括名称、资源 ID、IP/网段、绑定资源数

量、项目组、创建时间及操作项，如下图所示：

- 名称：IP 组的名称；
- 资源 ID：IP 组的全局唯一标识符；
- 状态：IP 组的状态，包括可用、失败；
- IP/网段：源数据（入站）或目标数据（出站）的 IP，地址的形式为 IP 地址、网段或连续地址段，例如 10.0.0.1 或 192.168.0.0/16；
- 绑定资源数量：IP 组绑定资源的数量，可以悬浮查看到具体的安全组规则 ID 列表，点击相应安全组 ID 可以跳到该安全组详情列表；
- 项目组：IP 组绑定的项目组；
- 创建时间：IP 组的创建时间。

列表上操作项是指对单条 IP 组的操作，包括编辑和删除，仅当 IP 组绑定资源数量为 0 时，才可进行删除操作；同时为方便租户对资源的维护支持对端口组进行批量删除操作。

6.3.4.3 编辑 IP 组

支持用户编辑 IP 组的 IP 地址，IP 组名称不可修改，可通过点击 IP 组列表操作栏的“编辑”按钮进行修改，如下图所示：

6.3.4.4 删除 IP 组

用户可在控制台删除账户内 IP 组，支持对 IP 组进行批量删除操作。可通过 IP 组列表操作项的“删除”进行操作，如下图所示：

6.3.5 端口组管理

6.3.5.1 创建端口组

可根据向导页面的提示，创建并配置端口组，包括端口组名称、协议端口及项目组等。

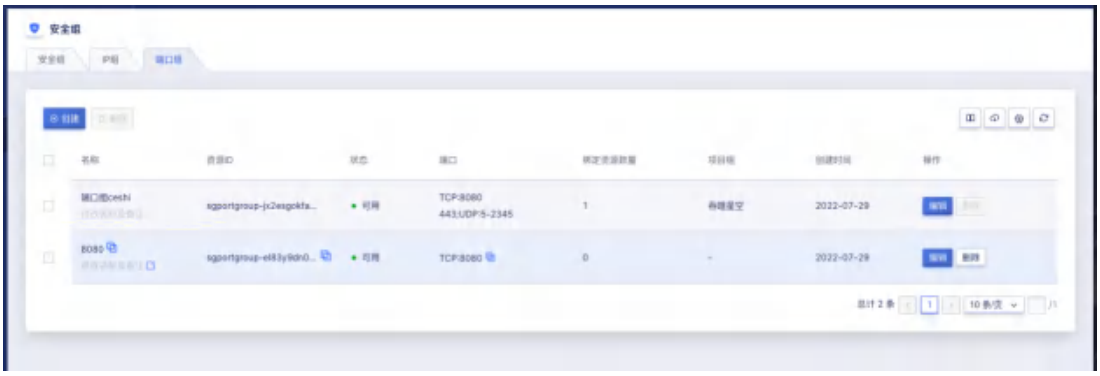
其中端口组名称指当前需要创建的端口组的名称标识，协议端口可增加多条，如下图所示：

- 端口组名称：IP 组的名称；
- 协议端口：支持换行输入多个协议端口，端口支持以下格式:
  - 单个端口:80
  - 多个单个端口:80,443
  - 连续端口段:3306-20000
- 项目组：可绑定当前租户下创建的项目组。

点击确定后，自动返回至端口组列表页面，端口组的状态为“可用”时，即代表创建成功。

6.3.5.2 查看端口组

用户查看已创建的端口组信息，包括名称、资源 ID、端口、绑定资源数量、项目组、创建时间及操作项，如下图所示：



- 名称：端口组的名称；
- 资源 ID：端口组的全局唯一标识符；
- 状态：端口组的状态，包括可用、失败；
- 端口：以协议：端口格式展示，协议类型如 TCP、UDP 等，源数据（入站）或目标数据（出站）的端口，值范围：1-65535；
- 绑定资源数量：端口组绑定资源的数量，可以悬浮查看到具体的安全组规则 ID 列表，点击相应安全组 ID 可以跳到该安全组详情列表；
- 项目组：端口组绑定的项目组；
- 创建时间：端口组的创建时间。

列表上操作项是指对单条端口组的操作，包括编辑和删除，仅当端口组绑定资源数量为 0 时，才可进行删除操作；同时为方便租户对资源的维护支持对端口组进行批量删除操作。

6.3.5.3 编辑端口组

支持用户编辑端口组的协议端口，端口组名称不可修改，可通过点击端口组列表操作栏的“编辑”按钮进行修改，如下图所示：

6.3.5.4 10.5.4 删除端口组

用户可在控制台删除账户内端口组，支持对端口组进行批量删除操作。可通过端口组列表操作项的“删除”进行操作，如下图所示：

6.4 组播

6.4.1 组播概述

作为一种与单播（Unicast）和广播（Broadcast）并列的通信方式，组播（Multicast）技术能够有效地解决单点发送、多点接收的问题，从而实现了网络中点到多点的高效数据传送，能够节约大量网络带宽、降低网络负载。

利用网络的组播特性方便地提供一些新的增值业务，包括在线直播、网络

电视、远程教育、远程医疗、网络电台、实时视频会议等互联网的信息服务领域。

组播是主机间一对多的通讯模式， 组播是一种允许一个或多个组播源发送同一报文到多个接收者的技术。组播源将一份报文发送到特定的组播地址，组播地址不同于单播地址，它并不属于特定某个主机，而是属于一组主机。一个组播地址表示一个群组，需要接收组播报文的接收者都加入这个群组。

- **组播组概述**

用 IP 组播地址进行标识的一个集合。任何用户主机（或其他接收设备），加入一个组播组，就成为该组成员，可以识别并接收发往该组播组的组播数据。

- **组播源概述**

信息的发送者称为“组播源”，一个组播源可以同时向多个组播组发送数据，多个组播源也可以同时向一个组播组发送报文。组播源通常不需要加入组播组，由源端 DR 负责管理组播源的注册和 SPT（Shortest Path Tree）的建立。

- **29.1.4 组播组成员概述**

所有加入某组播组的主机便成为该组播组的成员，组播组中的成员是动态的，主机可以在任何时刻加入或离开组播组。组播组成员可以广泛地分布在网络中的任何地方。

- **29.1.5 组播路由器概述**

支持三层组播功能的路由器或交换机。组播路由器不仅能够提供组播路由功能，也能够在与用户连接的末梢网段上提供组播组成员的管理功能。

- **29.1.6 IPv4 组播地址**

IANA（Internet Assigned Numbers Authority，互联网编号分配委员会）将 D 类地址空间分配给 IPv4 组播使用。IPv4 地址一共 32 位，D 类地址最高 4 位为 1110，因此地址范围从 224.0.0.0 到 239.255.255.255，具体分类及含义详见下表描述：

地址范围	含义
224.0.0.0～224.0.0.255	永久组地址。IANA 为路由协议预留的 IP 地址（也称为保留组地址），用于标识一组特定的网络设备，供路由协议、拓扑查找等使用，不用于组播转发。
224.0.1.0～ 231.255.255.255 233.0.0.0～ 238.255.255.255	ASM 组播地址，全网范围内有效。说明： 其中，224.0.1.39 和 224.0.1.40 是保留地址，不建议使用。
232.0.0.0～ 232.255.255.255	缺省情况下的 SSM 组播地址，全网范围内有效。
239.0.0.0～ 239.255.255.255	本地管理组地址，仅在本地管理域内有效。在不同的管理域内重复使用相同的本地管理组地址不会导致冲突。

- **组播转发机制**

在组播模型中，IP 报文的目的地址字段为组播组地址，组播源向以此目的地址所标识的主机群组传送信息。因此，转发路径上的组播路由器为将组播报文传送到各个方位的接收站点，往往需要将从一个入接口收到的组播报文转发到多个出接口。

为保证组播报文在网络中的传输，必须依靠单播路由表或者单独提供给组播使用的路由表（如 MBGP 路由表）来指导转发；

为处理同一设备在不同接口上收到来自不同对端的相同组播信息，需要对组播报文的入接口进行 RPF（Reverse Path Forwarding，逆向路径转发）检查，以决定转发还是丢弃该报文。RPF 检查机制是大部分组播路由协议进行组播转发的基础。

6.4.2 创建组播

云平台用户可以通过指定 VPC、组播组 IP、组播组端口、发送方机器、接

收方机器、项目组、组播名称等相关基础信息创建组播。

可通过导航栏进入【组播】资源控制台，通过“创建”进入向导页面，如下图所示：

选择并配置组播的基础配置：

- 规则名称/备注：申请组播的名称和备注，申请时必须指定名称
- 组播组 IP：组播 IP 仅支持 224.0.0.0/4 网段内的 IP
- 组播组端口：组播组端口需要用户指定，端口默认范围为 10000-64999
- VPC：创建组播时必须选择 VPC 网络，即选择要加入的网络
- 发送方：发送和接收方为相同 VPC 下的虚拟机，发送方为单一虚拟机
- 接收方：发送和接收方为相同 VPC 下的虚拟机，接收方可以为多个虚拟机

注意：单个 VPC 可以添加的组播组规则限制为 9 个，一个组播组接收方数量限制为 9 个。

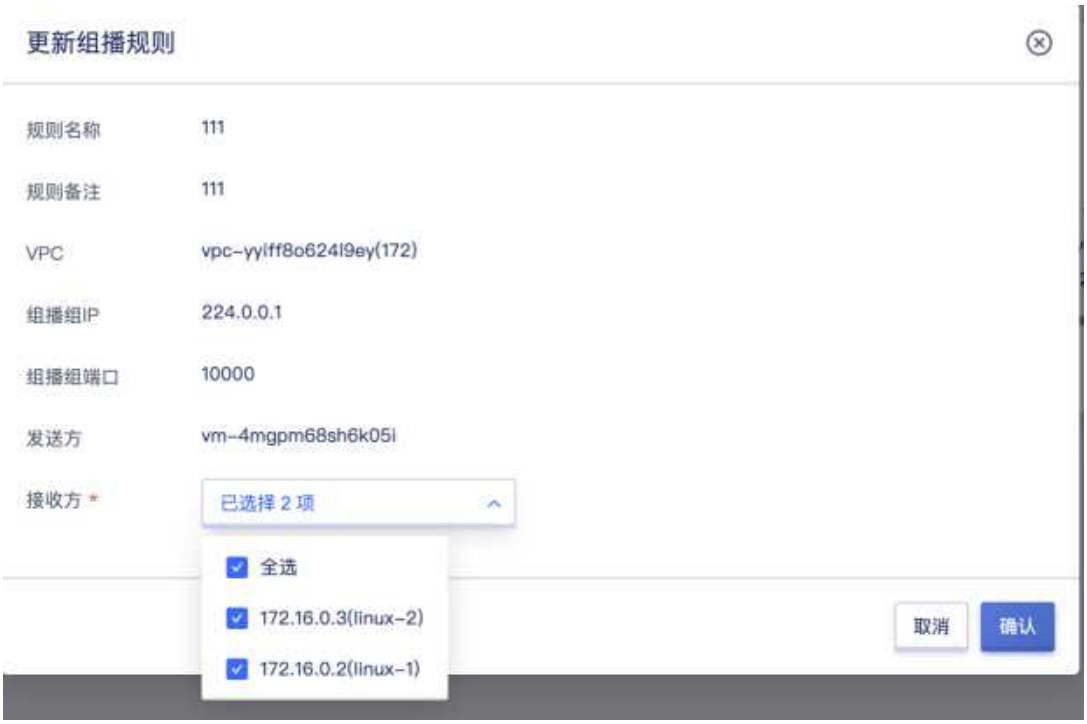
6.4.3 组播列表

通过导航栏进入组播控制台，可查看组播资源列表。组播列表可查看当前账户下所有组播资源的列表信息，包括名称、资源 ID、状态、VPC、组播组 IP、组播组端口、发送方、接收方、项目组、创建时间、更新时间及操作项，如下图所示：

- 名称：组播资源的名称；
- 资源 ID：组播的资源 ID 作为全局唯一标识符；
- 状态：组播资源的状态，包括可用、删除中等状态；
- 组播组 IP：需要用户指定，组播 IP 仅支持 224.0.0.0/4 网段内的 IP
- 组播组端口：需要用户指定，端口默认范围为 10000-64999
- 发送方：同 VPC 下的发送机器，可以作为组播源发送组播消息
- 接收方：同 VPC 下的接收机器，可以接收组播消息
- VPC：组播创建时所指定的 VPC 网络；
- 项目组：组播创建时所绑定的项目组；
- 创建时间/更新时间：组播资源的创建时间和更新组播规则的时间；
- 操作：列表上的操作项是对单个组播的操作，包括更新、删除。

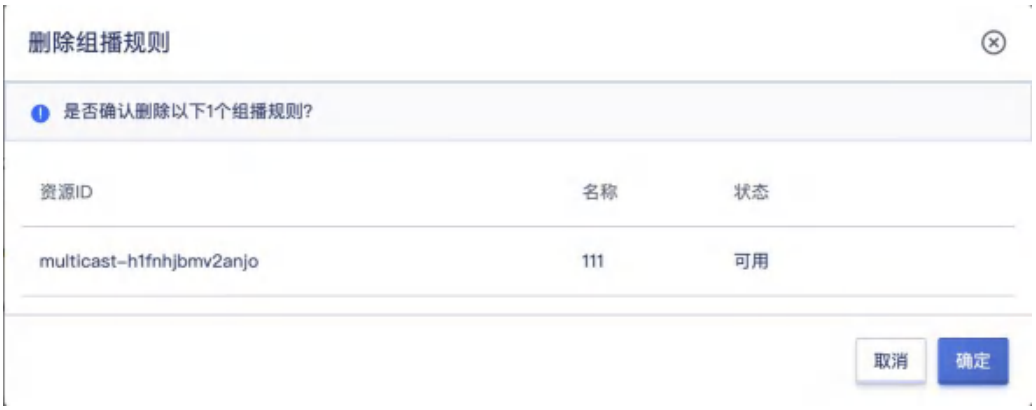
6.4.4 更新组播规则

更新组播的规则，添加或删除接收方的机器。可通过点击组播列表名称右侧的“更新”按钮进行修改，如下图所示：



6.4.5 删除组播

用户可在控制台删除账户内组比，支持对组播进行批量删除操作。可通过组播列表操作项中的“删除”进行操作，如下图所示：



6.5 外网 IP（EIP）

6.5.1 EIP 简介

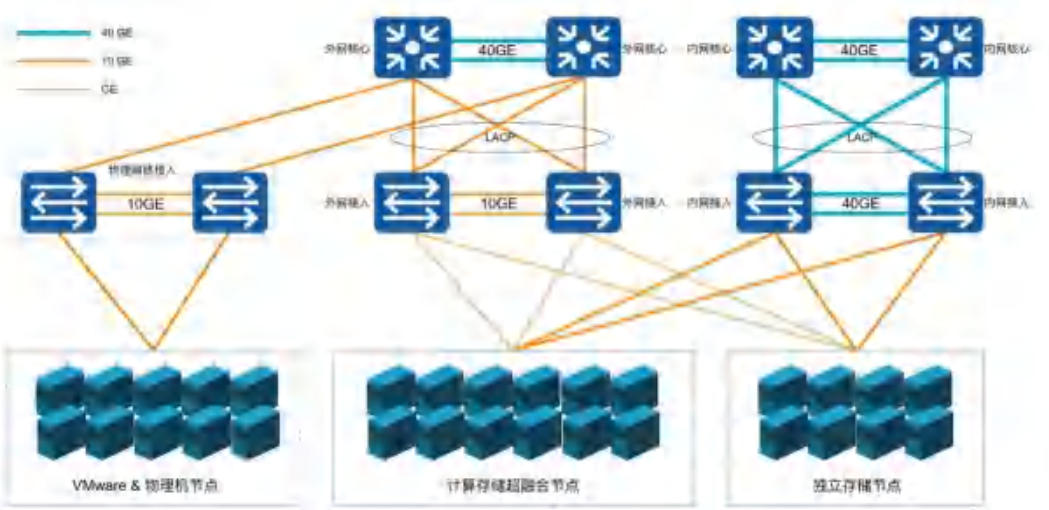
6.5.1.1 概述

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。

6.5.1.2 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

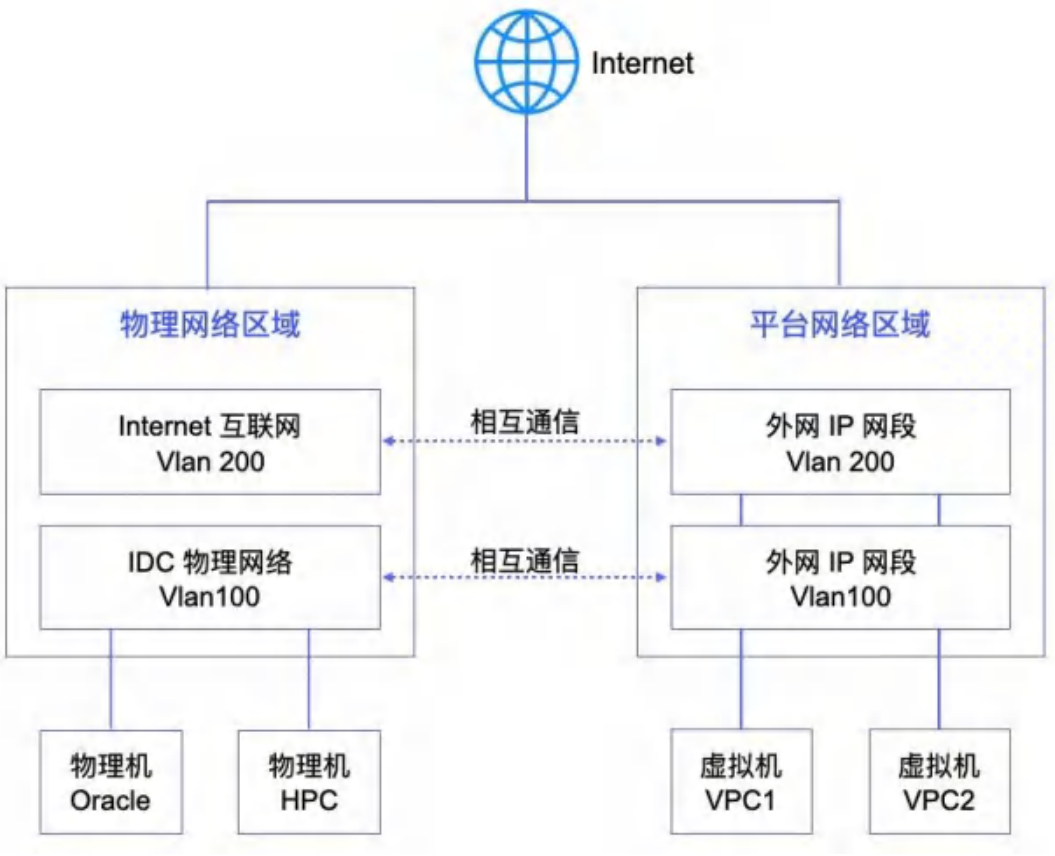
访问方式，使运行在计算节点上虚拟机可通过外网物理网卡直接与外部网络进行通信：

- 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。

6.5.1.3 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

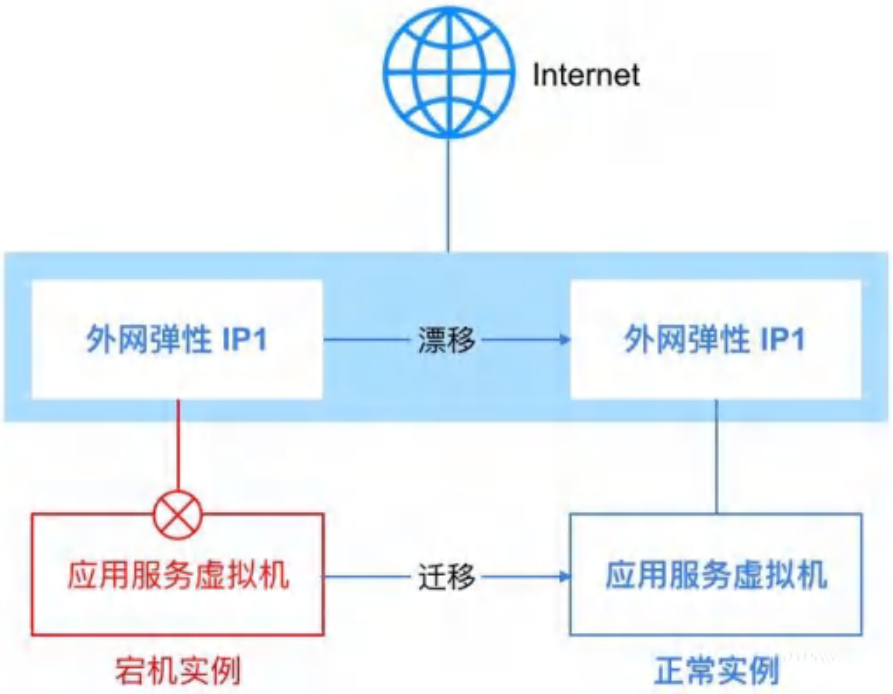
或 IDC 物理网络区域，完成通信。

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。

6.5.1.4 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 50 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。
- 目前仅支持 QEMU-Agent 机器绑定直通模式弹性外网 IPv6

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。

6.5.2 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。若手动指定的 IP 地址已被使用，则会弹出占用提示。
- 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。

6.5.3 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。

6.5.3.1 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/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，包括创建中、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。

6.5.3.2 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。

6.5.4 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、负载均衡及 VPN 网关，为虚拟资源提供外网服务能力。

- 虚拟机支持绑定 50 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。
- IPv6 外网 IP 仅支持绑定至虚拟机，不支持绑定至其它资源。
- 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 且有默认路由的 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且有默认路由 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 且有默认路由 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：

（1）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。

（2）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 50 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，不支持为负载均衡绑定 IPv6 外网 IP。
- 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，不支持为 NAT 网关绑定 IPv6 外网 IP。
- 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，不支持为 VPN 网关绑定 IPv6 外网 IP。

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；若发现网络不通时，需先查看资源已绑定的安全组规则是否放通网络访问，针对虚拟机需针对场景分别检测内网安全组和外网安全组的规则策略。

6.5.5 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。
- 若 NAT 网关仅绑定一个外网 IP 地址，则外网 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 SNAT 和 DNAT 规则中关联的资源均无法通过 NAT 网关访问外网或对外提供端口映射服务，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。

6.5.6 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：

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。

6.5.7 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。

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。

6.5.8 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。

6.5.9 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：

6.5.10 续费外网 IP

支持用户手动对外网 IP 进行续费，续费操作只针对资源本身，不对资源额外关联的资源进行续费，如虚拟机、NAT 网关、负载均衡、VPN 网关等。额外关联的资源到期后，会自动解绑，为保证业务正常使用，需及时对相关资源进行续费操作。

外网 IP 续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

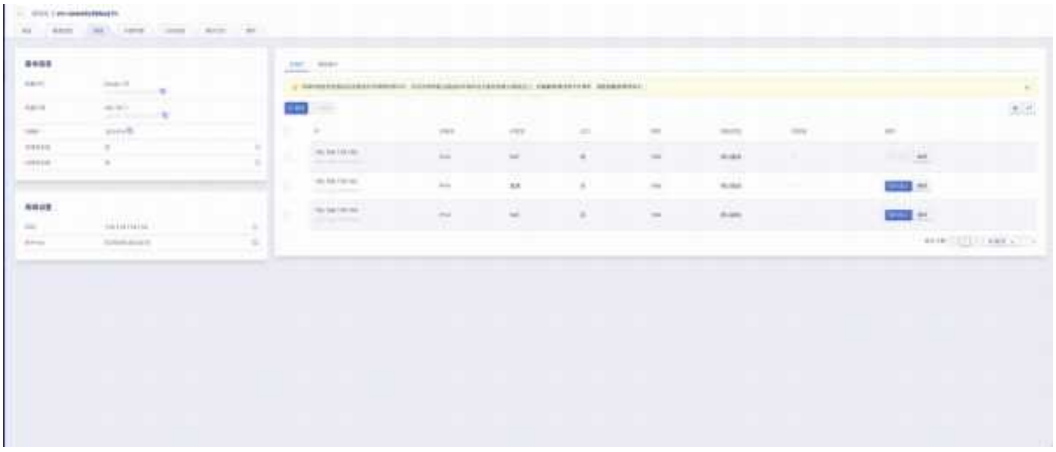
外网 IP 续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当外网 IP 的计费方式为【小时】，则续费时长指定为 1 小时；当外网 IP 的计费方式为【按月】，则续费时长可选择 1 至 11 月；当外网 IP 的计费方式为【按年】，则续费时长为 1 至 5 年。

6.5.11 NAT-EIP

创建 VPC 时，开启 VPC 网关后支持 NAT 模式 EIP 功能，将会消耗 2 核 2G 资源，如图所示：

申请 NAT-EIP 与直通模式外网 IP 相同，在开启 VPC 网关下创建的虚拟机支持绑定 NAT-EIP，如图所示：

其中已经创建的 VPC 资源，当无需使用 NAT-EIP 时，可通过禁用 VPC 网关关闭 NAT-EIP 功能；对于已经创建的 VPC 网关，也可通过启用 VPC 网关使用 NAT-EIP，虚拟机可同时绑定直通模式外网 IP 和 NAT 模式外网 IP，如图所示：



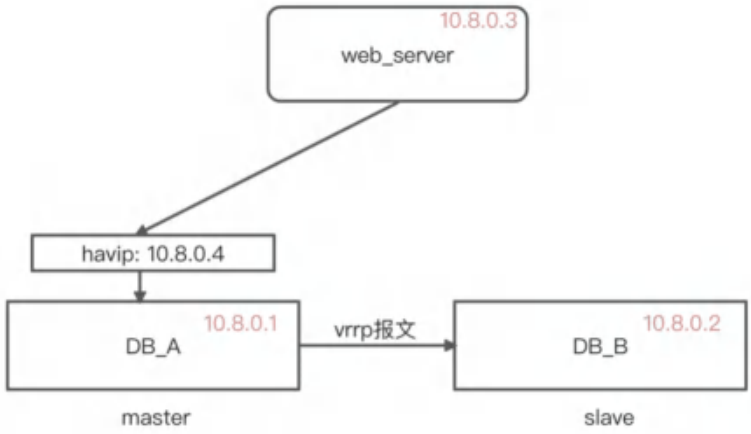
6.6 高可用 VIP

6.6.1 概述

高可用 VIP（High available Virtual IP Address，简称 HAVIP），高可用虚

拟 IP 地址，是归属于 VPC 内某个子网内的可漂移内网 IP，用户可将 HAVIP 与高可用服务结合，以便在服务出现故障时进行服务入口的漂移，以实现服务的高可用。

HaVIP 作为一个不绑定特定设备的浮动 IP，通常和高可用软件（keepalived、heartbeat、Failover Cluster）配合使用，用于搭建高可用主备集群，比如 HA 负载均衡、主备版数据库。这里以 keepalived 为例介绍下 HaVIP 的工作原理

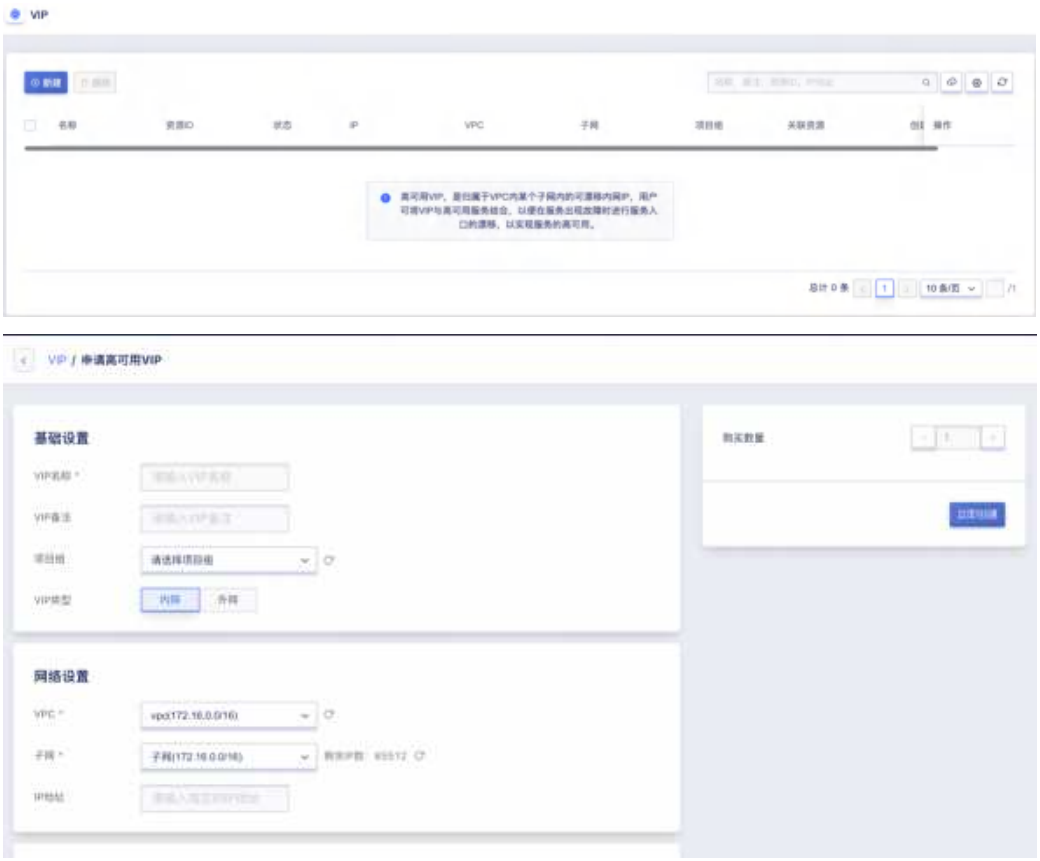


- Master 和 Slave 均安装 keepalived，配置从控制台申请出来的 HaVIP 为 VRRP VIP，分别设置优先级（priority 值）；
- Keepalived 中的 VRRP 协议通过对比两台虚拟机的初始优先级大小，选举出 Master 服务器；
- Master 服务器向外发送 ARP 报文，宣告 VIP，实现 VIP 和 MAC 的地址映射更新（arp 缓存)；
- 此时真正对外提供服务的服务器为 Master 服务器，通信的内网 IP 为 HaVIP；
- Master 服务器周期性发送 VRRP 报文给 Slave 服务器。如果 Master 服务器异常，Backup 服务器在一定时间内没有收到 VRRP 报文，则会将自己设置为 Master，并对外发送 ARP 更新（GARP），报文携带自己的 MAC 地址；
- 此时 Slave 服务器将作为 Master 服务器对外提供通信服务，外部访问

的报文将转发至 Slave 处理，直至实现了 realserver 的切换；

6.6.2 申请高可用 VIP

云平台用户可通过API接口或控制台创建高可用VIP，用于服务的高可用，创建高可用 VIP 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【VIP】管理页面，点击“新建”按钮进入高可用 VIP 创建向导弹窗，如下是创建高可用 VIP 的示意图:

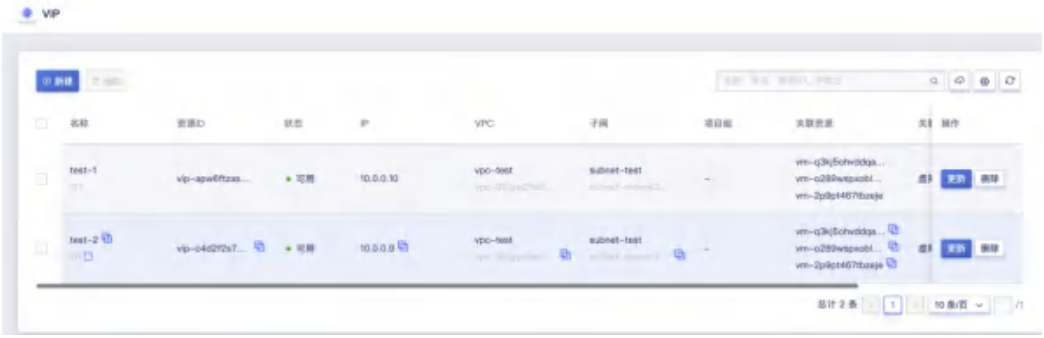


- 名称/备注：申请高可用 VIP 的名称和备注，申请时必须指定名称。
- VIP 类型：内网和外网
- 网络设置：高可用 VIP 的所属网络，创建时必须指定。
- IP 地址：用户手动指定 IP 地址申请 HAVIP，指定的 IP 地址必须在所选网段的 IP 范围内。若手动指定的 IP 地址已被使用，则会弹出占用提示。

- 关联虚拟机：用户可以选择所属 VPC 下的虚拟机，并绑定 HAVIP。
  - 单 VIP 可绑定虚拟机不超过 3 台。
  - 一台虚拟机只能绑定五个 VIP。
- 确认创建：点击确认后，会返回 HAVIP 资源列表页，在列表页可查看 HAVIP 的资源状态，通常创建成功后会显示“可用”的状态，如果因为某些原因没有创建成功会显示”失败“的状态。

6.6.3 查看高可用 VIP

通过导航栏进入虚拟机控制台，切换至 VIP 管理页面可查看高可用 VIP 资源的列表及相关信息，包括高可用 VIP 的名称备注、资源 ID、状态、VPC 子网、IP 地址、关联资源、项目组、创建时间及操作项，如下图所示：



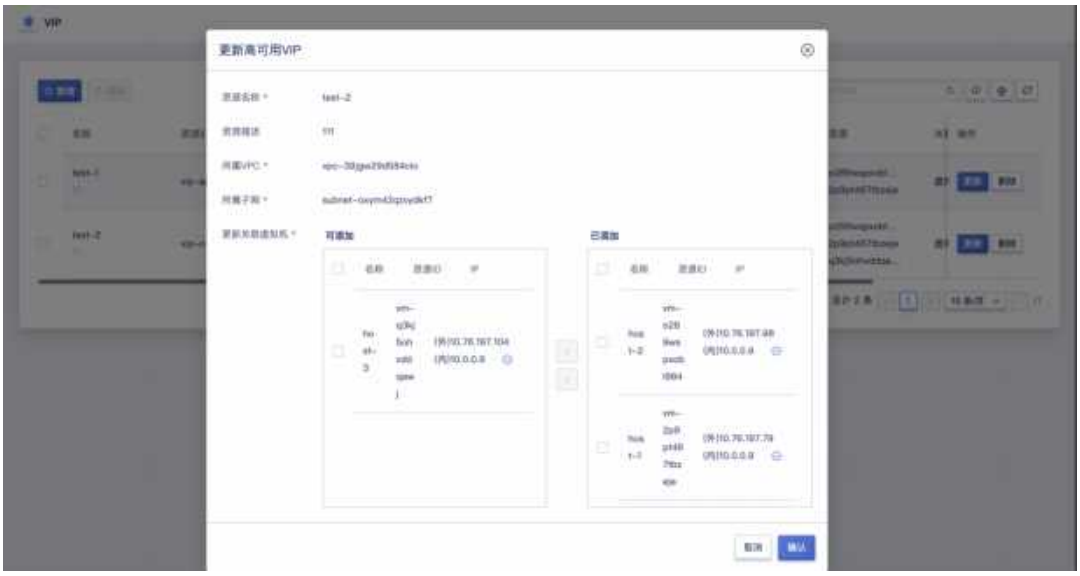
- 名称/备注：申请高可用 VIP 的名称和描述。
- 资源 ID：高可用 VIP 的全局唯一标识符。
- VPC 子网：高可用 VIP 的所属网络
- IP 地址：用户手动指定 IP 地址申请 HAVIP，指定的 IP 地址必须在所选网段的 IP 范围内。
- 关联虚拟机：用户可以选择所属 VPC 下的虚拟机，并绑定 HAVIP。
- 创建时间：当前弹性网卡的创建时间。
- 状态：高可用 VIP 当前的状态，包括可用、失败、删除中等状态

列表上的操作项是指对单个 HAVIP 的操作，包括创建、更新、删除等，可通过搜索框对 HAVIP 列表进行搜索和筛选，支持模糊搜索。

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

6.6.4 更新高可用 VIP

修改 HAVIP 的名称和备注，在任何状态下均可进行操作。可通过 VIP 列表页面每个 HAVIP 名称右侧的“编辑”按钮进行修改；更新关联虚拟机，可以替换、删除、新增虚拟机，关联虚拟机数量不可超过 3 台，如图所示：



6.6.5 删除高可用 VIP

支持用户删除高可用 VIP 资源，可支持删除【可用】【失败】状态的高可用 VIP。删除弹性网卡后，会自动解绑与之关联的虚拟机。用户可通过 VIP 列表进

行高可用 VIP 的删除操作，支持批量删除。

6.6.6 使用外网 VIP

1、查看 keepalived 软件包版本号是否符合要求。

```
yum list keepalived
```

2、使用 yum 方式安装软件包。

```
yum install -y keepalived
```

3、配置 keepalived，绑定高可用 VIP 到主备云服务器，登录主节点云服务器 HAVIP-01，执行 vim /etc/keepalived/keepalived.conf ，修改相关配置。

```
! Configuration File for keepalived
global_defs {
    router_id LVS_DEVEL
    vrrp_skip_check_adv_addr
    vrrp_garp_interval 0
    vrrp_gna_interval 0
}
vrrp_script checkhaproxy
{
     script "/etc/keepalived/do_sth.sh"
      interval 5
}
vrrp_instance VI_1 {
# 注意主备参数选择
state BACKUP                  # 设置初始状态均为“备“
     interface eth0            # 设置绑定 VIP 的网卡 例如 eth0
     virtual_router_id 51      # 配置集群 virtual_router_id 值
     nopreempt                    # 设置非抢占模式
     priority 100              # 两设备是相同值的等权重节点
```



```
    advert_int 5
    authentication {
        auth_type PASS
        auth_pass 1111
    }
    unicast_src_ip 10.0.240.14   # 设置本机内网 IP 地址
    unicast_peer {
        10.0.240.15              # 对端设备的 IP 地址
        10.0.240.16
    }
    virtual_ipaddress {
        192.168.177.204/24 dev eth1      # 设置高可用虚拟 VIP
    }
    virtual_routes {
        0.0.0.0/0 via 192.168.177.1 dev eth1   自定义路由规则
    }
}
```

4、退出编辑状态，输入:wq!保存并退出，重启 keepalived 进程使配置生效。

```
systemctl restart keepalived
```

6.7 负载均衡

6.7.1 负载均衡简介

6.7.1.1 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 LB—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。

LB 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。

6.7.1.2 11.1.2 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。

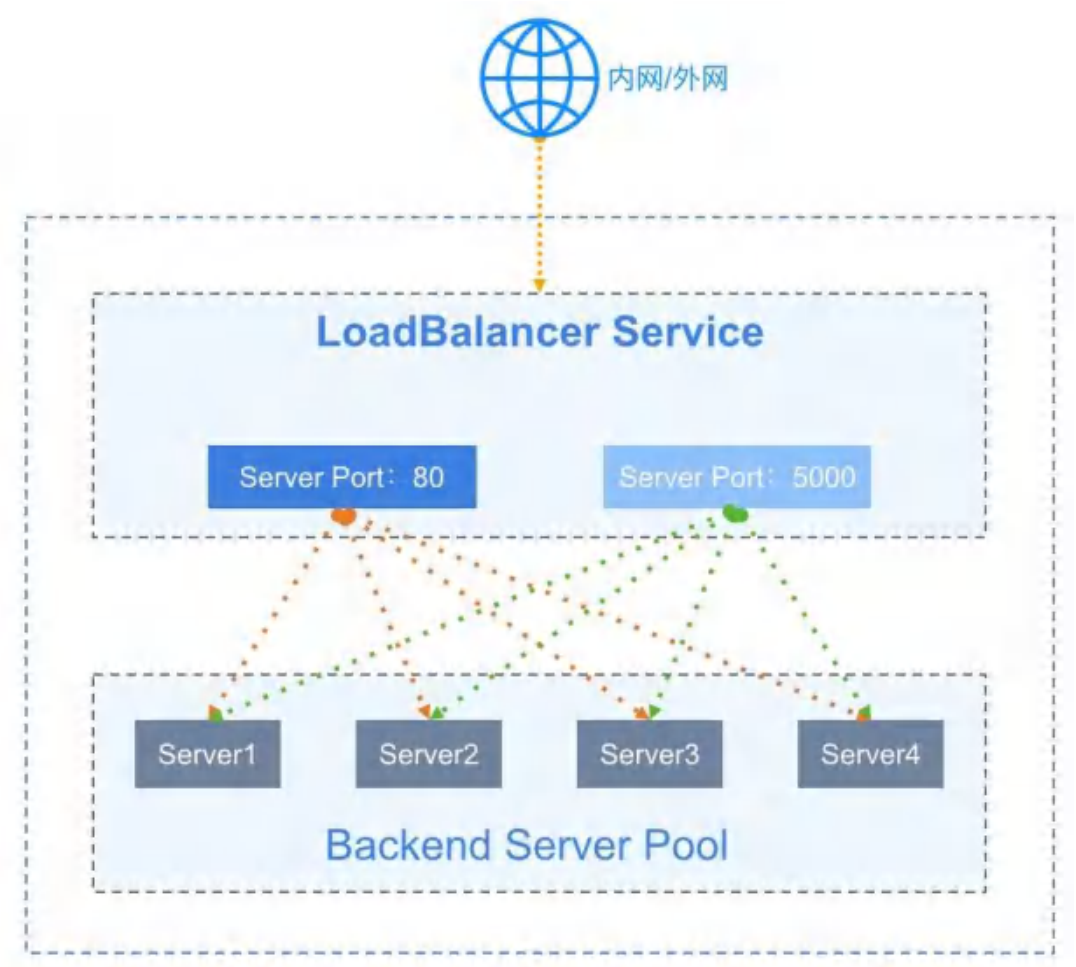
- 外网类型的负载均衡使用场景：
  - 部署在平台的业务服务需要构建高可用虚拟机集群，且需对互联网提供统一访问入口。
  - 部署在平台的业务服务需要构建高可用虚拟机集群，且需对 IDC 数据中心提供统一访问入口。
- 内网负载均衡使用场景：
  - 部署在平台的业务服务需要构建高可用虚拟机集群，且仅需对 VPC 内网提供统一访问入口。
  - 部署在 VPC 私有网络的虚拟机集群需要对其它用户或服务屏蔽真实 IP 地址，对客户端提供透明化服务。

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。

6.7.1.3 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。

6.7.1.4 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。TCP 支持通过 Proxy Protocol 获取客户端真实地址，确保您的后端服务节点支持 Proxy Protocol 即可。
- 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。
- 重定向功能：支持将 HTTP 访问重定向至 HTTPS，HTTPS 是加密数据传输协议，安全性较高。

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。

注意：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。

6.7.1.5 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。

6.7.2 负载均衡管理

6.7.2.1 使用流程

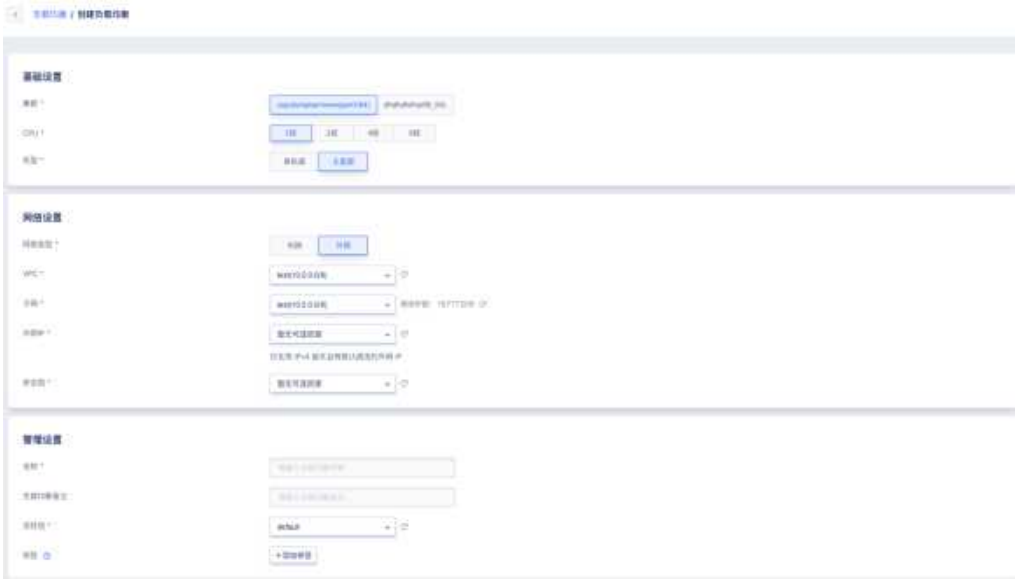
在使用负载均衡服务前，需根据业务需求规划负载均衡的网络类型及监听类型，并根据业务需求在平台部署并配置好业务虚拟机，具体流程如下：

1. 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；
2. 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；
3. 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；
4. 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；
5. 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；

6. 通过负载均衡服务提供的统一入口 IP 地址访问业务服务。

6.7.2.2 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：



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：

- 集群：负载均衡实例所在节点的集群类型，由平台管理员自定义，如 x86 机型和 ARM 机型，通过 ARM 机型创建的实例为 ARM 版负载均衡实例，已适配国产芯片、服务器及操作系统。
- CPU：选择实例对应 CPU 规格，支持 1 核，2 核，4 核，8 核四种规格。
- 机型：支持单机版，主备版两种机型。
- 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。
- 项目组：设置实例所属项目，默认为 default。
- 标签：选择对应的资源标签，便于管理。

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；

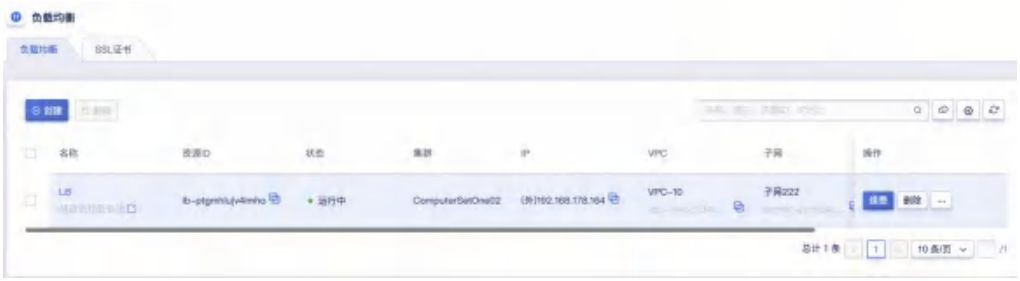
确认订单无误后点击立即购买，点击立即购买后，会返回负载均衡资源列表页，在列表页可查看资源的创建过程，通常会先显示“创建中”的状态，分钟内转换为“运行中”状态，即代表创建成功。

6.7.2.3 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。

6.7.2.3.1 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：



- 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：负载均衡的的运行状态，包括创建中、运行中、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。

6.7.2.3.2 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、内网 IP、状态、告警模板及日志管理信息，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，可点击日志管理右侧按钮选择存储位置。

（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。

（5）操作日志

操作日志页面可查看负载均衡的操作信息，支持查看 1 小时及自定义时间的日志信息，最长可查询 6 个月的操作日志信息。具体信息包括操作（API）名称、所属模块、地域、关联资源、操作者、操作结果及操作时间。

（6）事件信息

事件页面会记录负载均衡资源的部分核心操作事件，提供事件详细记录，用户可通过事件描述定位问题。

6.7.2.4 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，如图所示。

6.7.2.5 11.2.5 修改日志管理

负载均衡支持访问日志管理，仅支持 7 层访问日志，转储周期为 5 分钟。

- 开启日志管理功能选定的对象存储需要与负载均衡在同一个 VPC 下，

对象存储日志默认保留 6 个月，过期会自动删除。

- 负载均衡日志路径为如下：lb-log/lb-xxxx/2022/09/access.log-20220923185657-bhetvdnj.gz。

用户可将日志存储到指定对象存储，如图所示：

6.7.2.6 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。

6.7.2.7 11.2.7 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。

6.7.2.8 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。

6.7.2.9 负载均衡续费

支持用户手动对负载均衡进行续费，续费操作只针对资源本身，不对资源额外关联的资源进行续费，如绑定至负载均衡的外网 IP 资源。额外关联的资源到期后，会自动与负载均衡解绑，为保证业务正常使用，需及时对相关资源进行续费操作。

负载均衡续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

负载均衡续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当负载均衡的计费方式为【小时】，则续费时长指定为 1 小时；当负载均衡的计费方式为【按月】，则续费时长可选择 1 至 11 月；当负载均衡的计费方式为【按年】，则负载均衡的续费时长为 1 至 5 年。

6.7.2.10 配置升级

支持用户对负载均衡的配置进行升级。

6.7.2.11 升级机型

支持用户将单机版负载均衡升级为主备版，满足负载均衡网关高可用场景。当其中一个网关的虚拟机实例因故障宕机时，备实例会自动转换为主实例持续提供负载均衡服务。

6.7.2.12 修改标签

支持用户修改负载均衡的标签。

6.7.3 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。

6.7.3.1 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，支持将 HTTP 访问重定向至 HTTPS。
- 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。

6.7.3.1.1 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:111（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、Proxy 协议、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。**
- **Proxy 协议**：TCP 支持通过 Proxy Protocol 携带原始连接信息获取客户端的真实 IP，启用前，请确保后端服务节点 RS 也支持 Proxy Protocol，否则会连接失败。
- **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“正常”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。

6.7.3.1.2 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:33（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两种算法。
- **会话保持**：针对 UDP 协议的“加权轮询”负载均衡算法，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“正常”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。

6.7.3.1.3 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:8080（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：

根据向导页面配置 VServer 监听器，包括协议、端口、负载均衡算法、重定向开关按键、重定向至会话保持、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 8080 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。
- **重定向**：HTTP 协议支持选择重定向功能，将 HTTP 访问重定向至 HTTPS，本示例将 HTTP:8080 访问重定向转发至 HTTPS:88。
- **会话保持**：针对 HTTP 和 HTTPS 协议，为“加权轮询”的负载均衡算

法提供 Cookie 植入方式的会话保持功能，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。

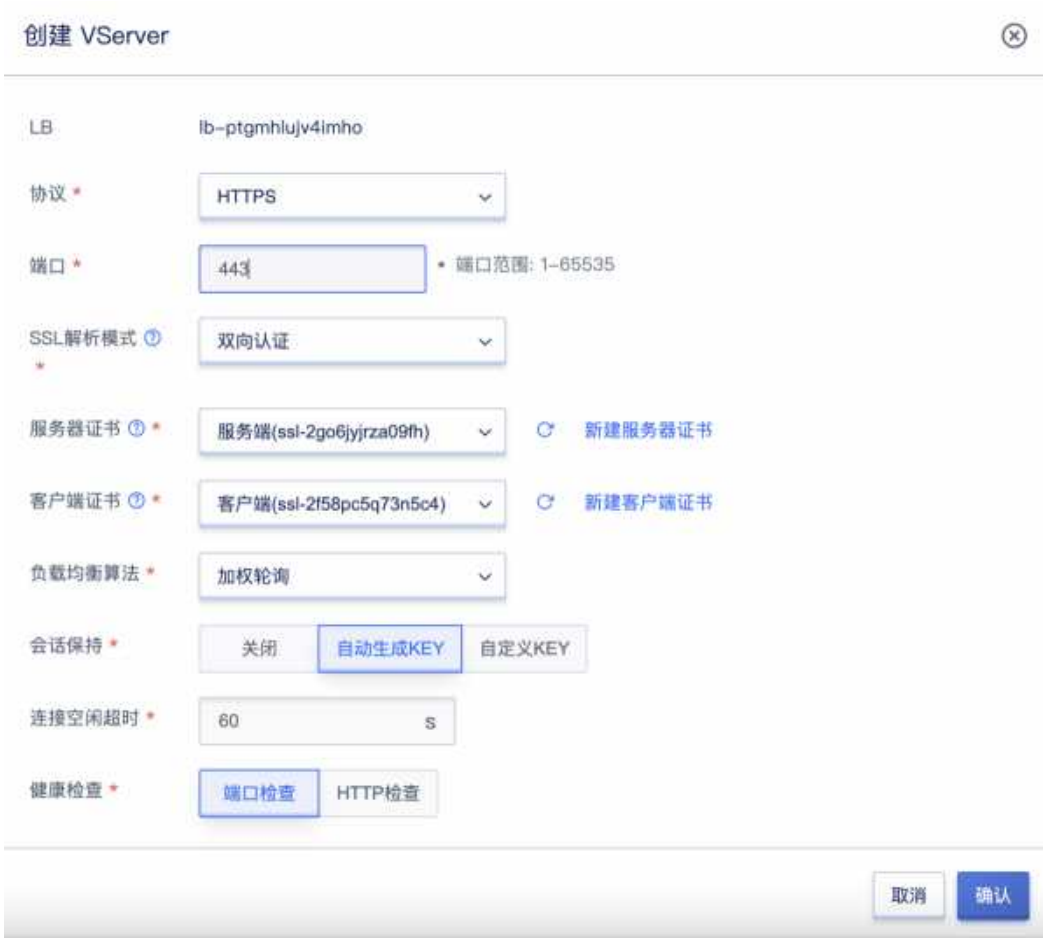
HTTP 健康检查中的域名作用：某些应用服务器会对请求中的 host 字段做校验，即要求请求头中必须存在 host 字段。若在健康检查中配置了域名，则负载均衡会将域名配置到 host 字段中，并在健康检查时携带域名对后端服务节点进行检查，若健康检查请求被服务节点拒绝，则健康检查失败，即代表服务节点状态为异常；若应用服务器需要校验请求的 host 字段，则需要配置相关域名，确保健康检查正常工作。

创建过程中 VServer 的资源状态为“创建中”，待状态更新为“有效”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。

6.7.3.1.4 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：



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。
- **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。
- **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，为“加权轮询”的负载均衡算法提供 Cookie 植入方式的会话保持功能，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“正常”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。

6.7.3.2 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。

6.7.3.2.1 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**：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；开启“重定向”的 HTTP 协议的 VServer 默认为绿色。
  - **黄色**：VServer 中添加的部分服务节节异常；
  - **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。

6.7.3.2.2 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：

（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、节点状态、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。
- **节点状态**：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、删除中。
- **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

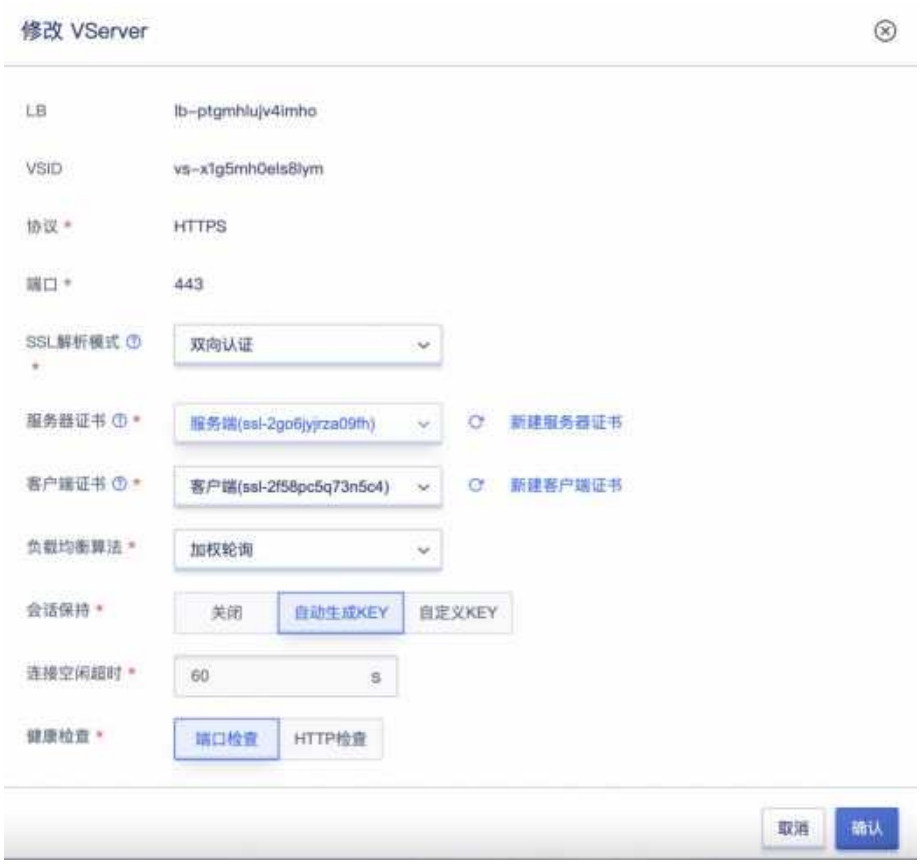
VServer 实例相关监控图表及信息，包括新建连接数、HTTP 2XX、HTTP 3XX、HTTP 4XX、HTTP 5XX，支持查看 1 小时、6 小时、12 小时、1 天及自定义时间的监控数据。

（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。
- 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。

6.7.3.3 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“正常”变更为“更新中”，更新成功后流转为“正常”，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。

注：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。

6.7.3.4 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。

6.7.3.5 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。

6.7.4 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，即服务节点状态为可用，则代表负载均衡可正常工作。

6.7.4.1.1 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：

- **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”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节点状态，节点状态“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。

注：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。

6.7.4.1.2 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：**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。

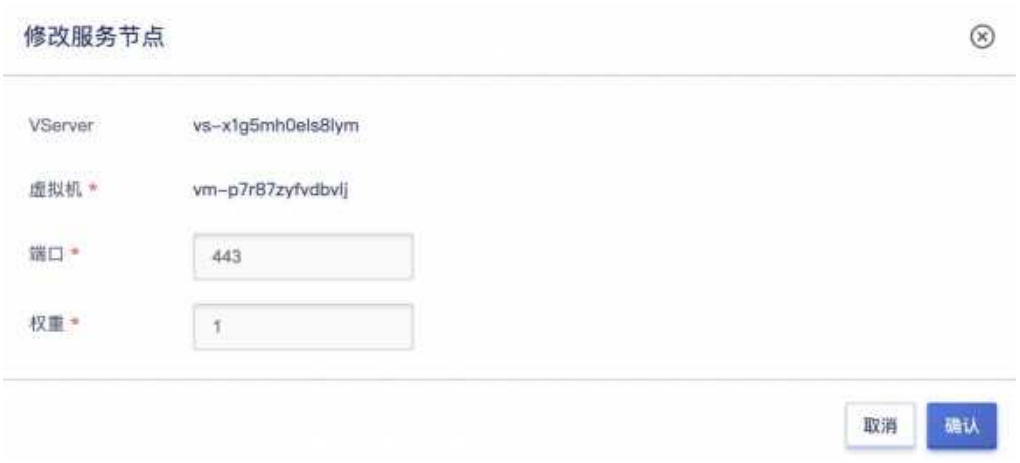
6.7.4.1.3 启用/禁用

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，若健康检查通过则分根据调度算法，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。

6.7.4.1.4 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”，可用则代表健康检查成功，服务节点可正常提供服务。

6.7.4.1.5 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。

6.7.5 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。

6.7.5.1 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：

- **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；
- **SNI**：SNI 主要是改善客户端和服务器的 SSL，解决一台服务器只可使用一个证书的问题。SNI 支持服务器绑定多个证书，服务器会根据域名返回合适的证书。
  - 仅 VServer 类型为 HTTPS，且非默认域名"_"，支持配置 SNI，仅支持单个 SNI。
  - SSL 单向认证只要求站点部署证书即可；双向认证要求服务器和用户均有证书才可访问，即要求双方提供身份认证。
- **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“可用”时，即代表创建成功。

6.7.5.2 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：

- **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、可用和删除中。

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和修改，不支持删除。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，可修改默认转发规则中的服务节点数量，以匹配精准转发策略。

6.7.5.3 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“可用”流转为“更新中”，待修改成功后，重新流转回“可用”，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。

6.7.5.4 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：

6.7.6 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。

6.7.6.1 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。

6.7.6.1.1 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-----
MIIFnDCCBISgAwIBAgIQD1pxAmxfzY+R4k4Ua1cVWDANBgkqhkiG9w0BAQsFADBy
MQswCQYDVQQGEwJDTjElMCMGA1UEChMcVHJ1c3RBc2lhIFRlY2hub2xvZ2llcywg
SW5jLjEdMBsGA1UECxMURG9tYWluIFZhbGlkYXRlZCBTU0wxHTAbBgNVBAMTFFRy
dXN0QXNpYSBUTFMgUlNBIENBMB4XDTE5MDQyMzAwMDAwMFoXDTIwMDQyMjEyMDAw
MFowHDEaMBgGA1UEAwwRKi51Y2xvdWRzdGFjay5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC2SDT5pJEQhRhQQ98vzuAvK1zUFMD1p1E3YyJGDISY
```

```
SINH38QTtVqWbZgmVkU6v2R1GrBz0iMfevO0/sjxefwHmiGYd1ytG9dm8D3fVZox
piST9hoIyjOFRstBLGXuxWSa2LdjVSePaFfxaN3UZLYY6MIHkdqxVZLhM4ANSLNr
PI6cRUZVBU29V3A2znkVEbx5dwKA3SGFVWfqjfzXqC+NTylLKb7H304BxspZlKDi
n+/aV/vSovVM7zg57AOtxjkSNzBDjdz+Ud3wqaT1O4vEG4tqqAnsIyJeaMueFti0
cjiMwLVsFsmV1eVSBiYWGO8U/YRFv+dNg4XG2MqYUFsRAgMBAAGjggKCMIICfjAf
BgNVHSMEGDAWgBR/05nzoEcOMQBWViKOt8ye3coBijAdBgNVHQ4EFgQUJYEWLiyn
YgqKaGaT8thKWAnuWfEwLQYDVR0RBCYwJIIRKi51Y2xvdWRzdGFjay5jb22CD3Vj
bG91ZHN0YWNrLmNvbTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUH
AwEGCCsGAQUFBwMCMEwGA1UdIARFMEMwNwYJYIZIAYb9bAECMCowKAYIKwYBBQUH
AgEWHGh0dHBzOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwCAYGZ4EMAQIBMH0GCCsG
AQUFBwEBBHEwbzAhBggrBgEFBQcwAYYVaHR0cDovL29jc3AuZGNvY3NwLmNuMEoG
CCsGAQUFBzAChj5odHRwOi8vY2FjZXJ0cy5kaWdpdGFsY2VydHZhbGlkYXRpb24u
Y29tL1RydXN0QXNpYVRMU1JTQUNBLmNydDAJBgNVHRMEAjAAMIIBBAYKKwYBBAHW
eQIEAgSB9QSB8gDwAHYA7ku9t3XOYLrhQmkfq+GeZqMPfl+wctiDAMR7iXqo/csA
AAFqSaRkyQAABAMARzBFAiEAuovTHM3SEWQRyktGXvtm1hLHd7gxhPNzdzrzkJFX
rWMCIAPideB1BqUSUcpRME6NxIXJD7066ldWuSqgPkOiPtwLAHYAh3W/51l8+IxD
mV+9827/Vo1HVjb/SrVgwbTq/16ggw8AAAFqSaRl4wAABAMARzBFAiBiIpO59m6U
bmlmuQ8cL7WzoDkHiyE+UloEKZXiDpqCfQIhAPIKRdaJfh/5IZHFq31oJVd/TZ3g
pTQ6RpHe0BseSSefMA0GCSqGSIb3DQEBCwUAA4IBAQARaNWOJbAI7Rv6QPChPeWL
Mqryk+tOlterdxYZay6tr3Ea8VOqSS7YdVtvdkR1/k4k87H5AwCQT60/yu4N5J7M
Vkzmqo3tVQTtzVFo0SavgARY12XuU0jhG3LGFI0a43CgfMYMcZ0DiylhYUM48GWz
/axza5uangnIQxBwv+4KXGUfplJujv8WfBepeh+tqPgS8qCqn6e0+sdkUN7yHcA/
O24DiQajtMXG5nR6qHdZhRLCFRXRghYdvVKrkOVFogYqwa4dViyuP/6EFDkuMwDs
7XrxJljL8qp9Lrw2sHN1F+USKhlPRaNBtWzDELf54zVgAIAeFUriqtER8ZWBWgp4
-----END CERTIFICATE-----
```

6.7.6.1.2 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
MQswCQYDVQQGEwJDTjElMCMGA1UEChMcVHJ1c3RBc2lhIFRlY2hub2xvZ2llcywg
SW5jLjEdMBsGA1UECxMURG9tYWluIFZhbGlkYXRlZCBTU0wxHTAbBgNVBAMTFFRy
dXN0QXNpYSBUTFMgUlNBIENBMB4XDTE5MDQyMzAwMDAwMFoXDTIwMDQyMjEyMDAw
MFowHDEaMBgGA1UEAwwRKi51Y2xvdWRzdGFjay5jb20wggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC2SDT5pJEQhRhQQ98vzuAvK1zUFMD1p1E3YyJGDISY
SINH38QTtVqWbZgmVkU6v2R1GrBz0iMfevO0/sjxefwHmiGYd1ytG9dm8D3fVZox
piST9hoIyjOFRstBLGXuxWSa2LdjVSePaFfxaN3UZLYY6MIHkdqxVZLhM4ANSLNr
PI6cRUZVBU29V3A2znkVEbx5dwKA3SGFVWfqjfzXqC+NTylLKb7H304BxspZlKDi
n+/aV/vSovVM7zg57AOtxjkSNzBDjdz+Ud3wqaT1O4vEG4tqqAnsIyJeaMueFti0
cjiMwLVsFsmV1eVSBiYWGO8U/YRFv+dNg4XG2MqYUFsRAgMBAAGjggKCMIICfjAf
BgNVHSMEGDAWgBR/05nzoEcOMQBWViKOt8ye3coBijAdBgNVHQ4EFgQUJYEWLiyn
YgqKaGaT8thKWAnuWfEwLQYDVR0RBCYwJIIRKi51Y2xvdWRzdGFjay5jb22CD3Vj
bG91ZHN0YWNrLmNvbTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUH
AwEGCCsGAQUFBwMCMEwGA1UdIARFMEMwNwYJYIZIAYb9bAECMCowKAYIKwYBBQUH
AgEWHGh0dHBzOi8vd3d3LmRpZ2ljZXJ0LmNvbS9DUFMwCAYGZ4EMAQIBMH0GCCsG
```

AQUFBwEBBHEwbzAhBggrBgEFBQcwAYYVaHR0cDovL29jc3AuZGNvY3NwLmNuMEoG
CCsGAQUFBzAChj5odHRwOi8vY2FjZXJ0cy5kaWdpdGFsY2VydHZhbGlkYXRpb24u
Y29tL1RydXN0QXNpYVRMU1JTQUNBLmNydDAJBgNVHRMEAjAAMIIBBAYKKwYBBAHW
eQIEAgSB9QSB8gDwAHYA7ku9t3XOYLrhQmkfq+GeZqMPfl+wctiDAMR7iXqo/csA
AAFqSaRkyQAABAMARzBFAiEAuovTHM3SEWQRyktGXvtm1hLHd7gxhPNzdzrzkJFX
rWMCIAPideB1BqUSUcpRME6NxIXJD7066ldWuSqgPkOiPtwLAHYAh3W/51l8+IxD
mV+9827/Vo1HVjb/SrVgwbTq/16ggw8AAAFqSaRl4wAABAMARzBFAiBiIpO59m6U
bmlmuQ8cL7WzoDkHiyE+UloEKZXiDpqCfQlhAPIKRdaJfh/5IZHFq31oJVd/TZ3g
pTQ6RpHe0BseSSefMA0GCSqGSIb3DQEBCwUAA4IBAQARaNWOJbAI7Rv6QPChPeWL
Mqryk+tOlterdxYZay6tr3Ea8VOqSS7YdVtvdkR1/k4k87H5AwCQT60/yu4N5J7M
Vkzmqo3tVQTtzVFo0SavgARY12XuU0jhG3LGFI0a43CgfMYMcZ0DiylhYUM48GWz
/axza5uangnIQxBwv+4KXGUfplJujv8WfBepeh+tqPgS8qCqn6e0+sdkUN7yHcA/
O24DiQajtMXG5nR6qHdZhRLCFRXRghYdvVKrkOVFogYqwa4dViyuP/6EFDkuMwDs
7XrxJIjL8qp9Lrw2sHN1F+USKhlPRaNBtWzDELf54zVgAIAeFUriqtER8ZWBWgp4
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIErjCCA5agAwIBAgIQBYAmfwbyIVM0jhwYWI7uLjANBgkqhkiG9w0BAQsFADBh
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMSAwHgYDVQQDExdEaWdpQ2VydCBHbG9iYWwgUm9vdCBD
QTAeFw0xNzEyMDgxMjI4MjZaFw0yNzEyMDgxMjI4MjZaMHIxCzAJBgNVBAYTAkNO
MSUwIwYDVQQKExxUcnVzdEFzaWEgVGVjaG5vbG9naWVzLCBJbmMuMR0wGwYDVQQL
ExREb21haW4gVmFsaWRhdGVkIFNTTDEdMBsGA1UEAxMUVHJ1c3RBc2lhIFRMUyBS
U0EgQ0EwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCgWa9X+ph+wAm8
Yh1Fk1MjKbQ5QwBOOKVaZR/OfCh+F6f93u7vZHGcUU/IvVGgUQnbzJhR1UV2epJa
e+m7cxnXIKdD0/VS9btAgwJszGFvwoqXeaCqFoP71wPmXjjUwLT70+qvX4hdyYfO
JcjeTz5QKtg8zQwxaK9x4JT9CoOmoVdVhEBAiD3DwR5fFgOHDwwGxdJWVBvktnoA
zjdTLXDdbSVC5jZ0u8oq9BiTDv7jAlsB5F8aZgvSZDOQeFrwaOTbKWSEInEhnchK
ZTD1dz6aBlk1xGEI5PZWAnVAba/ofH33ktymaTDsE6xRDnW97pDkimCRak6CEbfe
3dXw6OV5AgMBAAGjggFPMIIBSzAdBgNVHQ4EFgQUf9OZ86BHDjEAVlYijrfMnt3K
AYowHwYDVR0jBBgwFoAUA95QNVbRTLtm8KPiGxvDl7I90VUwDgYDVR0PAQH/BAQD
AgGGMB0GA1UdJQQWMBQGCCsGAQUFBwMBBggrBgEFBQcDAjASBgNVHRMBAf8ECDAG
AQH/AgEAMDQGCCsGAQUFBwEBBCgwJjAkBggrBgEFBQcwAYYYaHR0cDovL29jc3Au
ZGlnaWNlcnQuY29tMEIGA1UdHwQ7MDkwN6A1oDOGMWh0dHA6Ly9jcmwzLmRpZ2lj
ZXJ0LmNvbS9EaWdpQ2VydEdsb2JhbFJvb3RDQS5jcmwwTAYDVR0gBEUwQzA3Bglg
hkgBhv1sAQIwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cuZGlnaWNlcnQuY29t
L0NQUzAIBgZngQwBAgEwDQYJKoZIhvcNAQELBQADggEBAK3dVOj5dlv4MzK2i233
lDYvyJ3slFY2X2HKTYGte8nbK6i5/fsDImMYihAkp6VaNY/en8WZ5qcrQPVLuJrJ
DSXT04NnMeZOQDUoj/NHAmdfCBB/h1bZ5OGK6Sf1h5Yx/5wR4f3TUoPgGlnU7EuP
ISLNdMRiDrXntcImDAiRvkh5GJuH4YCVE6XEntqaNIgGkRwxKSgnU3Id3iuFbW9F
UQ9Qqtb1GX91AJ7i4153TikGgYCdwYkBURD8gSVe8OAco6IfZOYt/TEwii1Ivi1C
qnuUlWpsF1LdQNIdfbW3TSe0BhQa7ifbVIfvPWHYOu3rkg1ZeMo6XRU9B4n5VyJY
RmE=
-----END CERTIFICATE-----

6.7.6.1.3 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
E7Valm2YJlZFOr9kdRqwc9ljH3rztP7I8Xn8B5ohmHdcrRvXZvA931WaMaYkk/Ya
CMozhUbLQSxl7sVkmti3Y1Unj2hX8Wjd1GS2GOjCB5HasVWS4TOADUizazyOnEVG
VQVNvVdwNs55FRG8eXcCgN0hhVVn6o3816gvjU8pSym+x99OAcbKWZSg4p/v2lf7
0qL1TO84OewDrcY5EjcwQ43c/lHd8Kmk9TuLxBuLaqgJ7CMiXmjLnhbYtHI4jMC1
bBbJldXlUgYmFhjvFP2ERb/nTYOFxtjKmFBbEQIDAQABAoIBAAbLqdftu+/A+n9R
jHJIlOCFThRlAq2V04gMVNSGNnJD78r/61wtvGcTxmKVgEa4qGraOB5VRPRxPcEv
Z3fjK5Nv+lUoDAczHMRsa+4Vz6YOstnmSKGvwhxzn3O6T0GHz+Ca+DlGjS9CPVcV
aQG4UHacxNEJ7byDO3LUW++C2JeEjg2LVLJt+jRwFlAwmk8XjM/jyOn5kCj2kvz6
w/yHbmwAac2mfA42CQN78o1bvEHlHH1cVDRHZ482pNlfp8WBGgCFWHBGeMpLOq9R
YXEt+SyJ84o80mTeR2DgswpW577uZLGfPyFUwKPc/XGZSzbfKX5L9ctGQrr4lsQ+
F2stOk0CgYEA5JyQ5S7qPf8YcczQfXblVueslDL56Zt1/KUdUQ4L9i2as+5LkiN+
7gVK8INhvYi8dRAqZxqXLqU5dXEWbkcnFbenjoQyPCfYI5lZE2+cZriLtO3I0YKP
nc9NwSE+gRR9kXbgGSiANJmGC5TxOU99hR7Nx6wUMAflatCaSmP5RbUCgYEAzB67
MOWzeVD8Eq/DhEE5N0o3hpyhiMy++A/LC8lAjFAi6ldc70zMYMUjfh+eTNK89Z6H
1z3xBaQMMlHAy8pU5uI9LOgm/xWaPNZ034Xx4fWftBnEGFtBgLfbNphoUz3Df5vK
XvXhjdKEkwevcLoZWHfNZIJnennlEV26Tk1DGW0CgYBYCKaPasqPRy2NnRZoSiG0
npBJnXu5ZsE/ogGxFdyrVxJs2YXGZ97YH7ek+KLpzr7rwWbiv02ai8udmwfNPZ8i
cM+YRPXnTlygEMxJfMBYmhZKfQrJCyLs3UiO55NfN5nHK2TOq1b7amdBDID71c17
Nsp9apl3iYLh6CSSIv95xQKBgCHmKKhiPYA0VuizkADy5BGunblZaSpS9pQz60C1
16Z12Jaak7CaTIb1toNHtP6FMSSJg33Xp6OMLwpcUWyG2brOb+J5W6CZcdgQtbA5
ioZASJmcfdidry81WY6jmQ/Z/hG/ScijhSYMhD/20sgh3/u1ScMbdRv+CnDr4/kF
E9OxAoGBAK0mCJyyKNkWSdOg7fbBwYJKQ1BBZ6lh1gVpc7recSreNPRFWTd6l+cw
eCxXqbSJJw4oYYF4IoBX1fCfFd82engRkwmkDykGMwpomnJoZqjFhmVtDb81xRQL
pscHorV4flpOcSwg6b3jq0N6+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
```

6.7.6.1.4 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-----
```

6.7.6.2 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。

6.7.6.2.1 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。

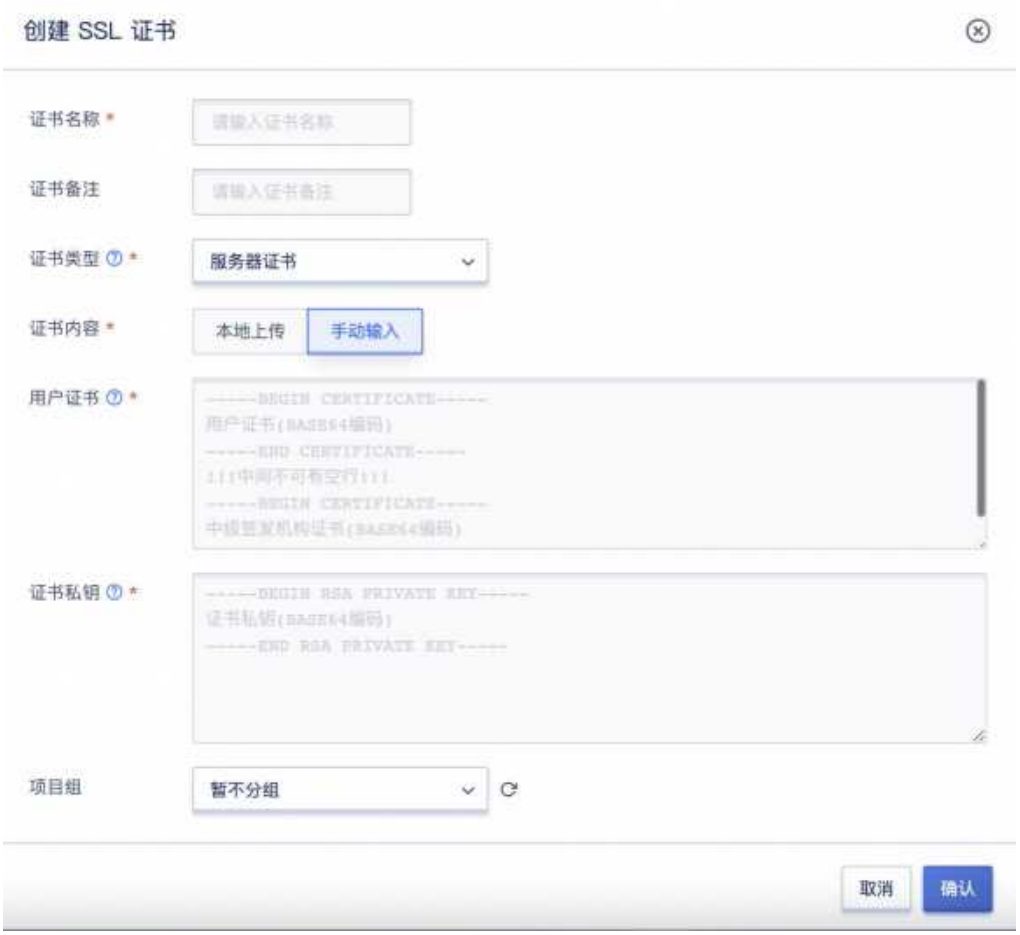
（1）本地上传证书文件的方式创建如下图所示：

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：



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。

6.7.6.2.2 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。

6.7.6.3 11.6.3 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。

6.7.6.3.1 11.6.3.1 SSL 证书列表

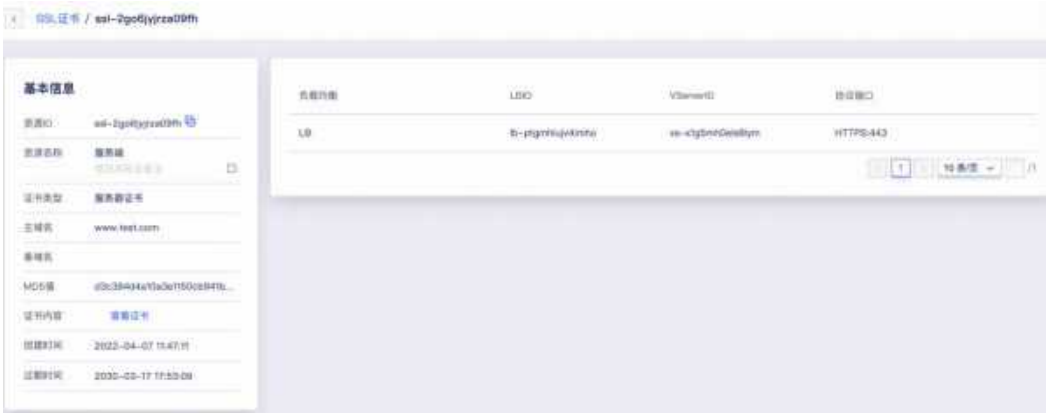
SSL 证书列表可查看当前账户下所有 SSL 证书的资源列表信息，包括名称、资源 ID、证书类型、域名、MD5 值、创建时间、证书过期时间及操作项，如下图所示：

- **名称/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。

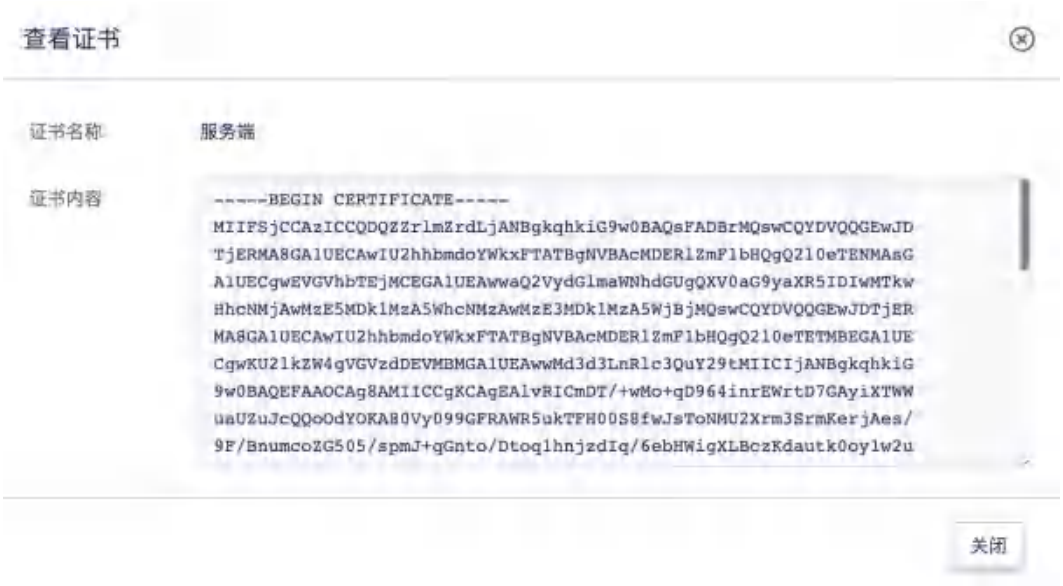
6.7.6.3.2 SSL 证书详情

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：



（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）。

6.7.6.4 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。

6.8 NAT 网关

6.8.1 NAT 网关简介

6.8.1.1 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，支持互联网或物理网地址转换能力。平台 NAT 网关服务通过的 SNAT 和 DNAT 规则分别实现 VPC 内虚拟资源的 SNAT 转发和 DNAT 端口映射功能。

- **SNAT 规则**

通过 SNAT 规则实现 VPC 级、子网级及虚拟资源实例级的 SNAT 能力，使不同维度的资源通过 NAT 网关访问外网。

- **DNAT 规则**

通过 DNAT 规则，可配置基于 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。

作为一个虚拟网关设备，需要绑定外网 IP 作为 NAT 网关的 SNAT 规则出口及 DNAT 规则的入口。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。

6.8.1.2 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。

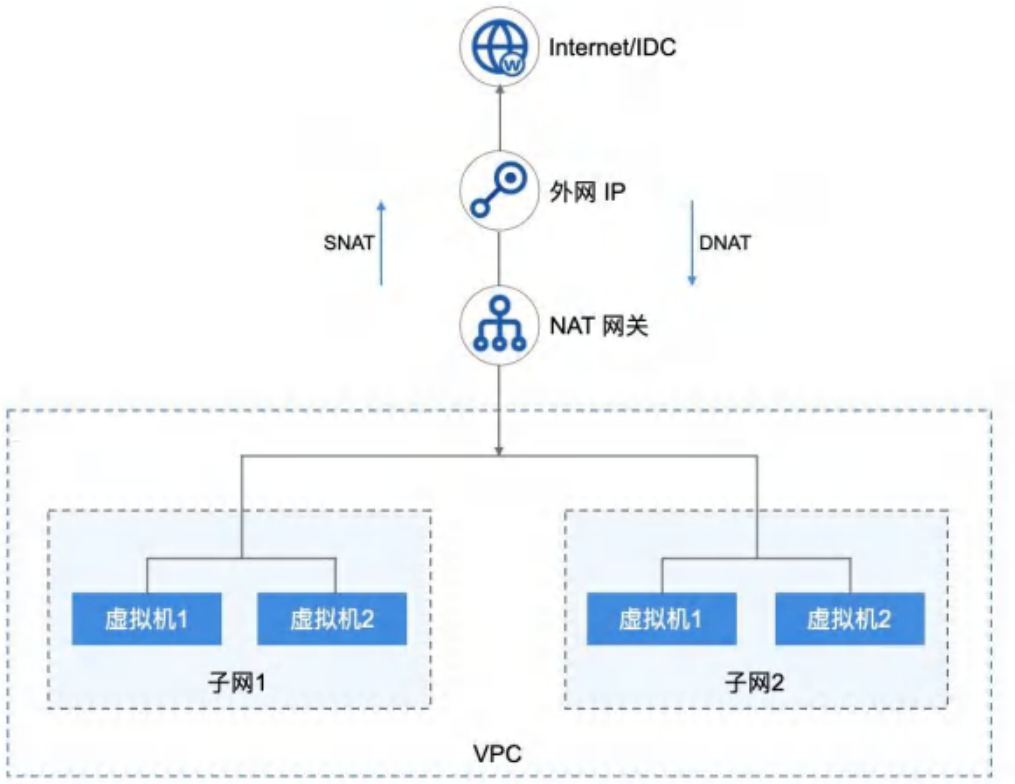
- **VPC 内网虚拟机提供外网服务**

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。

6.8.1.3 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 SNAT 和 DNAT 规则为租户虚拟资源提供 SNAT 和 DNAT 代理服务。

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 VPC 网络，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。

6.8.1.4 功能特性

云平台提供高可用 NAT 网关服务，并支持网关的全生命周期管理，包括外网 IP、SNAT 规则及 DNAT 端口转发及监控告警，同时为 NAT 网关提供网络及资源隔离的安全保障。

一个 VPC 允许创建 20 个 NAT 网关，相同 VPC 下所有 NAT 网关中 SNAT 规则不可重复，即 20 个 NAT 网关中的 SNAT 规则不允许重复。场景举例：

- 当 NATGW(VPC：192.168.0.0/16）中创建了子网（192.168.0.1/24）的 SNAT 规则，则相同 VPC 下 NATGW 不可在创建子网（192.168.0.1/24）为源地址的 SNAT 规则，当 NATGW01 中该子网规则删除后，才可进行创建。
- 当 NATGW(VPC：192.168.0.0/16）中创建了 VPC 级别的规则，则相同 VPC 下不可在创建 VPC 级别的规则。
- 当 NATGW(VPC：192.168.0.0/16）中创建了虚拟机（192.168.1.2）的 SNAT 规则，则相同 VPC 下 NATGW 不可在创建虚拟机（192.168.1.2）为源地址的 SNAT 规则。

6.8.1.4.1 SNAT 规则

NAT 网关通过 SNAT 规则支持 SNAT（Source Network Address Translation 源地址转换）能力，每条规则由源地址和目标地址组成，即将源地址转换为目标地址进行网络访问。平台 SNAT 规则支持多种场景的出外网场景，即源地址包括 VPC、子网、虚拟机三种类型：

- **VPC 级别**

指 NAT 网关所属 VPC 下的所有虚拟机可通过 NAT 网关访问外网。

- **子网级别**

指 NAT 网关所属 VPC 下被指定子网中的所有虚拟机可通过 NAT 网关访问外网。

- **虚拟机级别**

指 NAT 网关所属 VPC 下被指定的虚拟机才可通过 NAT 网关访问外网。

规则的目标地址为 NAT 网关绑定的外网 IP 地址，通过规则策略即可将源地址在 VPC、子网、虚拟机的 IP 地址转换为网关绑定的外网 IP 进行网络通信，即通过 SNAT 规则虚拟机可在不绑定外网 IP 的情况下与平台外网进行通信，如访问 IDC 数据中心网络或互联网。

SNAT 规则中不同源地址类型的规则优先级不同，以优先级高的规则为准：

（1）源地址为 VPC

- NAT 网关所属 VPC 下所有虚拟机均可通过 NAT 网关访问外网。

（2）源地址为子网 CIDR

- 每个子网仅可创建一条 SNAT 规则，不允许重复。
- 支持为子网下虚拟机单独配置 SNAT 规则，优先级高于源地址为 VPC 的 SNAT 规则。

（3）源地址为虚拟机 IP

- 虚拟机可通过 NAT 网关访问外网。
- 每个虚拟机 IP 仅可创建一条 SNAT 规则，不允许重复。
- 源地址为虚拟机 IP 的 SNAT 规则优先级高于源地址为子网的 SNAT 规则。
- 已绑定 EIP 的虚拟机不允许创建源地址为虚拟机 IP 的 SNAT 规则。

注意：一个 NAT 网关默认可创建 100 条 SNAT 规则。

用户配置 SNAT 规则后，NAT 网关会自动下发默认路由至源地址匹配的虚拟机，使虚拟机通过 SNAT 规则的外网 IP 访问外网。具体通信逻辑如下：

- 虚拟机未绑定 IPv4 外网 IP，则默认通过 NAT 网关访问外网。
- 虚拟机已绑定 IPv4 外网 IP 且存在默认网络出口，则通过虚拟机默认网络出口访问外网。
- 虚拟机已绑定 IPv4 外网 IP 且无默认网络出口，则通过 NAT 网关访问外网。

虚拟机通过 NAT 网关访问外网时，使用的外网 IP 取决于 SNAT 规则的配置，会把外网 IP 地址作为虚拟机的出口。

6.8.1.4.2 DNAT 规则

NAT 网关支持 DNAT（Destination Network Address Translation 目的地址转换），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。

6.8.1.4.3 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。默认查询数提成为 1 小时的数据，最多可查看 1 个月的监控数据。

6.8.1.4.4 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。

6.8.1.4.5 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。为保证 NAT 网关的资源和网络安全，平台为 NAT 网关提供资源隔离及网络隔离机制：

（1）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。

（2）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。

6.8.2 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，并根据业务需求配置 SNAT 和 DNAT 规则。具体流程如下：

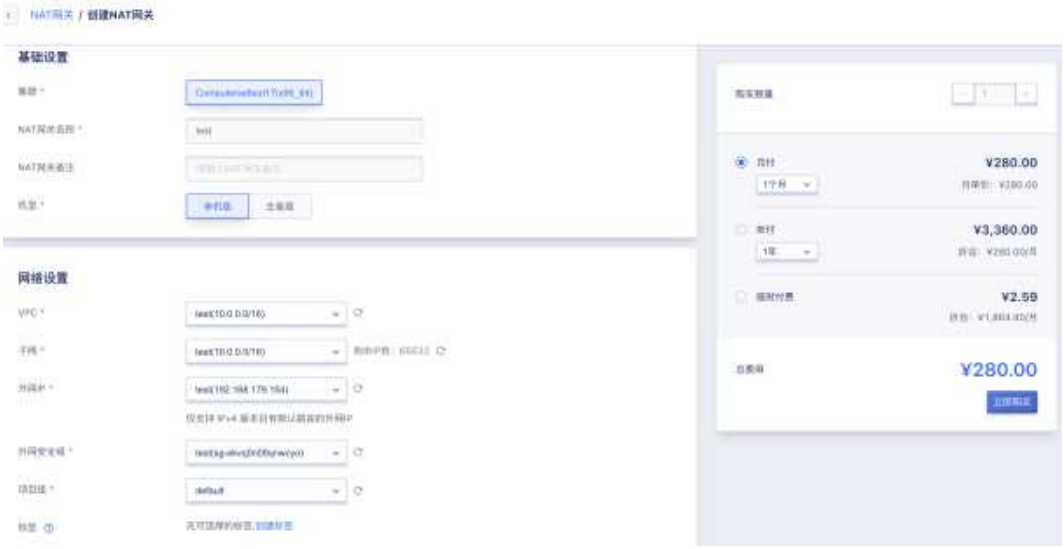
1. 租户根据需求创建 VPC 和子网，并在多个子网中创建虚拟机；
2. 租户根据需求创建外网 IP 地址，并通过 API 或控制台指定网络类型、关联子网及绑定的出口 IP 地址，创建一个 NAT 网关；
3. 通过 SNAT 规则添加 VPC、子网或虚拟机类型的 SNAT 规则，则关联的虚拟机可通过 NAT 网关访问外网；
4. 通过 DNAT 规则配置需要通过对外提供服务的虚拟机规则，则外网可访问 VPC 网络中未绑定外网 IP 的资源；
5. 如需对 NAT 网关的进出流量进行限制，可通过 NAT 网关绑定的安全组进行配置；

6. 可为 NAT 网关绑定外网 IP 地址，配置外网 IP 的 SNAT 规则和 DNAT 规则。

6.8.3 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。一个 VPC 允许创建 20 个 NAT 网关，相同 VPC 下所有 NAT 网关中 SNAT 规则不可重复，即 20 个 NAT 网关中的 SNAT 规则不允许重复。

用户可通过导航栏进入【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：



1. 选择并配置 NAT 网关基础配置及网络设置信息：

- **集群**：NAT 网关实例所在节点的集群类型，由平台管理员自定义，如 x86 机型和 ARM 机型，通过 ARM 机型创建的实例为 ARM 版 NAT 网关实例，已适配国产芯片、服务器及操作系统。
- **名称/备注**：NAT 网关的名称及备注信息。
- **机型**：NAT 网关支持单机版和主备版。
- **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，同时仅支持添加所属 VPC 网络

的资源作为 SNAT 规则的源地址及 DNAT 规则的目标地址。

- **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。
- **项目组**：设置实例所属项目，默认为 default。
- **标签**：选择对应的资源标签，便于管理。

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“运行中”。

注意：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。

6.8.4 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。

6.8.4.1 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：

- **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。
- **VPC 网络**：NAT 网关所服务的 VPC 网络，即 NAT 网关仅为 VPC 内的资源提供 SNAT 和 DNAT 服务，同时仅支持添加所属 VPC 网络的资源作为 SNAT 规则的源地址及 DNAT 规则的目标地址。
- **子网**：仅代表 NAT 网关实例所在子网
- **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。

6.8.4.2 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 SNAT 规则、DNAT 规则、外网 IP 管理页面，分别管理当前 NAT 网关的 SNAT 规则、DNAT 规则及绑定的外网 IP 管理，如概览页所示：

（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）SNAT 规则

NAT 网关的 SNAT 规则管理，即可通过 NAT 网关访问外网的虚拟资源及出口 IP 管理，包括 SNAT 规则的添加、查看、修改及删除操作，详见。

（4）DNAT 规则

NAT 网关的 DNAT 规则管理，即可通过 NAT 网关外网 IP 访问 VPC 内虚拟

资源的端口映射管理，包括 DNAT 规则的添加、查看、修改及删除操作，详见。

（5）外网 IP 管理

NAT 网关的外网 IP 管理，即已绑定至 NAT 网关的外网 IP 地址管理，包括外网 IP 查看、绑定及解绑操作，详见。

6.8.5 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。

6.8.6 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 SNAT/DNAT 规则及路由策略。

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，否则可能影响业务访问。

6.8.7 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。

6.8.8 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。

6.8.9 NAT 网关续费

支持用户手动对 NAT 网关进行续费，续费操作只针对资源本身，不对资源额外关联的资源进行续费，如绑定的外网 IP 资源。额外关联的资源到期后，会自动从 NAT 网关进行解绑，为保证业务正常使用，需及时对相关资源进行续费操作。

NAT 网关续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

NAT 网关续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当 NAT 网关的计费方式为【小时】，则续费时长指定为 1 小时；当 NAT 网关的计费方式为【按月】，则续费时长可选择 1 至 11 月；当 NAT 网关的计费方式为【按年】，则续费时长为 1 至 5 年。

6.8.10 SNAT 规则

NAT 网关通过 SNAT 规则支持 SNAT（Source Network Address Translation 源地址转换）能力，每条规则由源地址和目标地址组成，即将源地址转换为目标地址进行网络访问。

平台 SNAT 规则支持多种场景的出外网场景，即源地址包括 VPC、子网、虚拟机三种类型。通常只需要指定一条 VPC 类型的 SANT 规则，即可实现 NAT 网关所属 VPC 网络下所有虚拟机访问外网的能力。

SNAT 规则仅支持 SNAT 能力，不对 DNAT 端口转发能力进行限制，即添加至 SNAT 规则的虚拟机可通过 NAT 网关访问外网或 IDC 物理网；若虚拟机需要同时对外网提供业务服务，则可同时针对虚拟机配置 DNAT 规则。

6.8.10.1 创建 SNAT 规则

用户创建一条 SNAT 规则，为指定虚拟资源指定访问外网的 IP 地址，规则内的源地址资源必须与 NAT 网关处于相同的 VPC 网络。用户可通过 NAT 网关详情页面“SNAT 规则”控制台中的“创建 SNAT 规则”进入规则添加向导页面，如下图所示：

在向导页面，用户需指定 SNAT 规则的源地址类型、子网、虚拟机及外网 IP，源地址是需要通过 NAT 网关访问外网的资源类型；子网是指通过 NAT 网关访问外网的子网 CIDR；虚拟机指通过 NAT 网关访问外网的虚拟机 IP 地址；外网 IP 是指资源访问外网时的出口 IP 地址。

（1）源地址类型

指定 SNAT 规则的源地址类型，包括 VPC 级别、子网级别、虚拟机级别，一条规则仅支持一种类型的规则。

- **VPC 级别**：指当前 NAT 网关所属 VPC 下所有的虚拟机均可通过 NAT 网关访问外网，一个 VPC 下所有 NAT 网关仅支持指定一条 VPC 级别的 SNAT 规则。
- **子网级别**：指当前指定的子网下所有虚拟机均可通过 NAT 网关访问外网，子网 SNAT 规则优先级高于源地址类型为 VPC 类型的规则。
- **虚拟机级别**：指当前指定的虚拟机可通过 NAT 网关访问外网，虚拟机

类型的 SNAT 规则优先级高于 VPC 和子网类型的 SNAT 规则。

（2）子网

仅当源地址类型为子网时指定，可指定 NAT 网关所属 VPC 的子网，每个子网仅可创建一条 SNAT 规则，如 VPC CIDR 为 192.168.0.0/16，子网可指定 192.168.1.1/24。

（3）虚拟机

仅当源地址类型为虚拟机时指定，可指定 NAT 网关所属 VPC 的虚拟机，每个虚拟机 IP 仅可创建一条 SNAT 规则，如 VPC CIDR 为 192.168.0.0/16，虚拟机可指定 192.168.1.2。

（4）外网 IP

指当前 SNAT 规则源地址访问外网时指定的出口 IP 地址，仅支持选择绑定至 NAT 网关的外网 IP。

添加 SNAT 规则成功后，平台会自动下发默认路由至规则中指定的虚拟机，使虚拟机可通过 NAT 网关访问互联网或 IDC 数据中心网络，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，并在虚拟机中检测与外网的联通性。

注意：SNAT 规则添加成功后，平台仅会下发默认路由至无 IPv4 默认路由的 VM，针对有默认路由的虚拟机会自动通过 VM 自身的默认路由访问外网。

6.8.10.2 查看 SNAT 规则

用户通过 NAT 网关详情页面的“SNAT 规则”可查看已添加至当前网关的 SNAT 规则列表及信息，包括资源 ID、源地址类型、源地址、外网 IP、状态、创建时间及操作项，如下图所示：

- **资源 ID**：已添加 SNAT 规则的全局唯一标识符。
- **源地址类型**：当前 SNAT 规则的源地址类型，如 VPC 级别、子网级别、虚拟机级别。
- **源地址**：当前指 SNAT 规则的源地址资源的 CIDR 或 IP 地址：
  - 当源地址类型为 VPC 时，源地址为 VPC 的 CIDR 网段和名称；
  - 当源地址类型为子网时，源地址为指定的子网 CIDR 网段和名称；
  - 当源地址类型为虚拟机时，源地址为指定的虚拟机内网 IP 和名称。
- **外网 IP**：当前 SNAT 规则的目标外网 IP 地址。
- **状态**：指当前 SNAT 规则的状态，包括创建中、可用、删除中。
- **创建时间**：指当前 SNAT 规则的创建时间。

列表上操作项是指对单条 SNAT 规则的操作，支持删除。可通过搜索框对 SNAT 规则进行搜索和筛选，支持模糊搜索。同时为方便租户对资源的维护支持对 SNAT 规则进行批量删除操作。

6.8.10.3 删除 SNAT 规则

支持用户删除 SNAT 规则，规则删除后将会立即销毁，规则关联的 SNAT 能力即时失效。可在控制台 SNAT 规则列表上删除 SNAT 规则，并支持批量删除，如下图所示：

删除过程中，SNAT 规则的状态为【删除中】，待列表上 SNAT 规则被清除即代表删除成功。删除 SNAT 规则不影响虚拟机本身的正常运行，自动下发的路由将被清除，即不可通过 NAT 网关访问外网，可通过重新添加 SNAT 规则或绑定外网 IP 地址访问外网。

6.8.11 DNAT 规则

DNAT 规则是 NAT 网关提供 DNAT 服务的入口，支持 TCP 和 UDP 两种转发协议。用户可通过端口转发为 NAT 网关配置端口映射，将 VPC 子网内虚拟机内网端口映射到 NAT 网关的外网 IP，使虚拟机可对外网提供服务。

每条规则由协议、源 IP（外网 IP）、端口、目的 IP（虚拟机 IP）、目的端口五元组组成，即将源 IP 的端口请求转发至目的 IP 的端口，使用户直接通过源 IP 地址访问 VPC 内网虚拟机提供的服务。

6.8.11.1 添加 DNAT 规则

用户为一个 NAT 网关添加转发规则，用于支持 DNAT 代理。转发规则添加成功后，若目的 IP 虚拟机上运行服务正常，用户可通过 NAT 网关绑定的外网 IP 访问目的 IP 虚拟机提供的应用服务。

添加转发规则需用户指定 NAT 网关名称、协议、源 IP、源端口、目标 IP、目标端口及多端口，可通过 NAT 网关详情的【DNAT 规则】列表添加 DNAT 规则，如下图所示：

- 协议：指 DNAT 端口转发规则的转发协议，支持 TCP 和 UDP，创建时必须指定，默认为 TCP。
- 源 IP：DNAT 端口转发规则的源 IP 地址，即 NAT 网关的所绑定的外网 IP，一条规则仅支持一个外网 IP。
- 源端口：DNAT 端口转发规则的源端口，即 NAT 网关所绑定的外网 IP 暴露出来的端口。
  - 创建时必须指定源端口，端口范围为 1~65535。
  - 仅支持指定未创建的源端口，相同协议下不支持重复的源端口规则。
- 目的 IP：DNAT 端口转发规则的目的 IP，即 NAT 网关所属 VPC 网络下虚拟机的内网 IP 地址。
  - 创建时必须指定目的 IP 地址，仅支持指定 NAT 所属 VPC 下的虚拟机 IP 地址。
  - 目的 IP 地址不受 SNAT 规则限制，即一台虚拟机可同时添加 SNAT 规则和 DNAT 规则。
- 目的端口：DNAT 端口转发规则的目的端口，即目的 IP 虚拟机对外提供服务的端口。

- 创建时必须指定目的端口，端口范围为 1~65535。
- 目的端口可与源端口相同或不同，如源端口为 TCP:80，目的端口为 TCP:8080，即代表将源 IP 地址的 TCP 80 端口流量转发至目的 IP 地址 TCP 8080 端口。
- 支持创建同一目的 IP 重复的目的端口，如将两个源地址为的 80 端口均转发至同一个目的地址的相同端口进行业务数据处理。

- 端口范围：DNAT 规则还支持多端口映射规则，即支持指定源端口为连续范围，如 1024~1030；指定端口范围时，目的端口范围的数量必须与源端口一致。

相同协议情况，不支持重复的源端口规则。添加 DNAT 规则成功后，用户即可通过源 IP 地址访问目的虚拟机提供的应用服务。

6.8.11.2 查看 DNAT 规则

用户查看已添加的端口转发规则列表信息，包括转发规则协议、源 IP、源端口、目的 IP、目的端口、状态及操作项，如下图所示：

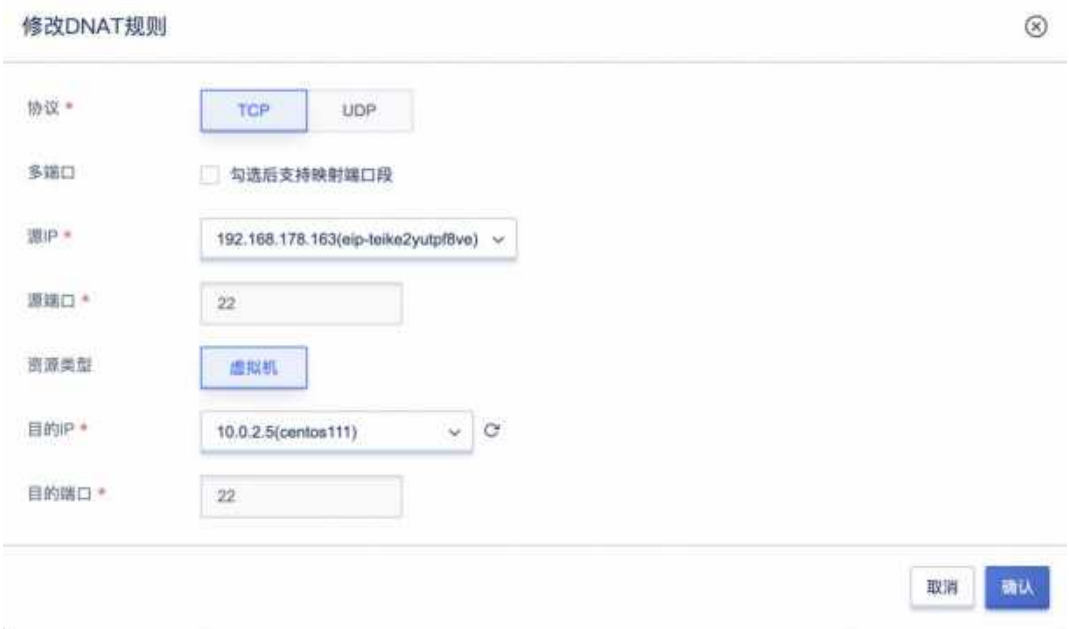
- **协议**：当前 DNAT 规则的协议，如 TCP 或 UDP。
- **源 IP**：当前 DNAT 规则的源 IP 地址，即当前规则所指定的外网 IP。
- **源端口**：DNAT 规则源 IP 地址的源端口。
- **目的 IP**：DNAT 规则端口转发的目的 IP 地址，即当前规则所指定的虚拟机 IP。

- **目的端口**：DNAT 规则目的 IP 地址的目的端口，即最终处理流量的端口。
- **状态**：当前 DNAT 规则的状态，包括创建中、可用、删除中。

列表上操作项是指对单条 DNAT 规则的操作，包括修改和删除；同时为方便租户对资源的维护支持对 DNAT 规则进行批量删除操作。

6.8.11.3 修改 DNAT 规则

用户修改已添加 DNAT 规则，包括协议、源 IP、源端口、目的 IP、目的端口，如下图所示：



用户修改源 IP 必须为 NAT 网关中已绑定的外网 IP 地址，修改后即时生效。

6.8.11.4 删除 DNAT 规则

用户可删除一条或多条 DNAT 转发规则，删除后即时生效，不可通过 DNAT 规则指定的外网 IP 地址访问目标 IP 地址的业务服务。如下图所示：

支持批量删除多条转发规则，规则被删除后即被销毁，删除前需谨慎操作。

6.8.12 外网 IP 管理

NAT 网关支持绑定 50 个默认路由类型的 IPv4 外网 IP 地址，为 NAT 网关指定子网的虚拟资源提供共享的外网 IP 资源池，以提供更加灵活便捷的 SNAT 及 DNAT 能力。

用户可通过外网 IP 管理查看 NAT 网关已绑定的外网 IP 地址及信息，同时支持对 NAT 网关的外网 IP 进行绑定和解绑操作。

6.8.12.1 查看绑定的外网 IP

用户可通过 NAT 网关详情【外网 IP 管理】标签页查看已绑定至 NAT 网关的外网 IP 地址列表及信息，包括资源 ID、IP、带宽、状态及操作项等，如下图所示：

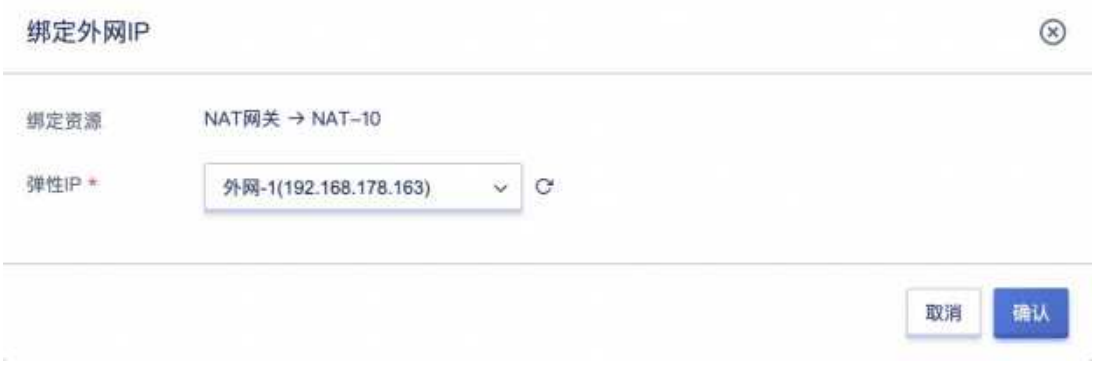
- **资源 ID**：当前已绑定至 NAT 网关的 EIP 全局唯一标识符。
- **IP 地址**：外网 IP 地址。
- **带宽**：外网 IP 地址的当前带宽，单位 Mb。

- **状态**：当前外网 IP 地址的状态，包括绑定中、已绑定、解绑中。

列表上操作项是指对单个外网 IP 地址的解绑操作，同时为方便租户对资源的维护，支持对已绑定的外网 IP 地址进行批量解绑操作。

6.8.12.2 绑定外网 IP

支持用户为 NAT 网关绑定 50 个默认路由类型的 IPv4 外网 IP 地址，为 NAT 网关的指定的虚拟资源提供共享外网 IP 池，提供灵活便捷的 SNAT 及 DNAT 能力。具体绑定操作如下图所示：



绑定成功后，用户添加 SNAT 和 DNAT 规则时，即可选择绑定的 IP 地址为 SNAT 的外网 IP 或 DNAT 的源 IP 地址。注：不支持绑定 IPv6 及非默认路由类型的 IPv4 外网 IP 地址。

6.8.12.3 解绑外网 IP

支持用户解绑 NAT 网关的外网 IP 地址，解绑后相关联的 SNAT 规则和 DNAT 规则网络通信都将失效。

- 解绑后，外网 IP 会自动从 SNAT 规则的外网 IP 池中清除。
- 解绑后，外网 IP 会自动从 DNAT 规则的源 IP 中清除。

用户可通过修改 SNAT 和 DNAT 规则，分别设置新的出口 IP 及入口源 IP 地址。

6.8.13 升级机型

支持用户将单机版 NAT 网关升级为主备版。

6.8.14 修改标签

支持用户修改 NAT 网关标签。

6.9 IPSecVPN

6.9.1 产品简介

6.9.1.1 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。

6.9.1.2 概述

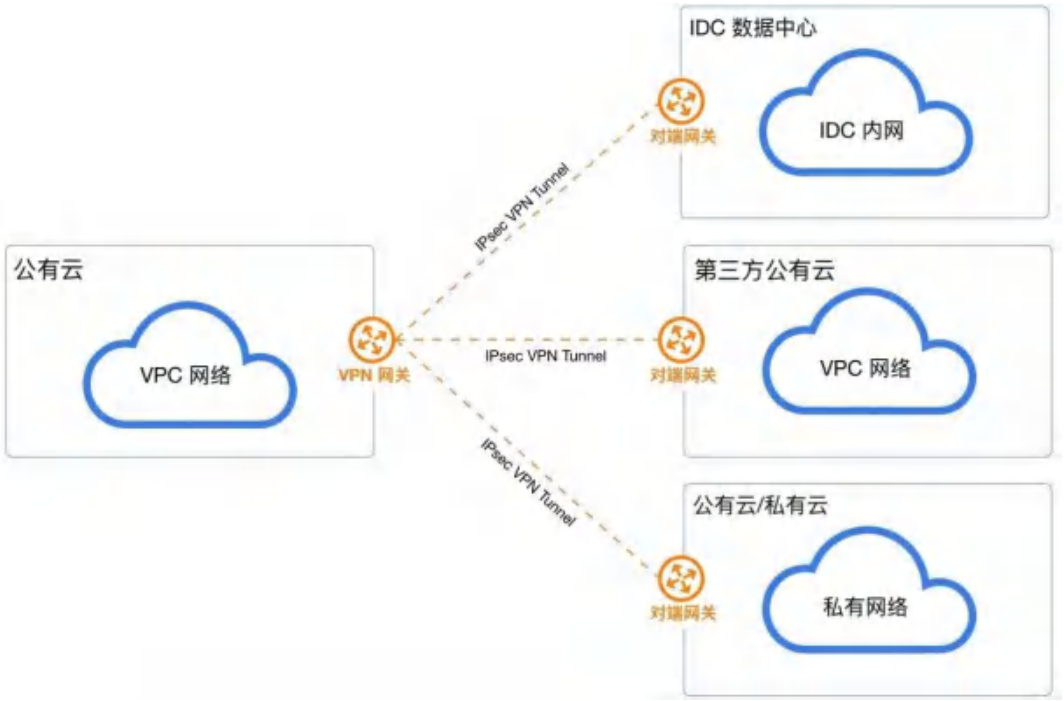
IPsec VPN 是一种采用 IPsec 协议加密的隧道技术，由 Internet Engineering Task Force（IETF）定义的安全标准框架，在互联网上为两个私有网络提供安全通道，通过加密保证连接的安全。有关 IPsec 可参考 RFC2409（IKE—Internet Key Exchange 因特网密钥交换协议）和 RFC4301（IPsec 架构）。

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。

6.9.1.3 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。

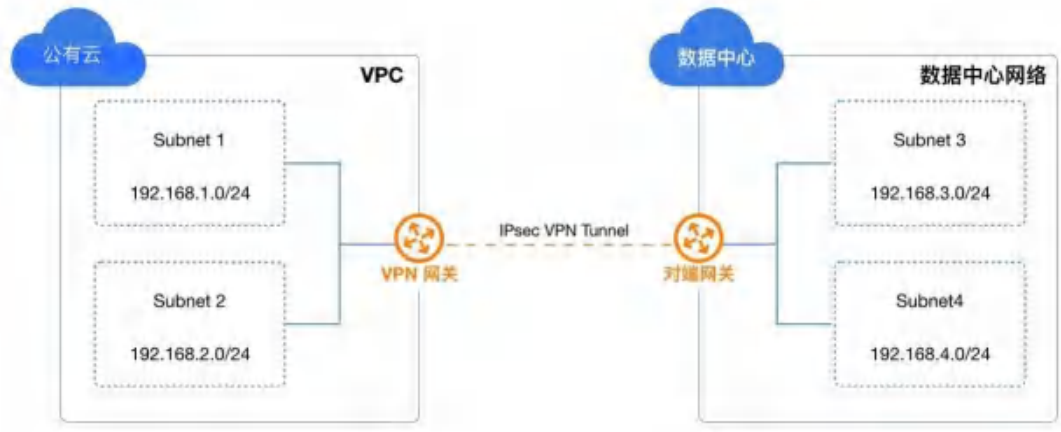
- **对端网关**

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。

6.9.1.4 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。

6.9.1.5 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。

6.9.1.6 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 与的另一个 VPC 网络进行连接，实现 VPC 打通的场景。

6.9.2 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 IPsev 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。

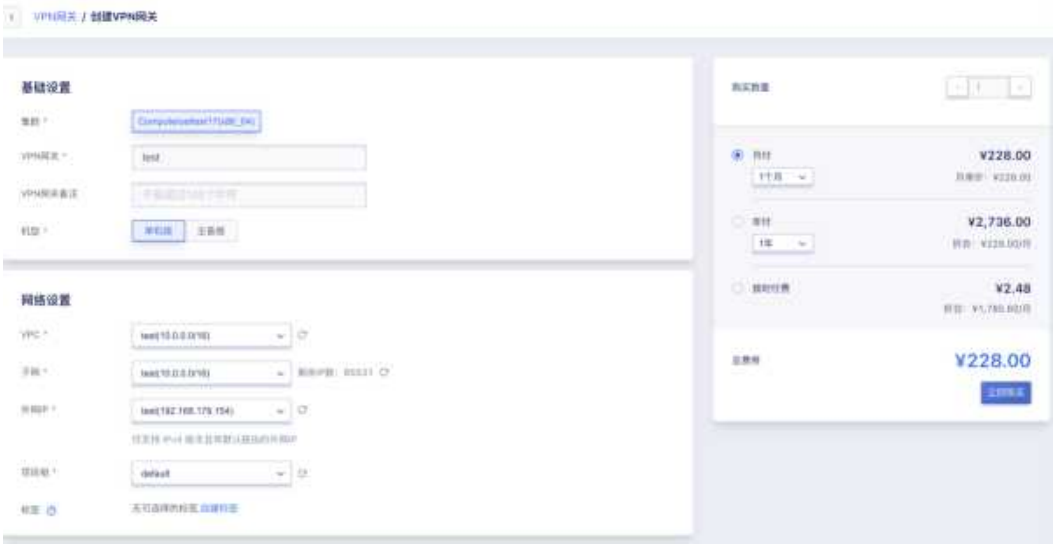
注意：IPSecVPN 服务是基于互联网的加密通信服务，在使用 IPSecVPN 前需确认两端网关均有固定或 NAT 后的互联网 IP 地址。

6.9.3 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。

6.9.3.1 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：



1. 选择并配置 VPN 网关基础配置及网络设置信息：

- **集群**：VPN 网关实例所在节点的集群类型，由平台管理员自定义，如 x86 机型和 ARM 机型，通过 ARM 机型创建的实例为 ARM 版 IPsecVPN 网关实例，已适配国产芯片、服务器及操作系统。
- **机型**：VPN 网关支持单机版和主备版
- **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。

- **项目组**：设置实例所属项目，默认为 default。
- **标签**：选择对应的资源标签，便于管理。

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”。

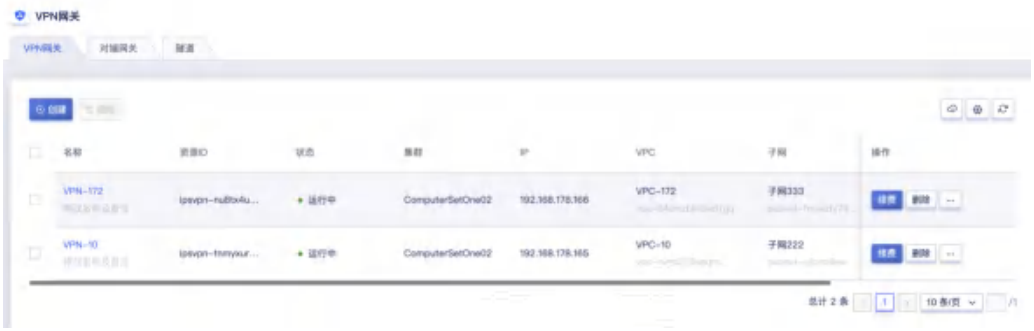
注：允许在一个 VPC 下创建多个 VPN 网关，将 VPC 下子网分别与不同的对端网关建立隧道，实现同 VPC 下不同子网与对端不同子网建立隧道的通信场景。

6.9.3.2 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。

6.9.3.2.1 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：



- 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。

6.9.3.2.2 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。

6.9.3.3 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。

6.9.3.4 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。

6.9.3.5 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。

6.9.3.6 VPN 网关续费

支持用户手动对 VPN 网关进行续费，续费操作只针对资源本身，不对资源额外关联的资源进行续费，如绑定的外网 IP 资源。额外关联的资源到期后，会自动从 VPN 网关进行解绑，为保证业务正常使用，需及时对相关资源进行续费操作。

VPN 网关续费时支持更改续费方式，只可由短周期改为长周期，例如按月的续费方式可更改为按月、按年。

VPN 网关续费时会按照续费时长收取费用，续费时长与资源的计费方式相匹配，当 VPN 网关的计费方式为【小时】，则续费时长指定为 1 小时；当 VPN 网关的计费方式为【按月】，则续费时长可选择 1 至 11 月；当 VPN 网关的计费方式为【按年】，则续费时长为 1 至 5 年。

6.9.3.7 升级机型

支持用户将单机版 VPN 网关升级为主备版。

6.9.3.8 修改标签

支持用户修改 VPN 网关标签。

6.9.4 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。

6.9.4.1 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。

6.9.4.2 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：

- **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。

6.9.4.3 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。

6.9.4.4 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。

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。

6.9.5 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。

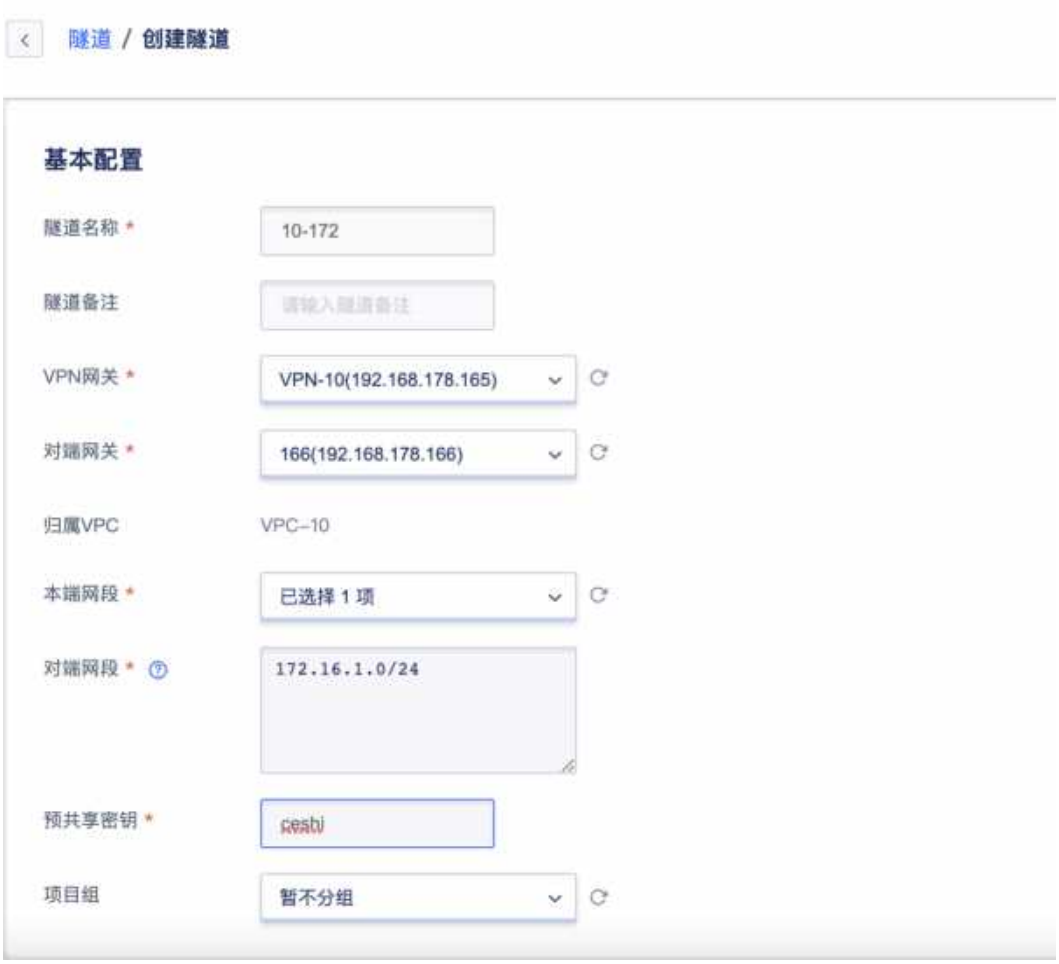
6.9.5.1 VPN 隧道配置流程

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。

6.9.5.2 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：



1. 选择配置 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，每个网段间用回车进行分隔，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。

1）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，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。

2）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。

6.9.5.3 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。

6.9.5.3.1 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/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。

6.9.5.3.2 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。

（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。

（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 IKE 配置信息进行修改，详见。

（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国。

6.9.5.4 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 ipsvpn_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
```

具体参数描述如下：

- 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。

6.9.5.5 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。

6.9.5.6 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：

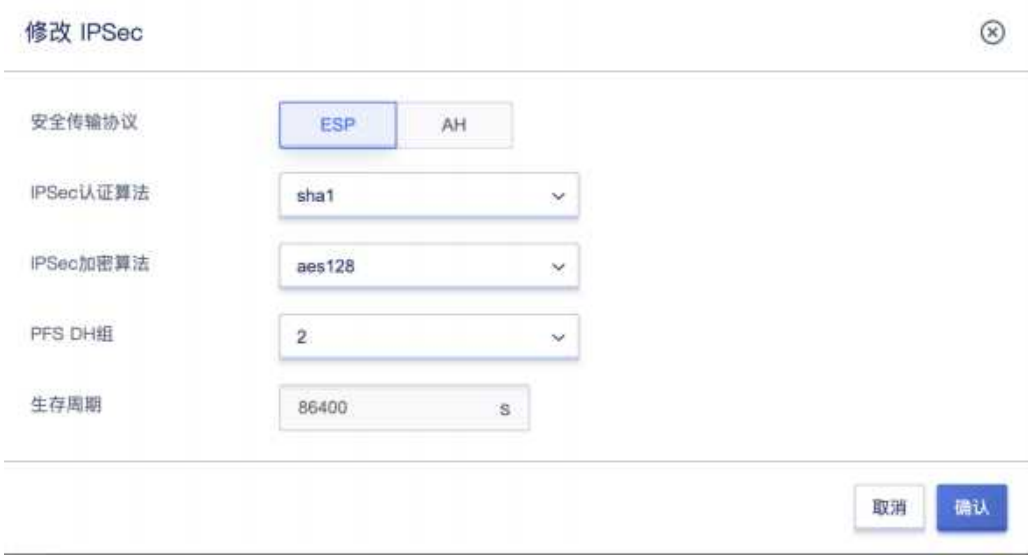
支持修改预共享密钥及 IKE 策略的所有配置参数，两端隧道的预共享密钥、IKE 版本、协商模式（IKEv1）、认证算法、加密算法、DH 组、本端标识、对端标识必须保持一致，生存周期可以不一致。

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。

6.9.5.7 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：



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。

6.9.5.8 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。

6.9.5.9 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。

6.9.5.10 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。

6.9.6 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

6.9.6.1 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。

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。

6.9.6.1.1 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、PFSDH 2	认证 SHA1、加密 AES128、PFSDH 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。

6.9.6.1.2 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。

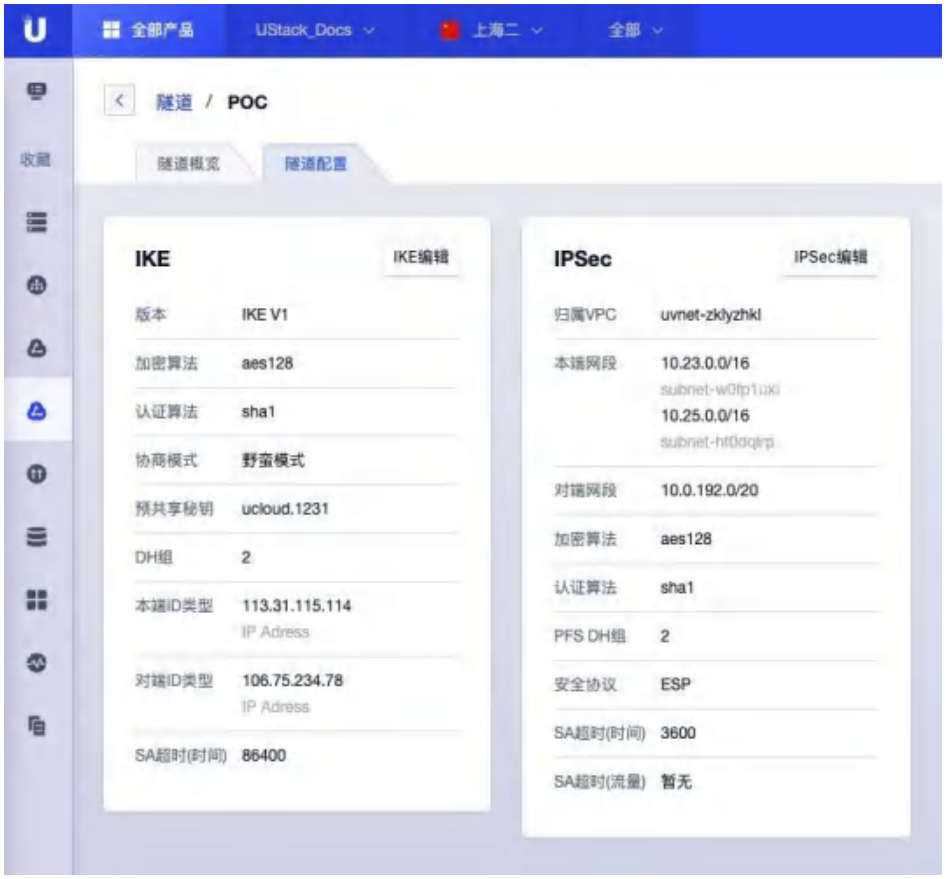
1. 使用 113.31.115.114 外网 IP 地址创建 VPN 网关，如下图所示：

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：

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。

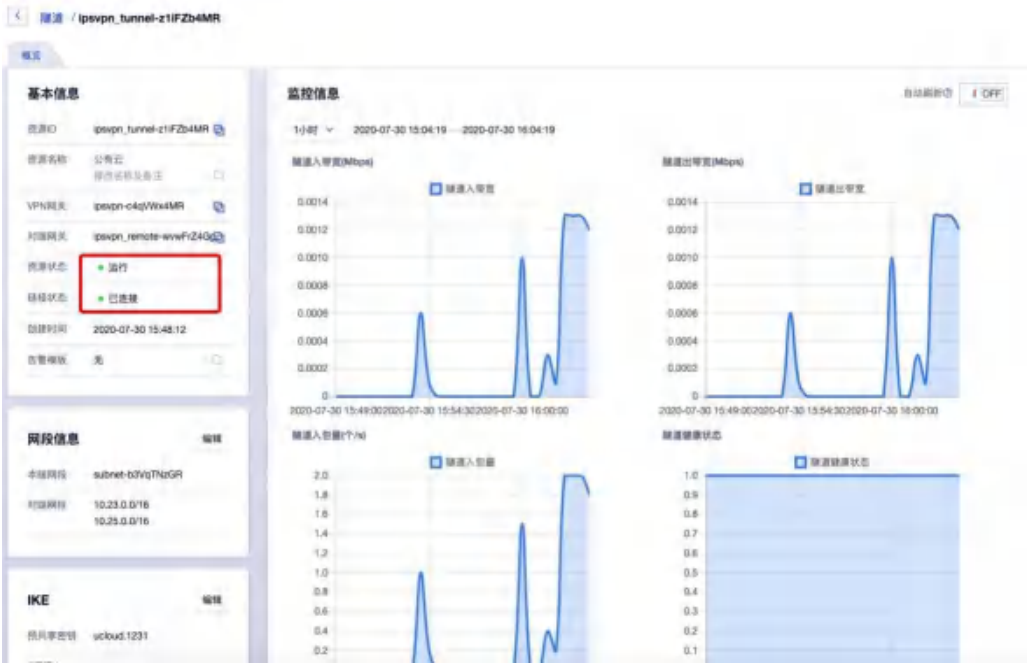
3. 使用已创建的 VPN 网关和客户网关，采用前提条件中的 IKE 和 IPSec 策略创建 VPN 隧道，如下图所示：



- 本端网段和对端网段与 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可查看“VPN 隧道状态”的监控。

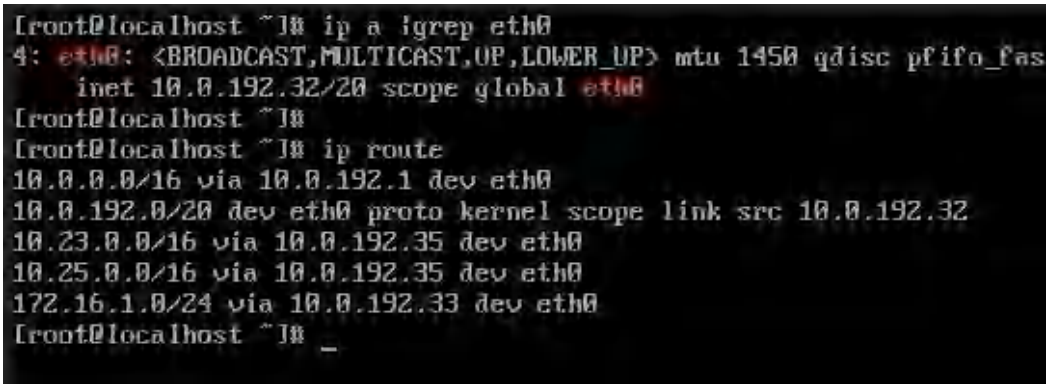
5. 在 UCloud 公有云的隧道监控中查看 VPN 隧道状态已变为 1，代表 VPN 已连接，同时在 UCloudStack 中隧道的连接状态流转为“已连接”，如下图所示：



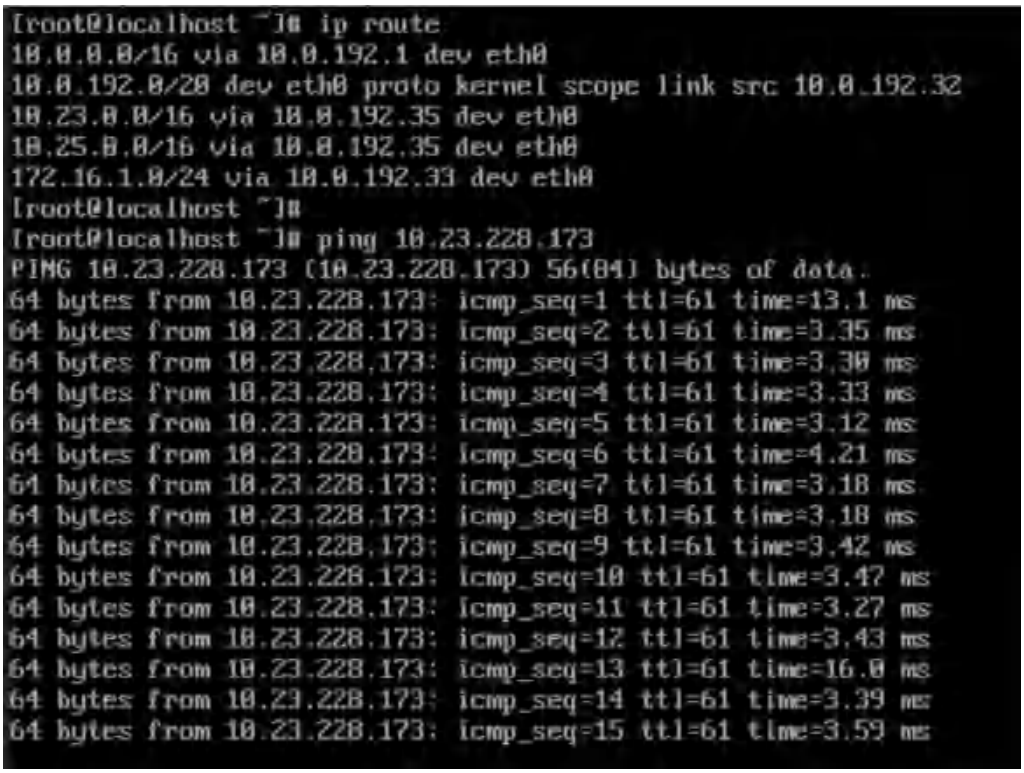
6.9.6.1.3 配置验证

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。



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。



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。

6.9.6.2 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。

6.9.6.2.1 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、PFSDH 2	认证 SHA1、加密 AES128、PFSDH 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。

6.9.6.2.2 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。若有多个网段，则需要分别对多个网段添加 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
```

6.9.6.2.3 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。

6.9.6.3 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。

6.9.6.3.1 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、PFSDH 5	认证 SHA1、加密 AES128、PFSDH 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。

6.9.6.3.2 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
```

6.9.6.3.3 配置验证

1. 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
```

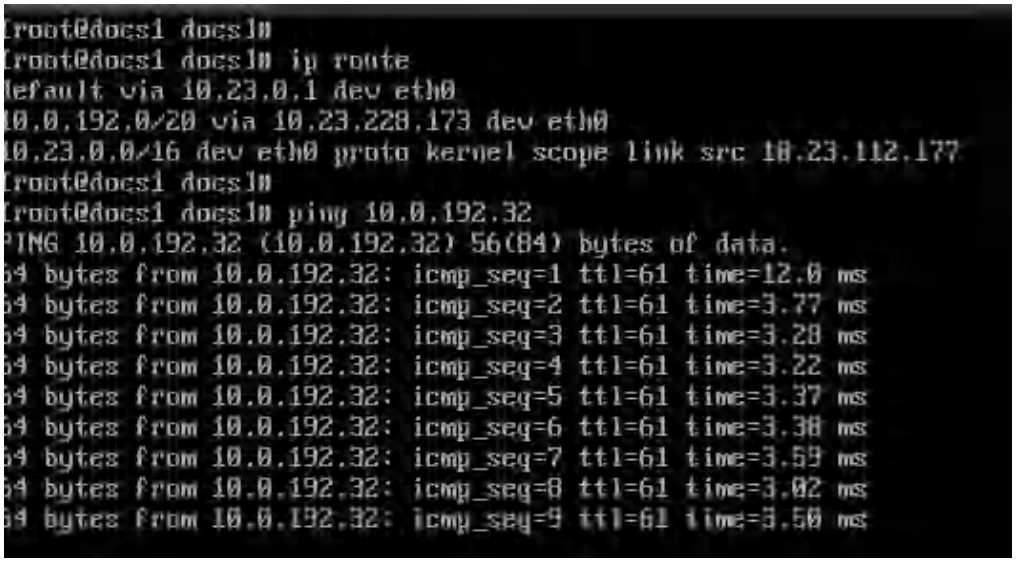


```
pgp dnskey sshkey pem openssl gcrypt fips-prf gmp curve25519 chapoly xcbc cmac hmac ctr ccm gcm curl attr kernel-netlink resolve socket-default farp stroke vici updown eap-identity eap-sim eap-aka eap-aka-3gpp eap-aka-3gpp2 eap-md5 eap-gtc eap-mschapv2 eap-dynamic eap-radius eap-tls eap-ttls eap-peap xauth-generic xauth-eap xauth-pam xauth-noauth dhcp led duplicheck 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
```

2. 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。



6.9.6.4 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 IKIEv2 ，本文描述在两个 VPC 网络间建立基于 IKEv2 版本的 IPSecVPN 连接。

6.9.6.4.1 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、PFSDH 2	认证 SHA1、加密 AES128、PFSDH 2

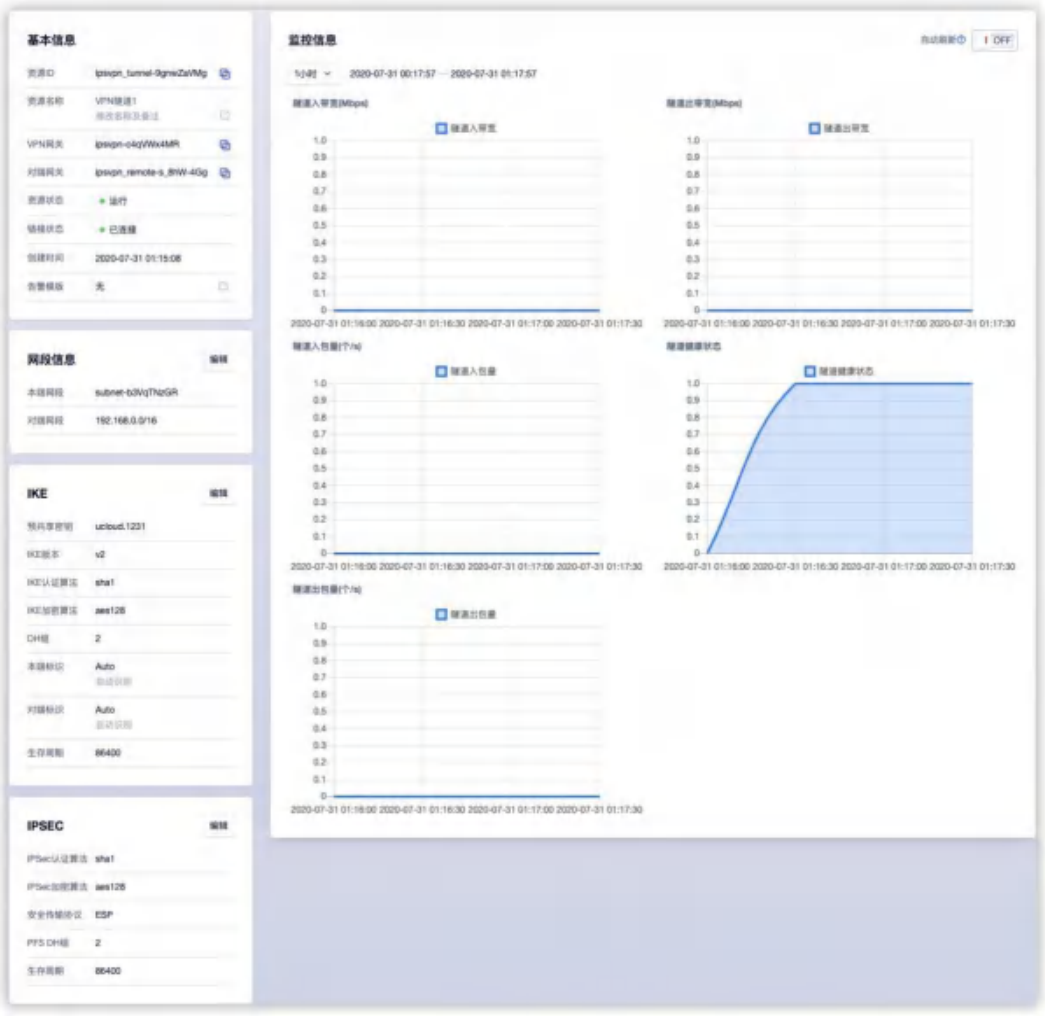
6.9.6.4.2 配置 VPN 网关和隧道

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。

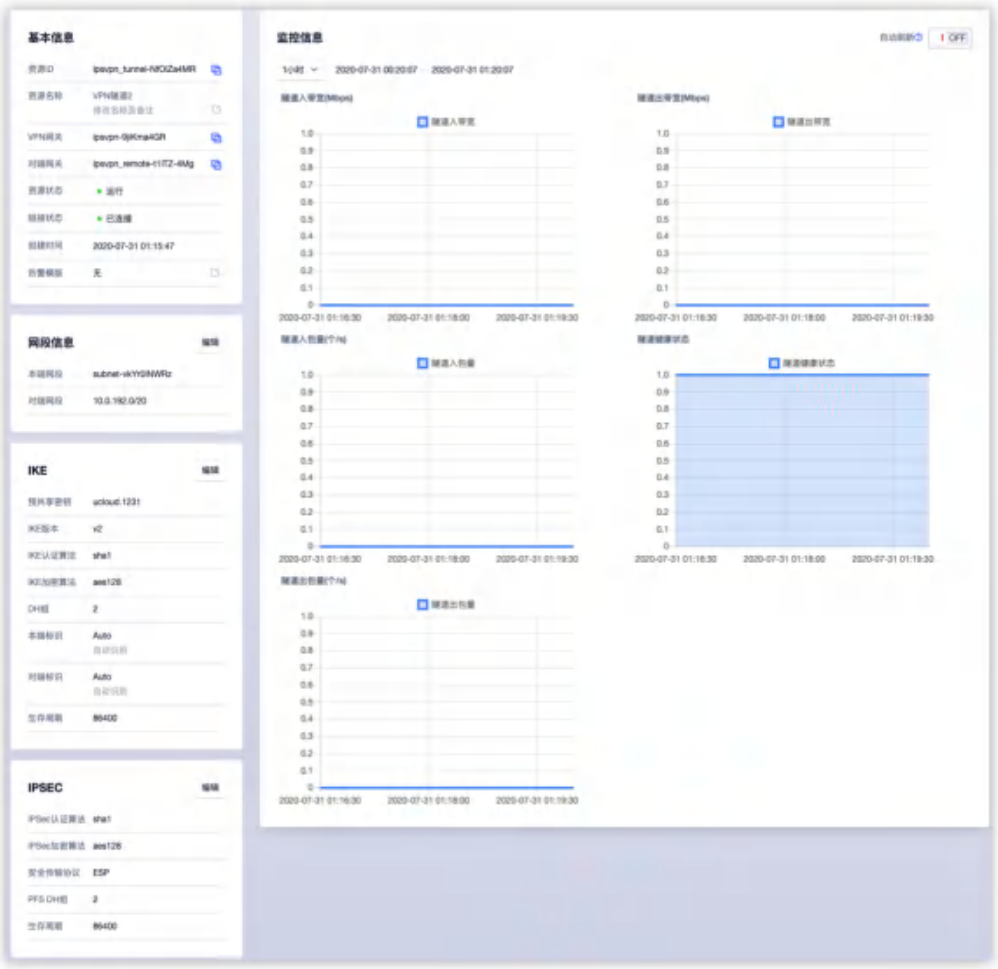
1. 分别在 VPC1 和 VPC2 中创建 VPN 网关，并确认两个网关地址分别为 106.75.234.78 和 106.75.234.74，如下图所示；

2. 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：

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：

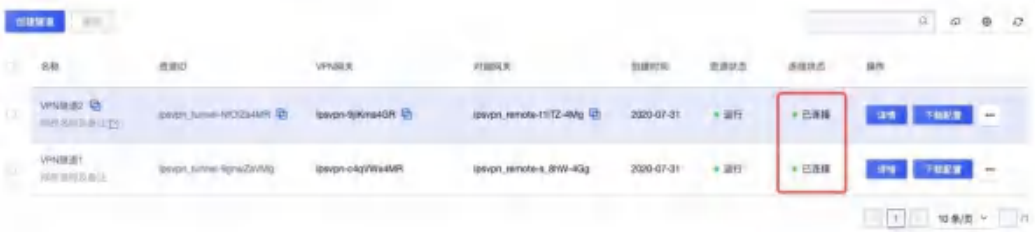


4. 使用 VPN 网关-VPC2 和对端网关 2 结合前提条件中的网段信息及参数配置创建 VPN 隧道 2，需确保网段信息与隧道 1 匹配，同时保证 IKE 策略、IPSec 策略与隧道 1 保持一致才可正常建立连接，如下图所示：



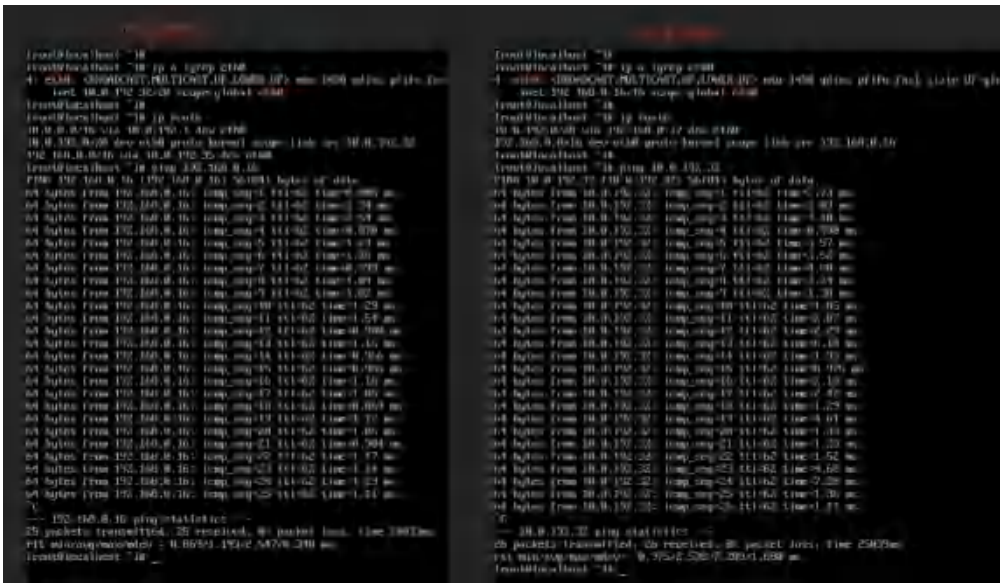
如图所示，隧道 2 的对端网段为 隧道的本端网段，IKE 及 IPSec 策略配置均和 隧道 1 一致，均使用 IKEv2 版本，IKE 策略均为：认证 SHA1、加密 AES128、DH 组 2 ，IPSec 策略均为：认证 SHA1、加密 AES128、PFSDH 2。

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：



6.9.6.4.3 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 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。

6.9.6.5 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端匹配规则不可相同，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：两端调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 HD 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。

7 数据库缓存服务

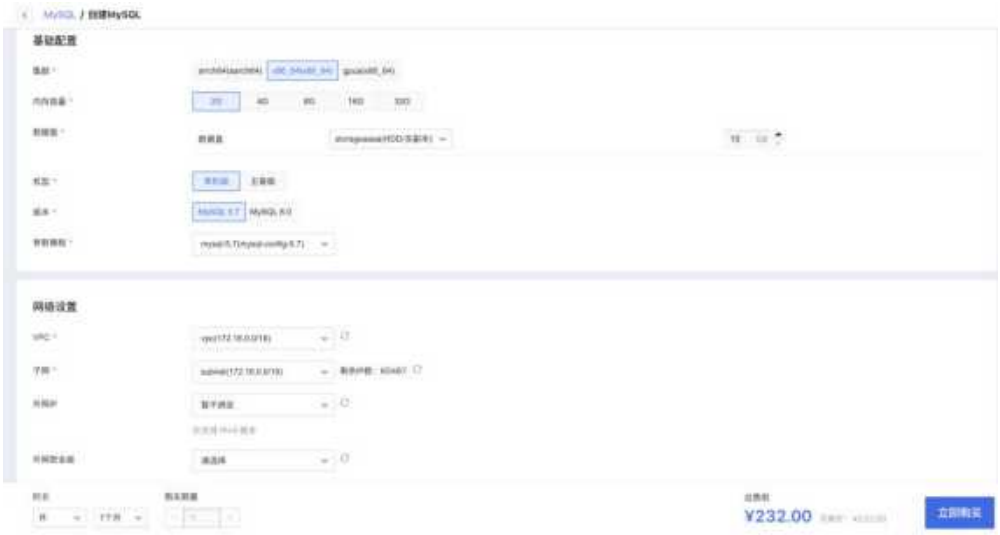
7.1 MySQL 服务

7.1.1 概览

MySQL 是平台提供的一种数据库服务，支持单机版和主备版两种机型，并提供了备份、升级机型、监控等功能。

7.1.2 创建 MySQL

平台用户可以通过指定集群、内存容量、数据盘、版本、参数模板、VPC、子网、外网 IP、外网安全组、MySQL 名称、密码等相关基础信息创建 MySQL，可通过导航栏进入[MySQL]资源控制台，通过“创建”按钮进入向导页面，如下图所示：



1. 选择并配置 MySQL 的基础配置、网络设置及管理配置信息：

- 集群：创建 MySQL 的集群信息，支持 X86 集群；
- 内存容量：选择创建 MySQL 的内存容量，支持 2G、4G、8G、16G、32G;
- 数据盘：创建 MySQL 的数据信息，可选容量 10-32000GB；
- VPC 和子网：创建 MySQL 时必须选择 VPC 网络和所属子网，即选择要加入的网络及 IP 网段；
- 外网 IP：外网 IP 为 MySQL 提供外网访问服务，支持创建 MySQL 时申请并绑定一个外网 IP 作为外网访问地址，MySQL 支持最多绑定一个外网 IP；

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 Mysql 的创建：

- 购买数量：默认支持创建 1 个 MySQL；
- 付费方式：选择 MySQL 的计费方式，支持按月、按年、按时三种方式，可根据需求选择合适的付费方式；
- 合计费用：用户选择 MySQL 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 MySQL 资源列表页，在列表页可查看 MySQL 的创建过程。

7.1.3 查看 MySQL 列表

平台支持用户查看 MySQL 列表信息，包括名称、资源 ID、状态、机型、集群、存储类型、版本、IP、内存容量、数据盘容量、VPC、子网、安全组、计费方式、项目组、创建时间、过期时间、操作。可通过导航栏进入[MySQL]资源控制台查看，如下图所示：

- 名称：MySQL 的名称，可点击进入 MySQL 详情页；
- 资源 ID：MySQL 的资源 ID，作为全局唯一标识；
- 状态：MySQL 的状态，包括启动中、更改配置中、删除中等；
- 机型：MySQL 的机型信息，支持单机版和主备版；

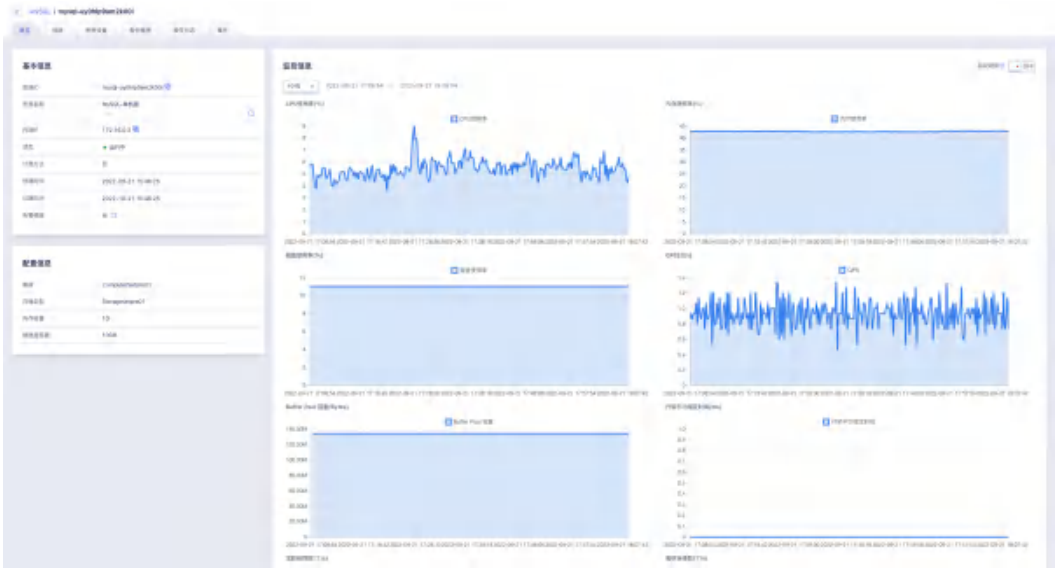
版本：MySQL 的版本信息，目前支持 MySQL 5.7 和 MySQL 8.0；

- IP：MySQL 的网络信息，包括内网 IP 和外网 IP；
- 内存容量：MySQL 创建时选择的内存容量信息，可通过配置升级功能升级内存容量；
- 数据盘容量：MySQL 创建时选择的数据盘容量，可通过配置升级功能升级数据盘容量；
- VPC/子网：MySQL 内网信息，包括 VPC/子网的名称和资源 ID；
- 安全组：MySQL 绑定外网 IP 后支持关联安全组；
- 计费方式：MySQL 资源的计费方式，支持小时、月、年；
- 项目组：MySQL 资源所属的安全组，可通过安全组的转入/转出功能修改关联关系；
- 创建时间/过期时间；MySQL 的创建时间和过期时间；

MySQL 资源的可操作项内容，包括创建从库、删除、续费、重置密码、应用参数模板、配置升级、升级至主备版、修改告警模板、绑定外网 IP、解绑外网 IP、修改安全组等。

7.1.4 查看 MySQL 概览信息

平台支持用户查看 MySQL 资源概览信息，包括基本信息、配置信息、监控信息。可通过点击 MySQL 列表中的名称进入概览页面，如下图所示：

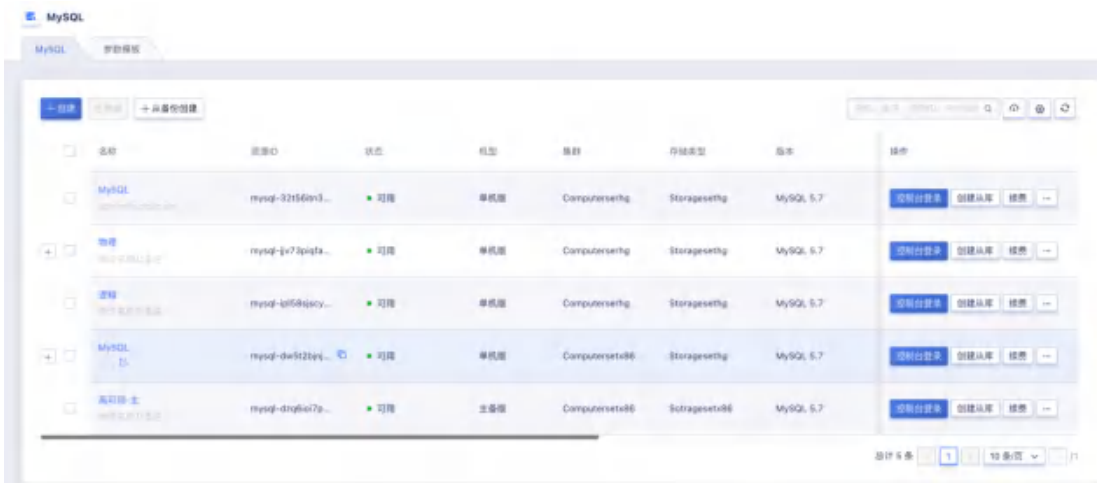


7.1.5 MySQL 控制台登录

平台支持用户，通过页面登录管理页面对数据库进行管理操作，如下图所示：

7.1.6 MySQL 创建从库

平台支持用户对 MySQL 主库进行创建从库的操作，可选择内存容量、数据盘容量、外网 IP、安全组，可通过 MySQL 列表中操作项的“创建从库”按钮进行操作，如下图所示：



每个 MySQL 主库支持最多创建 5 个从库。

7.1.7 MySQL 续费

平台支持用户对 MySQL 进行续费操作，可通过 MySQL 列表中操作项的“续费”按钮进行操作，如下图所示：

续费支持更改续费方式和续费时长，更改续费方式只支持由短周期改为长周期，比如从“小时”更改为“月”。

7.1.8 MySQL 重置密码

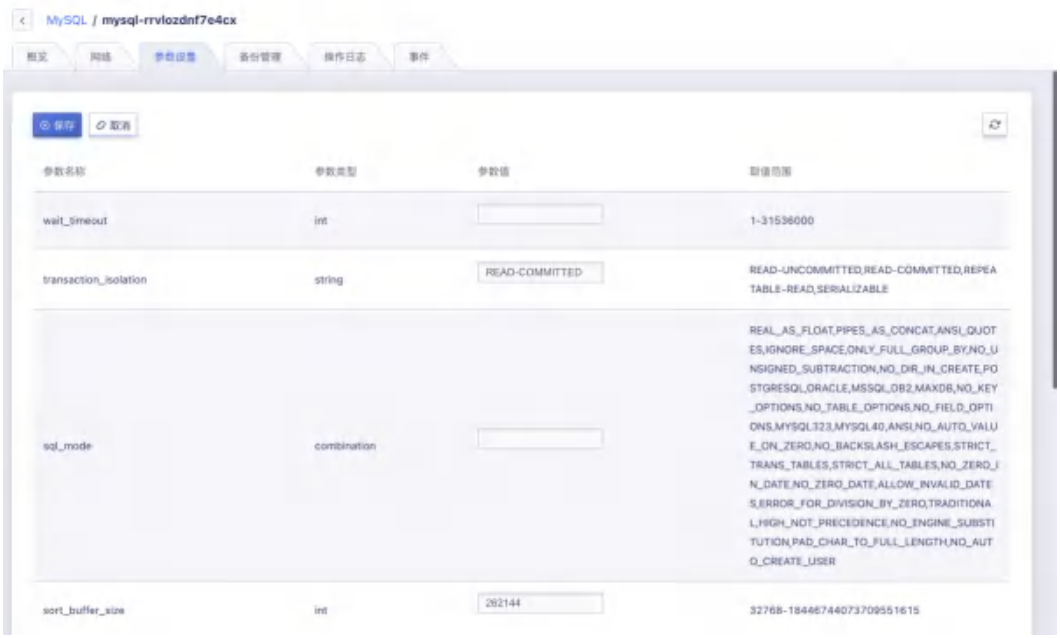
平台支持用户对 MySQL 进行重置密码操作，可通过 MySQL 列表中操作项的“重置密码”按钮进行操作，如下图所示：

7.1.9 参数配置

平台支持用户对 MySQL 进行参数配置相关操作，包括修改实例参数、应用参数模板、导入参数文件、导出为模板、导出参数文件。可点击 MySQL 名称进入详情页，切换到“参数设置”页面查看，如下图所示：

7.1.9.1 修改实例参数

平台支持用户对 MySQL 进行修改实例参数操作，可点击“修改实例参数”按钮进行操作，如下图所示：



7.1.9.2 应用参数模板

平台支持用户对 MySQL 进行应用参数模板操作，可点击“应用参数模板”进行操作，也可通过 MySQL 列表操作项的“应用参数模板”进行操作，如下图所示：

7.1.9.3 导入参数文件

平台支持用户对 MySQL 进行导入参数文件操作，可点击“导入参数文件”进行操作，如下图所示：

7.1.9.4 导出为模板

平台支持用户对 MySQL 参数配置进行导出为模板操作，可点击“导出为模板”进行操作，如下图所示：

导出为模板操作成功后，参数模板列表新增一条模板数据。

7.1.9.5 导出参数文件

平台支持用户对 MySQL 参数配置进行导出参数文件操作，可点击“导出参数文件”进行操作，下载参数配置文件。

7.1.10 配置升级

平台支持用户对 MySQL 进行配置升级操作，包括内存容量和数据盘容量更改。可点击 MySQL 列表中操作项的“配置升级”按钮进行操作，如下图所示：

7.1.11 升级主备版

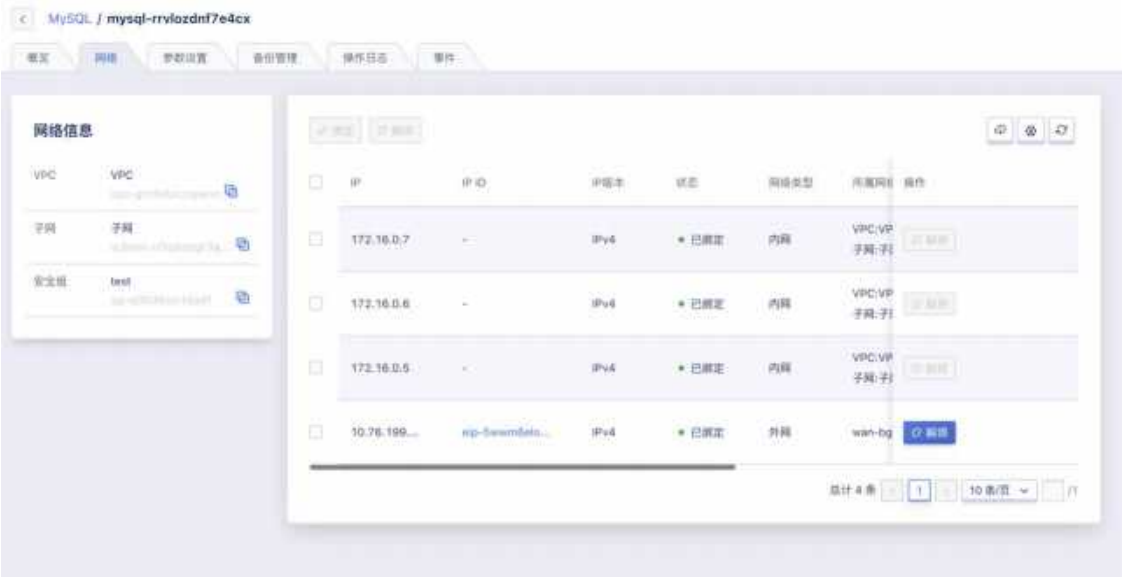
平台支持用户对单机版 MySQL 进行升级至主备版操作，计算集群、内存容量、存储集群、数据盘容量不可修改。可点击 MySQL 列表中操作项的“升级至主备版”按钮进行操作，如下图所示：

7.1.12 修改告警模板

平台支持用户对 MySQL 进行修改告警模板操作。可点击 MySQL 列表中操作项的“修改告警模板”按钮进行操作，如下图所示：

7.1.13 MySQL 网络

平台支持用户查看 MySQL 的网络信息，包括基本信息和 IP 列表。可点击 MySQL 名称进入详情页，切换到“网络”页面进行查看，如下图所示：



7.1.13.1 查看网络列表

平台支持用户查看 MySQL 的网络列表信息，包括 IP、IP ID、IP 版本、状态、网络类型、所属网络、是否 VIP、带宽、绑定资源、MAC 地址、操作，如下图所示：

7.1.13.2 绑定外网 IP

平台支持用户对 MySQL 进行绑定外网 IP 操作，可通过“绑定”按钮进行操作，也可通过 MySQL 列表中操作项的“绑定外网 IP”进行操作，如下图所示：

外网 IP 绑定成功后，在 MySQL 网络列表中新增一条 IP 数据。

注：每个 MySQL 支持最多绑定一个外网 IP。

7.1.13.3 解绑外网 IP

平台支持用户对已绑定外网 IP 的 MySQL 进行解绑外网 IP 操作，可通过“解绑”按钮进行操作，也可通过 MySQL 列表中操作项的“解绑外网 IP”进行操作，如下图所示：

7.1.13.4 修改安全组

平台支持用户对已绑定外网 IP 的 MySQL 进行修改安全组操作，可通过 MySQL 列表中操作项的“修改安全组”进行操作，如下图所示：

7.1.13.5 修改 IP

支持用户修改 MySQL 的内网 IP(VIP)地址。

7.1.14 备份管理

7.1.14.1 查看备份管理列表

平台支持用户查看备份管理列表信息，包括资源 ID、状态、所属存储池、来源备份计划、保留时间(天)、保存路径、创建时间、更新时间、到期时间、操作。可点击 MySQL 名称进入详情页，切换到“备份管理”页面进行查看，如下图所示：

7.1.14.2 删除备份

平台支持用户对备份数据进行删除操作，可点击备份列表中操作项的”删除“按钮进行操作，也可通过备份列表的“批量删除”按钮进行操作，如下图所示：

7.1.14.3 从备份创建

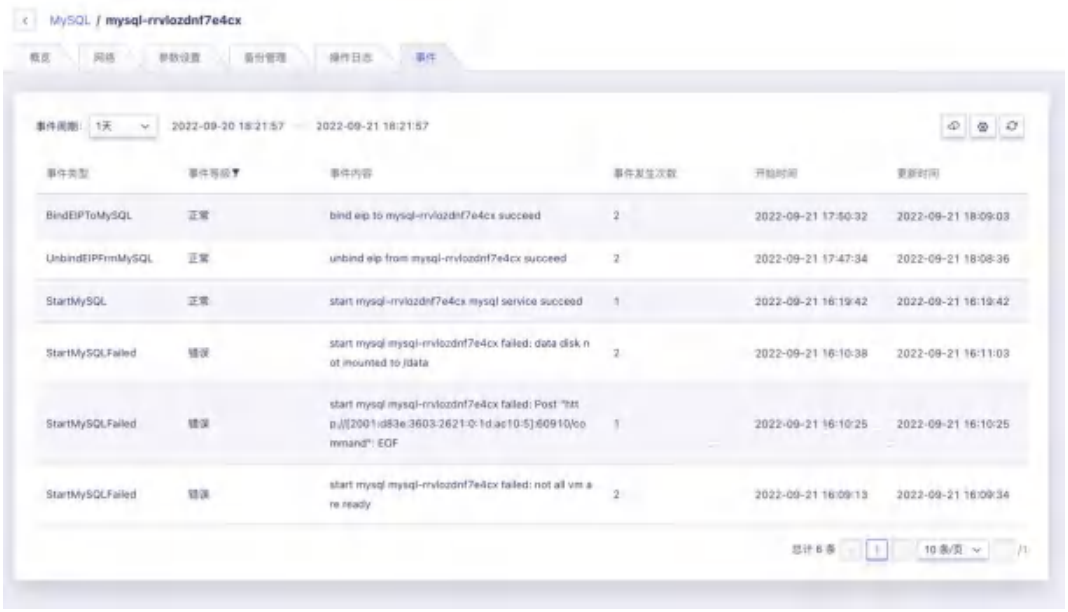
平台支持用户从备份创建 MySQL。

7.1.15 查看操作日志

平台支持用户查看 MySQL 的操作日志，并可根据操作结果和操作周期进行筛选，可点击 MySQL 名称进入详情页，切换到“操作日志”页面进行查看，如下图所示：

7.1.16 查看事件

平台支持用户查看 MySQL 的事件，并可根据事件周期进行筛选，可点击 MySQL 名称进入详情页，切换到“事件”页面进行查看，如下图所示：



7.1.17 删除 MySQL

平台支持用户对 MySQL 进行删除操作，删除主库前需先将从库删除。可点击 MySQL 列表中操作项的“删除”按钮进行操作，如下图所示：

7.1.18 创建参数模板

平台支持用户指定创建方式创建参数模板，包括复制现有模板和导入模板文件，如下图所示：

7.1.19 应用到实例

平台支持用户对参数模板进行应用到实例操作，可选择要应用到的 MySQL 资源，点击参数模板列中操作项的“应用到实例”按钮进行操作，如下图所示：

7.1.20 下载参数模板

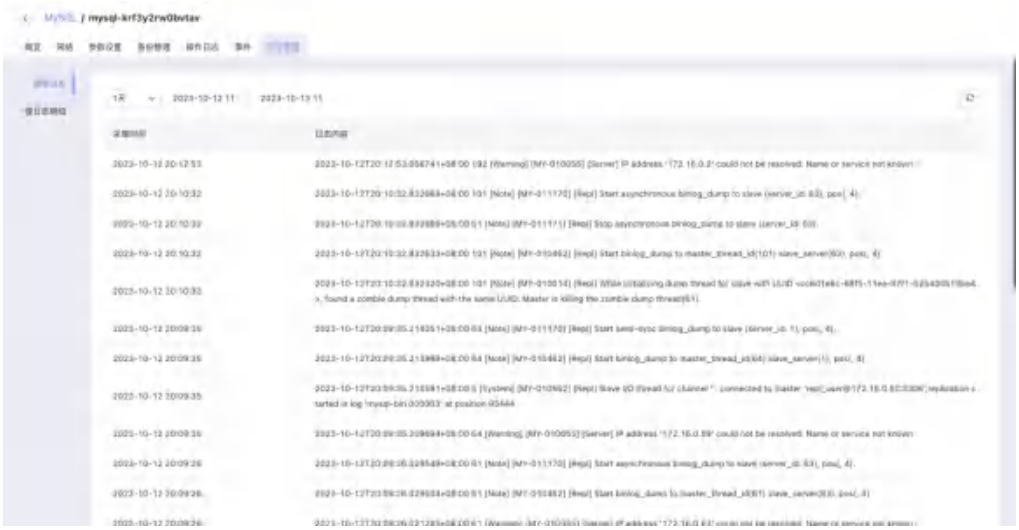
平台支持用户进行下载参数模板操作，可点击参数模板列中操作项的“应用到实例”按钮进行操作。

7.1.21 删除参数模板

平台支持用户对自定义参数模板进行删除操作，可点击参数模板列中操作项的“删除”按钮进行操作，如下图所示：

7.1.22 查看错误日志信息

支持用户查看 mysql 错误日志信息



7.1.23 查看慢日志信息

支持用户查看 mysql 慢日志信息

7.2 Redis 服务

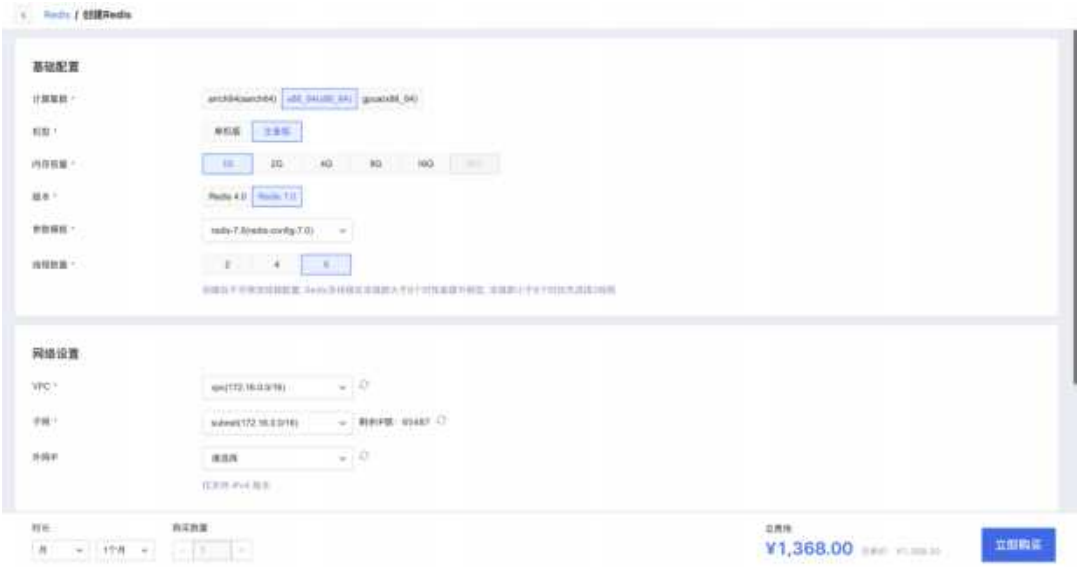
7.2.1 概览

Redis 是平台提供的一种数据库服务，支持单机版和主备版两种机型，并提

供了备份、监控等功能，满足高读写的性能场景。

7.2.2 创建 Redis

平台用户可以通过指定集群、内存容量、参数模板、VPC、子网、外网 IP、外网安全组、Redis 名称/备注、密码、项目组等相关基础信息创建 Redis，可通过导航栏进入[Redis]资源控制台，通过“创建”按钮进入向导页面，如下图所示：



（1）选择并配置 Redis 的基础配置、网络设置及管理配置信息：

- 集群：创建 Redis 的集群信息；
- 内存容量：选择创建 Redis 的内存容量，支持 1G、2G、4G、8G、16G、32G;
- 数据盘：创建 Redis 的数据信息，可选容量 10-33000GB；
- VPC 和子网：创建 Redis 时必须选择 VPC 网络和所属子网，即选择要加入的网络及 IP 网段；
- 外网 IP：外网 IP 为 Redis 提供外网访问服务，支持创建 Redis 时申请并绑定一个外网 IP 作为外网访问地址，Redis 支持最多绑定一个外网 IP；

（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 Redis 的

创建：

- 购买数量：默认支持创建 1 个 Redis；
- 付费方式：选择 Redis 的计费方式，支持按月、按年、按时三种方式，可根据需求选择合适的付费方式；
- 合计费用：用户选择 Redis 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 Redis 资源列表页，在列表页可查看 Redis 的创建过程。

7.2.3 查看 Redis 列表

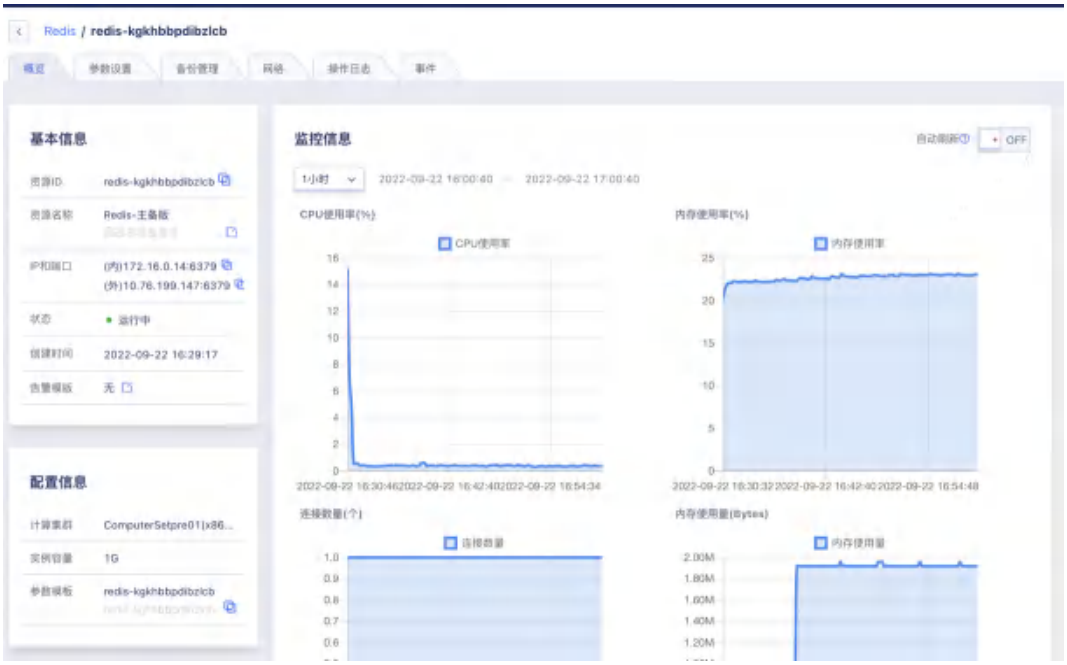
平台支持用户查看 Redis 列表信息，包括名称、资源 ID、状态、机型、IP 和端口、实例容量、VPC、子网、安全组、计费方式、项目组、创建时间、过期时间、操作。可通过导航栏进入[Redis]资源控制台查看，如下图所示：

- 名称：Redis 的名称，可点击进入 Redis 详情页；
- 资源 ID：Redis 的资源 ID，作为全局唯一标识；
- 状态：Redis 的状态，包括启动中、更改配置中、删除中等；
- 机型：Redis 的机型信息，支持单机版和主备版；
- 版本：Redis 的版本信息，支持 Redis4.0 和 Redis7.0；
- 线程数量：Redis7.0 版本，支持选择线程数量：2、4、6；
- IP 和端口：Redis 的网络信息，包括内/外网 IP 和端口；

- 实例容量：Redis 创建时选择的内存容量信息，可通过升级内存功能升级内存容量；
- VPC/子网：Redis 内网信息，包括 VPC/子网的名称和资源 ID；
- 安全组：Redis 绑定外网 IP 后支持关联安全组；
- 计费方式：Redis 资源的计费方式，支持小时、月、年；
- 项目组：Redis 资源所属的安全组，可通过安全组的转入/转出功能修改关联关系；
- 创建时间/过期时间：Redis 的创建时间和过期时间；
- 操作：Redis 资源的可操作项内容，包括创建从库、删除、续费、重置密码、应用参数模板、升级内存、清除数据、升级至主备版、修改告警模板、绑定外网 IP、解绑外网 IP、修改安全组等。

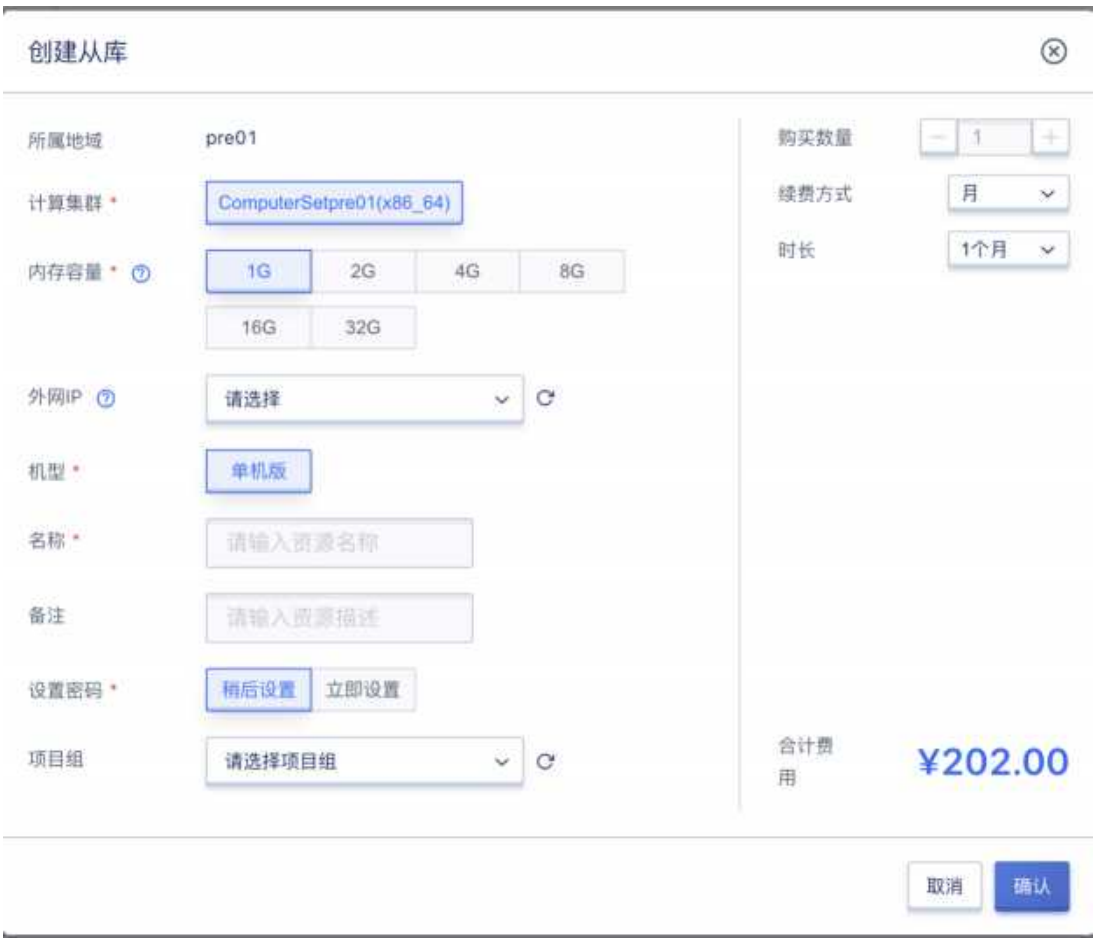
7.2.4 查看 Redis 概览信息

平台支持用户查看 Redis 资源概览信息，包括基本信息、配置信息、监控信息。可通过点击 Redis 列表中的名称进入概览页面，如下图所示：



7.2.5 Redis 创建从库

平台支持用户对 Redis 主库进行创建从库的操作，可选择内存容量、外网IP、安全组，内存容量不可低于主库。可通过 Redis 列表中操作项的“创建从库”按钮进行操作，如下图所示：



每个 Redis 主库支持最多创建 5 个从库。

7.2.6 Redis 续费

平台支持用户对 Redis 进行续费操作，可通过 Redis 列表中操作项的“续费”按钮进行操作，如下图所示：

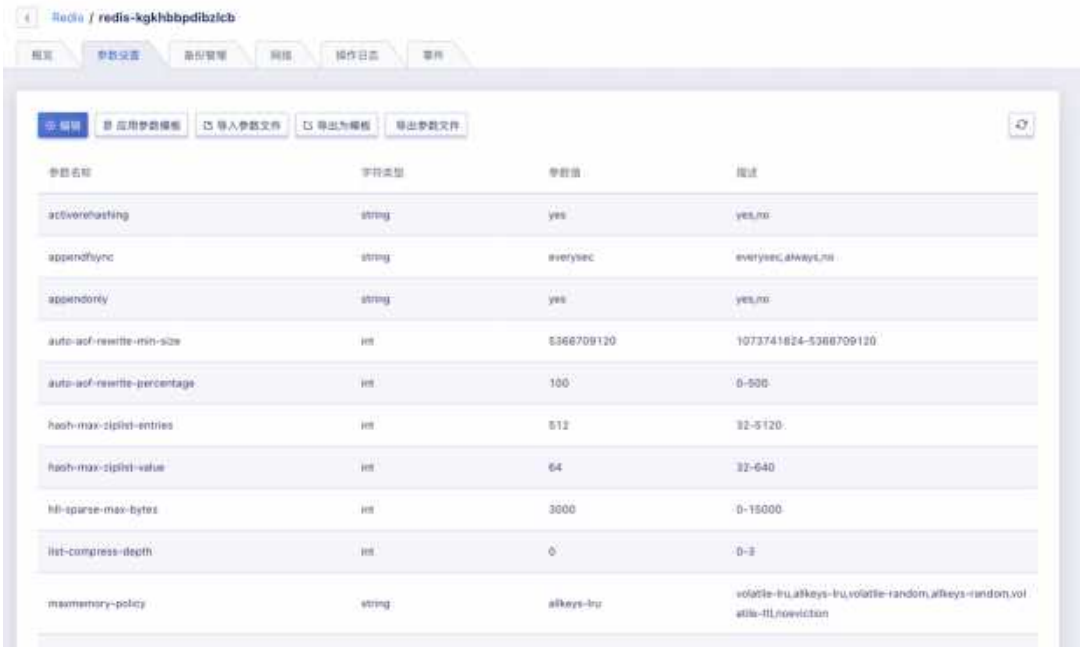
续费支持更改续费方式和续费时长，更改续费方式只支持由短周期改为长周期，比如从“小时”更改为“月”。

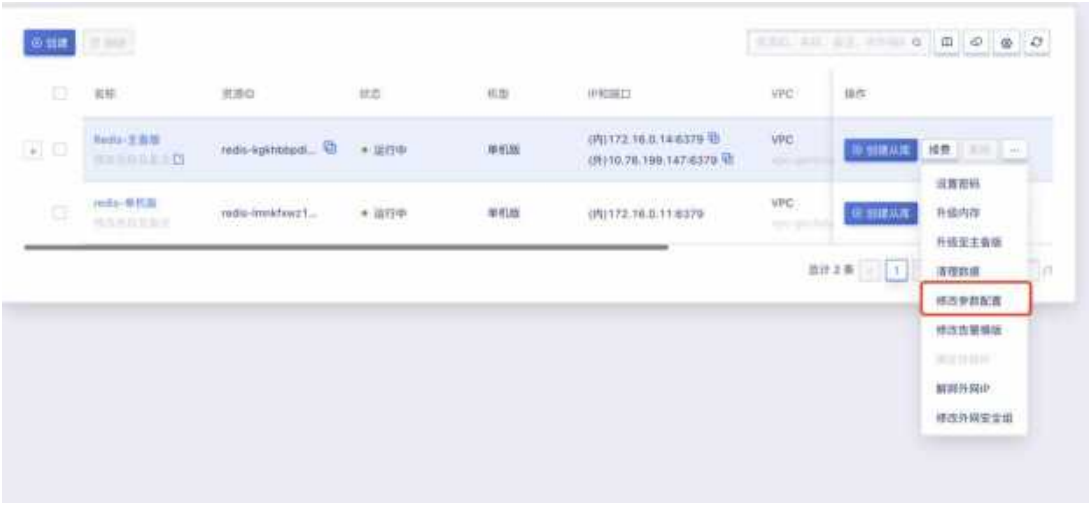
7.2.7 重置密码

平台支持用户对 Redis 进行设置密码操作，可通过 Redis 列表中操作项的“设置密码”按钮进行操作，如下图所示：

7.2.8 参数配置

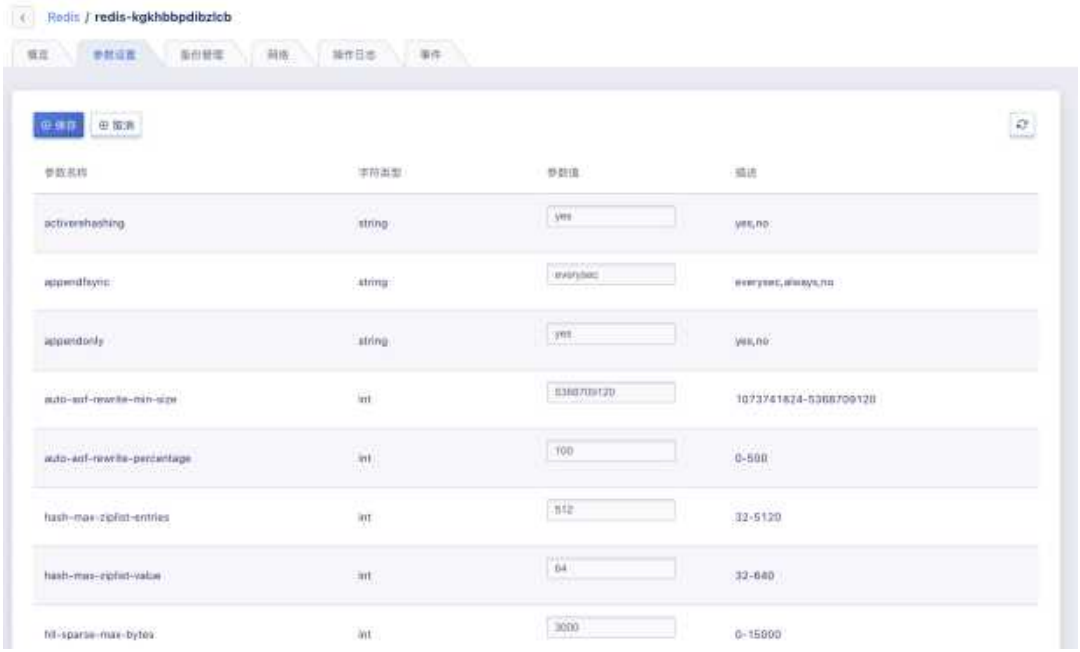
平台支持用户对 Redis 进行参数配置相关操作，包括修改实例参数、应用参数模板、导入参数文件、导出为模板、导出参数文件。可点击 Redis 名称进入详情页，切换到“参数设置”页面查看；也可通过 Redis 列表操作项的“修改实例参数”按钮点击跳转，如下图所示：





7.2.8.1 修改实例参数

平台支持用户对 Redis 进行修改实例参数操作，可点击“修改实例参数”按钮进行操作，如下图所示：



7.2.8.2 应用参数模板

平台支持用户对 Redis 进行应用参数模板操作，可点击“应用参数模板”进行操作，如下图所示：

7.2.8.3 导入参数文件

平台支持用户对 Redis 进行导入参数文件操作，可点击“导入参数文件”进行操作，如下图所示：

7.2.8.4 导出为模板

平台支持用户对 Redis 参数配置进行导出为模板操作，可点击“导出为模板”进行操作，如下图所示：

导出为模板操作成功后，参数模板列表新增一条模板数据。

7.2.8.5 导出参数文件

平台支持用户对 Redis 参数配置进行导出参数文件操作，可点击“导出参数文件”进行操作，下载参数配置文件。

7.2.9 升级内存

平台支持用户对 Redis 进行升级内存操作，可点击 Redis 列表中操作项的“升级内存”按钮进行操作，如下图所示：

7.2.10 升级主备版

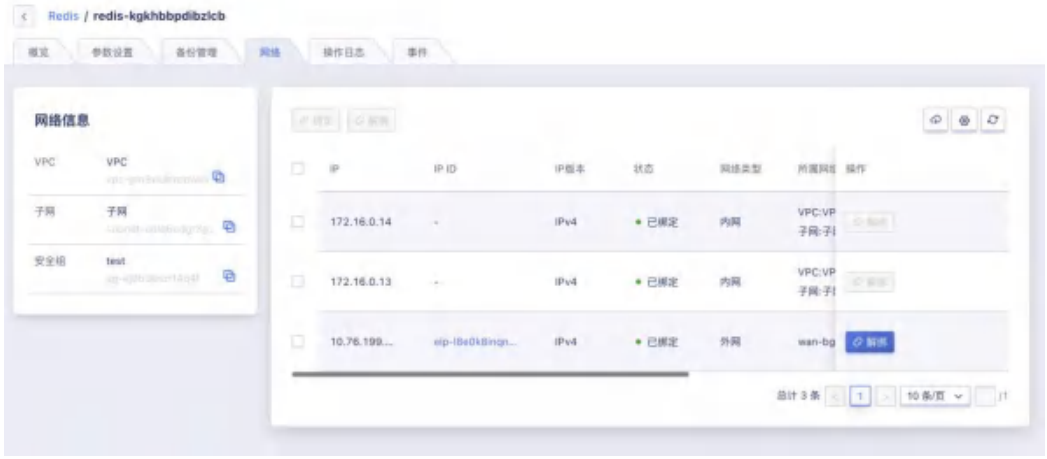
平台支持用户对单机版 Redis 进行升级至主备版操作，计算集群、内存容量、存储集群、数据盘容量不可修改。可点击 Redis 列表中操作项的“升级至主备版”按钮进行操作，如下图所示：

7.2.11 修改告警模板

平台支持用户对 Redis 进行修改告警模板操作。可点击 Redis 列表中操作项的“修改告警模板”按钮进行操作，如下图所示：

7.2.12 网络

平台支持用户查看 Redis 的网络信息，包括基本信息和 IP 列表。可点击 Redis 名称进入详情页，切换到“网络”页面进行查看，如下图所示：



7.2.12.1 查看网络列表

平台支持用户查看 Redis 的网络列表信息，包括 IP、IP ID、IP 版本、状态、网络类型、所属网络、是否 VIP、带宽、绑定资源、MAC 地址、操作，如下图所示：

7.2.12.2 绑定外网 IP

平台支持用户对 Redis 进行绑定外网 IP 操作，可通过“绑定”按钮进行操作，也可通过 Redis 列表中操作项的“绑定外网 IP”进行操作，如下图所示：

外网 IP 绑定成功后，在 Redis 网络列表中新增一条 IP 数据。

每个 Redis 支持最多绑定一个外网 IP。

7.2.12.3 解绑外网 IP

平台支持用户对已绑定外网 IP 的 Redis 进行解绑外网 IP 操作，可通过“解绑”按钮进行操作，也可通过 Redis 列表中操作项的“解绑外网 IP”进行操作，如下图所示：

7.2.12.4 修改安全组

平台支持用户对已绑定外网 IP 的 Redis 进行修改安全组操作，可通过 Redis 列表中操作项的“修改安全组”进行操作，如下图所示：

7.2.12.5 修改 IP

平台支持用户修改 Redis 的内网 IP(VIP)地址。

7.2.13 清理数据

平台支持用户对 Redis 进行清理数据操作，可通过 Redis 列表中操作项的“清理数据”进行操作，如下图所示：

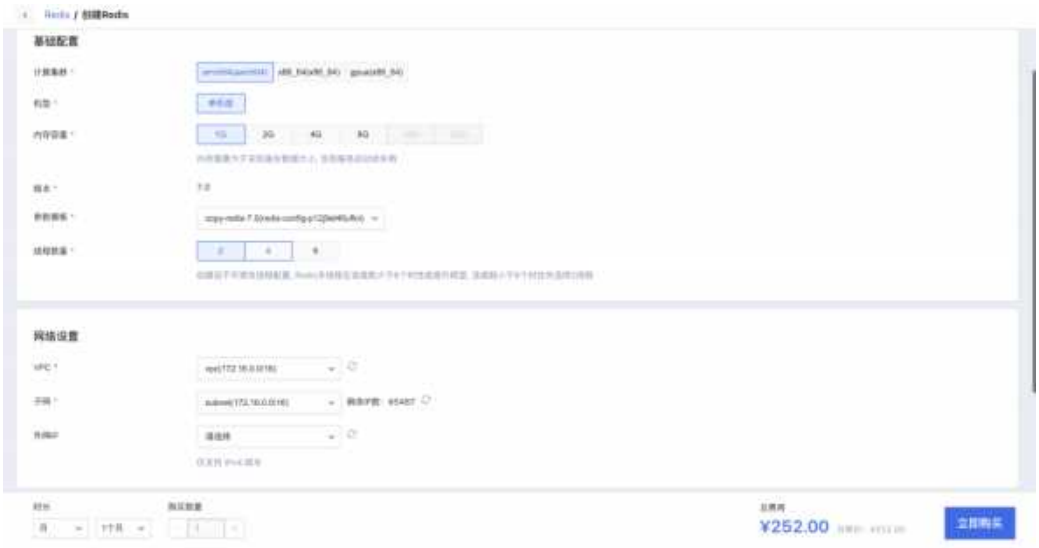
7.2.14 备份管理

7.2.14.1 查看备份管理列表

平台支持用户查看备份管理列表信息，包括资源 ID、状态、所属存储池、来源备份计划、保留时间(天)、保存路径、创建时间、更新时间、到期时间、操作。可点击 Redis 名称进入详情页，切换到“备份管理”页面进行查看，如下图所示：

7.2.14.2 从备份创建

平台支持用户从备份创建 Redis。

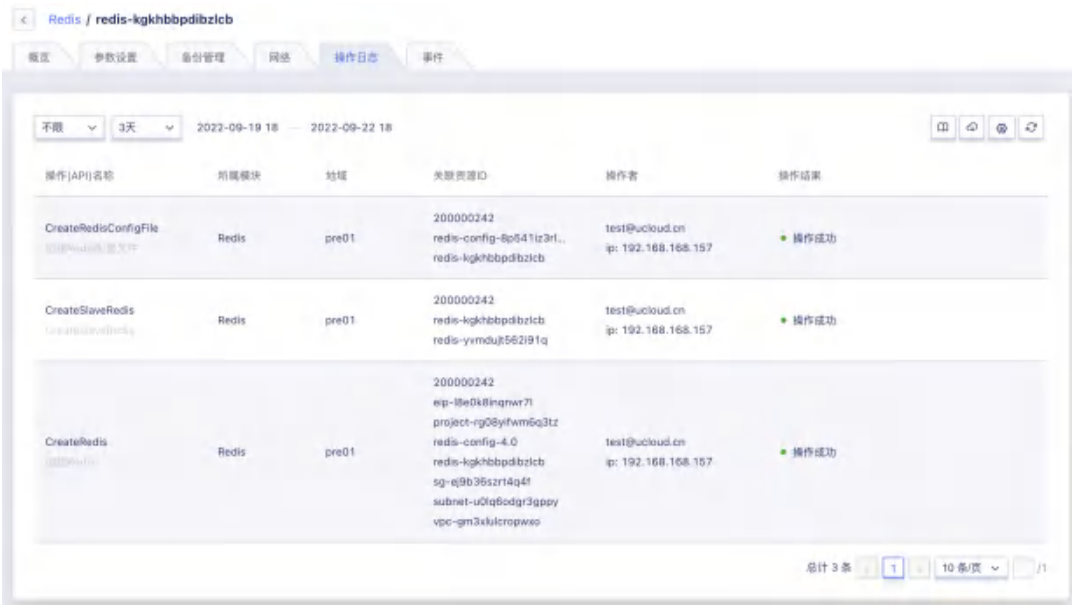


7.2.14.3 删除备份

平台支持用户对备份数据进行删除操作，可点击备份列表中操作项的”删除“按钮进行操作，也可通过备份列表的“批量删除”按钮进行操作，如下图所示：

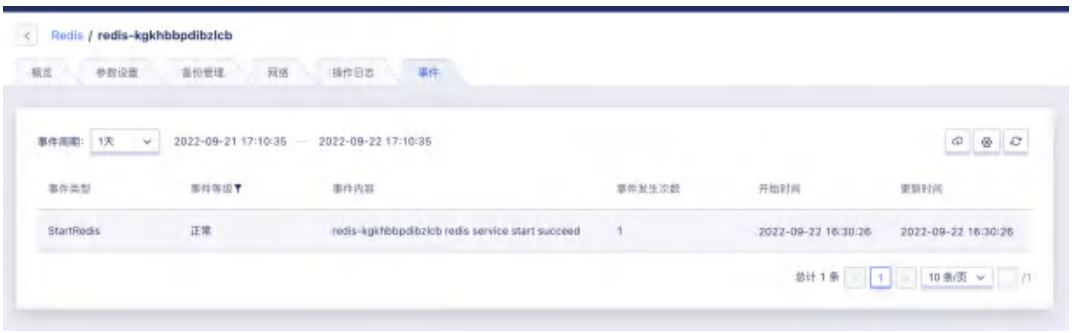
7.2.15 查看操作日志

平台支持用户查看 Redis 的操作日志，并可根据操作结果和操作周期进行筛选，可点击 Redis 名称进入详情页，切换到“操作日志”页面进行查看，如下图所示：



7.2.16 查看事件

平台支持用户查看 Redis 的事件，并可根据事件周期进行筛选，可点击 Redis 名称进入详情页，切换到“事件”页面进行查看，如下图所示：



7.2.17 删除 Redis

平台支持用户对 Redis 进行删除操作，删除主库前需先将从库删除。可点击 Redis 列表中操作项的“删除”按钮进行操作，如下图所示：

7.2.18 创建参数模板

平台支持用户指定创建方式创建参数模板，包括复制现有模板和导入模板文件，如下图所示：

7.2.19 删除参数模板

平台支持用户对自定义参数模板进行删除操作，可点击参数模板列中操作项的“删除”按钮进行操作，如下图所示：

7.2.20 查看慢日志信息

支持用户查看 redis 慢日志信息

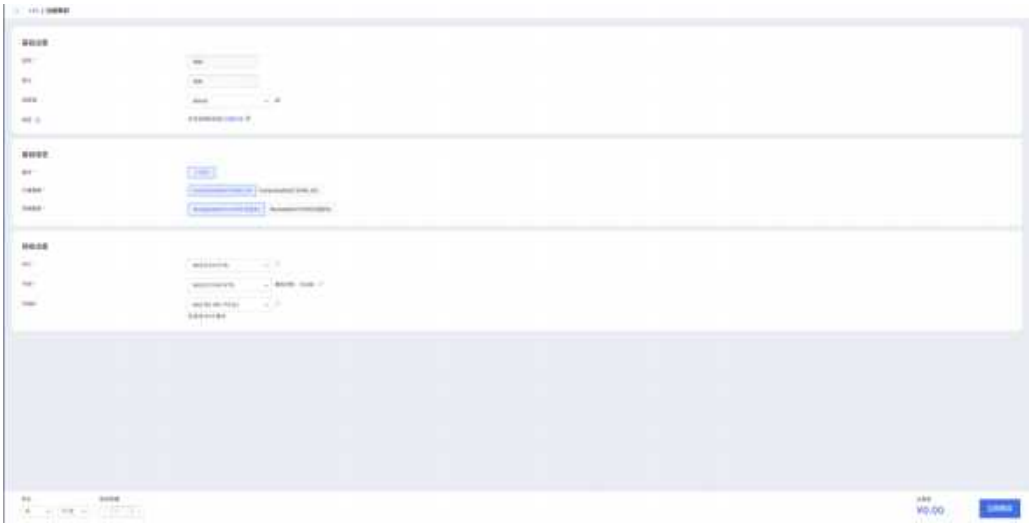
8 容器集群

8.1 容器集群概述

容器集群是一个自主构建的云原生容器平台，用于部署、管理和扩展容器化应用程序。它提供了高度可靠、弹性和可扩展的基础架构，以支持在分布式环境中运行容器化工作负载。该容器集群由多个逻辑节点组成，通过 VPC 网络相互连接，形成一个集群。集群通过 API Server 对外提供服务，并支持多架构计算集群的混合使用。同时，它支持使用平台内的分布式存储系统，用于持久化数据和应用程序状态的存储。容器集群提供了网络和服务发现机制，使容器能够相互通信和发现服务。通过平台的负载均衡实现服务路由，结合 Service 和 Ingress 功能，为容器应用程序提供灵活的网络配置。为了实时监控集群和应用程序的运行状态，容器集群提供了监控和事件上报机制。它能够收集和分析日志数据，帮助进行故障排除和性能优化。通过这个容器集群，用户可以更灵活、高效地部署和管理容器化应用程序，提高应用程序的可靠性、可伸缩性和可维护性，从而加速应用程序的交付和创新。

8.2 创建容器集群

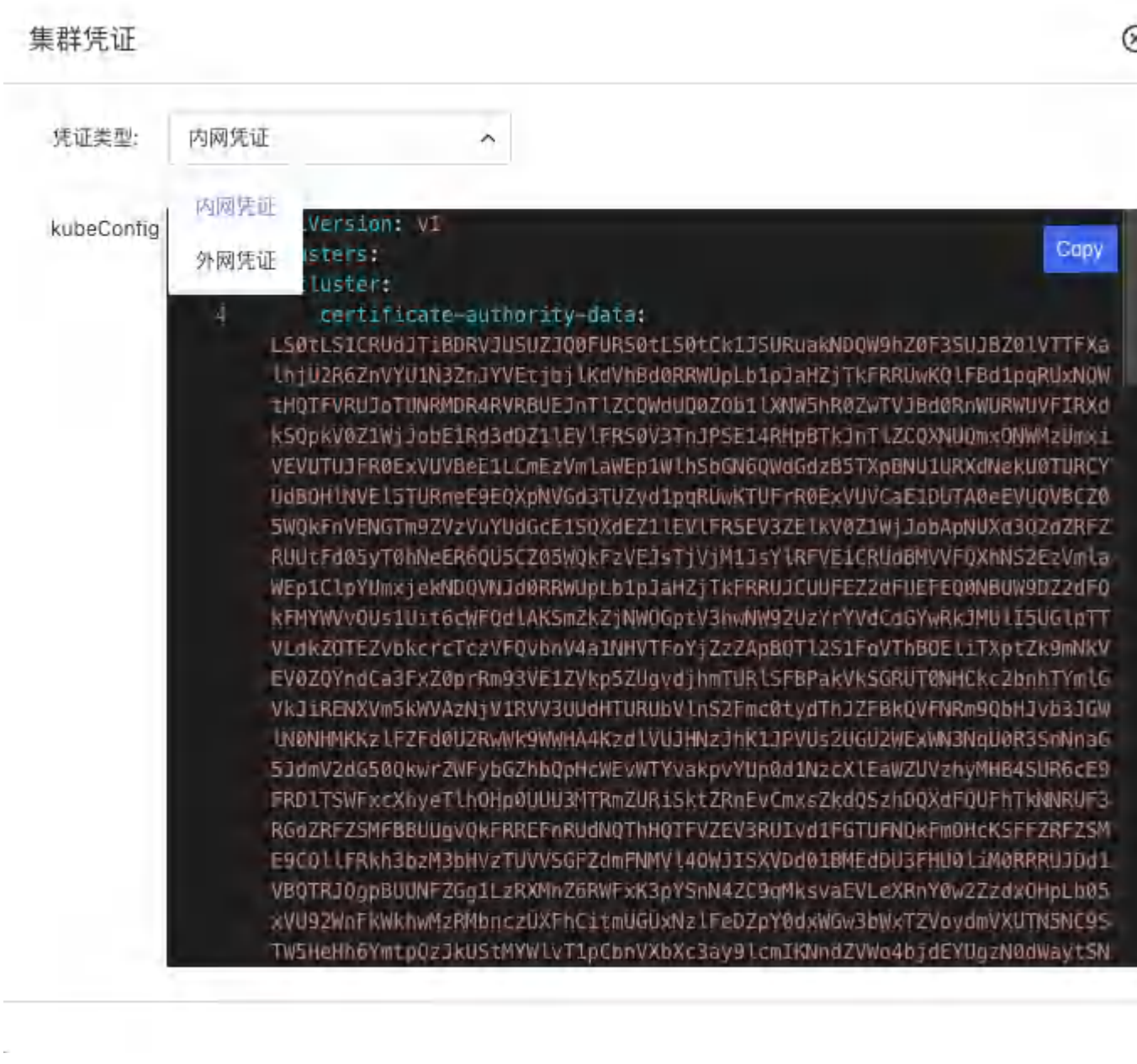
用户可以通过控制台创建一个容器集群，创建时需要指定容器集群名称，版本，计算集群，存储集群，VPC，子网，外网 IP。当前平台版本只支持 1.25.0 版本，容器集群的管理服务会在对应计算集群，存储集群中创建，选择 VPC 子网后，容器网络和同 VPC 的其它资源互通，新创集群的对应子网 IP 余量必须要大于等于 10 个。如需外部访问平台容器集群，需要在创建时配置外网 IP，外网 IP 在容器集群创建后，不支持更改，当前版本外网 IP 只支持 IPv4。支持用户按时，月，年购买容器集群。集群默认最大 CPU 数量为 100 核，最大内存数量为 204800MB，最大 Pods 数量为 100。



创建完成后，在容器集群列表展示容器集群信息。包括：名称，集群 ID，状态，版本，集群类型，apiServer 列表，所属 VPC，所属子网，操作（包括：查看集群凭证，更新，修改告警模版，删除）。容器集群创建通常需要十分钟左右，创建完成后集群状态会从创建中变为运行中，如果管理服务出现异常，集群状态会变为异常。容器集群列表支持租户按照名称，备注，资源 ID，apiServer 地址，版本搜索。

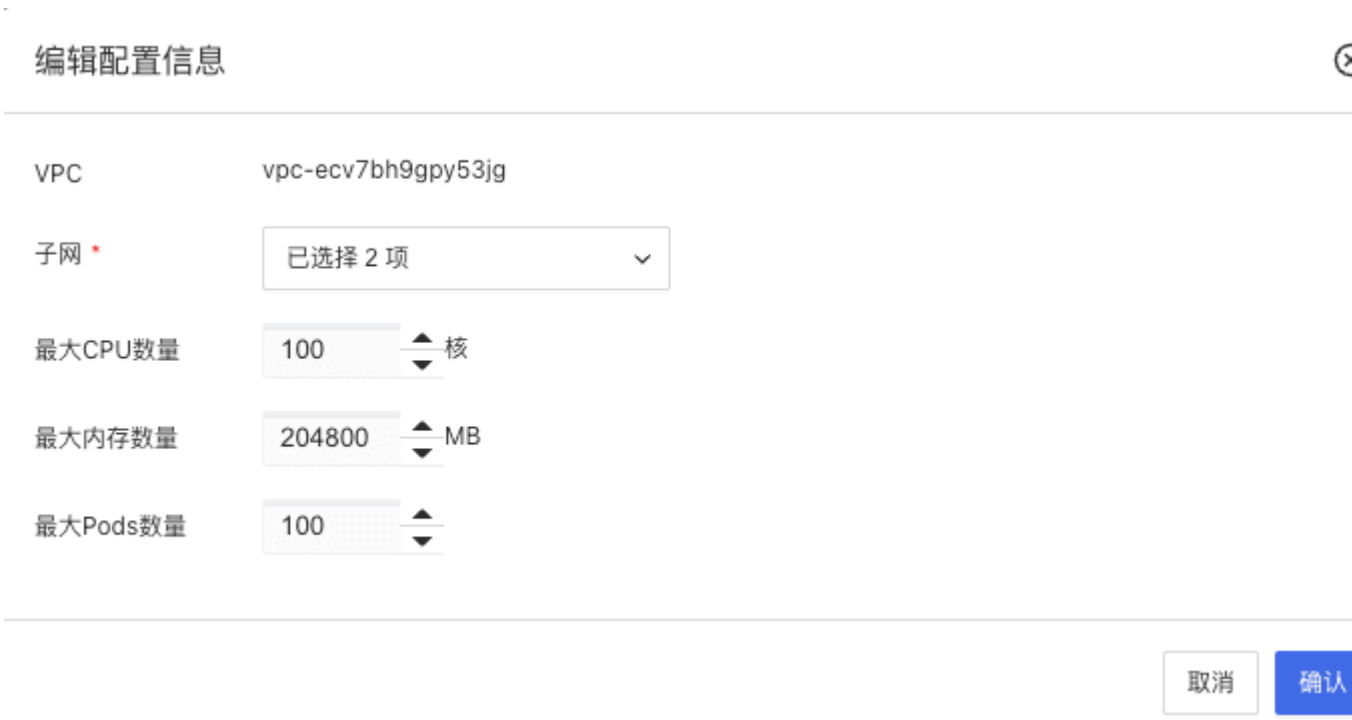
8.3 查看容器集群凭证

用户通过查看集群凭证，获取容器集群的配置文件，默认展示内网集群凭证，创建时绑定外网 IP，则展示内外网集群凭证。将集群配置文件添加到.kube/config，即可通过 kubectl 访问容器集群。



8.4 编辑配置信息（管理员功能）

支持管理员编辑租户的容器集群配置，支持设置子网，最大 CPU 数量，最大内存数量，最大 Pods 数量，子网 IP 已被容器集群使用的情况下，不能将子网从容器集群中移除。



8.5 更新容器集群

支持租户更新容器集群子网信息，子网 IP 已被容器集群使用的情况下，不能将子网从容器集群中移除。

8.6 修改告警模版

支持租户修改容器集群告警模版，支持租户通过集群内存利用率，集群内存容量 ，集群 CPU 利用率，集群 CPU 数量等监控指标，设置告警规则。触发告警后通过通知组将告警发送到对应通知人。

8.7 查看容器集群概览

查看容器集群概览，展示容器集群的基本信息，配置信息，监控信息。基本信息包括：集群 ID，集群名称，状态，版本，apiServer 列表，集群凭证，镜像仓库（当前地域的 Registry 镜像仓库地址，格式：ip:port/comanyID），创建时间，告警模版。配置信息包括：所属 VPC，所属子网，最大 CPU 数量，最大内存数量，最大 pods 数量。监控信息包括：集群 CPU 数量，集群 CPU 利用率，

集群内存容量，内存利用率,支持按时间查询，支持自动刷新。

8.8 容器集群镜像上传

支持用户通过平台外网从本地上传镜像到镜像仓库。上传方式如下：

1.登录镜像仓库输入平台租户的账号密码

```
docker login 192.168.179.20:6451/200000233
```

2.拉取公共源镜像

```
docker pull docker.io/library/nginx:latest
```

3.镜像打 tag

```
docker tag docker.io/library/nginx:latest
192.168.179/20:6451/200000233/nginx:latest
```

4.推送镜像到镜像仓库

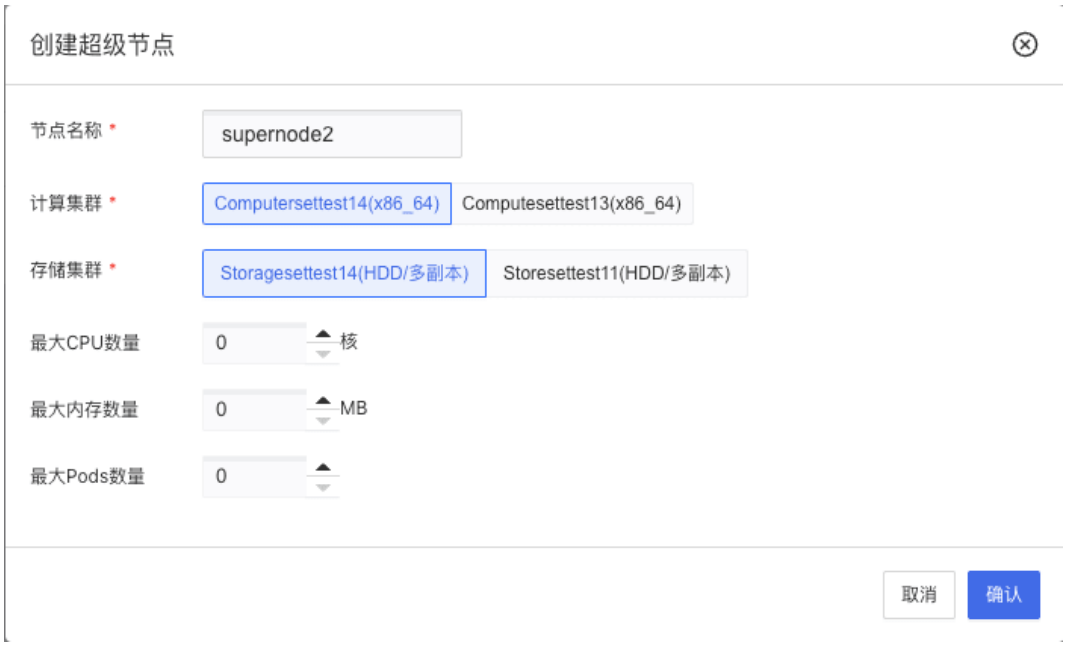
```
docker push 192.168.179/20:6451/200000233/nginx:latest
```

8.9 超级节点管理

超级节点为用于运行应用程序和容器化工作负载的工作节点，是逻辑上的节点。支持租户创建超级节点，更新超级节点，锁定节点，解锁节点，删除节点。集群创建完成后会默认创建一个节点名称为 supernode01 的节点，该节点默认最大 CPU 数量为 50 核，最大内存数量为 102400MB，最大 Pods 数量为 50 个，状态默认为锁定状态，不可删除。

8.9.1.1 创建超级节点

支持租户创建超级节点，创建超级节点时，可以选择当前地域下的任意计算集群，存储集群。支持用户设置节点最大 CPU 数量，最大内存数量，最大 Pods 数量，未设置时默认设置当前集群一半的可用余量。超级节点无个数限制，节点资源用量和不得超过容器集群资源用量。

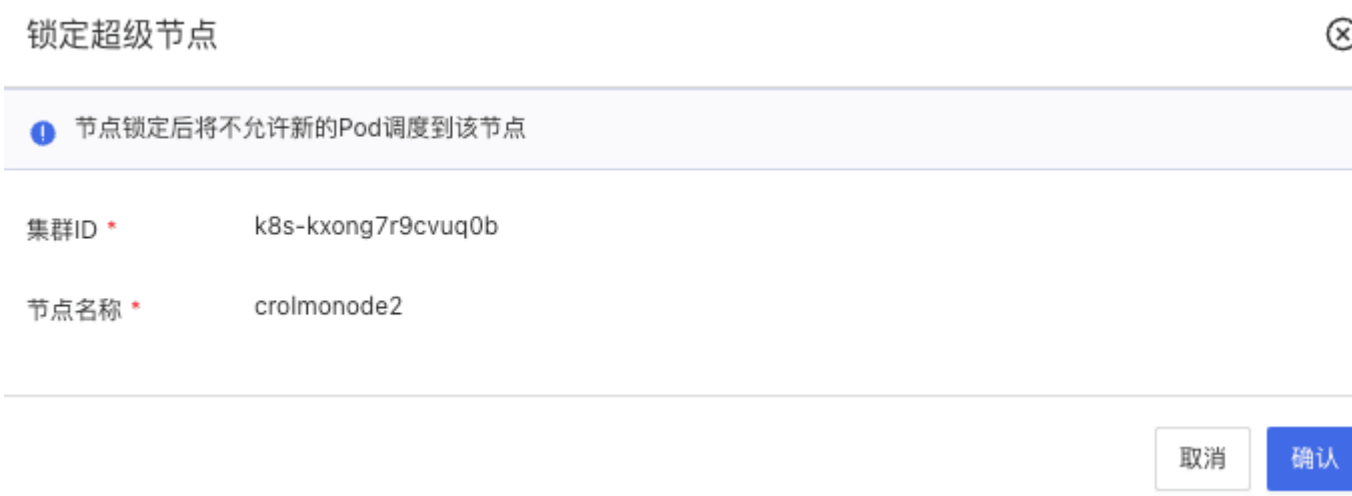


8.9.1.2 更新超级节点

支持租户更新超级节点，修改节点最大 CPU 数量，最大内存数量，最大 Pods 数量。

8.9.1.3 锁定超级节点

支持租户锁定超级节点，锁定节点后，pod 不再调度到该节点，已经调度到该节点的 pods 仍会继续运行，直到删除。



8.9.1.4 解锁超级节点

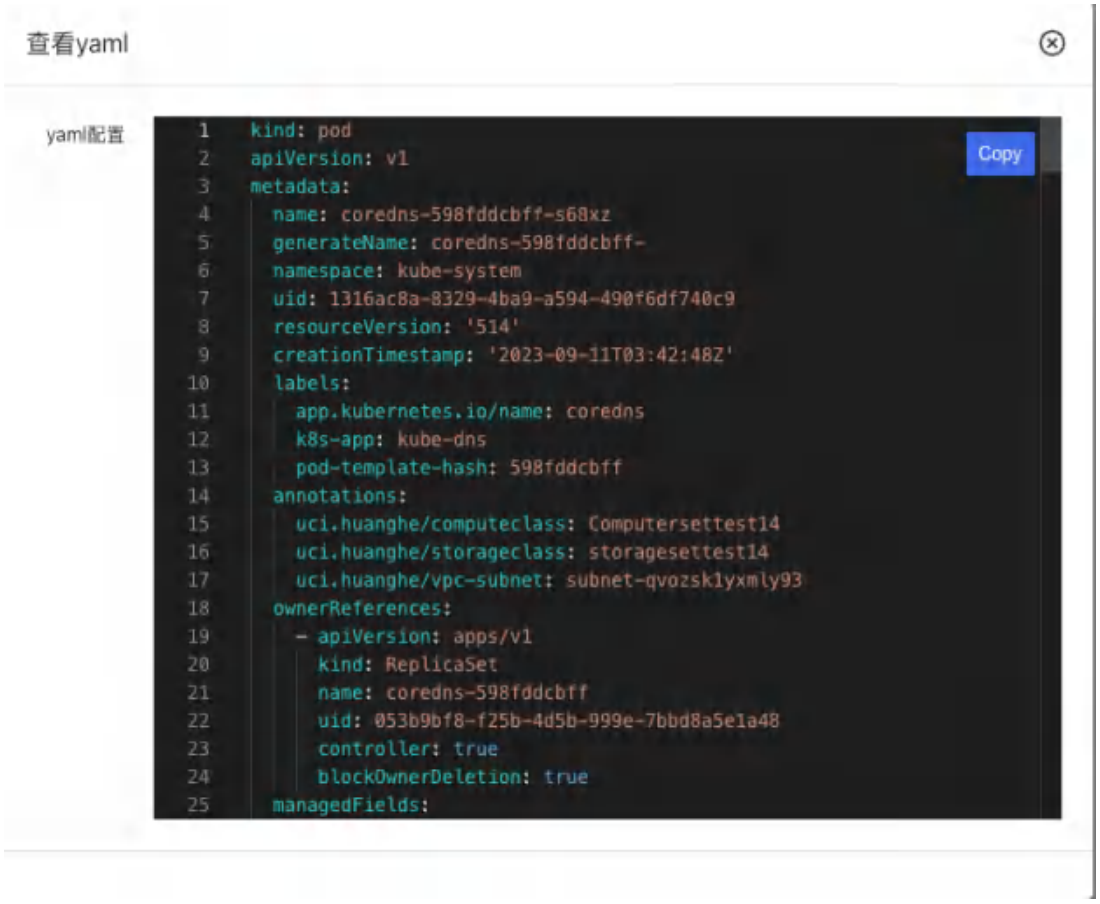
支持用户解锁超级节点，解锁节点后，pod 会调度到该节点上。

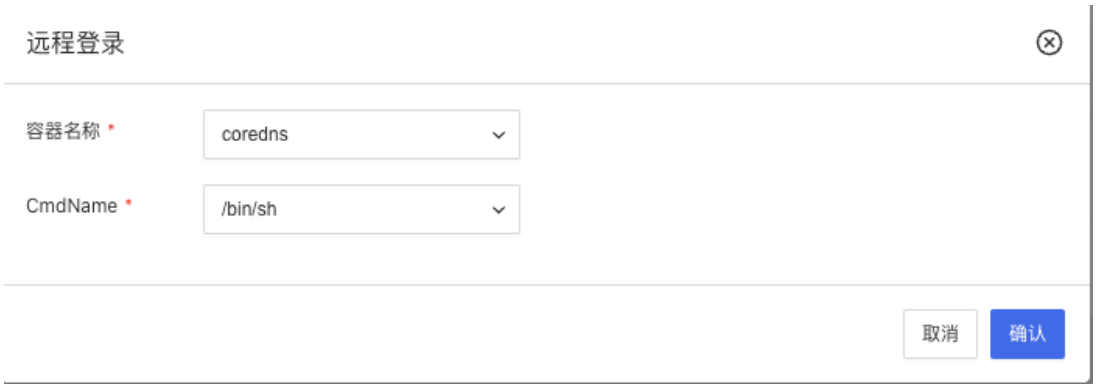
8.9.1.5 删除超级节点

支持用户删除超级节点，节点删除前需要将节点上的 pod 全部删除。

8.9.1.6 Pod 管理

支持用户管理节点下的 Pod，批量销毁 Pod，按照命名空间筛选 Pod，查看 Pod 的 yaml 配置，远程登录 pod。远程登录时需选择容器名称，命令行模式。Pod 管理列表展示 Pod 实例名称，命名空间，状态，实例 IP，Request/Limits 资源用量配置，创建时间，操作（销毁，查看 yaml，远程登录）。未通过工作负载调度创建的 pod 销毁后不会重建。





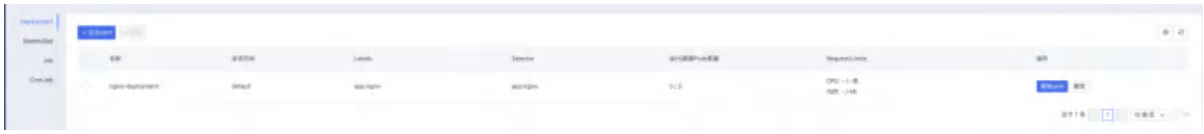
8.10 工作负载

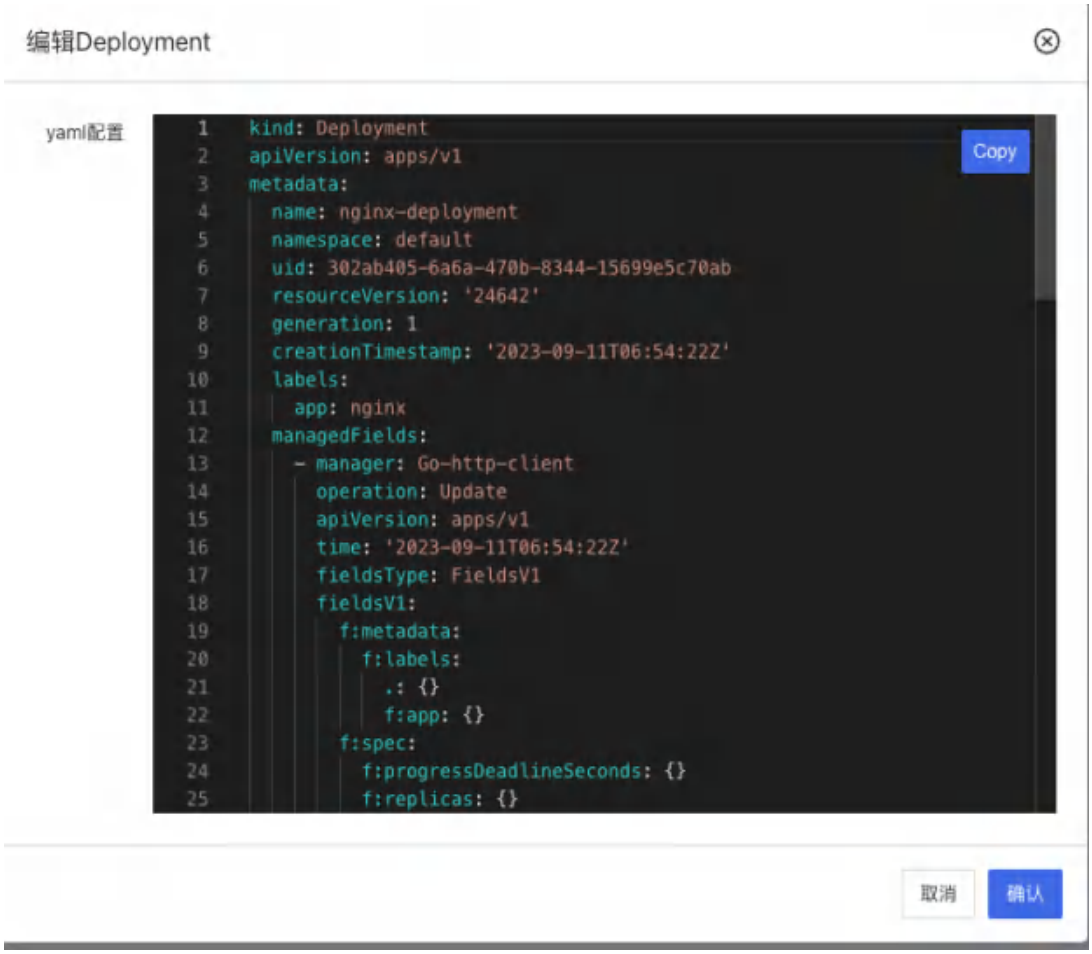
支持用户在控制台通过 yaml 配置创建，更新工作负载。创建工作负载时，需要先选择命名空间，然后选择工作负载类型，点击添加 yaml，添加工作负载配置，创建工作负载。默认会显示工作负载的配置模版。工作负载包括：Deployment，StatefulSet，Job，CronJob。

8.10.1 Deployment

Deployment 是 Kubernetes 中的一种资源对象，用于声明式地管理应用程序的部署和扩展。它提供了一种便捷的方式来定义和控制应用程序在 Kubernetes 集群中的副本数量、容器镜像、存储卷、网络配置等方面的规范。

工作负载 Deployment 列表展示 Deployment 的名称，命名空间，Labels，Selector，运行/期望 Pods 数量，Request/Limit，操作（编辑 yaml，删除）





Deployment 模版

```
apiVersion: apps/v1
kind: Deployment
metadata:
name: nginx-deployment
labels:
    app: nginx
spec:
replicas: 3
selector:
    matchLabels:
    app: nginx
template:
    metadata:
    labels:
        app: nginx
```

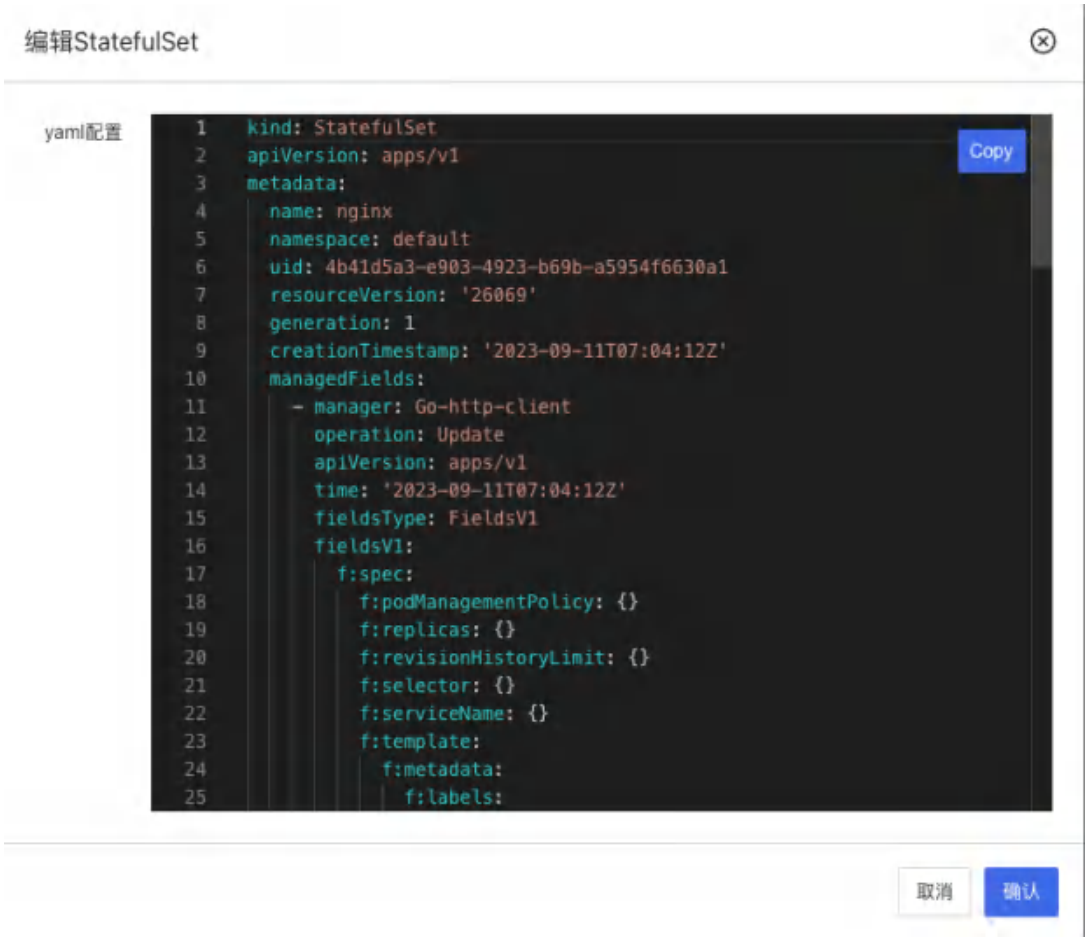


```
spec:
containers:
- name: nginx
    image: 172.31.255.3:5000/nginx:latest
    ports:
    - containerPort: 80
```

8.10.2 StatefulSet

StatefulSet 是 Kubernetes 中用于管理有状态应用程序的资源对象。它为每个 Pod 实例分配唯一标识符，并保持标识符的稳定性。StatefulSet 还支持有状态的持久性存储，使每个 Pod 实例能够访问自己的持久化数据。部署和扩展操作按照定义的顺序进行，确保应用程序的有状态性和稳定性。

工作负载 StatefulSet 列表展示 StatefulSet 的名称，命名空间，Labels，Selector，运行/期望 Pods 数量，Request/Limit，操作（编辑 yaml，删除）



StatefulSet 模版

```
apiVersion: apps/v1
kind: StatefulSet
metadata:
```

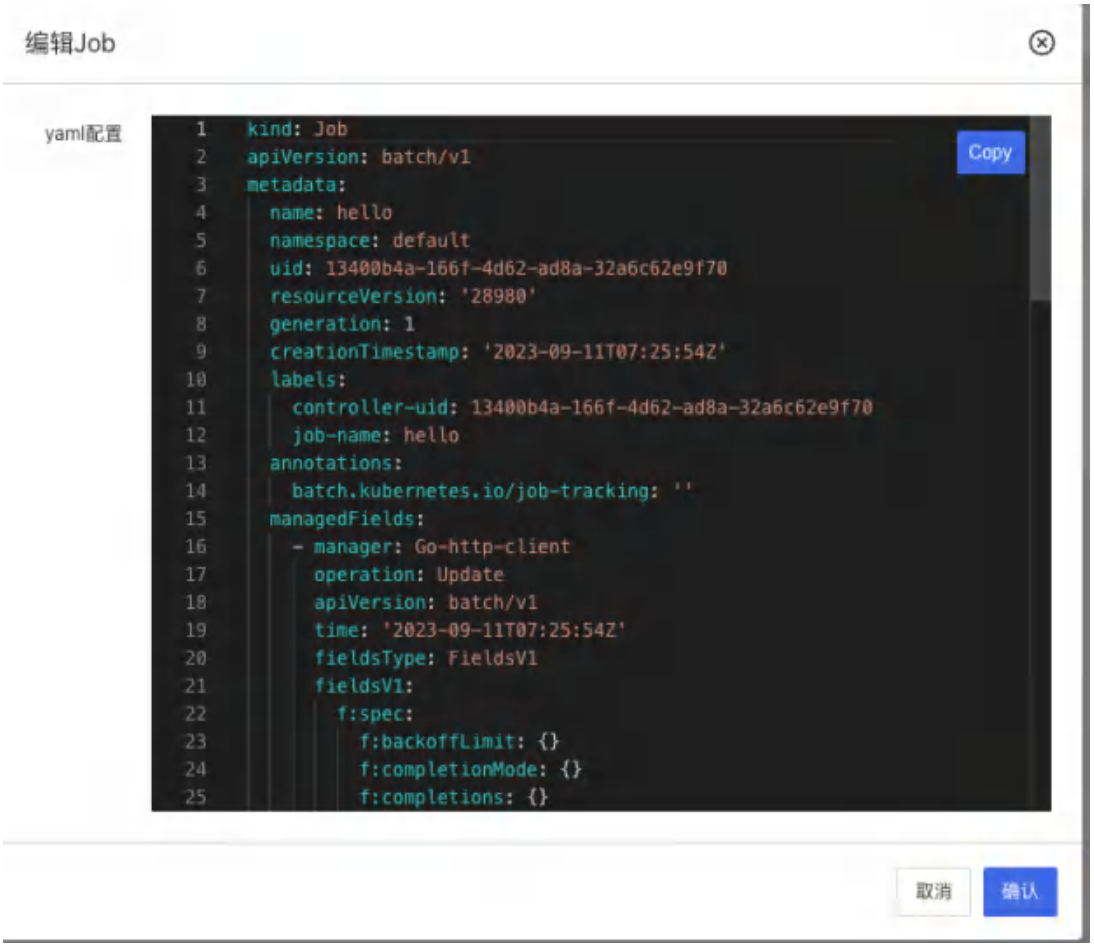


```
    name: nginx
spec:
    serviceName: "nginx"
    replicas: 3
    selector:
        matchLabels:
            app: nginx
    template:
        metadata:
            labels:
                app: nginx
        spec:
            containers:
            - name: nginx
                image: 172.31.255.3:5000/nginx:latest
                ports:
                - containerPort: 80
                    name: web
```

8.10.3 Job

Job 是 Kubernetes 中用于执行一次性任务或批处理作业的资源对象。它并行地创建和管理多个 Pod 实例来运行任务，并确保任务成功完成。Job 适用于需要执行短暂任务的场景，可以自动重试失败的任务，并提供任务顺序性的控制机制。

工作负载 Job 列表展示 Job 的名称，命名空间，Labels，Selector，并行数，重复次数，Request/Limit，操作（编辑 yaml，删除）



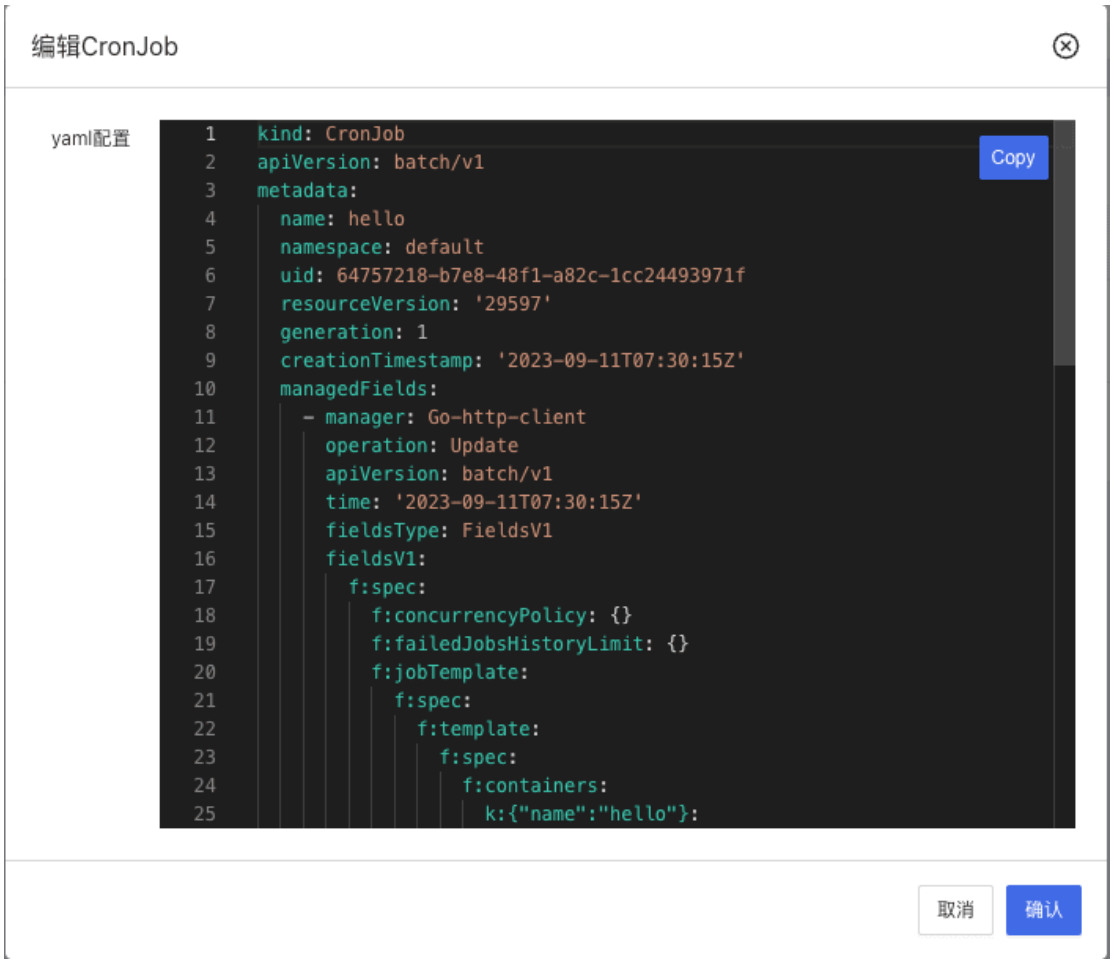
Job 模版

```
apiVersion: batch/v1
kind: Job
metadata:
  name: hello
spec:
  template:
    spec:
      containers:
      - name: hello
        image: 172.31.255.3:5000/busybox:latest
        command: ["echo", "Hello World"]
      restartPolicy: Never
```

8.10.4 CronJob

CronJob 是 Kubernetes 中的一种资源对象，用于在指定的时间间隔或特定时间点运行周期性任务。它类似于传统的 Cron 调度器，允许用户在集群中定义和自动执行定时任务。

工作负载 CronJob 列表展示 CronJob 的名称，命名空间，Labels，Selector，并行数，重复次数，活跃 JOB 数，Request/Limit，操作（编辑 yaml，删除）



CronJob 模版

```
apiVersion: batch/v1

kind: CronJob

metadata:
```



```
    name: hello
spec:
    schedule: "*/1 * * * *"
    jobTemplate:
      spec:
        template:
          spec:
            containers:
            - name: hello
              image: 172.31.255.3:5000/busybox:latest
              command: ["echo", "Hello World"]
            restartPolicy: OnFailure
```

8.11 服务路由

支持用户在控制台通过 yaml 配置创建，更新服务路由。服务路由依赖平台负载均衡，创建服务路由前要在同 VPC 下创建负载均衡。服务路由包括 Service 和 Ingress，Service 和 Ingress 不能共用同一个负载均衡。

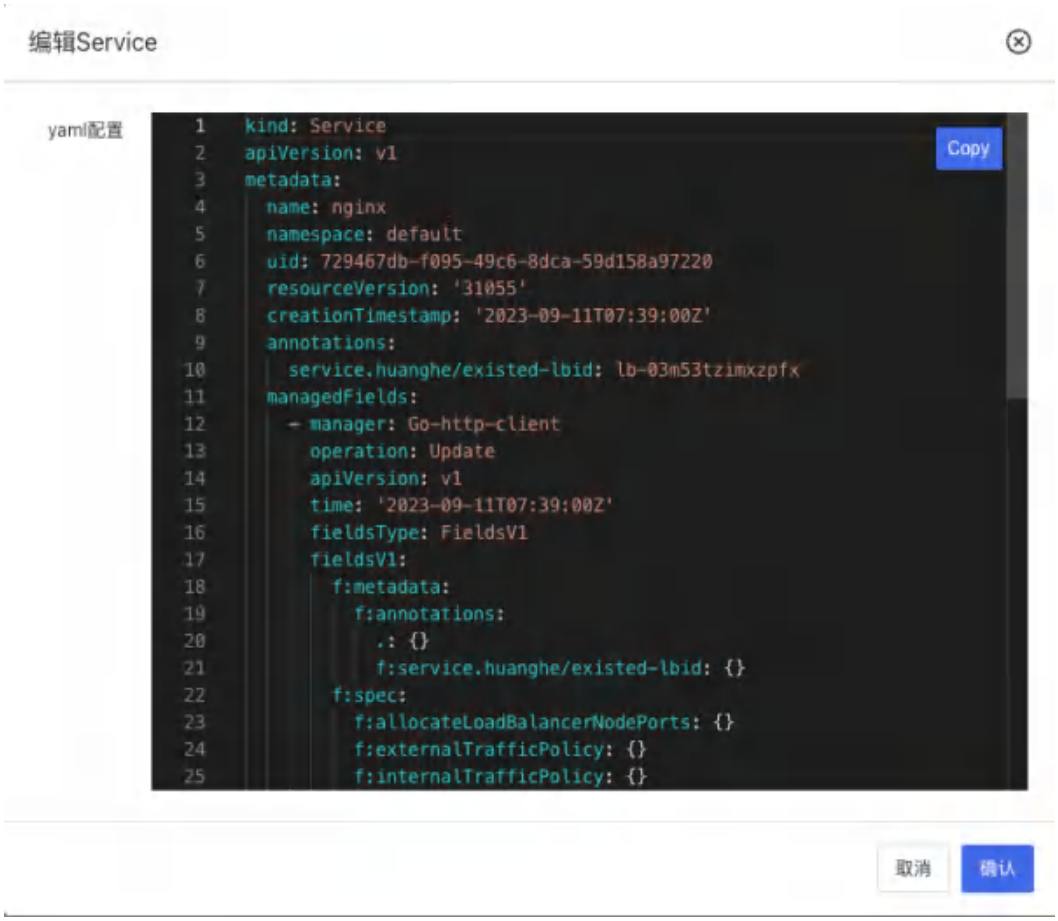
创建服务路由时，需要先选择命名空间，然后选择服务路由类型，点击添加 yaml，添加服务路由配置，创建服务路由。默认会显示服务路由的配置模版。服务路由包括：Service，Ingress。

8.11.1 Service

Service 是 Kubernetes 中的一种资源对象，用于提供稳定的网络访问和负载均衡，以将流量路由到运行在集群中的应用程序。

Service 列表展示 Service 的名称，命名空间，类型，Labels，Selector，访

问入口，操作（编辑 yaml，删除）。



Service LoadBalancer 模版


```
apiVersion: v1
kind: Service
metadata:
  annotations:
    # 指定当前 service 使用的 lb，必填项
    service.huanghe/existed-lbid: "lb-03m53tzimxzpfx"
    # 源地址探测协议支持的值 On/Off，默认 Off，只支持 TCP 协议
    # service.huanghe/proxy-protocol: "Off"
    # 负载均衡调度算法: rr/least_conn/ip_hash, 默认 "rr"
    # service.huanghe/scheduler: "rr"
    # 会话保持类型: None/Auto 默认 "None" UDP: 基于源 IP 实现会话保持,只支持 UDP 协议
    #ingress.huanghe/persistence-type: "None"
    # 连接空闲超时 1~86400 默认 "60"
    #ingress.huanghe/keepalive-timeout: "60"
  name: nginx
spec:
  ports:
    - name: nginx
      port: 80
      protocol: TCP
      targetPort: 80
  selector:
```

```
    run: nginx
  type: LoadBalancer
```

Service ClusterIP 模版

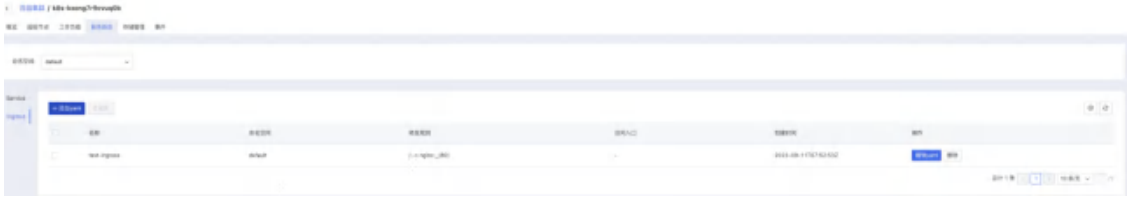
```
apiVersion: v1
kind: Service
metadata:
  name: nginx
spec:
  clusterIP: None
  ports:
    - name: nginx
      port: 80
      protocol: TCP
      targetPort: 80
  selector:
    run: nginx
```

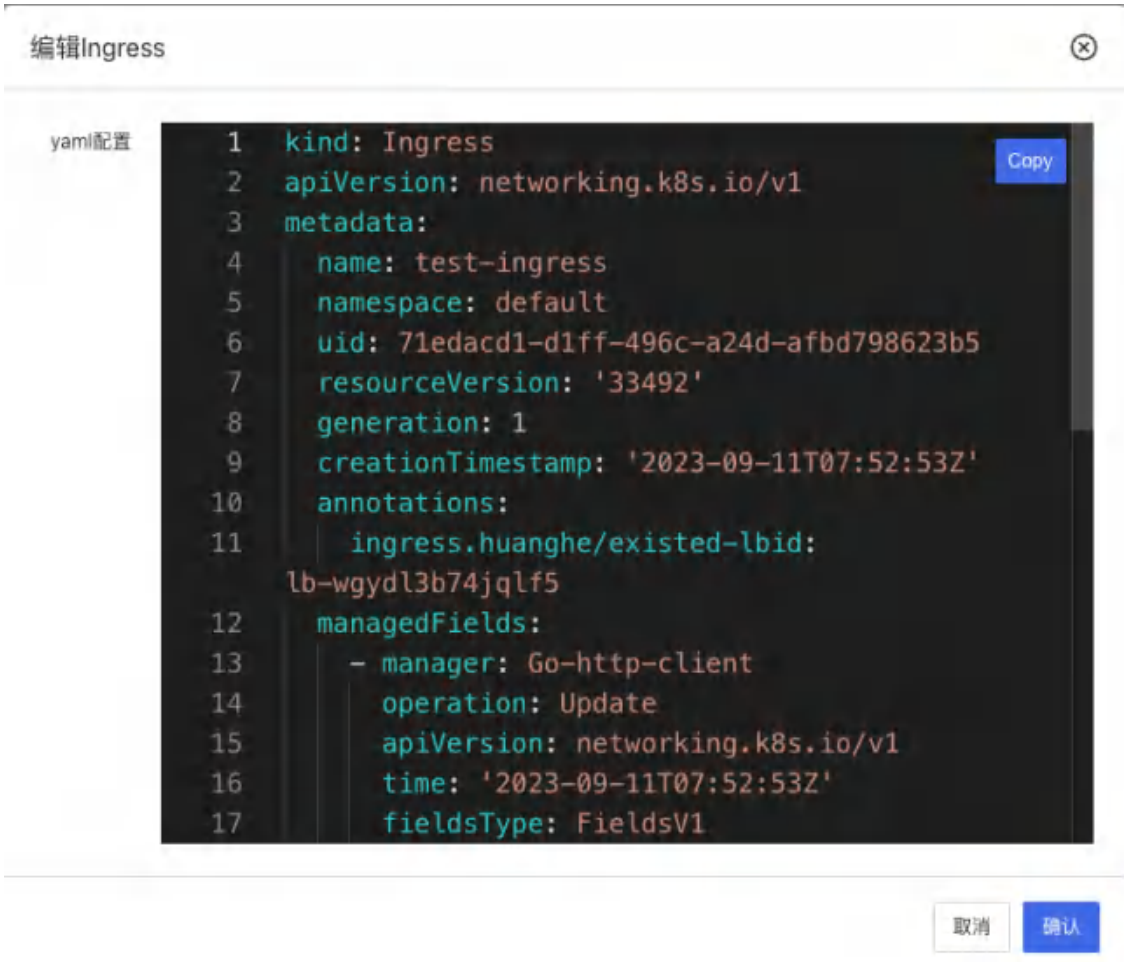
8.11.2 Ingress

Ingress 是 Kubernetes 中的一种资源对象，用于管理集群内部外部的 HTTP 和 HTTPS 路由。它充当了集群内部服务和外部世界之间的入口，允许外部流量流向不同的服务。

通过 Ingress，可以定义和配置 HTTP 和 HTTPS 的路由规则，将请求流量路由到集群内部的不同 Service 或 Pod。它提供了高级的负载均衡、SSL/TLS 终止和路径路由等功能，使集群内的服务能够以统一的方式对外提供访问。

Ingress 列表展示 Ingress 的名称，命名空间，转发规则，访问入口，创建时间，操作（编辑 yaml，删除）。Ingress 和负载均衡一一对应，不能多个 Ingress 共用同一个负载均衡。





Ingress 模版

```
apiVersion: networking.k8s.io/v1
kind: Ingress
metadata:
  name: test-ingress
  annotations:
    # 指定当前使用的 lb 实例 id，必填项
    ingress.huanghe/existed-lbid: "lb-wgydl3b74jqlf5"
    # 调度算法：rr/least_conn/ip_hash 默认 "rr"
    #ingress.huanghe/scheduler: "rr"
    # 会话保持类型：None/Auto/Manual 默认 "None"
    #ingress.huanghe/persistence-type: "None"
    # 会话保持 Key：当会话保持模式是 Manual 时，可以设定此值
HTTP/HTTPS: 基于 cookie 实现会话保持
    #ingress.huanghe/persistence-key: ""
    # 连接空闲超时 1~86400 默认 "60"
    #ingress.huanghe/keepalive-timeout: "60"
```



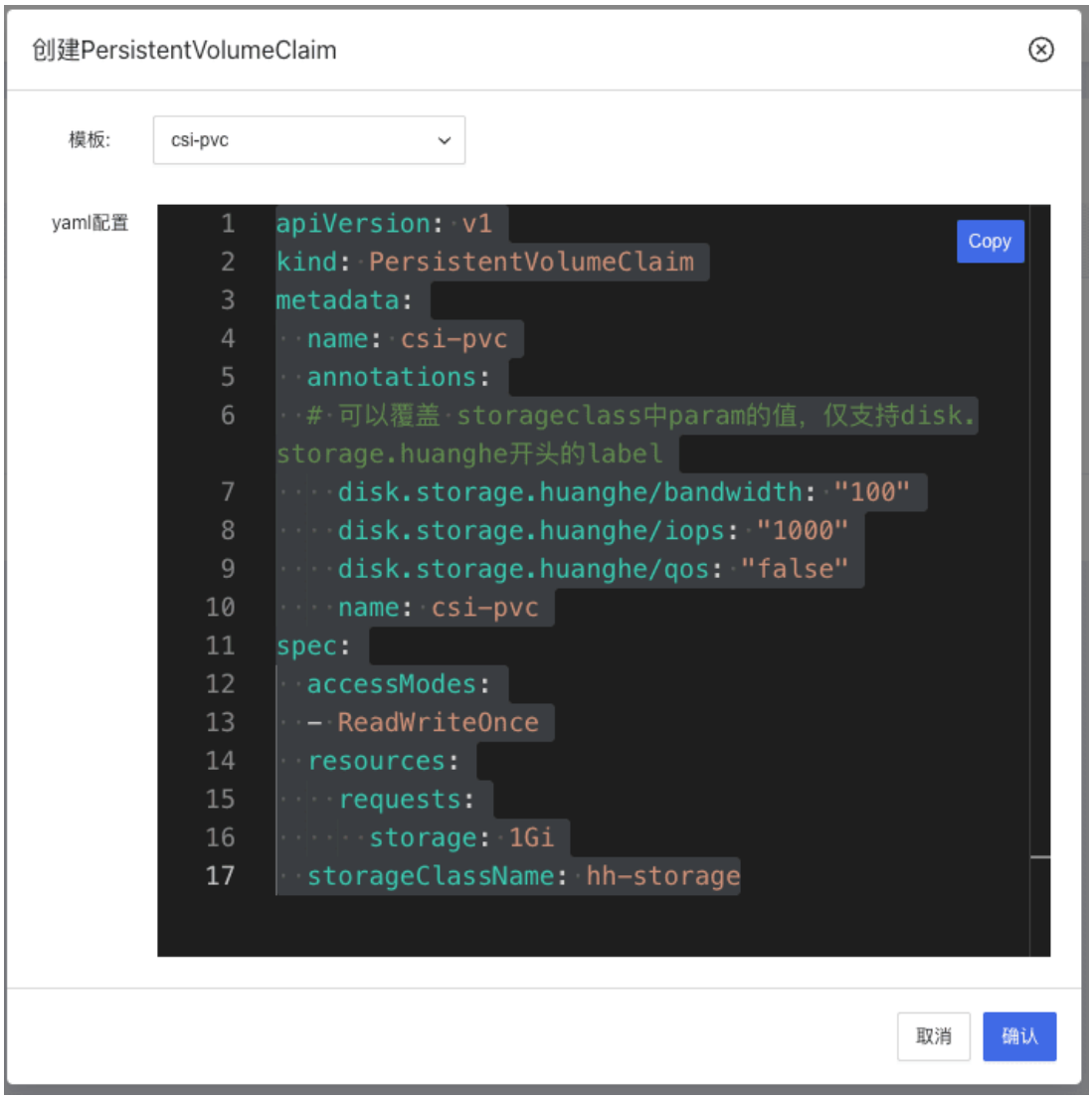
```
        # ingress 选取后端服务的模式，支持的值 true/false 默认值 "true"
        #ingress.huanghe/direct-access: "true"
spec:
    ingressClassName: ingress-ulb
    rules:
    - host: example.com
        http:
            paths:
            - path: /
                pathType: Prefix
                backend:
                    service:
                        name: nginx
                        port:
                            number: 80
```

8.12 存储管理

PersistentVolumeClaim（PVC）是 Kubernetes 中用于声明持久化存储资源的对象。它允许应用程序声明对持久卷（PersistentVolume）的需求，并提供了一种与持久化存储进行交互的机制。当前版本只支持平台内的分布式存储集群。

8.12.1 创建 PersistentVolumeClaim

选择命名空间后，添加 yaml，创建 PVC。



PVC 模版

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: csi-pvc
  annotations:
  # 可以覆盖 storageclass 中 param 的值，仅支持 disk.storage.huanghe 开头的 label
    disk.storage.huanghe/bandwidth: "100"
```



```
        disk.storage.huanghe/iops: "1000"
        disk.storage.huanghe/qos: "false"
        name: csi-pvc
spec:
    accessModes:
    - ReadWriteOnce
    resources:
        requests:
            storage: 1Gi
    storageClassName: hh-storage
```

从 PVC 克隆模版

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
    name: csi-pvc-clone
spec:
    storageClassName: hh-storage
    dataSource:
        name: csi-pvc
        kind: PersistentVolumeClaim
        apiGroup: ""
    accessModes:
```



```
  - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```

从 PVC 创建快照模版

```
apiVersion: snapshot.storage.k8s.io/v1
kind: VolumeSnapshot
metadata:
  name: csi-pvc-snapshot
spec:
  volumeSnapshotClassName: hh-snapclass
  source:
    persistentVolumeClaimName: csi-pvc
```

从快照创建 PVC 模版

```
apiVersion: v1
kind: PersistentVolumeClaim
metadata:
  name: restored-pvc
spec:
  storageClassName: hh-storage
  dataSource:
    name: csi-pvc-snapshot
```



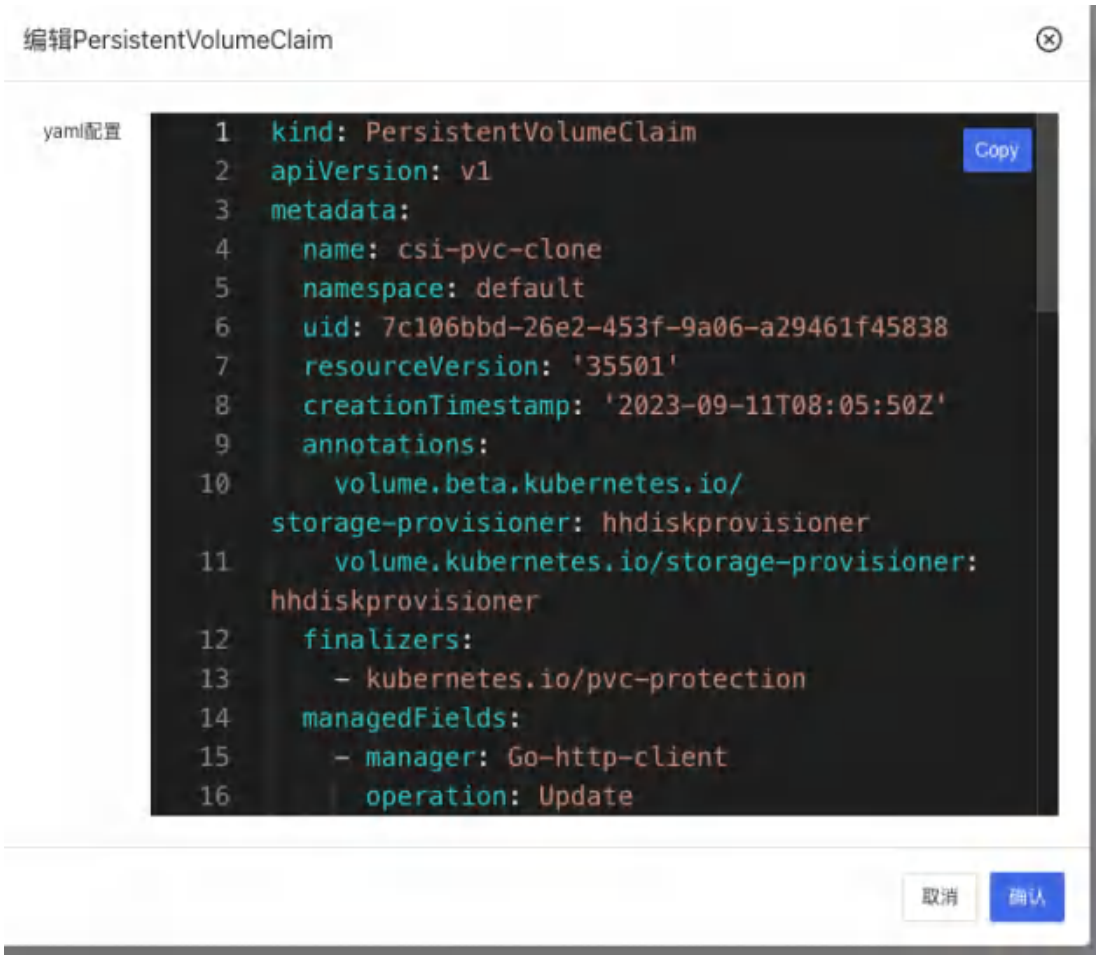
```
    kind: VolumeSnapshot
    apiGroup: snapshot.storage.k8s.io
  accessModes:
    - ReadWriteOnce
  resources:
    requests:
      storage: 1Gi
```

8.12.2 查看 PVC 列表

PVC 列表展示 PVC 名称，命名空间，状态，容量，访问权限，StorageClass，操作（编辑 yaml）

8.12.3 编辑 PVC

支持用户修改 PVC 的 yaml 配置。



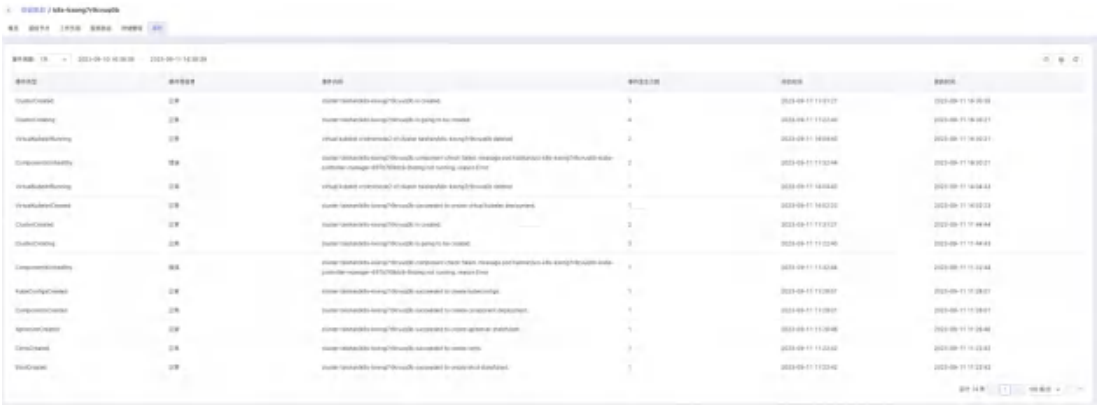
8.12.4 删除 PVC

支持用户删除 PVC。

8.13 容器集群事件

支持用户查看容器集群事件，支持按时间筛选，展示事件类型，事件等级，

事件内容，事件发生次数，开始时间，更新时间。



8.14 版本说明

当前版本与标准 Kubernetes 能力对比：

- 1.暂不支持 hostNetwork
- 2.暂不支持 Pod 健康检查
- 3.暂不支持与实际物理机亲和，反亲和
- 4.暂不支持 NetworkPolicy
- 5.暂不支持 HPA
- 6.QosClass 不受限的情况下会分配一个默认值
- 7.暂不支持 windows Pod
- 8.暂不支持 PDB(Pod 中断预算)
- 9.暂不支持 service ClusterIP，Service spec.ClusterIP 需要设置为 None
- 10.service loadbalance 类型暂不支持 DNS 域名访问

9 运维与管理

9.1 资源模板

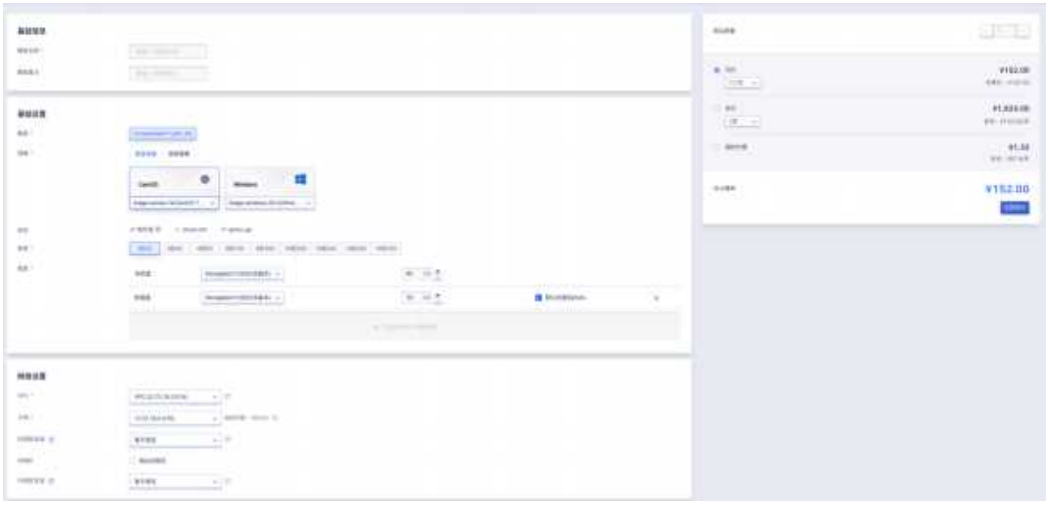
9.1.1 概述

资源模版支持租户预定义创建资源的参数配置，保存到模版中，便于后续快速创建，以及结合水平弹性伸缩完成业务节点的快速阔缩。

9.1.2 创建虚拟机模版

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虚拟机模板，用于从模板创建虚拟机实例。虚拟机模板不占用实际资源。

1. 选择地域（数据中心）后，在左侧导航栏选择虚拟机模板，进入虚拟机模板控制台，点击“创建”，弹出虚拟机模板创建向导；



2. 选择虚拟机模板的机型，并确定虚拟机模板的操作系统镜像；

- 机型是运行虚拟机的节点的集群类型，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，通过 ARM 机型创建的实例为 ARM 版虚拟机实例，已适配国产芯片、服务器及操作系统，并可运行国产化操作系统，如 UOS 或银

河麒麟。

- 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，同时基础镜像的默认时区为上海。
  - 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。

3. 选择虚拟机模板的规格配置，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。
4. 选择并配置虚拟机模板的系统盘和数据盘，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，创建虚拟机模板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，步长为 1GB，即容量应为 1GB 的倍数。

- 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，创建虚拟机模板配置一块云盘。
  - 数据盘挂载路径可选择默认为/data（windows 系统除外）。

5. 配置网络相关设置，包括 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；

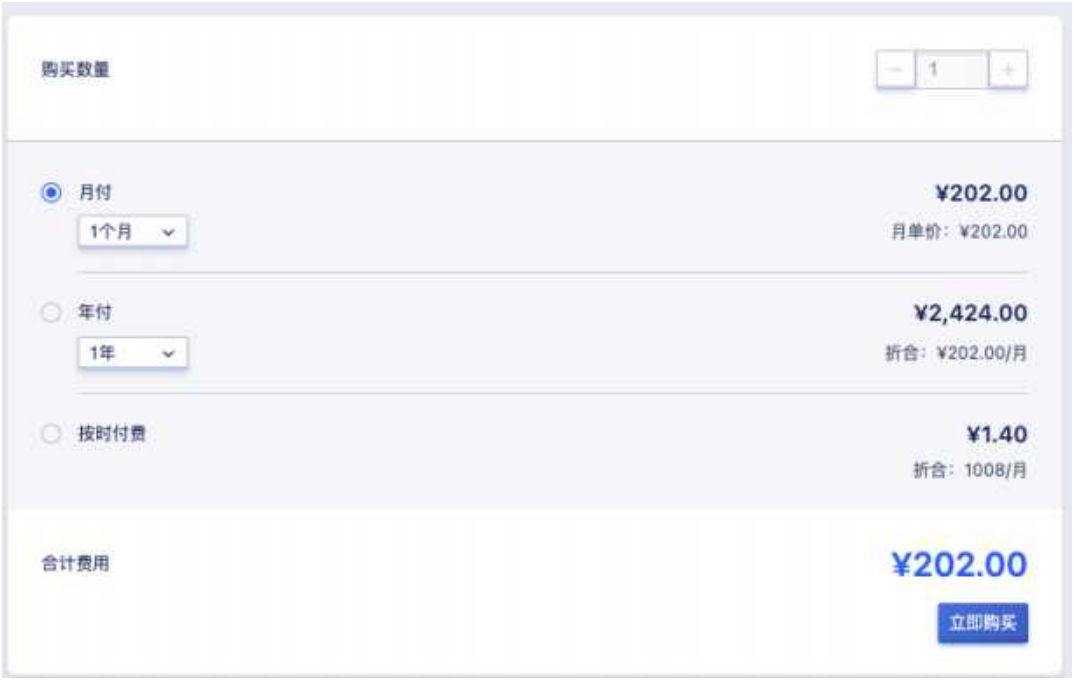
- 创建虚拟机模板时必须选择 VPC 网络和所属子网；
- 控制台已为用户计算所选子网的可用 IP 数量，创建时需指定可用 IP 数量足够的子网；
- 安全组是平台提供的虚拟防火墙，提供出入双方向流量访问控制规则，定义哪些网络或协议能访问资源；
- 外网安全组用于控制虚拟机南北向（外网 IP）的流量，内网安全组用于虚拟机东西向（网卡间）的安全访问控制；
- 外网 IP 为虚拟机提供的弹性外网出口服务，平台支持 IPv4/IPv6 双栈网络。创建虚拟机模板时选中外网 IP，可在虚拟机模板创建虚拟机时为虚拟机绑定一个外网 IP 地址。

6. 选择并配置虚拟机模板基础管理配置，包括登录方式、登录密码（可选择随机生成）和项目组信息等。

- 管理员名称：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；
- 登录方式：为虚拟机模板设置登录凭证，即登录虚拟机的密码，可选择随机生成；

选择的镜像既无 cloud-init 特性也无 qemu-ga 特性时，不支持设置密码，管理员名称、登录方式、管理员密码不展示。

7. 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。



- 购买数量：固定为 1；

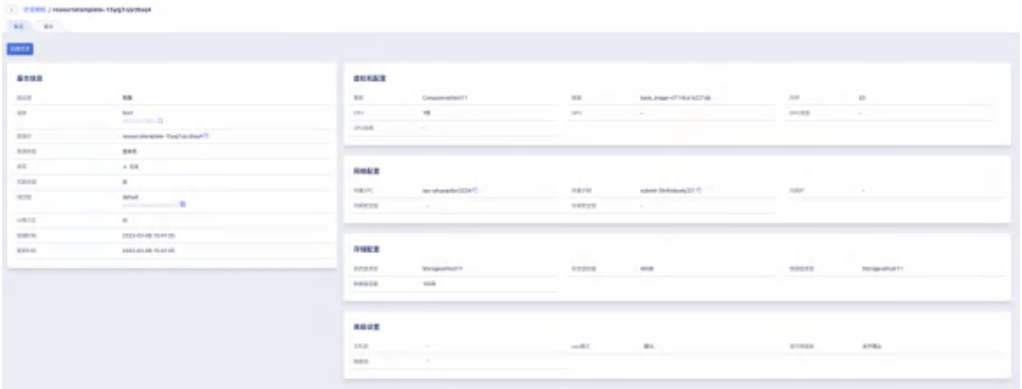
- 付费方式：选择虚拟机的计费方式，支持按时、按年、按月三种方式，可根据需求选择适合的付费方式；
- 合计费用：用户选择虚拟机 CPU、内存、数据盘、外网 IP 等资源按照付费方式的费用展示；
- 立即购买：点击立即购买后，会返回虚拟机模板列表页，不进行实际的扣费操作。从虚拟机模板创建虚拟机时需进行扣费操作。

9.1.3 查看资源模版列表

资源模板列表页可查看当前账户下已有的资源模板，包括名称、资源 ID、状态，资源类型，项目，标签，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。

9.1.4 查看虚拟机模板详情信息

在资源模板列表上点击模板名称进入模板详情页面，虚拟机模版包含基本信息、虚拟机配置、网络配置、存储配置、高级设置。

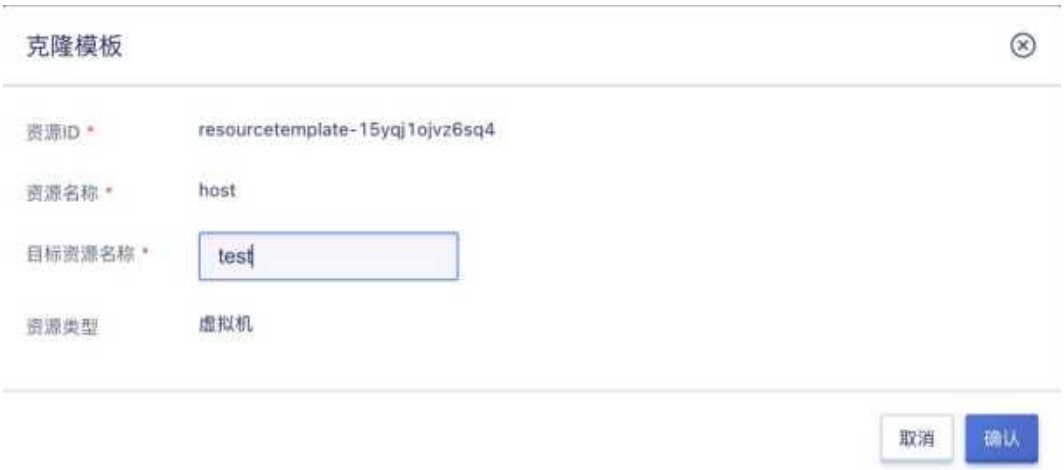


9.1.5 创建资源

在资源模版列表点击创建资源，设置资源名称，管理员密码，即可创建出对应配置的虚拟机。

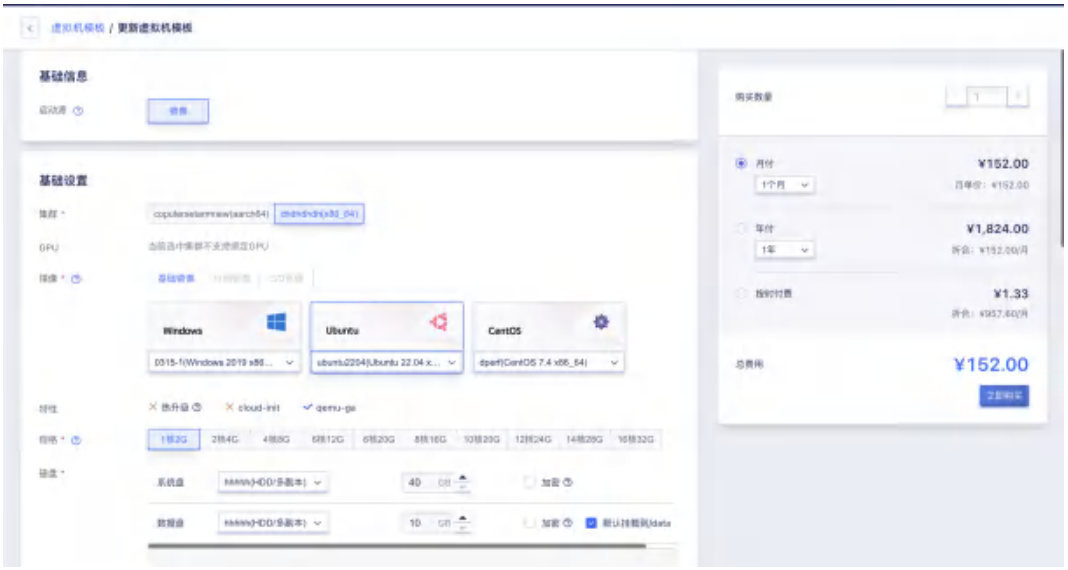
9.1.6 克隆模版

在资源模版列表点击克隆模版，设置目标资源名称，即可克隆出相同配置的资源模版。



9.1.7 更新模版

在资源模版列表点击更新，打开更新资源模版页，更新要修改的配置点击立即购买，即可更新资源模版。



9.1.8 修改标签

在资源模版列表点击修改标签按钮，选择要修改的标签点击确认，即可更新资源模版的标签。

9.1.9 删除资源模版

在资源模版列表点击删除按钮，点击确认即可删除资源模版。资源模板已关联资源时不可删除，删除资源模板后对通过资源模板创建的资源无影响。

9.2 标签管理

9.2.1 标签功能简介

9.2.1.1 产品概述

标签用于标记各项云资源，从不同维度对具有相同特征的云资源进行分类、搜索和聚合，让资源管理变得更加方便。标签由一对键值对（key:value）构成，用户可根据需求自定义键值对内容，绑定不同资源。

9.2.1.2 标签功能

标签管理模块具有以下功能：

- 支持标签批量创建，单次创建，删除标签功能
- 支持查看资源，展示该条标签下所有绑定的资源
- 支持绑定资源，可选择不同地域下不同资源类型进行绑定
- 支持解绑资源，可批量解绑

同时，标签支持资源创建时选择需要的标签进行添加，支持在资源界面对标签进行添加与删除操作。资源界面将会展示当前资源所绑定的标签键值对。

支持统一的搜索入口，可根据 key/value，资源 ID，资源类型，三个维度进行绑定资源到查询，灵活操作资源，可在云资源界面以及标签管理界面进行搜索，方便查询管理较大数量的标签，以及快速的匹配资源。

9.2.1.3 使用限制

- **标签命名限制**

标签键以及 value 值支持最大 127 位字符，不能为空，区分大小写-标签 key 以及 value 内容支持 utf-8 格式表示的大小写数字、汉字、数字、空格以及特殊字符

- **数量规范**

1 个资源最多可以绑定 50 个标签-1 个标签包含 1 个标签键和 1 个标签值（tagKey:tagValue）-1 个资源上的同一个标签键只能对应 1 个标签值-单次批量创建标签数量最多不超过 5 个

- **资源状态限制**

虚拟机除过删除，删除中和失败的资源不能更新标签，其他状态下可修改资源绑定的标签内容。

9.2.1.4 支持的资源

目前租户侧支持的资源类型包括：虚拟机、虚拟机模版、镜像、VPC、子网、云硬盘、弹性网卡、快照、弹性 IP、负载均衡、SSL 证书、安全组、IP 组、端口组、NAT 网关、Redis、MySQL、对象存储、文件存储、VPN 网关、对端网关、隧道、伸缩组、VIP、组播、隔离组。

管理侧支持的资源类型包括：外网网络、专线接入。

9.2.2 查看标签管理界面

进入运维与管理模块，点击标签管理进入管理界面，支持查看标签的标签键、标签值、绑定资源数量、操作（查看资源、绑定资源、删除）如下图所示：

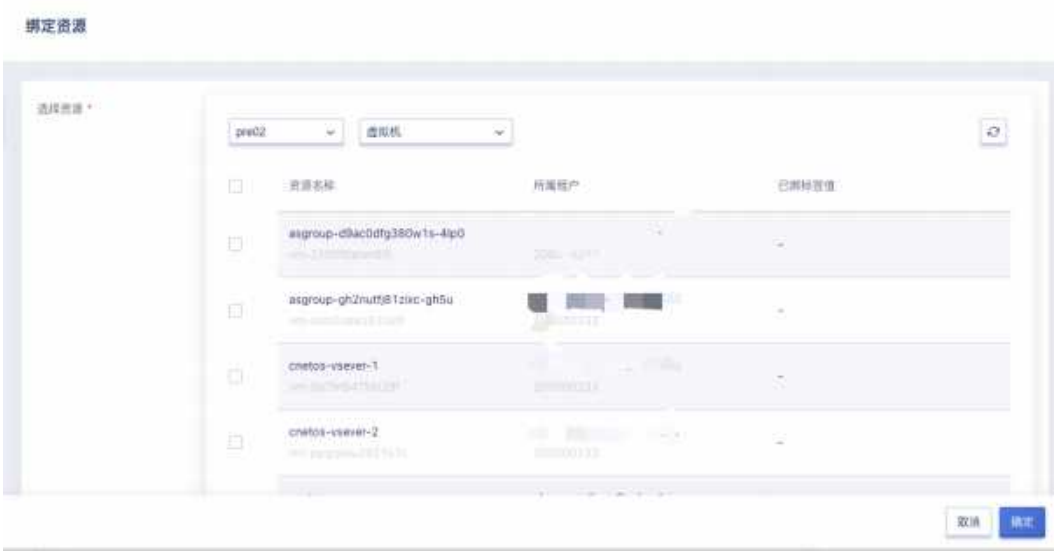
9.2.3 创建标签

点击标签管理左上角创建按钮，弹出标签创建弹窗，按照格式要求填写标签键和标签值，点击添加行后面加号可添加新的一条键值对，点击标签值后边的加号可添加该标签下的新 value 值。如下图所示：

9.2.4 标签添加资源

点击标签操作中的绑定资源按钮，弹出绑定资源弹窗，支持查看不同地域

下不同类型的可绑定资源列表。点击列表前方框可批量添加资源，已绑定标签值中展示的是当前键下该资源已绑定的一个 value 的值。未展示则该键下当前资源还未绑定 value 值。添加界面如下图所示：



如果该资源在此键下已绑定标签值，绑定新标签值后将与旧标签值解绑，每个资源同一个标签键只能对应 1 个标签值.

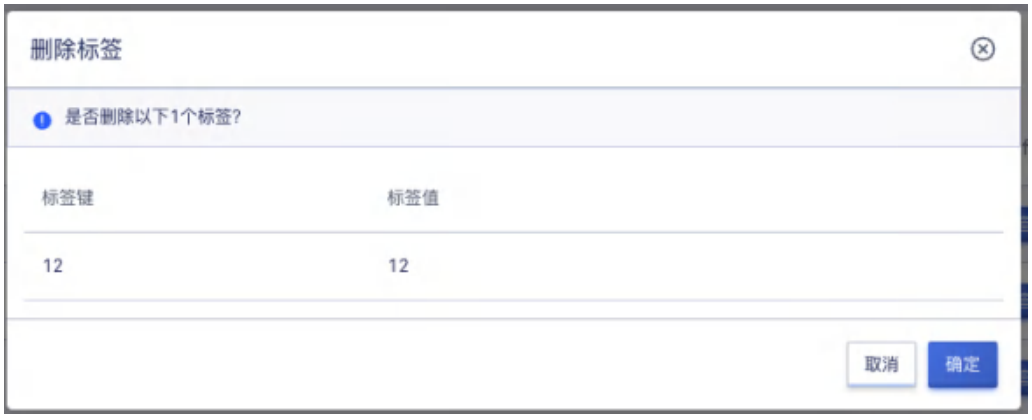
可以在相关资源界面点击修改标签，修改该资源下绑定的标签，支持对该资源下的标签进行删除，添加操作。

9.2.5 标签解绑资源

点击标签操作中的查看资源，弹出此标签所绑定的资源列表，支持查看资源 ID，资源类型，地域信息，操作解绑资源。选择资源前方框可批量选择，点击左上方解绑资源批量解绑，也可在资源行最后通过解绑资源按钮来实现解绑资源。

9.2.6 删除标签

点击标签行删除按钮，弹出如下图所示弹窗，点击确定删除标签，支持批量删除。删除时需要确定标签内未绑定资源，否则无法删除。



9.3 弹性伸缩

9.3.1 产品简介

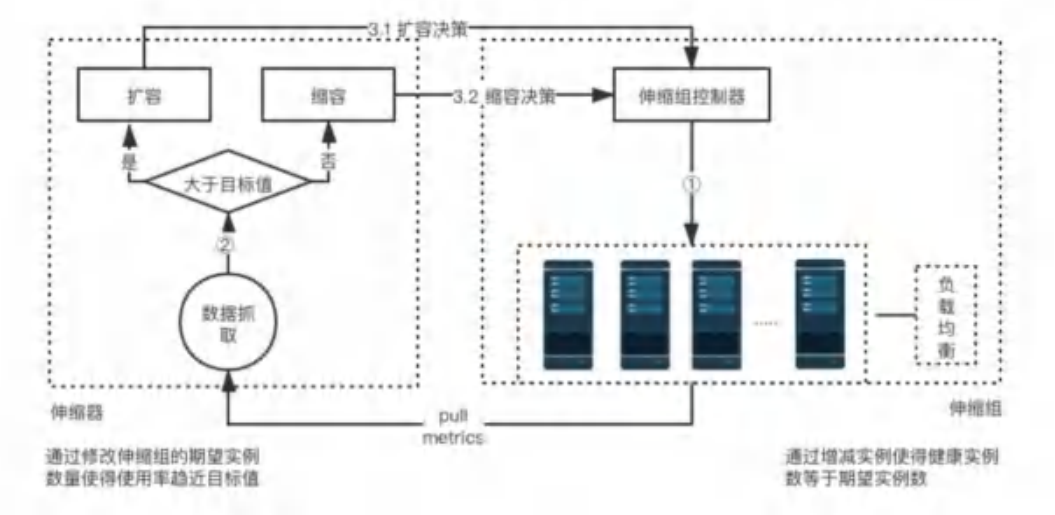
9.3.1.1 概述

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。

9.3.1.2 逻辑架构

水平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，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。
  - 虚拟机类型根据 CPU、内存使用率的阈值触发伸缩动作，
  - 监听器类型根据负载均衡中 Vsever 的七层连接数、七-层 QPS、七层响应时间、四层连接数、四层 CPS 的阈值触发伸缩动作
- 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。

9.3.1.3 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。若伸缩组关了负载均衡，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。

9.3.1.4 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伸缩阈值数据，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伸缩阈值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伸缩阈值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伸缩指标监控数据平均值，用于判断是否需要缩容伸缩组中的实例。**

9.3.1.5 功能特性

水平伸缩通过伸缩组、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，虚拟机类型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。监听器类型的伸缩组创建时需要绑定负载均衡。

- 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伸缩组中的实例。

- 支持按照伸缩组中健康实例的虚拟机和监听器指标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，避免因阈值过高，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，避免因阈值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事件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监控指标数据，并可通过告警模板对监控数据进行告警配置，在使伸缩指标触发扩缩容时，为用户发送告警邮件。

虚拟机类型的伸缩策略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。

9.3.2 虚拟机模板管理

虚拟机模板是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，支持虚拟机模板的

创建、查看、删除及创建虚拟机等生命周期管理。

9.3.2.1 创建虚拟机模板

用户可根据业务需要通过虚拟机控制台——虚拟机模板资源列表创建适合业务的虚拟机模板，用于伸缩器自动增加虚拟机实例时的模板。虚拟机模板与创建虚拟机一致，只需要额外提供模板名称及模板备注即可，如下图所示：

模板名称和备注是指当前要创建的虚拟机模板的名称和描述，基础配置、网络设备、管理配置与创建虚拟机一致，代表使用该模板创建虚拟机时指定的参数，如虚拟机规格和操作系统等；同时虚拟机模板无需指定虚拟机名称，由弹性伸缩组创建时自动生成虚拟机名称。

创建模板时需要指定模板中虚拟机的付费方式，即代表通过该模板创建的虚拟机的付费方式，如按月；同时创建模板时会展示该模板创建虚拟机时需要付的费用。

创建模板时并不会真正扣费，仅当弹性伸缩组自动创建实例时才会根据预计费用进行扣费。

9.3.2.2 查看虚拟机模板

用户可通过虚拟机模板列表页面查看虚拟机模板的列表信息，包括名称、ID、VPC、子网、机型、配置、关联资源、计费方式及操作项，如下图所示：

- 名称/ID：指虚拟机模板的名称及全局唯一标识符。
- VPC/子网：指通过虚拟机模板创建的虚拟机所属 VPC 和子网。
- 机型/配置：指通过虚拟机模板创建的虚拟机所属机型及配置。
- 关联资源：指虚拟机模板已关联的弹性伸缩组，即伸缩组会通过虚拟机模板中的配置创建实例。
- 计费方式：指通过虚拟机模板创建的虚拟机的付费方式。

列表上操作项是指通过虚拟机模板手动创建虚拟机，同时用户也可点击虚拟机模板的名称进入虚拟机模板详情，查看虚拟机模板的详细信息，包括基本信息、虚拟机配置、网络配置及存储配置信息。

9.3.2.3 模板创建虚拟机

支持用户通过模板手动创建虚拟机，适用于需要通过模板创建虚拟机的场景。如下图所示：

通过模板创建虚拟机时需要指定虚拟机名称，也可指定虚拟机的登录密码，如不指定则采用创建模板时指定的登录密码。

9.3.2.4 修改名称和备注

修改虚拟机模板的名称和备注，在任何状态下均可进行操作。可通过点击虚拟机模板列表页面每个镜像名称右侧的“编辑”按钮进行修改。

9.3.3 水平伸缩

水平伸缩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，适应多种自动伸缩场景。伸缩组是通过伸缩策略中对于伸缩规则及伸缩实例数来维护组内实例的期望水平，并通过虚拟机模板创建新的实例。

- 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伸缩组中的实例，即固定数量模式无需指定伸缩策略。

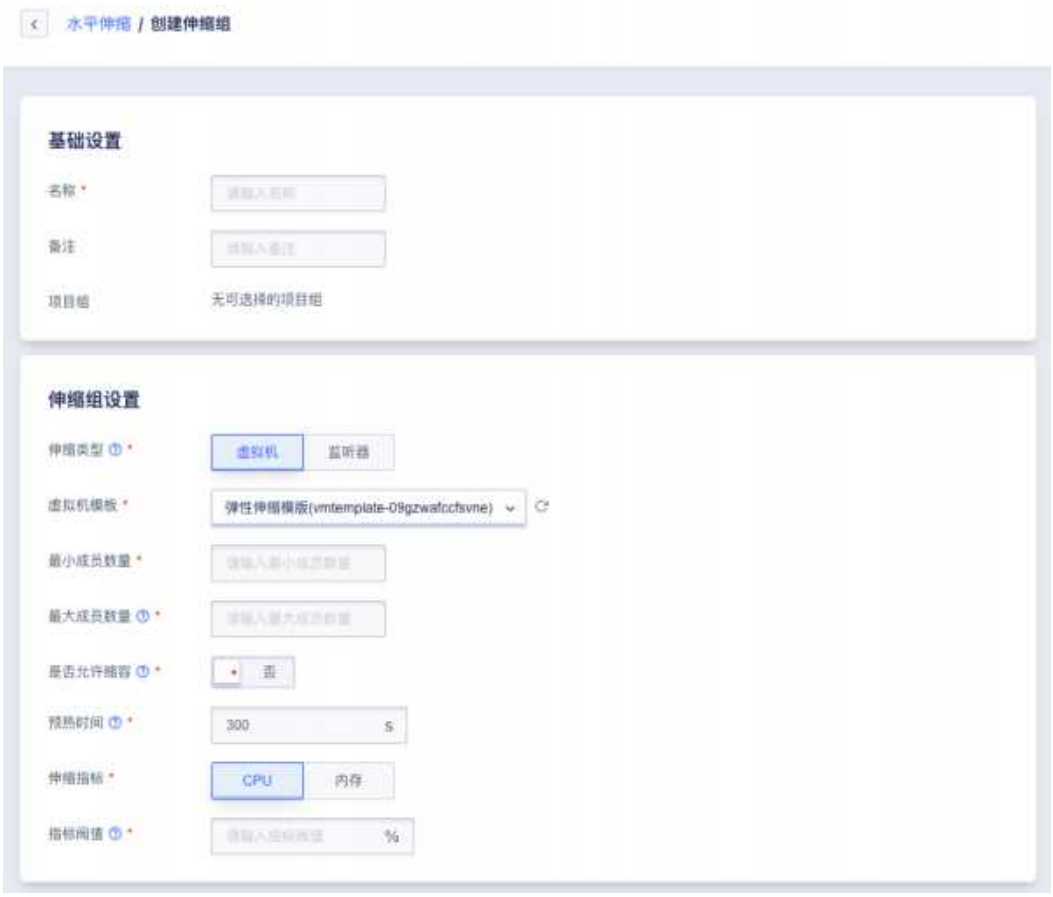
支持伸缩组预热时间，使虚拟机创建成功后，在预热时间内拉起应用程序以承接业务流量；同时支持虚拟机类型伸缩组关联负载均衡，为伸缩组中的虚拟机业务提供负载均衡服务，同时通过监听器的健康检查机制，判断伸缩组中所有实例的业务健康状况，自动剔除业务不健康的实例并新增健康实例到业务集群。

作为自动伸缩服务的最核心模块，支持水平伸缩的全生命周期管理，包括创建伸缩组、查看伸缩组、修改伸缩组、启动/禁用伸缩组、绑定/解绑负载均衡、查看伸缩日志及删除伸缩组等。

9.3.3.1 创建水平伸缩

用户可通过伸缩组控制台，指定虚拟机模板、预热时间、伸缩模式创建一个弹性伸缩组，用于动态扩缩组内的虚拟机实例，适应需要弹性伸缩的业务场

景。如下两图创建虚拟机类型和监听器类型的伸缩组示例：



（1）虚拟机伸缩类型

目前支持设置 CPU、内存使用率作为伸缩指标，可后续绑定负载均衡为伸缩组中资源提供负载均衡服务。

（2）监听器伸缩类型

目前支持 TCP、HTTP、HTTPS 三种协议类型，选择 TCP 协议时伸缩指标可选四层连接数、四层 CPS 作为伸缩指标，选择 http 以及 https 协议时可选择七层连接数、七层 QPS、七层响应时间作为伸缩指标。监听器类型伸缩组创建时需要预先创建负载均衡以及相应协议的 Vsever 监听器。

- **名称/备注：**伸缩组的名称和备注信息，用于标识伸缩组。

- **虚拟机模板**：伸缩组为组内新增虚拟机实例时所使用的虚拟机模板，即会根据所选虚拟机模板为组内新增虚拟机实例，创建时必须指定，仅支持选择有权限的虚拟机模板。
- **预热时间**：伸缩组内虚拟机实例创建成功后的预热时间，在预热时间内虚拟机可拉起应用程序以承接业务流量，预热中的虚拟机实例在伸缩组中处于【启动中】状态。创建时必须指定，默认为 300s。
- **成员数量设置**：可设置最小成员数量和最大成员数量，调度后的资源数量不会超过设置的成员数量上下限。如果想要达到固定数量的效果，可以将最大成员数量、最小成员数量设置成一致。
- **是否允许缩容**：允许缩容时伸缩组会在未满足指标时减少资源数量，缩容时会给虚拟机内的业务进程发送 SIGTERM 信号，最多等待 90 秒后关闭并删除虚拟机，业务进程可利用该机制优雅关闭。
- **伸缩指标**
  - 虚拟机指标 CPU 内存（单位%）
  - 监听器指标七层连接数（个）、七层 QPS（个/s）、七层响应时间（ms）、四层连接数（个）、四层 CPS（个/s）
- **指标阈值**：统计标准 10min 内所有虚拟机监控数据的平均值

模板配置界面展示了当前伸缩组所使用的模版基本信息，包括镜像、CPU、内存、磁盘配置，外网绑定情况（如果绑定 EIP，模版启动虚拟机时将自动申请 EIP）如下图所示

点击创建后，平台即会根据指定的配置创建伸缩组，并自动维护伸缩组内的实例数量，同时会扣取新增实例的费用（伸缩组不收取额外费用，但用户需要为伸缩组中创建的虚拟机实例付费），用户可通过伸缩组列表及详情查看伸缩组的实例及相关信息。

9.3.3.2 伸缩组列表

用户可通过弹性伸缩控制台查看账户内拥有的所有伸缩组的列表及相关信息，并可通过列表的名称进入伸缩组详情查看伸缩组的监控信息、实例信息、事件，同时可通过伸缩组的负载均衡对伸缩组进行负载均衡的绑定和解绑操作，具体列表信息如下图所示：

- 名称/ID：伸缩组的名称及全局唯一标识符。
- 启动模板：伸缩组关联的虚拟机模板，即组内新增实例时所使用的虚拟机模板。
- 伸缩类型：伸缩类型分为虚拟机和监听器两种。
- 当前实例：伸缩组内当前的虚拟机实例数量，正常情况下等于期望实例数量。
- 状态：指伸缩组的运行状态，包括可用、不可用。

列表上支持对伸组组进行更新、启动、禁用、删除等操作，同时支持对伸缩组进行批量启用、批量禁用及批量删除操作。

9.3.3.3 水平伸缩详情

用户可进入伸缩组详情查看伸缩组内的详细信息，包括伸缩组的基本信息、伸缩策略、监控信息、实例信息、事件及关联的负载均衡信息，如下图所示：

（1）基本信息

包括资源 ID、资源名称、虚拟机模板、预热时间、当前实例数量。

（2）伸缩策略

包括伸缩模式和期望寮例数量。

（3）监控信息

伸缩指标的监控信息，用户可通过监控信息查看组内所有虚拟机实例的平均 CPU 使用率，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，默认可查看一小时，可通过时间筛选，查看自定义时间的监控信息。

（4）实例信息

指伸缩组内当前实例的列表信息，包括实例的名称、ID、启动模板、IP 地址、创建时间及状态，详见。

（5）负载均衡

指伸缩组已关联的负载均衡实例，并可通过负载均衡管理绑定或解绑负载均衡，详见。

（5）事件

指伸缩组内的实例伸缩信息，如添加或移除实例的事件信息，详见。

9.3.3.3.1 查看伸缩组实例

用户可通过伸缩组详情中的【实例】标签页查看当前伸缩组中的实例信息，如下图所示：

伸缩组实例支持从已创建的虚拟机资源中添加到伸缩组中，也可从伸缩组实例中移除虚拟机，移除后的虚拟机将会被自动删除。

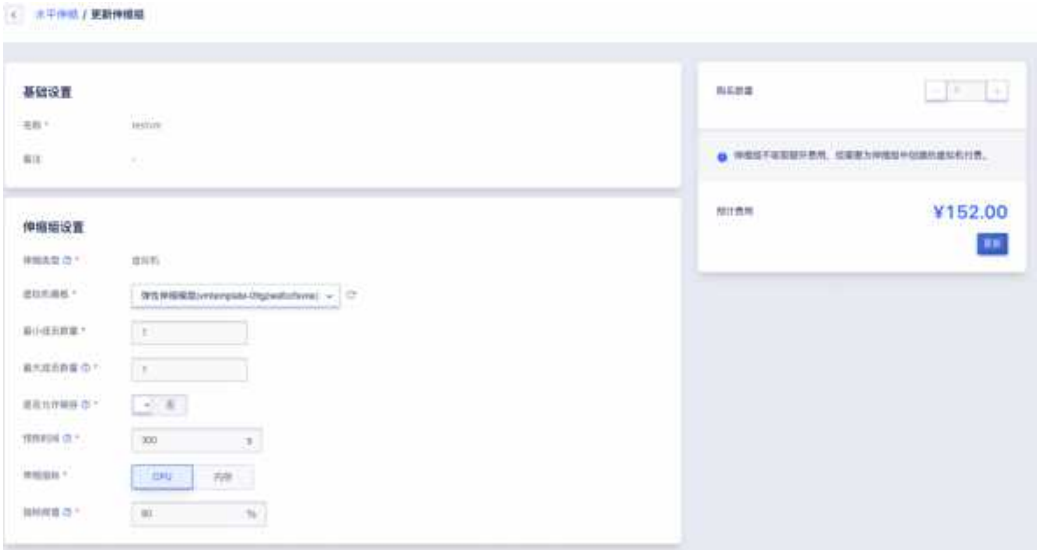
- 实例的名称为伸缩组自动命名，通常为伸缩组的名称+随机字符串。
- 启动模板为创建当前实例所使用的虚拟机模板，可通过虚拟机模板查看具体配置信息。
- IP 地址为虚拟机实例的 VPC 内网 IP 地址。
- 状态为当前实例的状态信息，包括启动中、运行及其它虚拟机相关状态信息。其中启动中指伸缩组中的虚拟机正在启动，或在伸缩组预热时间内，实例的状态会一直保持启动中，待超过预热时间后，会自动转换为运行，代表虚拟机为健康状态。
- 伸缩组每 15 秒获取一次被其控制的所有虚拟机状态，判断是否需要添加或删除实例。若伸缩组关了负载均衡，则由负载均衡判断伸缩组内的实例是否健康。
- 创建时间指当前实例的创建时间。

9.3.3.3.2 查看伸缩事件

可通过伸缩组详情中【事件】查看当前伸缩组中的实例变更事件，如添加实例或移除实例，并展示每次变更的详情原因和状态，包括事件类型、事件等级、事件内容、事件发生次数、开始时间、更新时间，方便用户对伸缩组集群业务进行维护，如下图所示：

9.3.3.4 修改伸缩组

支持用户自定义修改伸缩组的虚拟机模板、最小成员数量、最大成员数量、缩容策略、预热时间、伸缩指标、指标阈值，可通过伸缩组列表操作项中的更新进行操作，伸缩类型在创建后不可修改，如下图所示：



- **虚拟机模板**

若用户修改了伸缩组的虚拟机模板，不影响组内已有的虚拟机实例配置和

参数，仅影响新添加实例，即更新后新添加实例时以新的虚拟机模板创建虚拟机。

- **预热时间**

用户修改预热时间后，新添加的实例会根据新的预热时间进行运行状态，并接受业务处理。

- **实例数量/伸缩策略/伸缩指标/缩容策略/指标阈值**

用户修改伸缩组后，伸缩组会立即依据新的伸缩期望的实例数量维护组内虚拟机实例。

9.3.3.5 启用/禁用伸缩组

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。

仅支持在禁用状态启用伸缩组，从禁用状态执行启用后，伸缩组的状态变更为可用，并会根看成伸缩模式期望的实例数量对伸缩组执行实例数量及健康状态维护。

9.3.3.6 负载均衡管理

平台支持伸缩组关联负载均衡，**仅虚拟机类型伸缩组可绑定解绑**，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。

一个伸缩组可支持绑定多个负载均衡的监听器（VServer），使伸缩组对外提供多种业务服务。每一个负载均衡的监听器均会对组内虚拟机实例进行负载均衡的业务健康检查，并会自动剔除非健康实例，并由伸缩组自动启动健康实例到组内。

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。当伸缩组关了负载均衡，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。

平台支持支持对伸缩组的负载均衡进行绑定、解绑及查看已绑定负载均衡等管理，使用户可基于自动伸缩的负载均衡为伸缩组内的虚拟机实例提供负载分发服务，提升业务的可用性。

9.3.3.6.1 绑定负载均衡

支持用户将一个伸缩组绑定至多个负载均衡的 VServer 监听器仅虚拟机类型伸缩组可绑定解绑，由负载均衡监听器监控伸缩组内虚拟机实例的健康状态，绑定后伸缩组内的所有实例将自动作为服务节点加入至所绑定的负载均衡 VServer，用户可通过伸缩组详情——负载均衡中的绑定进入向导页面，如下图所示：

- 负载均衡/VServer：需要绑定的负载均衡及 VServer 监听器，必须指定已存在且有权限的负载均衡实例，绑定时必须指定，一次仅允许指定一个。
- Port：伸缩组内加入到负载均衡服务节点的虚拟机实例所提供的业务服务端口，即负载均衡转发流量至虚拟机的后端服务端口。

绑定后伸缩组内的所有实例将自动作为服务节点加入至所绑定的负载均衡 VServer，由负载均衡负责检查组内虚拟机实例的健康状态。

9.3.3.6.2 查看已绑定负载均衡

伸缩组绑定负载均衡后，可通过伸缩组内的负载均衡详情查看已绑定的负载均衡信息，包括负载均衡、VServerID、端口、权重及操作项，如下图所示：

在列表中负载均衡和 VServer 为已绑定的负载均衡名称及 VServer 的实例 ID；端口和权重代表伸缩组内虚拟机实例加入至负载均衡服务节点中的后端服务端口及权重。

同时在列表上操作项中可对每一个已绑定的负载均衡进行解绑操作，支持批量解绑，方便资源维护。

9.3.3.6.3 解绑负载均衡

用户可在业务需求时将伸缩组与负载均衡的关联进行解绑，解绑后伸缩组内的虚拟机实例均会从负载均衡的服务节点中进行移除，不会影响组内虚拟机及业务本身的运行，健康状态由伸缩组进行检查。

用户可通过伸缩组详情——负载均衡中的解绑或批量解绑进行操作，如下图所示：

9.3.3.7 删除伸缩组

平台支持用户删除不适合业务场景的伸缩组，在任何状态下均可进行删除。如下图所示：

删除后伸缩组会自动与虚拟机模板、伸缩策略、负载均衡进行解绑，同时会自动删除伸缩组创建出来的虚拟机，被伸缩组删除的虚拟机实例会直接销毁，不会进入回收站。

9.3.4 垂直伸缩

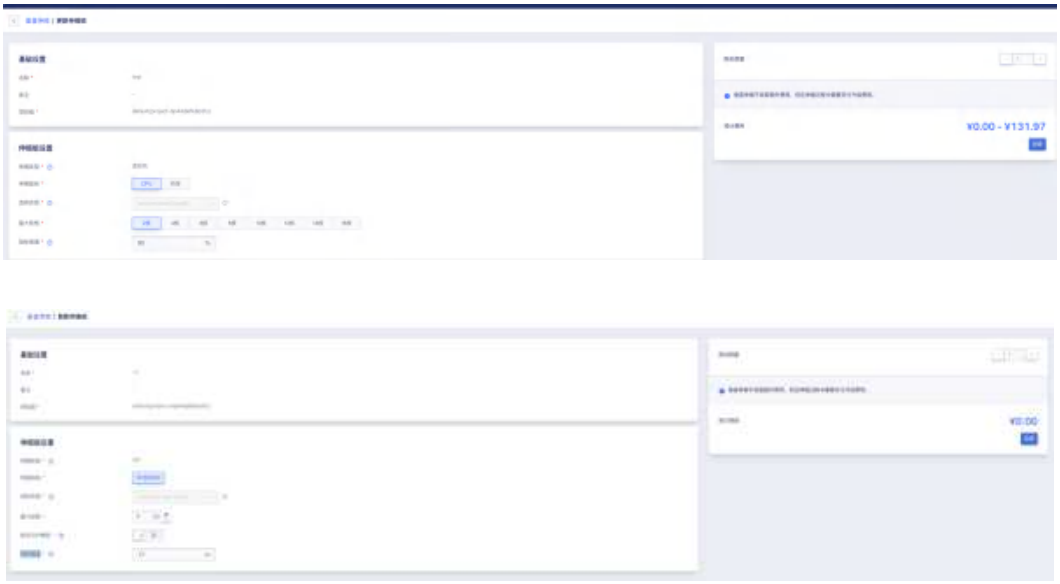
垂直伸缩支持虚拟机和 EIP 两种资源类型的伸缩组设置，其中虚拟机不支持缩容，需要支持热升级。虚拟机伸缩指标包括 CPU、内存；EIP 伸缩指标为带宽使用率。EIP 支持缩容操作。

9.3.4.1 创建垂直伸缩

创建垂直伸缩，基础设置包括名称，备注，项目组，标签，伸缩组设置包括伸缩类型，伸缩指标，选择资源，最大规格，指标阈值。

9.3.4.2 更新垂直伸缩

更新伸缩组，虚拟机类型支持更新伸缩指标，最大规格，指标阈值，最大规格不得小于当前虚拟机规格。EIP 类型支持更新最大规格，是否允许缩容，指标阈值。



9.3.4.3 查看垂直伸缩详情

展示垂直伸缩组的基本信息，伸缩组设置，监控信息及事件。

9.4 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，以邮件的方式给予通知及预警；同时监控告警服务实时为用户提供资源告警状态，让用户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，租户对虚拟机、云硬盘、EIP 、负载均衡、NAT 网关、弹性伸缩、VPN 网关，对象存储，文件存储等资源指定的监控指标数据进行完整挖掘；管理员可对节点、计算集群、存储集群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、持续时间、重要程度、通知组及选择对比方式，可通过设置告警持续时间，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，可通过告警记录查询实时告警信息，以判断故障的发生时间和重要程度。

9.4.1 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。

平台为租户构建的虚拟机、弹性 EIP 、负载均衡、NAT 网关、弹性伸缩、VPN 网关、对象存储、文件存储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、GPU 使用率、GPU 总显存、GPU 显存使用量、GPU 总消耗、GPU 平均功耗、GPU 温度；
- 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。
- 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。
- 对象存储监控图表：通过对象存储服务详情页面的监控信息可查看，包括 CPU 使用率、内存使用率、对象数量、存储容量、当前存储量、存储容量使用率、存储总写吞吐、存储总读吞吐。
- 文件存储监控图表：通过文件存储详情页面的监控信息可查看，包括 CPU 使用率、内存使用率、存储容量、当前存储量、存储容量使用率、存储总写吞吐、存储总读吞吐。

平台为管理员的节点、计算集群、存储集群提供多种监控指标的实时监控图表，并可按照用户的需求对告警模版进行配置，用于阈值超标的时给予告警和通知。

- 节点监控图表：通过节点详情页面的监控信息可查看，包括 CPU 使用率、内存使用率、GPU 使用率。
- 计算集群监控图表：通过计算集群详情页面的监控信息可查看，包括 CPU 分配率、内存分配率、GPU 分配率。
- 存储集群监控图表：通过存储集群详情页面的监控信息可查看，包括存储分配率。

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 小时及自定义时间的监控数据及图表信息。

9.4.2 监控告警模板

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联系人。

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，涵盖：虚拟机、弹性网卡、外网弹性 IP、NAT 网关、负载均衡 、VPN 网关、对象存储、裸金属、数据库等；
- 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指标、对比方式、告警阈值、持续时间、重要程度及通知组；
- 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，支持邮件的通知方式。

9.4.2.1 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“监控告警”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：

- 模版类型：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，对象存储、文件存储及 VPN 网关等，一个告警模板仅支持一种资源类型；

- 模板名称/描述：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。

9.4.2.2 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。

9.4.2.2.1 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：

- 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。

9.4.2.2.2 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：

- 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：；
- 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：。

9.4.2.3 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。

9.4.2.4 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。

9.4.2.5 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。

9.4.2.5.1 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指标、对比方式、告警阈值、持续时间、触重要程度及通知组参数，如图所示：

- 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>=、<=、>、<：
  - 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；
  - 当选择>时，即代表监控数据大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；
- 持续时间：监控指标数据触发阈值持续的时间，持续时间内均达到告警阈值才会触发告警；
- 重要程度：用户可根据业务需要在创建告警规则时选择合适的等级，分为一般、重要、危险三种，在告警记录中可根据重要程度进行记录的筛

选；

- 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。

9.4.2.5.2 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，列表信息包括监控指标、对比方式、告警阈值、持续时间、重要程度、通知组及操作项，如下图所示：

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。

9.4.2.5.3 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。

9.4.2.5.4 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。

9.4.2.5.5 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、模版名称、模版 ID，如下图所示：

9.4.3 告警记录

告警记录是指当前账户所有告警记录及信息，通过告警记录实时的历史告警信息：

如上图所示，告警记录列表信息包括告警的指标说明、目标 ID、模版类型、标签、当前值、状态、重要程度及告警时间：

- 指标说明：触发当前告警记录的资源监控指标项，即数据来源；
- 模版类型：触发当前告警记录的资源类型及资源；
- 标签：显示磁盘空间使用率指标的数据盘信息；
- 目标 ID：告警模版监控的资源 ID；
- 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；
- 状态：告警记录的当前状态，分为触发中、待触发、未触发，可根据需求进行状态的筛选；

- 重要程度：根据监控规则显示当前告警记录的重要程度，包含危险、重要、一般，可根据需求进行告警记录的筛选；
- 告警时间：触发告警规则的具体时间。

9.5 通知组

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,webhook 地址的记录，将不同资源告警通过以上两种方式通知给通知人，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，webhook 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。

9.5.1 创建通知组

用户可通过控制台左侧导航栏进入“运维与管理”模块，切换至“通知组”页面通过通知组管理页面的“创建通知组”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：

通知组名称：当前需要创建的通知组名称及标识；

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。

9.5.2 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名称进入详情页面，用于查看通知组的详细信息及通知人的管理。

9.5.2.1 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，列表信息包括名称、ID 及对单个通知组的操作项，如下图所示：

- 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。

9.5.2.2 通知组详情

通过通知组列表的 ID 进入通知组详情页面，可查看当前基础通知的基本信息，如下图所示：

- **基础通知信息**

包括通知人名称、通知人邮箱以及创建、更新、删除操作；选择 Webhook

按键进入 webhook 通知人详情页面，可查看当前 webhook 通知的基本信息，并可通过通知人管理进行通知联系人的管理，如下图所示：

- **Webhook 通知信息**

包括通知人名称、请求方法、请求地址、创建时间、更新时间以及创建、更新、删除操作；

- **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。

9.5.3 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。

9.5.4 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：

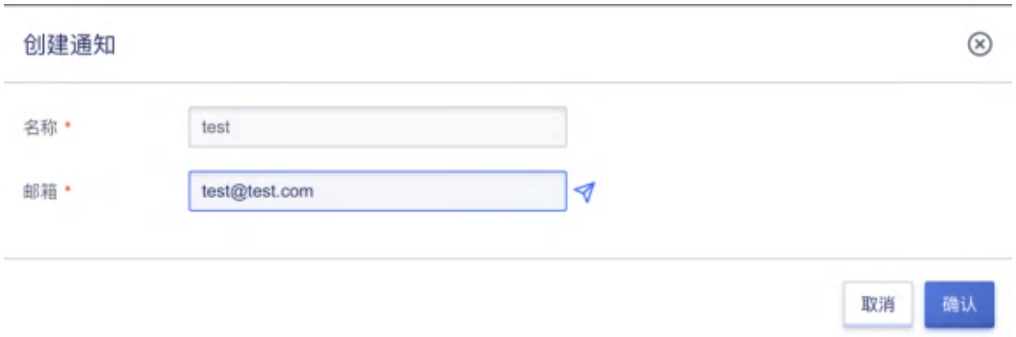
9.5.5 通知人管理

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、邮箱或者 webhook 地址等信息。每个通知组可添加 1 个或多个通知人，在资源发生告警时会通过所设置的通知方式至所有通知人。

9.5.5.1 创建通知人

用户可通过通知组基础通知页面和 webhook 页面的“创建”功能进行通知人的添加，创建通知人时需更具不同通知方式添加相应参数，如下图所示：

（1）基础通知创建示意



- 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；

（2）Webhook 通知创建示意

- 通知人名称：指当前需要创建的联系人姓名或昵称；
- 请求方式：发送的警告信息请求方式，可选 get 和 post(钉钉不支持 get 的请求方式)
- 请求地址：从相应产品的群机器人设置中获取，具体设置方式可参考以下文档:
  - 钉钉 https://open.dingtalk.com/document/robots/custom-robot-access
  - 飞书 https://www.feishu.cn/hc/zh-CN/articles/360024984973

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。

9.5.5.2 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。

9.5.5.3 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。

9.6 操作日志

9.6.1 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。

租户通过操作日志控制台可查看整个平台属于用户所有的资源操作及平台登录登出审计日志等，同时也可通过 API 查询租户内所有资源的操作日志及审计信息。支持查看 1 小时及自定义时间的日志信息，最长可查询 6 个月的操作日志信息。具体信息包括操作（API）名称、所属模块、地域、关联资源、操作者、操作结果、备注及操作时间，如下图所示：

- 操作（API）名称：指操作日志的操作名称，包括调用 API 的接口名称及操作的界面展示名称，如调整带宽。
- 所属模块：指操作日志操作的资源类型，包括裸金属、虚拟机、虚拟机模板、镜像、VPC、云硬盘、弹性网卡、外网 IP、安全组、负载均衡、NAT 网关、VPN 网关、自动伸缩、监控告警模板、定时器、账户等。
- 可以切换地域，查看不同地域下的日志信息
- 关联资源：操作日志对应的资源标识符，并可查看一个操作中所有关联

的资源标识，如绑定弹性 IP 对应的虚拟机 ID 和外网 IP 的 ID。

- 操作者：操作日志对应的操作者，可追溯到具体的主账号和子账号。
- 操作结果：操作日志的结果，如操作成功、操作失败、参数异常、存储集群物理资源不足等。
- 备注：操作日志的备注信息。
- 操作时间：操作日志的操作时间。

为方便用户便捷的查看操作审计日志，控制台支持日志的筛选和搜索检索，同时支持对导出用户的操作审计日志为本地 Excel 表格，方便账户管理和运营。

操作日志查询筛选功能可支持所属模块、操作状态及查询时间范围等纬度。所属模块支持所有产品模块的筛选，同时支持查看全部资源的日志及审计信息，即不对所属模块进行筛选；操作状态支持状态为成功、失败的日志筛选，同时也支持查看全部状态的日志和审计信息；查询时间范围支持 1 小时及自定义时间的日志筛选，最长可查询半年的操作日志。

注意：操作日志不记录用户在虚拟机内部进行的操作和审计。

9.6.2 通知规则

通过创建通知规则，对资源事件进行监控并通过邮件通知通知人，可通过选择监控地域、通知组、监控模块及监控级别设置通知规则，资源事件符合通知规则要求时，会发送监控邮件到通知组内的成员。

9.6.2.1 创建通知规则

用户可通过通知规则页面的“创建”按钮创建通知规则，创建通知规则时需指定监控地域、通知组、监控模块及监控级别。如下图所示：

- 监控地域：通知规则的地域信息。
- 通知组：邮件通知的通知组信息，仅支持选择一个通知组。
- 监控模块：监控的资源模块内容，例如虚拟机、云硬盘，支持选择多个模块。
- 监控级别：操作日志的操作结果，包括操作成功、操作失败，支持多选。

9.6.2.2 查看通知规则

支持用户查看账号下的通知规则信息，包括监控地域、通知组、监控模块及监控级别，如下图所示：

9.6.2.3 更新通知规则

支持用户更新账号下的通知规则，包括监控地域、通知组、监控模块及监控级别。如下图所示：

9.6.2.4 删除通知规则

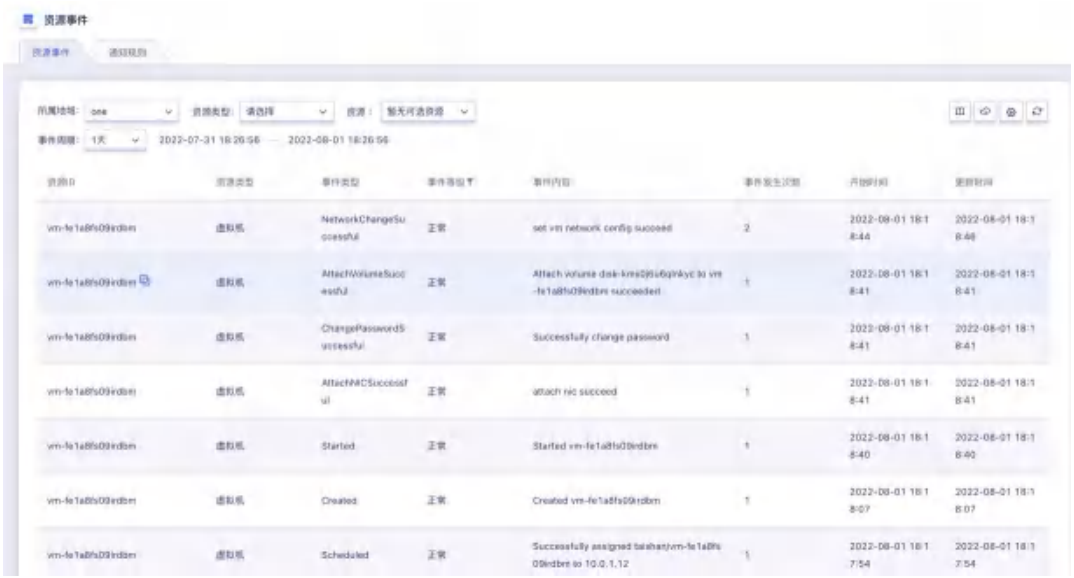
支持用户删除账号下的通知规则，规则删除后即直接销毁，如下图所示：

9.7 资源事件

9.7.1 资源事件管理

资源事件是用于对云平台核心资源的部分操作进行记录及通知，如资源生命周期状态的变化，操作运维执行情况等。资源事件会记录用户在资源类型的部分核心操作事件，提供事件详细记录查询及筛选，并及时通知用户、定位问题。

租户通过资源事件控制台可查看整个平台的资源事件记录信息等，支持根据所属地域、资源类型、资源选择、事件周期进行查询资源事件的详细信息，具体包括资源 ID、资源类型、事件类型、事件等级、事件内容、事件发生次数、开始事件及更新事件，如下图所示：



- 资源 ID：指资源事件监控的资源 ID。
- 资源类型：当前资源事件记录所指定的资源类型。
- 事件类型：事件类型分为生命周期变化事件和操作运维事件，例如虚拟机调度，虚拟机开关机，挂载磁盘等。
- 事件等级：事件等级分为以下几类，正常，警告，错误。
- 事件内容：详细记录触发事件的具体信息。
- 事件发生次数：记录该事件累计触发次数。
- 开始时间：第一次资源事件发现的时间。
- 更新时间：第二次及以后触发资源事件的时间。

为便于用户查看资源事件，控制台支持事件的筛选，同时支持用户导出资源事件为本地 Excel 表格，方便用户查看和定位。资源事件支持查看全部事件信息，即不对所属模块进行筛选；可根据事件等级进行筛选；查询时间范围支持 1 小时及自定义时间的日志筛选。

9.7.2 通知规则

通过创建通知规则，对资源事件进行监控并通过邮件通知通知人，可通过选择监控地域、通知组、监控模块及监控级别设置通知规则，资源事件符合通知规则要求时，会发送监控邮件到通知组内的成员。

9.7.2.1 创建通知规则

用户可通过资源事件的通知规则页面“创建”按钮创建通知规则，创建通知规则时需指定监控地域、通知组、监控模块及监控级别。如下图所示：

- 监控地域：通知规则的地域信息。
- 通知组：邮件通知的通知组信息，仅支持选择一个通知组。
- 监控模块：监控的资源模块内容，如虚拟机。
- 监控级别：对实例正常运行的影响程度进行划分，包括正常、警告、错误，可多选。

9.7.2.2 查看通知规则

支持用户查看账号下的通知规则信息，包括监控地域、通知组、监控模块及监控级别，如下图所示：

9.7.2.3 更新通知规则

支持用户更新账号下的通知规则，包括监控地域、通知组、监控模块及监控级别。如下图所示：

9.7.2.4 删除通知规则

支持用户删除账号下的通知规则，规则删除后即直接销毁，如下图所示：

9.8 定时器

9.8.1 产品简介

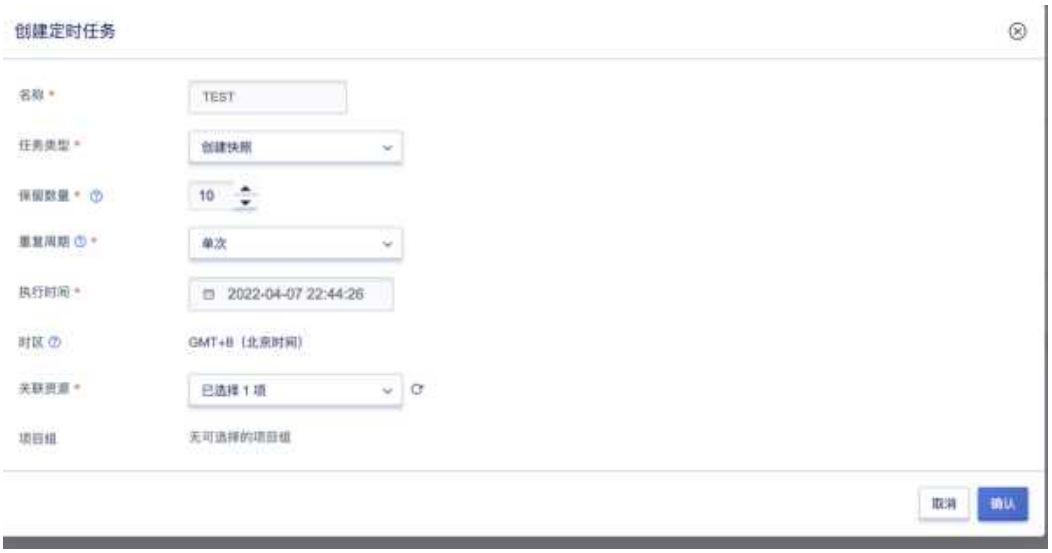
定时器（Scheduler）是平台为用户提供自动化任务功能，可用于定期执行一系列任务的，如创建快照。可在指定的周期重复执行，也可仅执行一次，且每个任务支持多个资源批量操作。

- 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。

平台支持定时器的全生命周期管理，包括创建定时任务、查看定时任务及记录、更新定时任务及删除定时任务。

9.8.2 创建定时任务

用户可通过控制台直接创建一个用于执行创建快照的定时任务，用于云硬盘的备份。创建定时任务时需要指定任务类型、重复周期、执行时间及关联资源，如下图所示：



- 名称：定时任务的名称，用于标识定时任务。
- 任务类型：定时任务的执行动作，当前仅支持创建快照。
- 重复周期：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、间隔的指定时间执行任务：
  - 单次执行：需要指定执行具体时间，24 小时制；默认当天执行，若执行时间已过则为次日执行。
  - 每天执行：需要指定每天执行的整点时间，支持从 0 点到 23 点的 24 个整点，支持每个整点均会执行定时任务。
  - 每周执行：需要指定每次执行的日期和执行时间，支持从周一到周日的 0 点到 23 点，支持周一到周日每天执行每个执行时间进行定时任务的执行。
  - 每月执行：需要指定每次执行的日期和执行时间，支持从 1 号到 31 号或月末的 0 点到 23 点，同时每月的每一天每个执行时间进行定时任务的执行。
  - 间隔：需要指定间隔执行的间隔时间，支持按照间隔时间执行定时任务。
- 执行时间：任务具体执行的时间，根据重复周期不同，执行时间可支持

不同的设置方法。

- 当重复周期为单次执行时，可支持设置日期的具体时、分、秒。
- 当重复周期为每天、每周、每月重复执行时，可支持 0 点到 23 点中每一个整点。
- 当重复周期为间隔时，可支持设置间隔的小时、分钟。

- 时区：默认定时任务的时区东八区时间，即 GMT+8（北京时间）
- 关联资源：即设置需要定时任务执行创建快照的云盘资源，支持虚拟机的系统盘和数据盘，并支持批量选择。

点击确认后，系统将自动生成一条定时任务，并立即检测定时任务的执行计划和时间，如果到达约定的时间即会立即执行定时任务，可通过定时任务的详情中的日志查看具体执行情况。

9.8.3 查看定时任务

9.8.3.1 定时任务列表

用户可通过控制台查看账户内拥有的所有定时任务列表及相关信息，并可通过列表的名称进入定时任务详情查看定时任务的基本信息及任务执行记录，具体列表信息如下图所示：

列表信息包括名称、ID、任务名称、定时器、关联资源、创建时间、更新时间及操作项：

- 名称/ID：当前定时任务的名称及全局唯一标识符。
- 任务名称：当前定时任务的执行动作，当前仅支持创建快照。

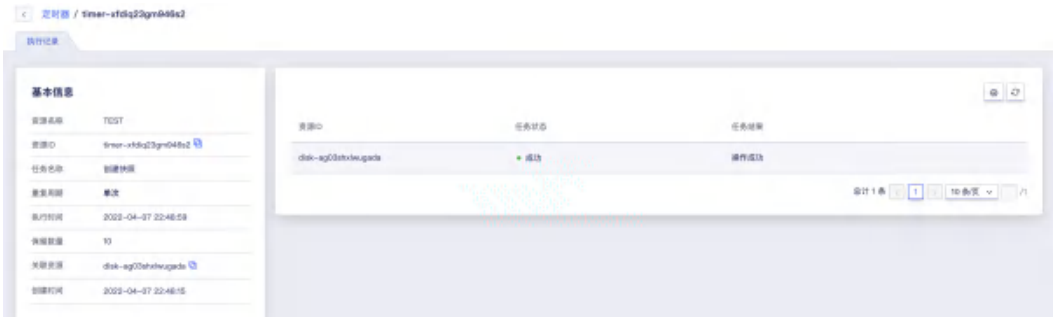
- 定时器：定时任务的执行规则，包括重复周期、执行日期及执行时间，其中执行日期仅在重复执行时有效。
- 关联资源：定时任务执行定时任务时的关联资源，即为关联资源执行创建快照或其它操作。

创建时间/更新时间：定时任务的创建时间和更新时间。

列表上支持对定时任务的更新及删除操作，同时支持对定时任务的批量删除操作；为方便用户管理定时任务的资源，平台支持对定时任务的搜索，支持模糊搜索。

9.8.3.2 定时任务详情

用户可进入定时任务详情查看定时任务的详细信息，包括基本信息及任务执行记录信息，如下图所示：



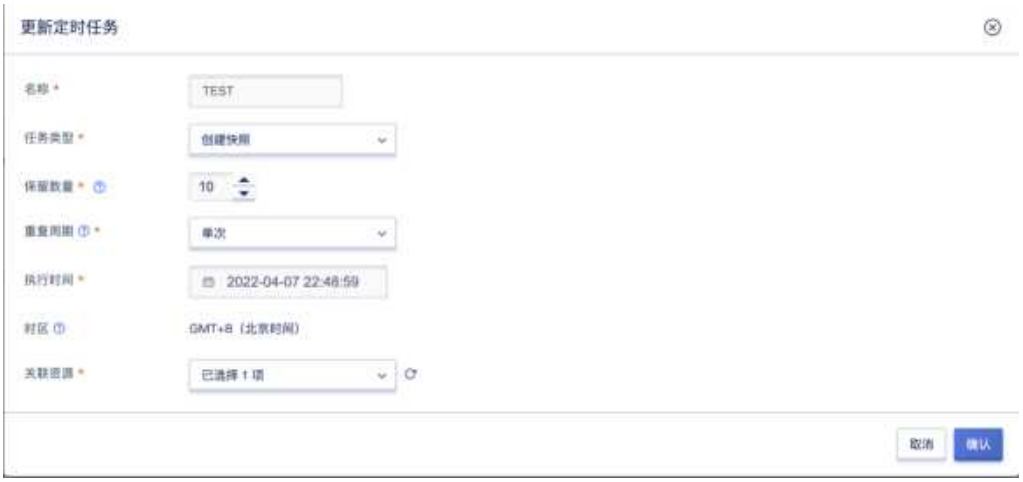
其中基本信息包括名称、ID、任务类型、重复制期、执行时间、关联资源及创建时间，而任务执行日志全面记录当前定时任务的任务执行计划及执行状态，包括资源 ID、开始时间、结束时间、任务状态及任务结果。

- 资源 ID：定时任务执行记录对应的关联资源。
- 开始时间：定时任务执行的开始时间。
- 结束时间：定时任务执行的结束时间。
- 任务状态：当前定时任务的状态，包括成功和失败。
- 任务结果：当前任务的最终资源操作状态，包括操作成功和操作换败。

通过执行记录可进行定时任务的追溯，用于判断任务执行的成功与否。

9.8.4 更新定时任务

用户可在业务需要时对定时任务进行变更，支持变更定时任务的任务类型、重复周期、执行日期、执行时间及关联资源，如下图所示：



定时任务更新后，不影响定时任务已执行的任务，执行新的任务类型时会根据新的定时策略进行操作。

9.8.5 删除定时任务

平台支持用户删除不适合业务场景的定时任务，在任何状态下均可进行删除。如下图所示：

删除定时任务会立即销毁，同时会自动停止定时任务中的执行计划，但不影响其关联或由其创建出来的资源。

9.9 回收站

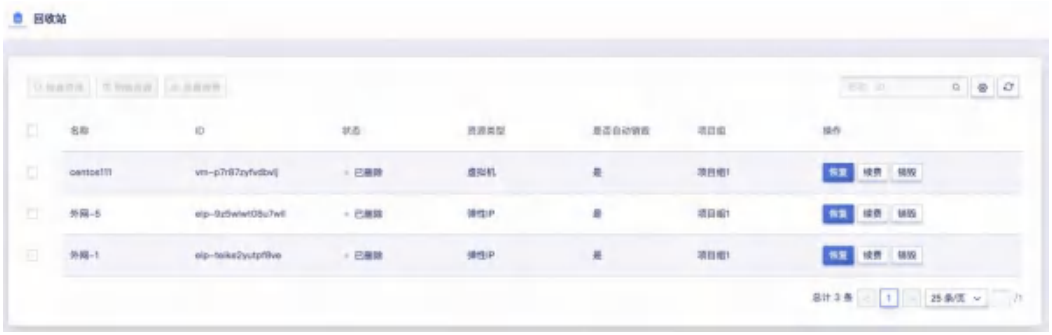
9.9.1 回收站概述

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。

9.9.2 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：



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、预定销毁时间及操作项：

- 资源名称/ID：当前留存资源的名称及全局唯一标识符；
- 状态：当前资源的状态，包括已删除、销毁中；
- 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、批量销毁资源及批量续费资源。其中批量续费资源会按照资湖泊的计费方式自动续费一个周期，如按时计费的资源，则自动续费一个小时；按月购买的资源，则自动续费一个月。

9.9.3 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。

9.9.4 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：

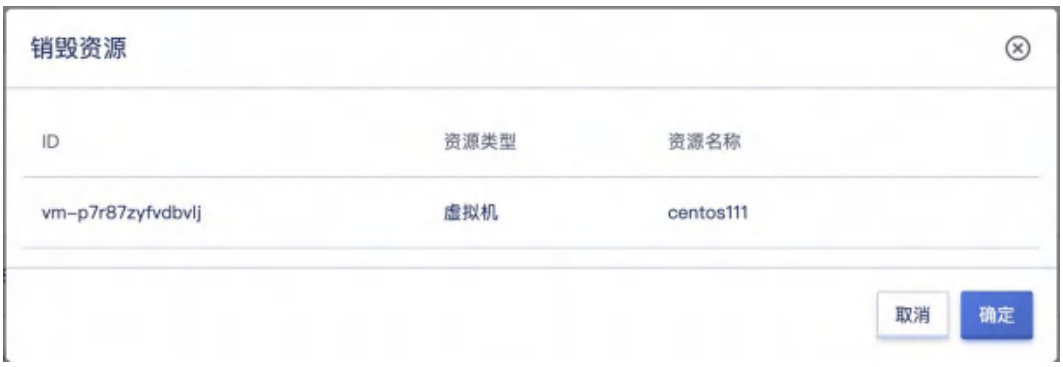
- 资源按按小时计费时：一次续费操作可续费 1 个小时，N 次续费操作即续费 N 个小时；
- 资源按月计费时：一次续费操作可续费 1 个月，N 次续费操作即续费 N 个月；
- 资源按年计费时：一次续费操作可续费 1 年，N 次续费操作即续费 N 年的费用周期。

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。

9.9.5 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。

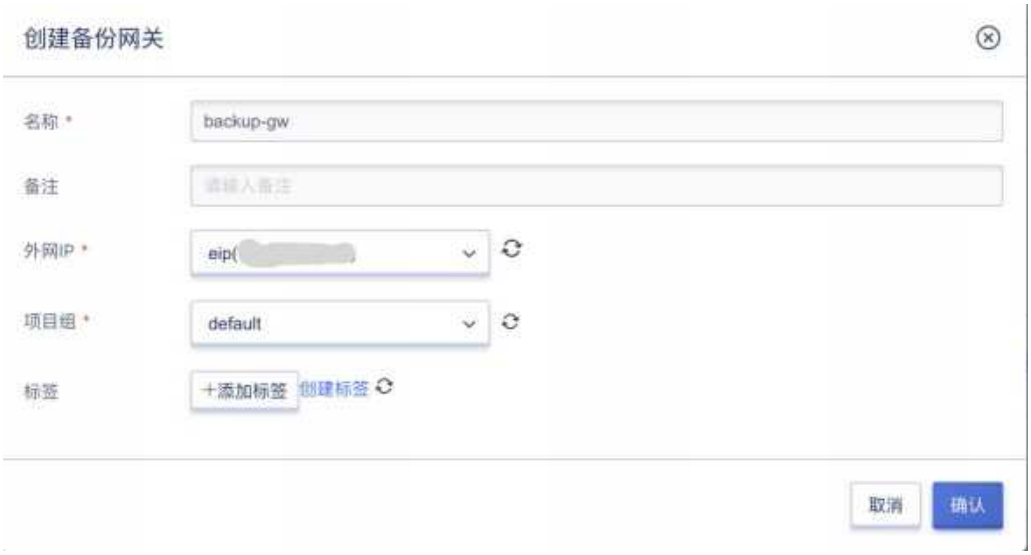
9.10 备份服务

9.10.1 概述

数据库备份服务（Database Backup Service，简称 DBS）是平台为用户提供数据保护的备份服务。支持对 Mysql，Redis，对象存储，文件存储进行定时自动备份和手动备份。Mysql 支持逻辑备份，物理备份，快照备份，增量备份；Redis 支持逻辑备份；对象存储和文件存储支持快照备份。

9.10.2 创建备份网关

平台支持用户创建备份网关操作，备份网关需要绑定外网 IP，用于和外部数据源备份通信，一个租户只支持创建一个备份网关。可通过导航栏进入【备份服务】模块，切换到“备份网关”页面进行操作，如下图所示：



9.10.3 查看备份网关

平台支持用户查看备份网关列表，包括名称、资源 ID、状态、IP 地址/网段、带宽、项目组、标签、操作，如下图所示：

9.10.4 调整备份网关带宽

平台支持用户调整备份网关带宽

9.10.5 修改外网 ip

平台支持用户修改备份网关的外网 IP

9.10.6 删除备份网关

平台支持用户删除备份网关，删除之前，保证存储池列表没有外部 S3 存储池资源

9.10.7 绑定存储池

平台支持用户进行存储池绑定操作，存储类型支持对象存储。可通过导航栏进入【数据库备份】模块，切换到“存储池”页面进行操作，如下图所示：

9.10.8 查看存储池列表

平台支持用户查看存储池列表，包括名称、资源 ID、状态、存储类型、对象存储、关联备份计划、创建时间、更新时间、操作，如下图所示：

9.10.9 更新存储池

平台支持用户对存储池进行更新操作，更新内容包括存储池名称、存储池备注。可通过存储池列表中操作项“更新”按钮进行操作，如下图所示：

9.10.10 解绑存储池

平台支持用户对已绑定存储池进行解绑操作，可通过存储池列表中操作项“解绑”按钮进行操作，如下图所示：

9.10.11 创建备份计划

平台支持用户进行备份计划创建操作，支持指定备份策略、备份源类型、备份资源、存储池、保留时间等信息。可通过导航栏进去【数据库备份】进行操

作，如下图所示：

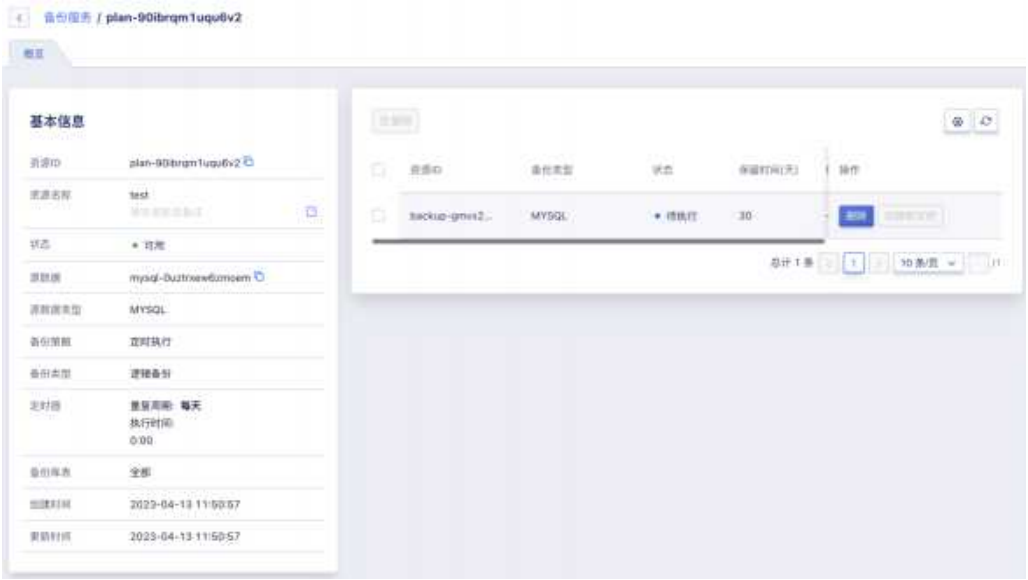
Mysql 支持创建部分库表的备份计划

9.10.12 查看备份计划列表

平台支持用户查看备份计划列表，包括名称、资源 ID、状态、存储池、源数据类型、源数据地域、源数据、备份策略、定时器、备份类型、备份保留时间(天)、创建时间、更新时间、操作。如下图所示：

9.10.13 查看备份计划详情

平台支持用户查看备份计划详情，包括基础信息和备份数据列表。可点击备份计划名称进入详情页。详情页如下图所示：



9.10.14 从备份数据创建实例

平台支持用户从备份计划的可用备份数据创建实例。如下图所示：

9.10.15 删除备份数据

平台支持用户删除备份数据，备份数据恢复中时不允许删除。如下图所示：

9.10.16 更新备份计划

平台支持用户进行备份计划的更新操作，更新内容包括备份计划名称/备注、备份策略、备份源类型、备份资源、重复周期、执行日期、执行时间、存储池、保留时间等。可通过备份计划列表中操作项的“更新”按钮进行操作。

9.10.17 执行备份计划

平台支持用户对备份计划进行执行操作，包括备份策略为定时器和手动备份的备份计划。可通过备份计划列表中操作项的“执行”按钮进行操作，如下图所示：

9.10.18 删除备份计划

平台支持用户对备份计划进行删除操作，可通过备份计划列表中操作项的“删除”按钮进行操作，如下图所示：

备份计划删除成功后，定时器中的备份任务也会被删除。

9.11 开放 API

9.11.1 36.1 概述

云平台 API 接口文档，提供对云平台 API 的调用和参数的解释说明。按照

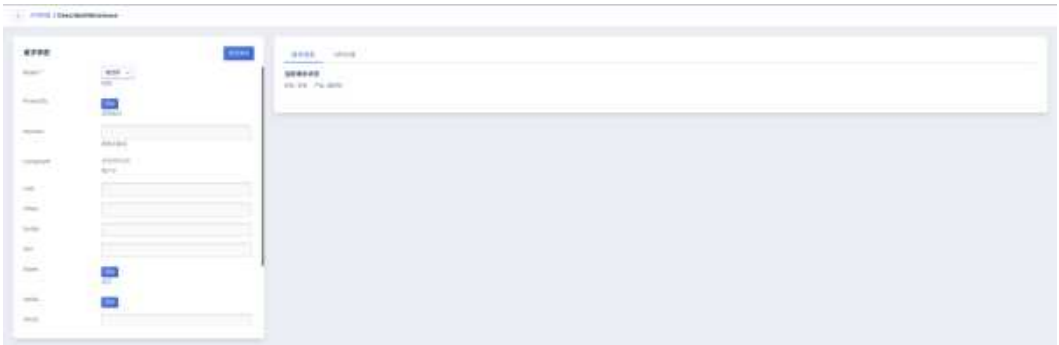
租户权限展示可以调用的 API 列表。租户可以在页面添加请求参数，发送请求对当前账号的线上资源操作，请求发送成功后会在请求信息中展示当前请求状态，请求内容，以及响应结果，在 API 文档中展示响应文档，展示响应值的参数，类型，及对应描述。

9.11.2 查看 API 列表

在开发 API 列表中，租户可以按照产品模块查看对应产品子模块的 API 列表，例如下图所示，计算产品，虚拟机的相关 API 信息。支持按照 API 名称和描述进行模糊搜索。

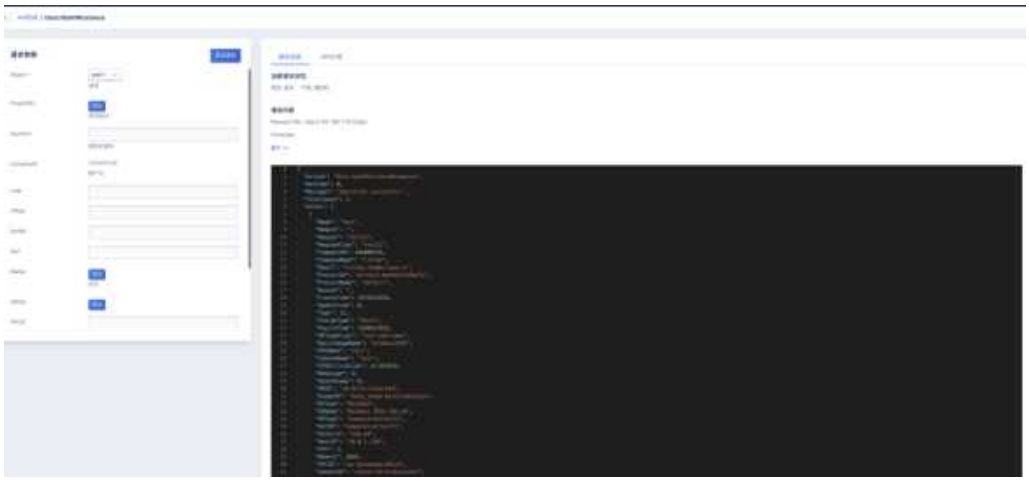
9.11.3 查看 API 详情

点击 API 操作栏“详情”按钮，跳转至 API 详情页，如下图所示:



9.11.4 发送请求

添加请求参数后点击发送请求，返回请求信息，包含当前请求状态，请求内容，响应信息，如下图所示:



9.11.5 查看 API 文档

API 文档中展示响应文档，包含参数名，类型，描述。如下图所示：

请求信息 API文档

响应文档

参数名	类型	描述
TotalCount	int	
Infos	VMInfo[]	

IPInfo

参数名	类型	描述
IPID	string	
SGName	string	
IPVersion	string	
ISDefaultGW	int	
IsElastic	string	
IsVIP	string	
Type	string	
SGID	string	
IP	string	
NicType	string	
InterfaceID	string	
MAC	string	

10 运营管理

10.1 账号管理

10.1.1 概述

组织和账号管理主要为企业用户提供组织架构管理，支持多租户模式，每个租户可代表一个组织/公司/子公司/部门。概念解释如下：

- **租户**

平台支持多租户模式，用于有多级组织架构的企业，可将租户作为一个单独的公司/子公司/部门进行运营，有效实现权限管理，除低总公司、子公司及不同部门资源混用可能造成的风险，并可实现资源审计。

租户是平台中一组资源的集合，提供资源隔离、子账号、权限控制、配额及价格配置等能力。不同租户间资源通过 VPC 网络及权限实现强隔离；租户内所有主账号和子账号的资源、费用、配额及审批均归属于租户。

- **账号**

主账号：一个租户默认有一个主账号，主账号即为租户下的初始管理人员，默认有租户下所有资源的管理权限以及组织管理权限。主账号可通过创建子账号，并管理子账号的权限。

子账号：子账号是主账号创建的用户，子账号在租户下的权限由主账号控制。一个租户可拥有多个子账号，支持对子账号进行资源管理的权限控制。

- 人员

企业中的人员，人员需要使用账号登录云平台使用资源。

- 角色

权限的集合，为用户和成员组赋予权限可获得调用相关 API 进行资源操作的能力。

- 项目组

以项目组为维度进行资源规划，可为一个具体项目或者业务建立独立的资源池，实现资源更细粒度地管理。同时针对子账号的授权也是基于项目组维度进行授权。项目组只是逻辑上面的分组，不具有资源隔离的作用，租户所有资源均需要属于某个项目组。

- 流程审批

为满足企业对核心云资源，如虚拟机、云硬盘、外网 IP 等资源使用的管控需求所引入的云资源工单审批流程。

- 审批管理

审批管理仅平台管理员 admin 可以进行操作。

10.1.2 我的账号

10.1.2.1 账号信息

可在账号和组织/我的账号页面可以查看账号基本信息并进行账号安全设置。

账号基本信息包括账号 ID、角色 ID、账号名称、账户邮箱、外部充值余额、平台充值余额及创建时间等信息。

- 账号 ID：当前登录平台账号的唯一标识 ID ；
- 账号名称：当前登录平台账号的账号名称或昵称，可直接通过编辑按钮进行修改，支持中文、英文或字符；
- 账号邮箱：当前登录平台账号的邮箱地址；
- 外部充值余额：指通过支付宝、微信、银行及新浪支付充值的金额；
- 平台充值余额：平台的增金，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。

账号安全是平台为用户账号提供的安全防护功能，可通过定期修改登录密码、

开启双子因验证登录保护，设置访问限制以保证登录账号的安全。对于需要调用 API 用户，云平台可为开发者提供 API 公钥和私钥信息，可通过复制密钥信息用于操作 API 指令，具体操作方式可参考 API 开发者手册。

10.1.2.2 修改登录密码

平台支持用户修改账号登录密码，可在我的账号页面对密码进行修改。

修改密码需要验证旧密码，若忘记旧密码，可联系管理员在后台帮助修改密码。

10.1.2.3 登录保护

10.1.2.3.1 开通登录保护

平台提供基于 TOTP（Time-Based One-Time Password Algorithm）的免费登录二次认证服务，开通本服务后，账号登录控制台均需通过授权认证，支持国密硬件版和普通软件版，用户可根据需要通过部署进行配置。开通登录保护的前提条件如下：

（1）开通对象为独立主账号或子账号；

（2）移动设备上安装有 FortiToken 或其他基于 TOTP 技术的令牌工具；

（3）推荐使用 FortiToken。

点击下一步，国密硬件版需输入 SN 信息，不可为空：

普通软件版显示如下：

为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

10.1.2.3.2 开通步骤

1. 登录控制台并进入账号与组织管理页面，在我的账号页面，可查看当前登录保护设置。未设置情况下，可点击“设置”按钮开启登录保护。
2. 检查移动设备上是否安装 FortiToken：

- 页面提供 IOS 和 Android 用户工具下载地址，若您未安装 FortiToken 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 FortiToken。

3. 打开 FortiToken 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。

10.1.2.3.3 关闭登录保护

登录控制台并进入账号与组织管理页面，在我的账户页面，可查看当前登录保护设置。已设置情况下，如果需要关闭登录保护设置，可点击“设置”按钮。按照页面提示获取并输入授权码即可关闭二次认证功能。

10.1.2.3.4 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认证码，系统判断认证码有效后，即可成功登录平台。

10.1.2.3.5 登录保护 FAQ

Q：如何下载 FortiToken？

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 FortiToken 身份认证器。

Q：FortiToken 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 FortiToken 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，如微信小程序“二次验证码”等，为安全起见，推荐使用谷歌官方“FortiToken”。

10.1.2.4 登录访问限制

为进一步保障账号安全，平台提供登录访问限制能力，可为租户设置可登录控制台和访问平台 API 的客户端 API 地址。配置后租户下的所有账号只能从指定的 IP 登录或发起 API 访问，有效保证账户登录及资源的安全性。

- 支持配置多个 IP 地址或 IP 地址段，多个 IP 地址/段间使用英文逗号

进行分隔。

- 配置的 IP 地址 或 IP 地址段为白名单模式，即配置的 IP 地址/段客户端才可正常登录控制台或访问 API 。
- 默认不指定任何 IP ，代表不限制登录控制台和访问 API 的客户端 IP 地址，即默认全网可访问登录控制台。

如果出现登录 IP 地址设置错误，导致租户下所有账号均无法登录时，可联系平台管理员通过管理控制台侧修改租户的登录访问限制策略。

可通过【账号安全】中“登录访问限制”功能进行登录策略配置，如下图所示，默认为空代表全网无限制。

可在登录访问范围内输入可登录平台的 IP 地址或 IP 地址段，点击确认即可生效。配置成功后，用户使用账号在未指定的 IP 网络中无法正常登录控制台，并提示当前的 IP 地址，如下图所示：

平台仅可限制访问控制台的 IP 地址，即直接请求到控制台 URL 地址的客户端 IP 地址，如用户访问平台的客户端地址在 NAT 路由内，则平台配置登录策略时，需要放通 NAT 后的 IP 地址，即需要将 NAT 后的出口地址配置在登录访问策略的白名单中，保证 NAT 路由器内的客户端均可正常访问控制台。

10.1.2.5 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。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。

10.1.2.6 数字证书验证

10.1.3 查看租户配额

可在账号和组织/配额信息页面查看租户下配额限制以及配额当前使用情况。

配额（quota）是一个租户在单个地域下可创建的云资源上限。通过限制每个账户拥有的资源配额，可合理分配云平台资源，提升资源利用率的同时，满足云平台上每一个账号的资源需求。租户初始化时，在每个数据中心都拥有默认配额。同时，云平台管理员可自定义每个租户的资源配额。

对于虚拟机、云硬盘、外网 IP 删除或未续费进入回收站的资源，不占租户资源配置，恢复资源时会检查资源配额。

租户下的每个人员在使用账号创建资源时，创建数量或容量的上限不能够超过租户下配额上限。如租户中云硬盘的配额为 10 ，则主账号和子账号可创建的云硬盘数量上限不可超过 10 个。可以分地域查看每个地域下的配额信息，配额列表的字段如下：

（1）产品类型和资源类型：

- 虚拟机：虚拟机（资源数量）
- 虚拟机：虚拟机（CPU 数量）
- 虚拟机：虚拟机（内存大小）
- VPC：VPC（资源数量）
- VPC：子网（资源数量）
- 镜像：镜像（资源数量）
- 云硬盘：云硬盘（资源数量）
- 云硬盘：云硬盘（磁盘空间）
- 网卡：弹性网卡（资源数量）
- 外网 IP：弹性 IP（资源数量）
- 负载均衡：负载均衡（资源数量）

- 负载均衡：SSL 证书（资源数量）
- 虚拟机模板：虚拟机模板（资源数量）
- NAT 网关：NAT 网关资源数量）
- 安全组：安全组（资源数量）
- 对象存储：对象存储（资源数量）
- 文件存储：文件存储（资源数量）
- VPN 网关：VPN 网关（资源数量）
- VPN 网关：对端网关（资源数量）
- VPN 网关：隧道（资源数量）
- 弹性伸缩：伸缩组（资源数量）
- 弹性伸缩：伸缩策略（资源数量）
- VIP：VIP（资源数量）

（2）配额

当前配额项在指定地域下可创建的资源数量或资源容量；

（3）更新时间

当前配额项的修改更新时间。

10.2 账号权限管理

10.2.1 概述

在账号和组织管理/项目组管理页面，可对项目组进行查看和管理。项目组可以帮助进行资源分组管理，帮助解决资源的精细化管理以及授权管理等复杂性问题。

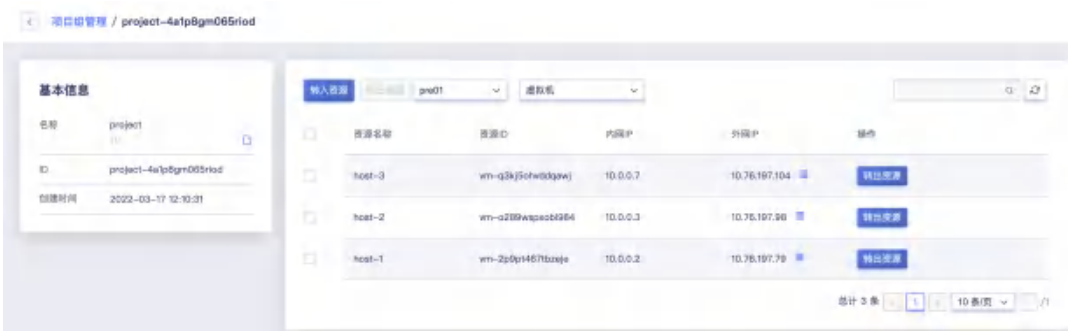
租户所有资源均需要属于某个项目组，分组的资源根据用户的角色授权决定

用户是否对组中资源具有权限。

10.2.2 项目组管理

支持对项目组进行资源管理，通过转入转出资源来管理项目组下的资源。转入资源到项目组时，可以选择不在当前项目组下的所有资源，可以在资源列表处查看到资源所属项目组。

转出资源到其他项目组时，只能够指定当前项目组下的资源，且转出到的项目组只能够时其他项目组。资源被转出到其他项目组后，有该项目组授权的用户将无法再查看和管理此资源。



资源转入/转出时以产品类型为维度，一次可以转入/转出同一产品类型下的多个资源。VPN 网关、负载均衡、伸缩组中有多个维度的资源，请在转入转出时注意将关联资源分配到同一组内。

- 支持修改项目组名称和备注。
- 支持删除项目组，当项目组中存在资源时，无法删除项目组，需要将资源转移到其他项目组。

项目组下存在角色授权时，需要先移除角色授权后，才能够删除项目组。

10.2.3 角色管理

在账号和组织管理/角色管理页面可查看和管理租户下所有的角色。角色分为两种类型，系统内置角色和自定义角色。

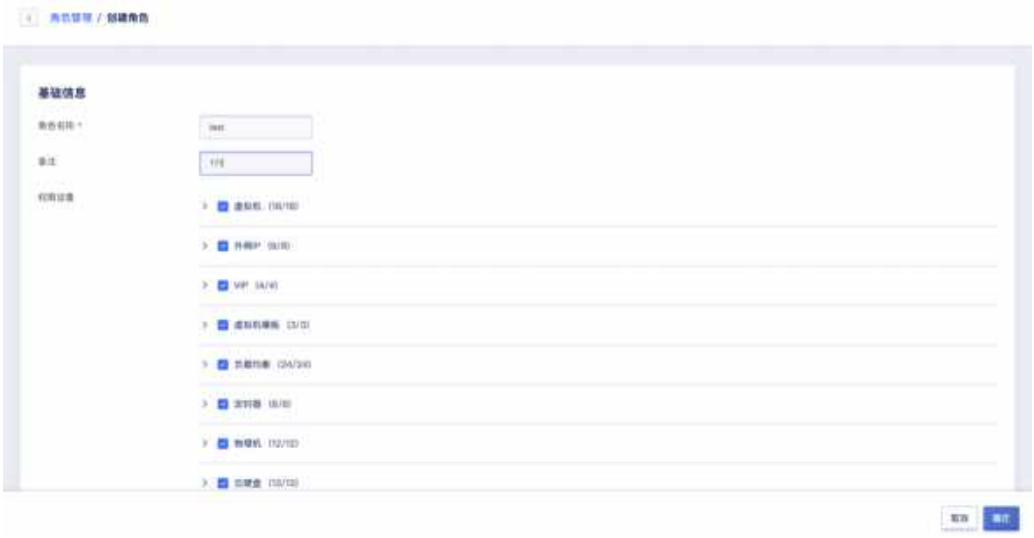
系统内置角色是平台提供给用户，以快速授权的角色给子账号，不能够编辑和删除。目前内置角色包括管理员和只读用户：

- 管理员：此角色中包含了租户下所有云资源操作和组织管理操作的授权。如果您不需要对子账号进行精细地权限管理，可直接使用系统管理员为子账号进行角色授权，更快捷地进行操作。
- 只读用户 此角色仅包含所有资源和组织管理功能的查看权限。

10.2.3.1 创建角色

可通过创建角色创建出一个自定义角色，创建角色时需要输入以下信息：名称：为角色设置合适的名称。备注：可选项权限设置：可分产品类型，按照查看、增加、编辑、删除的四个维度授权每个产品的操作权限，也可以根据实际使用需求，只勾选某几项权限。

创建角色时，系统默认勾选的操作，为各个模块必须要授权上的操作，建议不要取消，避免影响授权的完整性。如果您不需要为用户授权某个模块的权限，可以取消默认勾选的操作。



10.2.3.2 管理角色

可对角色进行编辑、修改名称和备注、删除、查看角色详情以及查看角色的授权记录。

点击进入详情页面，查看和更新角色的权限集合，可以更新每个产品类别

下的任意权限的授权。

更新角色授权的权限集合后，用此角色授权的用户，在授权范围下的权限也会更新。

10.2.4 人员管理

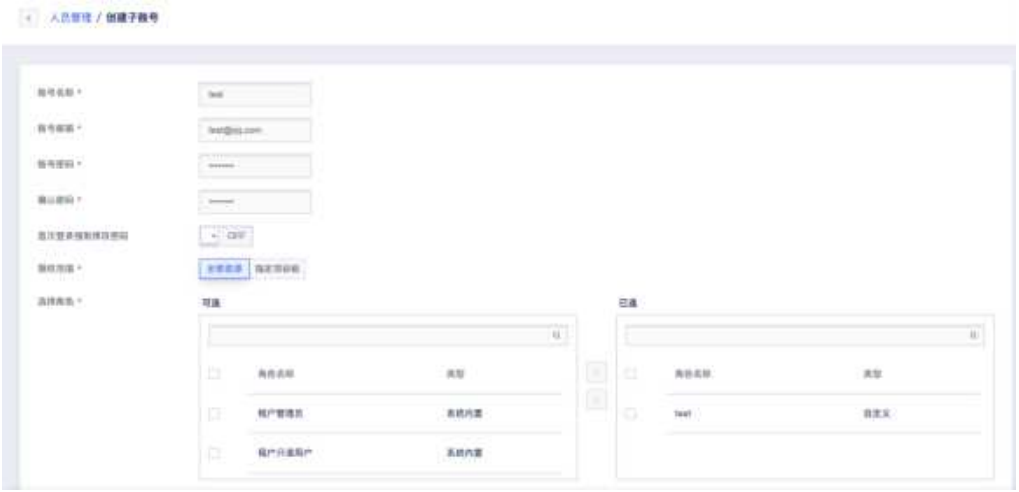
支持通过人员管理对租户下所有账号进行管理，建议谨慎地创建和管理组织下的账号，并为账号添加上适当的角色授权，防止权限扩大化，导致资源管理的混乱，影响企业 IT 资源使用的安全。

10.2.4.1 创建子账号

具有子账号创建权限的账号，可以在账号和组织管理/人员管理页面创建子账号。创建子账号需要输入以下参数：

- 账户名称:为账户指定一个具有标志性的名称
- 邮箱：账户的电子邮件地址，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 6-64 个字符。
- 首次登录强制修改密码：可设置账号首次登录是否需要强制修改密码。

- 授权范围：可以选择可子账号授权所有项目组资源/指定项目组资源。当资源没有项目组时
- 角色：为子账号在授权范围下授权合适的角色，支持同时授权多个角色，最后生效的权限为多个角色所允许操作的集合。



创建子账号前，建议先通过项目组对资源进行编组，并配置好子账号需要授权的角色。如果不需要授权自定义角色，可直接使用系统内置角色。

用户使用子账号登录后，可以正常查看一切操作，在进行相关操作时，会提示“权限不足”。比如一个用户未被授权查看虚拟机的权限，则在虚拟机列表处看到如下提示。

10.2.4.2 查看账号列表

可在人员管理界面查看租户下所有账号列表和详情信息。租户下默认有一个主账号，可以有多个子账号。列表参数如下：

- 账号 ID：当前账号在云平台全局的唯一标识符；
- 账号名称：当前账号的名称；
- 邮箱：当前账号的登录邮箱地址；
- 类型：标识账号为主账号还是子账号
- 状态：当前账号的状态，包括使用中、冻结中、删除中：
- 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；
- 操作项：对单个账号的操作项，包括查看详情、冻结和解冻、添加角色授权、删除

10.2.4.3 子账号详情

子账号详情页面可查看基本信息和角色授权记录，并管理子账号的角色授权

- 基本信息：当前子账号的基本信息，包括 ID、角色、账号邮箱及创建时间、更新时间；
- 角色管理：可管理子账号的角色授权，包括添加新的角色授权和移除已有的授权角色。

10.2.4.4 冻结账号

冻结账号是指将一个账号进行锁定，冻结后将不允许登录控制台。仅支持状态为“使用中”的账号进行冻结操作，用户可点击账号列表操作项中的“冻结”对

账号进行冻结。

平台管理员可对租户进行冻结，冻结后主账号和所有子账号都被冻结。

10.2.4.5 解冻账号

解冻账户是指解冻一个已冻结的账号，被成功解冻的的用户，可登录管理控制台。

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”对子账号进行解冻。

10.2.4.6 删除账号

可对账户进行删除，删除账号后用户无法再使用此账号密码登录平台。删除后，可以再使用账号邮箱在平台注册或者创建新的账号。

10.3 计费管理

10.3.1 概述

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、续费及过期回收等订单管理操作，同时基于基于账户提供充值、扣费等交易管理。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；

按年按月按时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 文件存储、对象存储、外网网卡、NAT 网关、VPN 网关、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，当账户余额不足时，可通过云平台管理员进行充值。

10.3.2 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：

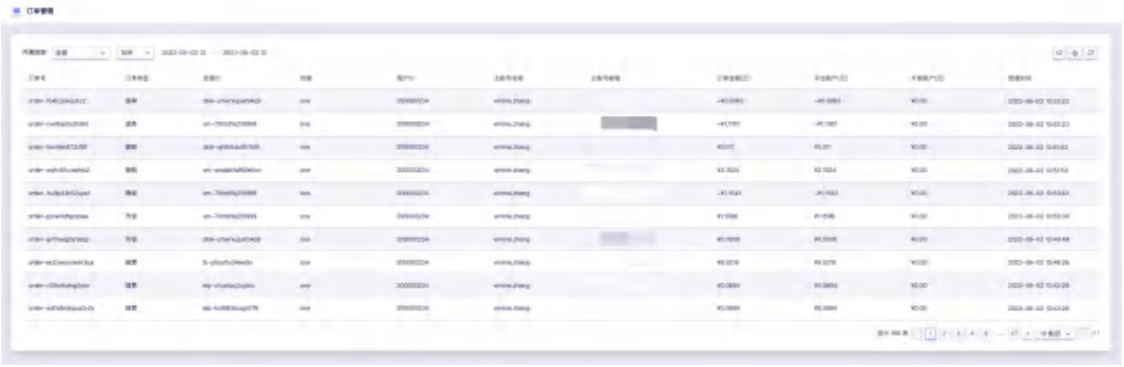
- 计价器中付费方式支持用户选择时、月、年，分别代表按时计费、按月计费、按年计费，其中选择月和年时，可以选择购买的月份数量和年份数量。
  - 月份可选择 1 ~ 11 ，分别代表 1 个月或 11 个月；
  - 年份可选择 1~ 5 ，分别代表 1 年或 5 年；
- 合计费用指当前订单中所有计费资源一个计费周期的费用合计，如一个虚拟机订单中，包括指定的 CPU 内存、云盘(若有)、EIP(若有)等资源按照付费方式的费用合计。

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，点击立即购买提示“租户的账号余额不足”，需要先对账号进行充值，才可进行购买和创建资源操作。

10.3.3 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，支持查看某个地域、 1 天、3 天、 7 天、14 天、30 天及自定义时间的历史订单记录。对资源进行创建、续费、变更配置或删除时，会分别产生新购、续费、升级、降级及退单等类型订单，如下图所示：



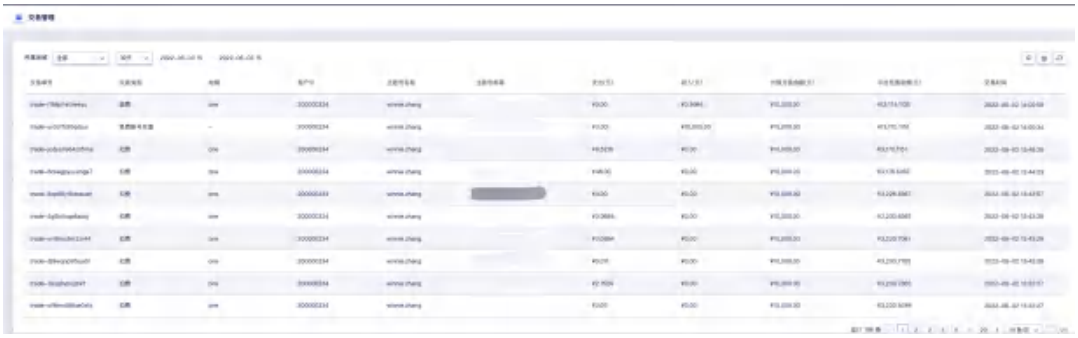
- 订单号：指当前订单的全局唯一标识符；
- 订单类型：当前订单的类型，包括新购、续费、升级、降级及退单五种类型；
  - 新购是指用户新创建的计费资源，包括虚拟机、云硬盘、弹性 IP、 外网网卡、文件存储、对象存储、NAT 网关、NAT 网关及负载均衡等；
  - 续费是指预付费资源每一个计费周期续费时产生的订单，包括手动续费和系统自动续费；
  - 升级是指按时按月按年计费的资源变更配置时产生的续费订单，如升级带宽、升级虚拟机配置等；
  - 降级是指按时按月按年计费的资源变更配置时产生的续费订单，如降级带宽、降级虚拟机配置等；
- 资源 ID ：产生当前订单的资源标识符；

- 地域：当前订单资源所在的区域；
- 订单金额：当前订单金额，即订单在新购、续费、升级所付的费用及退单、降级所退的费用（退费展示为负值）；
- 平台账户：当前订单平台账户支付的金额；
- 外部账户：当前订单外部账户支付的金额；
- 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。

10.3.4 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，支持查看某个地域、 1 天、3 天、 7 天、14 天、30 天及自定义时间的历史交易记录，如下图：



- 交易单号：当前交易记录在全局唯一的 ID 标识符，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、扣费和退费：
  - 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生命周期的计费操作，如创建资源时，进行扣费操作；

- 退费指系统针对每个资源生命周期的计费操作，如删除资源时，进行退费操作；

- 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，充值显示为 0.00 ；
- 收入：当前交易记录进账的金融，当交易类型为充值和退费时有效，扣费显示为 0.00 ；
- 外部充值余额：当前账户在当前交易记录发生后的外部充值余额；
- 平台充值余额：当前账户在当前交易记录发生后的内部充值余额；
- 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。

10.3.5 账单管理

账单管理包括账单总览、资源账单、账单明细。其中，账单总览可以查看费用趋势以及本月账单汇总，资源账单与账单明细支持筛选导出功能。

10.3.5.1 账单总览

租户可通过导航栏进入账单管理控制台，查看账单总览。账单总览包括费用趋势与本月账单汇总两个模块。

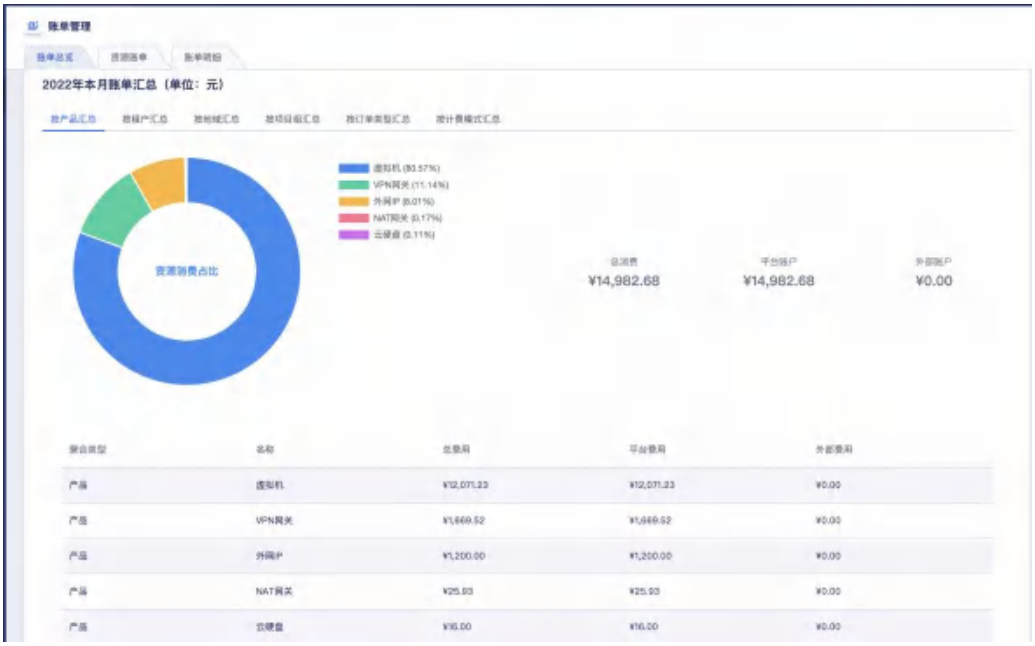
10.3.5.2 费用趋势

租户可在帐号总览页面查看费用趋势，可通过自定义费用类型查看云平台在近六个月内产生的交易信息，如下图所示：

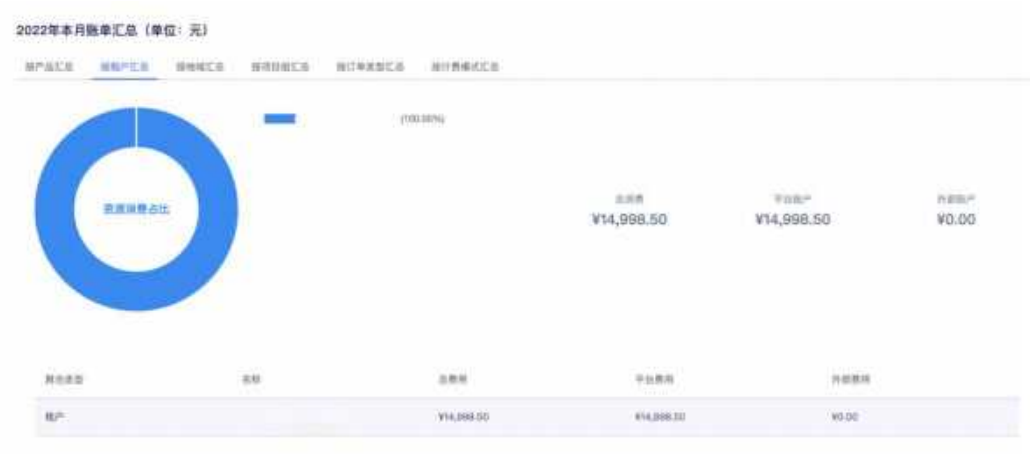
10.3.5.3 本月账单汇总

本月账单汇总从按产品汇总、按租户汇总、按地域汇总、按项目组汇总、按订单类型汇总及按计费模式汇总六个方面用饼图展示，列表包括聚合类型、名称、总费用、平台费用及外部费用。

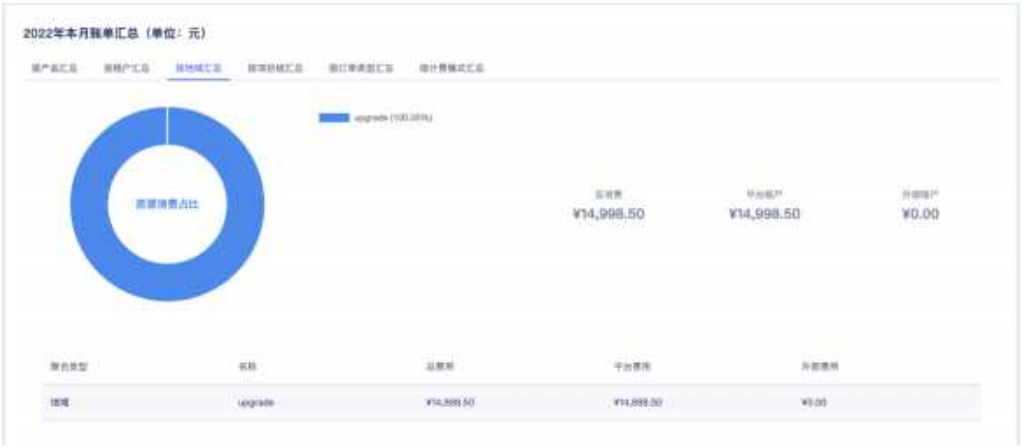
（1）按产品汇总



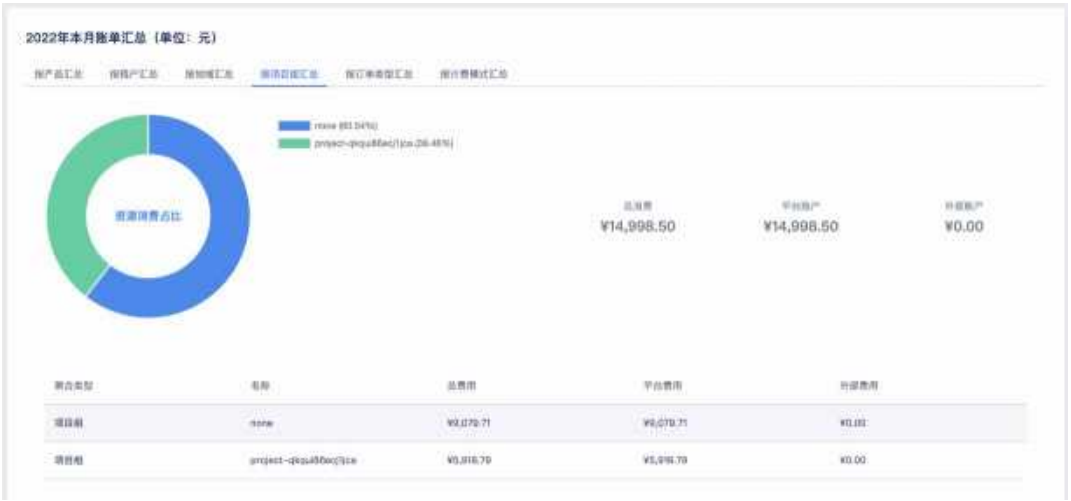
（2）按租户汇总



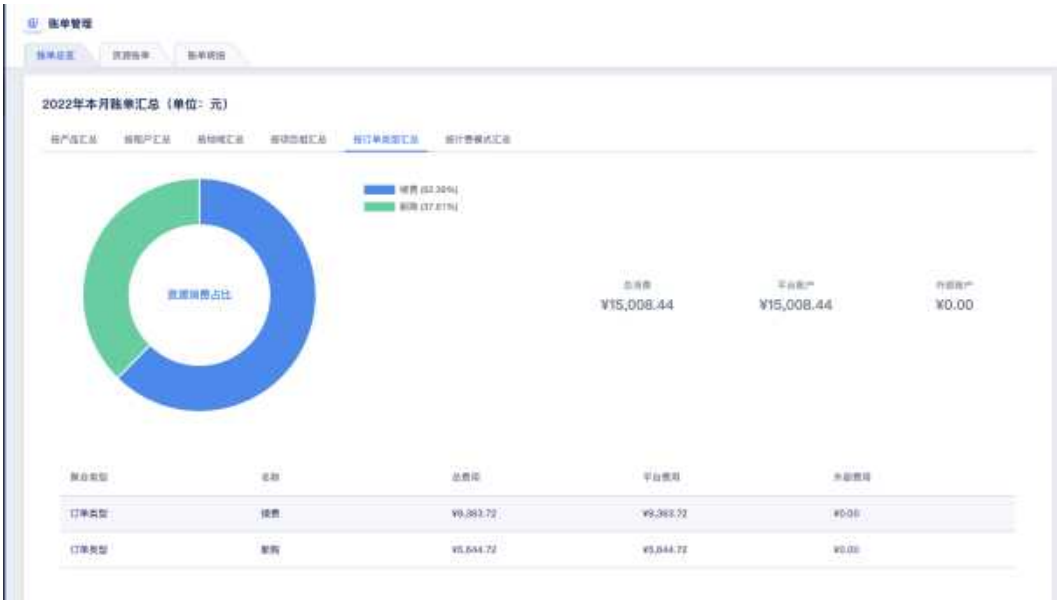
（3）按地域汇总



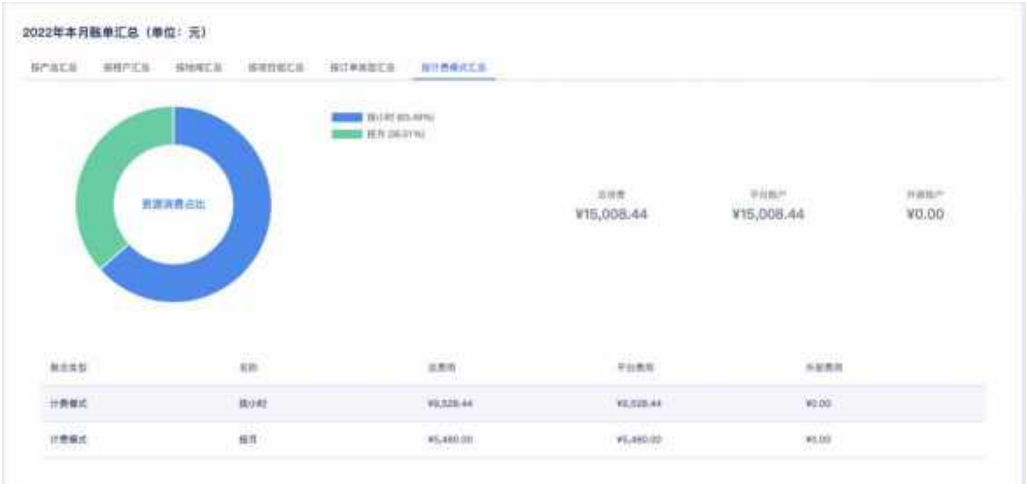
（4）按项目汇总



（4）按订单类型



（4）按计费模式汇总



10.3.5.4 资源账单

租户可从账单周期/所属产品/计费模式/所属地域/所属项目五个维度查看云平台的资源账单信息，列表包括资源 ID、地域、租户 ID、主账号名称、主账号邮箱、所属产品、所属项目、计费模式、总费用、平台账户、外部账户及交易时间，如下图所示：

- 资源 ID：账单的全局唯一标识符
- 地域：资源所在的地域信息
- 租户 ID：产生订单的租户信息
- 主账号名称：充值的租户下的主账号名称
- 主账号邮箱：充值的主账号邮箱
- 所属产品：云平台的产品，包括虚拟机、云硬盘、外网 IP、VPN 网关、负载均衡、NAT 网关、网卡
- 所属项目：本次交易资源所绑定的项目
- 计费模式：按小时、月、年的计费模式
- 总费用：本次交易的总费用
- 平台账户：本次交易消费平台账户的金额
- 外部账户：本次交易消费外部账户的金额
- 交易时间：本次交易产生的时间

10.3.5.5 导出资源账单

平台支持租户从账单周期、所属产品、计费模式、所属地域、所属项目五个维度筛选资源账单，并导出到本地 Excel 文件，为便平台运营管理和报表统计，如下图所示：

10.3.5.6 账单明细

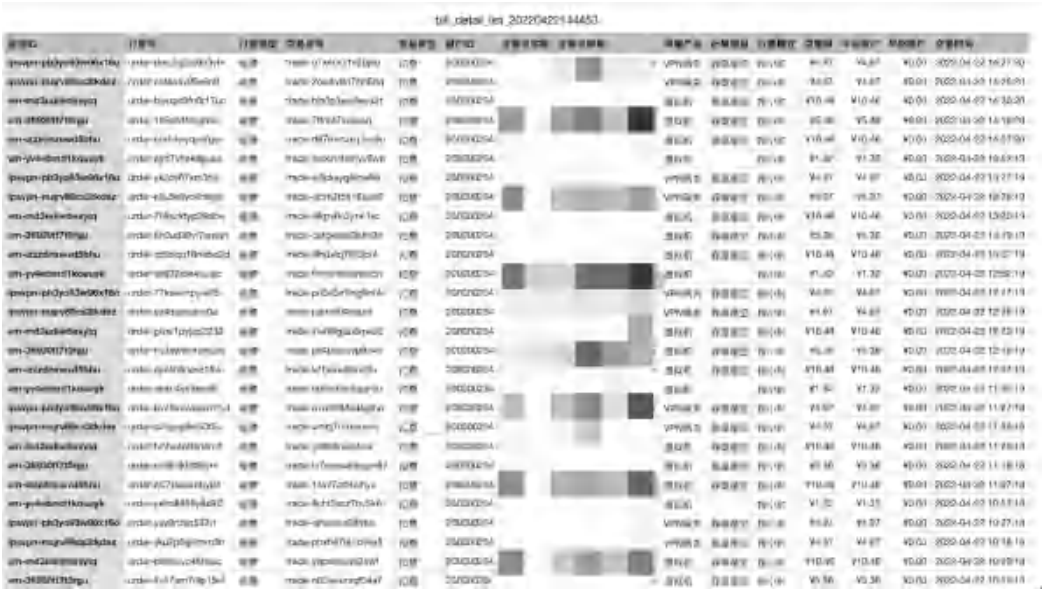
租户可从账单周期/所属产品/订单类型/计费模式/所属地域/所属项目六个维度查看云平台的账单明细，列表包括资源 ID、交易单号、交易类型、订单号、订单类型、地域、租户 ID、主账号名称、主账号邮箱、所属产品、所属项目、计费模式、总费用、平台账户、外部账户及交易时间，如下图所示：

- 资源 ID：账单的全局唯一标识符
- 交易单号：交易记录在云平台的唯一标识
- 交易类型：账户充值和扣费均会生成一次交易记录，因此交易类型包括账户余额充值、免费账户充值及扣费
- 订单号：订单在云平台的唯一标识符
- 订单类型：包括升级和新购两种
- 地域：资源所在的地域信息
- 租户 ID：产生订单的租户信息
- 主账号名称：充值的租户下的主账号名称
- 主账号邮箱：充值的主账号邮箱
- 所属产品：云平台的产品，包括虚拟机、云硬盘、外网 IP、VPN 网关、负载均衡、NAT 网关、网卡
- 所属项目：本次交易资源所绑定的项目
- 计费模式：按小时、月、年的计费模式
- 总费用：本次交易的总费用

- 平台账户：本次交易消费平台账户的金额
- 外部账户：本次交易消费外部账户的金额
- 交易时间：本次交易产生的时间

10.3.5.7 导出账单明细

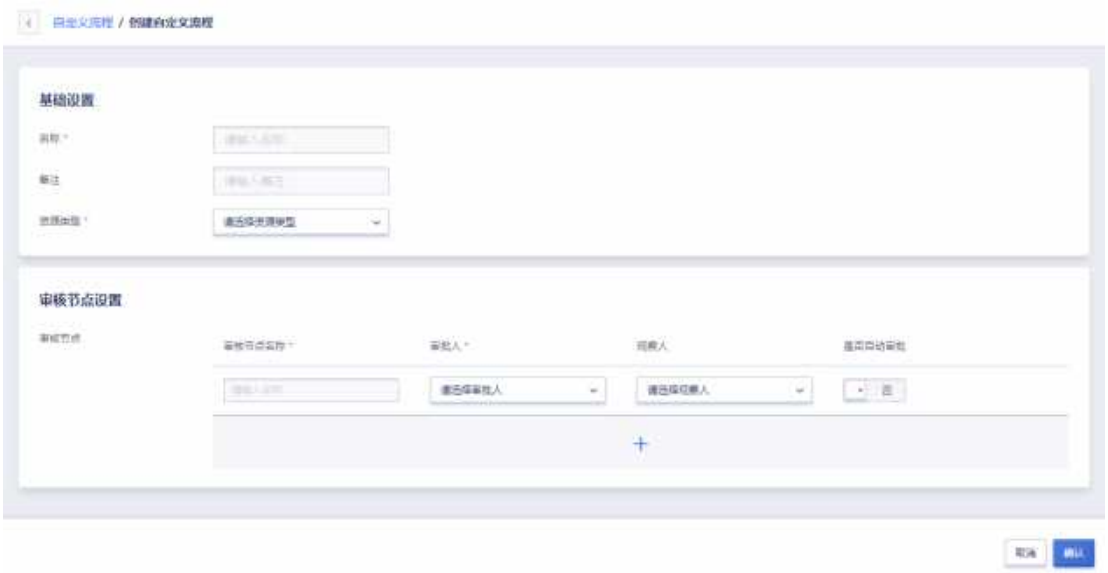
平台支持租户从账单周期、所属产品、订单类型、计费模式、所属地域、所属项目六个维度筛选账单明细，并导出到本地 Excel 文件，为便平台运营管理和报表统计，如下图所示：



10.4 自定义流程

平台支持云租户自定义流程，不同类型的资源都能创建和定义创建流程；租户主账号可以创建流程，并将流程分配给子账号，分配后，该租户以及旗下所有子账户创建资源时，都会走该流程；删除流程后，用户申请资源，将不再提交申请。

10.4.1 租户创建自定义流程



名称：审批流程的名称

- 备注：审批流程的备注
- 资源类型：审批流程的资源类型，包括虚拟机、云硬盘、文件存储、对象存储、Redis、MySQL、VPC 网络、外网 IP 、VIP、网卡、NET 网关、VPN 网关、负载均衡、资源模版、伸缩组
- 审核节点：审批流程的节点信息
  - 审核节点名称：审批流程节点的名称
  - 审批人：节点的审批人，包含当前租户及旗下子用户
  - 观察人：节点的观察人，包含当前租户及旗下子用户
  - 是否自动审批：是否自定审批该节点，包括手动审批、自定审批

10.4.2 自定义流程列表

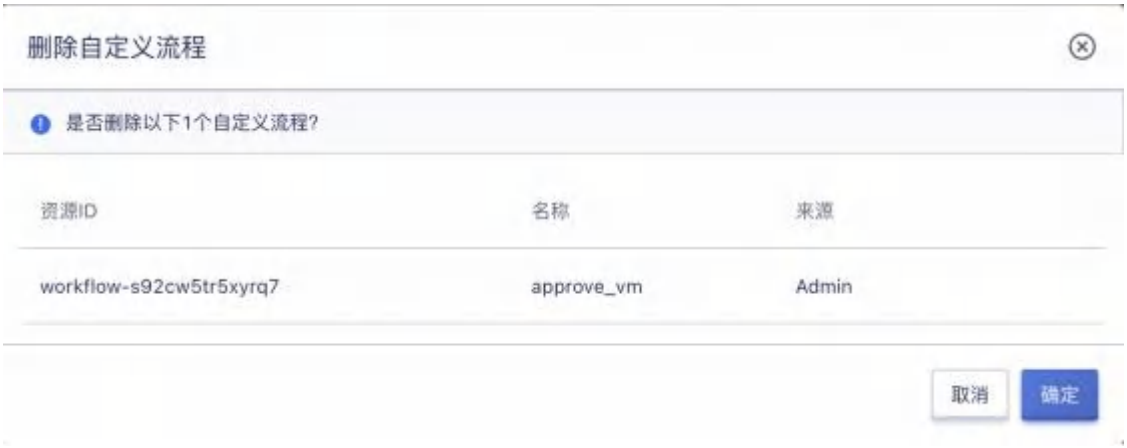
- 名称：自定义流程的名称
- 资源 ID：自定义流程的 ID
- 资源类型：自定义流程的资源类型，包括虚拟机、云硬盘、文件存储、对象存储、Redis、MySQL、VPC 网络、外网 IP 、VIP、网卡、NET 网关、VPN 网关、负载均衡、资源模版、伸缩组
- 来源：自定义流程的创建来源，包括管理员、租户
- 创建时间：自定义流程的创建时间
- 更新时间：自定义流程的更新时间
- 操作：修改、删除自定义流程，管理员可以操作所有自定义流程，租户只能操作自己创建的自定义流程

10.4.3 修改自定义流程

- 名称：审批流程的名称
- 备注：审批流程的备注
- 资源类型：审批流程的资源类型，包括虚拟机、云硬盘、文件存储、对象存储、Redis、MySQL、VPC 网络、外网 IP 、VIP、网卡、NET 网关、VPN 网关、负载均衡、资源模版、伸缩组
- 审核节点：审批流程的节点信息
  - 审核节点名称：审批流程节点的名称
  - 审批人：节点的审批人，来源为管理员时：包含管理员、所属租户及旗下子用户；来源为租户时：包含所属租户及旗下子用户
  - 观察人：节点的观察人，来源为管理员时：包含管理员、所属租户及旗下子用户；来源为租户时：包含所属租户及旗下子用户
  - 是否自动审批：是否自定审批该节点，包括手动审批、自定审批

10.4.4 删除自定义流程

支持删除流程，当流程被删除后，租户创建相关资源不再需要提交申请。



10.5 审批流程

10.5.1 概述

随着信息化数字转型在政企、教育、金融、制造等行业的实践和应用，企业对资源管理的标准化、流程化管理需求日益旺盛，对于云化资源同样需要设置标准的审批流程，满足平台资源的申请、审批的业务使用流程的需求。

针对企业云化资源的管理，云平台为为企业管理者提供的自助模式的资源审批服务，用于制定信息系统云化资源的标准使用流程，在租户或子账号需要使用或管理资源时，按照流程中定义的审批人和审批层级完成审批后，由平台自动化交付用户需要业务资源。

平台审批流程由平台管理员进行定义和发布，并由平台管理者设置是否为一个租户设置开通审批流程，支持手动审批和自动审批。

- 手动审批：租户下主账号和子账号进行虚拟资源操作时需要走申请、审批流程，待审批通过后，平台会自动为用户创建或操作所需资源，并生一条审批记录用于追溯。
- 自动审批：租户下主账和子账号进行虚拟资源操作无需人工介入，系统将自动审批通过，并自动生成一条审批记录用于保留相关申请记录和审批记录。

开通资源审批的前提是设置审批流程，用于定义租户申请资源时，需要多少

层级的审批，每一层级由谁进行审批，所有层级均通过后才可进行资源的创建和变更操作。为满足企业多种场景的审批业务，平台内置默认审批流程。

默认审批流程提供简单的审批逻辑，仅支持 1 级审批，当平台管理者为租户开启资源审批流程后，租户及子账号下资源的创建及变更申请统一由【平台管理员】进行审批，即平台管理员审批通过后，平台将自动执行资源的变更操作。

审批流程支持多种资源的变更操作，包括虚拟机、云硬盘、VPC 网络、外网 IP 及负载均衡 ，支持的变更如下：

- 虚拟机：创建虚拟机、修改配置、扩容系统盘、扩容数据盘；
- 云硬盘：创建云硬盘、扩容磁盘；
- VPC 网络：创建 VPC ；
- 外网 IP：创建外网 IP、调整带宽；
- 负载均衡：创建负载均衡。

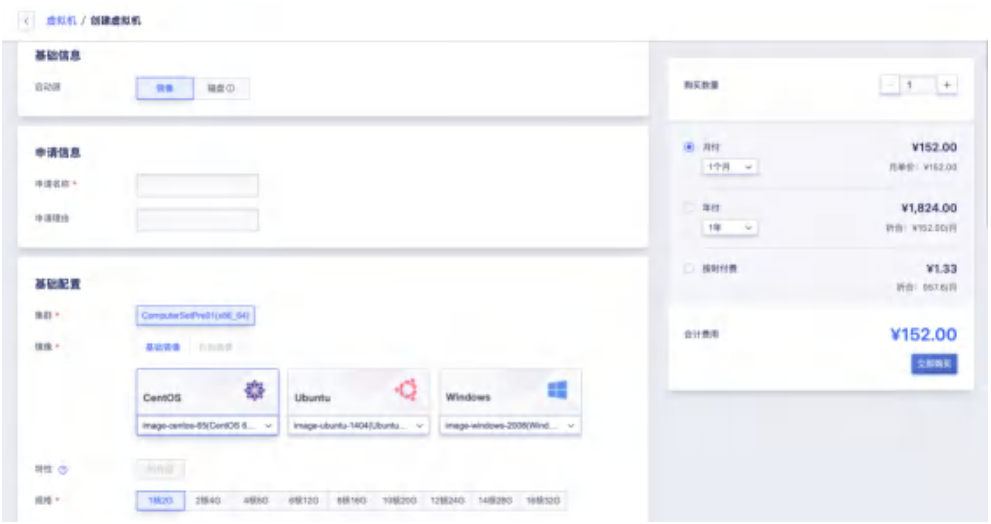
10.5.2 审批使用流程

本文以申请虚拟机为示例描述手工审批的使用流程：

(1) **前置条件：管理员为租户开启审批流程。**

(2) 申请入口：创建虚拟机。

- 进入虚拟机控制台，通过【创建虚拟机】进入虚拟机创建引导页面，如下图所示：



- 填写申请名称和申请备注，按照虚拟机的创建要求输入其它必填信息，点击【立即购买】提交申请。
- 提交申请后，页面会自动跳转至【申请管理】页面，并在申请列表中自动新增一条待审批的申请记录。

(3) 管理员审批：由平台管理员 admin 账号进行审批。

- 若平台管理员通过申请，则申请状态变更为【已申请】，并会自动执行虚拟机的创建操作，可通过虚拟机列表查看正在创建的虚拟机资源，待资源创建成功后，申请状态变更为【成功】。
- 若平台管理员拒绝申请，则申请状态变更为【已拒绝】，申请的资源变更将不被执行，可联系平台管理员或查看审批备注了解拒绝原因。

10.5.3 申请管理

租户在对资源进行变更并提交申请后，可通过申请管理控制台查看申请记录及申请状态。

10.5.3.1 查看申请列表

用户通过我的申请列表可查看租户下所有已提交的申请记录，包括手工审批和自动审批的所有记录。如下图所示：

- 申请名称：本次申请的名称。
- 资源类型：本次申请的资源类型，包括虚拟机、硬盘、VPC、外网 IP、负载均衡等五类资源。
- 操作：针对资源的操作。比如创建虚拟机，创建 VPC 。
- 账号邮箱：申请人的账号邮箱。
- 账号 ID：申请人的账号 ID 。
- 状态：申请的状态，包括处理中、成功、失败。
- 当前节点：申请的当前节点，快速了解申请的进展。
- 当前处理人：申请的当前处理人，默认流程均为平台管理员。
- 创建日期：本次资源变更的申请时间。

10.5.3.2 查看申请详情

用户通过申请记录右侧“详情”按钮可进入申请的概览页面。在此页面可查看申请信息、申请涉及到的资源的信息、申请的处理记录、申请的关联资源。

（1）申请信息

描述本次申请的详细信息，如申请名称、申请资源类型、申请的变更操作及申请的状态及时间。

（2）关联资源

描述本次申请的关联资源信息。管理员审批通过的申请记录会存在关联资源，被拒绝的申请将不执行资源操作，不会产生关联资源信息。

（3）资源信息

代表本次申请时提交的资源变更具体配置信息，如申请创建虚拟机时的规格、VPC 网络、镜像等，同时包括资源的申请时的计费信息。

（4）处理记录

当前申请记录的处理记录，并可查看所有处理节点的流程节点、处理人、备注及处理时间。

- 流程节点：指当前申请记录所使用的审批流程的所有节点，如平台默认的审批流程包括提交申请、默认审核节点、资源操作等。
- 处理人：指每一个流程节点的处理人，如提交申请人的邮件地址为 cinder.lv@ucloud.cn ，默认审核节点的处理人为 admin@ucloud.cn 。

- 备注：指每一流程节点的备注，如平台管理员通过或拒绝申请时给予的说明。
- 处理时间：指每一个流程节点人的处理时间。

有关租户审批流程开通、变更及平台管理者审批管理，可参考平台管理员手册中【审批流程】章节。

