

阿里云 ZStack for Alibaba Cloud

技术白皮书

产品版本：V2.1.0

文档版本：20170830









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。 |  危险：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。 |  注意：导出的数据中包含敏感信息，请妥善保管。 |
|  | 用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。 |  注：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。 |
| <code>courier</code> 字体 | 命令。 | 执行 <code>cd /d C:/windows</code> 命令，进入Windows系统文件夹。 |
| 斜体 | 表示参数、变量。 | <i>bae log list --instanceid Instance_ID</i> |
| []或者[a b] | 表示可选项，至多选择一个。 | <i>ipconfig [-all -t]</i> |
| { }或者{a b} | 表示必选项，至多选择一个。 | <i>switch {stand slave}</i> |

目录

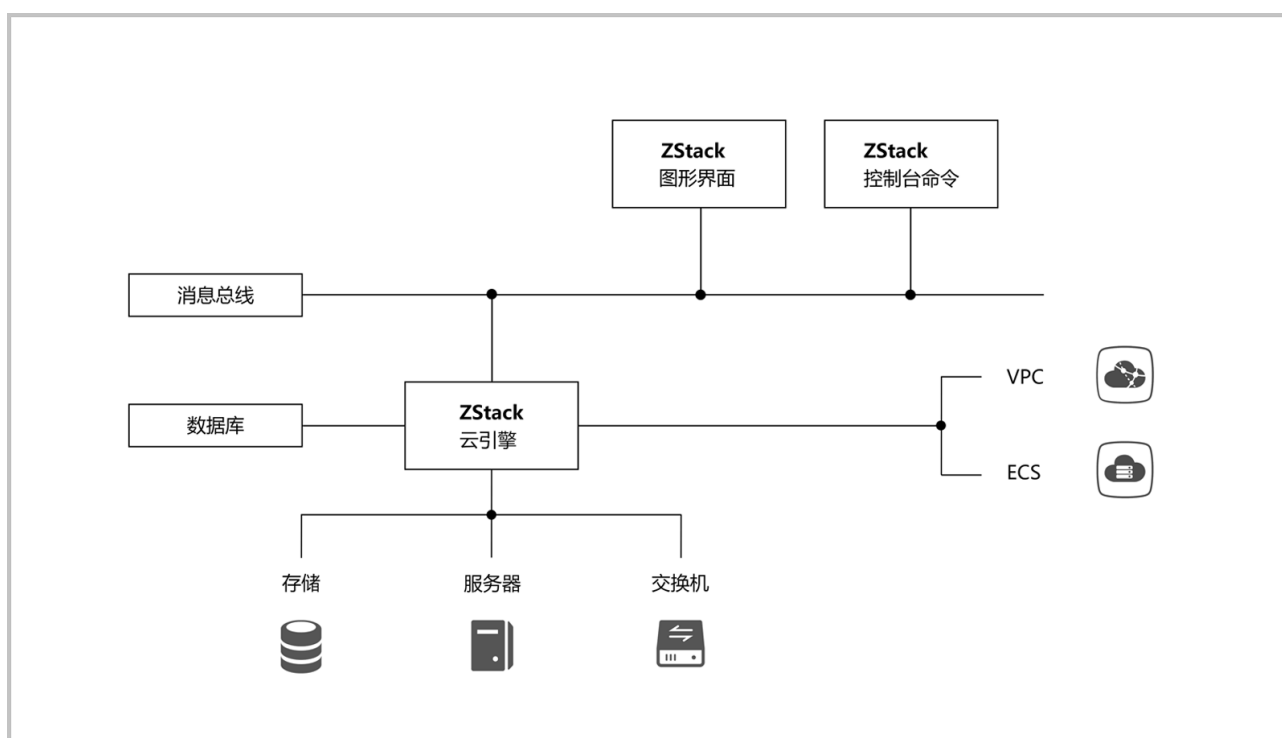
| | |
|-----------------------|-----------|
| 法律声明..... | I |
| 通用约定..... | I |
| 1 产品概述..... | 1 |
| 2 系统架构..... | 2 |
| 2.1 专有云架构..... | 2 |
| 2.1.1 ZStack功能架构..... | 2 |
| 2.1.2 ZStack资源结构..... | 5 |
| 2.2 混合云架构..... | 7 |
| 2.2.1 身份认证..... | 7 |
| 2.2.2 互联网络..... | 8 |
| 2.2.3 资源管理..... | 9 |
| 2.2.4 业务实现..... | 10 |
| 3 产品功能..... | 11 |
| 3.1 专有云功能..... | 11 |
| 3.2 混合云功能..... | 16 |
| 4 产品优势..... | 18 |
| 4.1 专有云优势..... | 18 |
| 4.2 混合云优势..... | 19 |
| 5 产品价值..... | 20 |
| 5.1 专有云价值..... | 20 |
| 5.2 混合云价值..... | 20 |
| 专有云术语表..... | 21 |
| 混合云术语表..... | 24 |

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。它结合了ZStack的简单、强壮、弹性、智能以及阿里云公共云的领先、安全、稳定等特点，并以“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: 系统架构示意图所示：

图 1: 系统架构示意图



2 系统架构

本章主要介绍了ZStack专有云架构，以及基于ZStack深度定制的ZStack for Alibaba Cloud混合云架构。

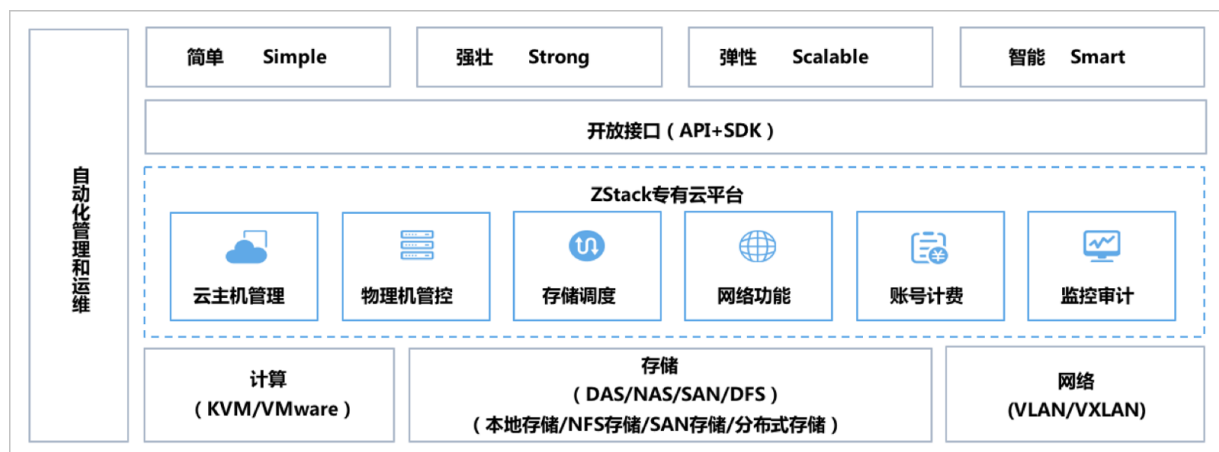
2.1 专有云架构

ZStack作为新一代轻量级私有云专有云管理平台，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: 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RabbitMQ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、强壮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RabbitMQ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可并发处理数万条API请求，还可同时管理数十万台服务器和数百万的云主机。

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。

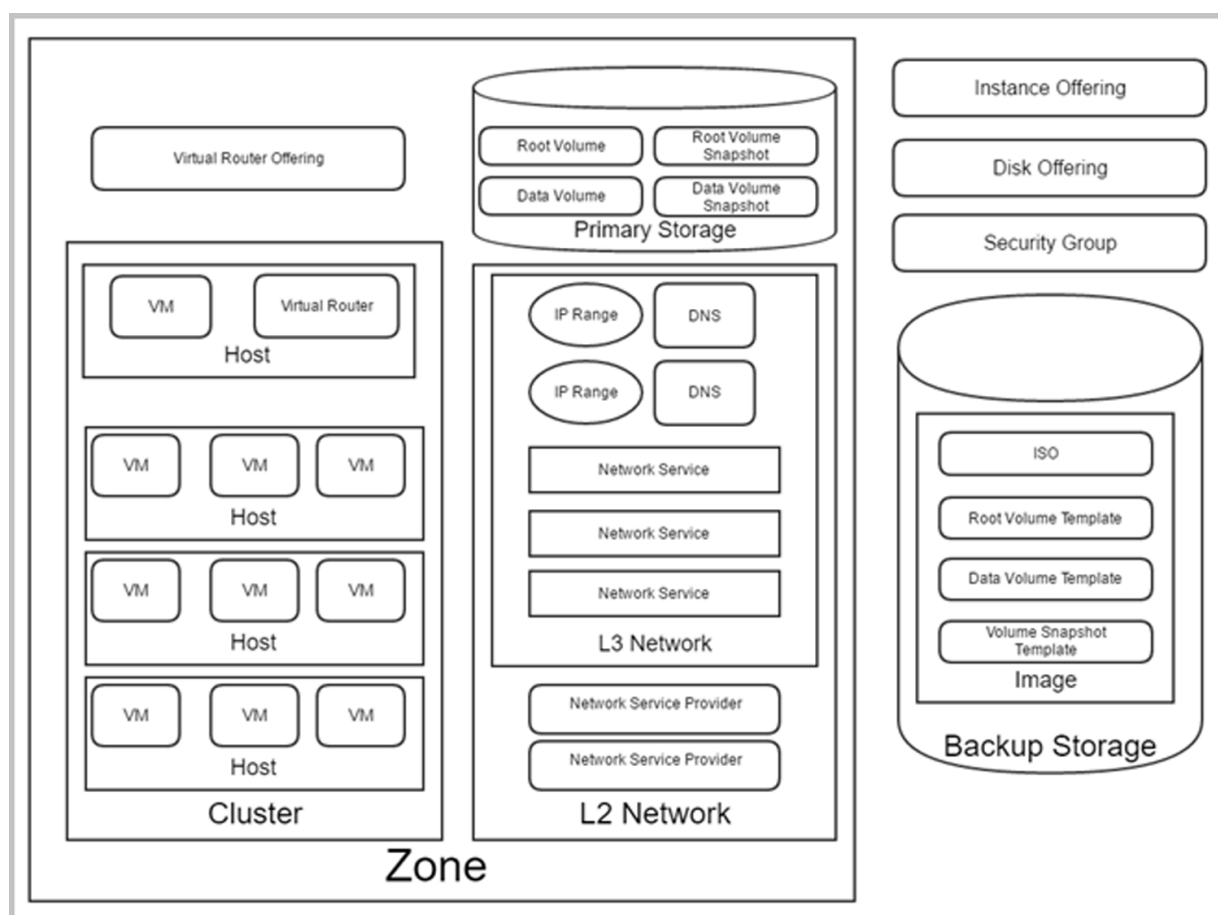
10. 全API查询：任意资源的任意属性均可查询。

- 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 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：集群是一群计算节点（物理机）的逻辑组合。
- 物理机：为云主机实例提供计算、网络、存储的物理主机。
- 主存储：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：备份存储服务器，主要用于保存云主机的镜像模板文件。
- 二层网络：二层广播域，进行二层相关的隔离，支持 L2NoVlanNetwork、L2VlanNetwork、VxlanNetworkPool、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：直接交付给用户使用的虚拟主机系统，是ZStack的核心组成部分。
- 镜像：云主机所使用的镜像模板文件，包括ISO和Image类型。
- 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。
- 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。
- 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。
- 安全组：给云主机提供三层网络防火墙控制。
- 云路由规格：指定云路由设备使用的CPU、内存、云路由镜像、管理网络、公有网络等资源定义。
- 云路由设备：为云主机提供DHCP、DNS、SNAT、弹性IP、端口转发、负载均衡、IPsec、安全组等各种网络服务的定制云主机。

ZStack资源间存在以下关系：

- 父子关系：例如集群和物理机，物理机和云主机。
- 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：例如集群和云主机，区域和物理机。
- 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备份存储进行保存为模板。

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。

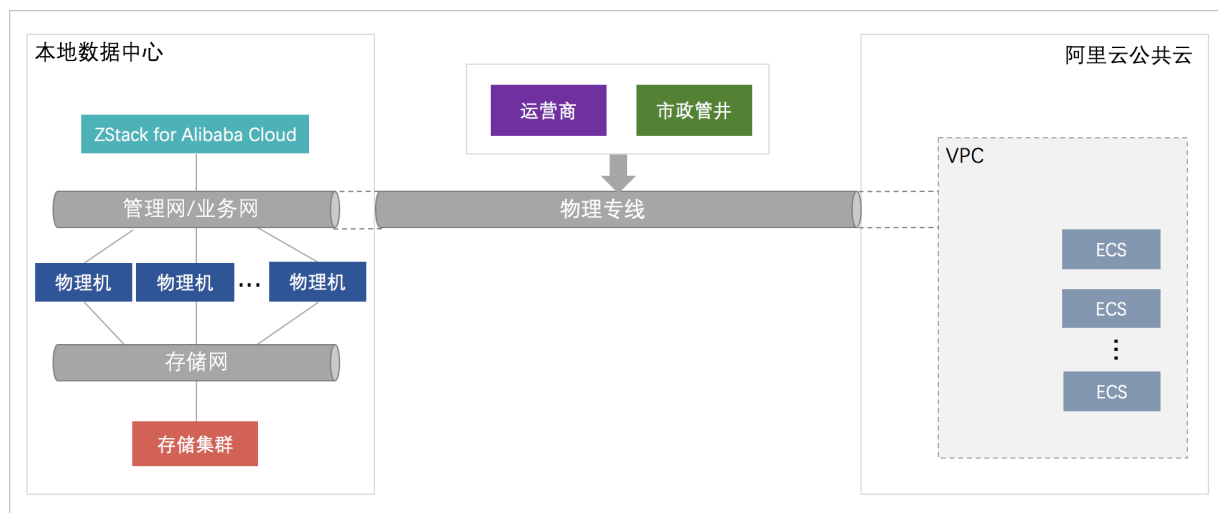
2.2 混合云架构

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。

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

如图 4: 混合云物理部署架构所示，通过物理专线构建“本地—远程”互连网络，从而连通本地数据中心和阿里云公共云。

图 4: 混合云物理部署架构



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

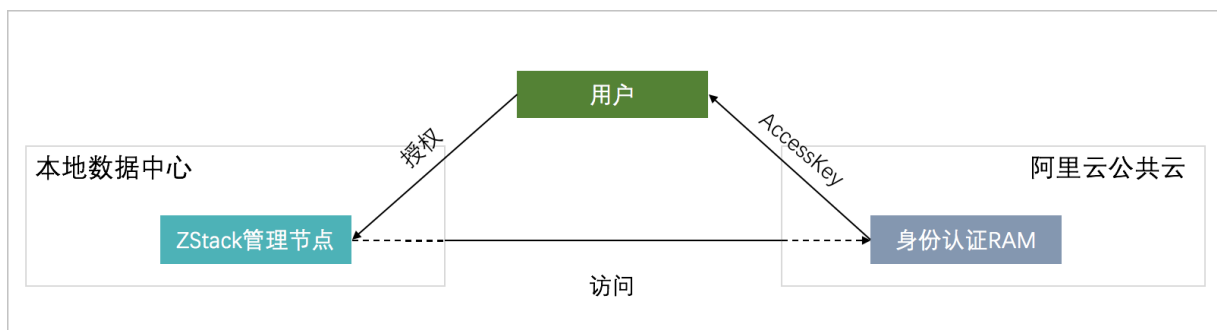
2.2.1 身份认证

ZStack for Alibaba Cloud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（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，可登陆到阿里云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 5: 混合云身份认证功能模块图



2.2.2 互连网络

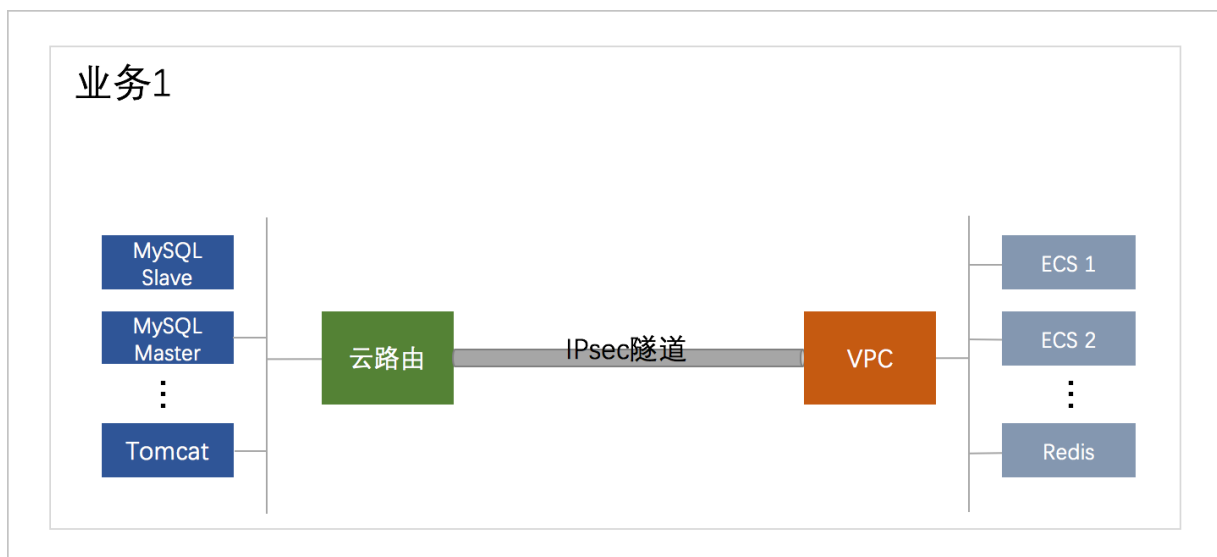
实现IPsec隧道和高速通道（Express Connect）连接本地专有云和阿里云公共云，使得“本地—远程”在三层网络可达下互访。“本地—远程”的互连网络，是混合云核心基础设施。

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

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。由于互连网络延迟较大、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。如图 6: IPsec隧道所示：

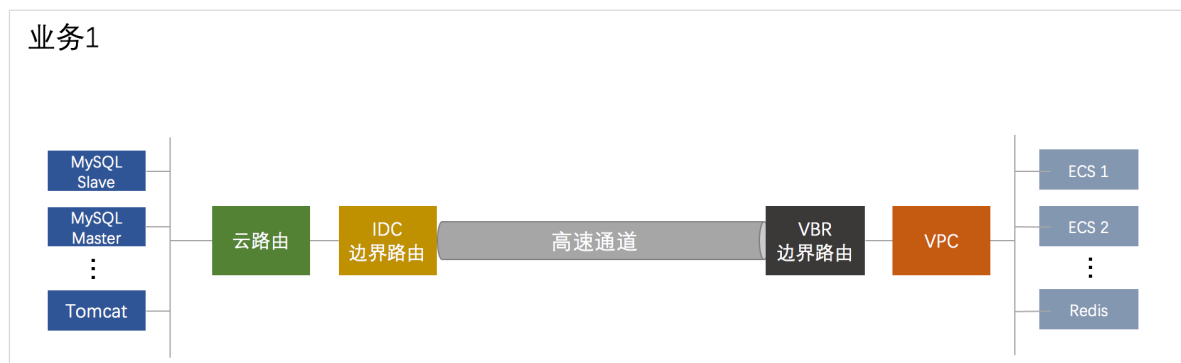
图 6: IPsec隧道



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。如图 7: 高速通道所示：

图 7: 高速通道



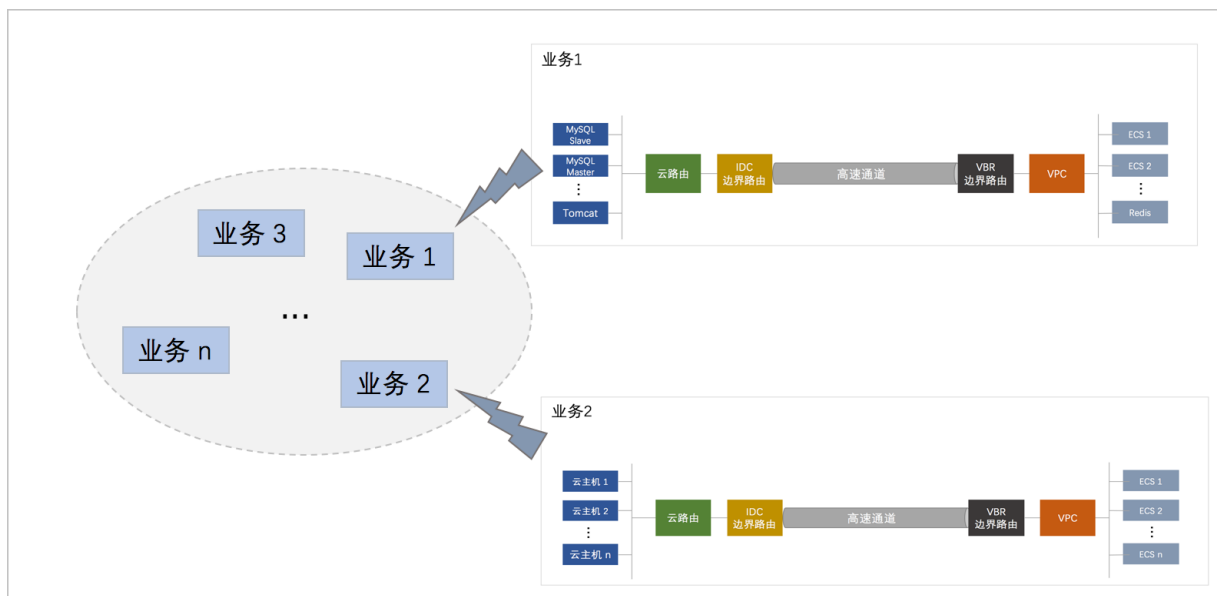
2.2.3 资源管理

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，管理员无需再登陆访问阿里云公共云门户控制台，直接通过ZStack for Alibaba Cloud混合云平台本地登陆后，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 8: 混合云资源管理功能模块



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），实现低成本的数据容灾方案，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作为轻量级私有云专有云平台，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专有云环境，并快速创建云主机、分配云盘和自动配置云主机网络。

ZStack for Alibaba Cloud拥有ZStack企业版的完整功能。

ZStack企业版功能列表：

| 类别 | 特性 | ZStack企业版 |
|------|-----------|---|
| 区域 | 接管vCenter | 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；在VMware vCenter集群中完成对云主机的常用操作 |
| | 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 |
| 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 |
| | 物理主机 | 集群内管理物理主机 |
| | 云主机 | 集群内管理云主机 |
| | 集群功能 | 提供高可用特性 |
| | 网络服务 | 支持VLAN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） |
| 物理主机 | 虚拟化 | 支持KVM虚拟化技术，支持VMware虚拟化 |
| | 资源设定超分 | 支持CPU、内存和存储空间设定超分比例，适应云环境资源使用 |
| | 嵌套虚拟化 | 支持KVM/ESXi嵌套虚拟化，云主机内部开启CPU硬件虚拟化功能 |
| | 实时监控 | 采集物理主机的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 |
|-----|------------|--|
| | 停用与启用 | 对物理主机设定可用属性，以便停止在该物理主机上创建云主机 |
| | 维护模式 | 对物理主机设定维护状态，设定维护模式后，物理主机的云主机将会进入迁移状态 |
| | 裸机管理 | 通过PXE技术，使管理员自动化完成对新上线物理机的批量添加和部署。 |
| | GPU透传 | 支持物理机PCI设备透传，让云主机拥有高性能计算和图形处理能力。 |
| | 操作日志 | 展示物理主机执行任务的事件审计 |
| 云主机 | 批量操作 | 批量创建/删除多个云主机 |
| | 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 |
| | 云主机在线快照 | 在云主机运行过程中进行快照 |
| | 云盘在线快照 | 在云盘挂载状态中进行快照 |
| | 云主机在线修改密码 | 支持Windows/Linux OS在线修改密码 |
| | 云主机QGA开关 | 灵活控制qemu guest agent的状态 |
| | 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显卡透传 |
| | userdata导入 | 支持创建云主机时导入userdata |
| | 云主机克隆 | 基于云主机快速克隆若干个云主机 |
| | 基于ISO部署 | 基于ISO系统光盘部署云主机，引导安装程序 |
| | 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 |
| | 云主机启动顺序 | 调整云主机的启动顺序，用于切换ISO启动 |
| | 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 |
| | 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 |
| | 高可用特性 | 物理主机故障，云主机自动重启 |

| 类别 | 特性 | ZStack企业版 |
|------|---------------|---|
| | 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，支持创建和删除密钥 |
| | 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 | 支持所有主存储类型上的云主机进行关机状态迁移 |
| | 热迁移 | 支持所有主存储类型上的云主机进行运行状态迁移 |
| | 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 |
| 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ISO镜像，支持从ISO镜像引导云主机 |
| 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 |
| | 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 |

| 类别 | 特性 | ZStack企业版 |
|------|--------------|---|
| 存储管理 | 本地存储 | 支持云盘存放到物理机本地 |
| | NFS存储 | 支持云盘存放到NFS协议存储，物理主机共享访问 |
| | 共享存储 | 支持云盘存放到POSIX兼容的共享存储，支持iSCSI/FC存储 |
| | Ceph存储 | 支持共享云盘；超融合管控节点高可用方案；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 |
| | FusionStor存储 | 支持云盘存放到FusionStor分布式存储 |
| | 多主存储支持 | 支持同一集群挂载多个主存储，包括多个本地存储或多个NFS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 |
| | 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 |
| | 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 |
| | | 支持基于云路由的负载均衡 |
| | | 支持基于多个EIP绑定同一个云主机网卡 |
| | | 支持基于云路由的IPsec隧道服务 |
| | | 支持一个云路由设备接多个公有网络 |
| | | 支持配置静态路由表 |
| | | 支持分布式DHCP提升服务性能 |
| 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 |
|------|----------|---|
| 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 |
| 性能分析 | 云主机性能统计 | 支持云主机CPU、内存、磁盘和网络的性能分析，排序筛选 |
| | 物理主机性能统计 | 支持物理主机CPU、内存、磁盘和网络的性能分析，排序筛选 |
| 实时监控 | 物理主机监控 | 支持物理主机运行实时监控，显示CPU、内存、磁盘和网络时序监控图 |
| | 云主机监控 | 支持云主机运行实时监控，显示CPU、内存、磁盘和网络时序监控图 |
| | 警报功能 | 支持物理机失联或其他原因引起的故障警报；支持物理机失联或其他原因引起的故障警报 |
| 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 |
| | 导出csv文件 | 支持云主机列表和物理机列表导出为csv表格，方便统计分析处理 |
| 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 |
| | 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、镜像总容量和弹性IP数量 |
| | 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 |
| | 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 <ul style="list-style-type: none"> 所有的全局配置都有一个默认值 |

| 类别 | 特性 | ZStack企业版 |
|--------|-------------|--|
| | | <ul style="list-style-type: none"> 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、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Web图形界面的访问云管理平台，账户（用户名密码方式或LDAP方式）和用户支持图形界面登陆访问 |
| | 命令行 | 支持通过命令行方式访问云管理平台，命令行支持全功能访问，账户和用户支持命令行登陆访问 |
| | 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 |
| VDI | 解决方案 | 通过定制盒子，支持SPICE，RDP，VNC等协议，并进行了优化 |
| 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 |
| 安装 | 一键安装 | 一条命令，15分钟完成私有云专有云搭建 |
| 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 |

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 混合云 |
|------|-------------|--|
| 数据中心 | 查看阿里云上的地域列表 | 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。不过，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 |
| | 虚拟数据中心管理 | 支持用户对虚拟数据中心的添加及删除 |
| | 可用区管理 | 支持可用区的添加和删除。同一可用区内的ECS实例网络延时更小；在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离；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 | 包括创建、启动、停止、释放、同步ECS云主机 |
| | ECS云主机控制台 | 通过ZStack管理界面即可打开ECS云主机控制台，以及修改控制台密码 |
| | 安全组、EIP管理 | 包括安全组和安全组规则的创建、远程同步、删除，以及EIP的创建、同步、加载到ECS、从ECS卸载及删除 |
| | ECS镜像管理 | 包括镜像创建、删除、同步等功能 |
| | ECS数据云盘 | 支持云主机加载/卸载数据云盘 |
| 网络 | VPC管理 | 支持VPC的创建、同步和删除；VPC内路由器的同步及路由条目的创建、同步和删除；虚拟交换机的创建、同步与删除 |
| | 高速通道 | 支持快速建立高速通道；支持接入点列表的查看、添加、删除；边界路由器及路由规则的创建、同步、删除；边界路由器的连接终止、恢复；路由器接口的创建、同步、删除以及属性修改； |
| | VPN | 支持创建、删除、同步以及修改VPN连接；同步VPN网关；创建、删除、同步VPN用户网关；自动创建VPN配置 |
| 其它 | 密钥管理 | 支持AccessKey以及KeySecret在本地的添加、删除、查看以及卸载到ZStack；支持多个AccessKey以及KeySecret的添加 |
| | 支持对象存储 OSS | 包括远程OSS的创建、删除、添加到本地以及远程OSS中相关资源的管理 |
| | 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强壮、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强壮，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，5分钟完成安装，10分钟完成部署。
- 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. 强壮（Strong）

- 稳定且高效的系统架构设计：拥有全异步的后台架构，进程类微服务架构，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。目前已实现单台管理节点管理十万台物理主机和百万台云主机。
- 支撑高并发的API请求：单ZStack管理节点可以轻松处理每秒至少3万个并发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主机动态迁移。

3. 弹性（Scalable）

- 支撑规模无限制：单管理节点可管理从一台到十万台物理机，百万台云主机。
- 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，主要用于保存云主机的镜像模板文件。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)

云主机使用的镜像模板文件，包含云主机的操作系统，也可以定制安装相应的软件。

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。

IPsec VPN

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

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。