技术白皮书

产品版本：ZStack 3.10.0

文档版本：V3.10.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴科技商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受云轴科技公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，云轴科技公司对本文档内容不做任何明示或暗示的声明或保证。

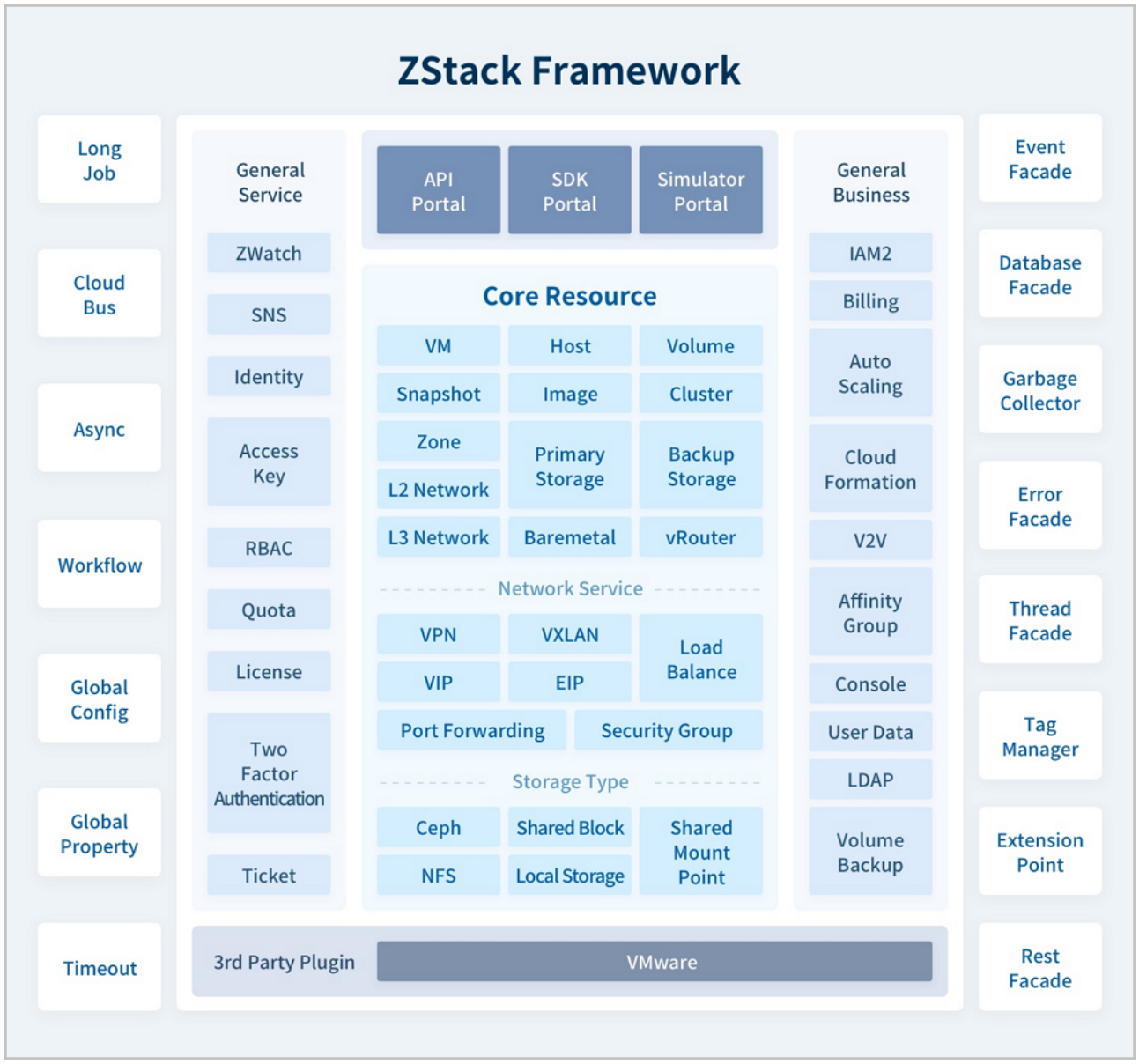
由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目录

1 产品概述

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

图 1: 系统架构示意图

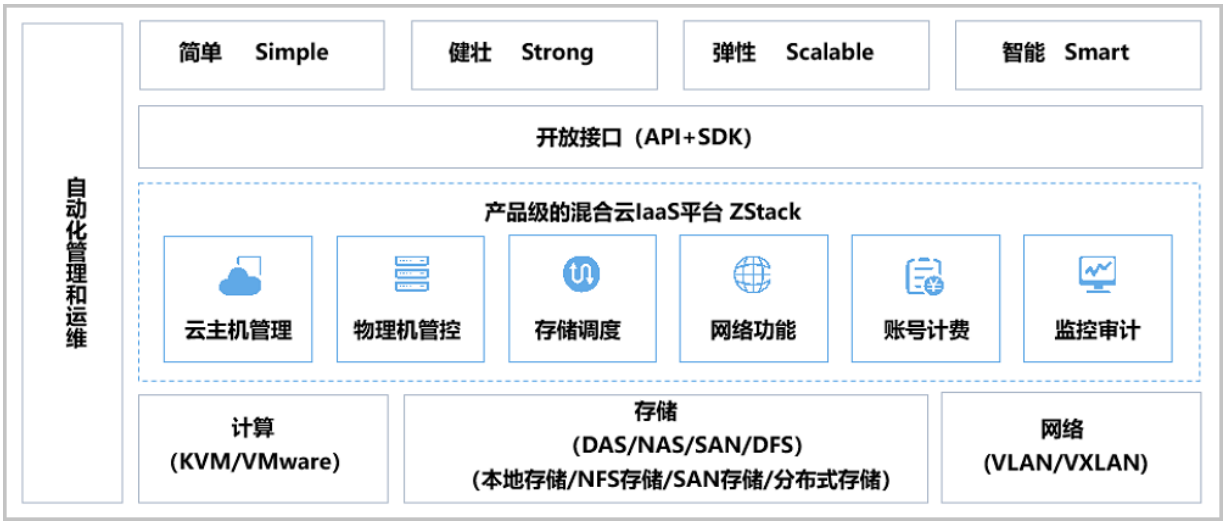


2 产品剖析

2.1 ZStack功能架构

ZStack功能架构如图 *2: ZStack功能架构*所示：

图 2: ZStack功能架构



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

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

ZStack核心架构设计特点：

1. **全异步架构**：异步消息、异步方法、异步HTTP调用。
   - ZStack使用消息总线进行各服务的通信连接，在调用服务时，源服务发消息给目的服务，并注册一个回调函数，然后立即返回；一旦目的服务完成任务，就会触发回调函数回复任务结果。异步消息可以并行处理。
   - ZStack服务之间采用异步消息进行通信，对于服务内部，一系列相关组件或插件，也是通过异步方法来调用，调用方法与异步消息一致。

- ZStack采用的插件机制，给每个插件设置相应的代理程序。ZStack为每个请求设置了回调URL在HTTP的包头，任务结束后，代理程序会发送应答给调用者的URL。
- 基于异步消息、异步方法、异步HTTP调用这三种方式，ZStack构建了一个分层架构，保证了所有组件均能实现异步操作。
- 基于全异步架构机制，单管理节点的ZStack每秒可并发处理上万条API请求，还可同时管理上万台服务器和数十万台云主机。

2. **无状态服务**：单次请求不依赖其他请求。

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

3. **无锁架构**：一致性哈希算法。

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

4. **进程内微服务**：微服务解耦。

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

5. **全插件结构**：插件支持横向扩展。

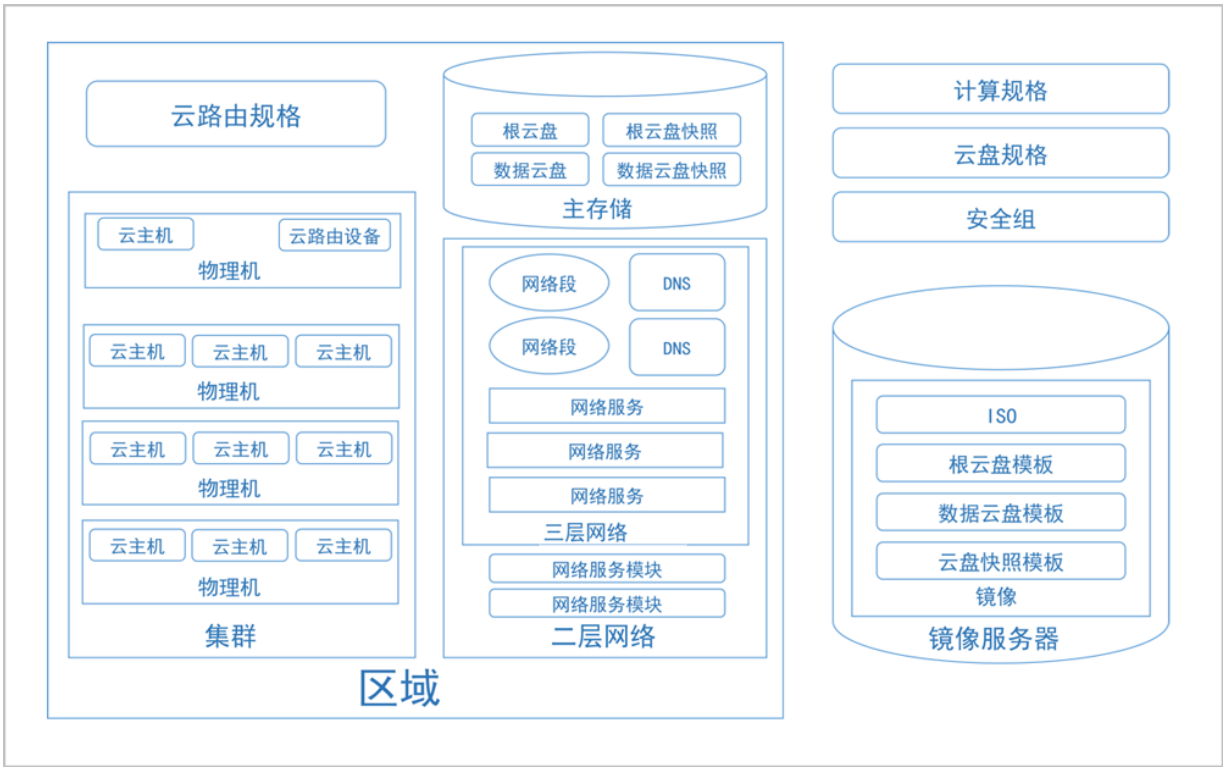
- ZStack使用中任何新加入的插件对目前其他的插件没有任何影响， 均是独立自主提供服务。
- ZStack支持策略模式和观察者模式进行插件设计。策略插件会继承父类的接口然后执行具体实现；观察者插件，会注册listener进行监控内部的业务逻辑的事件变化，当应用内部发现事件时，插件会对此事件做出自响应，在插件自身的代码里执行相应的业务流。
- ZStack支持插件的横向扩展，云平台可以快速更迭，而整体系统架构依然健壮。

6. **工作流引擎**：顺序管理，出错回滚。
   - ZStack工作流基于XML对每个工作流程进行清晰定义，在任何步骤出现错误均可按照原本执行路径进行回滚，清理掉执行过程的垃圾资源。
   - 每个工作流还可以包含子工作流用于扩展业务逻辑。
7. **标签系统**：支持业务逻辑变更，增加资源属性。
   - ZStack支持利用系统标签和插件机制对原本的业务逻辑进行扩展变更。
   - 使用标签机制，可对资源进行分组划分，支持对指定标签进行资源搜索。
8. **瀑布流架构**：支持资源的级联操作。
   - ZStack使用Cascade Framework对资源管理进行瀑布状的级联操作，对资源进行卸载或者删除时，会对相关的资源进行级联操作。
   - 资源也可以通过插件形式加入到瀑布框架中，加入或者退出瀑布框架，并不影响其他资源。
   - 级联机制使得ZStack的配置灵活轻便，快速满足客户资源配置的变更。
9. **全自动化Ansible部署**：Ansible无代理自动部署。
   - ZStack使用Ansible进行无代理的全自动化安装依赖、配置物理资源，部署代理程序，全过程对用户透明，无须额外干预，可透过重连代理程序对代理进行升级。
10. **全API查询**：任意资源的任意属性均可查询。
    - ZStack支持数百万个条件的资源查询，支持全API查询，支持任意组合。

2.2 ZStack资源结构

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

图 3: ZStack资源结构



ZStack主要包括以下资源：

- 区域：ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。
- 集群：一组物理主机（计算节点）的逻辑集合。
- 物理主机：也称之为计算节点，主要为云主机实例提供计算、网络、存储等资源的物理服务器。
- 主存储：用于存储云主机磁盘文件（包括：根云盘、数据云盘、根云盘快照、数据云盘快照、镜像缓存等）的存储服务器。支持本地存储、NFS、Shared Mount Point、Shared Block、Ceph类型。
- 镜像服务器：用于保存镜像模板的存储服务器，支持镜像仓库、Sftp、Ceph类型。
- VXLAN Pool：VXLAN网络中的Underlay网络，一个 VXLAN Pool可以创建多个VXLAN Overlay网络，这些Overlay网络运行在同一组Underlay网络设施上。VXLAN Pool支持软件SDN、硬件SDN两种类型。
- 二层网络：对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。支持L2NoVlanNetwork、L2VlanNetwork、VxlanNetwork、HardwareVxlanNetwork类型。
- 三层网络：云主机使用的网络配置，包含了IP地址范围、网关、DNS、网络服务等。
- 计算规格：云主机的CPU、内存、磁盘带宽、网络带宽的数量或大小规格定义。
- 云盘规格：云主机使用的云盘的大小规格定义。

- 云主机：运行在物理主机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务，是ZStack的核心组成部分。
- 镜像：云主机或云盘所使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像，其中系统云盘镜像支持ISO和Image类型， 数据云盘镜像支持Image类型。
- 根云盘：安装云主机操作系统的磁盘，用于支撑云主机的系统运行。
- 数据云盘：为云主机提供了额外的存储空间，用于云主机的存储扩展。
- 快照：采用增量机制对云盘在特定时间点上的数据进行备份。
- 网络服务模块：用于提供网络服务的模块。在UI界面已隐藏。
- 网络服务：给云主机提供的各种网络服务，主要包括VPC防火墙、安全组、虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道、流量监控等。
- VPC防火墙：负责管控VPC网络的南北向流量，通过配置规则集和规则来管控网络的访问控制策略。
- 安全组：给云主机提供三层网络防火墙控制，控制TCP/UDP/ICMP等数据包进行有效过滤，对指定网络的指定云主机按照指定的安全规则进行有效控制。
- 云路由规格：定义云路由器（普通云路由器、VPC路由器或ARM云路由器）使用的CPU、内存、云路由镜像、管理网络、公有网络等。
- 云路由器：作为定制的Linux云主机提供分布式DHCP、DNS、SNAT、路由表、弹性IP、端口转发、负载均衡、IPsec隧道等网络服务。
- VPC路由器：基于云路由规格直接创建的路由器，拥有公有网络和管理网络，是VPC的核心。提供各种网络服务，包括：DHCP、DNS、SNAT、路由表、弹性IP、端口转发、负载均衡、IPsec隧道、动态路由、组播路由、VPC防火墙、Netflow等。

ZStack资源间存在以下关系：

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

注: 主存储和镜像服务器的关系为：

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

ZStack资源均含有以下基本属性：

- UUID：通用唯一识别码UUIDv4（Universally Unique Identifier）来唯一标识一个资源。
- 名称：用于标记资源的可读字符串，名称可以重复，一般为必选项。
- 描述：也称之为简介，用于概述资源，可选项。
- 创建日期：资源创建的日期。
- 上次操作日期：资源上次被更新的时间。

ZStack资源一般都支持CRUD操作：

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

2.2.1 云资源池

2.2.1.1 云主机

云主机：运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务，是ZStack的核心组成部分。

2.2.1.2 云盘

云盘：为云主机提供存储。可分为：

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

云盘管理主要涉及数据云盘的管理。

2.2.1.3 镜像

镜像：云主机或云盘所使用的镜像模板文件。

- 镜像模板包括系统云盘镜像和数据云盘镜像。
- 系统云盘镜像支持ISO和Image类型，数据云盘镜像支持Image类型。

- Image类型支持raw和qcow2两种格式。
- 镜像保存在镜像服务器上，首次创建云主机/云盘时，会下载到主存储上作为镜像缓存。

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

- Linux：使用Virtio驱动；
- Windows：不使用Virtio驱动，使用Qemu模拟设备。镜像操作系统是未安装Virtio的Windows；
- WindowsVirtio：使用Virtio驱动，镜像操作系统是已安装Virtio驱动（包括磁盘驱动和网卡驱动）的Windows；
- Other：不使用Virtio驱动，使用Qemu模拟设备。镜像操作系统可以是任何操作系统，使用该平台类型可以兼容一些不支持Virtio驱动的低版本操作系统，例如RHEL5.8；
- Paravirtualization：使用Virtio驱动，镜像操作系统可以是已安装Virtio驱动的任何操作系统。

镜像路径支持添加URL路径或本地文件上传两种方式：

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

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

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

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

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

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

注:

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

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

注:

添加本地文件作为镜像，采用了本地浏览器作为中转上传镜像，请勿刷新或关闭当前浏览器，也不可停止管理节点服务，否则会添加失败。

2.2.1.4 亲和组

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

亲和组策略

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

- 反亲和组(非强制)：

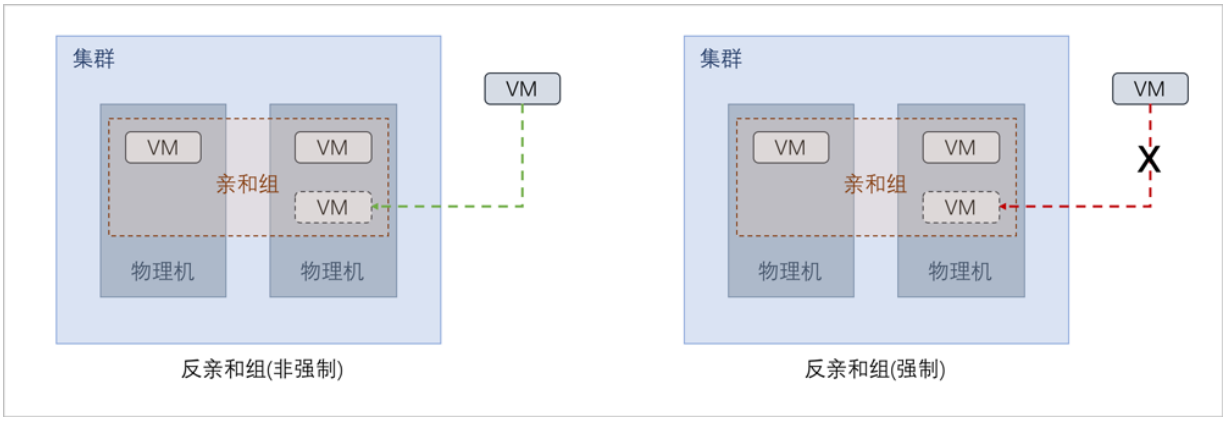
  将亲和组内的云主机尽量分配到不同物理机上，当没有更多物理机可分配时，回归普通分配策略。

- 反亲和组(强制)：

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

如图 *4: 反亲和组(非强制)与反亲和组(强制)*所示：

图 4: 反亲和组(非强制)与反亲和组(强制)



应用场景

以下介绍反亲和组(非强制)和反亲和组(强制)策略的应用场景。

- 反亲和组(非强制)策略应用场景举例：

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

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

- 反亲和组(强制)策略应用场景举例：

  承载主备数据库的两台云主机要求部署在不同的物理机上，保障业务高可用。

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

2.2.1.5 计算规格

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

2.2.1.6 云盘规格

云盘规格：云主机使用的云盘的大小规格定义。

云盘规格可以用来创建根云盘和数据云盘。

2.2.1.7 GPU规格

GPU规格：定义GPU帧数、显存、分辨率等参数大小的规格，包括：物理GPU规格、vGPU规格。

- 物理GPU规格：云平台内所有物理机上被扫描到的物理GPU规格列表及物理GPU规格相关基本信息。
- vGPU规格：经过虚拟化切割产生的可用vGPU规格列表及vGPU规格相关基本信息。

2.2.1.8 弹性伸缩组

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

伸缩模式

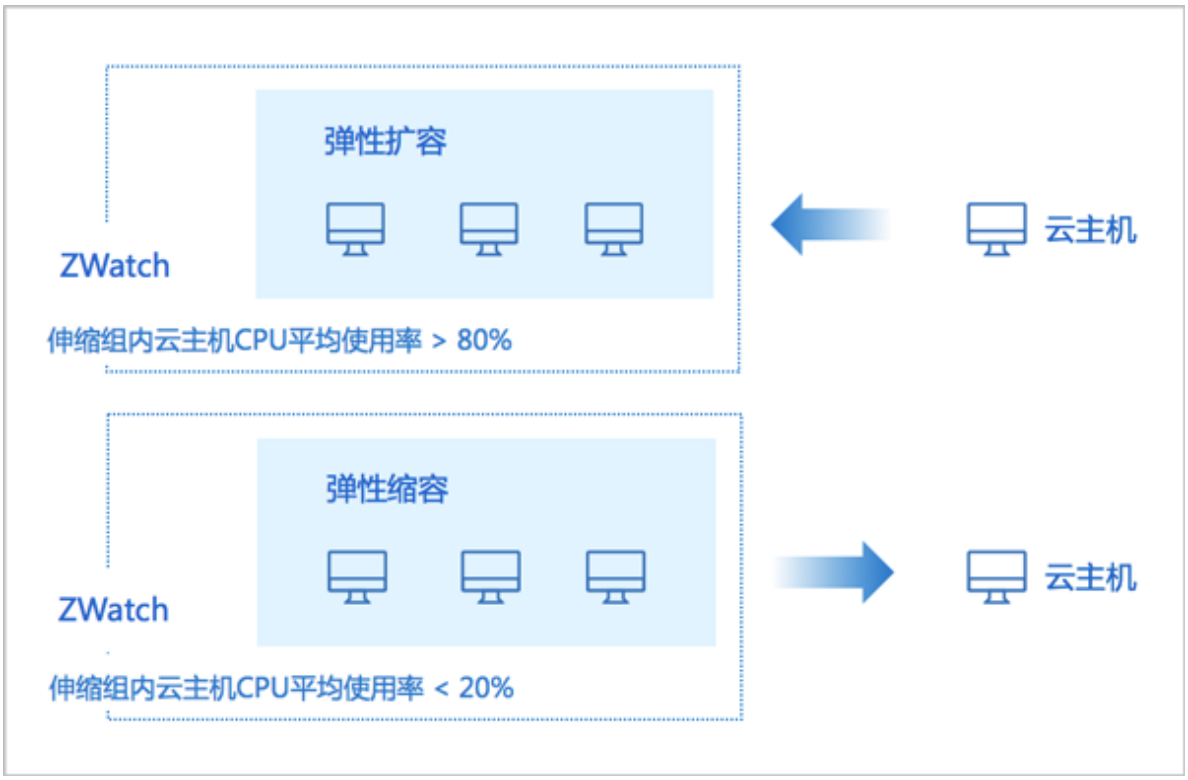
支持以下两种伸缩模式：

1. **弹性伸缩**

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

   如图 *5:* 弹性伸缩所示：

   图 5: 弹性伸缩

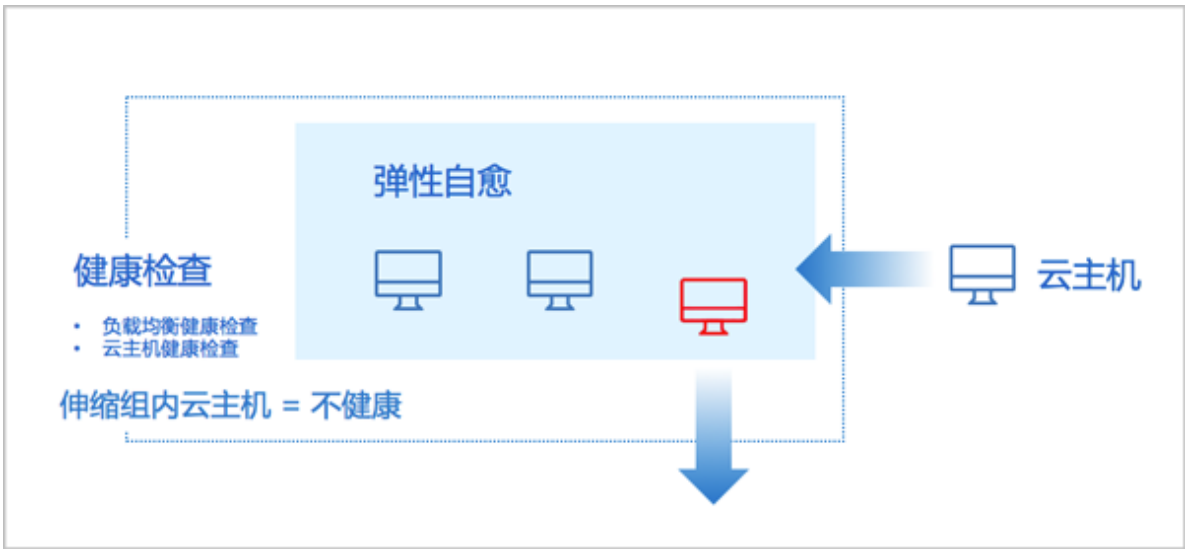


2. 弹性自愈

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

如图 *6:* 弹性自愈所示：

图 6: 弹性自愈



2.2.1.9 快照

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

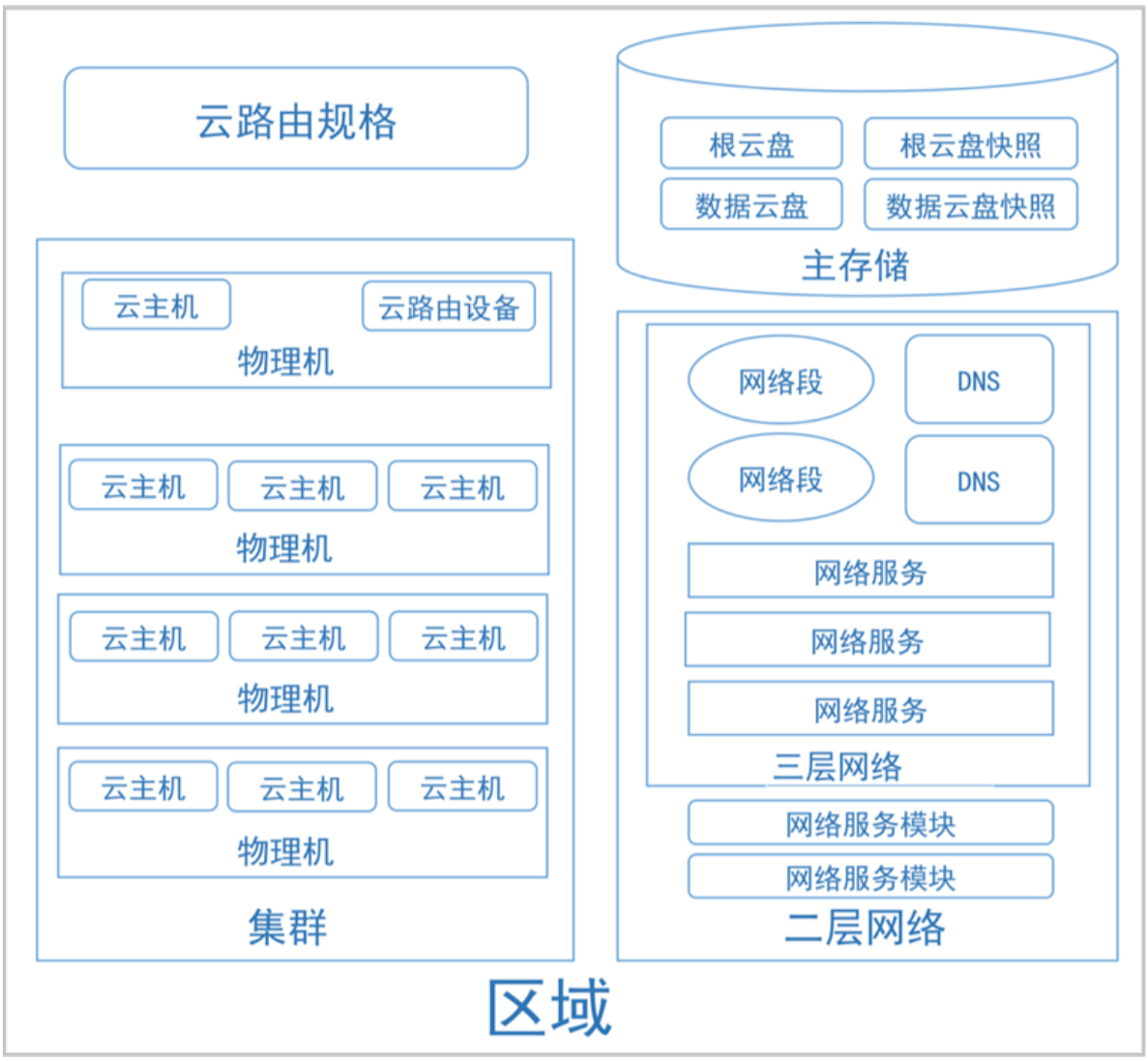
2.2.2 硬件设施

2.2.2.1 区域

区域：ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

- 在数据中心中，区域一般对应了一个机房。
- 区域定义了一个可见的边界，同一区域内的子资源互相可见并且可以形成某种关系，但不同区域内的子资源是不可见的，不能互相发生关系。
- 如图 7: 区域资源结构所示，区域中的资源以如下形式组织：

图 7: 区域资源结构



2.2.2.2 集群

集群：一组物理机（计算节点）的逻辑集合。在数据中心中，一个集群一般对应了一个机架。

规划集群时，需注意：

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

集群和各个资源之间的关系定义如下。

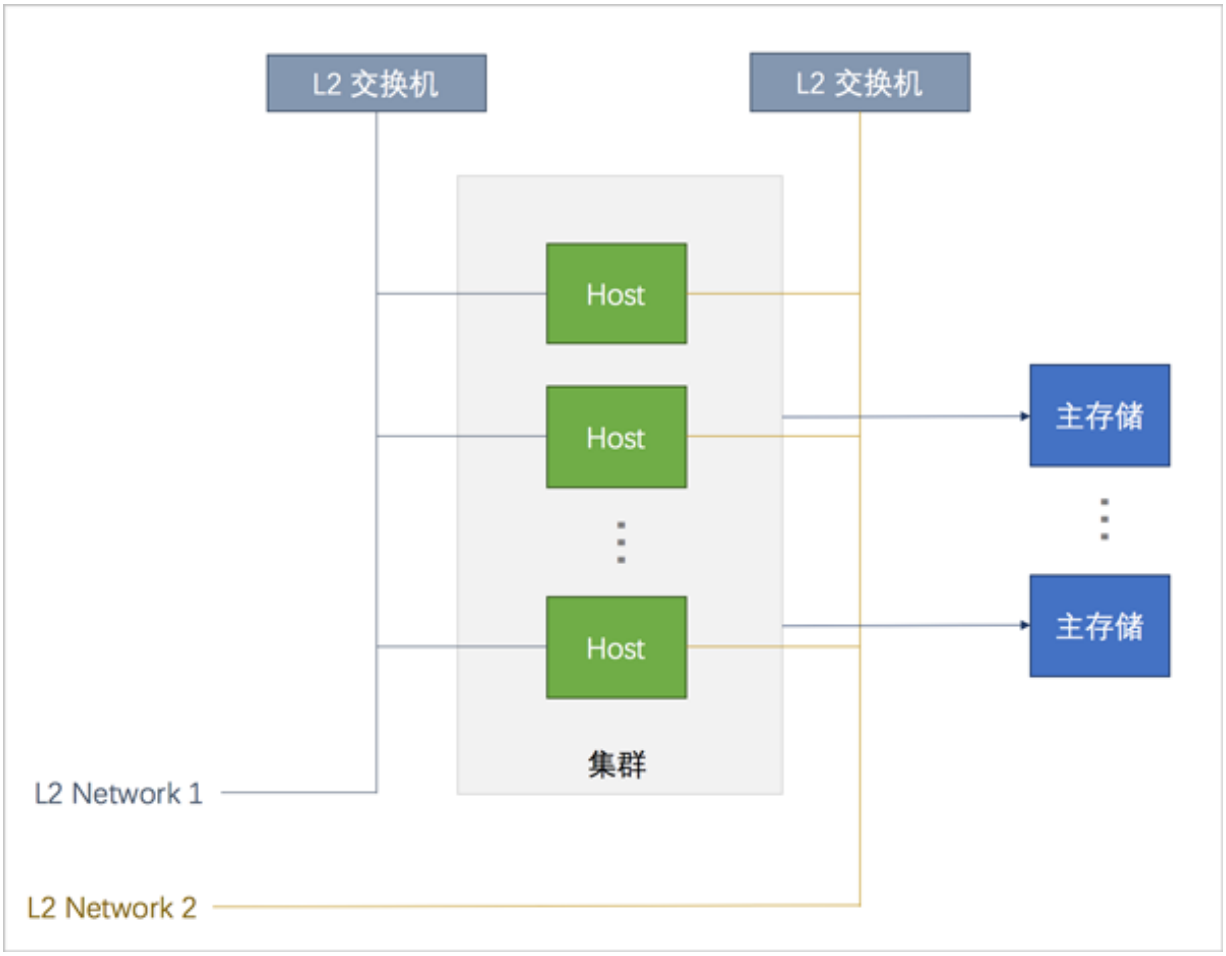
集群 | 区域

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

集群 | 主存储和二层网络

集群中可以加载或卸载主存储和二层网络，它们之间的结构关系如图 *8:* 集群、主存储、二层网络的关系所示：

图 8: 集群、主存储、二层网络的关系



注:

主存储和二层网络加载到集群时需注意：

1. 集群 | 主存储

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

   目前支持的同类型主存储场景如下：

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

目前支持的组合类型主存储场景如下：

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

主存储与集群的依赖关系如表 *1:* 主存储与集群关系所示：

表 1: 主存储与集群关系

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

- 集群挂载多个本地存储时，务必在添加物理机以及添加主存储之前，提前在物理机对应URL上做好分区，确保每个本地存储部署在独占的逻辑卷或物理磁盘上。

- 主存储可以被所在集群中的所有物理机访问。
- 如果数据中心的网络拓扑发生改变导致主存储不能被集群中的物理机继续访问时，主存储可以从集群卸载。

2. 集群 | 二层网络

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

集群 | 镜像服务器

集群与镜像服务器没有直接依赖关系，一个镜像服务器可以为多个集群提供服务。

注:

- 集群中所加载的主存储和镜像服务器具有相关性。
- Ceph主存储支持与镜像仓库类型的镜像服务器一同工作。
- 主存储（PS）和镜像服务器（BS）的相关性如表 2: 主存储与镜像服务器的关系所示：

表 2: 主存储与镜像服务器的关系

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

2.2.2.3 物理机

物理机：为云主机实例提供计算、网络、存储等资源的物理主机。

- 物理机是ZStack云平台的核心资产，云主机运行在物理机之上。

如图 *9:* 物理机所示：

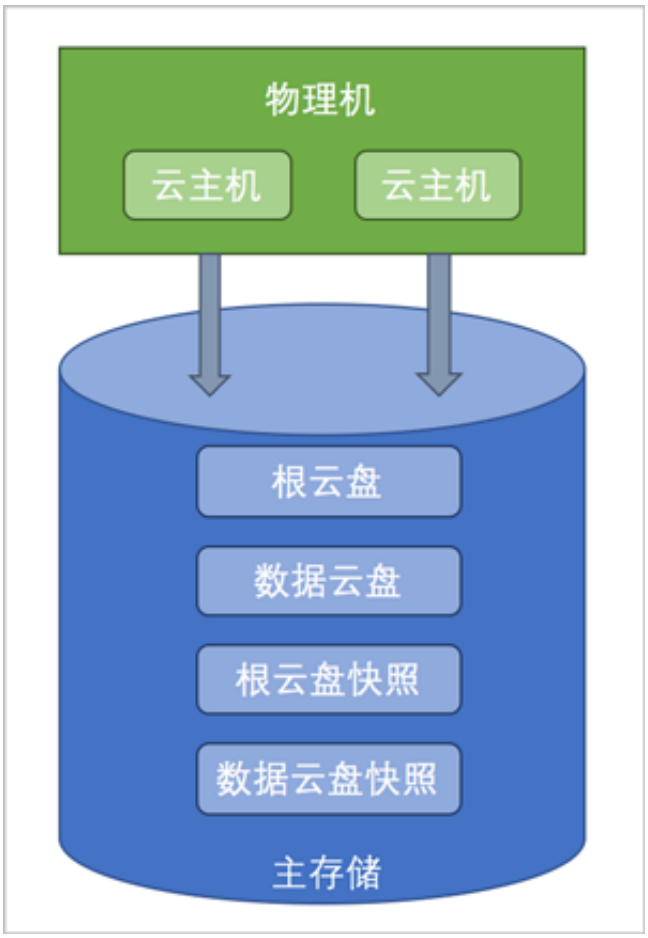
图 9: 物理机

2.2.2.4 主存储

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

如图 *10:* 主存储所示：

图 10: 主存储



主存储支持类型可分为以下两大类：

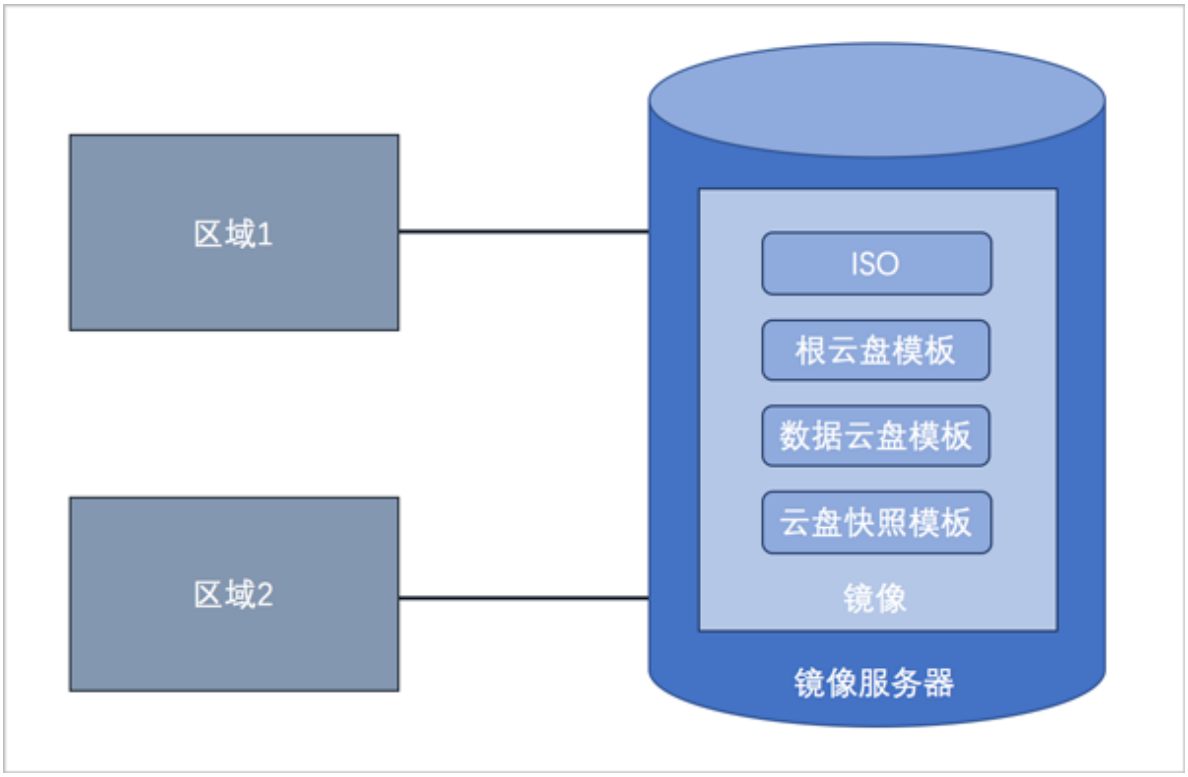
- **本地存储**（Local Storage）：使用物理机的硬盘进行存储。
- **网络共享存储**：支持NFS、Shared Mount Point、Ceph、Shared Block类型。
  - NFS为网络文件系统的存储方式。
  - Shared Mount Point支持常用的分布式文件系统提供的网络共享存储， 支持的常见类型有MooseFS、GlusterFS、OCFS2、GFS2等。
  - Ceph采用了分布式块存储方式。
  - Shared Block采用了共享块存储方式。

2.2.2.5 镜像服务器

镜像服务器：用于存储云主机镜像模板（含ISO）的存储服务器。

- 镜像服务器必须挂载到区域之后，区域中的资源才能访问它。通过镜像服务器，可在多个区域之间共享镜像。如图 *11:* 镜像服务器所示：

  图 11: 镜像服务器



- UI界面为便于管理镜像服务器和区域的关系，特别设置了一个镜像服务器只能对应一个区域。UI界面上，添加镜像服务器，默认会挂载到当前区域；删除区域的同时会直接删除挂载此区域的镜像服务器。

镜像服务器的类型

镜像服务器支持以下类型：

1. **ImageStore（镜像仓库）**：
   - 以镜像切片方式存储镜像文件，支持增量存储；
   - 支持云主机的在线/关机快照、在线/关机创建镜像；
   - 不带数据云盘克隆云主机时，支持在线/暂停/关机克隆；
   - 整机克隆时，LocalStorage、NFS、SMP、Ceph、Shared Block类型的主存储，支持在线/暂停/关机克隆；
   - 同一管理节点下的ImageStore类型的镜像服务器间支持镜像同步；
   - 支持获取已有镜像，可获取该镜像服务器中URL路径下的已有镜像文件。
2. **Sftp**：
   - 仅社区版支持；
   - 以文件方式存储镜像文件；

- 支持云主机的关机快照、关机创建镜像。
- 创建的镜像可以在镜像服务器上，以对应的镜像路径访问，拷贝到其他云环境可直接使用。

3. **Ceph镜像服务器**：

- 以Ceph分布式块存储方式存储镜像文件；
- 支持云主机的在线/关机快照、在线/关机创建镜像；
- 不带数据云盘克隆云主机时，支持在线/暂停/关机克隆；
- 不支持整机克隆；
- 导出镜像需在镜像服务器上导出。

  假定使用的镜像路径为：*ceph://bak-t-c9923f9821bf45498fdf9cdfa1749943/61ece0adc7244b0cbd12dafbc5494f0c*

  则需在镜像服务器上执行：

```
rbd export -p bak-t-c9923f9821bf45498fdf9cdfa1749943 --image 61ece0adc7244b
0cbd12dafbc5494f0c --path /root/export-test.image

# bak-t-c9923f9821bf45498fdf9cdfa1749943表示镜像所在的pool的名字
# 61ece0adc7244b0cbd12dafbc5494f0c表示镜像的名字
# /root/export-test.image表示导出的目标文件名字
```

镜像服务器 | 主存储

镜像服务器的类型与主存储的类型有关联性要求，如主存储与镜像服务器关系所示：

表 3: 主存储与镜像服务器的关系

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

- 当主存储为本地存储（LocalStorage）、NFS、Shared Mount Point类型时，镜像服务器的默认类型为ImageStore或Sftp。
- 当主存储为NFS或Shared Mount Point类型时，可将相应共享目录手动挂载到相应镜像服务器的本地目录上，从而使主存储和镜像服务器均能使用网络共享存储方式。

- 当主存储为Ceph类型时，镜像服务器可以使用同一个Ceph集群作为镜像服务器，也可以使用ImageStore类型的镜像服务器。
- 当主存储为Shared Block类型时，镜像服务器的默认类型为ImageStore。

2.2.2.6 SAN存储

ZStack支持对接iSCSI-SAN或FC-SAN存储上划分的块设备，直接透传给云主机使用，或将块设备添加为Shared Block主存储。对接SAN存储，目前包括：iSCSI存储、FC存储。

iSCSI服务器

ZStack支持添加iSCSI服务器，无需进入每个物理机进行配置，即可自动登录iSCSI，自动在线扫描并发现磁盘、自动配置iSCSI发起，方便快捷。其中，正确识别的iSCSI磁盘支持以下用途：

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

注:

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

FC存储

ZStack支持FC存储透传，自动在线扫描并发现已经配置的FC存储，并直观的展示FC存储详情。其中，正确识别的FC块设备支持以下用途：

- 将FC存储的块设备直接透传给云主机使用；
- 以共享块的方式，将FC存储的块设备添加为Shared Block主存储。

注:

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

2.2.3 网络资源

2.2.3.1 网络拓扑

ZStack 支持网络拓扑功能。不仅支持云平台的全局拓扑，还支持针对自定义资源生成拓扑图，快速定位资源状态。

图 12: 全局拓扑

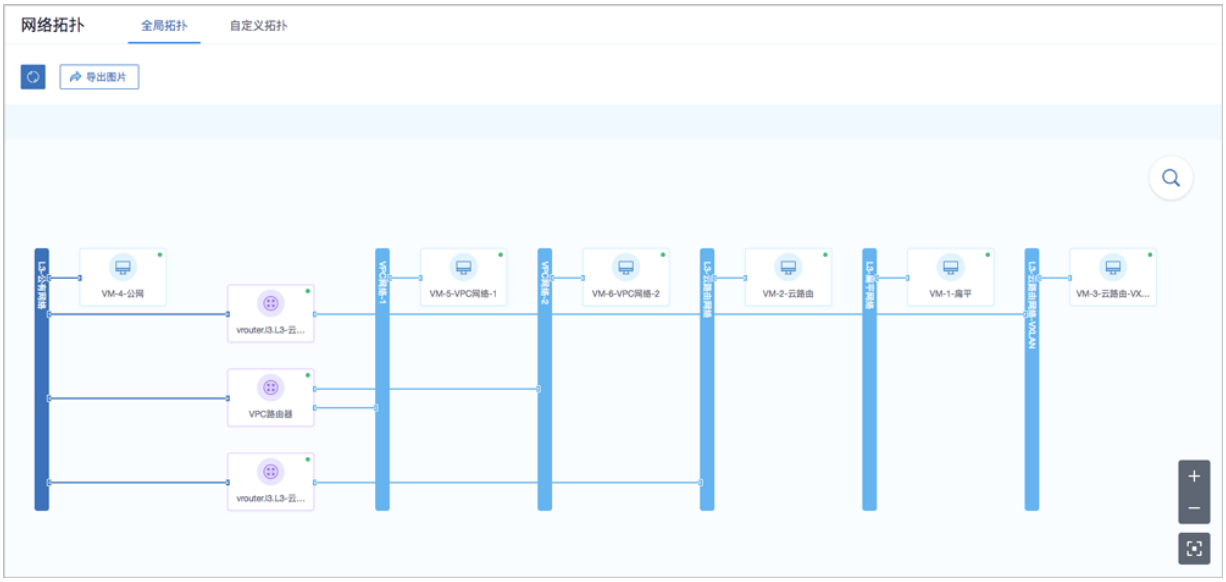
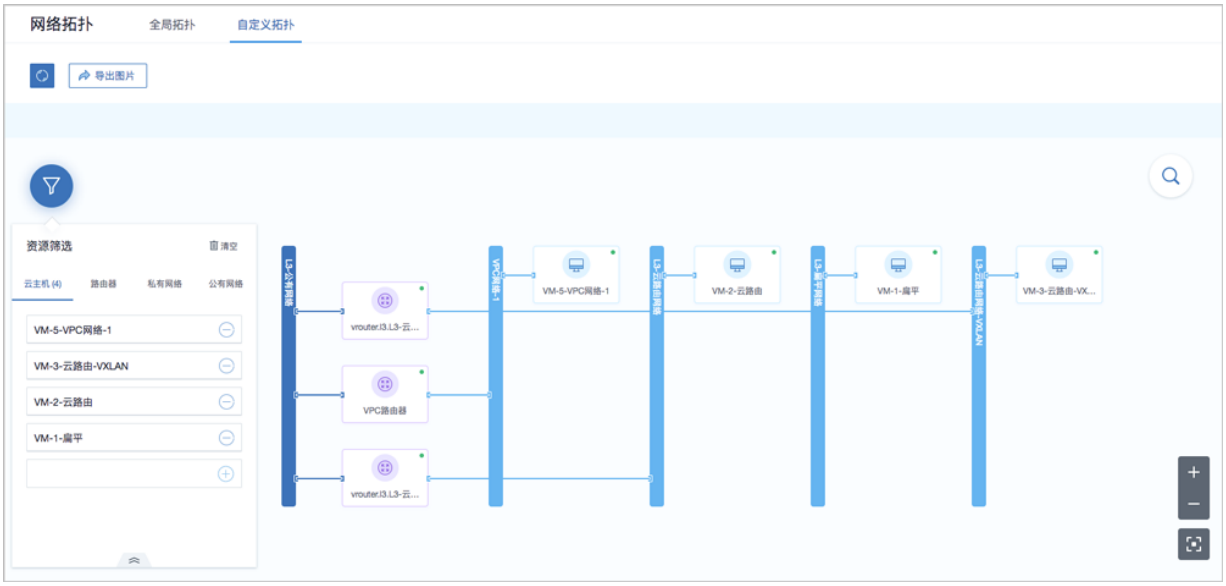


图 13: 自定义拓扑



2.2.3.2 SDN控制器

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

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

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

2.2.3.3 二层网络资源

VXLAN Pool

VXLAN Pool表示使用UDP进行报文封装的VXLAN类型的集合，是基于IP网络组建的大二层网络，可满足大规模云计算中心的需求。

- 使用VXLAN网络前需先建立VXLAN Pool；
- VXLAN Pool不能用于创建三层网络，只表示VXLAN网络的集合；
- VXLAN Pool支持两种类型：软件SDN、硬件SDN
  - 软件SDN类型：
    - 软件SDN类型VXLAN Pool的Vni范围支持1-16777214；
    - 挂载的集群内物理机在指定的CIDR应有IP作为VTEP（VXLAN隧道端点）。
      - VTEP一般对应于集群内计算节点中的某一网卡的IP地址，本云平台对VTEP的设置基于相应的CIDR进行配置，例如：
        - 假定计算节点某网卡的IP为*10.12.0.8*，子网掩码为*255.0.0.0*，网关为*10.0.0.1*，则VTEP输入的CIDR应为*10.0.0.1/8*；
        - 假定计算节点某网卡的IP为*172.20.12.13*，子网掩码为*255.255.0.0*，网关为*172.20.0.1*，则VTEP输入的CIDR应为*172.20.0.1/16*。
      - VXLAN Pool与集群进行挂载时，检查的是VTEP相关的IP地址，与物理的二层设备无关。
  - 硬件SDN类型：
    - 需提前添加SDN控制器到云平台；
    - 硬件SDN类型VXLAN Pool支持的Vni范围取决于SDN控制器对应的虚拟分布式交换机；

- 挂载的集群内物理机网卡应与SDN控制器管理下的交换机相连。
- 若使用VCFC配置硬件SDN，需提前在VCFC上配置VLAN与VXLAN的映射表，才能配置成功。

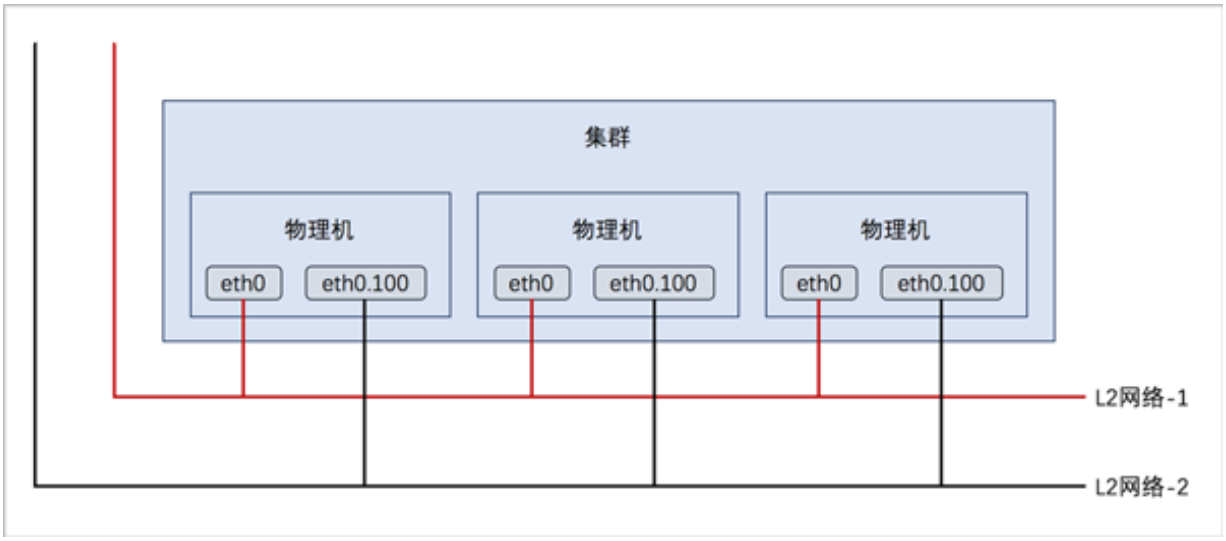
二层网络

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

- VLAN、VXLAN、或者SDN等能提供二层隔离技术都可作为二层网络。
- 二层网络负责为三层网络提供二层隔离。

如图 *14:* 二层网络所示：

图 14: 二层网络



二层网络主要支持以下四种类型：

1. **L2NoVlanNetwork**

   NoVlanNetwork类型表示相关的物理机对应的网络设备不设置VLAN。

   - 如果交换机端口设置了VLAN，则需在交换机端配置Access模式；
   - 如果交换机端口没有设置VLAN, 则无须特别设置；
   - 创建二层网络，会根据输入的网络设备创建网桥。

2. **L2VlanNetwork**

   VlanNetwork类型表示相关的物理机对应的网络设备需设置VLAN。

   - 需在物理机接入的交换机端进行Trunk设置；

- 从逻辑上划分虚拟局域网，支持1-4094个子网；
- 创建二层网络，会根据输入的网络设备创建VLAN设备，并基于此VLAN设备创建网桥。

3. **VxlanNetwork**

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

   - 需基于软件SDN类型VxlanNetworkPool创建VxlanNetwork；
   - 每个VxlanNetwork对应了软件SDN类型VxlanNetworkPool里的一个Vni；
   - 可用于创建三层网络。

4. **HardwareVxlanNetwork**

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

   - 需基于硬件SDN类型VxlanNetworkPool创建HardwareVxlanNetwork；
   - 每个HardwareVxlanNetwork对应了硬件SDN类型VxlanNetworkPool里的一个Vni；
   - 可用于创建三层网络。

注:

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

2.2.3.4 三层网络

三层网络：云主机使用的网络配置，包含了IP地址范围、网关、DNS、网络服务等。

- IP地址范围包含起始和结束IP地址、子网掩码、网关等，例如可指定*172.20.12.2*到*172.20.12.255*，子网掩码指定*255.255.0.0*，网关指定*172.20.0.1*；也可使用CIDR无域间路由来表示，例如*192.168.1.0/24*；
- DNS用于设置云主机网络的DNS解析服务。

公有网络

一般表示可直接连通互联网的网络，由于公有网络是一个逻辑概念，在无法连接互联网的环境中，用户也可以自定义该网络。在云路由网络、VPC中可以提供网络服务。

- 可用于扁平网络创建使用公网的云主机；

- 可用于云路由网络环境，单独创建使用公网的云主机；
- 可用于VPC网络环境，单独创建使用公网的云主机。

系统网络

管理节点用于特定用途的网络。

- 可用于部署配置相关资源的管理网络，例如部署物理机、主存储、镜像服务器、云路由等资源；
- 可用于云主机迁移的迁移网络；
- 如果网络资源不足，可与公有网络共用；
- 独立的系统网络用于特定用途，例如管理云路由器的网络；
- 系统网络不能用于创建普通云主机。

私有网络

可称之为业务网络或接入网络，云主机使用的网络，一般情况下设置为私网。私有网络指定为云主机使用的网络，支持三种网络架构模型：扁平网络、云路由网络、VPC。

特定场景网络

- 管理网络

  作为系统网络的一种，用于管理控制对应的物理资源。

  - 例如物理机、镜像服务器、主存储等需提供IP进行访问的资源时使用的网络；
  - 创建云路由器/VPC路由器时需要云路由器/VPC路由器存在管理节点互通的IP，以便部署agent及agent代理消息返回。
- 存储网络

  用于表示共享存储指定的存储网络，可使用此存储网络来判断云主机健康状态；建议提前规划单独的存储网络，避免潜在风险。
- VDI网络

  在创建集群时，可指定VDI网络的CIDR，此网络用于VDI连接的协议流量。如果不设置，VDI将默认使用管理网络。
- 迁移网络

  在创建集群时，可指定迁移网络的CIDR，此网络用于云主机在当前云平台内迁移。如果不设置，云主机迁移将默认使用管理网络。
- 镜像同步网络

同一管理节点下的ImageStore类型的镜像服务器间镜像同步使用的网络。

- 如果已部署镜像同步单独使用的网络，在添加镜像仓库时，可指定镜像同步网络的CIDR；
- 如果不设置，镜像同步将默认使用管理网络；
- 如果源镜像仓库和目标镜像仓库均设置镜像同步网络，起作用的是目标镜像仓库的镜像同步网络。

- 数据网络

  计算节点和镜像服务器之间进行数据通讯的网络。

  - 使用单独的数据网络，可避免网络拥塞，提高传输效率；
  - 如果不设置，将默认使用管理网络。

- 备份网络

  ZStack提供灾备服务高级功能。在本地灾备场景下，本地云主机/云盘/数据库备份到本地备份服务器、以及本地备份数据从本地备份服务器还原至本地时使用的网络。

  - 如果已部署本地灾备单独使用的网络，在添加本地备份服务器时，可指定备份网络的CIDR；
  - 使用单独的备份网络，可避免网络拥塞，提高传输效率；
  - 如果不设置，本地灾备将默认使用管理网络。

  注:

  灾备服务以单独的功能模块形式提供，需提前购买灾备服务模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

- 流量网络：

  端口镜像的专用网络，用于将网卡的网络流量镜像到远端，不能作为其他网络使用，不能用于创建云主机。

2.2.3.5 路由资源

云路由网络：主要使用定制的Linux云主机作为路由设备，提供DHCP、DNS、SNAT、路由表、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等网络服务。

云路由主要包括云路由镜像、云路由规格和云路由器。

- 云路由镜像：封装多种网络服务，只为创建云路由提供服务。
- 云路由规格：定义云路由器使用的CPU、内存、云路由镜像、公有网络、管理网络等。

- 云路由器：作为定制的Linux云主机提供DHCP、DNS、SNAT、路由表、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等网络服务。

云路由网络拓扑

云路由主要涉及以下3个基本网络：

- 公有网络：

  用于提供弹性IP、端口转发、负载均衡、IPsec隧道等网络服务需要提供虚拟IP的网络，公有网络一般要求可直接接入互联网。

- 管理网络：

  用于管理控制对应的物理资源，例如物理机、镜像服务器、主存储等需提供IP进行访问的资源时使用的网络。

- 私有网络：

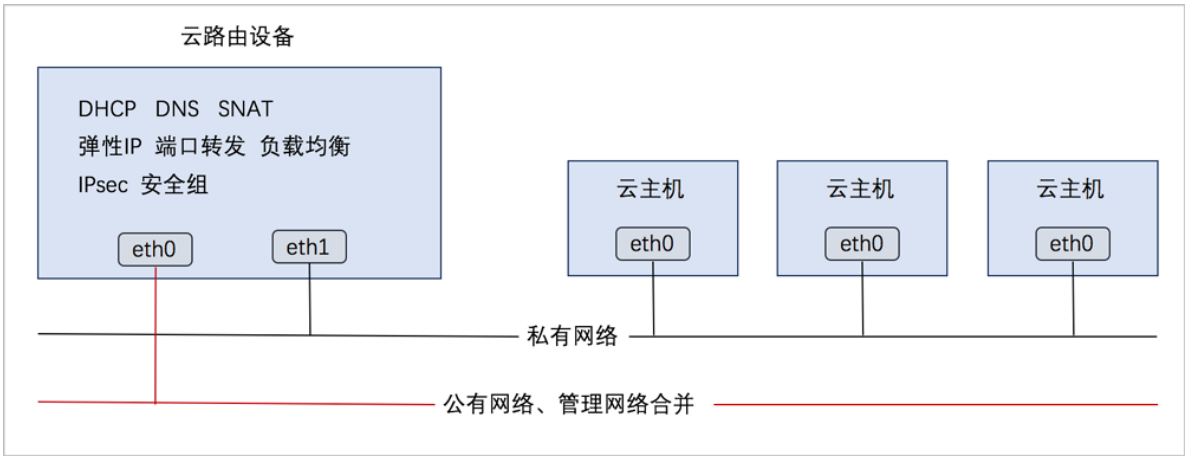
  也称之为业务网络或接入网络，是云主机使用的内部网络。

云路由网络部署方式：

- 公有网络和管理网络合并，私有网络独立部署

  如图 *15:* 部署方式-*1*所示：

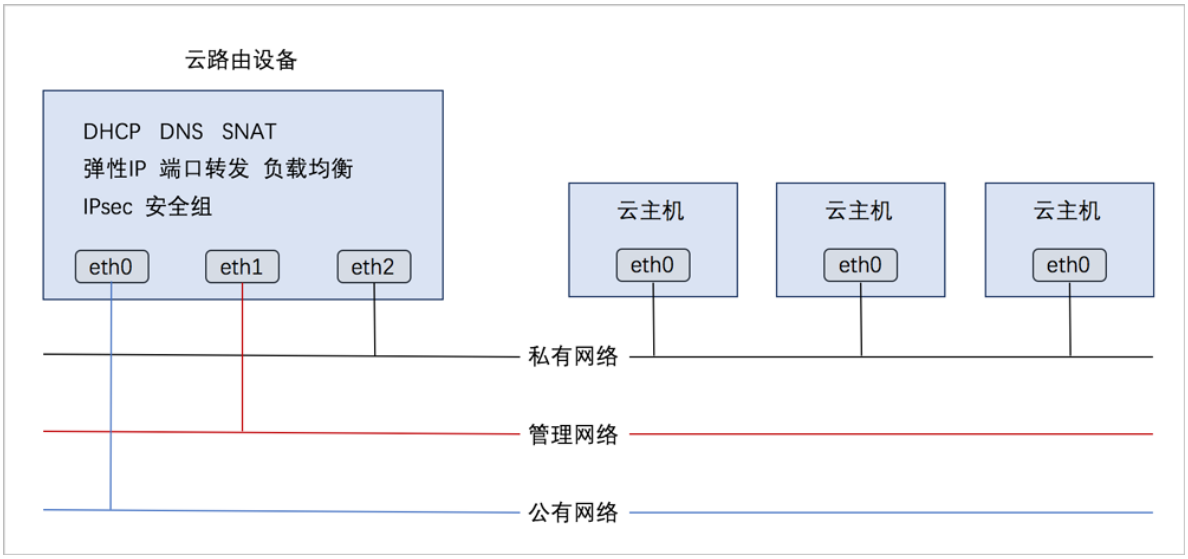
  图 15: 部署方式-1



- 公有网络、管理网络、私有网络均独立部署

  如图 *16:* 部署方式-*2*所示：

  图 16: 部署方式-2



云路由网络服务

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

- DHCP：
  - 在云路由器中，默认由扁平网络服务模块提供分布式DHCP服务。
- DNS：
  - 云路由器可作为DNS服务器提供DNS服务；
  - 在云主机中看到的DNS地址默认为云路由器的IP地址，由用户设置的DNS地址由云路由器负责转发配置。
- SNAT：
  - 云路由器可作为路由器向云主机提供源网络地址转换；
  - 云主机使用SNAT可直接访问外部互联网。
- 路由表、安全组、弹性IP、端口转发、负载均衡、IPsec隧道，将在专门章节中介绍。
- 弹性IP：使用云路由器可通过公有网络访问云主机的私有网络。
- 端口转发：提供将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。
- 负载均衡：将虚拟IP地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。
- 安全组：

- 由安全组网络服务模块提供安全组服务；
- 使用iptables进行云主机防火墙的安全控制。

2.2.3.6 VPC

专有网络VPC（Virtual Private Cloud，以下简称VPC），是基于VPC路由器和VPC网络共同组成的自定义私有云网络环境，帮助企业用户构建一个逻辑隔离的私有云。

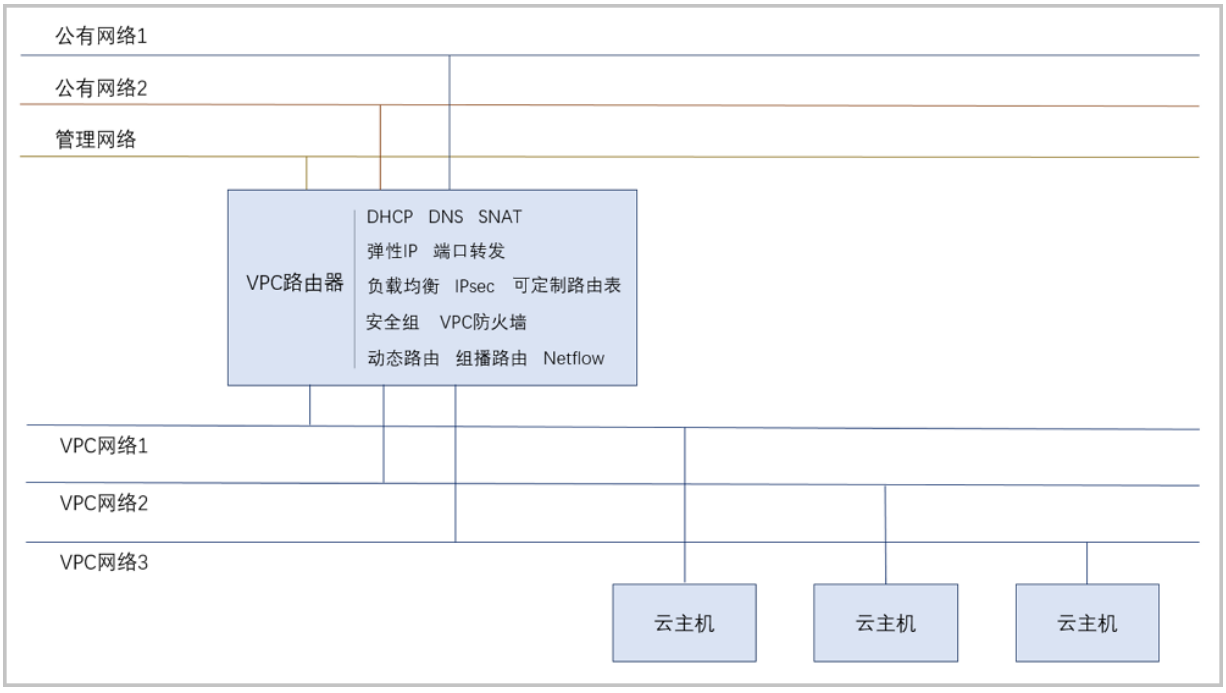
VPC路由器和VPC网络

VPC由VPC路由器和VPC网络组成。

- VPC路由器：基于云路由规格直接创建的虚拟路由器，拥有公有网络和管理网络。
- VPC网络：作为VPC的私有网络，可挂载至VPC路由器。

VPC网络拓扑如图 *17: VPC网络拓扑示意图*所示：

图 17: VPC网络拓扑示意图



VPC特点

VPC具有以下特点：

- 灵活的网络配置，不同的VPC网络可灵活挂载到VPC路由器，每个VPC网络可自定义独立的网络段和独立的网关，VPC路由器支持加载/卸载网卡，并支持动态配置路由表和路由条目。

- 安全可靠的隔离，不同VPC下的VPC网络互相逻辑隔离，支持VLAN和VXLAN进行二层逻辑隔离，不同账户的VPC互不影响。
- 多子网互通：同一VPC下的多个VPC网络互联互通。
- 网络流量优化：支持分布式路由功能，优化东西向网络流量，并有效降低网络延迟。
- VPC路由器高可用：可在一个VPC路由器高可用组内部署一对互为主备的VPC路由器，当主VPC路由器状态异常，会秒级触发高可用切换，自动切换至备VPC路由器工作，从而保障业务持续稳定运行。

VPC网络服务

VPC网络作为VPC的私有网络，使用VPC路由器提供各种网络服务。

- DHCP：默认采用扁平网络服务模块提供分布式DHCP服务。
- DNS：VPC路由器作为DNS服务器提供DNS服务。在云主机中看到的DNS地址默认为VPC路由器的IP地址，用户设置的DNS地址由VPC路由器负责转发配置。
- SNAT：VPC路由器向云主机提供原网络地址转换，云主机使用SNAT可直接访问外部互联网。
- 路由表：通过路由表，用户可管理自定义路由。
- 安全组：由安全组网络服务模块提供安全组服务，使用iptables进行云主机防火墙的安全控制。
- 弹性IP：可绑定弹性IP到VPC网络，实现公有网络到云主机私有网络的互联互通。
- 端口转发：提供公网IP到云主机私有网络IP的端口到端口的相关网络协议的互通。
- 负载均衡：将公网地址的访问流量分发到一组后端的云主机上，自动检测并隔离不可用的云主机。
- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的互联互通。
- 动态路由：VPC路由器支持OSPF动态路由协议，用于单一自治系统内决策路由。
- 组播路由：VPC路由器将组播源发送的组播消息转发给云主机，在发送端和接收端实现点对多点连接。
- VPC防火墙：通过对VPC路由器接口处南北向流量进行过滤，有效保护整个VPC通信安全及VPC路由器安全。
- Netflow：通过Netflow对VPC路由器网卡的进出流量进行分析监控，支持Netflow V5、V9两种数据流输出格式。

路由协议资源

相对于静态路由，动态路由支持自动拓扑变化，重新计算路由，无需人工干预，适用于大规模网络环境。VPC路由器支持OSPF动态路由协议。

OSPF协议：基于链路状态的内部网关协议，在数据中心网络、园区网络中有广泛应用。

2.2.4 网络服务

云平台为云主机提供以下网络服务：VPC防火墙、安全组、虚拟IP、弹性IP、端口转发、IPsec隧道、负载均衡、流量监控。

支持以下三种网络架构模型：

- 扁平网络
- 云路由网络
- VPC

网络服务模块

网络服务模块：用于提供网络服务的模块。在UI界面已隐藏。

主要有以下四种：

1. VirtualRouter（虚拟路由器网络服务模块，不建议使用）

   提供以下网络服务：DNS、SNAT、负载均衡、端口转发、弹性IP、DHCP

2. Flat Network Service Provider（扁平网络服务模块）

   提供以下网络服务：

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

     注: DHCP服务包含了DNS的功能。

   - VipQos：虚拟IP限速，限制上行及下行带宽。仅作用于弹性IP。

3. vrouter（云路由网络服务模块）

   提供以下网络服务：

   - IPsec：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。
   - VRouterRoute：通过路由表，用户可管理自定义路由。
   - CentralizedDNS：在启用分布式DHCP服务的场景下，提供DNS服务。
   - VipQos：虚拟IP限速，限制上行及下行带宽。
   - DNS：使用云路由器提供DNS服务。

- SNAT：云主机使用SNAT可以直接访问外部互联网。
- 负载均衡：将虚拟IP地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
- 端口转发：提供将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。
- 弹性IP：使用云路由器可通过公有网络访问云主机的私有网络。
- DHCP：集中式DHCP服务

4. SecurityGroup（安全组网络服务模块）

   提供以下网络服务：

   - 安全组：使用iptables进行云主机防火墙的安全控制。

扁平网络实践

生产环境中，一般建议使用以下网络服务的组合：

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

    注: DHCP服务包含了DNS的功能。
- 安全组网络服务模块：
  - 安全组：使用iptables进行云主机防火墙的安全控制。

云路由网络实践

生产环境中，一般建议使用以下网络服务的组合：

- 扁平网络服务模块：
  - Userdata：使用cloud-init进行云主机开机加载并执行特定的用户数据，例如ssh-key注入。
  - DHCP：分布式DHCP实现的动态获取IP地址。
- 云路由网络服务模块：
  - DNS：使用云路由器提供DNS服务。
  - SNAT：云主机使用SNAT可以直接访问外部互联网。
  - 路由表：通过路由表，用户可管理自定义路由。

  - 弹性IP：使用云路由器可通过公有网络访问云主机的私有网络。
  - 端口转发：提供将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。
  - 负载均衡：将虚拟IP地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
  - IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。
- 安全组网络服务模块：
  - 安全组：使用iptables进行云主机防火墙的安全控制。

VPC网络实践

生产环境中，一般建议使用以下网络服务的组合：

- 扁平网络服务模块：
  - Userdata：使用cloud-init进行云主机开机加载并执行特定的用户数据，例如ssh-key注入。
  - DHCP：分布式DHCP实现的动态获取IP地址。
- 云路由网络服务模块：
  - DNS：使用VPC路由器提供DNS服务。
  - SNAT：云主机使用SNAT可以直接访问外部互联网。
  - 路由表：通过路由表，用户可管理自定义路由。
  - 弹性IP：使用VPC路由器可通过公有网络访问云主机的私有网络。
  - 端口转发：提供将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。
  - 负载均衡：将虚拟IP地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
  - IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。
- 安全组网络服务模块：
  - 安全组：使用iptables进行云主机防火墙的安全控制。

高级网络服务

- 动态路由：支持OSPF动态路由协议，用于单一自治系统内决策路由，适用于VPC网络场景。
- 组播路由：将组播源发送的组播消息转发给云主机，在发送端和接收端实现点对多点连接，适用于VPC网络场景。
- VPC防火墙：通过对VPC路由器接口处南北向流量进行过滤，有效保护整个VPC通信安全及VPC路由器安全，适用于VPC网络场景。

- 端口镜像：将云主机网卡的网络流量复制一份到远端，对端口上的业务报文进行分析，方便对网络数据进行监控管理，适用于扁平/云路由/VPC网络场景。
- Netflow：通过Netflow对VPC路由器网卡的进出流量进行分析监控，支持Netflow V5、V9两种数据流输出格式，适用于VPC网络场景。

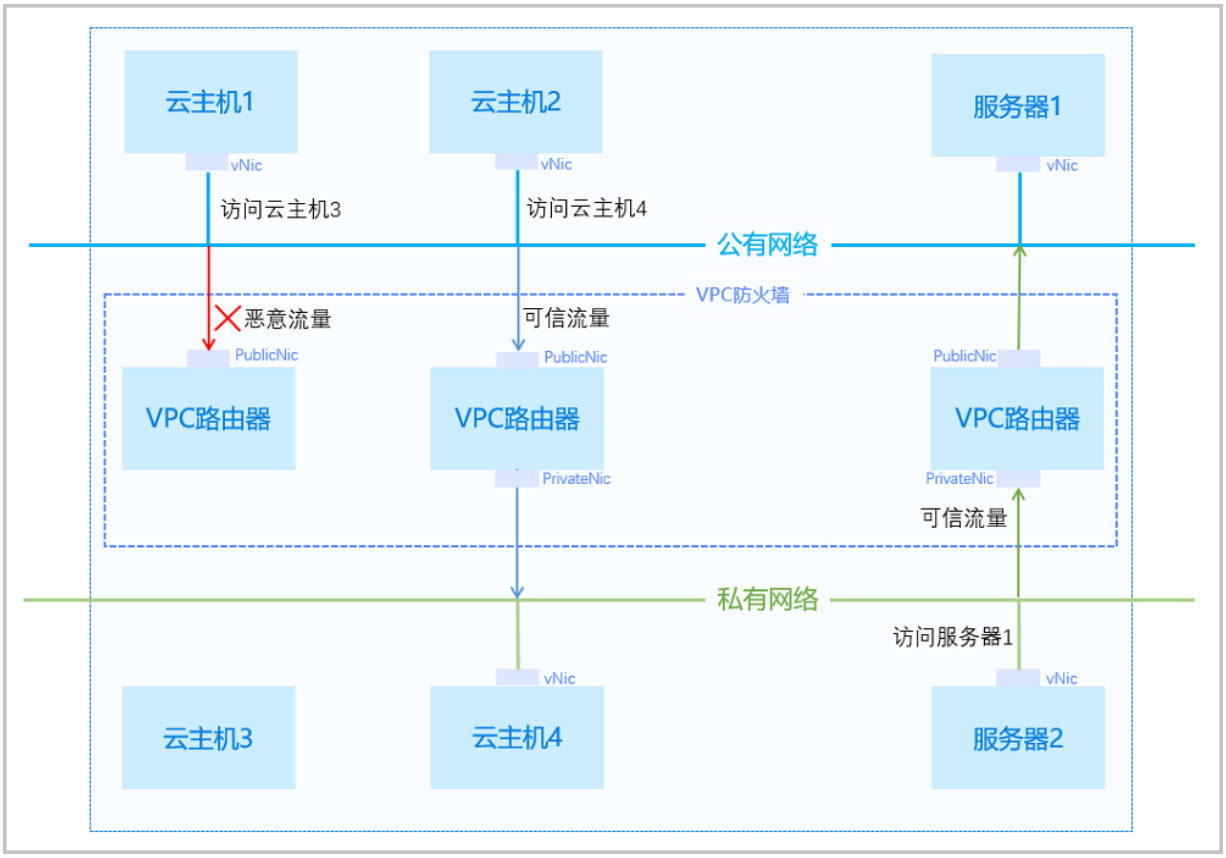
2.2.4.1 安全

2.2.4.1.1 VPC防火墙

VPC防火墙：负责管控VPC网络的南北向流量，通过配置规则集和规则来管控网络的访问控制策略。

如图 *18: VPC防火墙*所示：

图 18: VPC防火墙



- 云主机1访问云主机3：访问流量匹配公网网卡入方向规则集，检测为恶意流量，拒绝访问；
- 云主机2访问云主机4：访问流量匹配公网网卡入方向规则集，再匹配私网网卡出方向规则集，检测为可信流量，允许访问；

- 服务器2访问服务器1：访问流量匹配私网网卡入方向规则集，再匹配公网网卡出方向规则集，检测为可信流量，允许访问。

防火墙与安全组的区别：VPC防火墙管控南北向流量，作用范围是整个VPC；安全组主要管控东西向的流量，作用范围是云主机虚拟网卡，二者互为补充，具体区别如下：

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

注意事项

防火墙注意事项：

- 一个VPC路由器只能创建一个防火墙
- 一个网卡包含入（inbond）、出（outbond）两个防护方向，每个防护方向只能设置一个规则集
- VPC防火墙的防护机制会限制外部通过非EIP方式访问内部云主机，对于使用静态路由、OSPF的用户，若停用优先级9999的规则，则静态路由、OSPF服务将无法使用。若仍需使用静态路由、OSPF服务，请在停用后手动配置公有网络网卡入方向放行规则。

规则集注意事项：

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

规则注意事项：

- 规则隶属于规则集，不能复用在多个规则集上

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

2.2.4.1.2 安全组

安全组：给云主机提供三层网络安全组控制，控制TCP/UDP/ICMP等数据包进行有效过滤，对指定网络的指定云主机按照指定的安全规则进行有效控制。

- 扁平网络、云路由网络和VPC均支持安全组服务，安全组服务均由安全组网络服务模块提供，使用方法均相同：使用iptables进行云主机的安全控制。
- 安全组实际上是一个分布式防火墙；每次规则变化、加入/删除网卡都会导致多个云主机上的安全组规则被更新。

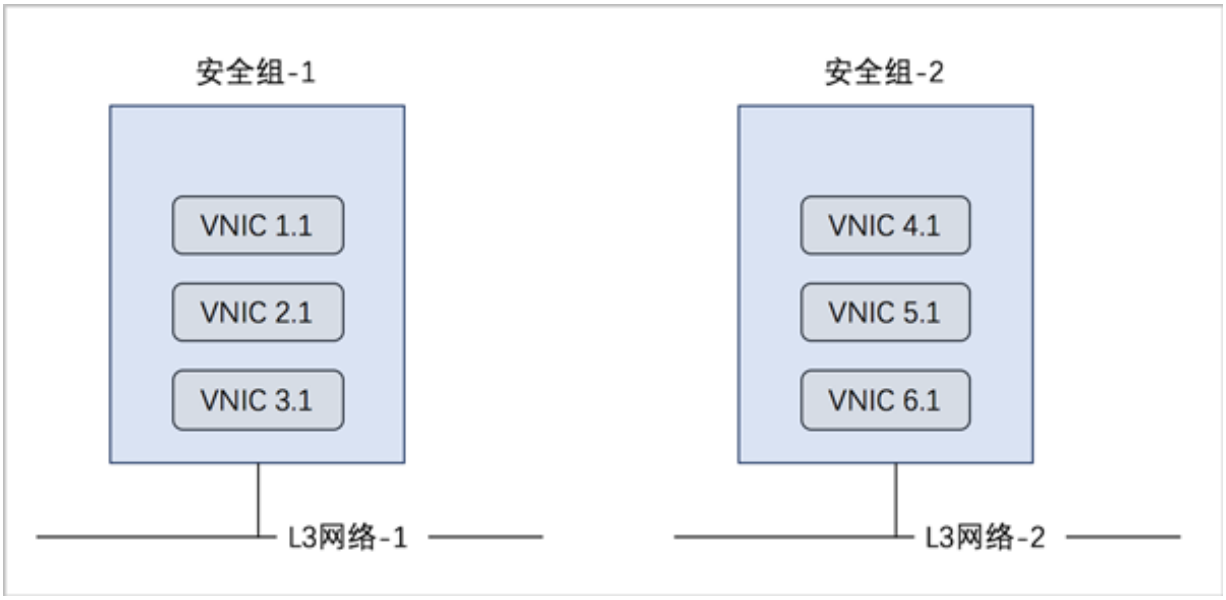
安全组规则：

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

注: 如果两者都设置，只取两者交集。

如图 *19:* 安全组所示：

图 19: 安全组



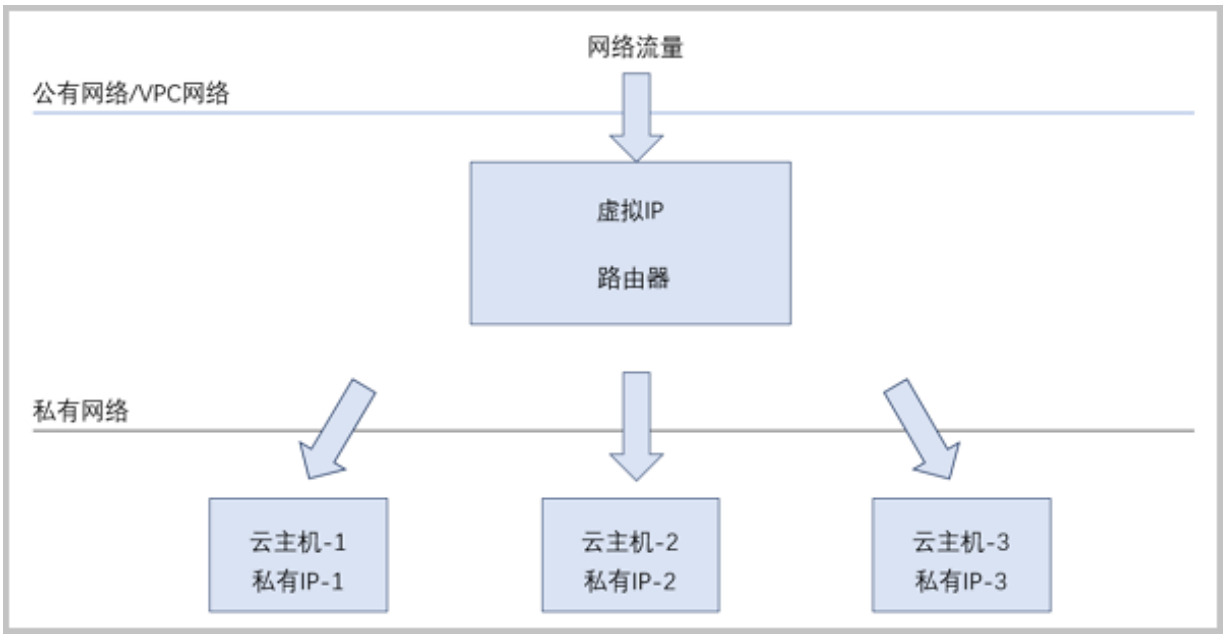
2.2.4.2 虚拟IP

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

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

以虚拟IP提供负载均衡服务为例，如图 *20: 虚拟IP提供负载均衡服务*所示：

图 20: 虚拟IP提供负载均衡服务



虚拟IP相关定义：

- 公网虚拟IP：使用公有网络创建的虚拟IP，支持自定义创建或跟随路由器自动创建
  - 公网虚拟IP支持为扁平网络提供弹性IP、负载均衡网络服务；支持为云路由网络/VPC网络提供弹性IP、端口转发、负载均衡、IPsec隧道网络服务。
  - 公网虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例，但不同类型服务不能使用相同的端口号。
  - 公网虚拟IP支持QoS、监控数据、性能TOP 5、性能分析、报警功能。
- VPC私网虚拟IP：使用VPC网络创建的虚拟IP，仅支持自定义创建
  - VPC私网虚拟IP支持为VPC网络提供负载均衡网络服务。
  - VPC私网虚拟IP暂不支持QoS、监控数据、性能TOP 5、性能分析、报警功能。
- 扁平私网虚拟IP：使用扁平网络创建的虚拟IP，支持自定义创建或跟随路由器自动创建
  - 扁平私网虚拟IP支持为扁平网络提供弹性IP、负载均衡网络服务。
  - 扁平私网虚拟IP支持QoS、监控数据、性能TOP 5、性能分析、报警功能。
- 自定义虚拟IP：用户手动创建的虚拟IP，支持自定义创建公网虚拟IP、VPC私网虚拟IP、扁平私网虚拟IP
  - 一个自定义公网虚拟IP仅用于一个弹性IP服务实例。
  - 自定义虚拟IP不支持跨普通云路由器/VPC路由器使用。

- 使用弹性IP、端口转发、负载均衡、IPsec隧道时，可选择**新建虚拟IP**重新创建自定义虚拟IP提供服务，也可选择**已有虚拟IP**中的已有自定义虚拟IP提供服务。

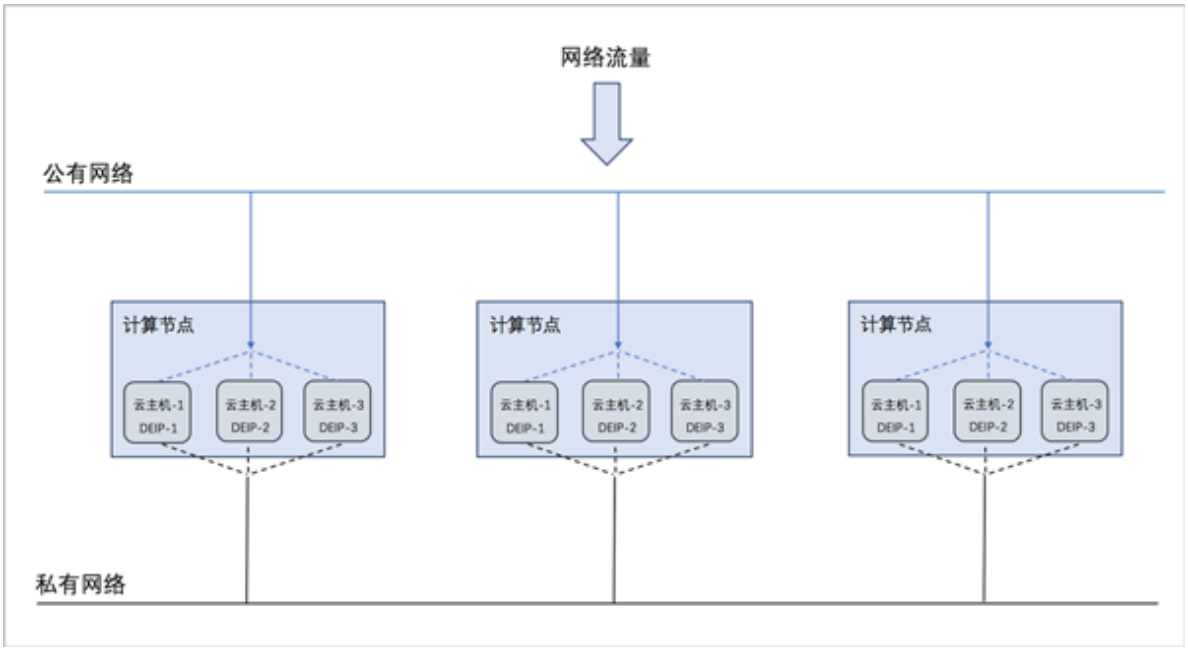
- 系统虚拟IP：路由器（云路由器/VPC路由器）成功创建后，系统使用路由器加载的三层网络自动创建的虚拟IP，支持跟随路由器自动创建公网虚拟IP或扁平私网虚拟IP
  - 系统虚拟IP与普通云路由器/VPC路由器一一对应，路由器每加载一条公有网络，系统将自动创建一个系统虚拟IP。且系统虚拟IP与云路由器/VPC路由器的默认IP相同。
  - 默认公有网络创建的系统虚拟IP，用于提供源地址转换服务。
  - 使用弹性IP、端口转发、负载均衡、IPsec隧道时，可选择**已有虚拟IP**中的系统虚拟IP提供服务。

2.2.4.3 弹性IP

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

- 以公网弹性IP为例，扁平网络下弹性IP的应用场景，如图 *21:* 扁平网络下弹性*IP*的应用场景所示：

图 21: 扁平网络下弹性IP的应用场景

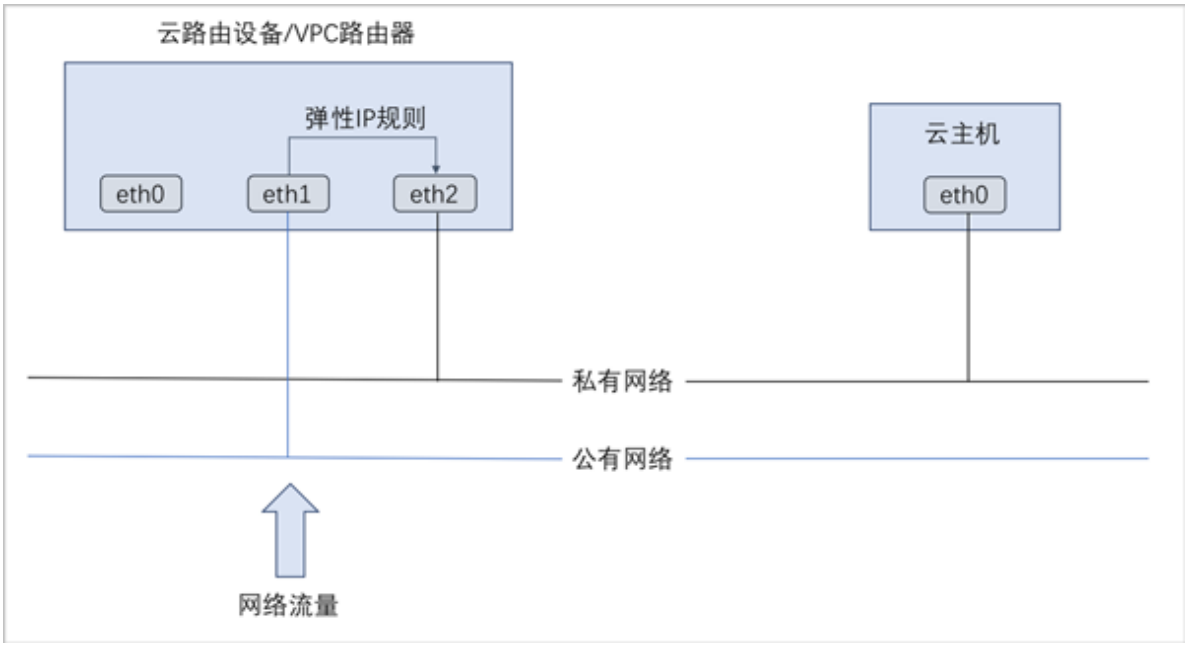


- 公有网络可通过防火墙连接到互联网。
- 私有网络（扁平网络）为各个计算节点内云主机提供IP地址，此IP地址默认情况下无法连接到互联网。

- 每个计算节点分别部署分布式EIP，可分别独立实现公网与私网的绑定。

- 云路由网络/VPC下弹性IP的应用场景，如图 *22: 云路由网络/VPC下弹性IP的应用场景*所示：

图 22: 云路由网络/VPC下弹性IP的应用场景



弹性IP相关定义：

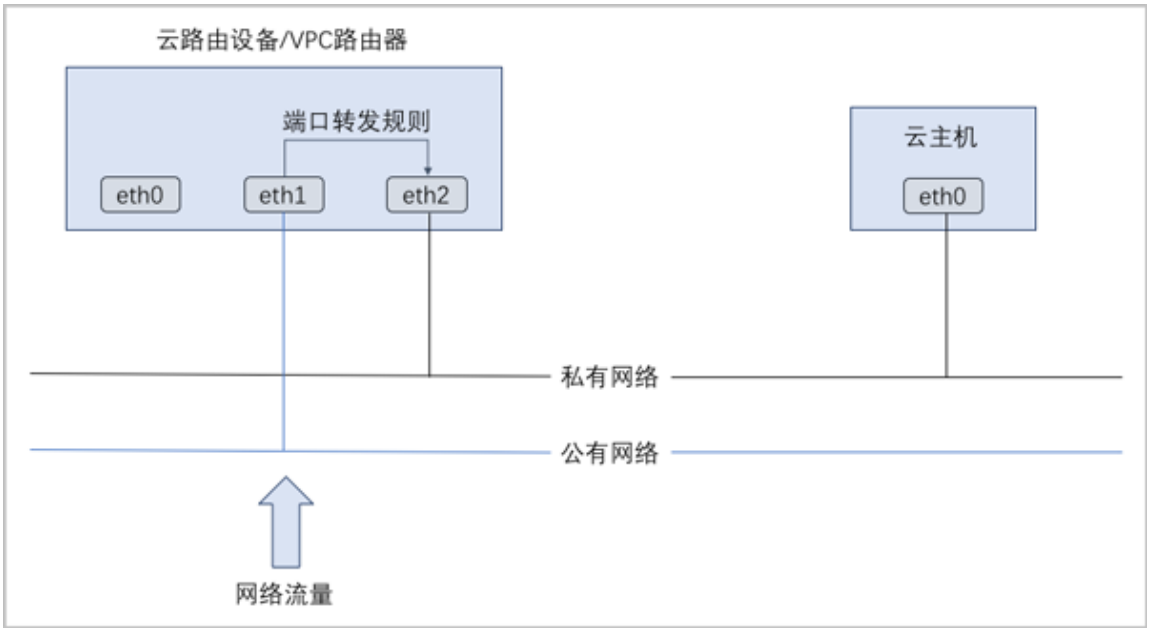
- 公网弹性IP：基于公有网络创建的公网虚拟IP提供弹性IP服务
  - 内部私有网络是隔离的网络空间，不能直接被外部网络访问，通过公网弹性IP可对公网的访问直接关联到内部私网的云主机IP。
  - 公网弹性IP可动态绑定到一个云主机，或从一个云主机解绑。
  - 公网弹性IP支持绑定私有网络（扁平网络/云路由网络/VPC网络）创建的云主机：
    - 基于分布式EIP实现的公网弹性IP地址，可通过公有网络访问扁平网络。
    - 可通过云路由器/VPC路由器使用公有网络访问云路由网络/VPC网络。
- 扁平私网弹性IP：基于扁平网络创建的扁平私网虚拟IP提供弹性IP服务
  - 不同网段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

2.2.4.4 端口转发

端口转发（PF）：基于云路由器/VPC路由器提供的三层转发服务，可将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。在公网IP地址紧缺的情况下，通过端口转发可提供多个云主机对外服务，节省公网IP地址资源。

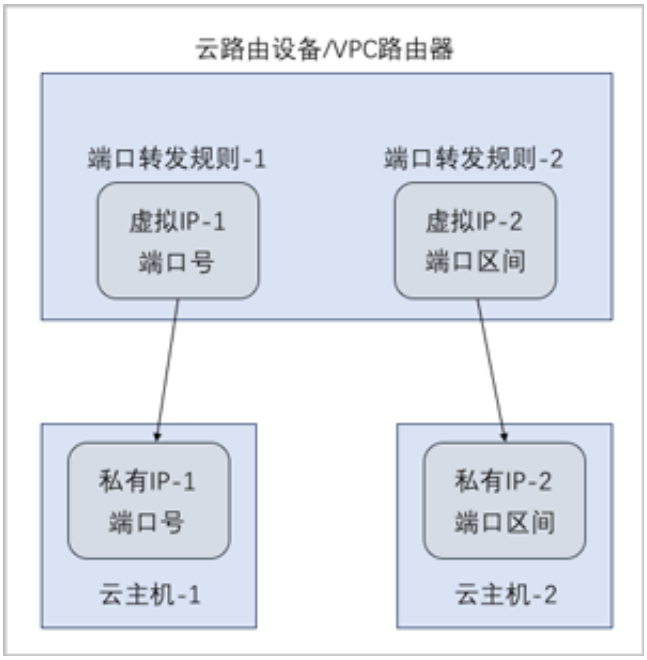
- 启用SNAT服务的私有网络中，云主机可访问外部网络但不能被外部网络所访问；使用端口转发规则，允许外部网络访问SNAT后面云主机的某些指定端口。
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *23:* 端口转发所示：

图 23: 端口转发



- 通过虚拟IP提供端口转发服务。
  - 虚拟IP对应于公网IP地址资源池中的一个可用IP。
  - 端口转发使用虚拟IP有两种方法：新建虚拟IP、使用已有虚拟IP。
  - 端口转发指定端口映射有两种方法：单个端口到单个端口的映射、端口区间的映射。
  - 如图 *24:* 虚拟*IP*-端口转发所示：

图 24: 虚拟IP-端口转发



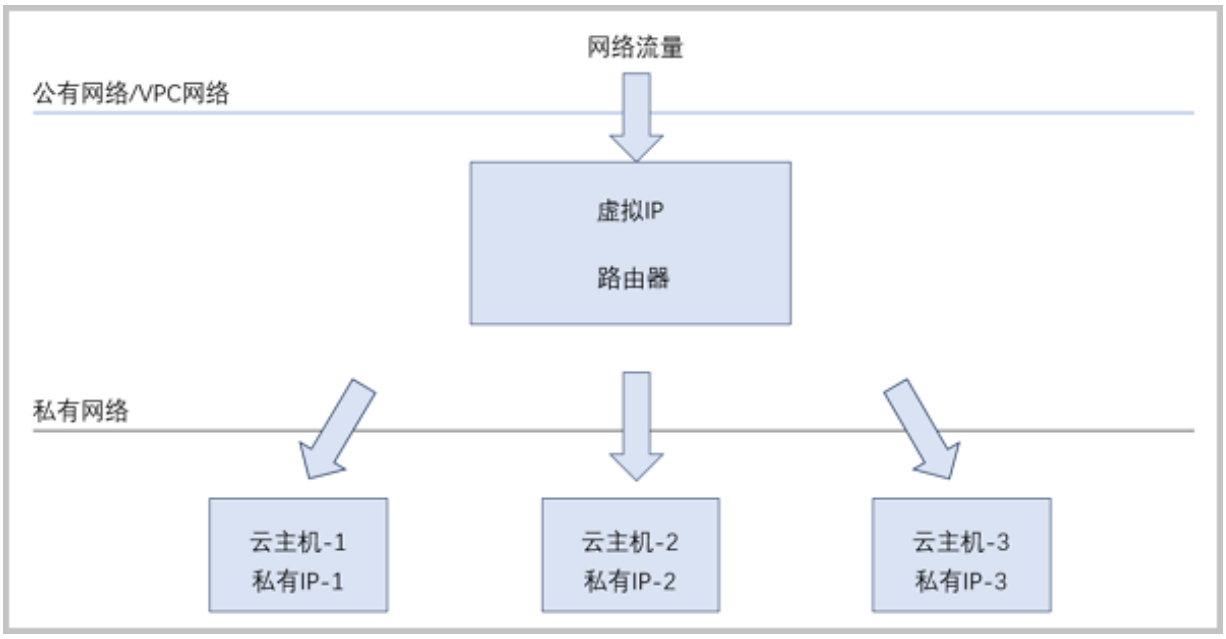
2.2.4.5 负载均衡

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

- 负载均衡自动把访问用户应用的流量分发到预先设置的多个后端云主机，以提供高并发高可靠的访问服务。
- 根据实际情况，动态调整负载均衡监听器中的云主机来调整服务能力，且不会影响业务的正常访问。
- 负载均衡监听器支持TCP/HTTP/HTTPS/UDP四种协议。
- 当监听协议为HTTPS，需绑定证书使用，支持上传证书和证书链。
- 负载均衡器支持灵活配置多种转发策略，实现高级转发控制功能。
- 负载均衡支持在监控数据中实时展示自己的SLB业务的流量和连接数情况。

扁平网络/云路由网络/VPC场景下虚拟IP提供负载均衡服务，如图 *25:* 虚拟*IP*-负载均衡所示：

图 25: 虚拟IP-负载均衡



负载均衡相关定义：

- 前端网络：负载均衡网络服务中，用于提供虚拟IP的网络，支持使用公有网络、扁平网络、VPC网络作为前端网络。
- 后端网络：负载均衡网络服务中，用于创建后端云主机的私有网络，支持：扁平网络、云路由网络、VPC网络。
- 公网负载均衡：使用公有网络作为前端网络，通过路由器（VPC路由器/云路由器）提供外网负载均衡服务。
  - 支持使用VPC网络作为后端网络，提供基于VPC网络的公网负载均衡服务。此场景支持使用多条后端网络，但后端网络必须加载到同一VPC路由器。
  - 支持使用云路由网络作为后端网络，提供基于云路由网络的公网负载均衡服务。此场景需确保前端网络与云路由器加载的三层网络相同。
  - 支持使用扁平网络作为后端网络，提供基于扁平网络的公网负载均衡服务。此场景需确保前端网络与云路由器加载的三层网络相同。
- VPC私网负载均衡：使用VPC网络作为前端网络，通过VPC路由器提供内网负载均衡服务。
  - 支持使用与前端网络同一VPC路由器上的VPC网络作为后端网络，提供基于VPC网络的VPC私网负载均衡服务。
  - 此场景支持使用多条后端网络，但后端网络必须加载到同一VPC路由器。
- 扁平私网负载均衡：使用扁平网络作为前端网络，通过云路由器提供内网负载均衡服务。

- 同时使用前端网络作为后端网络，提供基于扁平网络的扁平私网负载均衡服务。此时，前端网络加载的云路由规格中的三层网络支持使用公有网络或扁平网络。
- 使用其他扁平网络作为后端网络，提供基于扁平网络的扁平私网负载均衡服务。此场景需确保前端网络与云路由器加载的三层网络相同。

注: 若需要使用扁平私网负载均衡服务，需提前为该扁平网络加载云路由规格。

2.2.4.6 IPsec隧道

IPsec隧道：透过对IP协议的分组加密和认证来保护IP协议的网络传输数据，实现站点到站点（site-to-site）的虚拟私有网络（VPN）连接。

IPsec隧道的特性：

- **IPsec连接模式**

  基于安全考虑，只支持主动模式（Main Mode），不支持积极模式（Aggressive Mode）；仅支持ESP封装协议。

- **IPsec传输模式**

  仅支持站点到站点的隧道模式，不支持PC点对点模式（基于云端网络模型考虑）。

- **IPsec路由模型**

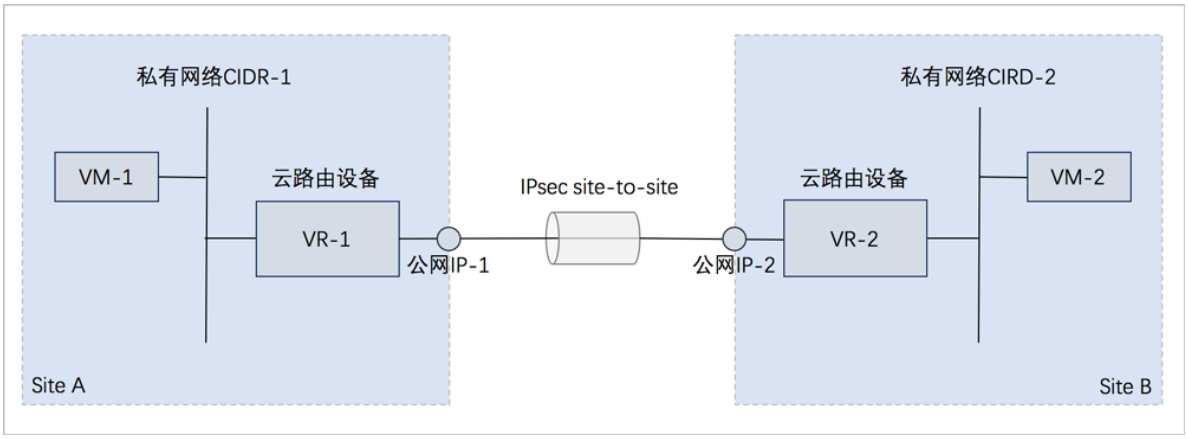
  仅支持基于对端网段配对模型，仅支持路由配对模式，不支持路由转发模式（不支持OSPF或BGP等动态路由协议）。

云路由网络下IPsec隧道的典型场景：

- 在两套隔离的ZStack私有云环境中，使用云路由网络；两套环境中云主机的私有网络无法直接通信，使用IPsec隧道可实现两套云主机的私有网络互相通信。

  如图 *26:* 云路由网络下*IPsec*隧道应用场景所示：

  图 26: 云路由网络下IPsec隧道应用场景



VPC IPsec隧道的典型场景：

- 在两套隔离的ZStack私有云环境中，分别搭建两套VPC环境，在两套VPC环境中，分别创建两套VPC网络（VPC子网），两套VPC环境的子网间无法直接通信，使用IPsec隧道后，就可实现两套VPC环境的子网间互相通信。

2.2.4.7 流量监控

2.2.4.7.1 流量网络

流量网络：端口镜像的专用网络，用于将网卡的网络流量镜像到远端，不能作为其他网络使用，不能用于创建云主机。

2.2.4.7.2 端口镜像

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

2.2.4.7.3 Netflow

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

2.2.5 vCenter接管

介绍

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

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

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

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

基础资源

vCenter的基础资源主要涉及ZStack对vCenter虚拟化资源的统一管理，目前包括：添加vCenter、同步数据和删除。

首次添加vCenter后，ZStack会自动同步vCenter的集群、物理机、虚拟机、模板、存储、网络等资源；使用过程中，需要点击**同步数据**按钮，将vCenter的资源手动同步至本地。相关资源均支持界面查看。

- 支持添加多个vCenter并进行管理；
- vCenter资源导入ZStack支持过滤。
  - dvSwitch场景：

    只有添加到dvSwitch中的物理机，其相关资源才能导入ZStack，未添加到dvSwitch中的物理机，其相关资源不能导入ZStack。
  - vSwitch场景：

    只有添加至少一个相同的vSwitch名称，且具备至少一个相同的端口组属性（包括：相同的网络标签和VLAN ID），满足以上条件的同一集群下的物理机，其相关资源（其上所有虚拟机、相同的端口组）才能导入ZStack。

    注: ZStack仅接管虚拟机网络，不接管VMkernel或管理网络。

云主机

添加vCenter后，vCenter云主机自动同步至ZStack；也支持本地创建vCenter云主机。

网络

要在ZStack接管的vCenter环境中新建云主机，需提前搭建好vCenter中的云路由网络或扁平网络。

vCenter网络服务目前支持云路由网络架构模型。

vCenter云路由网络提供了DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、Netflow等网络服务。

- DNS：
  - vCenter云路由器可作为DNS服务器提供DNS服务；
  - 在vCenter云主机中看到的DNS地址默认为vCenter云路由器的IP地址，由用户设置的DNS地址由vCenter云路由器负责转发配置。
- SNAT：
  - vCenter云路由器向vCenter云主机提供原网络地址转换；
  - vCenter云主机使用SNAT可直接访问外部互联网。
- 弹性IP：使用vCenter云路由器可通过公有网络访问vCenter云主机的私有网络。
- 端口转发：提供将指定公有网络的IP地址端口流量转发到vCenter云主机对应协议的端口。
- 负载均衡：将公网地址的访问流量分发到一组后端的vCenter云主机，并自动检测并隔离不可用的vCenter云主机。
- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。

网络服务

vCenter云路由网络提供了DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、Netflow等网络服务。

- DNS：
  - vCenter云路由器可作为DNS服务器提供DNS服务；
  - 在vCenter云主机中看到的DNS地址默认为vCenter云路由器的IP地址，由用户设置的DNS地址由vCenter云路由器负责转发配置。
- SNAT：
  - vCenter云路由器向vCenter云主机提供原网络地址转换；
  - vCenter云主机使用SNAT可直接访问外部互联网。
- 弹性IP：使用vCenter云路由器可通过公有网络访问vCenter云主机的私有网络。
- 端口转发：提供将指定公有网络的IP地址端口流量转发到vCenter云主机对应协议的端口。
- 负载均衡：将公网地址的访问流量分发到一组后端的vCenter云主机，并自动检测并隔离不可用的vCenter云主机。

- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。

ZStack对接管的vCenter支持多租户管理，普通账户/项目成员支持使用vCenter网络服务，包括：弹性IP、端口转发和负载均衡。

云盘

vCenter云盘：为vCenter云主机提供存储。可分为：

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

vCenter云盘管理主要涉及vCenter数据云盘的管理。

镜像

ZStack支持添加vmdk格式的本地镜像到vCenter。通过同步数据，vCenter镜像在本地和远端实现状态同步。支持添加两种镜像类型：系统镜像和云盘镜像。

事件消息

事件消息提供vCenter报警消息的查看。可查看该报警的消息描述、类型、所属vCenter、触发用户、目标和日期时间信息。

- 界面最多显示300条事件消息。支持设置时间段，可调整合适的时间段查看所设时间段内的报警消息。
- 支持调整每页显示的报警消息数量，可选值为：10、20、50、100；且支持翻页操作。

2.2.6 平台运维

2.2.6.1 性能TOP5

性能TOP5：支持直观查看云主机、路由器、物理机、三层网络、虚拟IP资源的各种监控指标TOP5信息，方便用户快速掌控当前云平台核心资源的实时性能状态以及资源使用情况，提高运维效率。

- 物理主机页面：

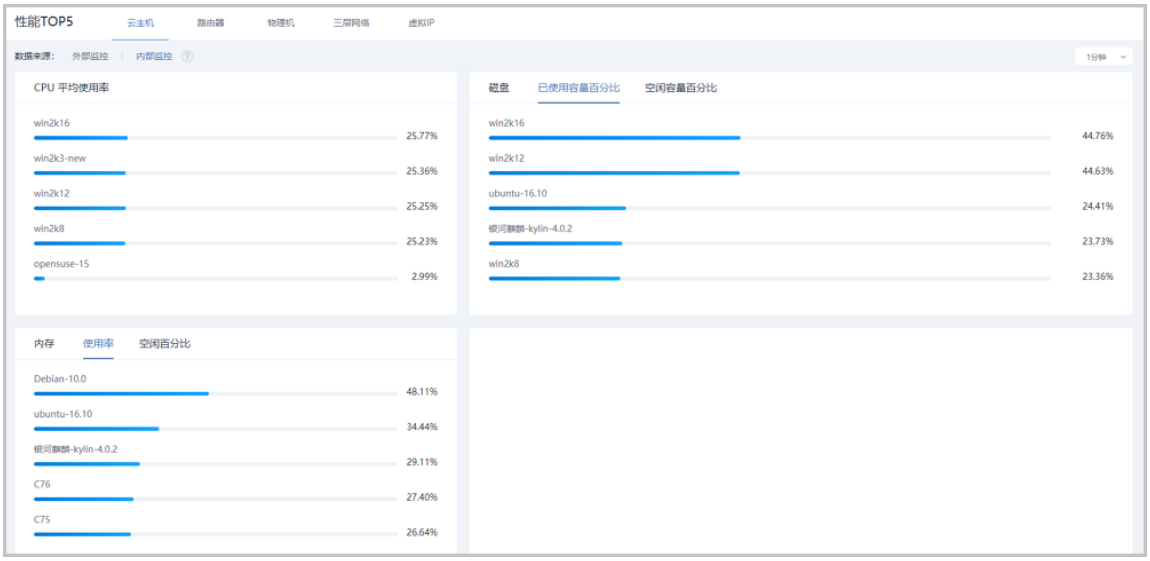
  通过对当前区域全部物理机的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、磁盘读写IOPS、磁盘已使用容量百分比、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

- 云主机页面：

云主机页面分为外部监控和内部监控：

- 外部监控同物理机页面类似，通过对当前区域全部云主机的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读写IOPS、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。
- 内部监控需要安装agent才能使用，安装方法请参考*agent*管理。通过对当前区域全部云主机的CPU、内存、磁盘使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读已使用容量百分比、磁盘空闲容量百分比为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。如图 *27: 云主机内部监控TOP5*所示：

图 27: 云主机内部监控TOP5



注: 对于内存数据而言，内部监控比外部监控拥有更好的准确性，推荐在监控内存数据时使用内部监控。

- 路由器页面：

  路由器页面分为外部监控和内部监控：

  - 外部监控同云主机页面类似，通过对当前区域全部路由器（包括云路由器和VPC路由器）的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读写IOPS、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百

分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

- 内部监控需要安装agent才能使用，安装方法请参考*agent*管理。通过对当前区域全部路由器的CPU、内存、磁盘使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读已使用容量百分比、磁盘空闲容量百分比为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

  注: 对于内存数据而言，内部监控比外部监控拥有更好的准确性，推荐在监控内存数据时使用内部监控。

- 虚拟IP页面：

  通过对当前区域全部虚拟IP的网络传输性能进行统计分析，以上行网络流量、下行网络流量、上行网络包速率、下行网络包速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的数值排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些虚拟IP出现传输性能瓶颈。

- 三层网络页面：

  对当前区域全部三层网络的IPv4类型地址使用情况进行统计分析，以已用IP百分比、已用IP数量、可用IP百分比、可用IP数量为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的数值排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些三层网络的IP资源出现告急。

2.2.6.2 性能分析

性能分析：支持选择不同时间段直观查看云主机、路由器、物理机、三层网络、虚拟IP、镜像服务器资源的各种监控指标的详细信息，并提供外部监控和内部监控两种方式，方便用户快速掌控当前云平台核心资源的实时性能状态以及资源使用情况，提高运维效率。

其中：

- **云主机、路由器、物理主机**：显示了名称、CPU平均使用率、内存使用率、磁盘读/写速度、网卡出/入速度信息
- **三层网络**：显示了名称、已用IP数量、已用IP百分比、可用IP数量、可用IP百分比信息
- **虚拟IP**：显示了名称、下行网络流量、下行网络入包速率、上行网络流量、上行网络入包速率信息
- **镜像服务器**：显示了名称、镜像存储可用容量百分比信息

2.2.6.3 容量管理

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

2.2.6.4 ZWatch

ZWatch：即ZWatch监控系统，支持对时序化数据和事件进行监控，并通过通知服务（SNS）推送报警消息至指定的接收端。支持资源报警器、事件报警器和第三方消息报警器三种报警器类型，支持系统/邮箱/钉钉/HTTP应用/短信/Microsoft Teams接收端类型，部分资源报警器需安装agent才能使用。

ZWatch监控系统示意图如图 *28: ZWatch监控系统*所示：

图 28: ZWatch监控系统

基本原理

- **ZWatch**：

  ZWatch监控系统提供以下功能：

  - 时序化监控：目前支持监控两种时序化数据类型：
    - 资源负载数据：例如云主机CPU使用率、物理机内存使用率等；
    - 资源容量数据：例如可用IP数量、运行中云主机的总数量等。
  - 事件收集：收集云平台中发生的预定义事件，例如物理机失联，云主机高可用功能启动等。
  - 报警功能：对时序化数据或事件进行报警。
  - 审计功能：记录所有操作并提供搜索。
  - 自定义功能：用户可自定义设置报警器和报警消息模板。
    - 报警器：目前支持以下报警器类型：
      - 资源报警器：对时序化数据进行报警。例如：对云主机CPU使用率设置一个报警器，当某云主机CPU使用率连续5分钟超过80%，以邮件方式报警。
      - 事件报警器：对事件进行报警，又称为事件订阅。例如：订阅物理机失联事件，当某个物理机失联后，以钉钉方式报警。
      - 第三方消息报警器：接收来自第三方消息源的报警消息。例如：存储池降级，当某个企业版存储的存储池降级后，在云平台以系统方式报警。
    - 报警消息模板：报警器或事件向SNS系统的主题发送消息时使用的文本模板。
      - 系统自带一个报警消息和恢复消息默认模板，若用户没有创建模板，系统将使用自带模板。
      - 用户可以创建多个消息模板，但只能指定一个为默认模板，发送消息时只会使用默认模板格式化信息。
      - 模板中可以通过${}引用报警器或事件提供的变量。
      - 目前报警消息模板支持邮箱/钉钉/Microsoft Teams/短信四种接收端平台。使用报警消息模板，可将通知邮件、钉钉消息、Microsoft Teams消息或短信以统一格式发出。
    - 消息源：用于连接第三方消息源，接管第三方报警消息并结合报警器统一推送至各类接收端，方便报警消息统一管理的同时提高运维效率，目前支持接管企业版存储的报警消息。
- **通知服务**（SNS）：

通知服务将报警消息推送至接收端，接收端类型包括：系统/邮箱/钉钉/HTTP应用/短信/Microsoft Teams。

接收端设置：

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

功能优势

ZWatch监控系统具有以下功能优势：

- 提供丰富的报警监控条目，对云平台核心资源以及事件进行全面监控报警；
- 支持系统/邮箱/钉钉/HTTP应用/短信/Microsoft Teams接收端用于订阅主题，用户可根据实际情况选择合适的报警接收方式；
- 一个报警器可同时对多个资源进行监控；
- 邮箱、钉钉、短信和Microsoft Teams接收端支持自定义报警消息模板，用户可按需设置报警消息模板，从报警消息中快速定位关键信息。

典型应用场景

ZWatch监控系统对云平台核心资源以及事件进行监控，并设置报警接收机制。当核心资源出现异常，ZWatch监控系统将按照报警级别发出实时响应，帮助运维人员快速定位解决问题。

补充说明

- 监控数据在本地默认保留6个月，在高级设置中可自定义设置监控数据保留周期，设置方法如下：

  在**设置** > **高级设置**页面，可设置**监控数据保留周期**，默认为6，单位为月，可设置1到12之间的整数。
- 监控数据在本地默认保留50GB，在高级设置中可自定义设置监控数据保留大小，设置方法如下：

  在**设置** > **高级设置**页面，可设置**监控数据保留大小**，默认为50GB，建议按需设置。
- ZStack私有云支持接收第三方报警消息，需要在**设置** > **全局设置** > **高级设置**中开启**第三方平台报警开关**全局设置，才能使用第三方消息报警器功能。

2.2.6.5 通知服务

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

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

邮箱类型接收端

- 发送到主题的消息都会以邮件方式通过邮箱服务器发送到指定的邮箱地址。
- 用户可提前创建报警消息模板，或使用系统自带模板，将通知邮件以统一格式发出。
- 需提前在当下区域内添加邮箱服务器，并测试邮箱服务器可用。

钉钉类型接收端

- 发送到主题的消息都会以钉钉方式发送到指定的钉钉机器人地址，若指定对象，会通过@电话号码通知相应的钉钉成员。
- 用户可提前创建报警消息模板，或使用系统自带模板，将钉钉消息以统一格式发出。
- 设置钉钉类型的报警消息模板，需遵循Markdown语法。目前钉钉只支持Markdown语法的子集，详情可登录钉钉官网进行了解。

HTTP应用类型接收端

- 发送到主题的消息都会以HTTP POST方式发送到指定的HTTP地址。
- 若指定的HTTP应用已设置了用户名和密码才可访问，需按实填写用户名和密码。

短信类型接收端

- 发送到主题的消息都会以短信方式发送到指定的电话号码；
- 用户需提前创建报警消息模板并设为默认，短信报警消息将按照报警消息模板发送。

2.2.6.6 消息中心

消息中心：ZStack中资源或事件报警消息提示、查看，支持报警消息收敛、报警消息详情跳转报警器/资源详情页等快捷操作，方便用户快速定位问题。

2.2.6.7 操作日志

操作日志：ZStack中用户操作记录。包括三个子页面：已完成、进行中、审计。

进行中子页面针对进行中的操作提供日志查看，可查看该操作的操作描述、任务结果、任务创建时间，可取消正在进行中的任务。

- 通过进度条实时展示任务进度，可点击**取消任务**按钮取消进行中的任务。

  注: 仅部分任务支持取消操作。

- 支持通过输入操作描述搜索正在进行的操作日志。
- 支持调整每页显示的进行中操作日志数量，可选值为：10、20、50、100；且支持翻页操作。
- 消息概览页增加创建时间和完成时间，更直观的显示信息详情。

已完成子页面针对已完成的操作提供日志查看，可查看该操作的操作描述、任务结果、操作员、登录IP、任务创建/完成时间，以及操作返回的消息详情，实现更细粒度管理。

- 支持设置时间段，可查看所设时间段内的已完成操作的日志。
- 支持通过输入操作描述/登录IP，搜索已完成的操作日志。
- 支持csv格式导出操作日志。
- 支持调整每页显示的已完成操作日志数量，可选值为：10、20、50、100；且支持翻页操作。
- 消息概览页增加创建时间和完成时间，更直观的显示信息详情。

审计子页面支持查看资源操作审计和登录操作审计。

- 资源操作审计：
  - 支持设置时间段，可查看所设时间段内调用API的审计信息。

    注: 界面最多显示300条审计信息，请调整合适的时间段进行搜索。

  - 支持通过输入资源类型/资源UUID/API名称/操作员，搜索调用API的审计信息。
  - 支持csv格式导出审计信息。
  - 支持调整每页显示的审计消息数量，可选值为：10、20、50、100；且支持翻页操作。
- 登录操作审计：
  - 支持设置时间段，可查看所设时间段内调用API的审计信息。

    注: 界面最多显示300条审计信息，请调整合适的时间段进行搜索。

  - 支持通过输入操作员/API名称/登录IP/浏览器，搜索调用API的审计信息。
  - 支持csv格式导出审计信息。

- 支持调整每页显示的审计消息数量，可选值为：10、20、50、100；且支持翻页操作。

2.2.6.8 资源编排

资源编排服务是一款帮助云计算用户简化云资源管理和自动化部署运维的服务。通过资源栈模板，定义所需的云资源、资源间的依赖关系、资源配置等，可实现自动化批量部署和配置资源，轻松管理云资源生命周期，通过API和SDK集成自动化运维能力。

如图 *29:* 资源编排所示：

图 29: 资源编排

资源编排具有以下功能优势：

1. 用户只需创建资源栈模板或修改已有模板，定义所需的云资源、资源间的依赖关系、资源配置等，资源编排将通过编排引擎自动完成所有资源的创建和配置；
2. 云平台提供示例模板，也可使用可视化编辑器，快速创建资源栈模板；

3. 可根据业务需要，动态调整资源栈模板，从而调整资源栈以灵活应对业务发展需要；
4. 如果不再需要某资源栈，可一键删除该栈及栈内所有资源；
5. 可重复使用已创建的资源栈模板快速复制整套资源，无需重复配置；
6. 可根据业务场景灵活组合云服务，以满足自动化运维的需求。

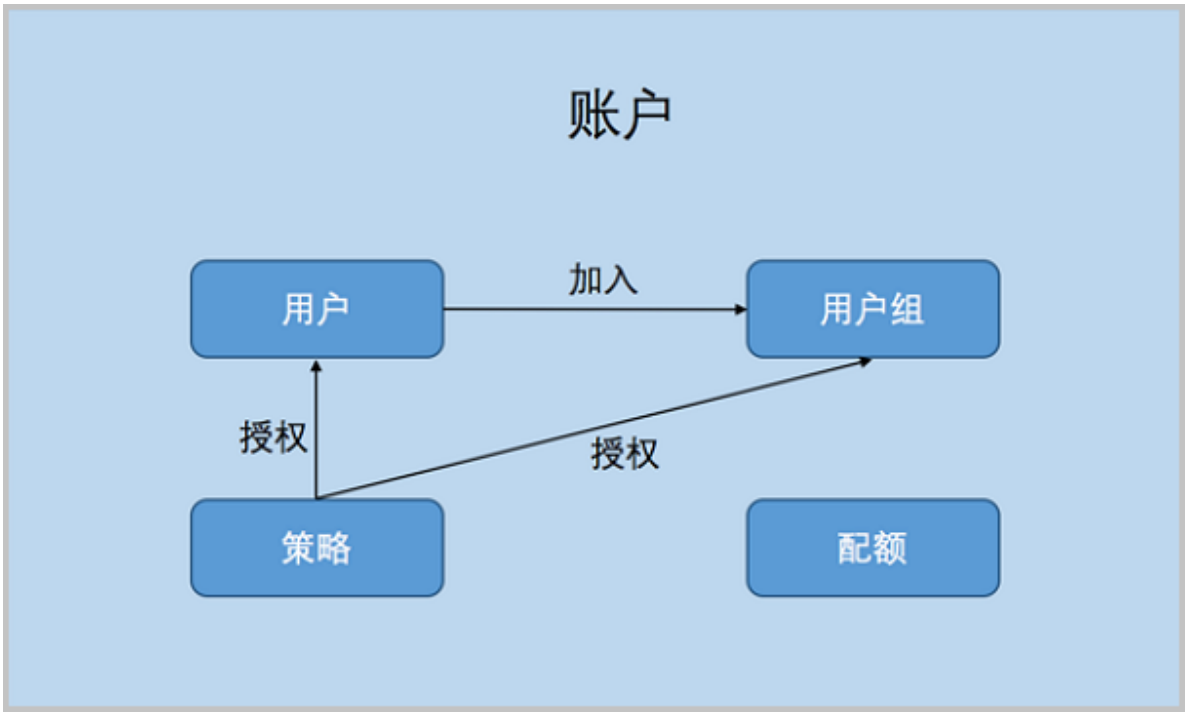
2.2.7 平台管理

2.2.7.1 用户管理

用户管理主要提供了用户对系统资源的访问控制，可实现以细粒度对资源归属及权限控制的划分。

- 用户管理提供账户、用户组、用户的管理，同时涉及策略、配额等概念。
- 用户管理系统的整体结构如图 *30:* 用户管理系统所示：

图 30: 用户管理系统



相关定义

- **账户**：

  作为资源拥有的基本单位，对作用域的资源可以进行创建、删除、分享、召回等操作。账户分为admin管理员账户和普通账户。

- **用户**：

用户账户创建，用于实现更细粒度的权限控制。admin创建的用户，也称之为admin用户，拥有和admin账户相同的全部权限。

- **用户组**：

  普通账户可以通过创建用户组对一组用户进行批量的权限控制。

- **资源配额**：

  简称配额，是admin账户对普通账户的资源总量进行控制的衡量标准。

  - 主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。
  - admin账户可修改以上各参数对各个普通账户进行资源总额的控制。当资源删除后，但还未彻底删除时，会占用主存储资源和云盘数量。

2.2.7.2 计费管理

2.2.7.2.1 账单

账单：按计费价目定义的计费单价和使用时间实时统计并显示所有项目/部门/账户下各资源的计费账单，精准至秒级。

2.2.7.2.2 计费设置

计费价目：以资源规格大小和时间周期为基本单位，定义不同资源单价的价目表。绑定到项目/账户，即可按量生成计费账单。

2.2.7.3 定时

2.2.7.3.1 定时器

定时器是承载定时任务的容器。该功能非常适用于长时间运行的操作，例如，为某个云主机定时创建快照。定时器和定时任务完全解耦，用户可按需创建不同规则的定时器、以及不同的定时任务，并将定时任务灵活加载到定时器或从定时器上卸载。定时器的操作会完整的进入审计中。

定时器执行策略：包括重复执行和按次数执行

- 选择**重复执行**：定时任务按周期无限重复执行
- 选择**选择次数**：定时任务按周期有限次执行，需设置执行次数

注: 对于周期内有限次执行的定时器，当定时任务执行完后，定时器状态将显示为**已完成。**

2.2.7.3.2 定时任务

定时任务是加载到定时器上的任务条目。定时器和定时任务完全解耦，用户可按需创建不同规则的定时器、以及不同的定时任务，并将定时任务灵活加载到定时器或从定时器上卸载。此外，定时任务支持选择性停用/启用/加载/卸载，可灵活处理生产环境中的特殊情况。定时任务的操作也会完整的进入审计中。

定时任务页面显示了定时任务的名称、任务类型、资源名称、开始日期、任务策略、启用状态、定时器状态、定时器和创建日期等信息。

2.2.7.4 标签

标签：支持对资源定制化创建标签，可通过标签类型及标签名称快速过滤出所需资源。

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

注意事项

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

2.2.7.5 应用中心

应用中心提供增强功能以及各类第三方应用快速访问。支持添加各类第三方应用入口URL，便于用户集中管理以及快速打开应用。

2.2.7.6 邮箱服务器

ZStack支持ZWatch监控报警功能，若接收端选择邮件类型，需设置邮箱服务器，用来发送报警邮件。

2.2.7.7 日志服务器

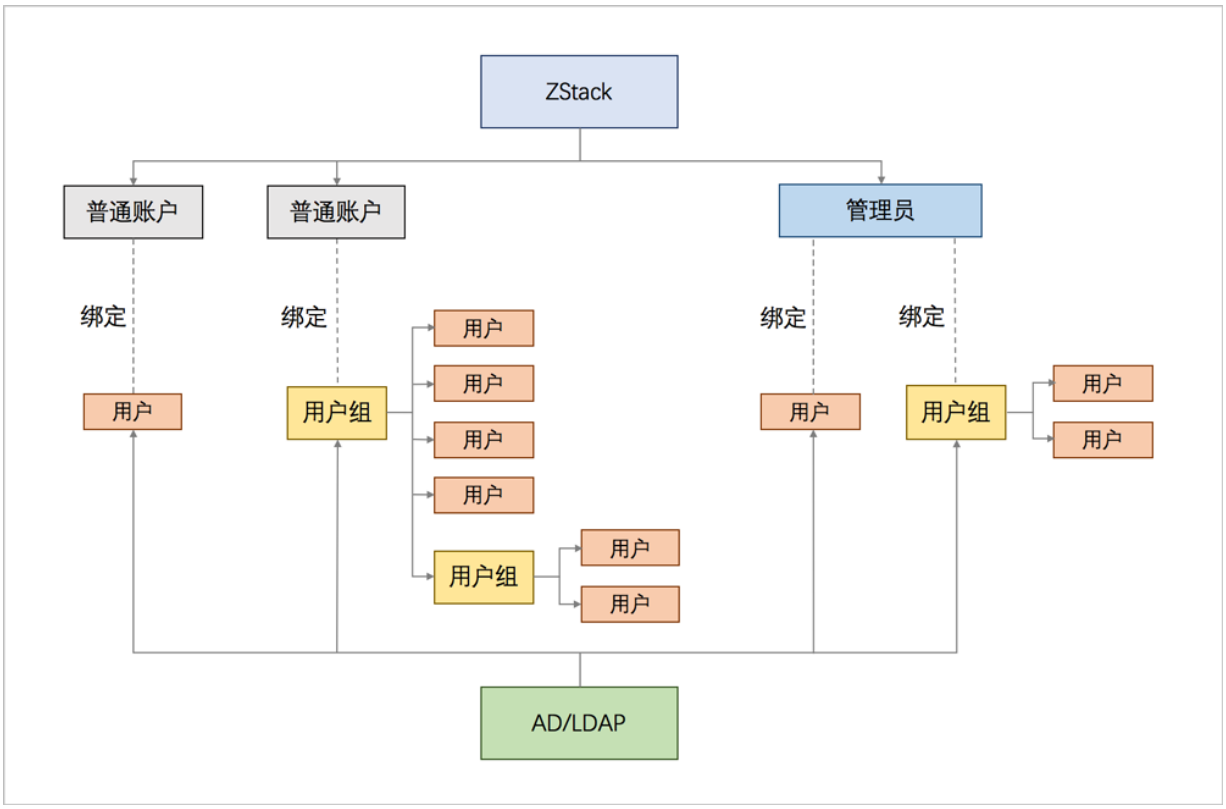
ZStack支持添加日志服务器至云平台，通过该日志服务器，用户可便捷收集管理节点日志，快速定位问题，提高云平台运维效率。

2.2.7.8 AD/LDAP

LDAP（Lightweight Directory Access Protocol）作为轻量级目录访问协议，可提供标准的目录服务。微软的WindowsAD软件（以下简称AD），以及众多流行的Linux发行版中提供的OpenLDAP软件（以下简称LDAP），均是基于LDAP协议的实现，它们为日益多样化的企业办公应用提供了一套独立、标准的登录认证系统。

ZStack账户（普通账户/管理员）与AD/LDAP成员（用户/用户组）的绑定关系如图 *31: ZStack-AD/LDAP绑定关系*所示：

图 31: ZStack-AD/LDAP绑定关系



2.2.7.9 控制台代理

- 控制台代理地址只需要在管理节点修改；
- 默认代理显示的地址为管理节点的IP地址；
- 显示类型为ManagementServerConsoleProxy；
- 只有当状态为**启用**和**已连接**时，才可正常打开控制台访问云主机。

2.2.7.10 管理节点监控

在多管理节点物理机高可用场景下，管理节点监控用于查看各管理节点的健康状态。

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

- 仲裁IP是否可达：

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

- 对端管理节点是否可达：

  监控备管理节点是否可达，若备管理节点不可达，无法与备管理节点通信。

- VIP是否可达：

  监控VIP是否可达，若VIP不可达，主管理节点不能通过VIP访问UI界面。

- 数据库状态：

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

2.2.7.11 IP黑白名单

ZStack支持配置登录IP黑白名单，对云平台登录IP进行防护。用户可按需配置IP黑白名单，从而实现对访客身份的识别和过滤，提升云平台访问控制安全。

2.2.7.12 证书

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

2.2.7.13 Access Key

AccessKey分为本地AccessKey和第三方AccessKey：

- ZStack私有云 本地AccessKey（包括AccessKey ID和AccessKey Secret）是云平台授权第三方用户调用ZStack私有云 API来访问其云资源的安全凭证，需严格保密。
- 第三方AccessKey（包括AccessKey ID和AccessKey Secret）是第三方用户授权云平台用户调用API来访问其云资源的安全凭证，需严格保密。

AccessKey是ZStack私有云对API请求进行安全验证的关键因子，请妥善保管。如果某些AccessKey出现泄漏风险，建议及时删除该AccessKey并生成新的替代AccessKey。

2.2.8 高级功能(Plus)

ZStack提供以下高级功能：

- 企业管理
- 裸金属管理
- 灾备服务
- 迁移服务

高级功能以单独的功能模块形式提供，需提前购买相应的模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

2.2.8.1 企业管理

企业管理主要为企业用户提供组织架构管理，以及基于项目的资源访问控制、工单管理、独立区域管理等功能。企业管理以单独的功能模块形式提供，需提前购买企业管理模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

企业管理账号体系

相关定义：

- **admin**：

  超级管理员，拥有所有权限，通常由IT系统管理员拥有。

- **用户**：

  表示自然人，是企业管理中的最基本单位，拥有平台管理员、项目管理员、部门负责人等多种属性。

- **本地用户**：

  云平台中创建的用户，支持加入组织、加入项目、绑定角色等操作。

- **第三方用户**：

通过第三方认证同步到云平台的用户，支持加入组织、加入项目、绑定角色、变更为本地用户等操作。

- **平台成员**：

  未加入项目的用户，包括平台管理员和普通平台成员。

- **平台管理员**：

  绑定平台管理员角色的用户，带有区域属性的管理员，管控所分配区域的数据中心。

- **部门负责人**：

  组织架构中负责管理部门的用户，拥有查看部门账单权限。

- **项目成员**：

  加入项目的用户，作为项目的基本组成人员，包括项目负责人、项目管理员和普通项目成员。

- **项目负责人**：

  拥有项目负责人角色的用户，负责管理项目的用户，在项目中拥有最高权限。

- **项目管理员**：

  拥有项目管理员角色的用户，协助项目负责人管理项目，同一项目可指定一个或多个项目成员作为项目管理员。

- **成员组**：

  项目成员的集合，对项目成员进行分组管理，支持以成员组为单位进行权限控制。

- **组织**：

  组织是企业管理中组织架构的基本单位，由自定义创建或通过第三方认证同步，分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门。

- **项目**：

  项目用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务。企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。

- **角色**：

  角色表示权限的集合，为用户赋予权限可获得调用相关API进行资源操作的能力。

- **系统角色**：

  系统角色是云平台预置的特殊角色，随版本升级更新权限内容，并自动勾选相关新增权限，不支持手动配置。

- **自定义角色**：

  自定义角色是自定义创建的角色，随版本升级自动更新权限内容，升级后的新增权限需要手动配置。

- **配额**：

  配额是对项目的资源总量进行控制的衡量标准。主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。

- **项目回收策略**：

  创建项目需指定项目回收策略，包括无限制、指定时间回收和指定费用回收三种。

  - 无限制：创建项目后，项目内资源默认一直处于启用状态。
  - 指定时间回收：
    - 项目有效期限不足14天时，项目成员登录云平台后智能操作助手将弹出**项目即将过期**的提醒信息。
    - 项目过期后，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。
  - 指定费用回收：项目费用达到限额时，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。

企业管理的四个子功能

企业管理主要包括**项目管理**、**工单管理**、**独立区域管理**、**第三方认证**四个子功能。

- **项目管理**：

  以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。通过对项目生命周期进行管理（包括确定时间、确定配额、确定权限等），以更细粒度更自动化的方式提高云资源利用率，同时加强项目成员间的协作性。

- **工单管理**：

  为了更高效地为每个项目提供基础资源支持，项目成员（项目负责人/项目管理员/普通项目成员）可对云平台资源提出工单申请，根据每个项目自定义工单审批流程，对工单进行审批，最终由admin或项目负责人审批，支持申请云主机、删除云主机、修改云主机配置、修改项目周期和修改项目配额五种工单类型。

- **独立区域管理**：

区域通常对应某地的一个真实数据中心。在对区域进行资源隔离的基础上，可对每个区域指定相应的区域管理员，实现各地机房的独立管理，同时admin可对所有区域进行巡查和管理。

- **第三方认证**：

  第三方认证是ZStack云平台提供的第三方登录认证服务，支持无缝接入第三方登录认证系统，相应账户系统将直接登录云平台，便捷使用云资源，目前支持添加AD/LDAP服务器。

2.2.8.1.1 组织架构

企业管理为企业用户提供组织架构管理功能，组织架构树以层级折叠方式展示，可直观查看企业组织架构全貌。主要涉及以下概念：

- **组织**：

  组织是企业管理中组织架构的基本单位，由自定义创建或通过第三方认证同步，分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门。

- **用户**：

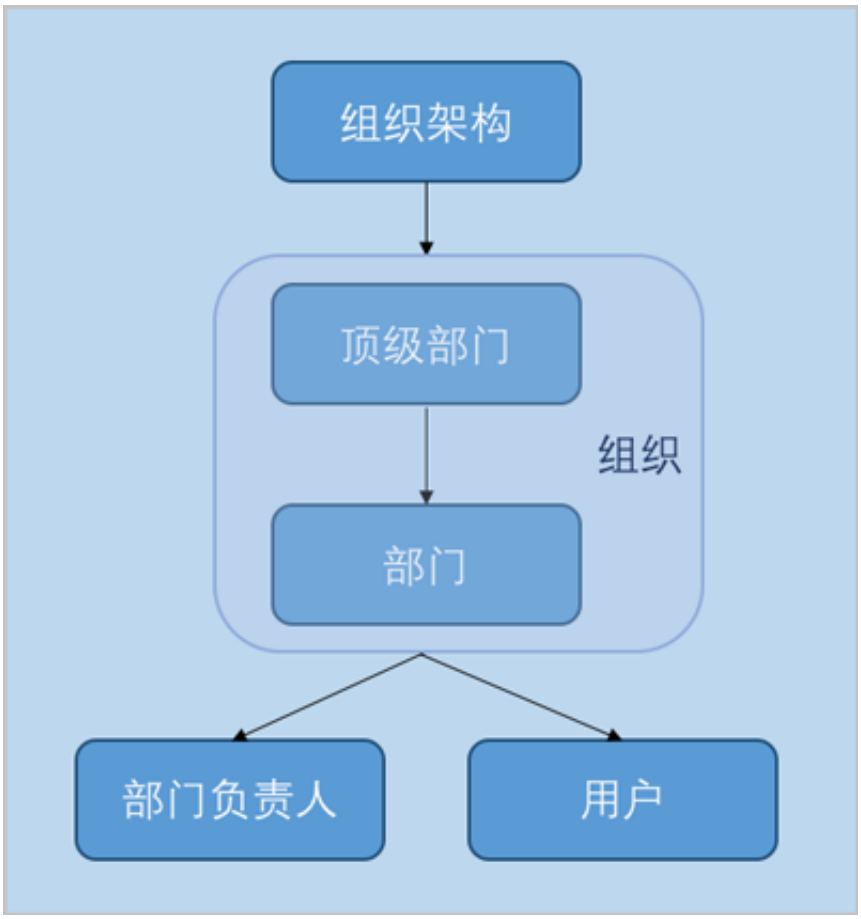
  表示自然人，是企业管理中的最基本单位，拥有平台管理员、项目管理员、部门负责人等多种属性。

- **部门负责人**：

  组织架构中负责管理部门的用户，拥有查看部门账单权限。

组织架构相关概念如图 *32:* 组织架构相关概念所示：

图 32: 组织架构相关概念



2.2.8.1.2 用户

用户表示自然人，是企业管理中的最基本单位，拥有平台管理员、项目管理员、部门负责人等多种属性。

ZStack云平台用户有两种分类方式：

- 方式一：根据来源分类
  - **本地用户**：

    云平台中创建的用户，支持加入组织、加入项目、绑定角色等操作。
  - **第三方用户**：

    通过第三方认证同步到云平台的用户，支持加入组织、加入项目、绑定角色、变更为本地用户等操作。

  注: 企业管理用户需从项目登录入口登录云平台，其中本地用户从本地用户入口登录；第三方用户从AD/LDAP入口登录。
- 方式二：根据是否加入项目分类

- **平台成员**：

  未加入项目的用户，包括平台管理员和普通平台成员。

- **项目成员**：

  加入项目的用户，作为项目的基本组成人员，包括项目负责人、项目管理员和普通项目成员。

2.2.8.1.3 角色

角色表示权限的集合，为用户赋予权限可获得调用相关API进行资源操作的能力。包括系统角色和自定义角色两类。

- **系统角色**：

  系统角色是云平台预置的特殊角色，随版本升级更新权限内容，并自动勾选相关新增权限，不支持手动配置。

- **自定义角色**：

  自定义角色是自定义创建的角色，随版本升级自动更新权限内容，升级后的新增权限需要手动配置。

2.2.8.1.4 第三方认证

第三方认证是ZStack云平台提供的第三方登录认证服务，支持无缝接入第三方登录认证系统，相应账户系统将直接登录云平台，便捷使用云资源，目前支持添加AD/LDAP服务器。

- AD认证：

  AD (Active Directory) 是面向Windows Standard Server、Windows Enterprise Server以及Windows Datacenter Server的目录服务, 为日益多样化的企业办公应用提供了一套独立、标准的登录认证系统。

  通过AD服务器可将AD用户/组织同步到ZStack云平台用户列表/组织架构，并支持使用指定的AD登录属性直接登录ZStack云平台。

- LDAP认证：

  LDAP (Lightweight Directory Access Protocol) 是轻量目录访问协议，可提供标准的目录服务, 为日益多样化的企业办公应用提供了一套独立、标准的登录认证系统。

  通过LDAP服务器可将LDAP用户同步到ZStack云平台用户列表，并支持使用指定的LDAP登录属性直接登录ZStack云平台。

2.2.8.1.5 项目管理

企业管理为企业用户提供项目管理功能。

项目管理：

以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。通过对项目生命周期进行管理（包括确定时间、确定配额、确定权限等），以更细粒度更自动化的方式提高云资源利用率，同时加强项目成员间的协作性。

主要涉及以下概念：

- **项目**：

  项目用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务。企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池。

- **项目成员**：

  加入项目的用户，作为项目的基本组成人员，包括项目负责人、项目管理员和普通项目成员。

- **项目负责人**：

  拥有项目负责人角色的用户，负责管理项目的用户，在项目中拥有最高权限。

- **项目管理员**：

  拥有项目管理员角色的用户，协助项目负责人管理项目，同一项目可指定一个或多个项目成员作为项目管理员。

- **成员组**：

  项目成员的集合，对项目成员进行分组管理，支持以成员组为单位进行权限控制。

- **角色**：

  角色表示权限的集合，为用户赋予权限可获得调用相关API进行资源操作的能力。

- **配额**：

  配额是对项目的资源总量进行控制的衡量标准。主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。

- **项目回收策略**：

  创建项目需指定项目回收策略，包括无限制、指定时间回收和指定费用回收三种。

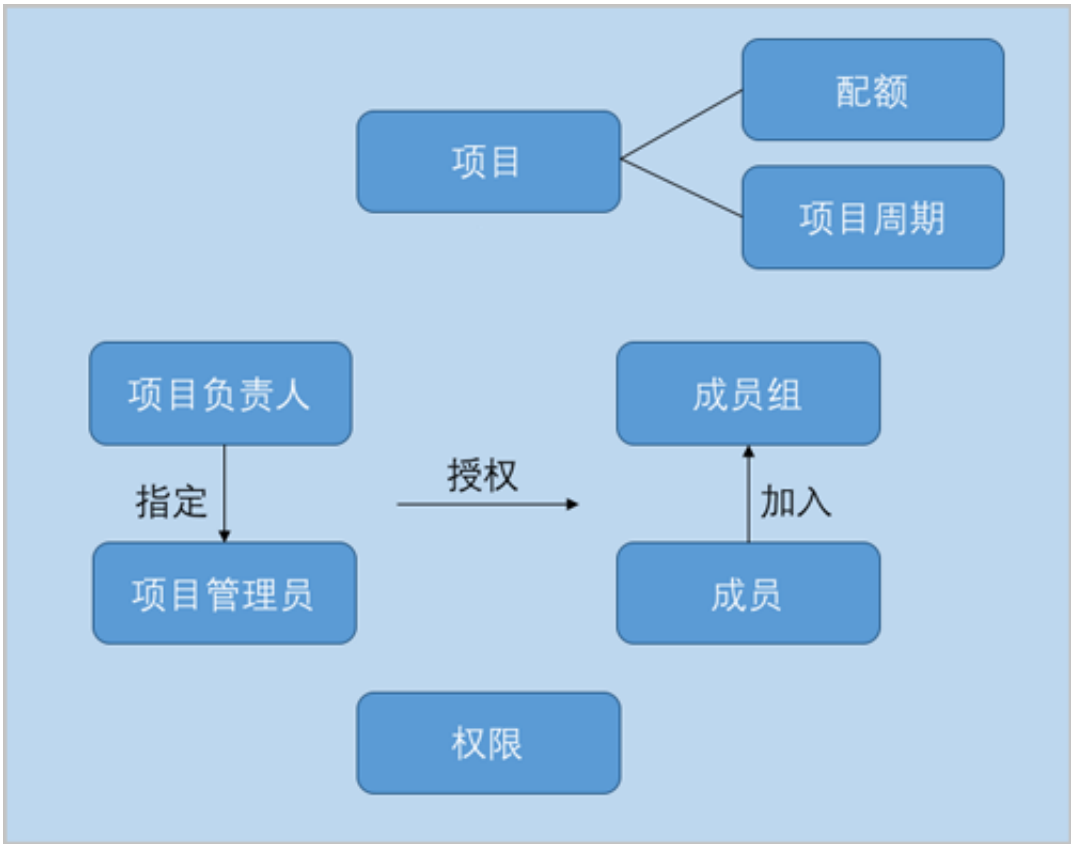
  - 无限制：创建项目后，项目内资源默认一直处于启用状态。
  - 指定时间回收：

- 项目有效期限不足14天时，项目成员登录云平台后智能操作助手将弹出**项目即将过期**的提醒信息。
- 项目过期后，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。

- 指定费用回收：项目费用达到限额时，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。

项目管理相关概念如图 *33:* 项目管理相关概念所示：

图 33: 项目管理相关概念



2.2.8.1.6 工单管理

为了更高效地为每个项目提供基础资源支持，项目成员（项目负责人/项目管理员/普通项目成员）可对云平台资源提出工单申请，根据每个项目自定义工单审批流程，对工单进行审批，最终由admin或项目负责人审批，支持申请云主机、删除云主机、修改云主机配置、修改项目周期和修改项目配额五种工单类型。

2.2.8.2 裸金属管理

ZStack提供裸金属管理服务，可为应用提供专属的物理服务器，保障核心应用的高性能和稳定性。在完成基本的服务器上架以及相关准备工作后，管理员可在UI界面批量部署裸金属设备，部署完成后可使用裸金属设备创建裸金属主机。通过预配置模板，可实现无人值守批量安装裸金属主机操作系统，支持为裸金属主机配置业务网络，并对裸金属主机进行全生命周期管理。

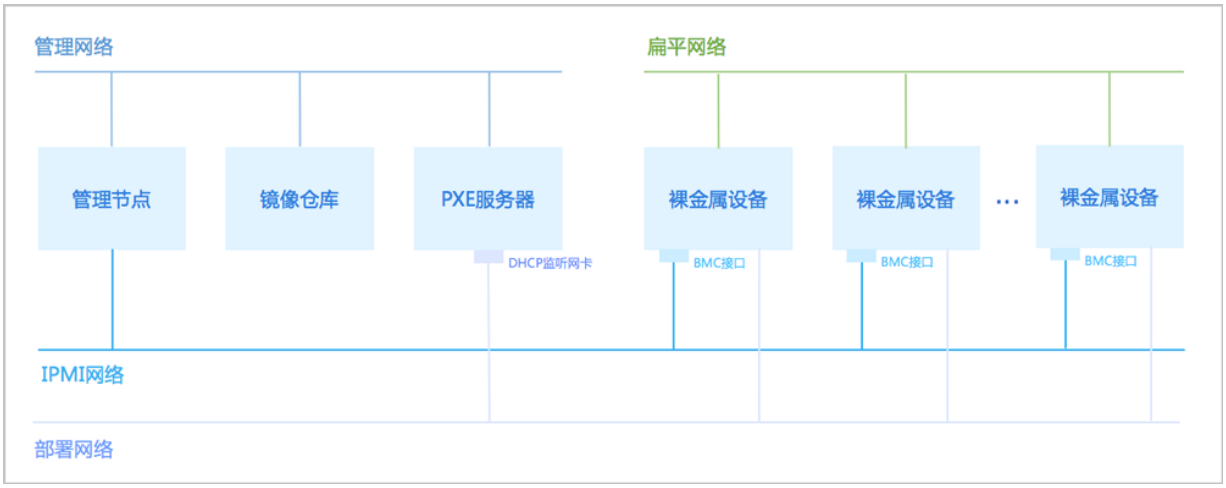
裸金属管理服务以单独的功能模块形式提供，需提前购买裸金属管理模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

基本原理

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

网络拓扑如图 *34:* 裸金属管理网络拓扑所示：

图 34: 裸金属管理网络拓扑



功能优势

裸金属管理服务具有以下功能优势：

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

- 管理员可在UI界面上批量添加裸金属设备，包括：手动添加和模板文件导入两种方式，支持批量添加IPMI地址，高效部署裸金属集群，提升运维效率；
- 通过预配置模板，可快速生成预配置文件，实现无人值守批量安装裸金属主机操作系统；
- 支持自定义安装操作系统，目前支持的操作系统版本包括：本云平台定制版操作系统、以及主流的Linux发行版操作系统（RHEL/CentOS系列、Debian/Ubuntu系列、SUSE/openSUSE系列等）；
- 支持扁平网络场景，同一个二层网络上的裸金属主机和云主机之间可互相访问，无需通过网关进行路由。

典型应用场景

裸金属管理服务适用于以下典型应用场景：

- 高安全严监管场景

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

- 高性能计算场景

  例如超算中心、基因测序等高性能计算场景，对服务器的计算性能、稳定性和实时性要求很高。虚拟化带来的性能损耗和超线程对业务性能有一定影响，部署一定规模的裸金属集群可以满足高性能计算的要求。

- 核心数据库场景

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

2.2.8.2.1 裸金属集群

裸金属集群：为裸金属设备提供单独的集群管理。

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

2.2.8.2.2 部署服务器

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

- 推荐独立部署PXE服务器，满足多管理节点物理机高可用场景需求，且避免单点故障，大幅提升部署效率；
- 要求部署服务器挂载到裸金属集群中；
- 一个裸金属集群只允许挂载一个部署服务器，一个部署服务器可同时挂载到多个裸金属集群；
- 要求部署服务器有足够的存储空间，保存用于PXE部署的镜像；
- 要求部署服务器连接到管理网络，与管理节点连通；
- 要求部署服务器连接到部署网络，与裸金属设备连通；
- 要求部署服务器上的DHCP监听网卡连接到部署网络，并保证该部署网络上不存在其他DHCP服务，以免冲突；
- 要求部署服务器安装最新版ZStack定制版ISO（推荐c76版），否则部署服务器无法通过FTP服务为裸金属设备提供软件包。

2.2.8.2.3 裸金属设备

裸金属设备：可用于创建裸金属主机，通过BMC接口以及IPMI配置进行唯一识别。通过IPMI网络，管理节点可远程控制裸金属设备的开关机、网络启动、磁盘启动等行为。支持admin在UI界面上完成所有裸金属设备的批量部署。

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

2.2.8.2.4 预配置模板

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

- 需提前在云平台中准备好预配置模板；
- 预配置模板包括以下两种类型：
  - 系统模板：由云平台默认提供，包含基础的系统变量，适用于简单的无人值守部署场景；

- 自定义模板：支持上传自定义模板文件，采用UTF8编码格式，除了包含基础的系统变量，可按需自定义变量，适用于复杂的无人值守部署场景。

2.2.8.2.5 裸金属主机

裸金属主机：裸金属设备的云实例。裸金属设备添加完成后可用于创建裸金属主机。

- 通过预配置模板，可快速生成预配置文件，实现无人值守批量安装裸金属主机操作系统；
- 支持自定义安装操作系统，目前支持的操作系统版本包括：本云平台定制版操作系统、以及主流的Linux发行版操作系统（RHEL/CentOS系列、Debian/Ubuntu系列、SUSE/openSUSE系列等），要求为ISO格式，且为非Live CD；
- 支持为裸金属主机配置业务网络，目前支持扁平网络场景，同一个二层网络上的裸金属主机和云主机之间可互相访问，无需通过网关进行路由。需提前将裸金属设备所在的裸金属集群挂载相应的二层网络。

2.2.8.3 灾备服务

灾备服务以业务为中心，融合定时增量备份、定时全量备份等多种灾备技术到ZStack私有云平台中，支持本地灾备、异地灾备、公有云灾备多种灾备方案，用户可根据自身业务特点，灵活选择合适的灾备方式。

灾备服务以单独的功能模块形式提供，需提前购买灾备服务模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

典型灾备场景

灾备服务模块提供本地灾备、异地灾备、公有云灾备三种典型灾备场景。

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

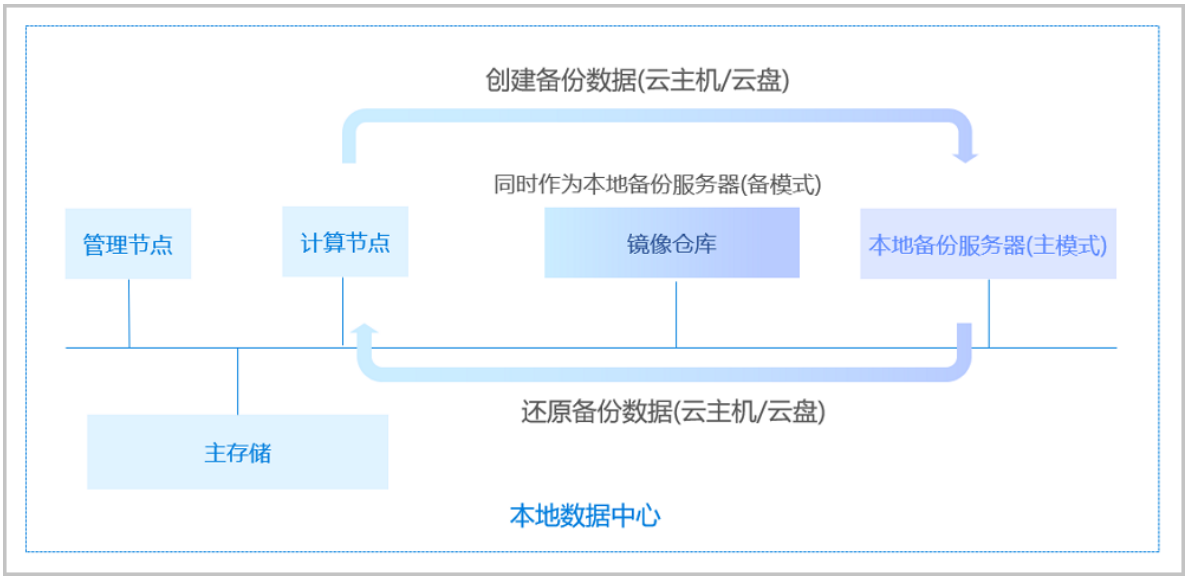
- **本地灾备**：

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

  当发生本地数据误删，或本地主存储中数据损坏等情况，可将本地备份服务器中的备份数据还原至本地。

如图 *35:* 本地灾备场景*1*所示：

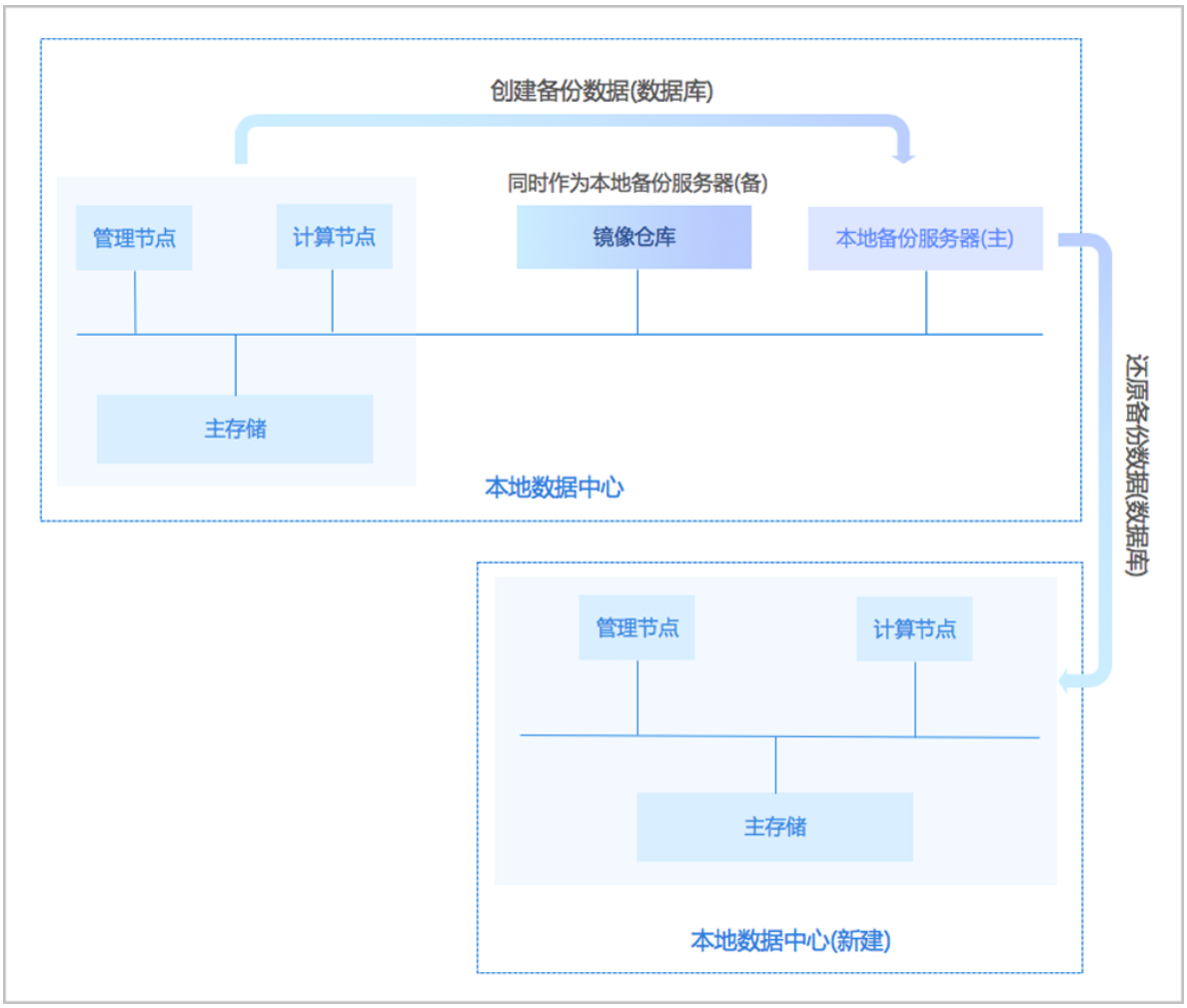
图 35: 本地灾备场景1



当本地数据中心发生灾难时，完全可依赖本地备份服务器重建数据中心并恢复业务。

如图 *36:* 本地灾备场景*2*所示：

图 36: 本地灾备场景2



更多详情可参考本地灾备实践章节。

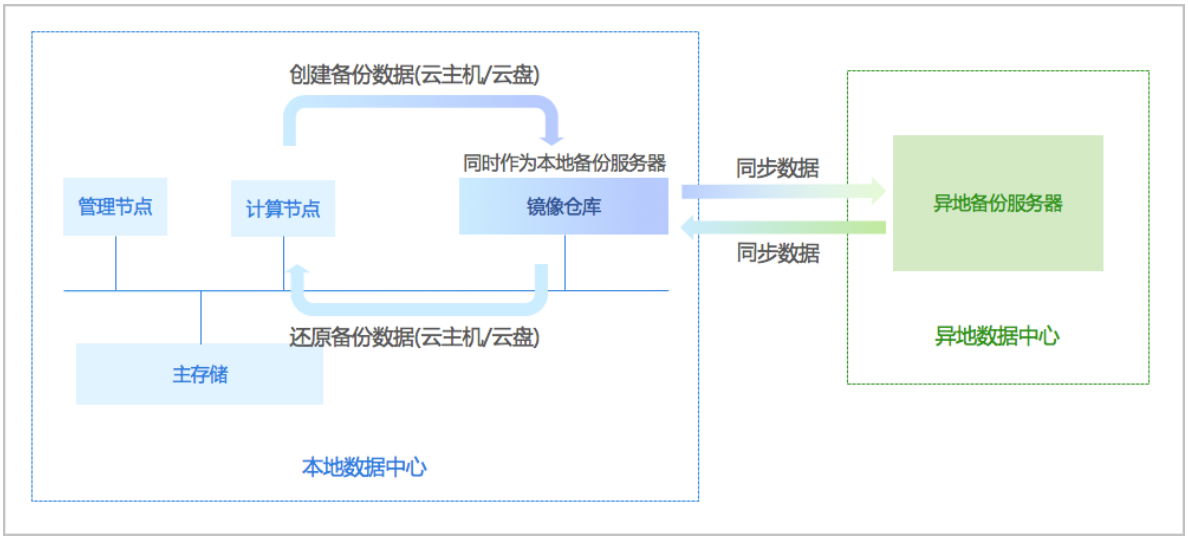
- **异地灾备**：

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

  当发生本地数据误删，或本地主存储中数据损坏等情况，可将异地备份服务器中的备份数据还原至本地。

  如图 *37: 异地灾备场景1*所示：

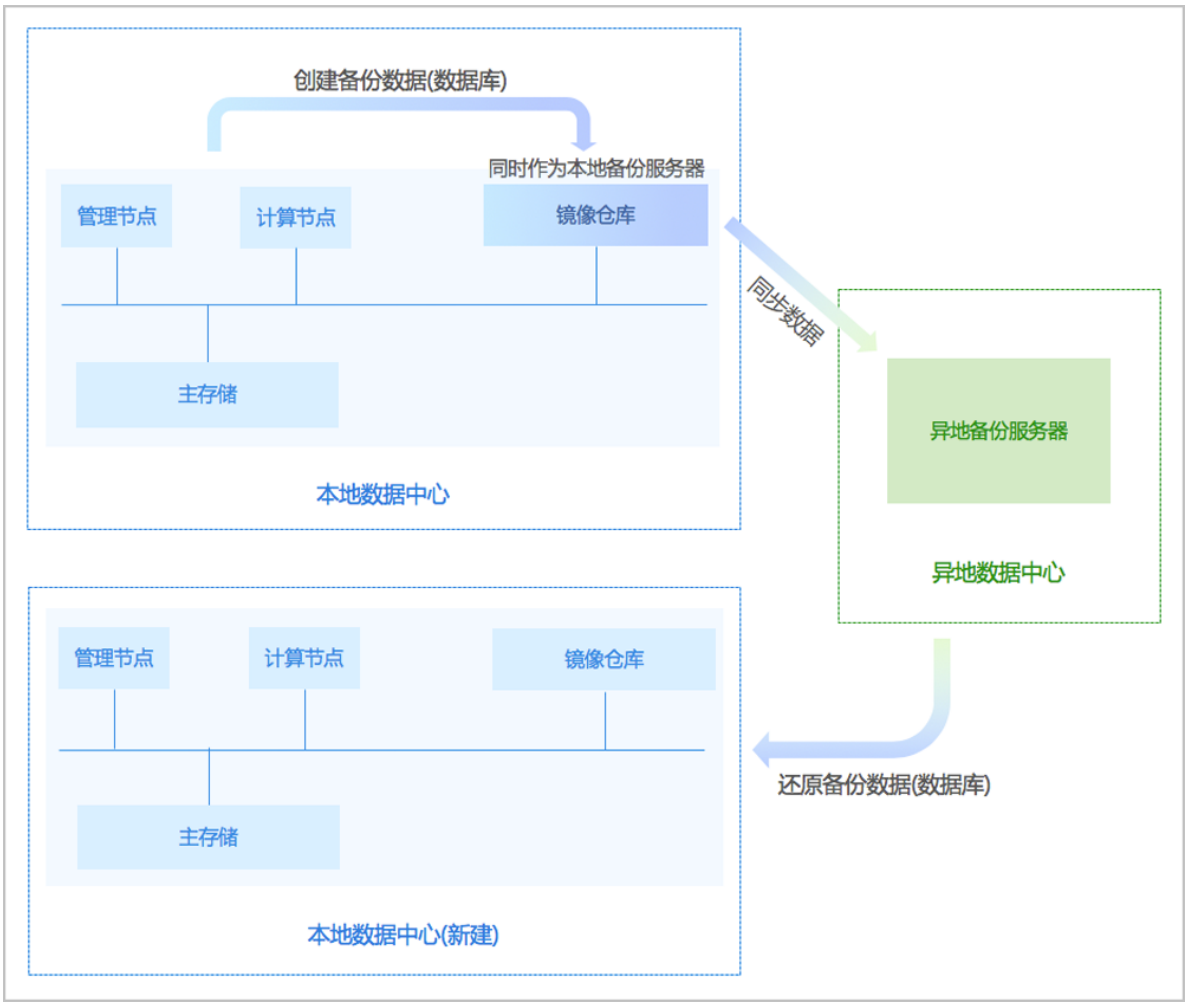
  图 37: 异地灾备场景1



当本地数据中心发生灾难时，完全可依赖异地备份服务器重建数据中心并恢复业务。

如图 *38:* 异地灾备场景*2*所示：

图 38: 异地灾备场景2



更多详情可参考异地灾备实践章节。

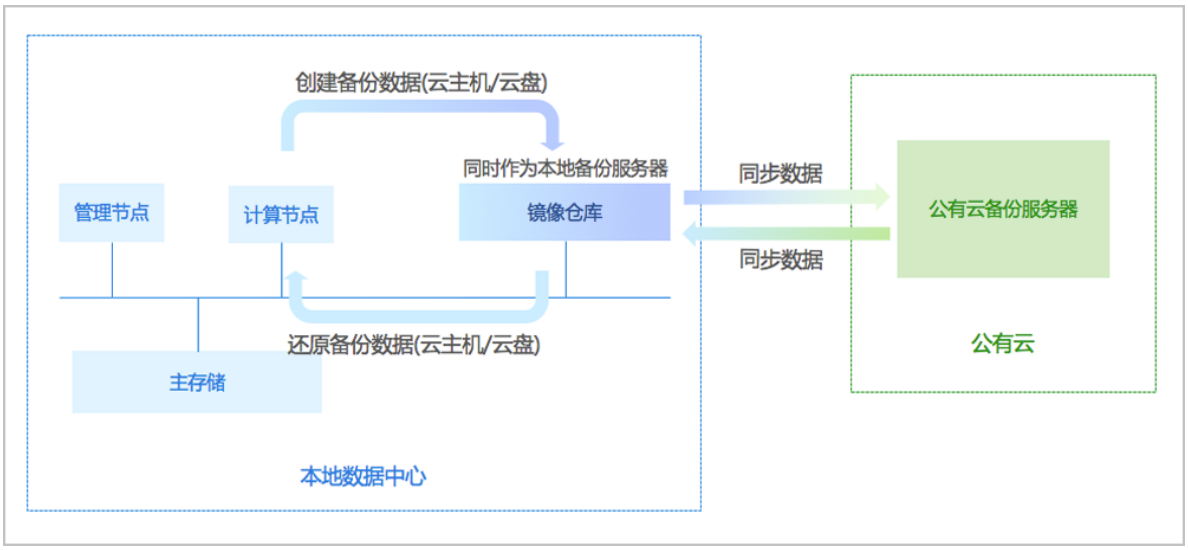
- **公有云灾备**：

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

  当发生本地数据误删，或本地主存储中数据损坏等情况，可将公有云备份服务器中的备份数据还原至本地。

  如图 *39: 公有云灾备场景1*所示：

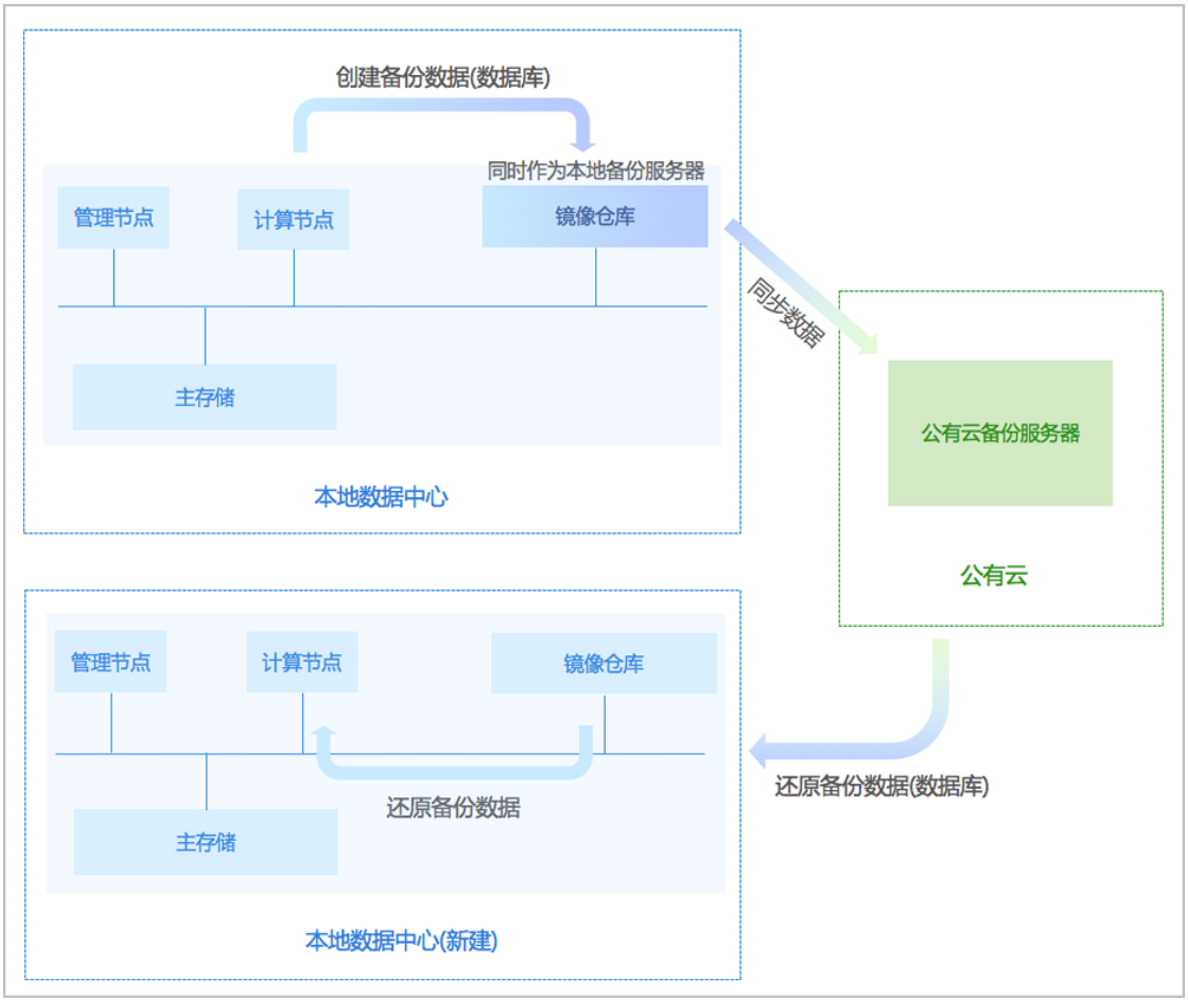
  图 39: 公有云灾备场景1



当本地数据中心发生灾难时，完全可依赖公有云备份服务器重建数据中心并恢复业务。

如图 *40:* 公有云灾备场景*2*所示：

图 40: 公有云灾备场景2



更多详情可参考公有云灾备实践章节。

2.2.8.3.1 备份任务

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

- 备份任务概览页展示了云主机、云盘、数据库的备份任务执行情况，并以可视化视图统计某一时间段内的备份任务，可以直观全面的获取全部备份任务信息。
- 通过备份任务，可将本地云主机/云盘资源定时备份到指定的本地存储服务器，同时备份数据可同步到指定的远端备份服务器（异地备份服务器/公有云备份服务器）。
  - 需提前添加本地备份服务器到云平台，若指定两个本地备份服务器，支持主备无缝切换；
  - 如需备份到远端，需提前添加远端备份服务器到云平台，只允许添加一个远端备份服务器；
  - 对于本地云主机/云盘的备份任务：
    - 单个备份任务支持多资源；
    - 用户可按需设置增量备份和全量备份策略；
    - 提供备份进度条，可随时查看资源备份状态；
    - 支持对备份任务更新备份策略；
    - 支持立即执行一次备份任务；
    - 支持对备份任务设置网络/磁盘QoS；
    - 创建备份任务提供富文本模式，用户可在操作过程中随时获取帮助信息；
    - 备份任务创建后支持立即备份一次；
    - 已关机的云主机错过备份，开机后会自动执行一次补充备份（技术预览）
    - 暂不支持共享云盘做定时备份；
  - 单个云主机/云盘资源支持立即备份，随时备份重要业务。
- 通过备份任务，可将管理节点数据库（简称数据库）定时备份到指定的本地存储服务器，同时备份数据可同步到指定的远端备份服务器（异地备份服务器/公有云备份服务器）。
  - 需提前添加本地备份服务器到云平台，若指定两个本地备份服务器，支持主备无缝切换；
  - 如需备份到远端，需提前添加远端备份服务器到云平台，只允许添加一个远端备份服务器；

2.2.8.3.2 本地备份数据

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

- 备份数据可还原至本地，或同步到远端备份服务器中；
- 还原数据库过程中，刷新浏览器会导致UI界面无法显示，但还原过程不受影响；
- 本功能模块支持对管理节点数据库中保存的数据进行备份与还原，操作日志以及监控信息等数据不在支持范围内。

2.2.8.3.3 本地备份服务器

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

- 可直接使用本地数据中心已部署的镜像仓库作为本地备份服务器；
- 也可部署新的本地备份服务器；
- 允许添加多个本地备份服务器；
- 当备份任务指定多个本地备份服务器时，支持主备无缝切换；
- 支持清理已被彻底删除的无效备份数据和过期的临时数据，释放存储空间；
- 备份到本地备份服务器上的备份数据可在详情页中查看。

2.2.8.3.4 远端备份服务器

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

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

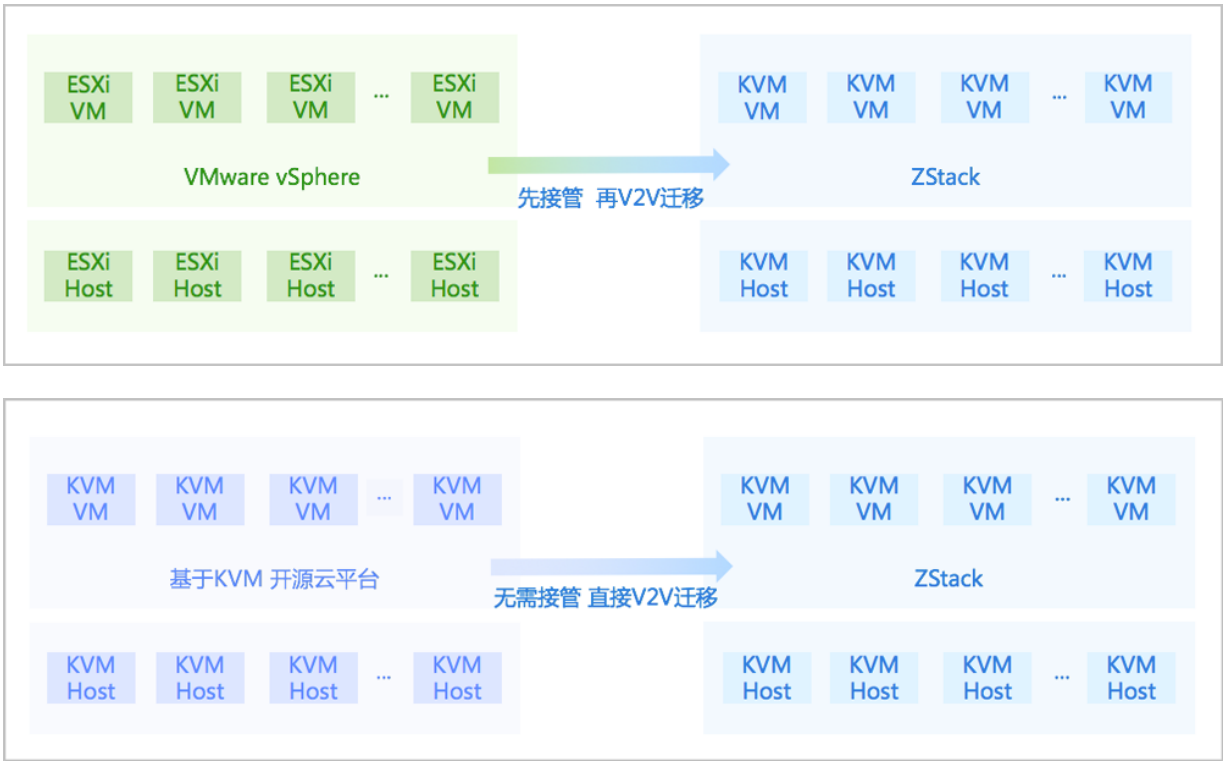
2.2.8.4 迁移服务

ZStack提供V2V迁移服务，可将其它虚拟化平台的云主机系统及数据完整迁移至当前云平台。目前支持：

- 将已接管的vCenter云主机迁移至当前云平台，支持迁移的源vCenter平台版本包括：5.0、5.1、5.5、6.0、6.5、6.7，且vCenter服务器（vCenter Server）和ESXi主机（ESXi Host）版本需保持一致。
- 将基于KVM的源云平台的云主机迁移至当前云平台。

如图 *41: V2V迁移*所示：

图 41: V2V迁移



V2V迁移服务以单独的功能模块形式提供，需提前购买迁移服务模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

V2V迁移服务具有以下功能优势：

- 支持对云主机进行一键式批量的V2V迁移；
- 用户只需添加迁移服务器并创建迁移任务，其余工作均交由云平台执行；
- 支持对迁移服务器设置单独的迁移网络以及网络QoS，控制传输瓶颈，提高迁移效率；
- 创建迁移任务过程中，支持对目标云主机进行自定义配置；
- 整个迁移过程可通过直观可视化的UI界面进行监控和管理。

2.2.8.4.1 V2V迁移

目前支持将VMware或KVM源云平台的云主机迁移至当前云平台。

源云平台: VMware

通过创建迁移任务，可将已接管的vCenter云主机迁移至当前云平台。

- 迁移前，请对已接管的vCenter执行**同步数据**操作，将vCenter资源最新状态手动同步至本地；

- 用户可对云主机进行批量的V2V迁移，并对迁移的目标云主机进行自定义配置；
- 支持迁移的源vCenter平台版本包括：5.0、5.1、5.5、6.0、6.5、6.7，且vCenter服务器（vCenter Server）和ESXi主机（ESXi Host）版本需保持一致；
- 迁移的源vCenter云主机系统支持：RHEL/CentOS 4.x/5.x/6.x/7.x、SLES 11/12/15、Ubuntu 12/14/16/18、Windows 7/Server 2003 R2/Server 2008 R2/Server 2012 R2/Server 2016；
- 云主机在V2V迁移过程中将强制关闭，注意业务影响；

注: 云主机会先尝试温和关闭，若失败再执行强制关闭。

- 迁移的源主存储类型无限制，目标主存储支持LocalStorage、NFS、Ceph以及Shared Block类型；
- 对于Windows云主机，迁移过程中支持自动安装WindowsVirtIO驱动，提高网卡、磁盘工作效率；
- 支持UEFI引导的源云主机进行V2V迁移，迁移后仍使用UEFI引导启动。

源云平台: KVM

通过创建迁移任务，可将基于KVM的源云平台的云主机迁移至当前云平台。

- 用户可对云主机进行批量的V2V迁移，并对迁移的目标云主机进行自定义配置；
- 支持对正在运行或已暂停的云主机进行迁移，待迁移的云主机请不要关机；
- 支持UEFI引导的源云主机进行V2V迁移，迁移后仍使用UEFI引导启动；
- 迁移的源主存储类型无限制，目标主存储支持LocalStorage、NFS、Ceph以及Shared Block类型；
- 针对不同类型源主存储/目标主存储，libvirt和Qemu版本需满足以下要求：
  - 源主存储或目标主存储任一为Ceph类型：libvirt要求1.2.16及以上版本，Qemu要求1.1及以上版本，才可进行V2V迁移；
  - 源主存储和目标主存储均为非Ceph类型：libvirt要求1.2.9及以上版本，Qemu要求1.1及以上版本，才可进行V2V迁移。

2.2.8.4.2 迁移服务器

V2V迁移需要指定目标集群内的物理机作为迁移服务器。

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

表 4: 迁移服务器最低配置建议

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

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

3 产品功能

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

ZStack企业版功能列表：

类别	特性	ZStack企业版
区域	管理多个区域	• 云平台支持创建/管理多个区域，推荐将一个物理数据中心归为一个区域管理 • 支持区域隔离，每个区域可建立独立的集群、主存储、网络等资源
vCenter	管理vCenter	通过VMware提供的公开API接口，接管多个VMware vCenter。良好地兼容和管理VMware vCenter Server虚拟化管理平台部分功能，实现多虚拟化平台的统一管理。 • 支持接管VMware vCenter Server管理的vSphere服务器、云主机、云盘、镜像资源，并支持在虚拟数据中心对接管的资源执行常用操作 • 支持以vCenter为单位查看云主机、云盘、镜像等资源 • 支持手动同步全部/某个vCenter数据，保证信息一致性 • 支持全局设置中配置vCenter自动同步数据，配置完成后支持周期性自动同步全部vCenter数据
	vCenter多租户管理	租户（普通账户/项目成员）支持管理已接管vCenter中的资源。 • 租户支持对已接管vCenter中的云主机、云盘资源执行常用操作 • 租户支持使用admin共享的vCenter网络、镜像资源 • 租户视角的首页界面支持分别展示KVM和vCenter云主机的使用量 • 租户视角支持分别展示KVM和vCenter账单信息 • 项目成员支持通过工单审批方式申请vCenter云主机
	vCenter资源池	• 已接管vCenter支持同步资源池及相关云主机信息，以层级形式展示 • 支持显示资源池的CPU容量限制、内存容量限制等资源配额信息
	ESX云主机	• 支持ESX云主机相关生命周期管理，包括：创建、启动、停止、重启、暂停、恢复、关闭电源、删除

类别	特性	ZStack企业版
		• 支持ESX云主机相关常规操作，包括：迁移、克隆、修改计算规格、设置高可用、打开控制台、设置控制台密码
	网络	• 支持基于vSwitch/dvSwitch交换机创建网络 • 支持创建公有网络和私有网络，其中私有网络包括扁平网络、云路由两种类型 • 云路由支持所有网络服务，包括：虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道等
	存储	支持按datastore区分主存储和镜像服务器
	镜像	支持镜像相关生命周期管理，包括：添加、删除、启用、停用
	物理机	支持物理机相关生命周期管理，包括：维护模式
	云盘	支持云盘相关生命周期管理，包括：创建、删除、加载、卸载
	实时性能监控	采集ESX云主机CPU、内存、存储和网络相关数据，可视化方式实时显示性能监控图表
集群	存储架构	集群内使用同构存储服务，将存储服务加载到集群，提供云主机高可用功能
	物理机	集群内管理的物理机。支持实时查看物理机全部CPU使用率、物理机全部内存使用百分比、物理机全部网卡出入速度和物理机全部磁盘读/写IOPS
	云主机	集群内管理的云主机。支持实时查看云主机全部CPU使用率、云主机全部内存已用百分比、云主机全部网卡出入速度和云主机全部磁盘读/写IOPS
	集群功能	• 提供高可用特性，支持按照物理机CPU架构定义集群属性 • 支持根据集群部署规模（包括：small、medium、large）适当优化配置参数
	网络服务	• 支持将VLAN、VXLAN网络加载到相同集群并统一管理，并提供网络自助服务（IP池管理和弹性网络） • 支持对集群指定迁移网络
	动态资源调度	以集群为单位监控物理机CPU或内存负载情况，根据配置的调度策略给出调度建议，用户可按照调度建议手动迁移云主机，平衡集群负载的同时有效提高云平台稳定性
	高级设置	以集群为粒度，对集群内资源配置参数：

类别	特性	ZStack企业版
		• 降低已有全局配置优先级，为集群内资源独立配置参数。例如：内存超分率、物理机保留内存、CPU超分率、云主机Hyper-V开关等 • 无对应全局设置，仅支持以集群为粒度配置参数。例如：集群大页开关、动态资源调度开关、Zero Copy开关
物理机	虚拟化	支持KVM和VMware虚拟化技术
	定制版 ISO	定制版ISO提供c76 ISO和c74 ISO两个版本： • c76 ISO是基于CentOS 7.6深度定制的ZStack定制版ISO，新装用户推荐使用此版本 • c74 ISO是基于CentOS 7.4深度定制的ZStack定制版ISO，已使用c74 ISO部署ZStack的用户，需使用此版本升级
	资源设定超分	支持设置CPU、内存、主存储超分比例，适应云环境资源使用场景
	嵌套虚拟化	支持KVM/ESXi嵌套虚拟化：云主机内部可开启CPU硬件虚拟化功能
	实时监控	采集物理机CPU、内存、磁盘IO、磁盘容量和网络相关数据，可视化方式实时显示性能监控图表
	停用与启用	• 设置物理机可用属性，方便自定义管理物理机 • 物理机停用后，其上不允许继续创建资源，已有资源不受影响
	维护模式	• 设置物理机维护状态，方便物理机计划性运维等场景 • 物理机进入维护模式后，其上云主机将会自动迁移（共享存储）
	物理GPU透传	以组为单位整体透传物理GPU设备上携带的全部外接设备（包括：GPU显卡、GPU声卡、其它GPU上的小设备），有效提高云主机高性能计算和图形处理能力
	vGPU	• 同时支持NVIDIA和AMD显卡虚拟化切割成vGPU • 支持指定规格和指定设备两种方式为云主机加载vGPU
	SR-IOV	支持基于SR-IOV规范，将一张物理网卡虚拟化切割成多张VF类型网卡，直接分配给云主机使用。实现更灵活弹性的资源使用、提高资源利用率、以及节约成本。
	PCI设置白名单	支持通过白名单的方式将任意VT-D设备透传给云主机使用，例如：Ali-NPU卡、IB卡（PCI模式）、FPGA卡等

类别	特性	ZStack企业版
	USB透传	• 将USB设备直接透传给云主机使用，满足多种USB应用场景 • 支持直连和转发两种透传方式
	Intel EPT硬件辅助	支持关闭Intel EPT硬件辅助虚拟化，有效解决CPU型号过旧导致创建云主机故障的问题
	密码加密存放	支持物理机密码加密存放
	操作日志	展示物理机操作过程的事件登录操作相关审计信息
	导出CSV文件	支持将物理机列表导出为CSV表格，方便统计分析处理
云主机	批量操作	批量管理云主机
	创建云主机	• 提供多种策略创建云主机，高效利用资源 • 支持通过数据云盘作为系统盘镜像创建云主机
	云主机生命周期	支持创建、停止、启动、重启、关闭电源、删除、暂停、恢复等基本生命周期控制
	根云盘在线扩容	云主机根云盘支持在线扩大容量，方便修改云主机配置
	数据云盘在线扩容	云主机数据云盘支持在线扩大容量，即时生效
	云主机控制台	• 不依赖远程工具，即可通过终端方式访问云主机 • 控制台支持SPICE、VNC、SPICE+VNC三种模式，其中，SPICE协议新增SSL加密通道，进一步保障桌面安全 • 支持设置控制台密码，并支持配置密码复杂度、密码长度等密码策略，以及是否强制设置VNC控制台密码
	云主机快照	• 做重要操作前，对根云盘或数据云盘在特定时间点进行临时状态保留，方便出现故障后迅速回滚。 • 包括单盘快照和快照组两种快照类型，其中快照组支持以组为单位批量恢复 • 在线快照（支持ImageStore/Ceph类型的镜像服务器） • 关机快照（支持ImageStore/Sftp/Ceph类型的镜像服务器） • 支持恢复快照后自动启动云主机 • 支持批量删除云主机快照
	CPU绑定	将云主机的逻辑CPU与计算节点的物理CPU绑定
	在线修改密码	支持Windows/Linux的云主机在线修改密码
	在线创建镜像	运行中的云主机在线创建镜像
	QGA开关	灵活控制qemu guest agent的状态

类别	特性	ZStack企业版
	RDP模式开关	针对VDI用户界面，启用后默认以RDP模式打开控制台
	显卡切换	支持选择云主机显卡类型，包括：qxl、cirrus、vga
	显卡透传	支持将NVIDIA/AMD的GPU设备直接透传给云主机使用
	User Data导入	支持创建云主机时导入User Data
	克隆（不带数据云盘）	• 基于云主机快速克隆若干个云主机 • 在线克隆（支持ImageStore/Ceph类型的镜像服务器） • 关机克隆（支持ImageStore/Ceph类型的镜像服务器）
	整机克隆（带数据云盘）	• 同时克隆云主机的根云盘和数据云盘，其中，加载共享云盘的云主机不支持整机克隆 • 仅支持ImageStore类型的镜像服务器 • LocalStorage/NFS/SMP/Ceph/Shared Block类型的主存储，支持在线/暂停/关机克隆
	更换系统	云主机关机状态下支持修改操作系统
	重置云主机	将云主机恢复到镜像初始状态，并覆盖根云盘内所有数据
	根云盘扩容	支持在线/关机状态下对云主机根云盘扩容，方便修改云主机配置
	基于ISO部署	• 基于ISO系统光盘部署云主机，引导安装系统 • 同一云主机支持加载多个ISO，提升业务部署效率
	基于模板部署	基于系统模板创建云主机
	BIOS模式	• 创建云主机会继承所选镜像的BIOS模式，包括Legacy和UEFI • 创建云主机镜像、克隆云主机操作，将继承原镜像BIOS模式 • 云主机详情页支持动态修改BIOS模式
	创建云主机镜像	基于当前云主机，制作模板镜像，方便定制化批量创建云主机。 • 支持在线创建云主机镜像（支持ImageStore/Ceph类型的镜像服务器） • 支持关机创建云主机镜像（支持ImageStore/Sftp/Ceph类型的镜像服务器）
	自定义MAC地址	• 创建云主机时支持指定MAC地址 • 已创建云主机支持修改MAC地址
	云主机启动顺序	调整云主机的启动顺序，用于切换ISO引导，支持光驱、硬盘、网络三种启动方式

类别	特性	ZStack企业版
	动态加载/卸载云盘	云主机支持动态加载/卸载云盘，支持优化驱动模型，支持SCSI WWN号唯一识别
	动态加载/卸载网卡	云主机支持动态加载/卸载网卡，支持设置默认网卡
	动态加载/卸载虚拟光驱	云主机支持动态加载/卸载虚拟光驱，支持为各个光驱加载卸载ISO，满足用户需求的同时，增强灵活度，提升用户操作体验
	加载GPU卡	支持创建云主机时加载GPU设备
	共享云盘	Ceph存储或Shared Block主存储时，多个云主机支持共享使用同一数据云盘
	实时性能监控	主流Linux/Windows以及国产操作系统均支持云主机负载实时监控： • 外部监控：由Libvirt从物理机采集云主机的CPU、内存、磁盘IO和网络相关数据，提供图形可视化 • 内部监控：由agent从直接云主机内部采集CPU、内存、磁盘容量的相关数据，提供图形可视化（支持通过性能优化工具手动安装agent）
	高可用特性	当物理机故障时，云主机支持自动重启，且支持UI上展示恢复过程
	在线修改云主机CPU/内存	无需重启云主机，即可在线修改CPU/内存配置
	实时更新云盘和网络QoS	云主机根云盘和网卡提供限速能力，避免单个云主机占用过量资源
	SSH密钥注入	• Linux和BSD操作系统支持SSH密钥注入 • 云主机支持创建、删除密钥 • 默认禁用vyos ssh认证方式登录，提升安全性
	自定义计算规格	支持自定义计算规格，满足各种应用资源消耗特性
	自定义标签	支持自定义标签，满足查询和编写定时任务
	自定义主列表	支持自定义云主机列表的展示条目，同时提供自定义云主机列表内容的CSV导出
	资源删除保护	云主机删除后，移入回收站，可按需恢复或彻底删除
	冷迁移	• 本地主存储上的云主机支持关机迁移 • 可选择按目标计算节点负载高低迁移云主机/云盘

类别	特性	ZStack企业版
	在线迁移	• 所有主存储类型上的云主机支持在线迁移 • 可选择按目标计算节点负载高低迁移云主机/云盘 • 针对Windows故障转移群集做了特定支持，云主机热迁移不会产生任何不良影响
	存储迁移	• 支持云平台内云主机跨同类型主存储的冷迁移： - 多NFS主存储之间的云主机支持不带云盘跨存储设备冷迁移 - 多Ceph主存储之间的云主机支持不带云盘跨存储设备冷迁移 - 多Shared Block主存储之间的云主机支持跨存储设备冷迁移，且支持同时迁移加载的云盘（共享云盘除外） • 支持云主机跨不同类型主存储的热迁移（不带快照），包括：Ceph主存储-SharedBlock主存储、本地存储-SharedBlock主存储、本地存储-Ceph主存储 • UI界面支持显示存储迁移保留的原始数据，支持清理操作。确保存储迁移后的数据完整无损时，可手动清理数据，释放存储空间
	跨集群高可用策略	云主机\VPC路由器支持设置跨集群高可用策略，云主机\VPC路由器自动迁移将被限制在策略生效时所在集群
	操作日志	展示云主机操作过程事件、登录操作相关审计信息
	性能优化工具	• Windows/Windows Virtio操作系统提供性能优化工具，支持一键安装Virtio驱动、agent、QGA等 • Linux操作系统提供性能优化工具，支持安装agent，安装后可从云主机内部获取监控数据
	USB重定向	将VDI客户端上的USB设备重定向至云主机使用
	导出CSV文件	云主机列表支持导出为CSV表格，方便统计分析处理
	防欺诈模式	• 全局设置云主机防欺诈模式，提升安全性 • 为单个云主机单独设置防欺诈模式开关，提升灵活度
	云主机优先级	• 提供正常和高两种云主机优先级。当出现资源竞争时，优先保证优先级为**高**的云主机的资源使用 • 默认提高VPC路由器的资源优先级，使VPC路由器的资源优先级高于云主机

类别	特性	ZStack企业版
	云主机多网关	支持通过*zstack-cli*方式开启多网关功能，开启后每个网口都有独立的网关
	网卡多队列	Virtio类型网卡的流量分配给多个CPU时，用户可自行设置队列数目，有效提升虚拟网卡性能
	云主机设置网卡型号	平台类型为Linux、Paravirtualization的云主机支持设置网卡型号（包括：Virtio、E1000、RTL8139）
	设置主机名/密码	• 支持SSH密码方式登录，创建云主机时可通过UI设置主机名/密码，简化操作，提升用户体验 • 支持配置密码复杂度、密码长度等密码策略，以及是否强制设置云主机root密码
	高级设置	以云主机为粒度，对云主机资源独立配置参数： • 降低已有全局配置优先级，为某个云主机独立配置参数。例如：NUMA、云主机Hyper-V开关等 • 无对应全局设置，仅支持以某个云主机为粒度配置参数。例如：网卡多队列等
弹性伸缩组	生命周期	支持弹性伸缩组相关生命周期管理，包括：创建、启动、停止、删除
	健康检查	支持自定义健康检查方式、健康检查时间、健康检查宽限时间
	弹性伸缩策略	• 支持自定义触发条目、触发条件、持续时间、冷却时间、每次增加数量的扩容策略 • 支持自定义触发条目、触发条件、持续时间、冷却时间、云主机移除策略、每次减少数量的缩容策略 • 触发伸缩条件后，根据所设定的策略自动增加或减少云主机数量 • 支持根据云主机CPU使用率、内存使用率判断监控条件，触发弹性扩容、弹性缩容。其中，监控数据可选择外部或内部（推荐）监控数据
	消息通知	• 支持查看伸缩记录 • 支持选择是否接收弹性伸缩活动的消息通知 • 支持通过ZWatch和站内信的形式发送消息通知
云盘	批量操作	批量管理云盘
	云盘管理	• 支持云盘相关生命周期管理，包括：创建、启用、停用、加载、卸载、删除

类别	特性	ZStack企业版
		• 支持云盘相关常用操作，包括：迁移、创建快照、创建镜像、扩容、更改所有者、存储迁移 • 支持基于Ceph存储或Shared Block主存储创建共享云盘，多个云主机共享使用一块数据云盘 • 支持使用云盘规格或云盘镜像两种方式创建共享云盘
	云盘快照	• 使用云盘过程支持创建快照 • 支持批量删除云盘快照
快照	快照统一管理	对云主机/云盘快照统一管理，所有存在快照的云主机/云盘都将展示在快照页面，且支持按快照数量或总容量排序，方便用户快速识别需要清理的快照，提高运维效率
	批量快照	• 支持对云主机及所加载云盘创建快照组，支持以快照组为单位统一恢复云主机及其所加载云盘 • 支持解绑快照组，将快照组恢复为单盘快照
云盘规格	云盘规格管理	• 云盘规格支持创建、启用、停用、全局共享、全局召回、云盘规格QoS、删除等操作 • 支持通过高级参数对不同类型的数据云盘分类，用于独立计费/显示，支持主存储：Ceph、LocalStorage、NFS、SharedBlock
	设置QoS	创建云盘规格时，通过设置总带宽或读写带宽的方式，为云盘设置QoS
计算规格	计算规格管理	• 计算规格支持创建、启用、停用、磁盘QoS、网络QoS、全局共享、全局召回、删除等操作 • 支持选择物理机分配策略，包括：运行云主机数量最少、CPU使用率最低、内存使用率最低、运行云主机最大数量、首选上次所在物理机、随机分配 • 当物理机分配策略为CPU使用率最低/内存使用率最低，支持选择强制、非强制策略模式 • 支持通过高级参数对不同类型的根云盘分类，用于独立计费/显示。支持主存储：Ceph、LocalStorage、NFS、SharedBlock
GPU规格	GPU规格	• 自动扫描云平台中可用的物理GPU规格和vGPU规格并统一管理，创建云主机时支持指定规格为云主机添加GPU设备 • 通过GPU规格为云主机加载GPU设备时，支持关机自动卸载高级功能

类别	特性	ZStack企业版
镜像管理	系统模板	支持系统模板，支持QCOW2和RAW格式，自动匹配镜像类型
	ISO镜像	支持通过ISO镜像引导云主机安装操作系统
	BIOS模式	• 添加镜像支持Legacy、UEFI两种BIOS模式 • 创建云主机、创建云主机镜像、克隆云主机操作，将继承原镜像BIOS模式
	系统镜像上传	支持URL上传和本地浏览器上传
	云盘镜像上传	支持URL上传和本地浏览器上传
	镜像迁移	支持Ceph主存储上的镜像跨存储设备迁移
镜像仓库	镜像存放	存放镜像数据，包括ISO和系统模板
	镜像导出	• 支持镜像导出下载链接 • 已导出镜像提供MD5校验值，用户可在已导出镜像详情页查看该镜像的MD5校验值，校验下载镜像的完整性
	获取已有镜像	添加ImageStore类型的镜像服务器时，可获取该镜像服务器中URL路径下的已有镜像文件
	镜像同步	• 支持镜像仓库间的镜像互传，可以跨区域使用 • 同一管理节点下不同镜像仓库间支持镜像同步
	镜像仓库清理	可视化清理镜像服务器中已被彻底删除的无效数据，释放存储空间
	标准系统镜像	支持Windows、红帽、Ubuntu和其他开源Linux等标准系统
	预设运行镜像	支持众多的软件运行环境： • 支持Windows IIS和Dot Net Framework运行环境 • 支持Linux Tomcat、JAVA、Apache Web、Jboss、PHP、Node JS、Golang、Python等语言和运行环境 • 支持数据库Oracle、MySQL、Postgres、Mongodb、Influxdb、Cassandra和Redis等数据库服务 • 支持广泛的应用中间件
	预设应用镜像	支持众多的应用系统： • 支持论坛BBS、社交SNS、博客Blog、微博的常用应用系统 • 支持phpmyadmin等运维管理应用 • 支持厂商提供的应用镜像

类别	特性	ZStack企业版
	自定义镜像	支持管理员根据标准系统镜像和预设运行镜像，定义满足自身业务系统运行环境的镜像，以增量方式保存镜像内容，并实现智能去重功能
	存储支持	与本地存储、NFS、SMP、Ceph、Shared Block类型的主存储无缝支持
存储管理	本地存储	• 支持云盘存放到物理机本地 • 支持实时查看主存储已用容量百分比趋势图 • 支持设置云盘预分配策略，可以选择厚置备或精简置备
	NFS存储	• 支持云盘存放到NFS协议存储，物理机共享访问 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持实时查看主存储已用容量百分比趋势图
	共享挂载存储	• 支持云盘存放到POSIX兼容的共享存储，支持iSCSI/FC存储 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持实时查看主存储已用容量百分比趋势图
	Shared Block存储	• 支持添加iSCSI/FC协议存储，物理机共享访问 • 支持添加iSCSI存储，支持自动在线扫描并发现磁盘和自动配置iSCSI发起等操作 • 支持共享云盘 • 支持添加多个LUN • 添加Shared Block主存储时，支持显示共享块设备候选列表 • 使用Shared Block主存储创建云主机或云盘，支持设置置备方式，包括精简置备或厚置备 • 支持FC-SAN透传，直观的展示透传的FC存储，并可将透传的块设备加载到云主机 • 支持iSCSI透传，透传的块设备可直接加载到云主机使用 • 添加Shared Block主存储时，支持清理VG数据 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持实时查看主存储已用容量百分比趋势图
	Ceph存储	• 支持共享云盘 • 支持指定不同性能的磁盘卷创建云盘 • 支持云盘存放到Ceph分布式存储

类别	特性	ZStack企业版
		• 支持数据冷迁移 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持创建Ceph pool，以pool计算容量并设置显示名 • 支持清理块设备，可强制清理块设备中的文件系统、RAID或分区表中的签名 • Ceph类型的主存储可通过添加pool扩容，支持指定pool创建云主机/云盘 • 支持实时查看主存储已用容量百分比趋势图 • 对接ZStack企业版Ceph，支持存储许可证服务有效期提醒
	多主存储支持	• 同一集群支持挂载多个本地存储 • 同一集群支持挂载多个NFS存储 • 同一集群支持挂载多个Shared Block存储 • 同一集群支持挂载一个本地存储和一个NFS/SMP/Shared Block存储 • 同一集群支持挂载一个Ceph存储和多个Shared Block存储
网络管理	VLAN二层隔离	支持VLAN 802.1q作为网络隔离手段
	VXLAN网络	• 支持VXLAN网络，有效解决云数据中心逻辑网段不足、上层交换机MAC地址溢出等问题 • 支持修改Vni名称：用户可自定义已创建的Vni名称，也可在创建Vni范围时设置Vni名称
	硬件VXLAN网络	通过添加SDN控制器，可在云平台接管硬件交换机的SDN网络，降低网络延迟的同时提升VXLAN网络性能
	分布式扁平网络	• 支持IPv6协议，用户可根据需求选择IPv4、IPv6或双栈（IPv4+IPv6）类型的扁平网络 • 支持云主机直接使用真实网络IP资源 • 扁平网络支持以下网络服务：安全组、扁平私网虚拟IP、弹性IP、内网负载均衡
	分布式弹性网络	支持云主机使用虚拟网络地址，与真实网络映射
	分布式DHCP服务	• 支持云主机自动获取分配的IP地址 • 创建三层网络时，支持为DHCP服务指定IP地址，防止网络规划过程中IP冲突
	网络地址空间预留	支持预留网络地址空间，以便与物理网络混合使用

类别	特性	ZStack企业版
	动态和静态分配IP	不仅支持动态分配IP地址，而且支持指定IP地址
	多级网络管理	云主机支持接入多个网络，构建复杂场景的业务
	虚拟IP的QoS设置	支持对虚拟IP做QoS限制，实现网络服务高效分配管理
	MTU	自定义限制网络传输数据包的大小
	自定义网关	• IP范围方式添加网络段支持自定义指定网关 • CIDR方式添加网络段支持自定义指定网关，使用CIDR的第一个或最后一个地址作为网关
	VPC路由器	• 支持创建VPC路由器相关生命周期管理，包括：创建、删除、启动、停止、重启 • 支持VPC路由器相关常用操作，包括：迁移、VPC网络的加载/卸载、东西向流量的设置 • 支持所有网络服务 • 支持集中在VPC路由器中配置DNS • 支持自定义开启或关闭SNAT网络服务 • 支持OSPF动态路由协议 • 支持组播功能，可将组播源发送的组播消息转发给云主机 • 支持分布式路由高级功能，优化东西向流量 • 创建单个VPC路由器支持指定默认IP • VPC路由器优先级默认高于普通云主机，物理机资源出现竞争时优先保证VPC路由器的资源使用 • VPC路由器可加载多个公有网络，且支持指定默认路由、配置源进源出功能 • VPC路由器的公有网络接口和VPC网络接口分别支持设置QoS限速，满足更加细粒度的流量控制场景需求
	防火墙	• 支持对VPC路由器配置防火墙：VPC防火墙创建后，系统为VPC路由器自动配置入方向规则集，用户也可灵活配置出方向规则集 • VPC路由器的每个接口方向允许应用一个规则集，对接口处的南北向流量进行过滤，有效保护整个VPC的通信安全以及VPC路由器安全 • VPC路由器网卡的入方向将会默认绑定一条规则集 • 支持IP地址、IP范围、CIDR多种方式添加防火墙规则，且支持多种IP书写方式同时使用，减少规则配置的复杂度，提高功能易用性

类别	特性	ZStack企业版
		• 添加防火墙规则支持选择是否立即生效
	VPC路由器高可用组	• 支持VPC路由器高可用功能，一个VPC路由器高可用组内部署一对互为主备的VPC路由器 • 当主VPC路由器状态异常，秒级触发高可用切换，自动切换至备VPC路由器工作，保障业务持续稳定运行 • 创建VPC路由器高可用组支持指定虚拟IP
	VPC网络	• 支持IPv6协议，用户可根据需求选择IPv4、IPv6或双栈（IPv4+IPv6）类型的VPC网络 • 支持创建VPC网络、添加网络段、加载/卸载VPC路由器、删除 • VPC网络支持以下网络服务：安全组、虚拟IP、弹性IP、端口转发、负载均衡 • 负载均衡支持TCP/HTTP/HTTPS/UDP协议 • 图形用户界面支持负载均衡器的即时流量监控
	公有网络	• 支持IPv6协议，用户可根据需求选择IPv4、IPv6或双栈（IPv4+IPv6）类型的公有网络 • 支持创建云主机 • 支持为网络服务提供虚拟IP • 支持地址池功能。已创建IPv4类型的公有网络，支持在普通网段基础上，添加IPv4类型地址池网络段，可用于创建虚拟IP，并基于VPC网络提供各种网络服务
	系统网络	可作为管理网络、存储网络、迁移网络等使用
	云路由网络	• 云路由支持以下网络服务：安全组、虚拟IP、弹性IP、端口转发、负载均衡 • 负载均衡支持TCP/HTTP/HTTPS/UDP协议 • 图形用户界面支持负载均衡器的即时流量监控 • 支持基于云路由的IPsec隧道服务 • 支持多个弹性IP绑定同一个云主机网卡 • 支持一个云路由器接多个公有网络 • 支持配置静态路由表 • 支持分布式DHCP提升服务性能
	网络拓扑	• 全局网络拓扑查看，支持高亮显示 • 自定义选择资源展示拓扑图

类别	特性	ZStack企业版

	负载均衡	• 支持以下几种负载均衡网络服务：
		  - 公网负载均衡：使用公有网络作为前端网络，通过路由器（VPC路由器/云路由器）提供外网负载均衡服务
		  - VPC私网负载均衡：使用VPC网络作为前端网络，通过VPC路由器提供内网负载均衡服务
		  - 扁平私网负载均衡：使用扁平网络作为前端网络，通过云路由器提供内网负载均衡服务
		• 负载均衡支持TCP/HTTP/HTTPS/UDP协议；健康检查协议支持TCP、UDP、HTTP
		• 支持的负载均衡算法包括：轮询、最小连接、源地址哈希、加权轮询
		• 支持通过zstack-cli命令为监听器配置黑白名单，控制特定IP访问负载均衡，防止恶意攻击，提高系统安全性

	Netflow	• VPC路由器新增Netflow网络服务，支持通过Netflow对VPC路由器网卡的进出流量进行分析监控 • 支持Netflow V5、V9两种数据流输出格式
	IP统计	• 支持在UI界面查看三层网络（私有网络、公有网络、VPC网络）的IP使用情况 • 三层网络IP统计详情页，可快速查看已用IP及其关联资源，以及未被占用IP情况，从而提高IP规划效率
	端口镜像	• 通过镜像端口对获取到的业务报文进行分析，方便企业对内部网络数据进行监控管理，快速定位网络故障 • 支持配置独立的流量网络用于端口镜像传输数据
定时任务	定时对象	支持云主机、云盘的定时操作
	定时操作	• 可对云主机关闭/重启，云盘快照等设置定时操作 • 创建云主机/云盘快照定时任务时，如果选择的所有云主机/云盘都使用Ceph主存储，支持设置保留快照数量
资源编排	资源栈	• 支持在线编辑方式和使用模板方式创建资源栈 • 支持预览/校验模板内容，支持云主机插入User Data • 支持删除资源栈和级联删除资源栈中所有资源
	自定义模板	支持通过文本编辑器方式和本地上传方式创建资源栈模板，并支持创建、查看、修改、删除、预览操作

类别	特性	ZStack企业版
	示例模板	云平台默认提供的资源栈模板示例，作为参考模板
	可视化资源编排	• 支持可视化拖拽资源方式创建资源栈模板 • 支持预览模板、生成资源栈、另存为资源栈模板 • 支持撤销、恢复、删除、清空画布操作
安全管理	三层安全策略	支持基于TCP/UDP端口的安全策略
	安全组统一管理	• 支持安全组统一管理云主机安全策略，实现组内互通，组间策略 • 支持启用、停用安全组
性能TOP5和性能分析	性能TOP5	• 支持物理机、云主机、路由器、虚拟IP、三层网络等多种资源排序，并可自定义不同时间段查看 • 支持切换数据来源，包括外部监控和内部监控（安装agent）
	云主机性能统计	• 支持自定义时间段查看，指定资源范围，指定所有者范围，对云主机CPU使用率、内存使用率、磁盘读速度、磁盘写速度、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序 • 支持切换数据来源，包括外部监控和内部监控（安装agent）
	路由器性能分析	• 支持自定义时间段查看，指定资源范围，指定所有者范围，对路由器CPU使用率、内存使用率、磁盘读速度、磁盘写速度、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序 • 支持切换数据来源，包括外部监控和内部监控（安装agent）
	物理机性能统计	支持自定义时间段查看，指定资源范围，对物理机CPU使用率、内存使用率、磁盘读速度、磁盘写速度、磁盘用量、磁盘读IOPS、磁盘写IOPS、磁盘已用量百分比、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	三层网络性能分析	支持自定义时间段查看，指定资源范围，对三层网络已用IP数、已用IP百分比、可用IP数、可用IP百分比行过滤分析排序
	虚拟IP性能分析	支持自定义时间段查看，指定资源范围，指定所有者范围，对虚拟IP的下行网络流量、下行网络入包速率、上行网络流量、上行网络入包速率进行过滤分析排序
	镜像服务器性能分析	支持自定义时间段查看，指定资源范围，对镜像服务器的可用容量百分比进行过滤分析排序

类别	特性	ZStack企业版
容量管理	容量管理	对云平台核心资源容量信息进行直观展示： • 以卡片形式展示各种核心资源详细容量信息 • 以及对各种核心资源容量信息进行TOP 10排序，方便用户整体掌控当前云平台核心资源容量使用情况，提高管理运维效率
ZWatch	物理机监控	对物理机运行实时监控，显示CPU、内存、磁盘和网络时序监控图
	云主机监控	对云主机运行实时监控，显示CPU、内存、磁盘和网络时序监控图
	监控	• 支持对系统时序数据进行监控，例如云主机内存使用率、物理机CPU使用率等 • 支持对系统事件进行监控，例如云主机状态变化事件、物理机失联事件等 • 首页支持按时间段查看物理机负载可视化图形

	报警	• 通过丰富的报警条目：
		  - 对云主机、裸金属主机、路由器、镜像、镜像服务器、系统数据目录、物理机、三层网络、云盘、虚拟IP、主存储、监听器、项目资源等多种资源进行监控报警
		  - 对云主机、路由器、镜像服务器、管理节点、物理机、主存储、vCenter、备份任务、项目资源等相关事件提供监控报警
		• 对时序性数据和事件设置报警器，并通过SNS通知系统接收报警信息，支持邮件/钉钉/HTTP应用/阿里云短信/Microsoft Teams方式接收报警信息
		• 提供常用默认报警器，实时监控基础资源状态
		• 按需选择监控范围，支持对监控对象的单个资源或全部资源进行监控
		• ZWatch报警消息收敛，事件报警消息策略调整为仅提示一次；资源报警器中报警周期类型新增**一次**选项，用户可根据自己的需求，灵活配置报警策略
		• ZWatch报警消息支持已读未读状态提示，方便用户快速定位问题，提高运维效率
		• ZWatch报警恢复后支持消息提示
		• 报警消息支持中英双语，更加易读易懂，方便快速定位问题

类别	特性	ZStack企业版
		• 支持对资源报警器/事件报警器设置报警级别，不同级别的报警器将会发出对应级别的报警消息，方便用户进行报警分类，按需查阅，提高运维效率
	多接收端	• 支持邮件/钉钉/HTTP应用/阿里云短信/Microsoft Teams/系统默认报警器等多种接收端 • 邮箱接收端和阿里云短信接收端支持添加多个接收端地址
	报警消息模板	邮件/钉钉/阿里云短信/Microsoft Teams类型接收端支持自定义报警消息模板，方便用户按需配置，增加报警消息可读性
	接管第三方报警消息	• 支持连接第三方消息源，接管第三方报警消息并统一推送，方便报警消息统一管理的同时提高运维效率 • 支持创建第三方消息报警器，并通过各类接收端推送第三方报警消息
审计	资源审计	• 支持所有资源的审计查询，用户能对该资源的所有操作行为审计，有效保障用户在云环境下核心数据的安全 • 支持查看调用API名称、消耗时间、任务结果、操作员，任务创建/完成时间，以及API行为的消息详情，且支持CSV格式导出
操作日志	操作日志	• 支持查看操作描述、任务结果、操作员、登录IP、任务创建/完成时间，以及操作返回的消息详情，实现更细粒度管理，且支持CSV格式导出 • 支持用户按需配置日志保留时间 • 支持展示执行任务的事件审计和登录操作审计 • 全局设置支持对管理节点日志保留时间以及保留容量进行按需设置
账户管理	账户和用户管理	账户管理功能，分为账户和用户，其中账户是资源计量团体，用户可定义操作权限
	AD/LDAP账户	• 支持添加AD/LDAP账户，并绑定普通账户 • 支持自定义清除规则
	账户云资源配额	支持自定义分配账户最大可用资源，包括云主机运行数量、CPU、内存、云盘数量、云盘总容量、镜像数量、镜像总容量、弹性IP数量等
	用户组权限分配	支持用户组权限分配，统一编排用户权限
	用户操作权限分配	支持对用户进行权限分配

类别	特性	ZStack企业版
	云主机更改所有者	支持变更云主机所有者，指定云主机所属账户
	云盘更改所有者	支持变更云盘所有者，指定云盘所属账户
	计算规格指定分配	支持计算规格共享特性，可指定账户是否可使用
	镜像资源指定分配	支持镜像资源共享特性，可指定账户是否可使用
	云盘规格指定分配	支持云盘规格共享特性，可指定账户是否可使用
	网络资源指定分配	支持二层网络和三层网络资源共享特性，可指定账户是否可使用
	全局设置	管理员可以直接在UI上对各种特性进行全局配置。 • 所有的全局配置都有一个默认值，支持一键恢复默认配置 • 更新全局配置并不需要重启管理节点 • 支持全局配置场景化封装，基于用户实际生产场景需求，提供场景化的一键全局设置，方便快速将云平台设置为所需状态，提高运维效率
	修改admin账户密码	忘记admin登录密码时，可以使用zstack-ctl reset_password还原默认值
计费	自定义计费价目	• 将各资源计费单价汇总为一份价目表，提供准公有云计费方式体验，支持的计费资源类型包括：CPU、内存、根云盘、数据云盘、GPU设备、公网IP（扁平网络）、公网IP（虚拟IP） • 计费单价支持秒、分、小时和天 • 动态可调的计费单价，满足周期性促销需求
	计费方式	• 提供准公有云计费方式体验，而且涵盖了多价目计费、按磁盘性能计费、公网IP计费等典型使用场景 • 支持基于项目/账户进行计费，统计各资源消费情况。且各项目/账户支持使用不同计费价目，制定不同定价策略 • 支持按需选择开启/关闭计费功能
	基于磁盘性能计费	不同类型的磁盘支持单独设置计费单价
	计费货币符号	支持对计费货币符号进行全局设置，支持的货币单位包括：人民币 ￥、美元 $ 、欧元 € 、英镑 £ 、澳元 A$ 、港元 HK$ 、日元 ¥ 、瑞士法郎 CHF 、加拿大元 C$
	账单	按计费单价和使用时间来统计并显示admin和所有租户的资源费用信息 • 支持实时显示账单 • 支持项目账单、部门账单（项目加载到部门）、账户账单

类别	特性	ZStack企业版
		• 账单明细默认每天零点生成一次，账单明细生成时间可通过全局设置修改
访问	TUI	支持常用运维操作，定制化OS界面
	图形界面	支持以HTTP/HTTPS方式访问图形界面管理云平台（UI界面）
	UI语言	• 更好满足不同地区用户的语言使用习惯，支持UI默认语言与当前用户浏览器语言一致 • 支持自定义并记录UI语言，交互更加友好，提升用户体验
	登录安全	• 支持动态验证码验证，多次登录（6次）失败触发验证码验证，防止恶意登录 • 支持双因子认证，额外增加安全码身份验证，进一步增强账号安全 • 支持设置登录密码复杂度，用户可自定义设置密码长度范围，并使用数字、大小写和特殊字符组合的密码策略 • 支持设置密码有效期，用户可自定义设置密码更新周期。建议定期修改云平台登录密码，保障登录安全 • 支持设置历史密码检查，用户可自定义设置密码不重复次数 • 支持设置锁定机制检查，用户可自定义设置连续登录失败次数上限、以及连续登录失败锁定用户时长；当连续登录失败次数超过设置值，用户账户将被锁定一段时间，保障登录安全 • 支持登录IP黑白名单，用户可按需配置IP黑白名单，从而实现对访客身份的识别和过滤，提升云平台访问控制安全 • 同一用户支持多会话登录，同时支持禁用多会话登录模式 • 支持设置默认登录链接访问的登录界面，使登录入口更加清晰明了
	命令行	支持通过命令行方式访问云管理平台，命令行支持全功能访问，账户和用户支持命令行登录访问
	API接口	支持全功能的API交付，API支持Java SDK（兼容版本：Java 8）、Python SDK（兼容版本：Python 2.7）以及标准RESTful接口访问
操作助手	智能提示	对云平台核心操作给出智能的环境检查和操作指导
亲和组	反亲和组	为了合理调度平台资源，提供针对云主机与物理机的两种亲和组策略：反亲和组(非强制)、反亲和组(强制)
UI强化	自定义产品信息	支持自定义UI界面的产品Logo产品名称等信息
	首页大屏	• 多款华丽主题的大屏实时展示平台资源情况

类别	特性	ZStack企业版
		• 支持切换虚拟化，分别展示KVM或vCenter大屏 • 支持切换区域，展示全部区域或某个区域的大屏 • 支持切换数据来源，包括外部监控和内部监控（安装agent）
	加密访问	支持HTTPS安全访问登录平台
	过程展示	增加多个场景进度条
VDI	解决方案	• 通过定制客户端，支持SPICE，RDP，VNC等协议，并进行了优化 • 支持指定VDI网络 • 支持USB重定向，兼容多种USB设备 • 支持设置独立VDI网络 • 支持多屏显示 • 支持麦克风 • 支持SPICE流量优化
UI导航	快速入口	增加快速进入产品与服务的入口，并支持高亮标注
UI信息导出	列表信息CSV导出	导出云主机和物理机主列表的信息，离线管理便于图表编辑
标签	资源标签	• 自定义创建不同名称/颜色的标签，并绑定到云主机、云盘、物理机、裸金属主机，方便资源管理和资源搜索 • 资源标签支持按绑定时间或名称进行排序
应用中心	应用中心	支持添加包括存储、数据库、安全、IaaS、PaaS、SaaS类型在内的应用插件
AccessKey	AccessKey管理	支持生成可供其他平台调用API权限的AccessKey，此AccessKey具有该创建者相同的权限
License	云平台许可证	• 云平台许可证 (Basic License) 包括企业版和混合云版 • 支持本地浏览器上传License • 支持License到期提醒 • 企业单机无限期试用版支持所有功能 • 支持CPU授权、Host授权两种授权方式
	模块许可证	• 模块许可证 (Plus License) 为用户提供附加功能 • 依赖于平台许可证使用 • 已包括：企业管理模块、VMware管理模块、裸金属管理模块、灾备服务模块、迁移服务模块、ARM64服务器管理、售后服务 (5x8、7x24)

类别	特性	ZStack企业版
		• 支持本地浏览器上传License • License到期提醒
	CPU架构许可证	• 支持x86服务器架构许可证类型，支持区分KVM和vCenter为计算节点提供独立的CPU授权 • 支持ARM64服务器管理许可证类型，支持添加许可证指定CPU数量/物理机数量的ARM64服务器到云平台，作为计算节点提供服务
	上传许可证	• 可根据需求自由打包许可证 • 针对双管理节点，支持在任一管理节点下载请求码并统一上传许可证
管理节点	多物理机管理节点高可用	• 支持多物理机管理节点高可用。采用主备方案，某个管理节点故障后能迅速切换到另一个管理节点，保证业务正常运行 • 通过VIP登录管理节点，支持分别为主备管理节点添加许可证 • 多管理节点高可用环境支持管理节点高可用监控与健康状态查询，并提供仲裁IP不可达、双管理节点数据库不同步默认资源报警器
	管理节点	• 管理节点支持不同版本源文件共存 • 管理节点数据库支持配置访问限制。可对管理节点数据库账号设置白名单策略，确保数据库安全
计算节点	批量添加物理机	• 可根据填写的网络段批量添加物理机 • 支持通过模板导入方式批量添加物理机
日志服务器	日志服务器	通过该日志服务器，用户可便捷收集管理节点日志，快速定位问题，提高云平台运维效率
安装	一键安装	• 一条命令，30分钟完成从裸机到云平台的安装部署 • 支持企业版管理节点、社区版管理节点、计算节点、专家模式多种安装模式
升级	无缝升级	支持低版本至高版本的无缝升级
	增量升级	支持增量升级，大幅提高升级速度
	环境升级	支持通过专家模式自定义安装升级

ZStack企业管理模块功能列表：

类别	特性	企业管理模块
组织架构	用户	• 用户是企业管理中的最基本单位 • admin/平台成员可创建用户，并基于用户建立相应的组织架构 • 支持添加用户、删除用户、修改用户名、修改密码、修改个人信息、加入部门、从部门移除、加入项目、从项目移除 • 用户的个人信息包括姓名、手机号码、邮箱地址和编号等 • 支持手动添加和模板导入两种方式创建用户，其中模板导入方式支持将用户的组织架构关系以及所属项目信息同步导入
	组织架构	• 组织架构是企业管理中的基本单位，admin/平台管理员可以看到云平台所有组织架构树，普通平台成员/项目成员仅能看到所属组织架构架构树 • 组织以组织架构树的方式呈现，分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门，支持创建多个顶级部门 • 弱化部门负责人与部门的绑定关系，允许部门不设置部门负责人 • 支持添加组织、删除组织、更改上级部门、更改部门负责人、创建子部门、删除子部门、添加用户、移除用户
	角色	• 角色表示权限的集合，为用户赋予权限可获得调用相关API进行资源操作的能力 • 企业管理租户与角色分离，角色可灵活绑定到企业管理租户或从企业管理租户解绑，分为系统角色和自定义角色 • 图形用户界面对企业管理租户进行API级别的权限控制，灵活适配各种场景的权限配置需求 • 允许超级管理员（admin）/平台管理员/普通平台成员对项目成员（项目负责人/项目管理员/普通项目成员）进行权限管理 • 平台管理员以用户形式存在，绑定平台管理员角色即可赋予身份并赋予相应的权限 • 提供平台管理员角色、项目负责人角色、项目管理员角色、监控大屏角色系统角色。其中，绑定监控大屏角色的用户仅拥有监控大屏查看权限，登录即可跳转到监控大屏界面
	第三方认证	• 支持添加AD/LDAP服务器，成功添加ADLDAP服务器后，自动化批量导入第三方用户/组织 (仅AD支持) 至云平台 • 支持设置用户映射和组织映射 (仅AD支持) ，根据配置的映射规则同步第三方用户/组织架构 (仅AD支持) • 支持自定义过滤规则，过滤不需要同步的用户

类别	特性	企业管理模块
项目管理	项目	• 用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务 • 企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池 • 支持创建项目、删除项目、启用项目、停用项目、更换项目负责人、生成项目模板、添加成员、移除成员、停用项目资源、恢复过期项目、加载部门、卸载部门 • 弱化项目负责人与项目的绑定关系，允许项目不设置项目负责人。 • 支持通过回收日期、费用阈值回收项目 • 支持使用官方提供的脚本批量创建项目
	项目模板	• 用于标识各个资源配额的模板 • 在创建项目时，可直接使用模板定义的配额来快速创建项目 • 支持创建项目模板、删除项目模板
	项目成员	• 项目成员作为项目的基本组成人员，一般由admin/平台成员/项目负责人/项目管理员添加进入项目 • 项目成员的权限可由admin/平台成员/项目负责人/项目管理员进行相应控制
	成员组	• admin/平台成员/项目负责人/项目管理员可在项目中创建成员组，对成员进行分组管理 • 支持以成员组为单位赋予角色，进行权限控制
	设置QoS	• admin/平台成员可以对云主机、云盘、网卡设置QoS • 磁盘QoS可通过设置总带宽或读写带宽的方式进行设置 • 控制QoS设置范围，普通账户/项目成员修改QoS上限不能超过admin/平台管理员设置的值
工单管理	工单申请	• 项目成员（项目负责人/项目管理员/普通项目成员）可对云平台资源提出工单申请 • 支持项目成员创建、撤回、重新打开以及删除工单
	工单审批	• 支持admin或项目负责人通过并部署工单以及驳回工单 • 支持默认流程审批和自定义流程审批 • 默认流程审批：项目成员提交工单申请，admin可进行一键审批，审批通过后，资源可自动部署成功并分发到项目中

类别	特性	企业管理模块
		• 自定义流程审批：项目成员提交工单申请，按自定义工单流程经由各级审批人进行审批，最终由admin或项目负责人进行一键审批，审批通过后，资源可自动部署成功并分发到项目中
	自定义流程管理	• 支持admin为不同项目设置不同类型的自定义工单流程 • 支持多种工单类型，包括：申请云主机、删除云主机、修改项目周期、修改云主机配置、修改项目配额 • 自定义工单流程支持将项目成员添加到各审批环节 • 支持启用、停用、修改、删除自定义工单流程
独立区域管理	平台管理员	• 平台管理员主要是带有区域属性的管理员 • admin可划分不同区域给不同平台管理员来管控不同区域的数据中心 • 支持创建/删除平台管理员、修改密码、添加区域和移除区域
	资源隔离	• 在对区域进行资源隔离的基础上，可对每个区域指定相应的区域管理员，实现各地机房的独立管理 • 同时admin可对所有区域进行巡查和管理

ZStack裸金属管理模块功能列表：

类别	特性	裸金属管理模块
裸金属管理	裸金属集群	• 通过创建裸金属集群，管理物理裸机 • 支持为裸金属集群加载二层网络
	部署服务器	• 通过部署服务器自动化对新上线裸金属设备进行系统安装部署 • 支持独立部署PXE服务器
	裸金属设备	• 通过IPMI网络批量部署裸金属设备 • 支持对裸机进行远程电源管理 • 可根据填写的网络段批量添加裸金属设备 • 支持通过模板导入方式批量添加裸金属设备 • 支持从控制台打开裸金属设备的IPMI管理界面（登录界面），输入已配置好的IPMI用户名和IPMI密码，即可登录
	裸金属主机	• 支持使用ISO类型镜像为裸金属设备安装Linux操作系统 • 支持Ubuntu、CentOS、suse操作系统无人值守安装 • 支持为裸金属主机添加网络配置 • 支持内部负载实时监控（需安装agent），可查看裸金属主机CPU、内存、磁盘、网卡的各项性能指标

类别	特性	裸金属管理模块
		• 提供裸金属主机CPU、内存、磁盘、网卡相关监控条目 • 支持对裸金属主机资源定制化创建标签（仅支持管理员标签），并通过标签快速检索裸金属主机

ZStack灾备服务模块功能列表：

类别	特性	灾备服务模块
灾备服务	备份	• 支持为云主机、云盘和管理节点数据库创建备份任务，其中支持云主机的整机备份 • 支持对当前备份任务进行统一直观展示，方便用户快速掌控当前备份任务整体情况，提高管理运维效率 • 通过优化大文件备份机制，大幅提升了大文件备份性能，并且支持物理带库和虚拟带库 • 支持用户按周/天/小时为任务设置备份策略，已创建的备份任务支持更新备份策略 • 可按数量或时间保存备份文件数据 • 创建备份任务后支持立即备份及定时全量备份数据 • 支持将数据备份在本地备份服务器并同步到远端备份服务器 • 支持查看云主机、云盘和数据库的本地备份数据/远端备份数据 • 支持删除本地备份数据/远端备份数据 • 可直接使用本地数据中心已部署的镜像仓库作为本地备份服务器，也可部署新的本地备份服务器 • 当备份任务指定多个本地备份服务器时，支持主备无缝切换 • 仅允许添加一个远端备份服务器，包括异地和阿里云两种类型 • 备份数据仅可从本地备份服务器同步至远端备份服务器 • 清理本地备份服务器/远端备份服务器中已被彻底删除的无效备份数据和过期的临时数据，释放存储空间 • 备份任务支持设置磁盘QoS和网络QoS • 备份任务支持查看备份进度 • 添加已有备份服务器，支持自动获取备份数据 • 支持对备份任务创建事件报警器，当备份任务执行失败，用户会在接收端接收到备份任务执行失败的报警详情
	还原	• 从本地云主机/云盘的本地/远端备份数据还原资源时，支持新建资源以及覆盖原始资源 • 支持云主机的整机还原

类别	特性	灾备服务模块
		• 本地云主机/云盘的远端备份数据需先同步至本地备份服务器，才可还原至本地，数据库的远端备份数据直接还原至本地 • 在本地有数据的情况下（Zone存在），可通过数据库的本地/远端备份数据一键还原数据中心 • 在本地无数据的情况下（Zone不存在），可通过数据库的本地/远端备份数据以Wizard引导界面的方式还原数据中心 • 支持将数据库的本地/远端备份数据导出进行手动还原

ZStack迁移服务模块功能列表：

类别	特性	迁移服务模块
迁移服务	迁移服务器	• 迁移服务器与所征用物理机状态解耦。当迁移服务器为启用状态但所征用物理机为停用状态时，该迁移服务器将作为V2V迁移场景专用，其它业务云主机不会被调度至该迁移服务器上，有效提升迁移效率 • 迁移服务器支持设置单独的迁移网络，用于从源主存储迁移至迁移服务器的数据转化 • 迁移服务器支持实时容量监控，可选择不同的时间跨度来监控迁移服务器已使用容量百分比 • 支持展示迁移服务器总容量以及可用容量
	V2V迁移 (VMware)	• 将已接管的vCenter云主机迁移至当前云平台 • 支持对云主机进行一键式批量的V2V迁移，迁移后置备方式保持不变 • 创建迁移任务过程中，支持对目标云主机进行自定义配置 • 支持设置迁移网络，并设置QoS • 支持取消、重新启动迁移任务 • 安全又节省资源的迁移服务，迁移过程中的文件在源主存储中压缩保存 • 支持迁移的源vCenter平台版本包括：5.0、5.1、5.5、6.0、6.5、6.7 • 支持多种操作系统的云主机进行V2V迁移，包括：RHEL/CentOS 5.x/6.x/7.x、SLES 11/12/15、Ubuntu 12/14/16/18、Windows 7/2003/2008/2012/2016 • 源主存储类型无限制；目标主存储支持Ceph、SharedBlock、NFS和本地存储类型
	V2V迁移 (KVM)	• 不需要接管，即可将云主机从KVM云平台在线迁移至当前云平台

类别	特性	迁移服务模块
		• 运行、暂停状态的云主机均支持V2V迁移 (KVM) • V2V迁移 (KVM)不限制主存储类型 • 迁移过程支持同时迁移加载的数据云盘，支持修改CPU、内存 • 迁移过程不同时迁移云主机快照 • 源主存储类型无限制；目标主存储支持Ceph、SharedBlock、NFS和本地存储类型

ZStack三员分立功能列表：

类别	特性	三员分立
三员分立	三员管理	将超级管理员 (admin) 权限分解并赋予系统管理员、安全管理员和安全审计员，相互独立，相互制约，可有效降低因超级管理员权限过大带来的安全风险，进一步加强云平台安全
	系统管理员	系统管理员负责云平台资源管理，支持对云平台内资源进行生命周期管理（不包括权限相关管理）
	安全管理员	安全管理员负责云平台权限管理，支持权限分配
	安全审计员	安全审计员负责云平台审计管理，支持日志查看和日志导出权限，用于对其他用户的操作进行审查

4 产品优势

ZStack是基于专有云平台4S（Simple简单，Strong健壮，Scalable弹性，Smart智能）标准设计的下一代云平台IaaS软件。

1. **简单**（Simple）
   - 简单安装部署：提供安装文件网络下载，30分钟完成从裸机到云平台的安装部署。
   - 简单搭建云平台：支持云主机的批量（生成，删除等）操作，提供列表展示和滑窗详情。
   - 简单实用操作：详细的用户手册，足量的帮助信息，良好的社区，标准的API提供。
   - 友好UI交互：设计精良的专业操作界面，精简操作实现强大的功能。
2. **健壮**（Strong）
   - 稳定且高效的系统架构设计：拥有全异步的后台架构，进程内微服务架构，无锁架构，无状态服务架构，一致性哈希环，保证系统架构的高效稳定。目前已实现：单管理节点管理上万台物理主机、数十万台云主机；而多个管理节点构建的集群使用一个数据库、一套消息总线可管理十万台物理主机、数百万台云主机、并发处理数万个API。
   - 支撑高并发的API请求：单ZStack管理节点可以轻松处理每秒上万个并发API调用请求。
   - 支持HA的严格要求：在网络或节点失效情况下，业务云主机可自动切换到其它健康节点运行；利用管理节点虚拟化实现了单管理节点的高可用，故障时支持管理节点动态迁移。
3. **弹性**（Scalable）
   - 支撑规模无限制：单管理节点可管理从一台到上万台物理主机，数十万台云主机。
   - 全API交付：ZStack提供了全套IaaS API，用户可使用这些APIs完成全新跨地域的可用区域搭建、网络配置变更、以及物理服务器的升级。
   - 资源可按需调配：云主机和云存储等重要资源可根据用户需求进行扩缩容。ZStack不仅支持对云主机的CPU、内存等资源进行在线更改，还可对云主机的网络带宽、磁盘带宽等资源进行动态调整。
4. **智能**（Smart）
   - 自动化运维管理：在ZStack环境里，一切由APIs来管理。ZStack利用Ansible库实现全自动部署和升级，自动探测和重连，在网络抖动或物理主机重启后能自动回连各节点。其中定时任务支持定时开关云主机以及定时对云主机快照等轮询操作。
   - 在线无缝升级：5分钟一键无缝升级，用户只需升级管控节点。计算节点、存储节点、网络节点在管控软件启动后自动升级。
   - 智能化的UI交互界面：实时的资源计算，避免用户误操作。
   - 实时的全局监控：实时掌握整个云平台当前系统资源的消耗情况，通过实时监控，智能化调配，从而节省IT的软硬件资源。

术语表

区域（Zone）

ZStack中最大的一个资源定义，包括集群、二层网络、主存储等资源。

集群（Cluster）

一个集群是类似物理主机（Host）组成的逻辑组。在同一个集群中的物理主机必须安装相同的操作系统（虚拟机管理程序，Hypervisor），拥有相同的二层网络连接，可以访问相同的主存储。在实际的数据中心，一个集群通常对应一个机架（Rack）。

管理节点（Management Node）

安装系统的物理主机，提供UI管理、云平台部署功能。

计算节点（Compute Node）

也称之为物理主机（或物理机），为云主机实例提供计算、网络、存储等资源的物理主机。

主存储（Primary Storage）

用于存储云主机磁盘文件的存储服务器。支持本地存储、NFS、 Ceph、Shared Mount Point、Shared Block类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。支持ImageStore、Sftp（社区版）、Ceph类型。

镜像仓库（Image Store）

镜像服务器的一种类型，可以为正在运行的云主机快速创建镜像，高效管理云主机镜像的版本变迁以及发布，实现快速上传、下载镜像，镜像快照，以及导出镜像的操作。

云主机（VM Instance）

运行在物理机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务。

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

云主机的数据盘，给云主机提供额外的存储空间，共享云盘可挂载到一个或多个云主机共同使用。

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

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

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

物理主机节点的网络连接采用Vlan设置，Vlan需要在交换机端提前进行设置。

VXLAN网络池（VXLAN Network Pool）

VXLAN网络中的 Underlay 网络，一个 VXLAN 网络池可以创建多个 VXLAN Overlay 网络（即 VXLAN 网络），这些 Overlay 网络运行在同一组 Underlay 网络设施上。

VXLAN网络（VXLAN）

使用 VXLAN 协议封装的二层网络，单个 VXLAN 网络需从属于一个大的 VXLAN 网络池，不同 VXLAN 网络间相互二层隔离。

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制，对IP地址、网络包类型或网络包流向等可以设置不同的安全规则。

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一时间点某一磁盘的数据状态文件。包括手动快照和自动快照两种类型。