阿里云
ZStack for Alibaba Cloud

技术白皮书

产品版本：V2.6.0

文档版本：20180809

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的”现状“、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含”阿里云”、Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

表 -1: 格式约定

格式	说明	样例
	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	**禁止**： 重置操作将丢失用户配置数据。
	该类警示信息可能导致系统重大变更甚至故障，或者导致人身伤害等结果。	**警告**： 重启操作将导致业务中断，恢复业务所需时间约10分钟。
	用于警示信息、补充说明等，是用户必须了解的内容。	**说明**： 导出的数据中包含敏感信息，请妥善保存。
	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	**说明**： 您也可以通过按**Ctrl** + **A**选中全部文件。
>	多级菜单递进。	**设置** > **网络** > **设置网络类型**
粗体	表示按键、菜单、页面名称等UI元素。	单击 **确定**。
courier字体	命令。	执行 **cd /d C:/windows** 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	**bae log list --instanceid** *Instance_ID*
[]或者[a|b]	表示可选项，至多选择一个。	**ipconfig** *[-all|-t]*
{}或者{a|b}	表示必选项，至多选择一个。	**swich** *{stand | slave}*

目录

法律声明 I
通用约定 I
1 产品概述 1
2 产品剖析 3
2.1 专有云 3
2.1.1 ZStack功能架构 3
2.1.2 ZStack资源结构 5
2.1.2.1 云资源池 8
2.1.2.1.1 云主机 8
2.1.2.1.2 云盘 8
2.1.2.1.3 镜像 8
2.1.2.1.4 亲和组 10
2.1.2.1.5 计算规格 11
2.1.2.1.6 云盘规格 11
2.1.2.2 硬件设施 12
2.1.2.2.1 区域 12
2.1.2.2.2 集群 12
2.1.2.2.3 物理机 16
2.1.2.2.4 主存储 17
2.1.2.2.5 镜像服务器 19
2.1.2.3 网络资源 21
2.1.2.3.1 网络拓扑 21
2.1.2.3.2 二层网络资源 22
2.1.2.3.3 三层网络 24
2.1.2.3.4 路由资源 25
2.1.2.3.5 VPC 27
2.1.2.4 网络服务 28
2.1.2.4.1 安全组 31
2.1.2.4.2 虚拟IP 32
2.1.2.4.3 弹性IP 34
2.1.2.4.4 端口转发 36
2.1.2.4.5 负载均衡 38
2.1.2.4.6 IPsec隧道 39
2.1.2.5 vCenter接管 40
2.1.2.6 裸金属管理（Plus） 42
2.1.2.6.1 裸金属集群 43
2.1.2.6.2 部署服务器 43

2.1.2.6.3 裸金属设备 44
2.1.2.6.4 裸金属主机 44
2.1.2.7 灾备服务（Plus） 44
2.1.2.7.1 备份任务 47
2.1.2.7.2 本地备份数据 47
2.1.2.7.3 本地备份服务器 47
2.1.2.7.4 远端备份服务器 48
2.1.2.8 企业管理（Plus） 48
2.1.2.8.1 平台管理员 51
2.1.2.8.2 组织架构 51
2.1.2.8.3 项目管理 52
2.1.2.8.4 工单管理 54
2.1.2.9 平台运维 55
2.1.2.9.1 性能TOP5 55
2.1.2.9.2 性能分析 56
2.1.2.9.3 ZWatch 56
2.1.2.9.4 通知服务 57
2.1.2.9.5 消息中心 58
2.1.2.9.6 操作日志 58
2.1.2.9.7 资源编排 58
2.1.2.10 平台管理 60
2.1.2.10.1 用户管理 60
2.1.2.10.2 计费管理 61
2.1.2.10.2.1 账单 61
2.1.2.10.2.2 计费设置 61
2.1.2.10.3 定时 61
2.1.2.10.3.1 定时器 61
2.1.2.10.3.2 定时任务 61
2.1.2.10.4 应用中心 62
2.1.2.10.5 邮箱服务器 62
2.1.2.10.6 AD/LDAP 62
2.1.2.10.7 控制台服务 63
2.1.2.10.8 证书 63
2.2 混合云 63
2.2.1 身份认证 65
2.2.2 互联网络 66
2.2.3 资源管理 68
2.2.4 业务实现 69
3 产品功能 70
3.1 专有云功能 70
3.2 混合云功能 84

4 产品优势 87
4.1 专有云优势 87
4.2 混合云优势 88
5 产品价值 89
5.1 专有云价值 89
5.2 混合云价值 89
专有云术语表 90
混合云术语表 93

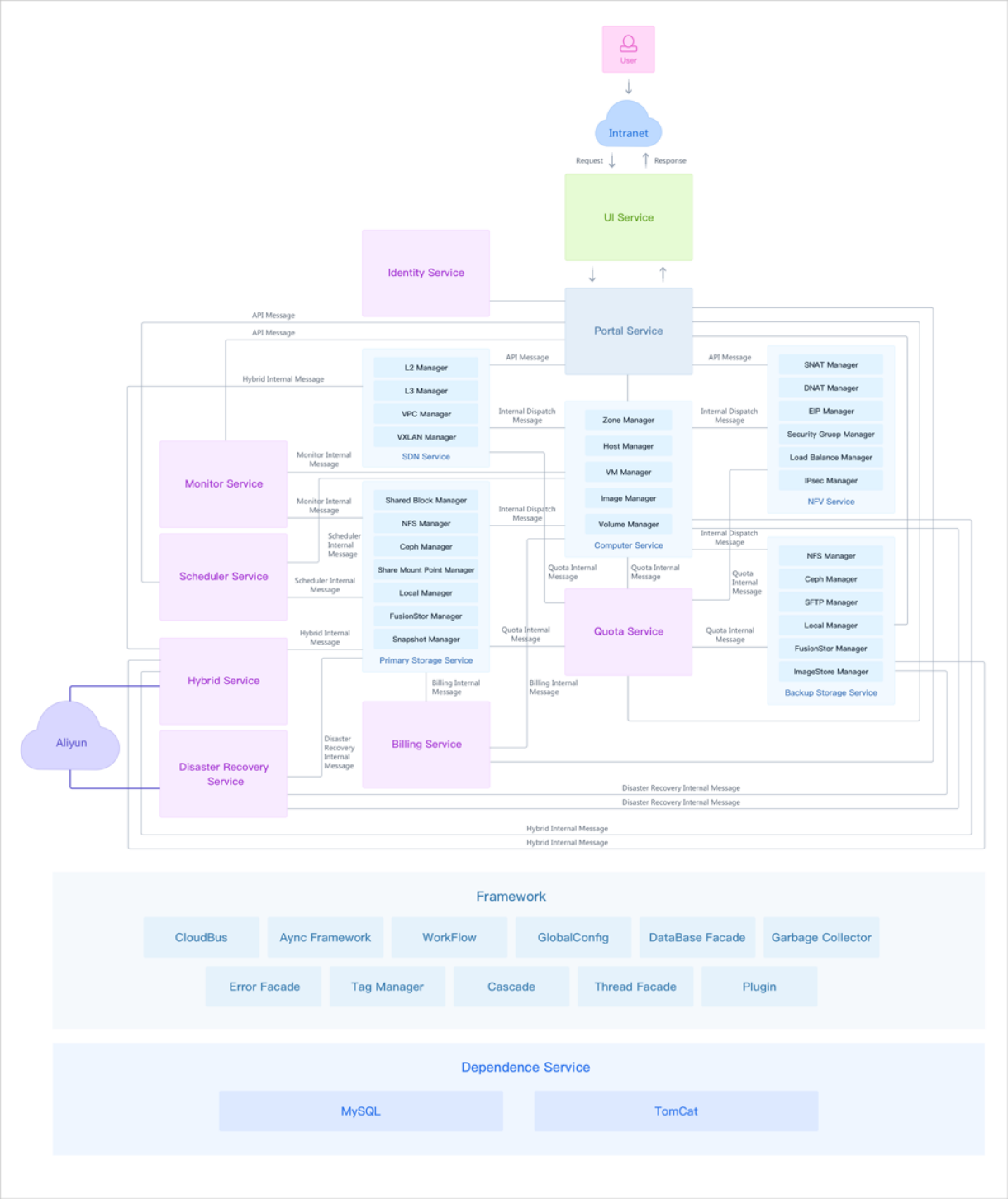
1 产品概述

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（软件及服务）等。

通过对ZStack云引擎的深度定制，阿里云和ZStack联合推出了具有混合云功能的ZStack for Alibaba Cloud，其结合了ZStack专有云的简单、健壮、弹性、智能以及阿里云公共云的领先、安全、稳定等特点，以**云+端**的形式提供了一套无缝集成的混合云管理方案。

系统架构如图 *1-1: 系统架构示意图*所示：

图 1-1: 系统架构示意图


User
Intranet
Request
Response
UI Service
Identity Service
Portal Service
API Message
API Message
API Message
API Message
Hybrid Internal Message
L2 Manager
L3 Manager
VPC Manager
VXLAN Manager
SDN Service
Internal Dispatch Message
Zone Manager
Host Manager
VM Manager
Image Manager
Volume Manager
Computer Service
Internal Dispatch Message
SNAT Manager
DNAT Manager
EIP Manager
Security Gruop Manager
Load Balance Manager
IPsec Manager
NFV Service
Monitor Service
Monitor Internal Message
Monitor Internal Message
Shared Block Manager
NFS Manager
Ceph Manager
Share Mount Point Manager
Local Manager
FusionStor Manager
Snapshot Manager
Primary Storage Service
Internal Dispatch Message
Scheduler Internal Message
Scheduler Service
Scheduler Internal Message
Internal Dispatch Message
Quota Internal Message
Quota Internal Message
Quota Internal Message
Quota Service
Quota Internal Message
Quota Internal Message
NFS Manager
Ceph Manager
SFTP Manager
Local Manager
FusionStor Manager
ImageStore Manager
Backup Storage Service
Hybrid Internal Message
Hybrid Service
Billing Internal Message
Billing Internal Message
Billing Service
Aliyun
Disaster Recovery Internal Message
Disaster Recovery Service
Disaster Recovery Internal Message
Disaster Recovery Internal Message
Hybrid Internal Message
Hybrid Internal Message
Framework
CloudBus
Aync Framework
WorkFlow
GlobalConfig
DataBase Facade
Garbage Collector
Error Facade
Tag Manager
Cascade
Thread Facade
Plugin
Dependence Service
MySQL
TomCat

2 产品剖析

本章主要对ZStack专有云以及基于ZStack深度定制的ZStack for Alibaba Cloud混合云产品进一步剖析介绍。

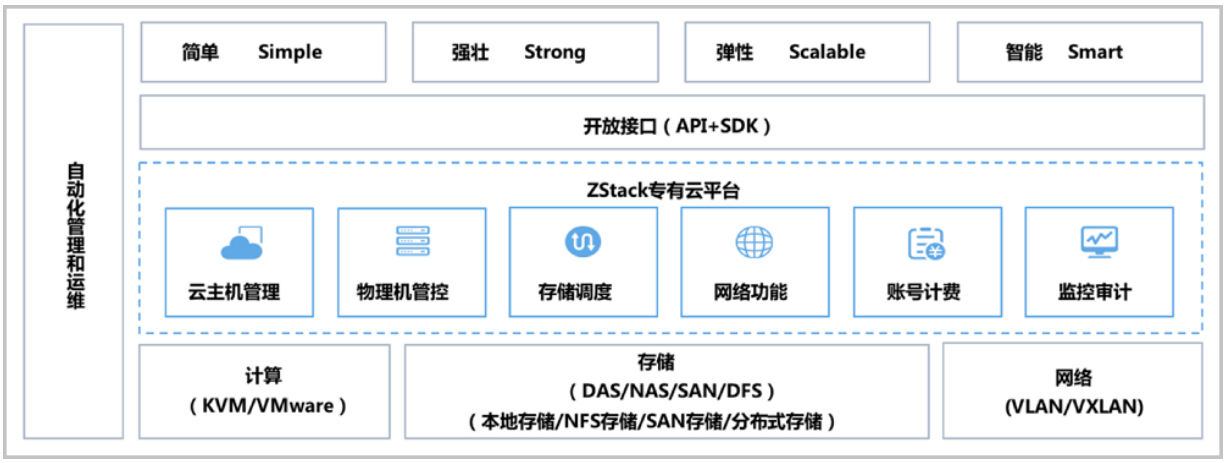
2.1 专有云

ZStack作为新一代产品级专有云管理平台，通过提供灵活完善的APIs来管理包括计算、存储和网络在内的数据中心各种资源。

2.1.1 ZStack功能架构

ZStack功能架构如图 *2-1: ZStack功能架构*所示：

图 2-1: 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。

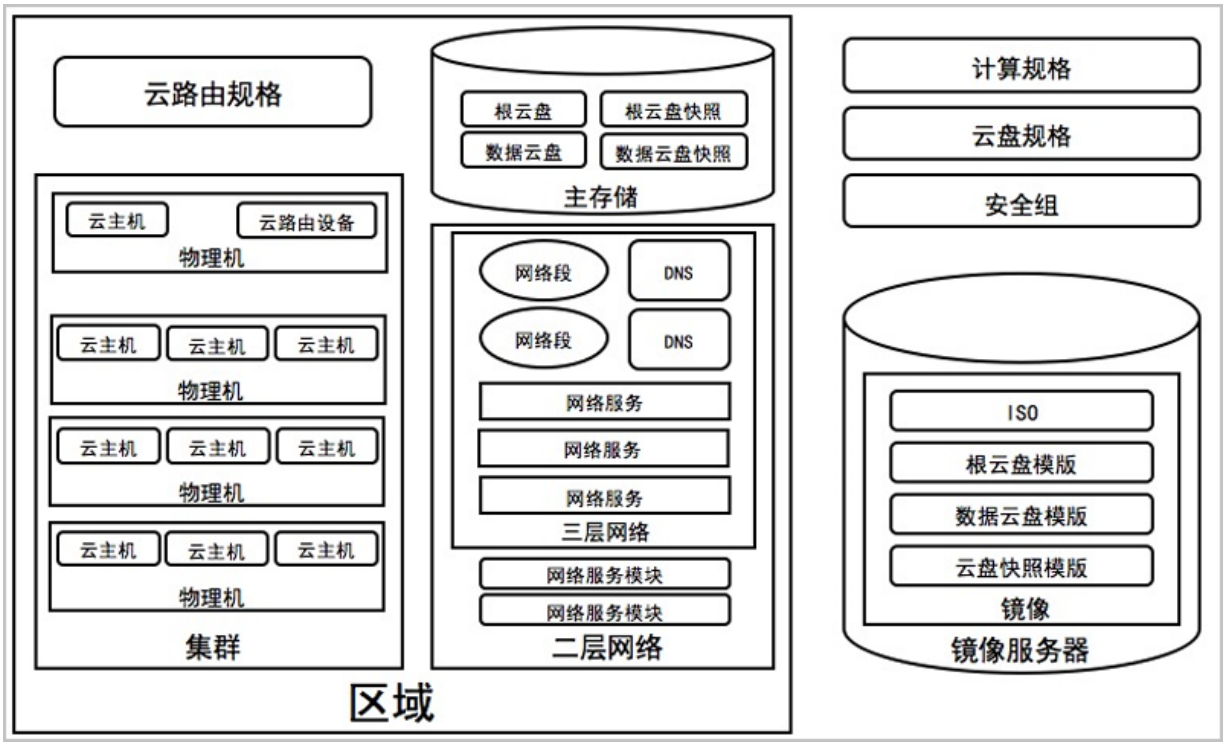
- 进程内微服务，以星状架构实现各服务独立运行，将高度集中的控制业务进行解耦，实现了系统的高度自治和高度隔离，任何服务出现故障并不影响其他组件。可靠性与稳定性得到有效保障。

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。

2.1.2 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 *2-2: ZStack资源结构*所示：

图 2-2: 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、FusionStor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、FusionStor类型。
- VXLAN Pool：VXLAN网络中的Underlay网络，一个 VXLAN Pool可以创建多个VXLAN Overlay网络，这些Overlay网络运行在同一组Underlay网络设施上。
- 二层网络：对应于一个二层广播域，进行二层相关的隔离。一般用物理网络的设备名称标识。支持 L2NoVLANNetwork、L2VLANNetwork、VXLANNetwork类型。
- 三层网络：云主机使用的网络配置，包含了IP地址范围、网关、DNS、网络服务等。
- 计算规格：云主机的CPU、内存、磁盘带宽、网络带宽的数量或大小规格定义。
- 云盘规格：云主机使用的云盘的大小规格定义。

- 云主机：运行在物理主机上的虚拟机实例，具有独立的IP地址，可以访问公共网络，运行应用服务，是ZStack的核心组成部分。
- 镜像：云主机或云盘所使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像，其中系统云盘镜像支持ISO和Image类型， 数据云盘镜像支持Image类型。
- 根云盘：安装云主机操作系统的磁盘，用于支撑云主机的系统运行。
- 数据云盘：为云主机提供了额外的存储空间，用于云主机的存储扩展。
- 快照：采用增量机制对云盘在特定时间点上的数据进行备份。
- 网络服务模块：用于提供网络服务的模块。在UI界面已隐藏。
- 网络服务：给云主机提供的各种网络服务，主要包括安全组、虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道等。
- 安全组：给云主机提供三层网络防火墙控制。
- 云路由规格：指定云路由器使用的CPU、内存、云路由镜像、管理网络、公有网络等资源定义。
- 云路由器：为云主机提供分布式DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等各种网络服务的定制云主机。
- VPC路由器：基于云路由规格直接创建的路由器，拥有公有网络和管理网络，是VPC的核心。公有网络作为默认网络，用于提供各种网络服务，包括：DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等。

ZStack资源间存在以下关系：

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

> **说明**：
>
> 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。

2.1.2.1 云资源池

2.1.2.1.1 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 for Alibaba Cloud的核心组成部分。

2.1.2.1.2 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。

2.1.2.1.3 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。
- 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*

说明：

- 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或FusionStor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或FusionStor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。

说明：

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。

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

- 反亲和组(非强制)：

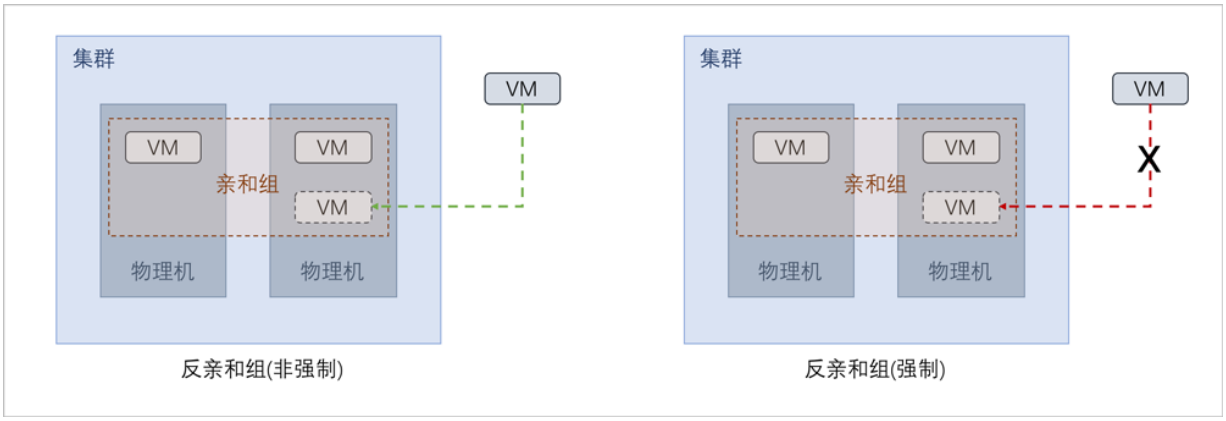
  将亲和组内的云主机尽量分配到不同物理机上，当没有更多物理机可分配时，回归普通分配策略。

- 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 *2-3: 反亲和组(非强制)与反亲和组(强制)*所示：

图 2-3: 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。

2.1.2.1.5 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。

2.1.2.1.6 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。

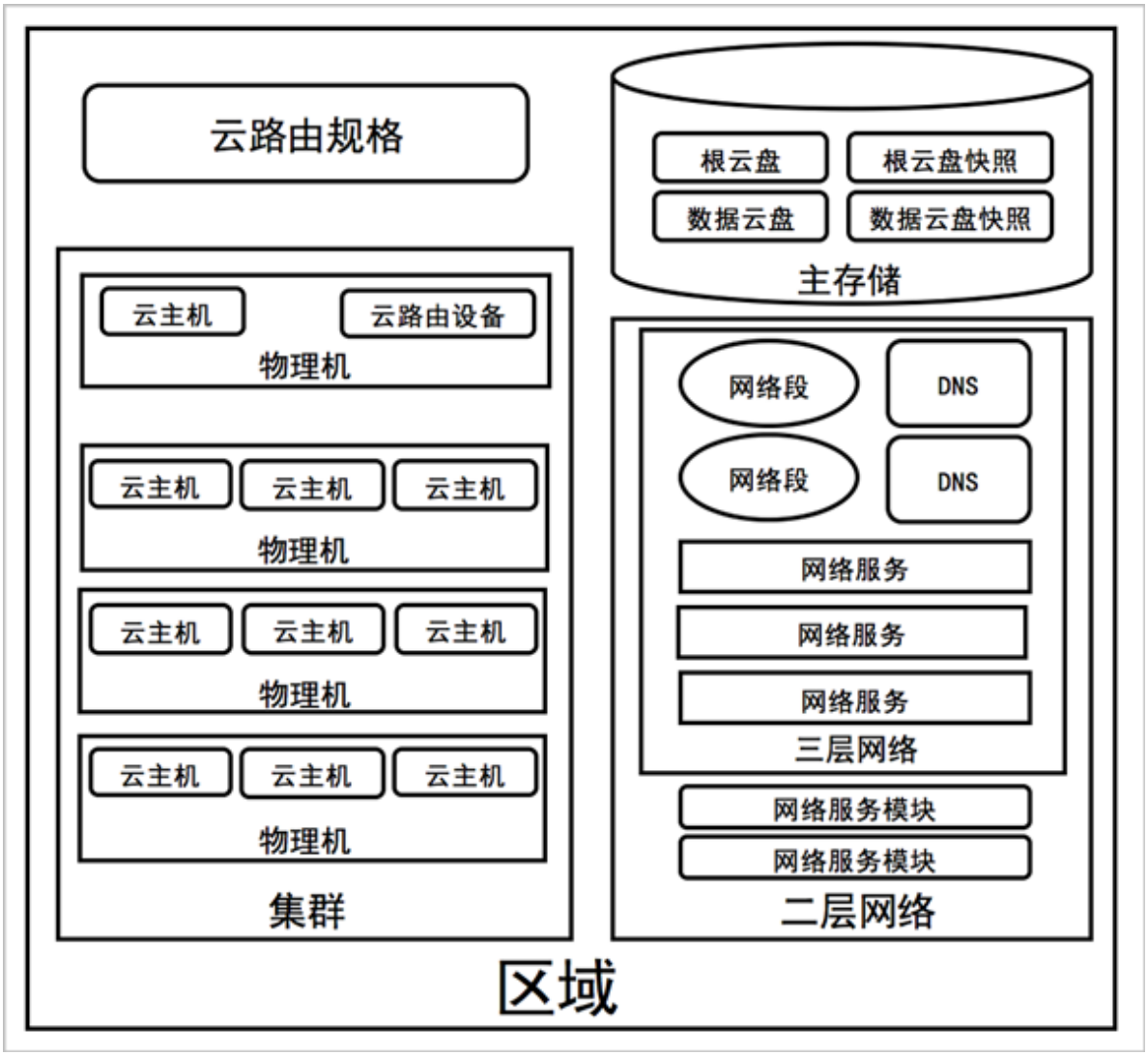
2.1.2.2 硬件设施

2.1.2.2.1 区域

区域：ZStack for Alibaba Cloud中最大的一个资源定义，包括集群、二层网络、主存储等资源。

- 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 *2-4:* 区域资源结构所示，区域中的资源以如下形式组织：

图 2-4: 区域资源结构



2.1.2.2.2 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：

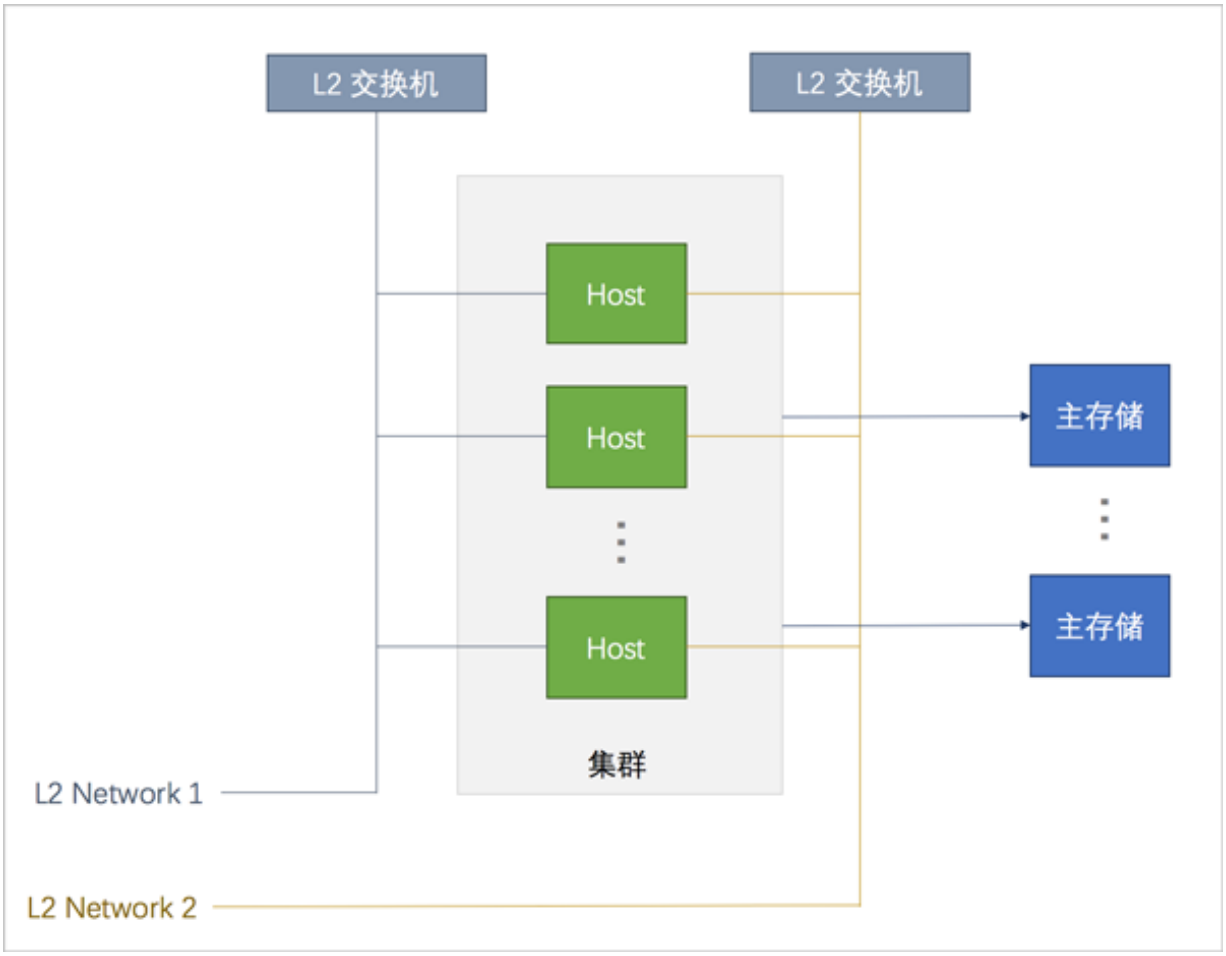
集群 | 区域

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 *2-5:* 集群、主存储、二层网络的关系所示：

图 2-5: 集群、主存储、二层网络的关系



说明：

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。

  目前支持的场景有：

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

- 一个集群可以挂载一个本地主存储和一个Shared Mount Point主存储。
- 一个集群可以挂载一个本地主存储和一个Shared Block主存储。
- 一个集群只能挂载一个Ceph主存储，除此外不能再挂载新的存储。
- 一个集群只能挂载一个FusionStor主存储，除此外不能再挂载新的存储。
- 一个集群只能挂载一个AliyunNAS主存储，除此外不能再挂载新的存储。
- 一个主存储可以挂载到多个集群 。

主存储与集群的依赖关系如表 *2-6:* 主存储与集群关系所示：

表 2-1: 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
Share Mount Point	支持挂载一个SMP
Ceph	为挂载到集群的Ceph，有且仅有一个
FusionStor	为挂载到集群的FusionStor，有且仅有一个
AliyunNAS	为挂载到集群的AliyunNAS，有且仅有一个
LocalStorage + NFS	支持挂载1个LocalStorage + 1个NFS
LocalStorage + SMP	支持挂载1个LocalStorage + 1个SMP
LocalStorage + Shared Block	支持挂载1个LocalStorage + 1个Shared Block

- 集群挂载多个本地存储时，务必在添加物理机以及添加主存储之前，提前在物理机对应URL上做好分区，确保每个本地存储部署在独占的逻辑卷或物理磁盘上。
- 主存储可以被所在集群中的所有物理机访问。
- 如果数据中心的网络拓扑发生改变导致主存储不能被集群中的物理机继续访问时，主存储可以从集群卸载。

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。

说明：

- 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 *2-6:* 主存储与镜像服务器的关系所示：

表 2-2: 主存储与镜像服务器的关系

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

2.1.2.2.3 物理机

物理机：也称之为计算节点，主要为云主机实例提供计算、网络、存储等资源的物理服务器。

如图 *2-6:* 物理机所示：

图 2-6: 物理机

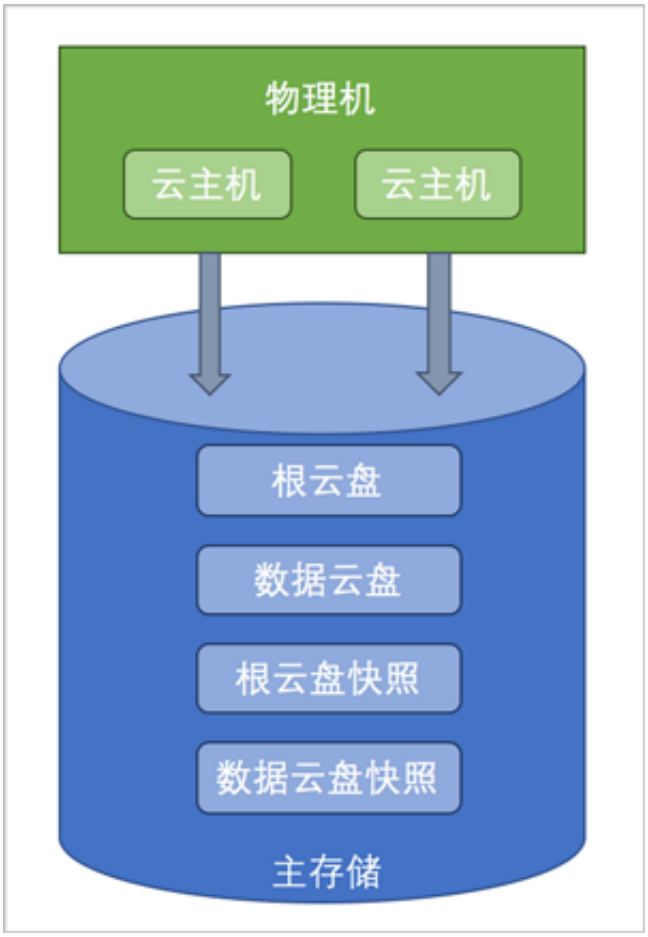
- 物理机是ZStack for Alibaba Cloud云管理平台里的核心资产，云主机运行在物理机之上。

2.1.2.2.4 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 *2-7:* 主存储所示：

图 2-7: 主存储



主存储支持类型可分为以下两大类：

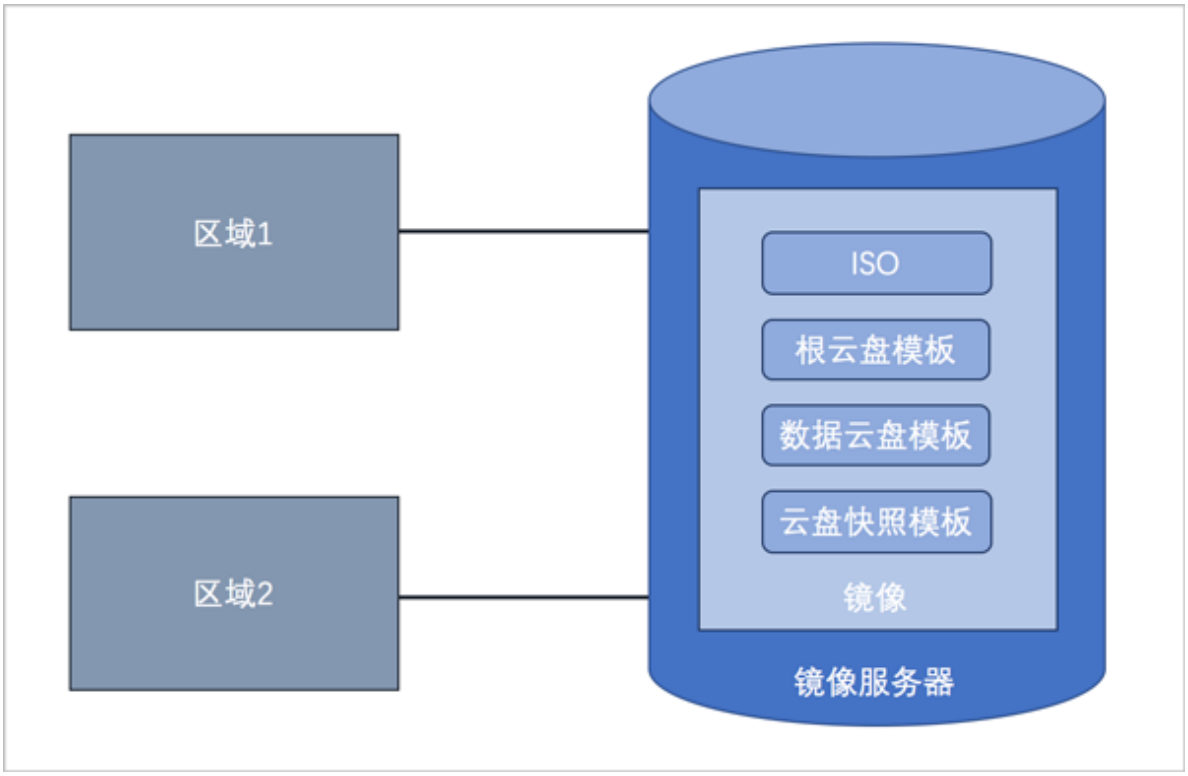
- **本地存储**（Local Storage）：使用物理机的硬盘进行存储。
- **网络共享存储**：支持NFS、Shared Mount Point、Ceph、FusionStor、Shared Block、AliyunNAS类型。
  - NFS为网络文件系统的存储方式。
  - Shared Mount Point支持常用的分布式文件系统提供的网络共享存储，支持的常见类型有MooseFS、GlusterFS、OCFS2、GFS2等。
  - Ceph采用了分布式块存储方式。
  - FusionStor采用了华云网际提供的分布式块存储方式。
  - Shared Block采用了共享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

2.1.2.2.5 镜像服务器

镜像服务器：用于保存镜像模板的存储服务器。

- 镜像服务器必须挂载到区域之后，区域中的资源才能访问它。通过镜像服务器，可在多个区域之间共享镜像。
- 如图 *2-8:* 镜像服务器所示：

图 2-8: 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和Ceph类型的主存储，支持在线/暂停/关机克隆；Shared Block类型的主存储，支持暂停/关机克隆；
   - ImageStore类型的镜像服务器间支持镜像同步。

2. **Sftp**：
   - 仅社区版本支持；
   - 以文件方式存储镜像文件；
   - 支持云主机的关机快照、关机创建镜像。
   - 创建的镜像可以在镜像服务器上，以对应的镜像路径访问，拷贝到其他云环境可直接使用。
3. **Ceph镜像服务器**：
   - 以Ceph分布式块存储方式存储镜像文件；
   - 支持云主机的在线/关机快照、在线/关机创建镜像；
   - 支持不带数据云盘在线/暂停/关机克隆；不支持整机克隆。
   - 导出镜像需在镜像服务器上导出。

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

     则需镜像服务器执行：

     ```
     rbd export -p bak-t-c9923f9821bf45498fdf9cdfa1749943 --image 61ece0adc7
     244b0cbd12dafbc5494f0c /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
     ```
4. **FusionStor镜像服务器**：
   - 以FusionStor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、关机创建镜像，不支持在线创建镜像和在线/关机克隆。
   - 导出镜像需要在镜像服务器上执行类似命令：

     ```
     lichbd export bak-t-8e694c40cf214db1af9e5d641b2e792d/8f1e0debfae042e5ae07
     4133a59c0622 /root/test.img -p nbd
     ```

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 2-3: 主存储与镜像服务器的关系

PS\BS	ImageStore	Sftp	Ceph	FusionStor
LocalStorage	○	○	×	×
NFS	○	○	×	×

Shared Mount Point	○	○	×	×
Ceph	○	×	○	×
FusionStor	×	×	×	○
Shared Block	○	×	×	×
AliyunNAS	○	×	×	×

- 当主存储为本地存储（LocalStorage）、NFS、Share Mount Point或Shared Block类型时，镜像服务器的默认类型为ImageStore（企业版）或Sftp（社区版）。
- 当主存储为NFS或Shared Mount Point类型时，可将相应共享目录手动挂载到相应镜像服务器的本地目录上，从而使主存储和镜像服务器均能使用网络共享存储方式。
- 当主存储为Ceph类型时，镜像服务器可以使用同一个Ceph集群作为镜像服务器，也可以使用镜像仓库类型的镜像服务器。Ceph集群提供分布式块存储方式存储镜像文件。
- 当主存储为FusionStor类型时，镜像服务器必须使用同一个FusionStor集群作为镜像服务器。FusionStor集群提供分布式块存储方式存储镜像文件。

2.1.2.3 网络资源

2.1.2.3.1 网络拓扑

ZStack for Alibaba Cloud 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 2-9: 全局拓扑

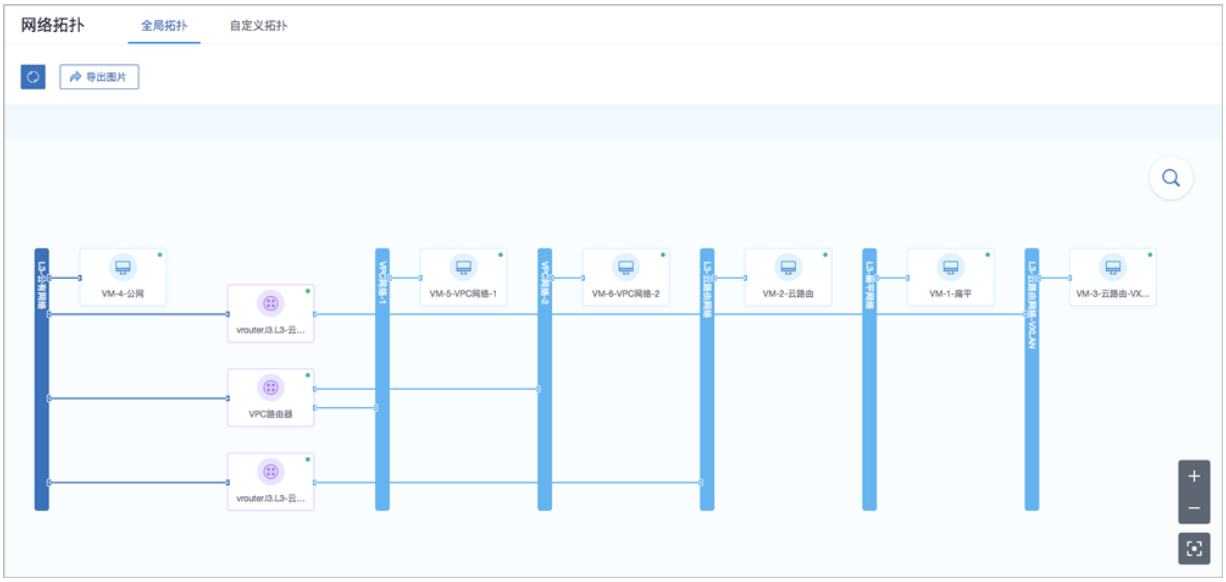
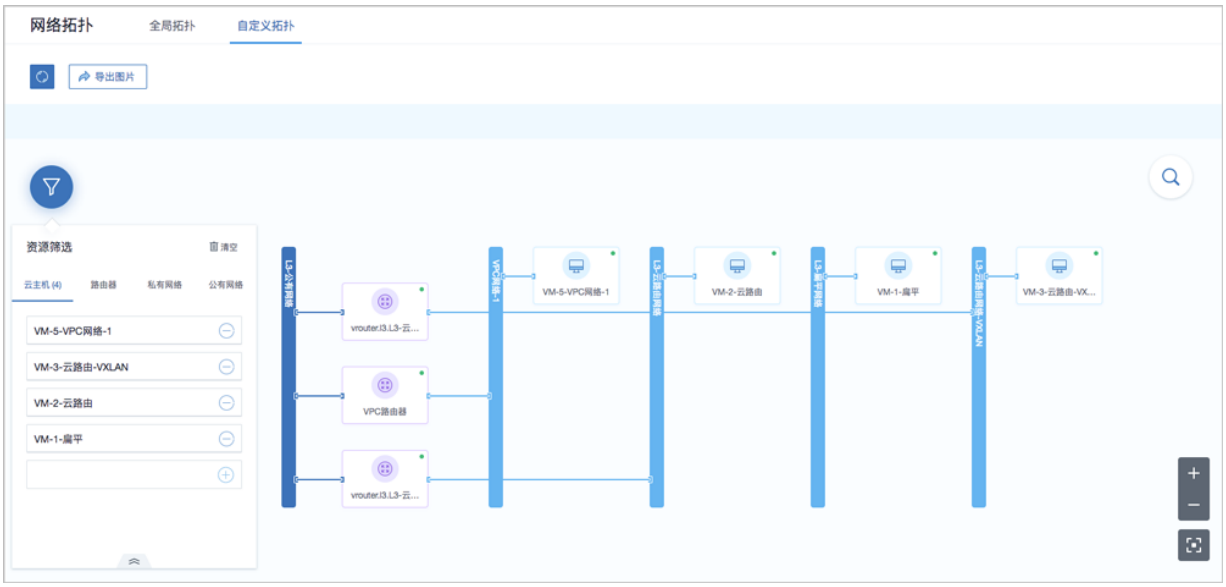


图 2-10: 自定义拓扑



2.1.2.3.2 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，最大支持16M个逻辑子网。

- VXLAN Pool和VxlanNetwork共同提供了VxlanNetwork类型的配置，使用VxlanNetwork需先创建VXLAN Pool，VxlanNetwork对应了VXLAN Pool里的一个虚拟网络。
- VXLAN Pool最大可支持16777216（16M）个虚拟网络。其Vni（VXLAN网络ID）范围可从1-16777216设置。
- 在创建VXLAN Pool时，如果需要加载到相应集群，则需设置相应的VTEP（VXLAN隧道端点）。
- VTEP一般对应于集群内计算节点中的某一网卡的IP地址，ZStack for Alibaba Cloud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。

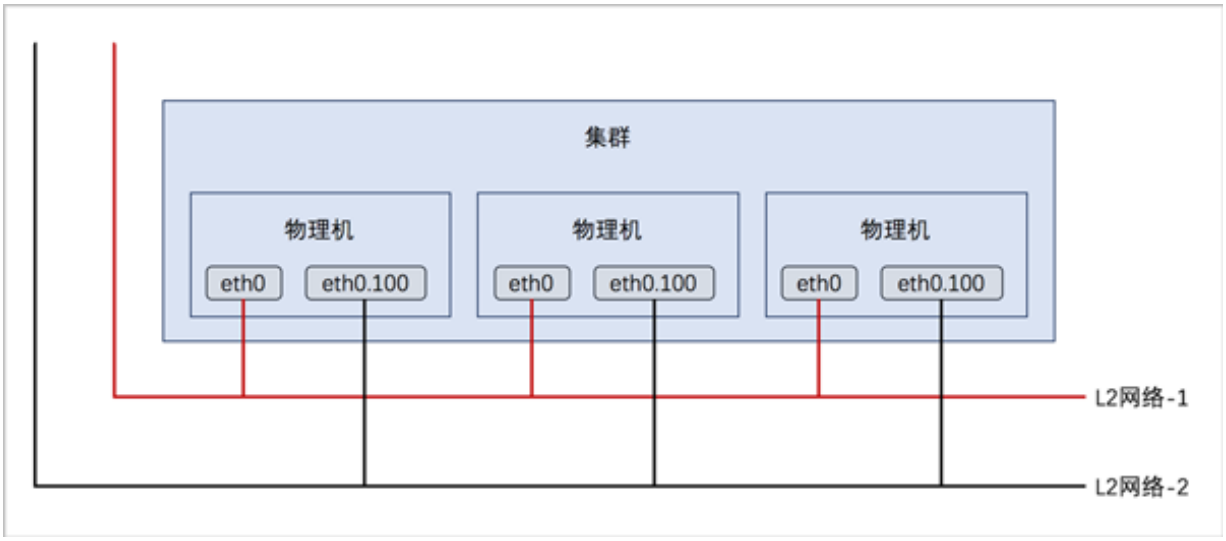
二层网络

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 *2-11:* 二层网络所示：

图 2-11: 二层网络



二层网络主要支持以下三种类型：

1. **L2NoVlanNetwork**

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

   - 如果交换机端口设置了VLAN，则需在交换机端配置Access模式
   - 如果交换机端口没有设置VLAN, 则无须特别设置

2. **L2VlanNetwork**

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

   - 从逻辑上划分虚拟局域网，支持1- 4094个子网
   - 此类型需在物理机接入的交换机端进行Trunk设置

3. **VxlanNetwork**

   VxlanNetwork类型表示使用VXLAN的子网进行网络配置，需要先建立VXLAN Pool，再建立VxlanNetwork。

说明：

- 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。

2.1.2.3.3 三层网络

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

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

公有网络

可直接连通互联网的网络，在云路由网络、VPC中可以提供网络服务。

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

系统网络

管理节点用于特定用途的网络。

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

私有网络

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

特定场景网络

- 管理网络

  作为系统网络的一种，用于管理控制对应的物理资源。

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

  特指在进行分布式存储部署时，底层存储系统通信使用的网络。在添加主存储时，可标识存储网络的CIDR，表示使用此网络来判断云主机健康状态。
- VDI网络

  在创建集群时，可以指定VDI网络的CIDR，此网络用于VDI连接的协议流量。

2.1.2.3.4 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、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等网络服务。

云路由主要包括云路由镜像、云路由规格和云路由器。

- 云路由镜像：封装多种网络服务，只为创建云路由提供服务。
- 云路由规格：定义云路由器使用的CPU、内存、云路由镜像、公有网络、管理网络等。
- 云路由器：作为定制的Linux云主机提供DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec隧道、安全组等网络服务。

云路由网络拓扑

云路由主要涉及以下3个基本网络：

- 公有网络：

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

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

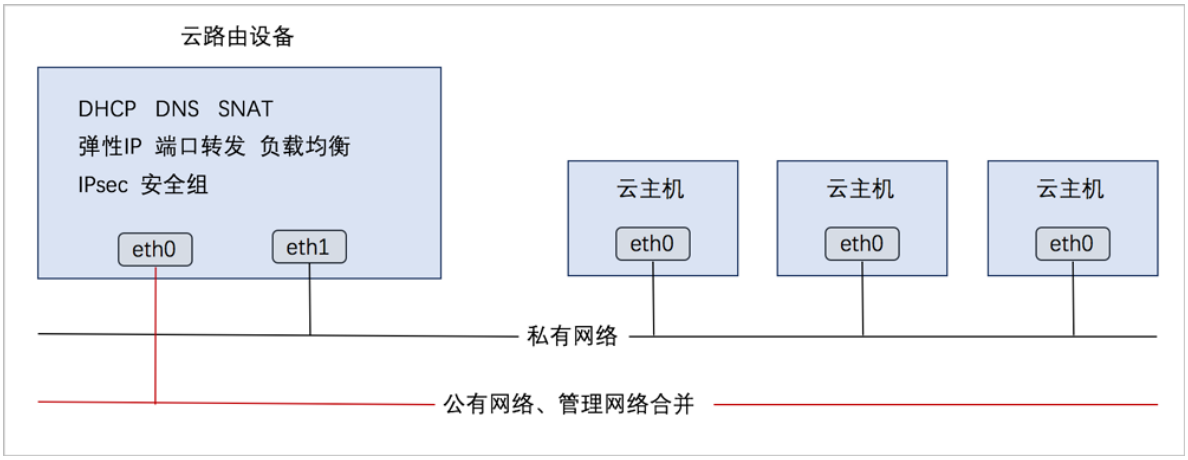
也称之为业务网络或接入网络，是云主机使用的内部网络。

云路由网络部署方式：

- 公有网络和管理网络合并，私有网络独立部署

  如图 2-12: 部署方式-1所示：

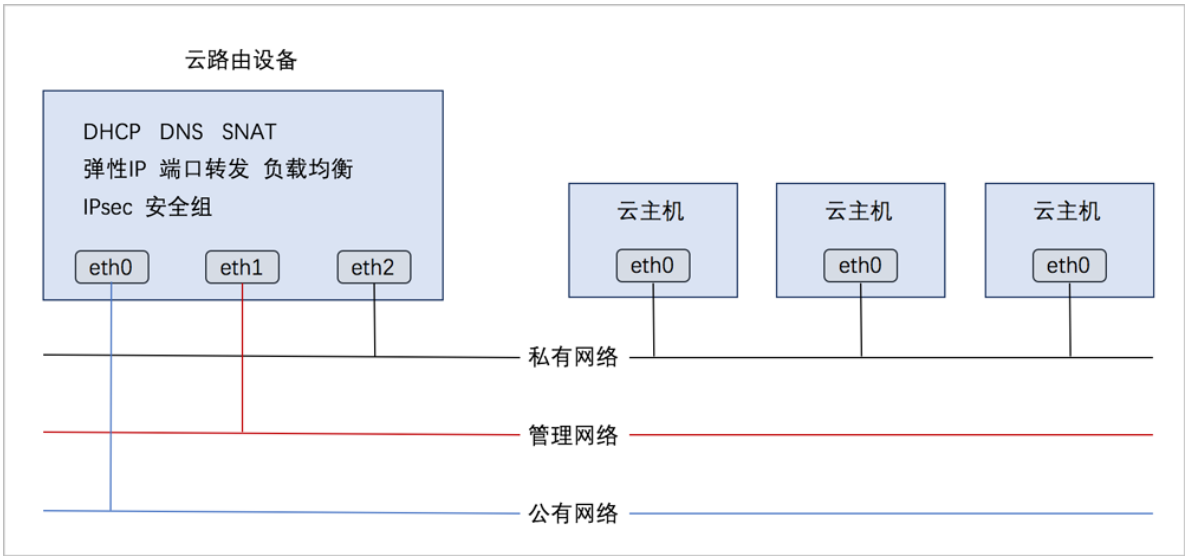
  图 2-12: 部署方式-1



- 公有网络、管理网络、私有网络均独立部署

  如图 2-13: 部署方式-2所示：

  图 2-13: 部署方式-2



云路由网络服务

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

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

2.1.2.3.5 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云路由器，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特点

VPC具有以下特点：

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

VPC网络服务

VPC网络作为VPC的私有网络，使用VPC路由器提供各种网络服务。

- DHCP：默认采用扁平网络服务模块提供分布式DHCP服务。
- DNS：VPC路由器作为DNS服务器提供DNS服务。在云主机中看到的DNS地址默认为VPC路由器的IP地址，用户设置的DNS地址由VPC路由器负责转发配置。
- SNAT：VPC路由器向云主机提供原网络地址转换，云主机使用SNAT可直接访问外部互联网。
- 安全组：由安全组网络服务模块提供安全组服务，使用iptables进行云主机防火墙的安全控制。
- 弹性IP：可绑定弹性IP到VPC网络，实现公有网络到云主机私有网络的互联互通。
- 端口转发：提供公网IP到云主机私有网络IP的端口到端口的相关网络协议的互通。
- 负载均衡：将公网地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
- IPsec隧道：使用IPsec隧道协议实现虚拟私有网络（VPN）的互联互通。

2.1.2.4 网络服务

ZStack for Alibaba Cloud给云主机提供各种网络服务，主要包括安全组、虚拟IP、弹性IP、端口转发、负载均衡、IPsec隧道等。

支持以下三种网络架构模型：

- 扁平网络
- 云路由网络
- VPC

网络服务模块

网络服务模块：用于提供网络服务的模块。在UI界面已隐藏。

主要有以下四种：

1. VirtualRouter（虚拟路由器网络服务模块，不建议使用）

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

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

   提供以下网络服务：

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

     说明：
     DHCP服务包含了DNS的功能。

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

3. vrouter（云路由网络服务模块）

   提供以下网络服务：

   - IPsec：使用IPsec隧道协议实现虚拟私有网络（VPN）的连接。
   - VRouterRoute：通过云路由路由表，用户可管理自定义路由。
   - CentralizedDNS：在启用分布式DHCP服务的场景下，提供DNS服务。
   - VipQos：虚拟IP限速，限制上行及下行带宽。
   - DNS：使用云路由器提供DNS服务。
   - SNAT：云主机使用SNAT可以直接访问外部互联网。
   - 负载均衡：将公网地址的访问流量分发到一组后端的云主机上，并自动检测并隔离不可用的云主机。
   - 端口转发：提供将指定公有网络的IP地址端口流量转发到云主机对应协议的端口。
   - 弹性IP：使用云路由器可通过公有网络访问云主机的私有网络。
   - DHCP：集中式DHCP服务

4. SecurityGroup（安全组网络服务模块）

   提供以下网络服务：

- 安全组：使用iptables进行云主机防火墙的安全控制。

扁平网络实践

生产环境中，一般建议使用以下网络服务的组合：

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

> **说明**：
> DHCP服务包含了DNS的功能。

- 安全组网络服务模块：
  - 安全组：使用iptables进行云主机防火墙的安全控制。

云路由网络实践

生产环境中，一般建议使用以下网络服务的组合：

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

VPC网络实践

生产环境中，一般建议使用以下网络服务的组合：

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

2.1.2.4.1 安全组

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

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

安全组规则：

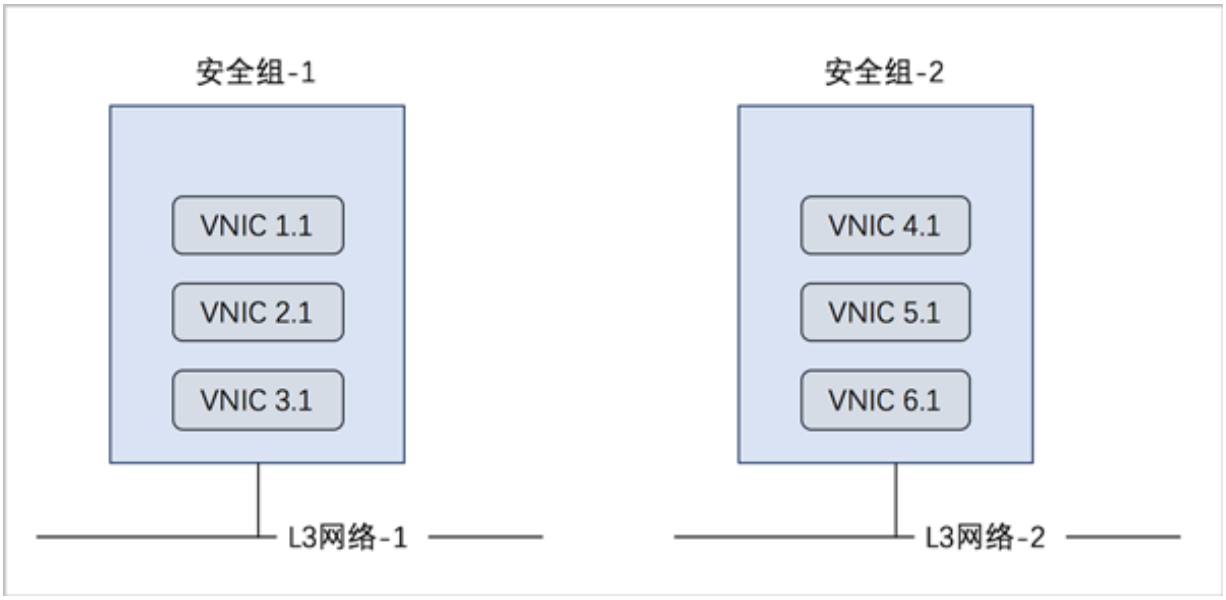
- 安全组规则按数据包的流向分为两种类型：
  - 入方向（Ingress）：代表数据包从外部进入云主机。
  - 出方向（Egress）：代表数据包从云主机往外部发出。
- 安全组规则对通信协议支持以下类型：
  - ALL：表示涵盖所有协议类型，此时不能指定端口。

  - TCP：支持1-65535端口。
  - UDP：支持1-65535端口。
  - ICMP：默认起始结束端口均为-1，表示支持全部的ICMP协议。
- 安全组规则支持对数据来源的限制，目前源可以设置为CIDR和安全组。
  - CIDR作为源：仅允许指定的CIDR才可通过
  - 安全组作为源：仅允许指定的安全组内的云主机才可通过

> **说明**：
> 如果两者都设置，只取两者交集。

如图 *2-14:* 安全组所示：

图 2-14: 安全组



2.1.2.4.2 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。

- 虚拟IP一般是将可以访问互联网的公有IP地址，路由到云主机的私有网络。
- 虚拟IP分为自定义虚拟IP和系统虚拟IP两类。

  1. 自定义虚拟IP
     - 创建：由用户手动创建。

- 提供网络服务：
  - 扁平网络下的自定义虚拟IP仅用于弹性IP服务。
  - 云路由网络/VPC下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务。
  - 一个自定义虚拟IP仅用于一个弹性IP服务实例。
  - 一个自定义虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

    说明：
    不同类型服务不能使用相同的端口号。
  - 自定义虚拟IP不支持跨普通云路由器/VPC路由器使用。
- 删除：
  - 删除自定义虚拟IP，将自动删除其上绑定的所有服务。
  - 删除自定义虚拟IP的某一服务，并不影响其上绑定的其它服务运行。

2. 系统虚拟IP

- 创建：

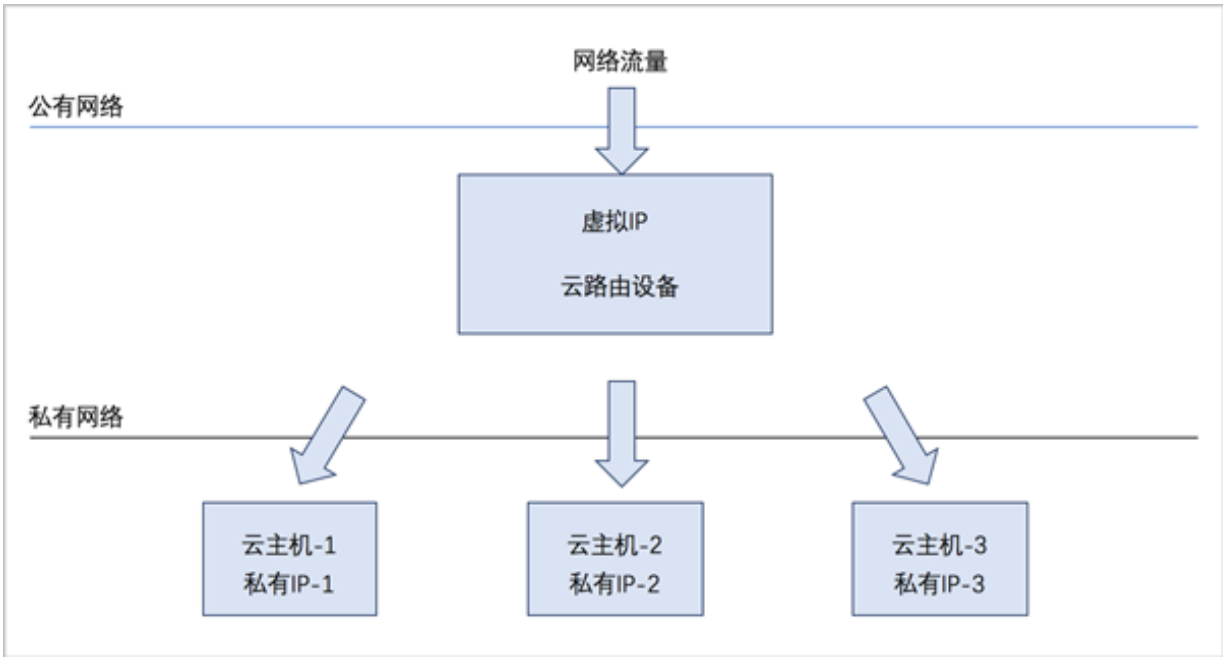
  普通云路由器/VPC路由器成功创建后，由系统自动创建，该系统虚拟IP地址就是路由设备的默认公网IP地址。
- 提供网络服务：
  - 云路由网络/VPC下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务。
  - 一个系统虚拟IP可同时用于端口转发、负载均衡、IPsec隧道服务，且支持一种服务的多个实例。

    说明：
    不同类型服务不能使用相同的端口号。
  - 系统虚拟IP与普通云路由器/VPC路由器一一对应。
- 删除：
  - 删除系统虚拟IP的某一服务，并不影响其上绑定的其它服务运行。
  - 删除普通云路由器/VPC路由器，将自动删除相应的系统虚拟IP以及其上绑定的所有服务。

- 虚拟IP支持QoS：通过设置端口、限制上行及下行带宽，实现虚拟IP的端口流量控制。
  - 扁平网络下的自定义虚拟IP仅用于弹性IP服务，因此虚拟IP的QoS功能仅作用于弹性IP。
  - 云路由网络/VPC下的自定义虚拟IP可用于弹性IP、端口转发、负载均衡、IPsec隧道服务，因此提供这四种服务的自定义虚拟IP均支持QoS设置。
  - 云路由网络/VPC下的系统虚拟IP可用于端口转发、负载均衡、IPsec隧道服务，因此提供这三种服务的系统虚拟IP均支持QoS设置。
  - 若使用VirtualRouter类型的云路由镜像创建云路由网络，不支持虚拟IP的QoS设置。
  - 同一虚拟IP可设置多个QoS规则，不设置端口的QoS规则优先级最低。

如图 *2-15: 虚拟IP-负载均衡*所示，云路由网络/VPC下虚拟IP提供负载均衡服务。

图 2-15: 虚拟IP-负载均衡



2.1.2.4.3 弹性IP

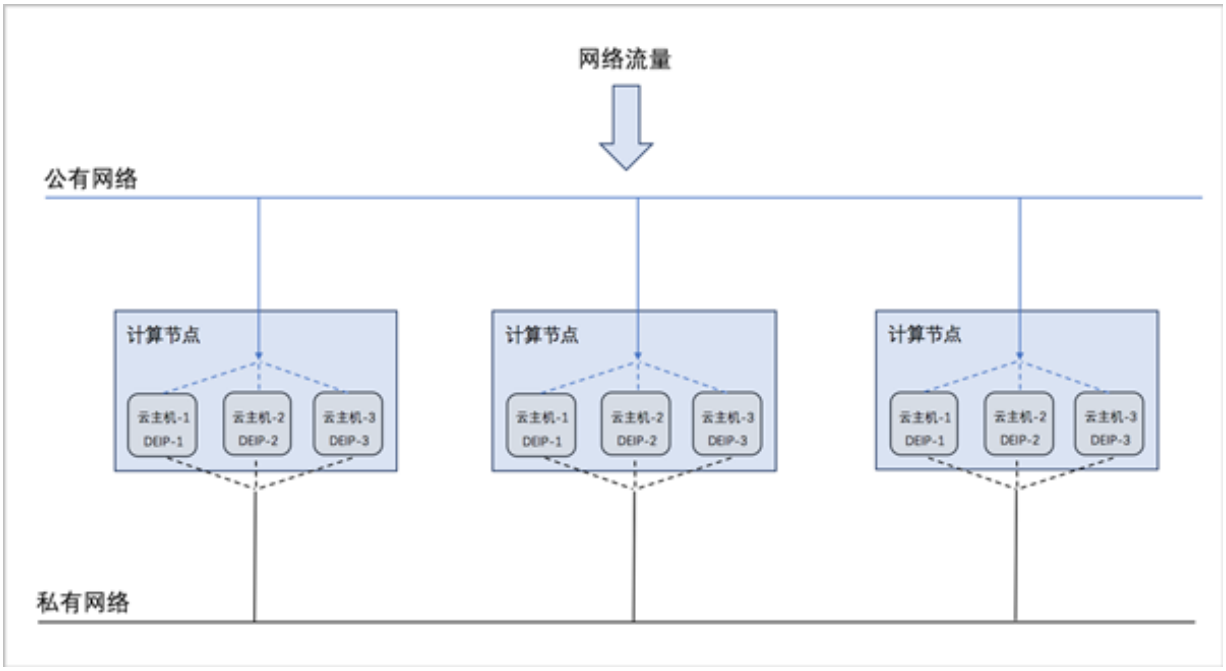
弹性IP（EIP）：定义了通过公有网络访问内部私有网络的方法。

- 内部私有网络是隔离的网络空间，不能直接被外部网络访问。
- 弹性IP基于网络地址转换（NAT），将一个网络（通常是公有网络）的IP地址转换成另一个网络（通常是私有网络）的IP地址；通过弹性IP，可对公网的访问直接关联到内部私网的云主机IP。
- 弹性IP可动态绑定到一个云主机，或从一个云主机解绑。

- 云主机使用的扁平网络、云路由网络、VPC均可使用弹性IP服务：
  - 扁平网络：分布式EIP实现的弹性IP地址，可通过公有网络访问内部私有网络。
  - 云路由网络/VPC：使用云路由器/VPC路由器可通过公有网络访问云主机的私有网络。

扁平网络下弹性IP的应用场景，如图 *2-16: 扁平网络下弹性IP的应用场景*所示：

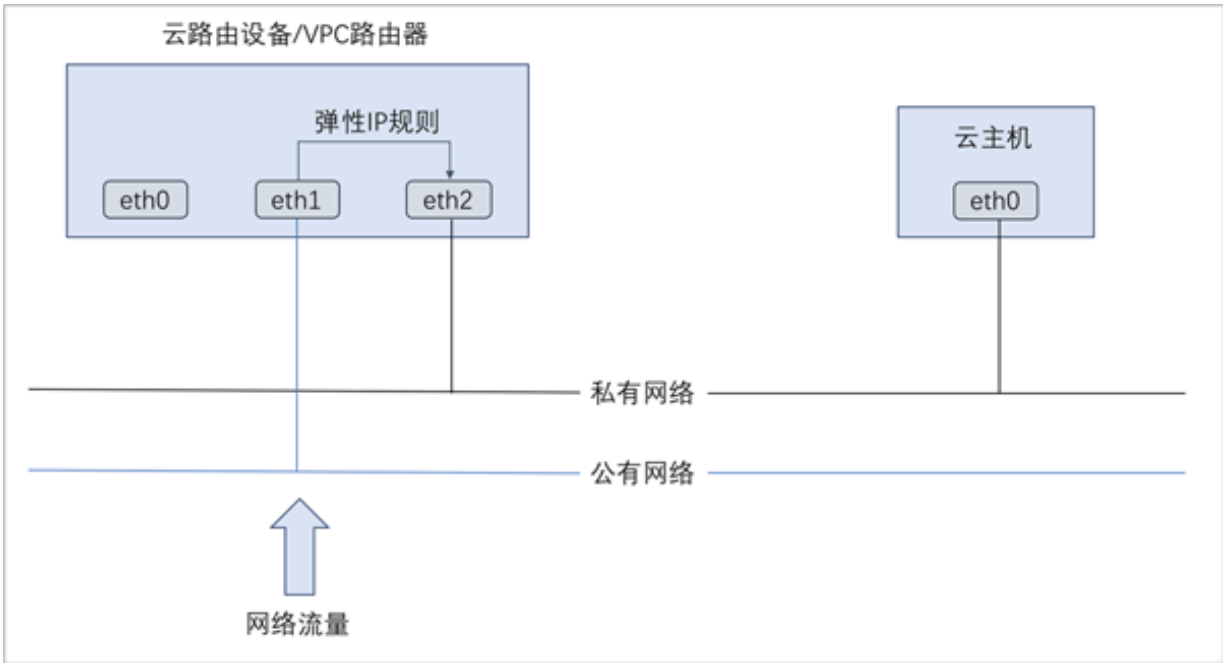
图 2-16: 扁平网络下弹性IP的应用场景



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

云路由网络/VPC下弹性IP的应用场景，如图 *2-17: 云路由网络/VPC下弹性IP的应用场景*所示：

图 2-17: 云路由网络/VPC下弹性IP的应用场景

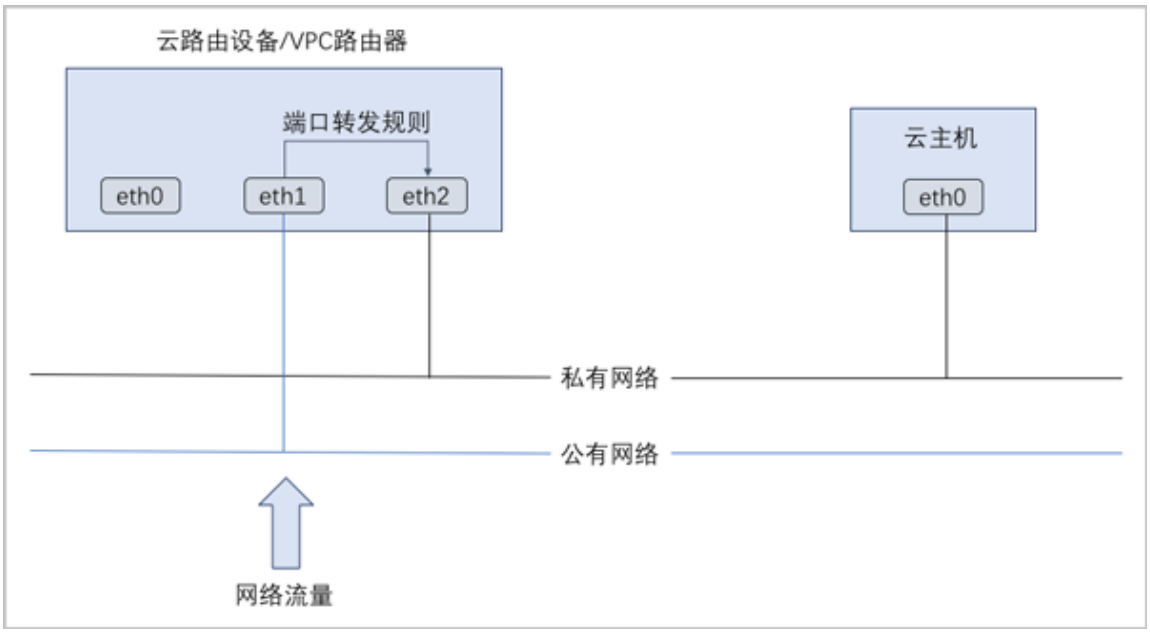


2.1.2.4.4 端口转发

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。

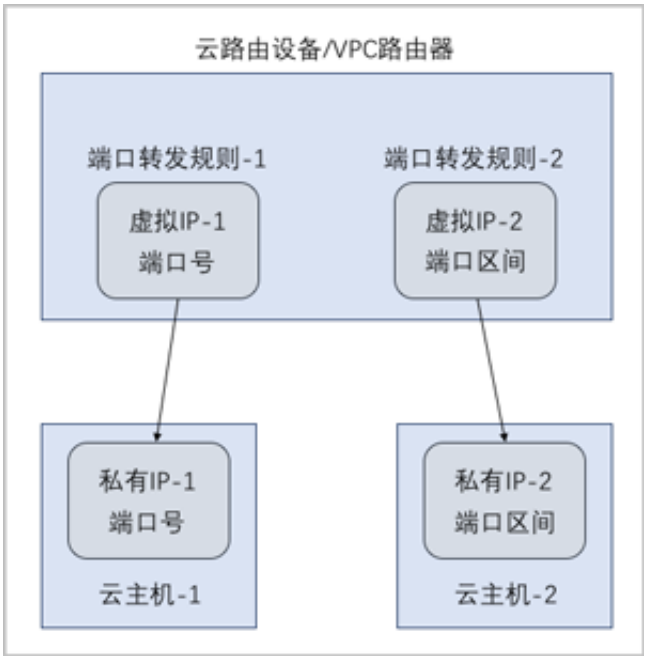
- 启用SNAT服务的私有网络中，云主机可访问外部网络但不能被外部网络所访问；使用端口转发规则，允许外部网络访问SNAT后面云主机的某些指定端口。
- 弹性端口转发规则可动态绑定到云主机，或从云主机解绑。
- 端口转发服务限于云路由器/VPC路由器提供。
  - 端口转发规则创建于云路由器/VPC路由器公有网络和云主机私有网络之间，如图 *2-18:* 端口转发所示：

图 2-18: 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 *2-19: 虚拟IP-端口转发*所示：

图 2-19: 虚拟IP-端口转发



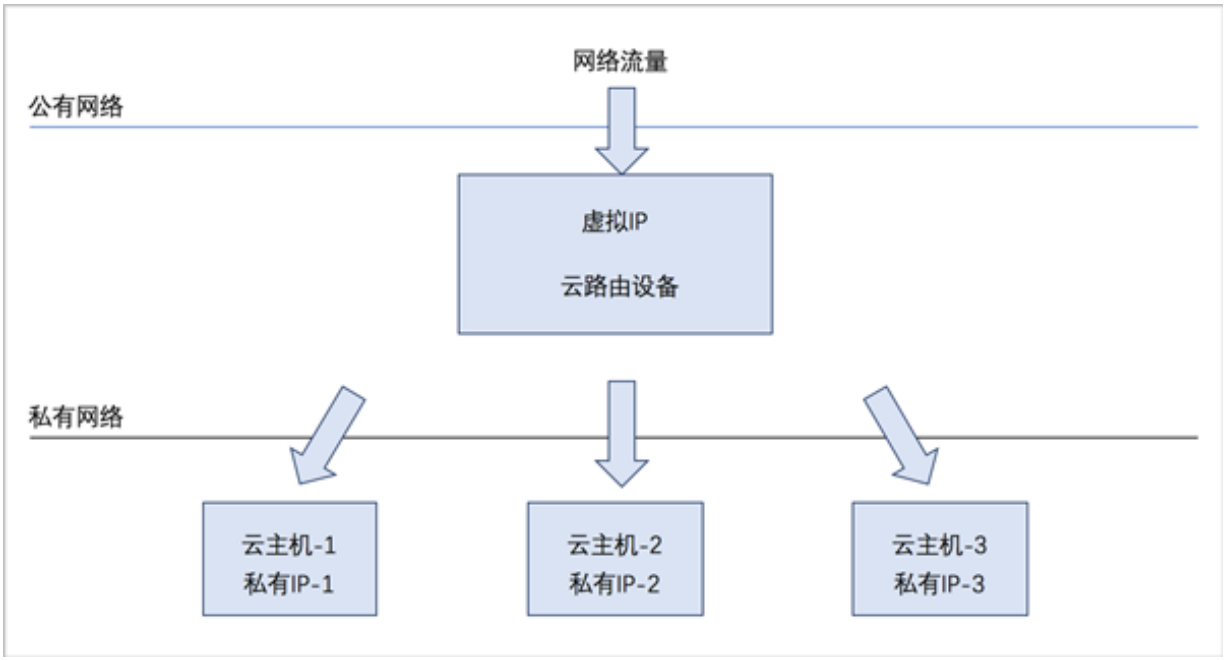
2.1.2.4.5 负载均衡

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

- 负载均衡自动把访问用户应用的流量分发到预先设置的多个后端云主机，以提供高并发高可靠的访问服务。
- 根据实际情况，动态调整负载均衡监听器中的云主机来调整服务能力，且不会影响业务的正常访问。
- 负载均衡监听器支持TCP/HTTP/HTTPS三种协议。
- 当监听协议为HTTPS，需绑定证书使用，支持上传证书和证书链。
- 负载均衡器支持灵活配置多种转发策略，实现高级转发控制功能。

如图 *2-20: 虚拟IP-负载均衡*所示，云路由网络/VPC下虚拟IP提供负载均衡服务。

图 2-20: 虚拟IP-负载均衡



2.1.2.4.6 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），不支持两端存在NAT网络。

- **IPsec路由模型**

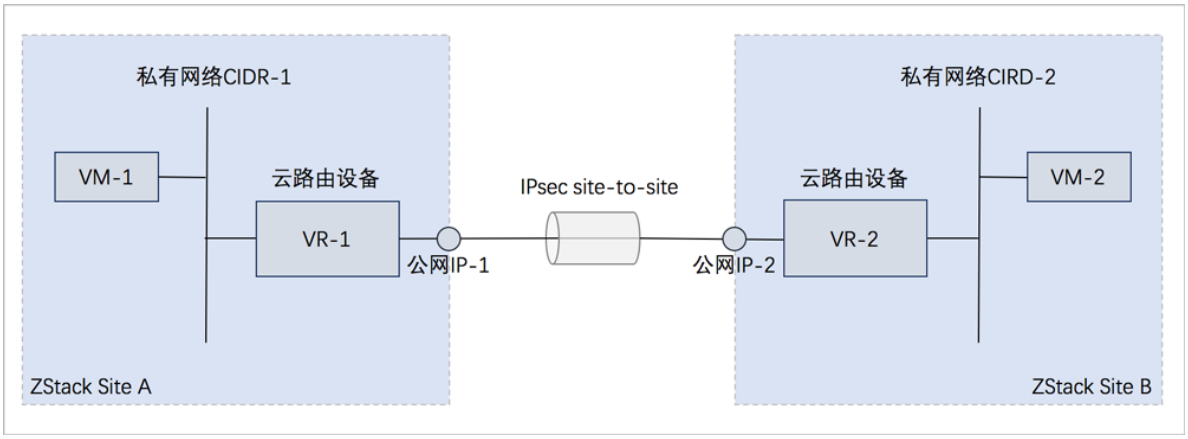
  仅支持基于对端网段配对模型，仅支持路由配对模式，不支持路由转发模式（不支持OSPF或BGP等动态路由协议）。

云路由网络下IPsec隧道的典型场景：

- 在两套隔离的ZStack for Alibaba Cloud专有云环境中，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 *2-21: 云路由网络下IPsec隧道应用场景*所示：

图 2-21: 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 for Alibaba Cloud专有云环境中，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。

2.1.2.5 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 for Alibaba Cloud支持管纳VMware vCenter，可以通过VMware提供的公开API接口，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 for Alibaba Cloud支持的vCenter版本包括5.5、6.0和6.5。

基础资源

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

添加vCenter后，ZStack for Alibaba Cloud会自动同步vCenter的集群、物理机、虚拟机、模板、存储、网络等资源。也可通过点击**同步数据**按钮，将vCenter的资源实时同步至本地。相关资源均支持界面查看。

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

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

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

    说明：
    ZStack for Alibaba Cloud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 for Alibaba Cloud；也支持本地创建vCenter云主机。

网络

要在ZStack for Alibaba Cloud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。

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

vCenter网络服务目前支持云路由网络架构模型。

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

- DNS：
  - vCenter云路由器可作为DNS服务器提供DNS服务；

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

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

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。

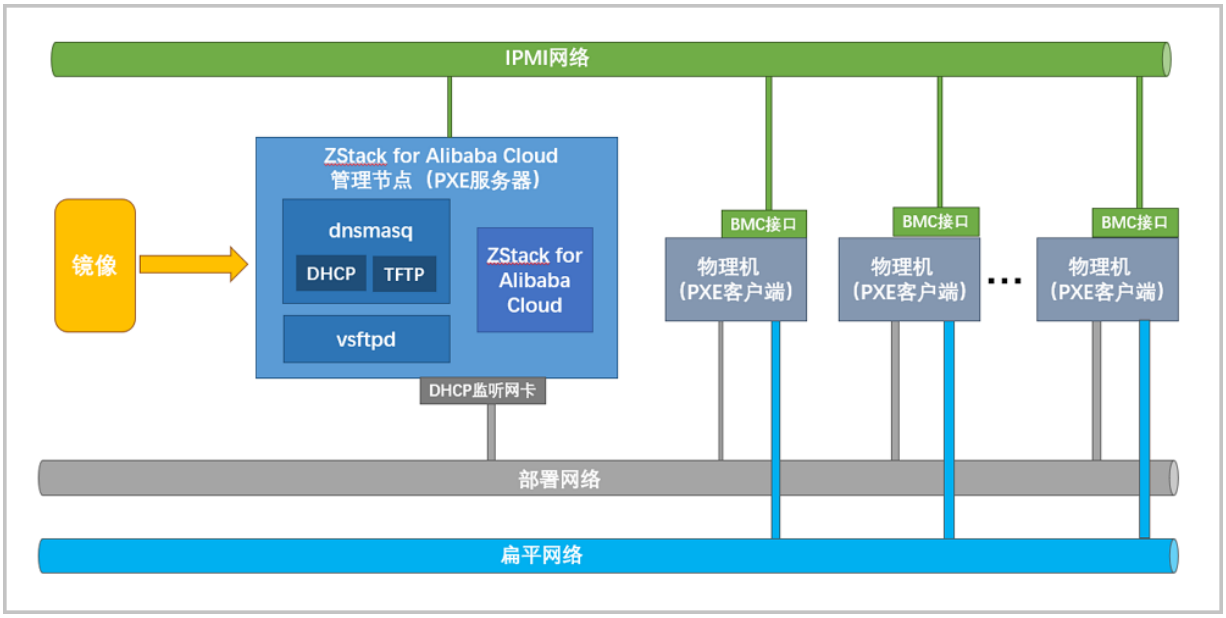
- 界面最多显示300条事件消息。支持设置时间段，可调整合适的时间段查看所设时间段内的报警消息。
- 支持调整每页显示的报警消息数量，可选值为：10、20、50、100；且支持翻页操作。

2.1.2.6 裸金属管理（Plus）

裸金属管理是一款为应用提供专属物理服务器的服务，能够保证核心应用的高性能和稳定性。支持自定义安装操作系统，并提供裸金属主机的全生命周期管理。

基本原理：管理节点通过部署服务器提供的PXE服务，指示多台物理机由IPMI网络启动，然后通过管理节点下载并安装相应的软件包为裸金属主机安装操作系统，并加载扁平网络与同一二层网络上的裸金属主机或云主机保持通信功能。基本原理图如图 2-22: 裸金属管理原理图所示：

图 2-22: 裸金属管理原理图



裸金属管理具有以下功能优势：

- 采用BMS部署，能够确保资源独享、数据隔离、可监管可追溯，确保资源安全可靠。
- 支持批量部署裸金属设备。当装机量较大且硬件支持IPMI时，admin可在ZStack for Alibaba Cloud UI界面上完成系统配置操作，并远程启动、部署众多物理机，无需进入机房。
- 支持自定义安装操作系统。用户可根据自己的需要，自定义为裸金属主机安装ISO类型的Linux操作系统。
- 为用户提供独享的高性能的物理服务器，支持添加扁平网络，能够与同一二层网络下的裸金属主机或云主机进行通信。

2.1.2.6.1 裸金属集群

裸金属集群：一组裸金属设备的逻辑集合。为裸金属设备提供单独的集群管理，支持加载二层网络，为集群中裸金属主机提供服务。

2.1.2.6.2 部署服务器

部署服务器：工作与管理节点，在开启PXE服务的网卡上配置DHCP服务和TFTP服务，用于远程引导安装裸金属主机系统。

2.1.2.6.3 裸金属设备

裸金属设备：未实例化的裸金属主机。在保证部署服务器存在且处于运行状态的前提下，可以进入**裸金属设备**界面，批量部署裸金属设备。

2.1.2.6.4 裸金属主机

裸金属主机：实例化的裸金属设备。可根据自己的需求，为裸金属设备安装ISO类型的Linux操作系统。支持加载网络，可与同一二层网络下的裸金属主机、云主机进行通信。

2.1.2.7 灾备服务（Plus）

灾备服务以业务为中心，融合定时增量备份等多种灾备技术到ZStack for Alibaba Cloud专有云平台中，支持本地灾备、异地灾备、公有云灾备多种灾备方案，用户可根据自身业务特点，灵活选择合适的灾备方式。灾备服务以单独的功能模块形式提供，需提前购买灾备服务模块许可证（Plus License），且需在购买云平台许可证（Base License）基础上使用，不可单独使用。

典型灾备场景

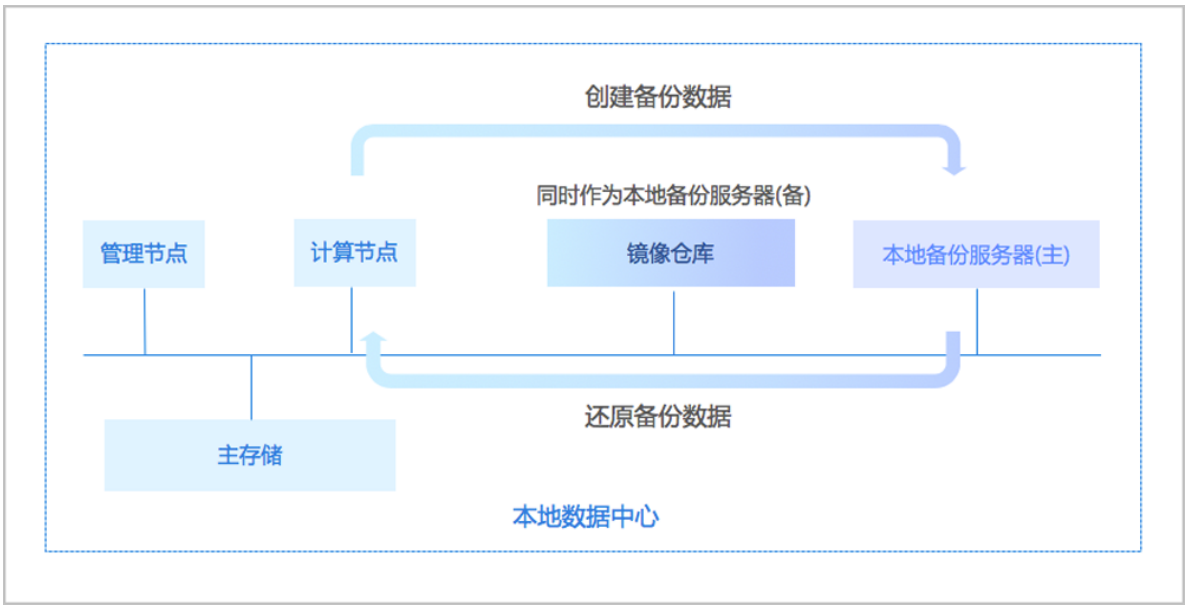
灾备服务模块提供本地灾备、异地灾备、公有云灾备三种典型灾备场景。

- **本地灾备**：

  支持将本地部署的镜像仓库作为**本地备份服务器**，用于存放本地云主机、云盘的定时备份数据。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。详情可参考本地灾备实践章节。

  本地灾备场景如图 *2-23: 本地灾备场景示意图*所示：

图 2-23: 本地灾备场景示意图

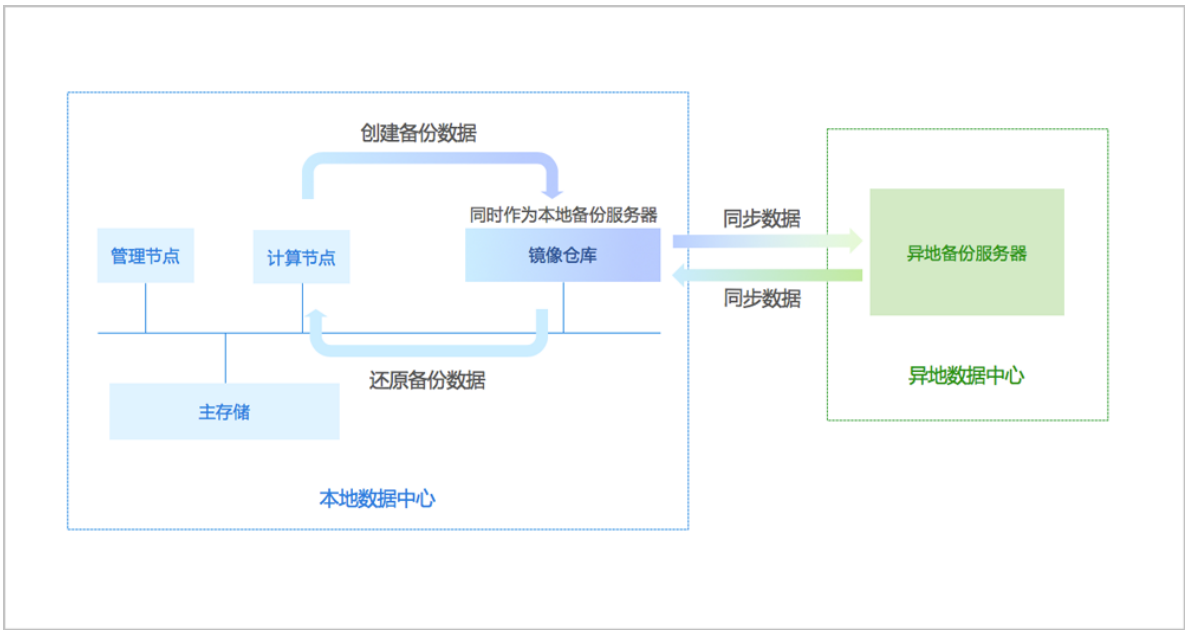


- **异地灾备**：

  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。详情可参考异地灾备实践章节。

  异地灾备场景如图 *2-24:* 异地灾备场景示意图所示：

图 2-24: 异地灾备场景示意图

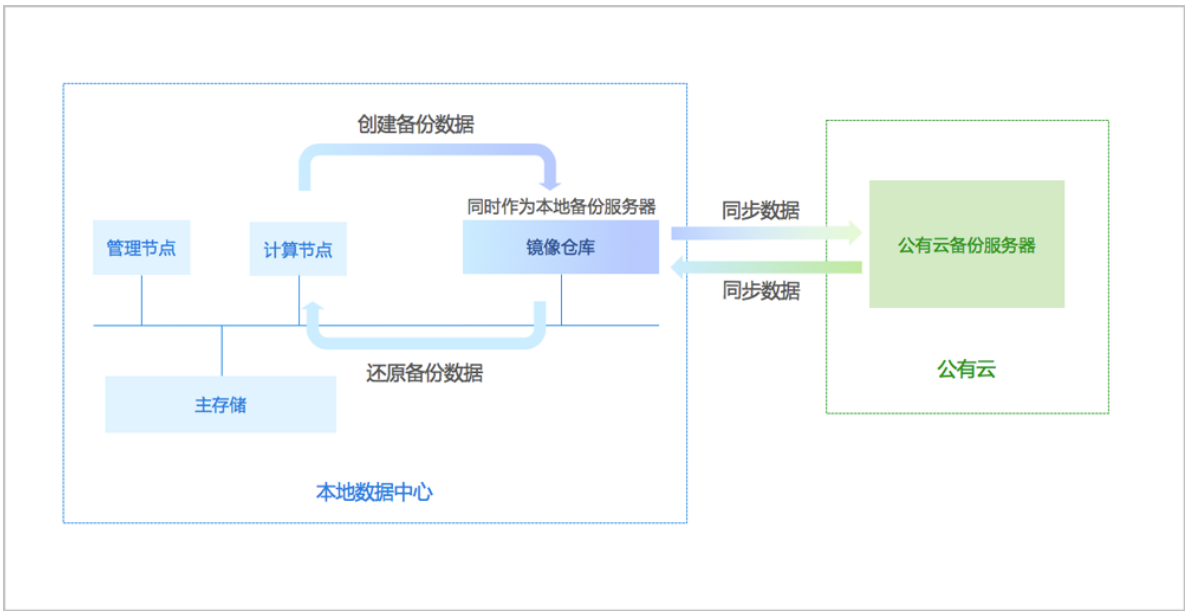


- **公有云灾备**：

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。详情可参考公有云灾备实践章节。

公有云灾备场景如图 *2-25:* 公有云灾备场景示意图所示：

图 2-25: 公有云灾备场景示意图



2.1.2.7.1 备份任务

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

2.1.2.7.2 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。

2.1.2.7.3 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，目前支持ImageStore类型；
- 允许添加多个本地备份服务器；
- 当备份任务指定多个本地备份服务器时，支持主备无缝切换；
- 支持定时增量备份；
- 备份到本地备份服务器上的备份数据可在详情页中查看。

2.1.2.7.4 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，目前支持ImageStore类型；
- 备份到远端备份服务器上的备份数据可在详情页中查看；
- 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。

2.1.2.8 企业管理（Plus）

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

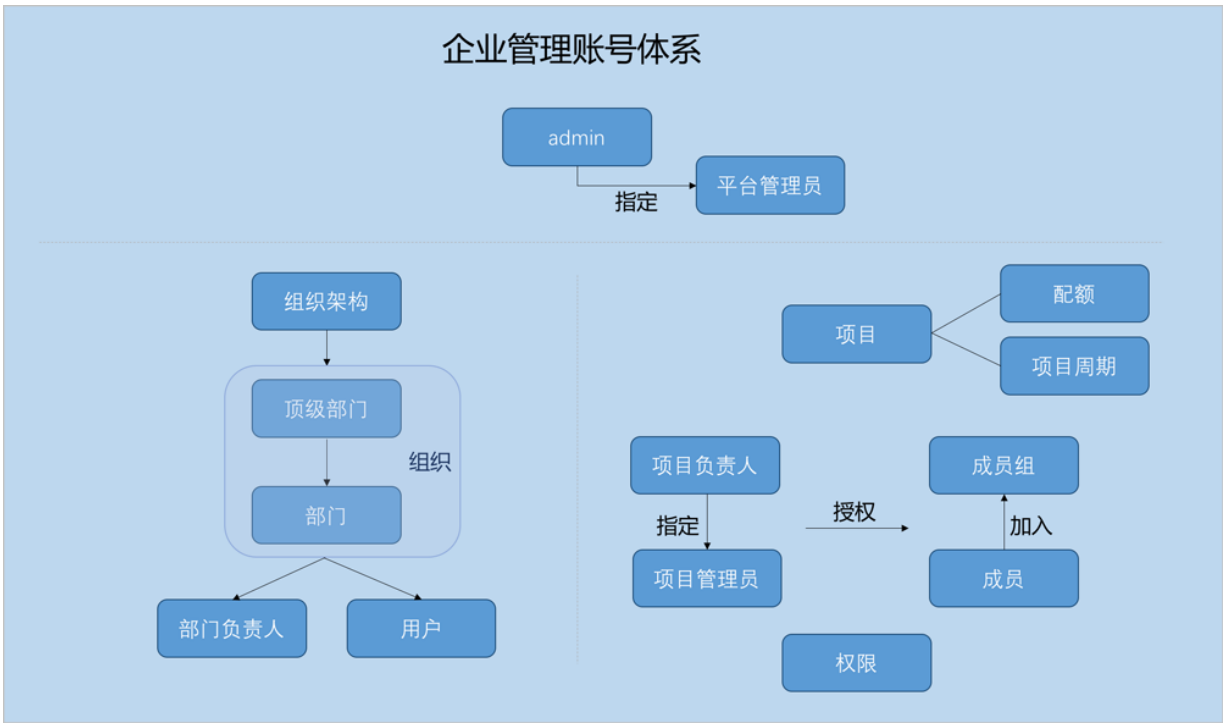
企业管理账号体系

企业管理账号体系主要涉及以下三类概念：

- 管理员账号：admin、平台管理员
- 未进入项目：用户、组织、部门负责人
- 已进入项目：项目负责人、项目管理员、成员、成员组、同时涉及项目、权限、配额等概念

企业管理账号体系如图 *2-26:* 企业管理账号体系所示：

图 2-26: 企业管理账号体系



相关定义：

- **admin**：

  admin不受权限控制，拥有超级权限，通常由IT系统管理员拥有。

- **平台管理员**：

  平台管理员主要是带有区域属性的管理员，admin可划分不同区域给不同平台管理员来管控不同区域的数据中心。

- **用户**：

  用户是企业管理中的最基本单位，admin/平台管理员可创建用户，并基于用户建立相应的组织架构。

- **组织**：

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

- **部门负责人**：

  创建组织，需指定相应的用户作为部门负责人。

- **项目**：

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

- **项目负责人**：

  创建项目，需指定组织内的用户作为项目负责人。

- **项目管理员**：

  项目负责人可指定一个或多个成员作为项目管理员。

- **成员**：

  成员作为项目的基本组成人员，一般由admin/平台管理员/项目负责人/项目管理员添加进入项目；项目成员的权限可由admin/平台管理员/项目负责人/项目管理员进行相应控制。

- **成员组**：

  项目负责人/项目管理员可在项目中创建成员组，对成员进行分组管理；可以成员组为单位进行权限控制。

- **权限**：

  项目负责人/项目管理员可对成员赋予权限，获得权限的成员可调用相关API进行资源操作。

- **配额**：

  配额是admin/平台管理员对项目的资源总量进行控制的衡量标准。

  - 主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。
  - admin/平台管理员可修改以上各参数对各个项目进行资源总额的控制。

- **项目周期**：

  创建项目需指定项目周期，包括无限制和定时回收两种。

  - 无限制：创建项目后，项目内资源默认一直处于启用状态。
  - 定时回收：
    - 项目有效期限不足7天时，项目负责人/项目管理员/项目成员登录云平台后智能操作助手将弹出**许可证即将过期**的提醒信息。
    - 项目过期后，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。

企业管理的三个子功能

企业管理主要包括**项目管理**、**工单管理**、**独立区域管理**三个子功能。

- **项目管理**：

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

  详情可参考项目管理详解章节。

- **工单管理**：

  为了更高效地为每个项目提供基础资源支持，项目成员可对云平台资源提出工单申请，管理员可进行一键审批，资源将自动部署成功并分发到项目中。

  详情可参考工单管理详解章节。

- **独立区域管理**：

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

  详情可参考独立区域管理详解章节。

2.1.2.8.1 平台管理员

平台管理员主要是带有区域属性的管理员，admin可划分不同区域给不同平台管理员来管控不同区域的数据中心。

- 新建的平台管理员，未划分区域前，默认可管控所有区域；
- 平台管理员划分区域后，只可管控指定区域；
- 一个平台管理员可管控多个区域，一个区域可由多个平台管理员共同管控；
- 除admin可对平台管理员进行管控外，平台管理员拥有和admin相同的全部权限；
- 平台管理员需从项目登录入口登录云平台。

2.1.2.8.2 组织架构

企业管理为企业用户提供组织架构管理功能。主要涉及以下概念：

- **用户**：

  用户是企业管理中的最基本单位，admin/平台管理员可创建用户，并基于用户建立相应的组织架构。

- **组织**：

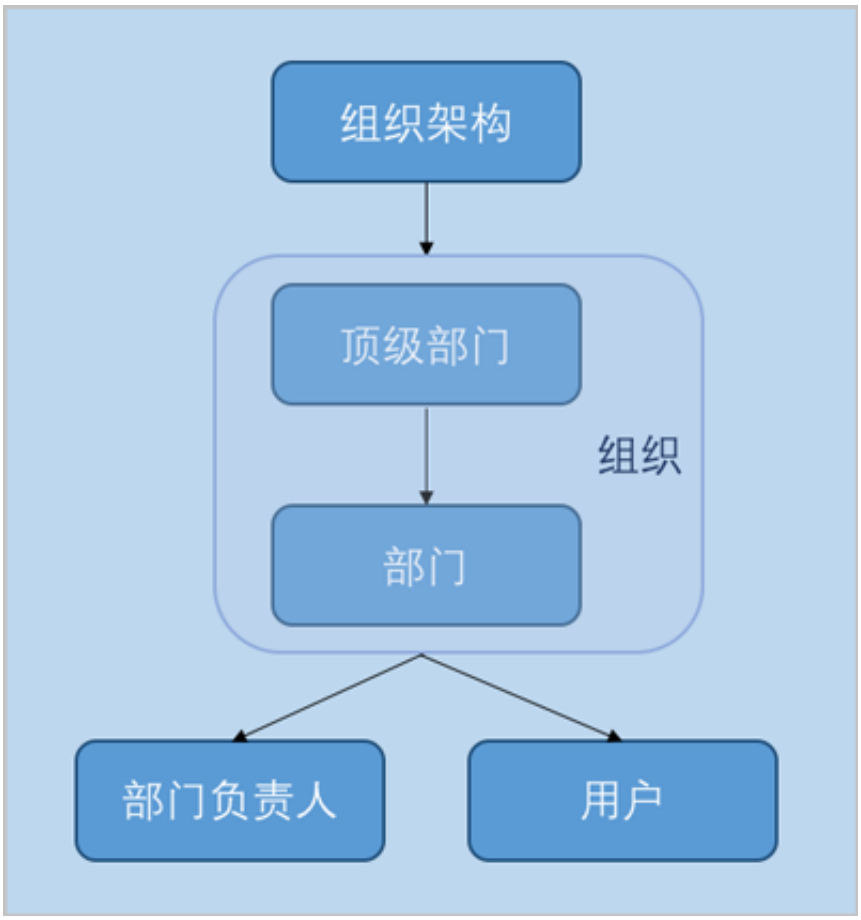
组织是企业管理中组织架构的基本单位，admin/平台管理员可基于用户建立相应的组织架构，组织可分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门。

- **部门负责人**：

  创建组织，需指定相应的用户作为部门负责人。

组织架构相关概念如图 2-27: 组织架构相关概念所示：

图 2-27: 组织架构相关概念



2.1.2.8.3 项目管理

企业管理为企业用户提供项目管理功能。

项目管理：

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

主要涉及以下概念：

- **项目**：

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

- **项目负责人**：

  创建项目，需指定组织内的用户作为项目负责人。

- **项目管理员**：

  项目负责人可指定一个或多个成员作为项目管理员。

- **成员**：

  成员作为项目的基本组成人员，一般由admin/平台管理员/项目负责人/项目管理员添加进入项目；项目成员的权限可由admin/平台管理员/项目负责人/项目管理员进行相应控制。

- **成员组**：

  项目负责人/项目管理员可在项目中创建成员组，对成员进行分组管理；可以成员组为单位进行权限控制。

- **权限**：

  项目负责人/项目管理员可对成员赋予权限，获得权限的成员可调用相关API进行资源操作。

- **配额**：

  配额是admin/平台管理员对项目的资源总量进行控制的衡量标准。

  - 主要包括云主机数量、CPU数量、内存容量、最大数据云盘数目和所有云盘最大容量等。
  - admin/平台管理员可修改以上各参数对各个项目进行资源总额的控制。

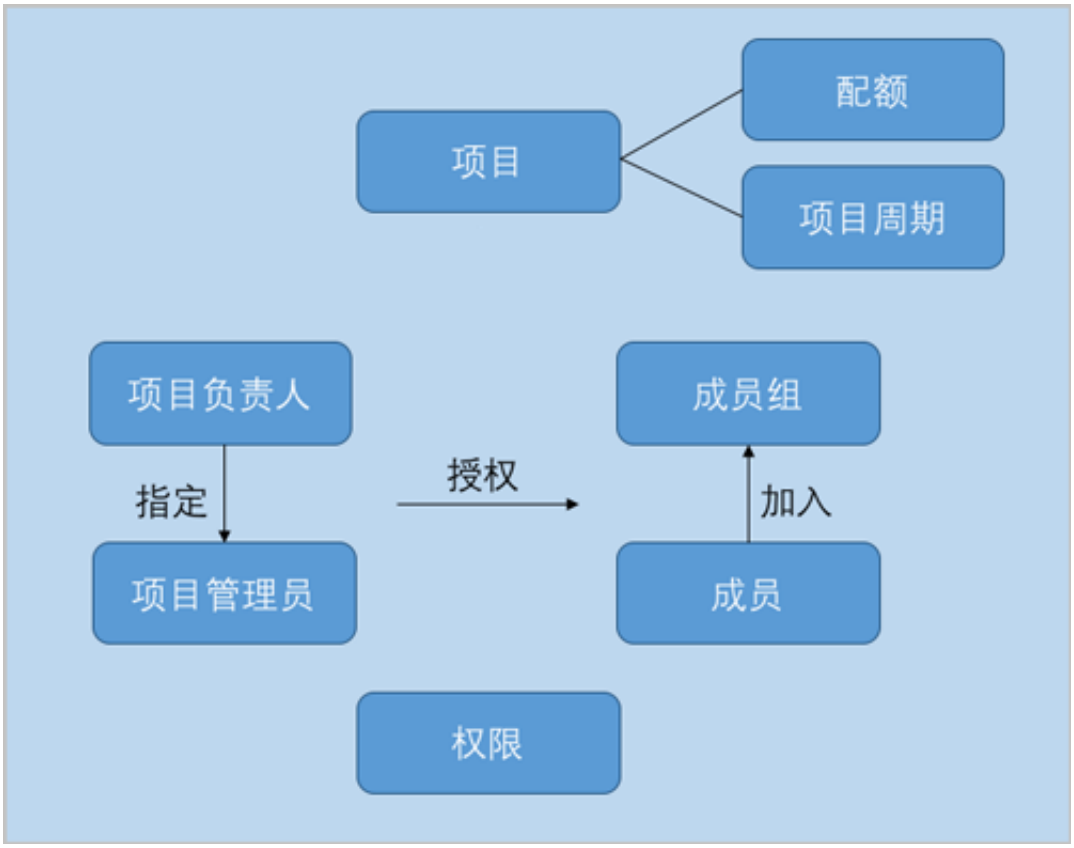
- **项目周期**：

  创建项目需指定项目周期，包括无限制和定时回收两种。

  - 无限制：创建项目后，项目内资源默认一直处于启用状态。
  - 定时回收：
    - 项目有效期限不足7天时，项目负责人/项目管理员/项目成员登录云平台后智能操作助手将弹出**许可证即将过期**的提醒信息。
    - 项目过期后，项目内资源按照指定的控制策略回收，回收策略有以下三种：禁止登录、停止资源、删除项目。

项目管理相关概念如图 *2-28:* 项目管理相关概念所示：

图 2-28: 项目管理相关概念

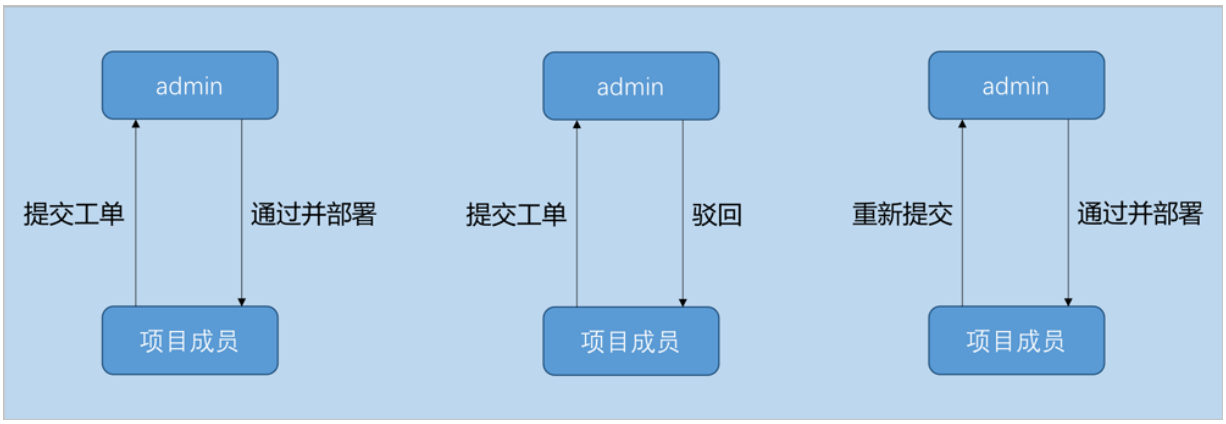


2.1.2.8.4 工单管理

为了更高效地为每个项目提供基础资源支持，项目成员可对云平台资源提出工单申请，管理员可进行一键审批，资源将自动部署成功并分发到项目中。

工单管理主要工作流如图 *2-29:* 工单管理主要工作流所示：

图 2-29: 工单管理主要工作流



2.1.2.9 平台运维

2.1.2.9.1 性能TOP5

性能TOP5是面向运维人员推出的可视化性能监控页面，在该页面可直观便捷查看物理机、云主机、路由器、虚拟IP、三层网络资源各种监控指标的TOP5信息，从而方便运维人员直观掌控云平台实时健康状态，以及快速定位问题。

- 物理主机页面：

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

- 云主机页面：

  同物理机页面类似，通过对当前区域全部云主机的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读写IOPS、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

- 路由器页面：

  同云主机页面类似，通过对当前区域全部路由器（包括云路由器和VPC路由器）的CPU、内存、磁盘、网络资源使用情况进行统计分析，以CPU平均使用率、内存使用率、内存空闲百分比、磁盘读写IOPS、磁盘读写速度、网卡出入速度、网卡出入包速率、网卡出入错误速率为指

标，分别挑选出各指标下的TOP5，进行实时展示监控。实时显示的百分比排行以及进度条的颜色区分提示，可直观告知运维人员当前哪些资源告急或出现性能瓶颈。

- 虚拟IP页面：

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

- 三层网络页面：

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

2.1.2.9.2 性能分析

性能分析直观的显示了云主机、路由器、物理主机、三层网络、虚拟IP、镜像服务器资源使用情况。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

2.1.2.9.3 ZWatch

- 针对各种资源类型提供了多样化报警条目，支持的接收端类型有邮件/钉钉/HTTP应用。
- 设计原理：报警器或事件向SNS通知系统的主题发送消息，消息会自动推送到订阅该主题的接收端。发送到接收端的消息会以邮件/钉钉/HTTP POST方式发送到指定地址。
- 由于ZWatch监控系统与SNS通知系统完全松耦合，且基于开放式设计，用户可自定义报警器或事件，按需扩展更多资源类型以及更多报警条目，实现全方位、细粒度、灵活监控所有系统信息。

报警器

ZWatch监控系统支持对时序性数据和事件设置报警器，并通过SNS通知系统接收报警信息。

- 资源报警器，主要针对系统时序数据进行监控，例如云主机内存使用率、物理机CPU使用率等。支持用户自定义资源报警器。
- 事件报警器，主要针对系统事件进行监控，例如云主机状态变化事件、物理机失联事件等。支持用户自定义事件报警器。

报警消息模板

报警消息模板：报警器或事件向SNS系统的主题发送消息时使用的文本模板。

- 目前报警消息模板支持邮箱和钉钉两种接收端平台。使用报警消息模板，可将通知邮件或钉钉消息以统一格式发出。
- 系统自带一个默认模板，若用户没有创建模板，系统将使用自带模板。
- 用户可以创建多个模板，但只能指定一个为默认模板，发送消息时只会使用默认模板格式化信息。
- 模板中可以通过${}引用报警器或事件提供的变量。

2.1.2.9.4 通知服务

用户可以用不同的接收端订阅主题，接收端类型包括：邮箱、钉钉、HTTP应用。

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。

2.1.2.9.5 消息中心

目前消息中心仅提供报警消息的查看。可查看该报警的消息内容、消息时间等信息。

- 支持设置时间段，可查看所设时间段内的报警消息，包括查看消息描述、消息时间、以及消息详情。
- 支持调整每页显示的报警消息数量，可选值为：10、20、50、100；且支持翻页操作。

2.1.2.9.6 操作日志

操作日志界面包括三个子页面：已完成、进行中、审计。

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

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

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

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

2.1.2.9.7 资源编排

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

如图 *2-30:* 资源编排所示：

图 2-30: 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。

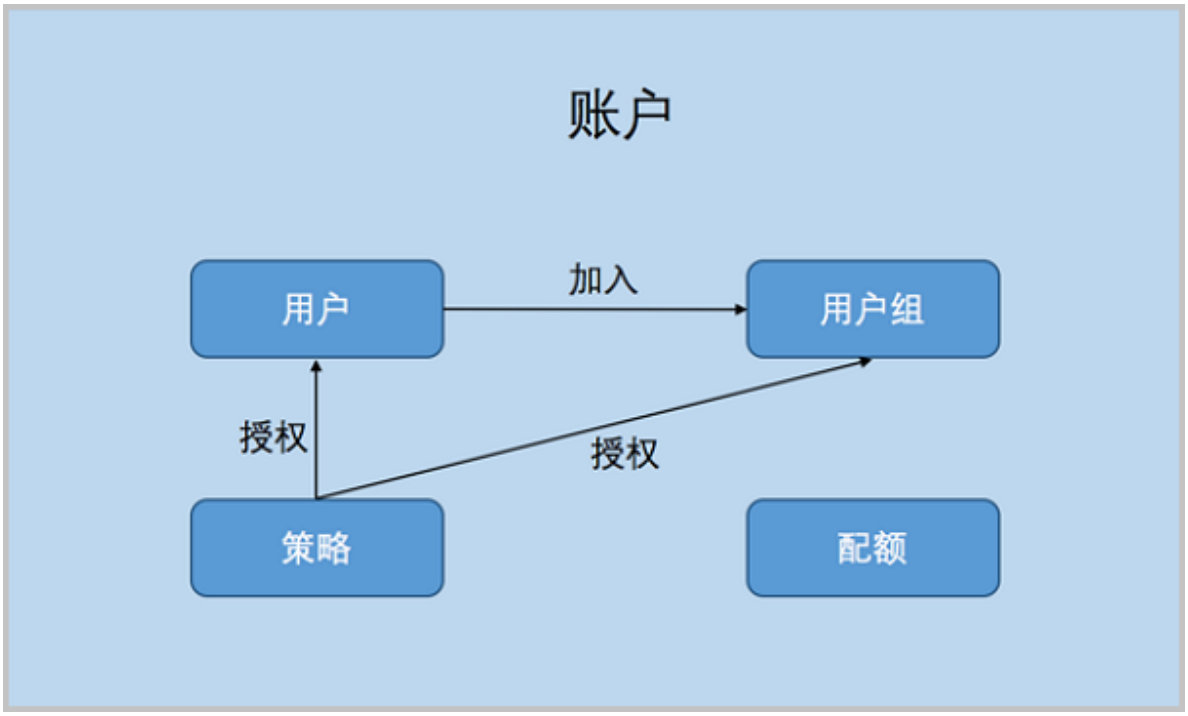
2.1.2.10 平台管理

2.1.2.10.1 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 *2-31: 用户管理系统*所示：

图 2-31: 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。

2.1.2.10.2 计费管理

2.1.2.10.2.1 账单

账单：按计费单价和使用时间来统计并显示所有项目或账户下各资源的资费信息。

2.1.2.10.2.2 计费设置

计费设置：计费信息的显示需提前对各资源创建计费单价。计费设置支持对处理器、内存、根云盘、数据云盘等基本计费资源进行计费单价设置。以各资源的规格大小和时间作为基本计费单位，并以时长作为服务使用记录，从而对不同账户使用的业务量进行统计计费。

2.1.2.10.3 定时

2.1.2.10.3.1 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

> **说明**：
> 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**。

2.1.2.10.3.2 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。

2.1.2.10.4 应用中心

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

2.1.2.10.5 邮箱服务器

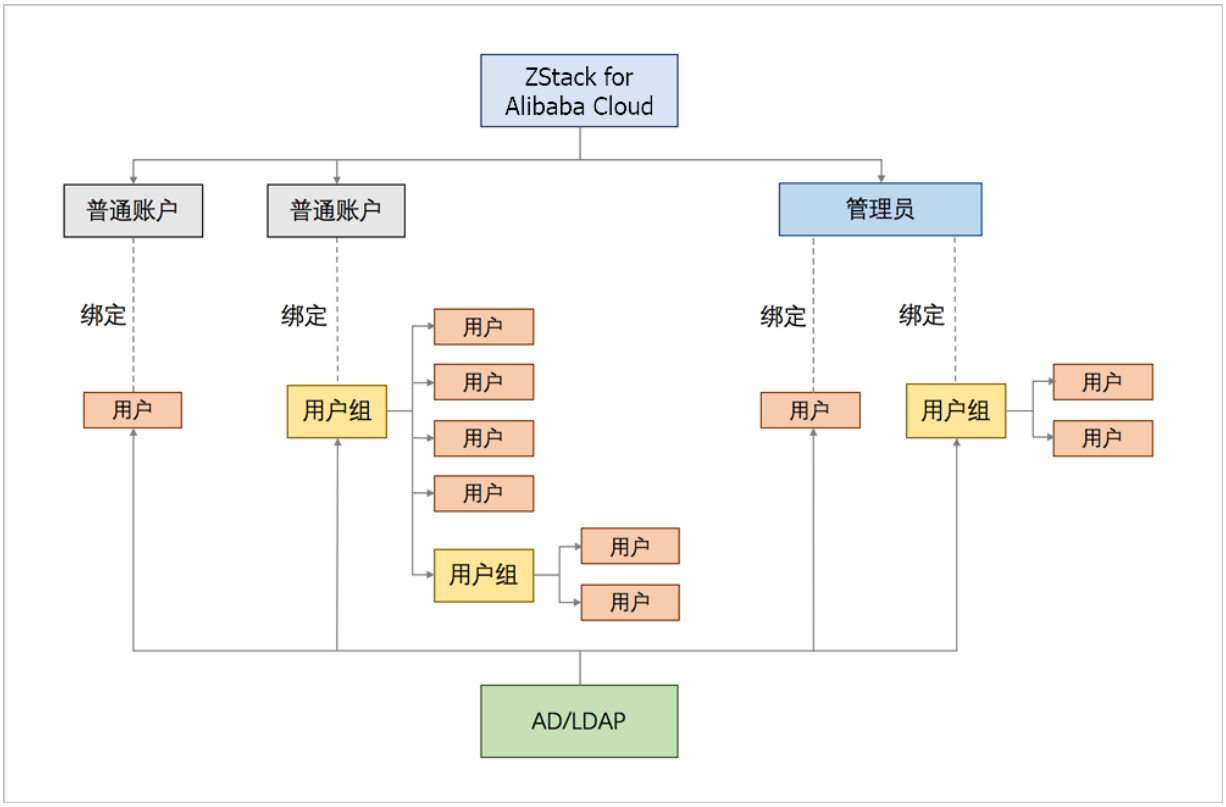
ZStack for Alibaba Cloud支持ZWatch监控报警功能，若接收端选择邮件类型，需设置邮件服务器，用来接收报警邮件。

2.1.2.10.6 AD/LDAP

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

ZStack for Alibaba Cloud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 2-32: ZStack for Alibaba Cloud-AD/LDAP绑定关系*所示：

图 2-32: ZStack for Alibaba Cloud-AD/LDAP绑定关系



2.1.2.10.7 控制台服务

- 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。

2.1.2.10.8 证书

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

2.2 混合云

基于ZStack云引擎深度定制的ZStack for Alibaba Cloud，提供了一套无缝集成的混合云管理方案。

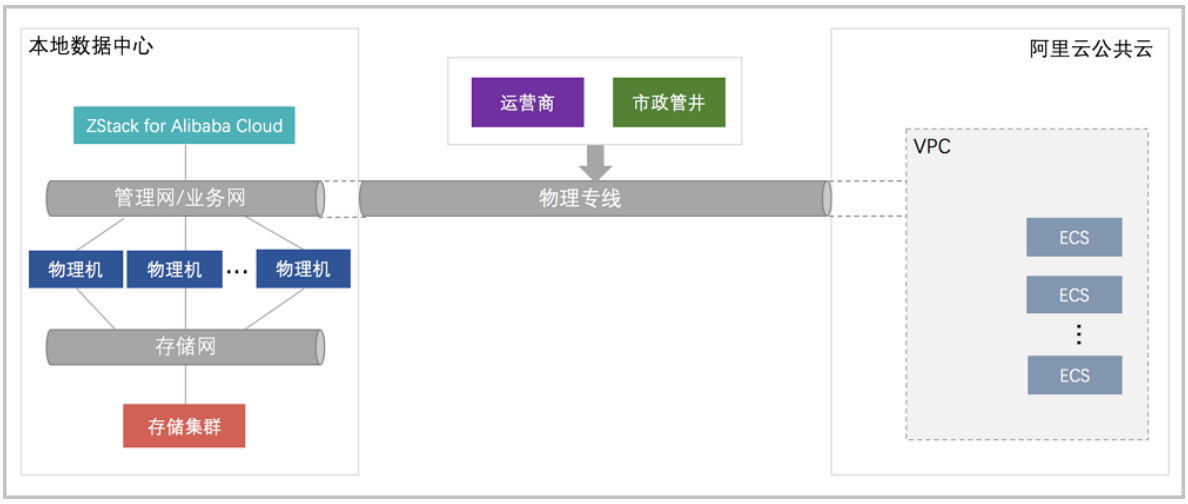
物理部署

由于ZStack采用进程内微服务架构，因此ZStack for Alibaba Cloud混合云平台的部署与ZStack完全一样，并不引入新的模块。但ZStack for Alibaba Cloud管理节点要求能够访问公网，以便调用阿里云公共云的OpenAPI。

1. 基于物理专线部署

   如图 *2-33: 基于物理专线部署*所示，通过物理专线构建**本地—远程**互联网络，从而连通本地数据中心和阿里云公共云。

   图 2-33: 基于物理专线部署



2. 基于SD-WAN部署

   如图 *2-34: 基于SD-WAN部署*所示，通过无缝对接大河云联的SD-WAN服务，提供灵活按需的混合云高速链路，从而连通本地数据中心和阿里云公共云。

图 2-34: 基于SD-WAN部署

混合云功能模块

ZStack for Alibaba Cloud混合云功能模块主要有：身份认证、互联网络、资源管理和业务实现。

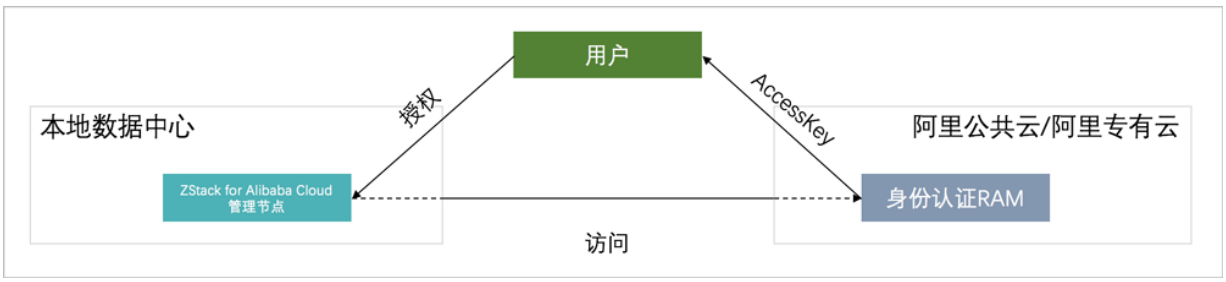
2.2.1 身份认证

阿里云AK

实现了阿里云公共云的账户身份认证RAM对接，采用授权子账户AK（AccessKey以及KeySecret）信息远程访问。

- 企业资产管理员（拥有全局的权限管理），可创建面向混合云平台的子账户，例如hybrid_cloud，并授予一定的资源访问权限，包括ECS、VPC、虚拟交换机和OSS等。
- 企业资产管理员将该子账户的AK信息提供给信息技术部门，则可导入ZStack for Alibaba Cloud混合云平台，授予管理阿里云公共云的资源权限。
- 若企业资产管理员需终止或回收该子账户，可登录到阿里云RAM身份认证系统，执行禁用或删除操作而无需协调信息技术部门。

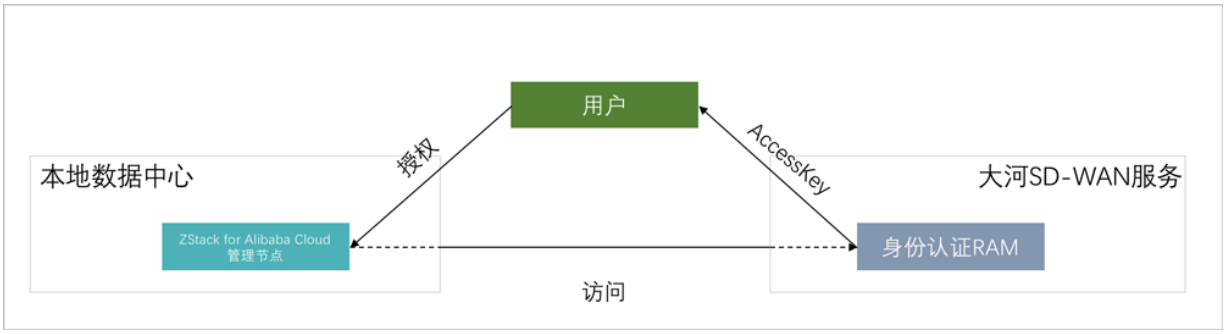
图 2-35: 身份认证



大河AK

实现了大河云联的DAHO Fabric自服务平台的账户身份认证对接，采用授权账户AK（AccessKey以及KeySecret）信息远程访问，如图 *2-36: 身份认证*所示：

图 2-36: 身份认证



2.2.2 互联网络

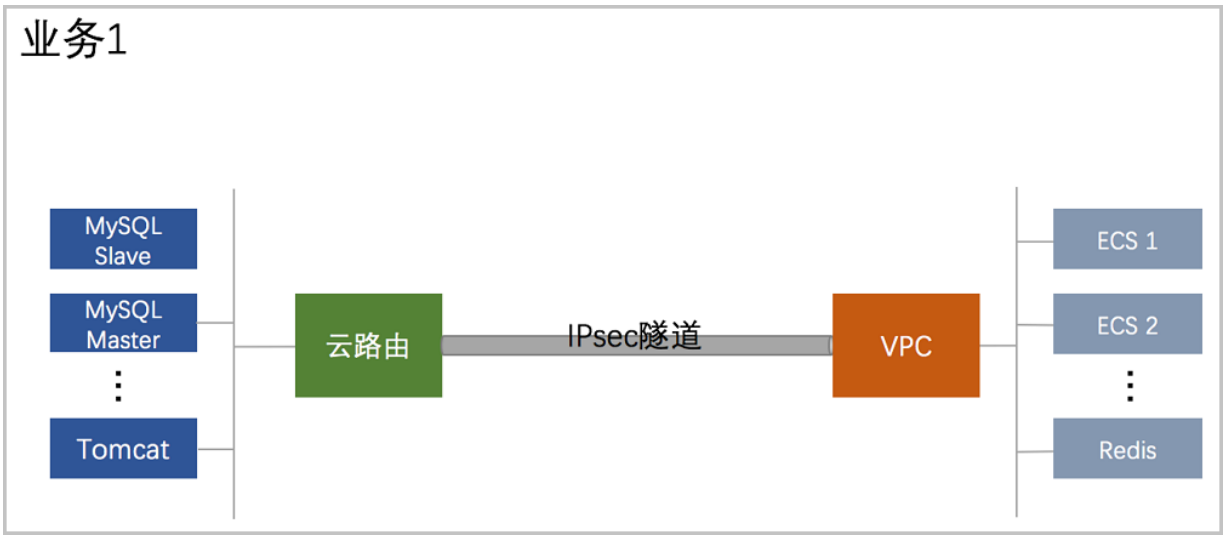
实现IPsec隧道和高速通道（Express Connect）连接本地专有云和阿里云公共云，使得"本地—远程"在三层网络可达下互访。"本地—远程"的互联网络，是混合云核心基础设施。

ZStack for Alibaba Cloud混合云平台支持IPsec隧道和高速通道构建互联网络。

IPsec隧道：

IPsec隧道实现了本地端的云路由与远程端的阿里云公共云的VPC模块互联，并以数据加密的方式传送数据。由于互联网网络延迟较大、带宽成本递增，一般情况下常用于演示测试与数据备份场景。如*IPsec隧道*所示：

图 2-37: IPsec隧道



高速通道：

高速通道则是一款便捷高效的网络服务，能提供"本地—远程"网络环境间的高速、稳定、安全的私网通信，有效提高网络拓扑的灵活性和跨网络通信的质量和安全性。混合云平台能基于高速通道实现快速的数据传输，保障所承载的业务架构稳定运行。如阿里云高速通道和大河高速通道所示：

图 2-38: 阿里云高速通道

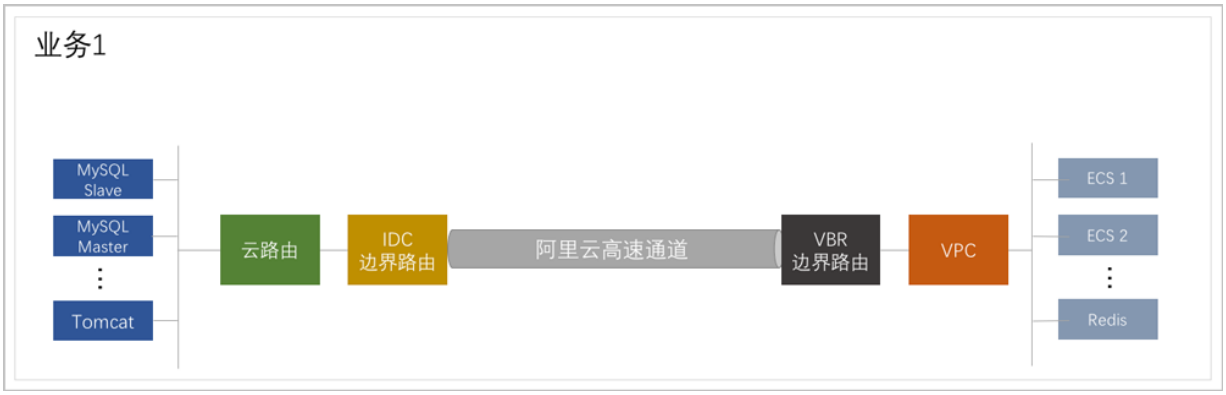
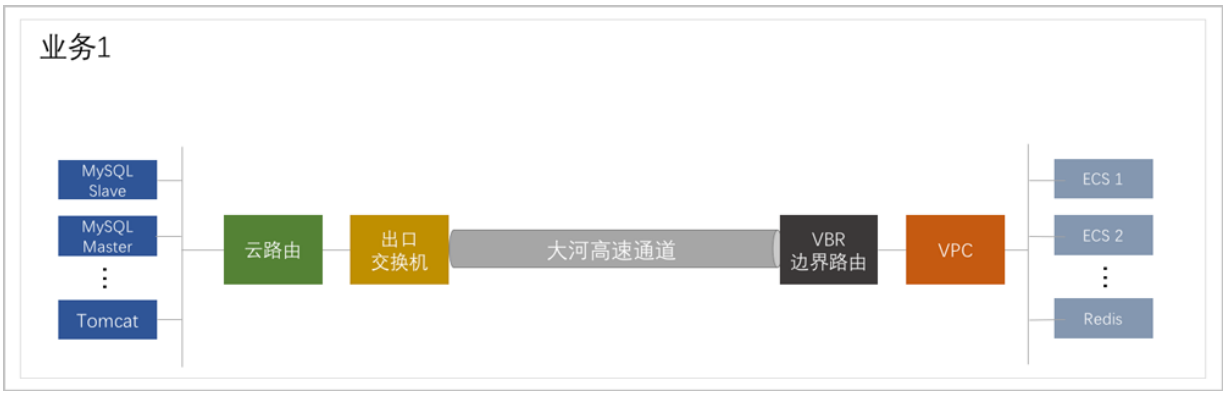


图 2-39: 大河高速通道

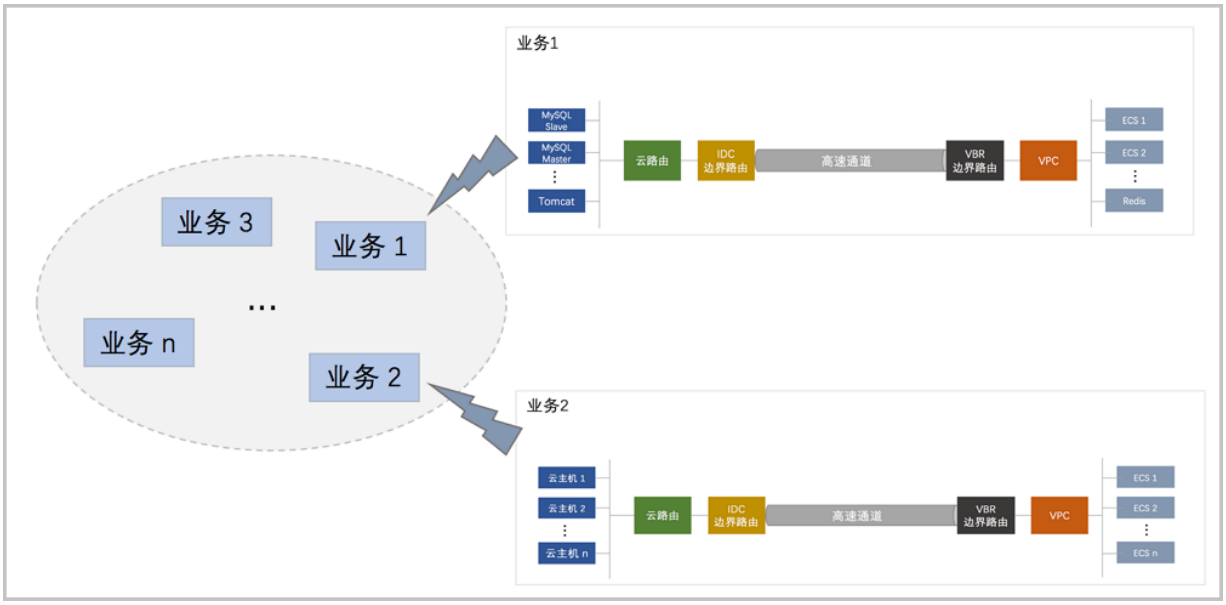


2.2.3 资源管理

通过授权子账户，访问阿里云公共云账户里的资源，包括管理ECS、OSS、VBR、VPC和虚拟交换机等服务。

- 基于上述的身份认证模块，管理员无需再登录访问阿里云公共云门户控制台，直接通过ZStack for Alibaba Cloud混合云平台本地登录后，就可以访问并管理公共云端的资源。目前，混合云平台支持管理的阿里云公共云资源包括：ECS、OSS、VBR、VPC和虚拟交换机等服务。
- ZStack for Alibaba Cloud混合云平台提供直观简捷的图形界面（UI）和全功能开放接口（API），以便信息系统管理员可见即可得操作，以及基于统一API实现上层的业务调度逻辑。

图 2-40: 资源管理



2.2.4 业务实现

基于上述的网络基础设施和管理控制方式，实现灵活弹性的业务系统架构。

混合云平台建成后，可在其上部署灵活多维的业务模式，场景列举如下：

- **应用与数据分离**：

  数据库和分析服务保留在专有云，缓存服务和Web应用部署在公共云（在混合云管理面板直接部署），从而既满足数据库关键数据自有，也满足业务灵活扩展和互联网访问的安全性。

- **数据归档备份**：

  企业可以选择对长久归档的数据（切片和加密）传送到阿里云对象存储（OSS），实现低成本的数据灾备方案，满足成本和随时访问恢复的需求。

- **弹性业务架构**：

  企业可以将持续稳定的业务负载量部署在专有云环境，将业务瞬时或周期高峰负载分摊到公共云，利用公共云的海量计算资源（相对专有云）满足资源申请与及时释放。

3 产品功能

ZStack for Alibaba Cloud不仅涵盖了ZStack全部专有云功能，还具备一系列混合云特色功能。

3.1 专有云功能

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

ZStack企业版功能列表：

类别	特性	ZStack企业版
区域	管理多个区域	用户可以根据实际情况创建并管理多个区域，一般情况下可将一个物理数据中心归为一个Zone来管理；用户根据不同的业务需求，每个Zone内建立自己独立的集群、主存储、网络等资源
vCenter	管理vCenter	• 支持对现有数据中心中的VMware虚拟化环境进行管理，VMware vCenter Server所管理的vSphere服务器资源和虚拟机资源，能够在虚拟数据中心中使用VMware vSphere资源，并在VMware vCenter集群中完成对云主机的常用操作 • 支持按vCenter区分查看云主机、云盘、镜像等资源
		支持以vCenter为单元对其下资源进行数据同步，保证信息一致
	vCenter多租户管理	• 普通账户/项目负责人/项目管理员/项目成员可对vCenter云主机或云盘进行相关操作 • 普通账户/项目负责人/项目管理员/项目成员可使用admin共享的vCenter网络或镜像 • 支持在普通账户/项目负责人/项目管理员/项目成员视角的首页分别展示KVM和vCenter云主机的使用量 • 工单审批支持申请vCenter云主机
	ESX云主机	支持云主机的创建、启动、停止、迁移、克隆、重启、暂停、恢复、关闭电源、修改计算规格、设置高可用、打开控制台、设置控制台密码、删除等全生命周期管理及常用功能
	网络	支持创建云路由网络和扁平网络，云路由网络支持所有ZStack网络服务
		支持vSwitch/dvSwitch

类别	特性	ZStack企业版
	存储	支持按datastore区分主存储和镜像服务器
	镜像	支持添加、启用、停用、删除镜像
	物理机	支持维护模式
	云盘	支持云盘的创建、删除、加载、卸载
	实时性能监控	采集ESX云主机的CPU、内存、存储和网络运行数据，提供图形可视化
集群	存储架构	集群内使用同构存储服务，存储服务挂载到集群，提供云主机高可用
	物理机	集群内管理物理机，支持实时查看物理机全部CPU使用率、物理机全部内存使用百分比、物理机全部网卡出入速度和物理机全部磁盘读/写IOPS
	云主机	集群内管理云主机，支持实时查看云主机全部CPU使用率、云主机全部内存已用百分比、云主机全部网卡出入速度和云主机全部磁盘读/写IOPS
	集群功能	提供高可用特性，支持按照物理机CPU架构定义集群属性
	网络服务	支持VLAN、VXLAN网络加载到集群并统一管理、提供网络自助服务（IP池管理和弹性网络）、支持集群指定迁移网络、支持定义集群的CPU模式
物理机	虚拟化	支持KVM虚拟化技术，支持VMware虚拟化
	c74 ISO	• 支持使用最新英特尔® 至强® 可扩展处理器，例如支持部署在DELL EMC R740 14代服务器上，提升平台稳定性 • 支持灾备模块，进一步提升平台稳定性 • 初装用户推荐安装c74 ISO
	资源设定超分	支持CPU、内存和存储空间设定超分比例，适应云环境资源使用
	嵌套虚拟化	支持KVM/ESXi嵌套虚拟化，云主机内部开启CPU硬件虚拟化功能
	实时监控	采集物理机的CPU、内存、存储和网络运行数据，提供图形可视化
	停用与启用	对物理机设定可用属性，以便停止在该物理机上创建云主机
	维护模式	对物理机设定维护状态，设定维护模式后，物理机上的云主机将会迁移（共享存储）

类别	特性	ZStack企业版
	GPU透传	支持物理机GPU设备透传，让云主机拥有高性能计算和图形处理能力
	USB透传	支持USB透传，满足多种USB应用场景
	操作日志	展示物理机执行任务的事件审计
	导出CSV文件	支持物理机列表导出为CSV表格，方便统计分析处理
云主机	批量操作	批量管理云主机
	创建云主机	提供多种策略创建云主机，高效利用资源
	云主机生命周期	支持创建、停止、启动、重启、关闭电源、删除、暂停、恢复等基本生命周期控制
	根云盘在线扩容	支持云主机根云盘在线扩大容量，方便修改云主机配置
	数据云盘在线扩容	支持云主机数据云盘在线扩大容量，即时生效
	云主机控制台	用户可通过终端方式访问云主机，而不依赖云主机远程工具，支持控制台设置密码
	云主机快照	• 在云主机运行过程中进行快照 • 在线快照（支持ImageStore/Ceph/FusionStor类型的镜像服务器） • 关机快照（支持ImageStore/Sftp/Ceph/FusionStor类型的镜像服务器）
	云盘在线快照	在使用云盘的过程中进行快照
	云主机在线修改密码	支持Windows/Linux的云主机在线修改密码
	云主机在线创建镜像	运行中的云主机在线创建镜像
	云主机QGA开关	灵活控制qemu guest agent的状态
	云主机RDP模式开关	针对VDI用户界面，启用后默认以RDP模式打开控制台
	云主机显卡切换	支持选择云主机显卡类型：qxl、cirrus、vga
	云主机显卡透传	支持英伟达和AMD GPU设备透传给云主机
	User Data导入	支持创建云主机时导入User Data
	云主机克隆（不带数据云盘）	• 基于云主机快速克隆若干个云主机 • 在线克隆（支持ImageStore/Ceph类型的镜像服务器） • 关机克隆（支持ImageStore/Ceph类型的镜像服务器）

类别	特性	ZStack企业版
	整机克隆（带数据云盘）	• 同时克隆云主机的根云盘和数据云盘内容 • 仅支持ImageStore类型的镜像服务器 • LocalStorage/NFS/SMP类型的主存储，支持在线/暂停/关机克隆 • Ceph类型的主存储，支持在线/暂停/关机克隆 • Shared Block类型的主存储，支持暂停/关机克隆 • 挂载共享云盘的云主机不支持整机克隆
	更换系统盘	支持云主机关机状态下修改操作系统
	重置云主机	支持恢复云主机状态为模板初始状态
	根云盘扩容	支持在线/关机状态下的云主机根云盘扩容，方便修改云主机配置
	基于ISO部署	• 基于ISO系统光盘部署云主机，引导安装系统 • 允许一个云主机加载多个ISO，提升业务部署效率
	基于模板部署	基于系统模板创建云主机
	制作镜像模板	基于当前某个云主机制作模板
	创建镜像	• 云主机运行中在线创建镜像 • 在线创建镜像（支持ImageStore/Ceph类型的镜像服务器） • 关机创建镜像（支持ImageStore/Sftp/Ceph/FusionStor类型的镜像服务器）
	自定义MAC地址	• 支持创建云主机时指定MAC地址 • 支持云主机修改MAC地址
	云主机启动顺序	调整云主机的启动顺序，用于切换ISO引导
	动态加载、卸载云盘	云主机可动态加载和卸载云盘，支持优化驱动模型，支持SCSI WWN号唯一识别
	动态加载、卸载网卡	云主机可动态加载和卸载网卡，支持设置默认网卡
	加载GPU卡	支持创建云主机时加载GPU设备
	共享云盘	支持Ceph存储或Shared Block主存储下多云主机共享使用同一数据云盘
	实时性能监控	采集云主机的CPU、内存、存储和网络运行数据，提供图形可视化

类别	特性	ZStack企业版
	高可用特性	物理机故障，云主机自动重启
	在线修改云主机CPU/内存	支持在线修改云主机配置，不用重启VM
	实时更新云盘和网络QoS	提供云盘和网络的限速能力，避免单个云主机占用过量资源
	SSH密钥注入	支持Linux和BSD操作系统SSH密钥注入，支持创建和删除秘钥
	自定义计算规格	支持自定义计算规格，满足各种应用资源消耗特性
	自定义标签	支持自定义标签，满足查询和编写定时任务
	资源删除保护	云资源删除后，将移入回收站，提供恢复和确认销毁
	冷迁移	支持本地主存储类型上的云主机进行关机状态迁移
	在线迁移	支持所有主存储类型上的云主机进行在线迁移
	存储迁移	• 多NFS主存储之间的云主机支持跨存储设备冷迁移 • 多Ceph主存储之间的云主机支持跨存储设备冷迁移 • 多Shared Block主存储之间的云主机支持跨存储设备冷迁移，且支持同时迁移加载的云盘
	操作日志	展示云主机操作过程的事件审计
	Windows系统性能优化	提供Windows云主机性能优化加速
	USB重定向	支持将VDI客户端USB设备重定向至云主机
	导出CSV文件	支持云主机列表导出为CSV表格，方便统计分析处理
云盘	云盘管理	支持云盘的创建、启用、停用、加载、卸载、迁移、创建快照、创建镜像、扩容、更改所有者、存储迁移、删除
云盘规格	云盘规格管理	支持云盘规格的创建、启用、停用、全局共享、全局召回、云盘规格QoS、删除
计算规格	计算规格管理	• 支持计算规格的创建、启用、停用、磁盘QoS、网络QoS、全局共享、全局召回、删除 • 支持选择物理机分配策略 • 当物理机分配策略为CPU使用率最低/内存使用率最低，支持选择强制、非强制策略模式
镜像管理	系统模板	支持系统模板，支持QCOW2和RAW格式，自动匹配镜像类型

类别	特性	ZStack企业版
	ISO镜像	支持ISO镜像，支持从ISO镜像引导云主机
	系统镜像上传	支持URL上传和本地浏览器上传
	云盘镜像上传	支持URL上传和本地浏览器上传
	镜像迁移	支持Ceph主存储上的镜像跨存储设备迁移、支持NFS主存储上的镜像跨存储设备迁移
镜像仓库	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
	镜像同步	支持镜像仓库间的镜像互传，可以跨区域使用
	标准系统镜像	支持标准的系统，支持Windows、红帽、Ubuntu和其他开源Linux系统
	预设运行镜像	支持众多的软件运行环境，支持Windows IIS和Dot Net Framework运行环境，支持Linux Tomcat、JAVA、Apache Web、Jboss、PHP、Node JS、Golang、Python等语言和运行环境，支持数据库Oracle、MySQL、Postgres、Mongodb、Influxdb、Cassandra和Redis等数据库服务；支持广泛的应用中间件
	预设应用镜像	支持众多的应用系统，论坛BBS、社交SNS、博客Blog、微博的常用应用系统；支持phpmyadmin等运维管理应用；支持厂商提供的应用镜像
	自定义镜像	支持管理员根据标准系统镜像和预设运行镜像，定义满足自身业务系统运行环境的镜像，以增量方式保存镜像内容，并实现智能去重功能
	存储支持	与本地存储、NFS、SMP、Ceph、Shared Block、阿里云NAS类型的主存储无缝支持
存储管理	本地存储	• 支持云盘存放到物理机本地 • 支持实时查看主存储已用容量百分比趋势图
	NFS存储	• 支持云盘存放到NFS协议存储，物理机共享访问 • 共享文件系统管理节点高可用方案 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持实时查看主存储已用容量百分比趋势图

类别	特性	ZStack企业版
	共享挂载存储	• 支持云盘存放到POSIX兼容的共享存储，支持iSCSI/FC存储 • 共享文件系统管理节点高可用方案 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持实时查看主存储已用容量百分比趋势图
	Shared Block存储	• 支持添加iSCSI/FC协议存储，物理机共享访问 • 支持共享云盘 • 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 • 支持实时查看主存储已用容量百分比趋势图
	NAS存储	• 支持云盘存放到POSIX兼容的分布式网络文件存储 • 支持实时查看主存储已用容量百分比趋势图
	Ceph存储	• 支持共享云盘 • 超融合管理节点高可用方案 • 支持指定不同性能的磁盘卷创建云盘 • 支持云盘存放到Ceph分布式存储 • 支持数据冷迁移 • 支持指定存储网络，支持存储网络和管理网络分离，增强云主机高可用 • 支持创建Ceph pool，以pool计算容量并设置显示名，并设置显示名 • 支持实时查看主存储已用容量百分比趋势图
	FusionStor存储	• 支持云盘存放到FusionStor分布式存储 • 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
	多主存储支持	支持同一集群挂载多个主存储，包括：多个本地存储、多个NFS存储、多个Shared Block存储、一个本地存储和一个NFS/SMP/Shared Block存储
网络管理	VLAN二层隔离	支持VLAN 802.1q作为网络隔离手段
	VXLAN网络	支持VXLAN网络，有效解决云数据中心逻辑网段不足、上层交换机MAC地址溢出等问题、支持云主机的跨地域迁移

类别	特性	ZStack企业版
	分布式扁平网络	支持云主机直接使用真实网络IP资源
	分布式弹性网络	支持云主机使用虚拟网络地址，与真实网络映射
	分布式DHCP服务	支持云主机自动获取分配的IP地址
	网络地址空间预留	支持预留网络地址空间，以便与物理网络混合使用
	动态和静态分配IP	支持动态分配IP地址，支持指定使用某个IP地址
	多级网络管理	支持云主机接入多个网络，构建复杂场景的业务
	虚拟IP的QoS设置	支持对虚拟IP做QoS限制，对网络服务的高效分配管理
	MTU	自定义限制网络传输数据包的大小
	VPC路由器	支持创建VPC路由器的全生命周期管理，包括：创建、删除、修改、VPC网络的加载/卸载，东西向流量的设置、云路由网络的所有网络服务，集中在VPC路由器中配置DNS
	VPC网络	支持创建VPC网络、添加网络段、加载/卸载VPC路由器、删除
	公有网络	• 支持创建云主机 • 支持为网络服务提供虚拟IP
	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	• 支持基于云路由的弹性IP • 支持基于云路由的端口转发 • 支持基于云路由的外部负载均衡以及内部访问业务流量的负载均衡 • 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
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

类别	特性	ZStack企业版
		• 创建云主机/云盘快照定时任务时，如果选择的所有云主机/云盘都使用Ceph主存储，支持设置保留快照数量
资源编排	资源栈	• 支持在线编辑方式和使用模板方式创建资源栈 • 支持预览/校验模板内容，支持云主机插入userdata • 支持删除资源栈和级联删除资源栈中所有资源
	自定义模板	支持通过文本编辑器方式和本地上传方式创建资源栈模板，并支持创建、查看、修改、删除、预览操作
	示例模板	云平台默认提供的资源栈模板示例，作为参考模板
	可视化资源编排	• 支持可视化拖拽资源方式创建资源栈模板 • 支持预览模板、生成资源栈、另存为资源栈模板 • 支持撤销、恢复、删除、清空画布操作
安全管理	三层安全策略	支持基于TCP/UDP端口的安全策略
	安全组统一管理	支持安全组统一管理云主机安全策略，实现组内互通，组间策略
性能TOP5和性能分析	性能TOP5	支持物理机、云主机、路由器、虚拟IP、三层网络等多种资源排序，并可自定义不同时间段查看
	云主机性能统计	支持自定义时间段查看，指定资源范围，对云主机CPU使用率、内存使用率、磁盘读速度、磁盘写速度、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	路由器性能分析	支持自定义时间段查看，指定资源范围，对路由器CPU使用率、内存使用率、磁盘读速度、磁盘写速度、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	物理机性能统计	支持自定义时间段查看，指定资源范围，对物理机CPU使用率、内存使用率、磁盘读速度、磁盘写速度、磁盘读IOPS、磁盘写IOPS、磁盘已用量百分比、网卡入速度、网卡出速度、网卡入包率、网卡出包率、网卡入错误速率、网卡出错误速率进行过滤分析排序
	三层网络性能分析	支持自定义时间段查看，指定资源范围，对三层网络已用IP数、已用IP百分比、可用IP数、可用IP百分比行过滤分析排序

类别	特性	ZStack企业版
	虚拟IP性能分析	支持自定义时间段查看，指定资源范围，对虚拟IP的下行网络流量、下行网络入包速率、上行网络流量、上行网络入包速率进行过滤分析排序
	镜像服务器性能分析	支持自定义时间段查看，指定资源范围，对镜像服务器的可用容量百分比进行过滤分析排序
ZWatch	物理机监控	对物理机运行实时监控，显示CPU、内存、磁盘和网络时序监控图
	云主机监控	对云主机运行实时监控，显示CPU、内存、磁盘和网络时序监控图
	监控	• 支持对系统时序数据进行监控，例如云主机内存使用率、物理机CPU使用率等 • 支持对系统事件进行监控，例如云主机状态变化事件、物理机失联事件等
	报警	对时序性数据和事件设置报警器，并通过SNS通知系统接收报警信息，支持邮件/钉钉/HTTP 应用方式接收报警信息
	多接收端	支持邮件/钉钉/HTTP应用等多种接收端
审计	资源审计	• 支持ZStack所有资源的审计查询，用户能对该资源的所有操作行为审计，有效保障用户在云环境下核心数据的安全 • 支持查看调用API名称、消耗时间、任务结果、操作员，任务创建/完成时间，以及API行为的消息详情，且支持CSV格式导出
操作日志	操作日志	支持查看操作描述、任务结果、操作员、登录IP、任务创建/完成时间，以及操作返回的消息详情，实现更细粒度管理，且支持CSV格式导出
账户管理	账户和用户管理	账户管理功能，分为账户和用户，其中账户是资源计量团体，用户可定义操作权限
	AD/LDAP账户	• 支持添加AD/LDAP账户，并绑定普通账户 • 支持自定义清除规则
	账户云资源配额	支持自定义分配账户最大可用资源，包括云主机运行数量、CPU、内存、云盘数量、云盘总容量、镜像数量、镜像总容量、弹性IP数量等
	用户组权限分配	支持用户组权限分配，统一编排用户权限

类别	特性	ZStack企业版
	用户操作权限分配	支持对用户进行权限分配
	云主机更改所有者	支持变更云主机所有者，指定云主机所属账户
	云盘更改所有者	支持变更云盘所有者，指定云盘所属账户
	计算规格指定分配	支持计算规格共享特性，可指定账户是否可使用
	镜像资源指定分配	支持镜像资源共享特性，可指定账户是否可使用
	云盘规格指定分配	支持云盘规格共享特性，可指定账户是否可使用
	网络资源指定分配	支持网络资源共享特性，可指定账户是否可使用
	全局配置	管理员可以直接在UI上对很多特性进行全局配置 • 所有的全局配置都有一个默认值 • 更新全局配置并不需要重启管理节点
	修改admin账户密码	忘记admin账户的登录密码，可以使用zstack-ctl reset_password还原默认值
计费	自定义计费单价	支持自定义CPU、GPU、内存、系统云盘和数据云盘的计费单价，其计费单价支持秒、分、小时和天；支持删除某时段的计费设置
	基于账户计费	基于账户进行计费，统计账户各项目消费情况
	灵活计费单价	动态可调的计费单价，满足周期性促销需求
访问	TUI	支持常用运维操作，定制化OS界面
	图形界面	• 支持以HTTP/HTTPS方式访问图形界面的云管理平台，账户（用户名密码方式或AD/LDAP方式）和用户支持图形界面登录访问 • 支持动态验证码验证。多次登陆（6次）失败触发验证码验证，防止恶意登陆 • 支持双因子认证。额外增加安全码身份验证，进一步增强账号安全
	命令行	支持通过命令行方式访问云管理平台，命令行支持全功能访问，账户和用户支持命令行登录访问
	API接口	支持全功能的API交付，API支持消息总线访问和HTTP接口访问
操作助手	智能提示	对ZStack的核心操作给出智能的环境检查和操作指导

类别	特性	ZStack企业版
亲和组	反亲和组	目前提供针对云主机与物理机的两种亲和组策略：反亲和组(非强制)、反亲和组(强制)，从而合理调度平台资源
UI强化	自定义产品信息	对UI上的产品Logo和产品名称等进行自定义
	首页大屏	华丽大屏展示平台整体情况
	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
应用中心	应用中心	支持添加包括存储、数据库、安全、IaaS、PaaS、SaaS类型在内的应用插件
License	云平台许可证	• 云平台许可证 (Basic License) 包括企业版和混合云版 • 支持本地浏览器上传License • 支持License到期提醒 • 企业单机无限期试用版支持所有功能
	模块许可证	• 模块许可证 (Plus License) 为用户提供附加功能 • 依赖于平台许可证使用 • 已包括：企业管理模块、VMware管理模块、裸金属管理模块、灾备服务模块 • 支持本地浏览器上传License • License到期提醒
管理节点	管理节点高可用（基于超融合方案）	• 支持基于Ceph的超融合场景 • 支持基于NFS、SMP的共享文件系统场景

类别	特性	ZStack企业版
		• 支持多网络灵活配置
	双物理机管理节点高可用	支持双物理机管理节点高可用。采用主备方案，某个管理节点故障后能迅速切换到另一个管理节点，保证业务正常运行
安装	一键安装	一条命令，30分钟完成从裸机到云平台的安装部署
升级	无缝升级	ZStack支持低版本至高版本的无缝升级
	增量升级	支持增量升级，大幅提高升级速度
	环境升级	可以指定只升级部署环境，通过专家模式自定义安装升级

ZStack企业管理模块功能列表：

类别	特性	企业管理模块
组织架构	用户	• 用户是企业管理中的最基本单位 • admin/平台管理员可创建用户，并基于用户建立相应的组织架构 • 支持添加用户、删除用户、修改用户名、修改密码、修改个人信息、加入部门、从部门移除、加入项目、从项目移除 • 用户的个人信息包括姓名、手机号码、邮箱地址和编号
	组织	• 组织是企业管理中组织架构的基本单位 • 组织以组织架构树的方式呈现，分为顶级部门和部门，顶级部门是组织的一级部门，其下可添加多级部门，支持创建多个顶级部门 • 支持添加组织、删除组织、更改上级部门、更改部门负责人、创建子部门、删除子部门、添加用户、移除用户
项目管理	项目	• 用于表示在特定时间、资源、预算下指定相关人员完成特定目标的任务 • 企业管理以项目为导向进行资源规划，可为一个具体项目建立独立的资源池 • 支持创建项目、删除项目、启用项目、停用项目、更换项目负责人、生成项目模板、添加成员、移除成员、停用项目资源、恢复过期项目
	项目模板	• 用于标识各个资源配额的模板

类别	特性	企业管理模块
		• 在创建项目时，可直接使用模板定义的配额来快速创建项目 • 支持创建项目模板、删除项目模板
	成员	• 成员作为项目的基本组成人员，一般由admin/平台管理员/项目负责人/项目管理员添加进入项目 • 项目成员的权限可由admin/平台管理员/项目负责人/项目管理员进行相应控制
	成员组	• 项目负责人/项目管理员可在项目中创建成员组，对成员进行分组管理 • 可以成员组为单位进行权限控制
工单管理	工单申请	• 项目成员可对云平台资源提出工单申请 • 支持项目成员创建、撤回、重新打开以及删除工单
	工单审批	• admin可进行一键审批，资源可自动部署成功并分发到项目中 • 支持admin通过、驳回工单，审批通过后会自动部署，该项目下的资源会立即生效
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
	裸金属设备	• 通过IPMI网络批量部署裸金属设备

类别	特性	裸金属管理模块
		• 支持对裸机进行远程电源管理 • 支持vnc无人值守模式
	裸金属主机	• 支持使用ISO类型镜像为裸金属设备安装Linux操作系统 • 支持为裸金属主机添加网络配置

ZStack灾备服务模块功能列表：

类别	特性	灾备服务模块
灾备服务	备份任务	• 支持为云主机和云盘创建备份任务 • 支持将数据备份在本地备份服务器并到远端服务器
	备份数据	• 支持查看云主机和云盘的备份数据的入口 • 支持查看和删除不同云主机和云盘的数据信息
	本地备份服务器	备份云主机和云盘的数据。支持使用ImageStore类型的备份服务器，支持主备服务器无缝切换
	远端备份服务器	• 支持将本地备份服务器的备份数据同步到远端备份服务器 • 支持异地机房和阿里云备份服务器，满足双重备份要求

3.2 混合云功能

ZStack for Alibaba Cloud支持管纳阿里云的ECS和VPC服务，统一的管理平台让用户操作阿里云的资源如同操作本地资源一样稳定快捷。

目前对于阿里云的管控界面包含如下功能：

类别	特性	ZStack for Alibaba Cloud
数据中心	阿里云地域管理	• 查看阿里云地域列表 • 支持地域的添加和删除；以及地域下资源同步 • 阿里云地域特性： 一般情况下，建议选择与目标用户所在地域最为接近的数据中心，以进一步提升用户访问速度 在基础设施、BGP网络品质、服务质量、云服务器操作使用与配置等方面，阿里云国内地域数据中心无明显差异。国内BGP网络可以保证全国地域的快速访问

类别	特性	ZStack for Alibaba Cloud
	阿里云可用区管理	• 查看阿里云可用区列表 • 支持可用区的添加和删除，以及可用区资源的一键同步 • 阿里云可用区特性： 同一可用区内的ECS实例网络延时更小； 同一地域内的可用区之间内网互通，且可用区之间故障隔离； 是否将ECS实例放在同一可用区内，主要取决于对容灾能力和网络延时的要求
ECS	ECS生命周期管理	包括ECS云主机的创建（支持批量创建）、启动、停止、重启、同步、删除，以及支持修改ECS云主机名称和简介、显示付费方式、修改系统用户密码
	ECS云主机控制台	通过ZStack for Alibaba Cloud混合云管理界面即可打开ECS云主机控制台，以及设置控制台密码
	安全组、EIP管理	包括安全组和安全组规则的创建、远程同步、查看、阿里云端删除、本地删除；以及EIP的创建、同步、查看、加载到ECS、从ECS卸载及删除
	ECS镜像管理	支持镜像的删除、同步；支持本地镜像上传为ECS自定义镜像，以及同步阿里云系统镜像，支持查看上传进度
	ECS数据云盘管理	支持数据云盘的创建、删除、同步；支持云主机加载/卸载数据云盘；以及修改数据云盘名称和简介、显示付费方式
阿里云NAS	文件系统	• 支持接管阿里云NAS文件系统，并创建NAS主存储 • 支持创建、修改、删除文件系统 • 支持从已有的文件系统中选择文件系统；支持自定义创建文件系统
	权限组	• 支持创建、删除权限组，可通过创建不同的权限组规则 • 支持从已有的文件系统中选择权限组；支持自定义新建权限组
	NAS存储	可以通过已经添加的阿里云NAS，添加阿里云NAS类型的主存储
网络	VPC管理	• 支持VPC的创建、同步、查看、阿里云端删除以及本地删除

类别	特性	ZStack for Alibaba Cloud
		• 支持虚拟交换机的创建、同步、查看、阿里云端删除以及本地删除 • 支持VPC内虚拟路由器的同步、查看以及路由条目的创建、同步、查看、阿里云端删除、本地删除
	高速通道	• 支持快速建立高速通道，配置双边路由 • 支持边界路由器的同步、查看 • 支持路由器接口的同步、查看

	VPN	• 支持VPN网关的同步、查看、本地删除
		• 支持VPN用户网关的创建、同步、查看、阿里云端删除、本地删除
		• 支持VPN连接管理：
		  - VPN连接的创建、同步、查看、修改、阿里云删除、本地删除
		  - IPsec配置的创建、查看、删除
		  - Ike配置的创建、查看、删除
		  - 快速建立VPN连接

混合云灾备	本地云主机、镜像、云盘	支持本地云主机、镜像、云盘创建灾备数据到异地或公共云的灾备服务器中
	灾备数据	支持灾备数据的还原、删除、恢复、彻底删除
	灾备服务器	支持灾备服务器的添加、重连、删除
SD-WAN	第三方专线接入	借助第三方专线接入，打通私有云到公共云的高速通道
其它	密钥管理	支持阿里云/大河AccessKey（包括AccessKey ID以及AccessKey Secret）在本地的添加、删除、查看以及默认设置；支持多个AccessKey的添加
	对象存储OSS	包括OSS bucket的添加、同步、查看、阿里云端删除、本地删除
	时区配置	支持配置时区以便部署到海外不同站点

4 产品优势

ZStack for Alibaba Cloud结合了ZStack专有云的4S优势（Simple简单、Strong健壮、Scalable弹性、Smart智能）以及阿里云公共云强大的弹性支撑能力和多数据中心容灾备份等能力。

4.1 专有云优势

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。

4.2 混合云优势

ZStack for Alibaba Cloud提供了一套无缝集成的混合云管理方案，用户能够无感知地在本地和远程数据中心混合作业，在确保安全性、可控性的前提下，为本地数据中心的服务引入强大的弹性支撑能力、全面的网络覆盖能力以及多数据中心容灾备份能力。

- **一套界面，统一管理**：通过打通账号、网络、存储等核心资源，用户可在ZStack云平台管理界面对本地专有云资源和阿里云公共云资源进行统一管理。
- **深度整合，无缝操作**：公共云资源与用户本地专有云资源在数据层面和控制层面均实现互通，这一深度整合让用户对公共云资源和本地专有云资源的操作体验是有机结合的一体而不是互相割裂的感觉。
- **两类云主机网络互通**：可自动化实现本地专有云主机与公共云主机在网络层面的互通，而且既支持以物理专线的方式进行网络互通，也支持以虚拟专线的方式进行网络互通。
- **利用公共云功能扩展专有云能力**：支持本地业务按需随时随地备份到公共云，或通过公共云备份到异地数据中心；也可将业务随时扩容到公共云上协同工作；本地业务如需使用阿里云CDN、RDS等服务，可在公共云上进行连接。

5 产品价值

ZStack for Alibaba Cloud不仅拥有ZStack专有云独有价值，还给用户带来一系列混合云价值。

5.1 专有云价值

以下是ZStack专有云平台带来的独有价值：

- 沿用了ZStack极速部署升级的特点，混合云的引入对ZStack本身独一无二的部署升级特点没有任何影响，用户可以放心使用 。
- 沿用了ZStack全异步、无状态的架构，用户会发现公共云主机的创建同ZStack本地云主机的创建一样快速稳定，在通知、监控、API、文档上都是一致的。
- 用户可以在同一个界面上管理公共云和专有云，最大的特点是数据互通。它们使用了同一套镜像，同一套计算规格，同样的管理节点，而不是各自选择。
- 用户可以通过阿里云的VPC，以及ZStack的云路由，以IPsec隧道或专线方式进行连接，实现内网打通，整个过程全自动化，非常轻松 。
- 用户可以很方便通过ZStack进行备份，将ZStack中的数据备份到公共云上进行容灾。

5.2 混合云价值

以下是ZStack for Alibaba Cloud带来的混合云价值：

- 将合适的应用放到合适的云上。追求成本的业务放到阿里云上按需付费，追求稳定性或者暂时无法迁移的应用在ZStack中运行。
- 不同开发阶段的业务放到不同的云上。例如开发测试在ZStack中进行，生产应用发布到阿里云上；或者将新业务放到阿里云上测试，稳定版本在企业中应用。
- 前端应用在阿里云上部署，可以利用阿里云的CDN等其它产品，而核心数据库业务在ZStack部署，通过专线进行互通 。
- 在业务高峰期利用公共云的弹性，扩大系统的高峰期能力。
- 多个ZStack数据中心利用公共云做迁移以及容灾备份。

ZStack for Alibaba Cloud能够提供优秀的混合云解决方案，源于ZStack自身就是轻量级IaaS专有云平台，因此并非简单的集成，而是把公共云的操作无缝集成到ZStack中，让ZStack专有云的所有优点都输出到混合云上，为用户提供一个真正的统一管理视图。

专有云术语表

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、FusionStor、Shared Mount Point等类型。

镜像服务器（Backup Storage）

也称之为备份存储服务器，主要用于保存镜像模板文件。建议单独部署镜像服务器。

镜像仓库（Image Store）

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

云主机（VM Instance）

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

镜像（Image）

云主机或云盘使用的镜像模板文件，镜像模板包括系统云盘镜像和数据云盘镜像。

云盘（Volume）

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

计算规格（Instance Offering）

启动云主机涉及到的CPU数量、内存、网络设置等规格定义。

云盘规格（Disk Offering）

创建云盘容量大小的规格定义。

二层网络（L2 Network）

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

三层网络（L3 Network）

云主机使用的网络配置，包括IP地址范围、网关、DNS等。

公有网络（Public Network）

由因特网信息中心分配的公有IP地址或者可以连接到外部互联网的IP地址。

私有网络（Private Network）

云主机连接和使用的内部网络。

L2NoVlanNetwork

物理主机的网络连接不采用Vlan设置。

L2VlanNetwork

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

VXLAN网络池（VXLAN Network Pool）

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

VXLAN网络（VXLAN）

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

云路由（vRouter）

云路由通过定制的Linux云主机来实现的多种网络服务。

安全组（Security Group）

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

弹性IP（EIP）

公有网络接入到私有网络的IP地址。

快照（Snapshot）

某一个时间点上某一个磁盘的数据备份。包括自动快照和手动快照两种类型。

混合云术语表

访问密钥（AccessKey）

用于调用阿里云API或大河云联API的唯一凭证，AccessKey包括AccessKeyID（用于标识用户）和AccessKeySecret（用于验证用户密钥）。

数据中心（Data Center）

包含阿里云的地域和可用区等地域资源，用于匹配阿里云资源的地域属性。

地域（Region）

物理的数据中心，划分地区的基本单位，ZStack混合云的地域对应了阿里云端的地域。

可用区（Identity Zone）

在同一地域内，电力和网络互相独立的物理区域，ZStack混合云的可用区对应了阿里云端的可用区（Zone）。

存储空间（Bucket）

用于存储对象（Object）的容器，ZStack使用对象存储（OSS）里的Bucket来上传镜像文件。

ECS云主机（Elastic Compute Service）

阿里云端创建的ECS实例，可在ZStack混合云界面进行ECS云主机生命周期的管理。

专有网络VPC（Virtual Private Cloud）

用户基于阿里云构建的一个隔离的网络环境，不同的专有网络之间逻辑上彻底隔离。

虚拟交换机（VSwitch）

组成专有网络VPC的基础网络设备，可以连接不同的云产品实例。ZStack混合云的虚拟交换机对应了阿里云VPC下的虚拟交换机。

虚拟路由器（VRouter）

专有网络VPC的枢纽，可以连接专有网络的各个虚拟交换机，同时也是连接专有网络与其它网络的网关设备。ZStack支持查看VPC下的虚拟路由器。

路由表（Route Table）

虚拟路由器上管理路由条目的列表。

路由条目（Route Entry）

路由表中的每一项是一条路由条目。路由条目定义了通向指定目标网段的网络流量的下一跳地址。路由条目包括系统路由和自定义路由两种类型。ZStack支持自定义类型的路由条目。

安全组（Security Group）

针对云主机进行第三层网络的防火墙控制。ZStack混合云的安全组对应了阿里云端ECS云主机三层隔离的防火墙约束。

镜像（Image）

云主机使用的镜像模板文件，一般包括操作系统和预装的软件。ZStack支持上传本地镜像到阿里云，以及使用阿里云端镜像。

弹性公网IP（EIP）

阿里云端公有网络池中的IP地址，绑定弹性公网IP的ECS实例可以直接使用该IP进行公网通信。

VPN连接（VPN Connection）

通过建立点对点的IPsec VPN通道，实现企业本地数据中心的私有网络与阿里云端VPN网络进行通信。

VPN网关（VPN Gateway）

一款基于Internet，通过加密通道将本地数据中心和阿里云专有网络VPC安全可靠连接起来的服务。用户在阿里云VPC创建的IPsec VPN网关，与本地数据中心的用户网关配合使用。

VPN用户网关（Customer Gateway）

本地数据中心的VPN服务网关。可通过ZStack混合云创建VPN用户网关，并将VPN用户网关与VPN网关连接起来。

高速通道（Express Connect）

通过物理专线（即租用运营商的专线：电缆或光纤），连通本地数据中心到阿里云专线接入点，与阿里云VPC环境打通，实现云上云下不同网络间高速，稳定，安全的私网通信。

边界路由器（VBR）

用户申请的物理专线接入交换机的产品映射。用户在物理专线上可以创建边界路由器，边界路由器负责专线上的数据在阿里云上进行转发。通过边界路由器，用户数据可以直达阿里云VPC网络。

路由器接口（Router Interface）

一种虚拟的网络设备，可以挂载在路由器并与其他路由器接口进行高速通道互联，实现不同网络间的内网互通。