混合云使用教程

产品版本：ZStack 3.2.0

文档版本：V3.2.0

ZStack

版权声明

商标说明

ZStack商标和其他云轴商标均为上海云轴信息科技有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

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

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

目录

1 概述

ZStack混合云平台，结合了ZStack私有云的简单、健壮、弹性、智能以及阿里云公有云的领先、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，实现了混合云真正意义上的控制面和数据面互联互通。

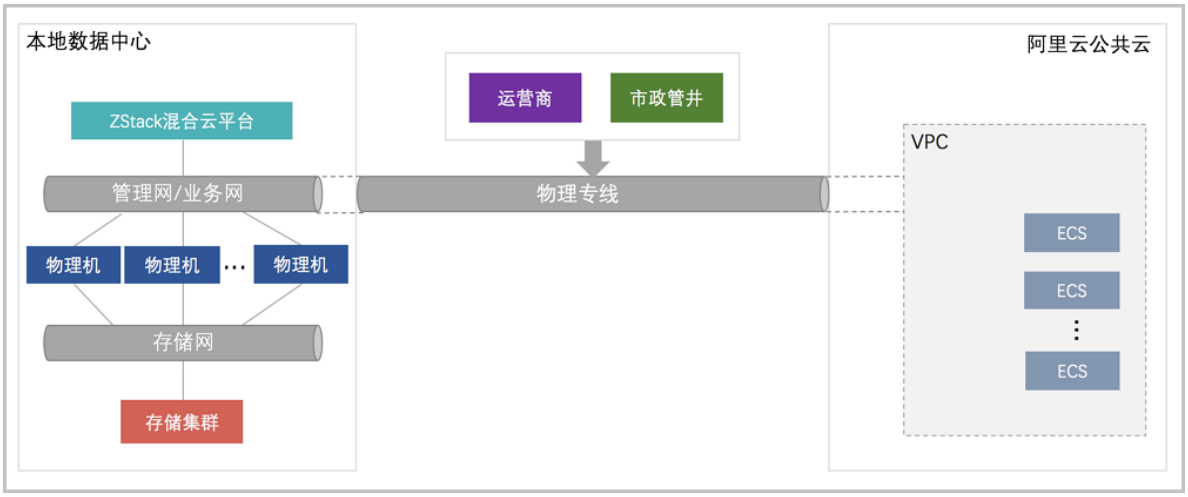
物理部署

由于ZStack采用进程内微服务架构，因此ZStack混合云平台的部署与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，以便调用阿里云公有云的OpenAPI。

1. 基于物理专线部署

   如图 *1:* 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有云。

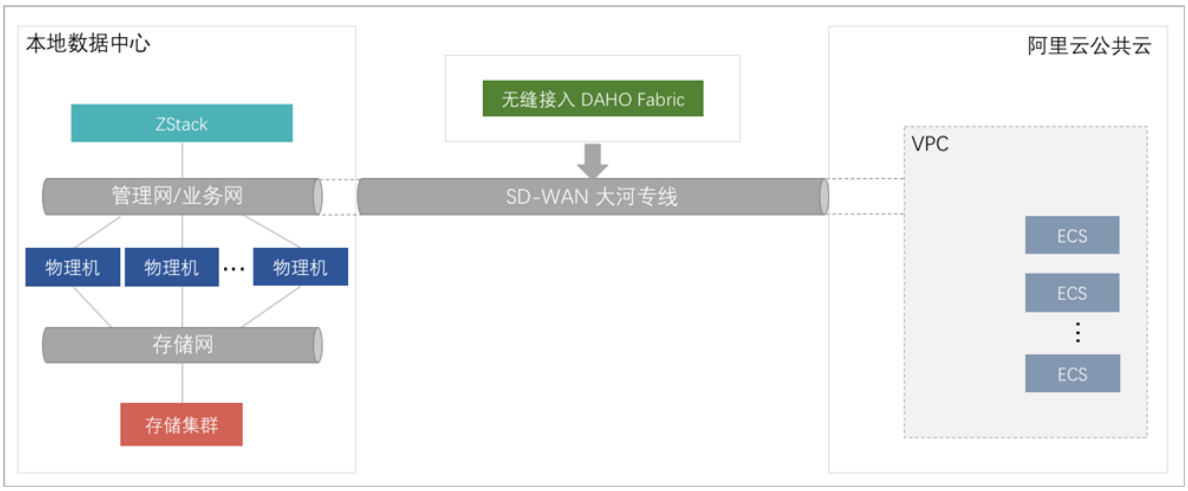
   图 1: 基于物理专线部署



2. 基于SD-WAN部署

   如图 *2:* 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有云。

   图 2: 基于SD-WAN部署



混合云功能模块

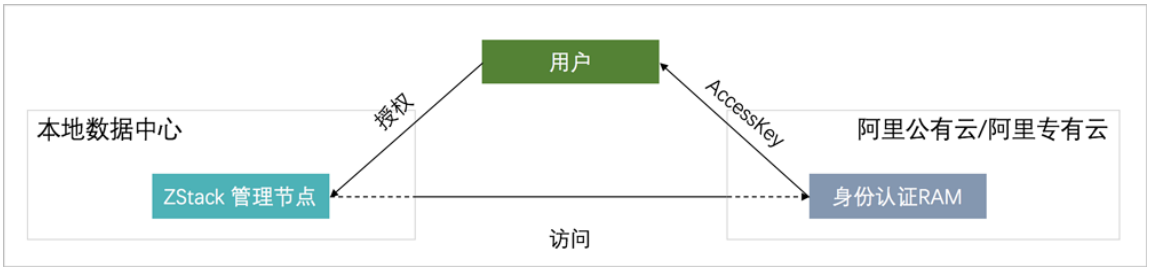
ZStack混合云功能模块主要有：身份认证、互联网络、资源管理和业务实现。

1. **身份认证**：

- 阿里云AK：

  实现了阿里云（阿里公有云）/阿里专有云的账户身份认证RAM对接，采用授权子账户AK（AccessKey以及KeySecret）信息远程访问，如图 *3:* 身份认证所示：

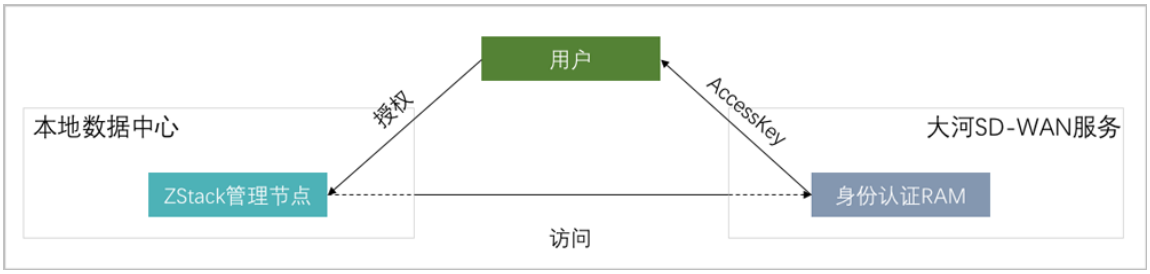
  图 3: 身份认证



- 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 *4:* 身份认证所示：

  图 4: 身份认证



2. **互联网络**：

实现IPsec隧道、阿里云高速通道（Express Connect）、大河高速通道连接本地私有云和阿里云公有云，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混合云平台支持IPsec隧道、阿里云高速通道、大河高速通道构建互联网络，如图 *5: IPsec*隧道、图 *6:* 阿里云高速通道和图 *7:* 大河高速通道所示：

图 5: IPsec隧道

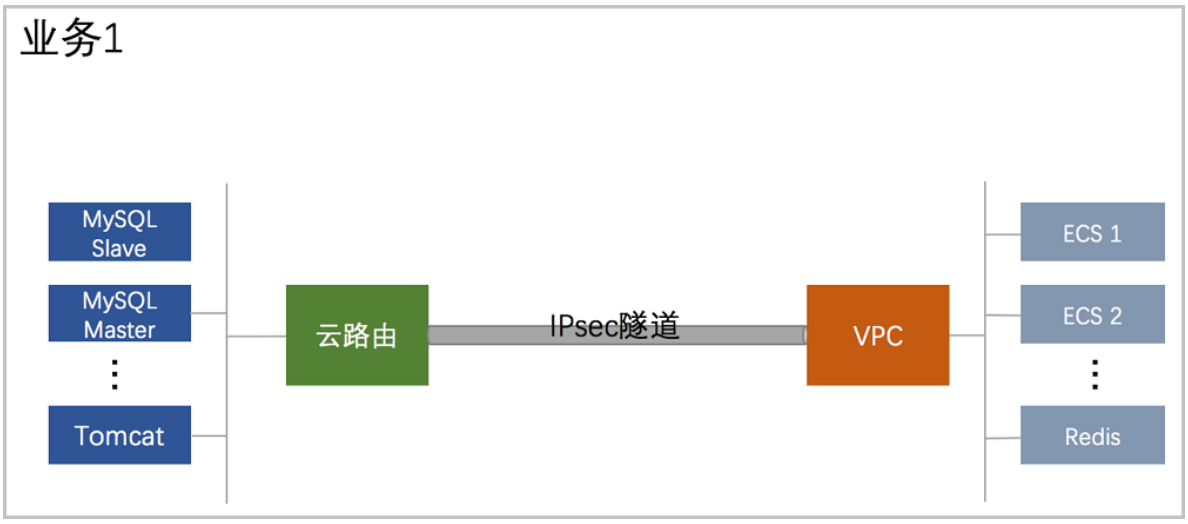


图 6: 阿里云高速通道

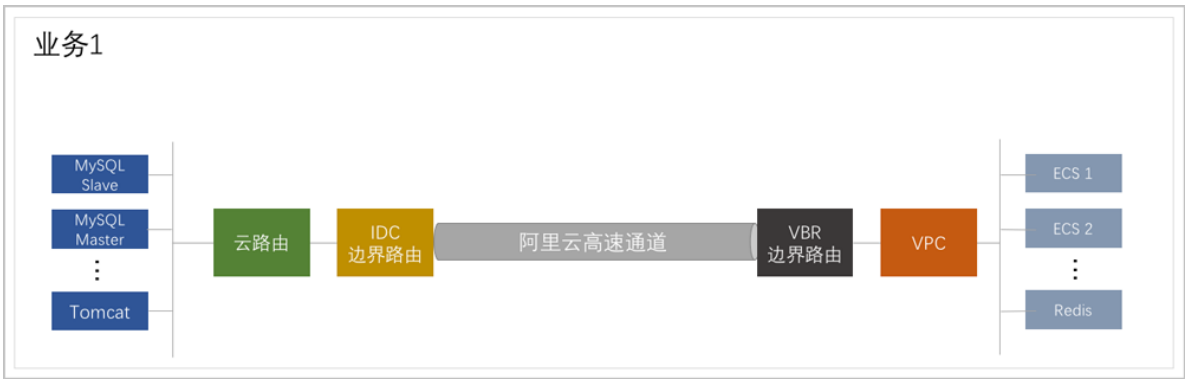
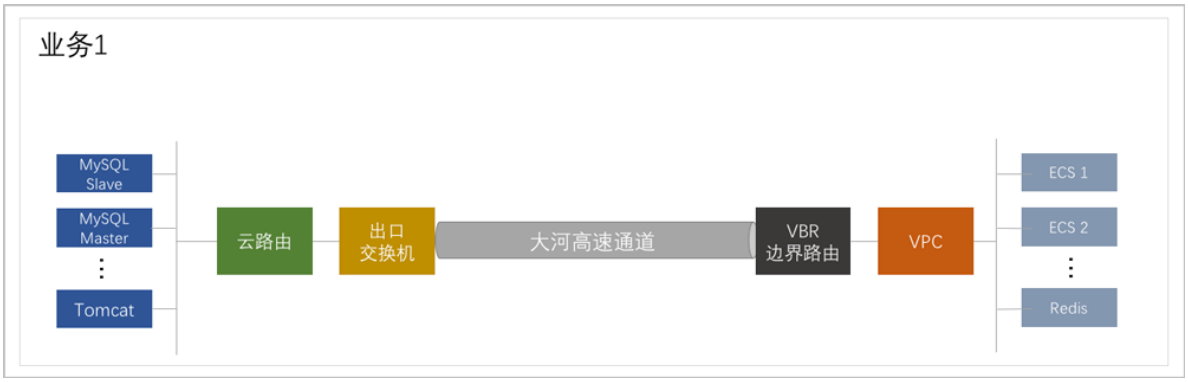


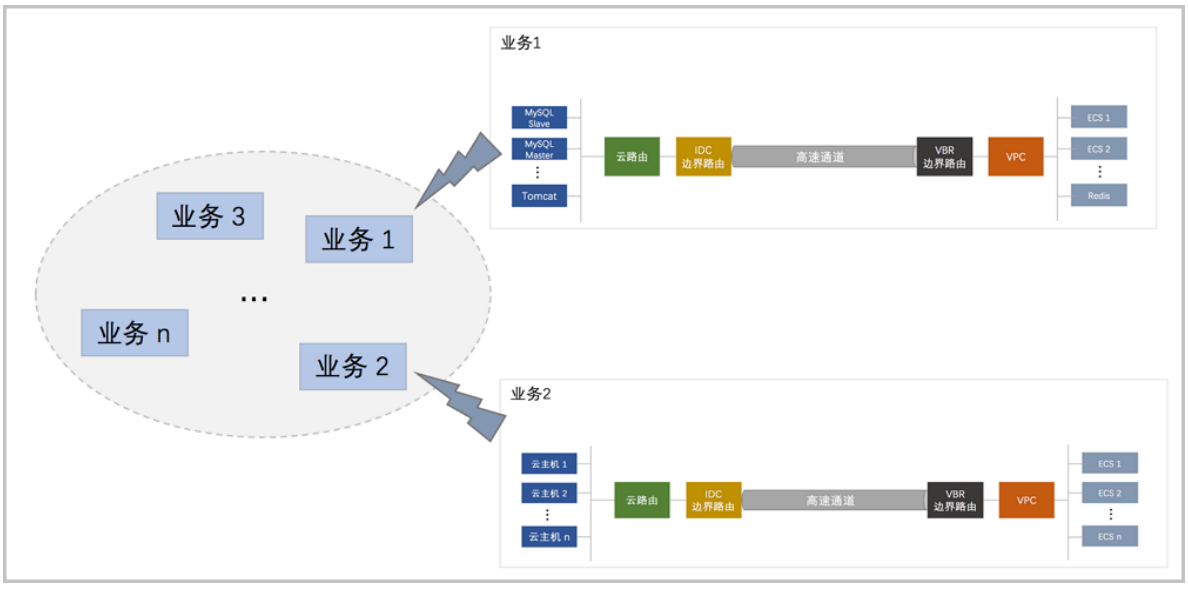
图 7: 大河高速通道



3. **资源管理**：

通过授权子账户，访问阿里云公有云账户里的资源，包括管理ECS、VBR、VPC和虚拟交换机等服务，如图 *8:* 资源管理所示：

图 8: 资源管理



4. **业务实现**：

   基于上述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。

ZStack之所以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私有云平台，因此并非简单的集成，而是把公有云的操作无缝集成到ZStack混合云平台中，让ZStack私有云的所有优点都输出到混合云上，为客户提供一个真正的统一管理视图。

2 准备工作

背景信息

使用ZStack的混合云功能需要进行以下相关准备。

操作步骤

1. 购买授权许可。

   购买ZStack混合云版本的License授权许可，并加载许可证书。

2. 请增添以下防火墙白名单，确保ZStack管理节点可访问阿里云API服务。

   - **.aliyuncs.com*

3. 创建阿里云账号。

   创建阿里云账号，可参考阿里云账号注册流程。

   若对阿里云企业主子帐号体系不熟悉，可参考阿里云身份管理，以下为推荐的实践步骤：

   1. 创建阿里云根账户；
   2. 使用根帐户登录阿里云控制台，在产品中选择 访问控制；
   3. 点击**用户管理** > **新建用户**，创建一个用户，例如 **zstack-user** ；
   4. 点击**群组管理** > **新建群组**，创建一个群组，例如 **zstack-developer-group**；
   5. 在**群组管理**中点击刚创建的群组，可见**群组详情**与**群组授权策略管理**两个子页，进入**群组授权策略管理**子页，点击**编辑授权策略**，添加至少如下权限：
      - AliyunRAMFullAccess
      - AliyunECSFullAccess
      - AliyunEIPFullAccess
      - AliyunVPCFullAccess
      - AliyunOSSFullAccess
      - AliyunExpressConnectFullAccess
      - AliyunVPNGatewayFullAccess
   6. 将刚才创建的用户加入创建的群组，点击**用户管理**，进入**用户详情**界面，点击**创建AccessKey**，请务必保存好创建出来的AccessKey（包括AccessKey ID和AccessKey Secret，简称AK），因为创建页面一旦关闭，AccessKey Secret将再不可见，只能重新生成。

注:

- ZStack不会记录您的账号信息，仅使用AccessKey信息，该键值对仅用于操作API。
- 建议严格遵守阿里云的RAM帐户访问体系，以提高安全性。
- 其中最重要的一条准则是**不要使用根账户的AK进行操作**。

4. 申请镜像导入白名单。

   申请**镜像导入白名单**，在阿里云控制台上，点击**工单** > **提交工单**，选择云服务器 ECS，点击**镜像咨询**，选择**创建工单**，在问题描述里填写类似“请帮忙添加镜像导入白名单，我们需要镜像导入服务”的工单信息，此工单需人工处理，需花费一定时间。

5. 开通并创建OSS Bucket。

   对象存储OSS承担了ZStack的云主机镜像到阿里云ECS云主机实例创建前的存储。ZStack使用对象存储OSS里面的Bcucket来上传镜像文件。

   注:

   - 使用ZStack本地镜像需要支持**在线修改密码**（Qemu-**guest-agent**）。
   - 镜像不支持EFI、LVM分区格式。
   - 镜像需要使用Linux或者Windows类型。

6. ZStack私有云云主机与阿里云ECS互通。

   如果希望ZStack私有云云主机与阿里云ECS互通，则需准备两边网络接入，接入有三种方式：

   1. 使用**IPsec VPN**方式，需购买阿里云VPN网关。

      在阿里云控制台上，选择**专有网络VPC** > **VPN网关**，点击**创建VPN网关**，选择地域、专有网络VPC、带宽规格等配置信息，并支付。

   2. 使用**物理专线**，需准备物理专线接入。

      在阿里云控制台上，选择**专有网络VPC** > **高速通道**，点击 **物理专线**，选择**申请专线接入**，或者请运营商接入**物理专线**。

   3. 使用**SD-WAN 大河专线**，需准备大河专线接入。

      SD-WAN 大河专线服务由大河云联提供。联系大河云联申请大河账号，获取大河提供的AccessKey。在混合云平台直接添加大河的AccessKey、同步大河端该账户下所有本地侧连接以及指定地域和可用区下的所有公有云侧连接。

7. 创建云主机。

使用云路由网络在ZStack私有云创建云主机，用于ZStack私有云云主机与阿里云ECS互通。

注:

- 目前ZStack混合云只支持专有网络VPC，不支持经典网络。
- 创建ECS时，只支持创建按量付费模式ECS。
- 支持接管包年包月付费的ECS。

3 混合云使用流程

使用ZStack混合云功能的基本流程如下：

1. **添加AccessKey信息**：使得混合云平台可在阿里云/阿里专有云/大河端调用对应账户的API，详情请见*AccessKey*。
2. **添加地域**：指定创建阿里云ECS时，选择对应的地域，详情请见添加地域。
3. **添加可用区**：指定创建阿里云ECS时，选择对应的可用区，详情请见添加可用区。
4. **添加Bucket**：使得本地的镜像可同步到阿里云的对象存储，并上传到对应地域作为镜像。如果全部使用阿里云系统镜像，暂时无须添加Bucket，详情请见添加*Bucket*。
5. **创建专有网络VPC**：指定创建阿里云ECS时使用的网络，详情请见创建专有网络*VPC*。
6. **创建安全组**：指定创建阿里云ECS时使用的安全组，详情请见创建安全组。
7. **创建阿里云ECS**：提供ECS云主机服务，详情请见创建*ECS*云主机。
8. **创建云路由网络**：用于创建私有云云主机，详情请见混合云互通实践。
9. **创建IPsec VPN/阿里云高速通道/大河高速通道**：实现本地私有云云主机和阿里云云主机互通，详情请见混合云互通实践。

4 AccessKey

阿里云AccessKey | 大河AccessKey

- 阿里云AccessKey：
  - 阿里云AccessKey（包括AccessKey ID和AccessKey Secret，简称AK），有阿里云（阿里公有云）和阿里专有云两种类型，是用于调用阿里云/阿里专有云API的唯一凭证。
  - 需在ZStack混合云平台添加对应账户的AK后，才能通过API获取阿里云/阿里专有云提供的云服务。

  注:
  - 如果不存在任何AK，操作助手会提示添加。
  - AK并不是用户的帐号，拥有AK并不代表拥有资源，资源属于阿里云帐号。
- 大河AccessKey：
  - 大河AccessKey（包括AccessKey ID和AccessKey Secret，简称AK）是用于调用大河云联API的唯一凭证。
  - 需在ZStack混合云平台添加对应账户的AK后，才能通过API获取大河云联提供的SD-WAN服务。

  注:
  - 如果不存在任何AK，操作助手会提示添加。
  - AK并不是用户的帐号，拥有AK并不代表拥有资源，资源属于大河云联帐号。

ZStack对阿里云/大河AccessKey进行以下操作：

- 查看AccessKey基本属性
- 添加AccessKey
- 删除AccessKey
- 将AccessKey设为默认
- 修改AccessKey名称和简介

查看AccessKey基本属性

ZStack支持查看AccessKey基本属性，例如通过阿里云AK可查看所属的阿里云根账户ID和子账户名称，方便用户管理。

在ZStack混合云主菜单，点击**AccessKey**按钮，进入**AccessKey**界面，如图 *9: 查看AccessKey基本属性*所示：

图 9: 查看AccessKey基本属性

添加AccessKey

以下分别介绍添加阿里云AccessKey、阿里专有云AccessKey、大河AccessKey。

- 添加阿里云AccessKey

  在**AccessKey**界面，进入**阿里云**子界面，点击**添加AccessKey**按钮，弹出**添加阿里云AccessKey**界面，可参考以下示例输入相应内容：

  - **阿里云**：选择添加阿里云AccessKey
  - **名称**：可自定义输入，用于标识此AccessKey
  - **简介**：可选项，可留空不填
  - **AccessKeyID**：输入阿里云账户的AccessKey ID，注意确保正确
  - **AccessKeySecret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确

  注: 首次添加AccessKey会自动设置为默认。

  如图 *10: 添加阿里云AccessKey*所示：

  图 10: 添加阿里云AccessKey

- 添加阿里专有云AccessKey

  在**AccessKey**界面，进入**阿里云**子界面，点击**添加AccessKey**按钮，弹出**添加阿里云AccessKey**界面，可参考以下示例输入相应内容：

  - **阿里专有云**：选择添加阿里专有云AccessKey
  - **名称**：可自定义输入，用于标识此AccessKey
  - **简介**：可选项，可留空不填
  - **类型**：选择阿里专有云AccessKey的类型，可选类型包括：AliyunEBS、AliyunNAS
  - **AccessKeyID**：输入阿里专有云账户的AccessKey ID，注意确保正确
  - **AccessKeySecret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确

  注: 首次添加AccessKey会自动设置为默认。

  如图 *11: 添加阿里专有云AccessKey界面*所示：

  图 11: 添加阿里专有云AccessKey界面

- 添加大河AccessKey

  在**AccessKey**界面，进入**大河**子界面，点击**添加AccessKey**按钮，弹出**添加大河AccessKey**界面，可参考以下示例输入相应内容：

  - **名称**：可自定义输入，用于标识此AccessKey
  - **简介**：可选项，可留空不填
  - **AccessKeyID**：输入大河账户的AccessKey ID，注意确保正确
  - **AccessKeySecret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确

  注: 首次添加AccessKey会自动设置为默认。

如图 *12: 添加大河AccessKey界面*所示：

图 12: 添加大河AccessKey界面

删除AccessKey

在**AccessKey**界面，选择某个AccessKey，点击 **更多操作** > **删除**，可删除AccessKey，如图 *13: 删除AccessKey*所示：

图 13: 删除AccessKey

将AccessKey设为默认

在**AccessKey** 界面，选择某个AccessKey，点击 **更多操作** > **设为默认**，将AccessKey设为默认，设为默认即设为使用状态。如图 *14: 将AccessKey设为默认*所示：

图 14: 将AccessKey设为默认

注:

当存在多个AccessKey的情况下，有且仅有一个AccessKey可被设置为默认，被设置为默认的AccessKey可使用此AK调用阿里云/阿里专有云/大河API来控制对应账户的云资源。

修改AccessKey名称和简介

在**AccessKey** 界面，选择某个AccessKey，展开其详情页，支持修改AccessKey的名称和简介。

5 同步数据

阿里云端数据同步

阿里云端同步数据是在添加数据中心相关资源后，对阿里云对应数据中心的资源同步到ZStack本地来管理。

- 同步数据需要存在数据中心的地域和可用区资源。如果不存在地域和可用区，操作助手会提示添加对应资源。
- 同步数据会同步当前AccessKey、已添加地域和可用区下的ECS、云盘、专有网络VPC、虚拟交换机、安全组、镜像、弹性公网IP、VPN、边界路由器、路由器接口等阿里云资源。
- 在首次添加地域和可用区时，ZStack会自动同步相关资源。
- 如果存在多个地域或多个可用区时，同步数据可能需要等待较长时间。

大河端数据同步

大河端同步数据是在添加数据中心相关资源后，对大河云联对应数据中心的资源同步到ZStack本地来管理。

- 同步数据需要存在数据中心的地域和可用区资源。如果不存在地域和可用区，操作助手会提示添加对应资源。
- 同步数据会同步当前AccessKey、大河端该账户下所有本地侧连接以及指定地域和可用区下的所有公有云侧连接。
- 在首次添加地域和可用区时，ZStack会自动同步相关资源。
- 如果存在多个地域或多个可用区时，同步数据可能需要等待较长时间。

如图 *15:* 同步数据所示：

图 15: 同步数据

6 操作向导

操作向导定义了快捷实现ZStack混合云相关复杂功能的业务逻辑。目前支持以下模块：

- 创建ECS云主机
- 创建阿里云VPN连接
- 创建阿里云高速通道
- 创建大河高速通道

在ZStack混合云导航栏，点击**产品与服务**按钮，进入**操作向导**界面，如图 *16:* 操作向导所示：

图 16: 操作向导

注: 在执行操作向导的过程中，如果需要的资源不存在，操作助手会提示相关资源的创建链接。

6.1 创建ECS云主机

操作步骤

1. 进入创建ECS云主机向导。

   在**操作向导**界面，点击**创建ECS云主机**按钮，可按照向导来创建ECS云主机，如图 *17:* 创建*ECS*云主机界面所示：

   图 17: 创建ECS云主机界面

2. 添加地域。

在**地域**界面，可参考以下示例输入相应内容：

- **地域**：选择地域
- **可用区**：选择可用区

注:

- 如果当前AK没有添加地域或可用区，操作助手会提示添加链接
- 添加完毕后，ZStack会同步该地域和可用区下的各种资源

如图 *18: 添加地域和可用区*所示，点击 **下一步**，进入添加镜像。

图 18: 添加地域和可用区

3. 添加镜像。

可选择阿里云系统镜像或者自定义镜像，如图 *19: 添加镜像*所示。

- 如果首次打算快速体验ECS云主机的创建，建议选择阿里云系统镜像。
- 自定义镜像，需要使用OSS对象存储，将本地镜像上传到阿里云，需等待较长时间。

点击 **下一步**，进入添加**专有网络VPC**。

图 19: 添加镜像

4. 添加专有网络VPC。

在**专有网络VPC**界面，可参考以下示例输入相应内容：

- **专有网络VPC**：选择专有网络VPC
- **虚拟交换机**：选择VPC下可用的虚拟交换机
- **安全组**：根据情况选择安全组

> **注:** 创建ECS时选择的安全组需保证相应的协议或端口允许ZStack私有云端内网通过。

> **注:** 以上任一资源如果不存在，操作助手会主动提示，可以按照提示添加所缺资源。

如图 *20: 专有网络VPC*所示，点击 **下一步**，进入创建云主机。

图 20: 专有网络VPC

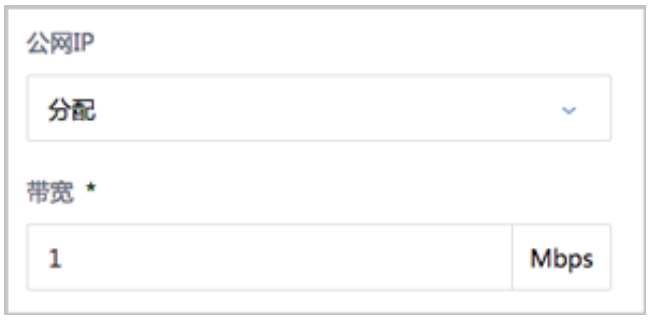
5. 创建云主机。

   在 **云主机**界面，可参考以下示例输入相应内容：

   - **名称**：设置ECS云主机名称
   - **简介**：可选项，可留空不填
   - **镜像**：此镜像已选择
   - **安全组**：此安全组已选择
   - **虚拟交换机**：此虚拟交换机已选择
   - **计算规格**：选择计算规格，计算规格为从阿里云同步的关于ECS云主机的CPU、内存等规格定义
   - **私网IP**：可选项，代表指定静态的私网IP地址
     - 如果指定，则需要确定不会与其他ECS IP冲突；
     - 在选择虚拟交换机后，ZStack列出了当前交换机的CIDR和可用的IP数量，用于提示。
   - **公网IP**：可选项，可选择是否给此ECS云主机分配一个公网IP，默认**不分配**

     注: 如果选择**分配**，需设置ECS云主机的网络带宽，如图 *21: 分配公网IP*所示：

     图 21: 分配公网IP



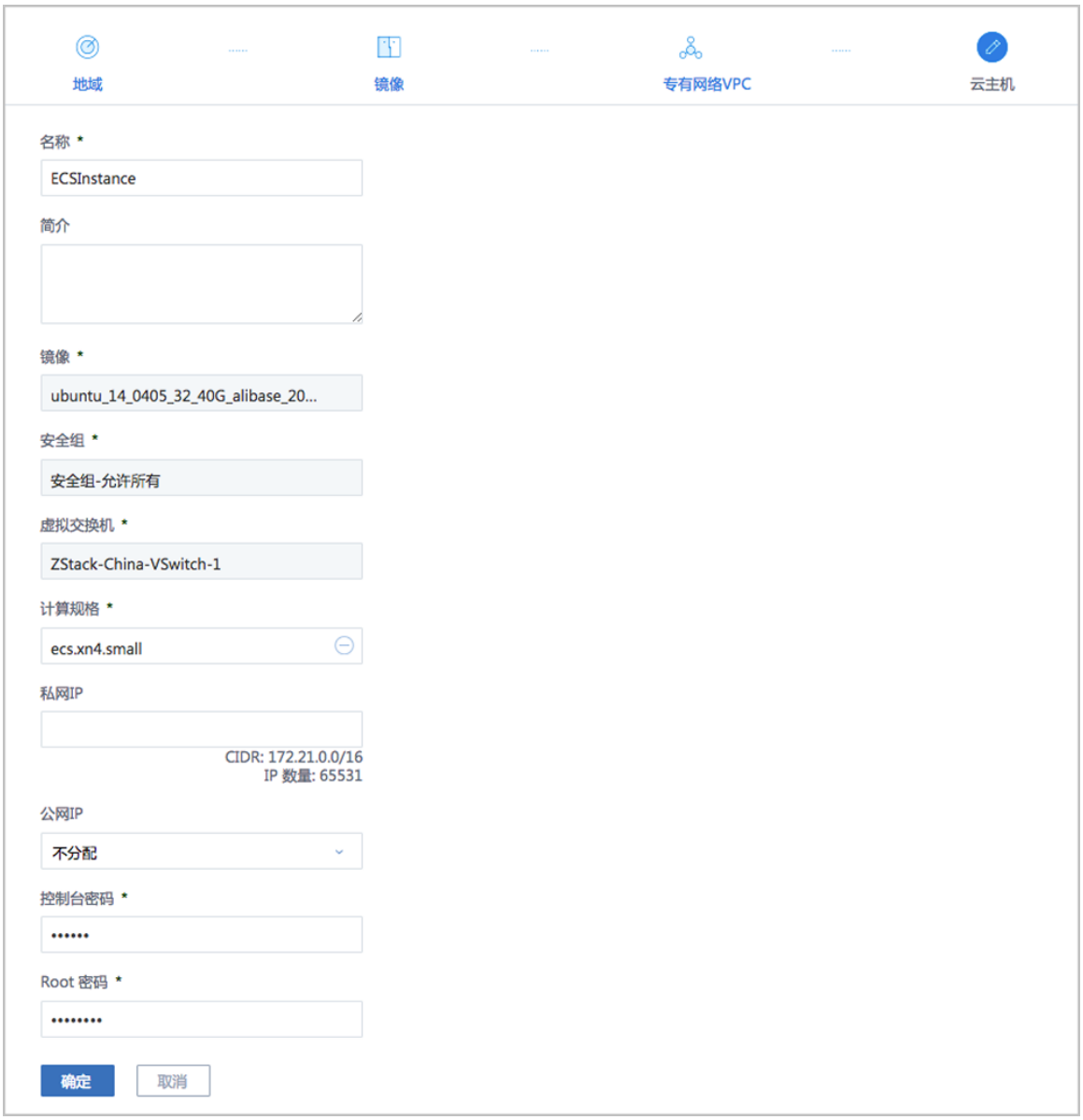
- **控制台密码**：请输入6个字符，包含数字或字母
- **Root密码**：请输入8到30位字符，且同时三种以上的大写、小写字母、数字和特殊字符

注:

Linux云主机的默认指定用户名为root，Windows默认指定的用户名是administrator，在打开控制台后，需输入正确的用户名和此处指定的密码登录ECS云主机。

如图 *22: ECS云主机配置*所示，点击 **确定**，创建ECS云主机。

图 22: ECS云主机配置



6.2 创建阿里云VPN连接

背景信息

IPsec VPN：使用企业本地的公网IP和阿里云提供的VPN网关进行IPsec VPN互通。

操作步骤

1. 进入创建阿里云VPN连接向导。

   在**操作向导**界面，点击**创建阿里云VPN连接**按钮，可按照向导来创建阿里云VPN连接，如图 *23: 创建阿里云VPN连接*所示：

   图 23: 创建阿里云VPN连接

2. 选择阿里云网络。

在**阿里云网络**界面，可参照以下示例选择相应内容：

- **VPN网关**：选择已购买的VPN网关

> **注:** 如果选择的地域没有可用的VPN网关，目前必须通过阿里云控制台直接购买。

如图 *24:* 选择阿里云网络所示，点击 **下一步**，进入连接配置。

图 24: 选择阿里云网络

3. 连接配置。

在**连接配置**界面，可参考以下示例输入相应内容：

- **名称**：设置VPN连接名称
- **简介**：可选项，可留空不填
- **预共享密钥**：建议设置强度高的密钥

- **云路由器**：选择创建本地云主机时自动创建的云路由器
- **公有网络**：选择云路由挂载的公有网络，如果云路由仅挂载一个公网则会默认选中该公网
- **IP地址**：可选项，表示所选择公有网络下可用的IP地址，此IP地址应为互联网公网IP地址。如果留空，系统会自动选择一个可用IP地址
- **私有网络**：选择云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网
- **高级选项**：默认选项为可连通的选项，不建议修改
  - **SA生存周期（秒）**：86400（默认）
  - **IPsec 加密算法**：3des（默认）
  - **IPsec 认证算法**：sha1（默认）
  - **IPsec DH分组**：group2（默认）
  - **IKE 版本**：ikev1（默认）
  - **IKE 协商模式**：main（默认）
  - **IKE 加密算法**：3des（默认）
  - **IKE 认证算法**：sha1（默认）
  - **IKE DH分组**：group2（默认）

如图 *25:* 连接配置所示，点击**确定**，将自动创建IPsec VPN连接。

图 25: 连接配置

4. 互通验证。

登录本地云主机，检查是否能够ping通ECS云主机。然后再登录ECS云主机，检查是否能够ping通本地云主机。

注:

如果步骤3中VPN连接失败，或者步骤4中互通验证失败，打算重新配置，需检查以下资源：

- 本地用于创建IPsec连接的虚拟IP是否已经占用，如果已使用，则需删除此虚拟IP；
- 阿里云VPN连接是否已经存在，如果存在，则需要删除，删除阿里云VPN连接同时需删除远端阿里云资源；
- 阿里云VPN用户网关是否已存在重复的IP，如果存在，则需要删除，删除需同时删除远程阿里云资源；
- VPC的虚拟路由器下是否存在已经指向ZStack私有云对应内网的路由条目，如果存在，则需要删除。

后续操作

至此，若验证成功，则IPsec VPN连接创建成功。

IPsec VPN详细部署教程请参考*IPsec VPN实践*。

6.3 阿里云高速通道

阿里云高速通道：使用物理专线配置阿里云高速通道以实现网络互通。

在创建阿里云高速通道时，需提前在CPE IP端，ZStack私有云端和阿里云公有云端进行网络配置。

CPE IP端配置

在创建阿里云高速通道时，需要准备物理专线，由运营商创建边界路由器和配置路由器接口。

配置完成后，可获取如下信息：

- 边界路由器：CPE客户端设备到VPC下的虚拟路由器之间的路由器；
- 边界路由器接口：边界路由器的两侧接口，分别为ZStack侧和阿里云侧；
- VPC路由器接口：VPC虚拟路由器的接口；
- CPE IP：运营商提供的CPE设备IP地址。

ZStack私有云端配置

在对ZStack私有云端进行配置之前，需先进行网络规划，具体如下：

- 私有网络段：私有网络段使云路由管理ZStack私有云云主机；
- 管理网络段：管理网络段使管理节点管理云路由；
- 公有网络段：公有网络段绑定云路由，使云路由可以访问互联网；
- 物理专线网络段：云路由至CPE IP再连通阿里云的网络。

注: 公有网络段与管理网络段可为同一网络段。

配置网络段成功后，便可进行ZStack私有云端配置：

1. 创建L2私有网络
2. 创建L3私有网络（云路由方式）
3. 创建L2管理网络
4. 创建L3管理网络（公有网络）
5. 创建L2公有网络
6. 创建L3公有网络（公有网络）
7. 创建ZStack私有云云主机
8. 创建云路由（将云路由绑定至公有网络）
9. 创建L2物理专线网络
10. 创建L3物理专线网络（公有网络）
11. 加载物理专线网络到云路由器

注: 如何配置网络，详情可参考*ZStack*官网产品教程。

ZStack私有云端配置完成后，需在CPE设备处配置双向路由。

阿里云公有云端配置

在进行阿里云高速通道配置时，需在阿里云端拥有以下环境：

- 专有网络VPC
- VPC下交换机
- ECS云主机实例

注: 详情可参考准备工作。

拥有以上环境后，需进行以下配置：

- 使用对应的VPC下的虚拟交换机创建ECS实例

注: 详情可参考阿里云文档。

ZStack混合云端配置

上述配置完成后需进行ZStack混合云端配置，配置过程如下：

1. 添加AccessKey：添加AccessKey，详情可参考*AccessKey*；
2. 添加地域：添加VPC所在地域，详情可参考地域管理；
3. 添加可用区：添加VPC所在可用区，详情可参考可用区；
4. 点击**同步数据**按钮同步数据。

至此，阿里云高速通道所有前提环境已部署完毕。

阿里云高速通道详细部署教程请参考阿里云高速通道实践。

下面将介绍通过操作向导创建阿里云高速通道的步骤。

6.3.1 创建阿里云高速通道

操作步骤

1. 进入创建阿里云高速通道向导。

   在**操作向导**界面，点击**创建阿里云高速通道**按钮，可按照向导来创建阿里云高速通道，如图 *26: 创建阿里云高速通道*所示：

   图 26: 创建阿里云高速通道

2. 配置ZStack网络。

   在**ZStack网络**界面，可参照以下示例输入相应内容：

   - **云路由器**：选择本地云路由器
   - **公有网络**：选择可以连接本地至边界路由器接口的专线网络
   - **私有网络**：选择本地创建的私有网络（云路由网络）

如图 *27: ZStack网络界面*所示，点击 **下一步**，进入配置阿里云网络。

图 27: ZStack网络界面

3. 配置阿里云网络。

   在**阿里云网络**界面，可参考以下示例输入相应内容：

   - **专有网络VPC**：选择专有网络VPC
   - **边界路由器**：选择边界路由器，目前由运营商创建并配置路由
   - **CPE IP（运营商）**：运营商提供物理专线接入本地数据中心的客户端设备IP地址

   如图 *28: 配置阿里云网络*所示，点击**确定**，创建阿里云高速通道。

   图 28: 配置阿里云网络

创建高速通道过程中，ZStack将自动配置以下4条路由：

- VPC自定义路由1：目的地址为*ZStack*私有网络段，下一跳为VPC虚拟路由器接口；
- 边界路由器自定义路由1：目的地址为*ZStack*私有网络段，下一跳为边界路由器ZStack私有云侧的路由器接口；
- 边界路由器自定义路由2：目的地址为*ECS VPC*网络段，下一跳为边界路由器阿里云侧的路由器接口；
- 云路由自定义路由1：目的地址为*ECS VPC*网络段，下一跳为客户端CPE设备的IP地址。

4. 在CPE设备处配置双向路由。

   CPE设备的两条路由条目，应由客户自行创建：

   - 设置CPE自定义路由1：目的地址为*ZStack*私有网络段，下一跳为云路由器的物理专线IP；
   - 设置CPE自定义路由2：目的地址为*ECS VPC*网络段，下一跳为专线的地址。

5. 查看阿里云高速通道拓扑图。

   在**专有网络VPC**界面，点击相应的VPC，进入**专有网络VPC**详情页，点击**拓扑图**，进入**拓扑图**页面，可查看网络拓扑，如图 *29:* 拓扑图所示：

   图 29: 拓扑图

6. 互通验证。

   登录本地云主机，检查是否能够ping通ECS云主机。然后再登录ECS云主机，检查是否能够ping通本地云主机。

后续操作

至此，若验证成功，则阿里云高速通道创建成功，ZStack私有云到阿里云的网络可实现互通。

6.4 大河高速通道

大河高速通道：使用大河云联提供的SD-WAN服务配置大河高速通道以实现网络互通。

本文档针对**无盒子**场景，即：本地数据中心已提供大河SD-WAN专线服务。

在创建大河高速通道时，需提前联系大河云联申请大河账号，并在本地出口交换机端、ZStack私有云端和阿里云公有云端进行网络配置。

申请大河账号

需提前联系大河云联申请大河账号，获取大河提供的AccessKey。具体申请方法请咨询大河云联官方技术支持。

本地出口交换机端配置

需提前在本地出口交换机上配置二层VLAN网络，例如：VLAN ID为700。

ZStack私有云端配置

在对ZStack私有云端进行配置之前，需先进行网络规划，具体如下：

- 私有网络段：私有网络段使云路由管理ZStack私有云云主机。
- 管理网络段：管理网络段使管理节点管理云路由。

  注: 出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。

- 公有网络段：需与本地出口交换机二层互通，例如：VLAN ID为700；使用提前准备好的一对互联地址【*10.255.255.221*（ZStack私有云端）和*10.255.255.222*（阿里云端）】配置三层网络，例如：IP地址段为*10.255.255.221~10.255.255.221*，子网掩码为*255.255.255.252*，网关为*10.255.255.222*。此处公有网络并非传统意义上的公有网络，仅用于连通大河专线。

配置网络段成功后，便可进行ZStack私有云端配置：

1. 创建L2私有网络
2. 创建L3私有网络（云路由方式）
3. 需关闭L3私有网络的SNAT服务
4. 创建L2管理网络
5. 创建L3管理网络（独立的管理网络）
6. 创建L2公有网络
7. 创建L3公有网络（公有网络）
8. 创建ZStack私有云云主机

阿里云公有云端配置

在进行大河高速通道配置时，需在阿里云端拥有以下环境：

- 专有网络VPC
- VPC下交换机
- ECS云主机实例

注: 详情可参考准备工作。

拥有以上环境后，需进行以下配置：

- 使用对应的VPC下的虚拟交换机创建ECS实例

  注: 详情可参考阿里云文档。

ZStack混合云端配置

上述配置完成后需进行ZStack混合云端配置，配置过程如下：

1. 添加阿里云AccessKey以及大河AccessKey，详情可参考*AccessKey*；
2. 添加地域：添加阿里云VPC所在地域，详情可参考地域管理；
3. 添加可用区：添加阿里云VPC所在可用区，详情可参考可用区；
4. 点击**同步数据**按钮同步数据。

至此，大河高速通道所有前提环境已部署完毕。

大河高速通道详细部署教程请参考大河高速通道实践。

下面将介绍通过操作向导创建大河高速通道的步骤。

6.4.1 创建大河高速通道

操作步骤

1. 进入创建大河高速通道向导。

   在**操作向导**界面，点击**创建大河高速通道**按钮，可按照向导来创建大河高速通道，如图 *30:* 创建大河高速通道所示：

   图 30: 创建大河高速通道

2. 配置大河专线。

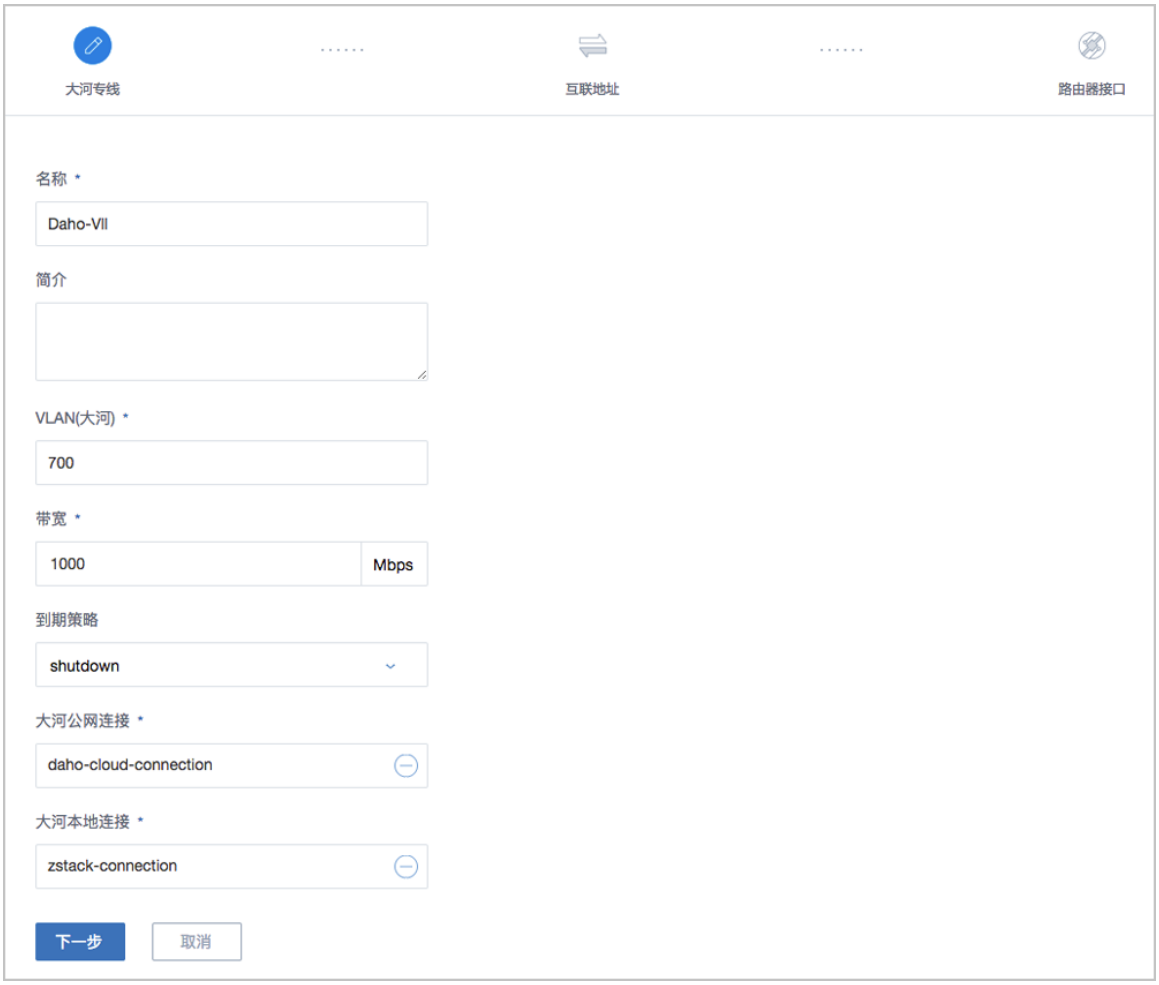
   在**大河专线**界面，可参考以下示例输入相应内容：

   - **名称**：设置大河专线名称
   - **简介**：可选项，可留空不填
   - **VLAN(大河)**：设置VLAN ID号，需与本地出口交换机二层互通

- **带宽**：设置大河专线的带宽，单位为Mbps
- **到期策略**：可选项，所购买的大河专线服务到期后是否续期，有两种到期策略可选：shutdown（服务到期后停止续期）、renewal（服务到期后自动续期）
- **大河公网连接**：选择大河端提供的公有云侧连接
- **大河本地连接**：选择大河端提供的本地侧连接

如图 *31:* 配置大河专线所示，点击**下一步**，配置互联地址。

图 31: 配置大河专线



大河专线配置完成同时，大河在阿里云端自动购买创建一个边界路由器，以及边界路由器在ZStack侧的路由器接口（VBR接口1），该边界路由器以及路由器接口自动同步至本地。

3. 配置互联地址。

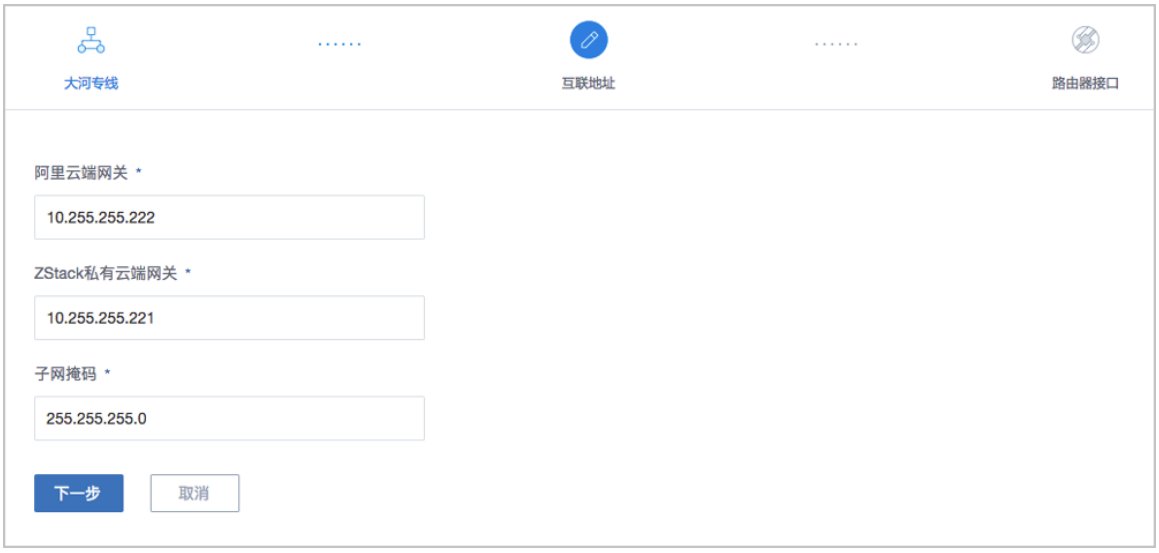
将已准备的一对互联地址：*10.255.255.221*（ZStack私有云端）和*10.255.255.222*（阿里云端）输入边界路由器。

在**互联地址**界面，可参考以下示例输入相应内容：

- **阿里云端网关**：输入*10.255.255.222*到边界路由器，作为阿里云端网关
- **ZStack私有云端网关**：输入*10.255.255.221*到边界路由器，作为ZStack私有云端网关
- **子网掩码**：设置边界路由器的子网掩码，使阿里云端网关和ZStack私有云端网关可以互通

如图 *32: 配置互联地址*所示，点击**下一步**，配置路由器接口。

图 32: 配置互联地址



4. 配置路由器接口。

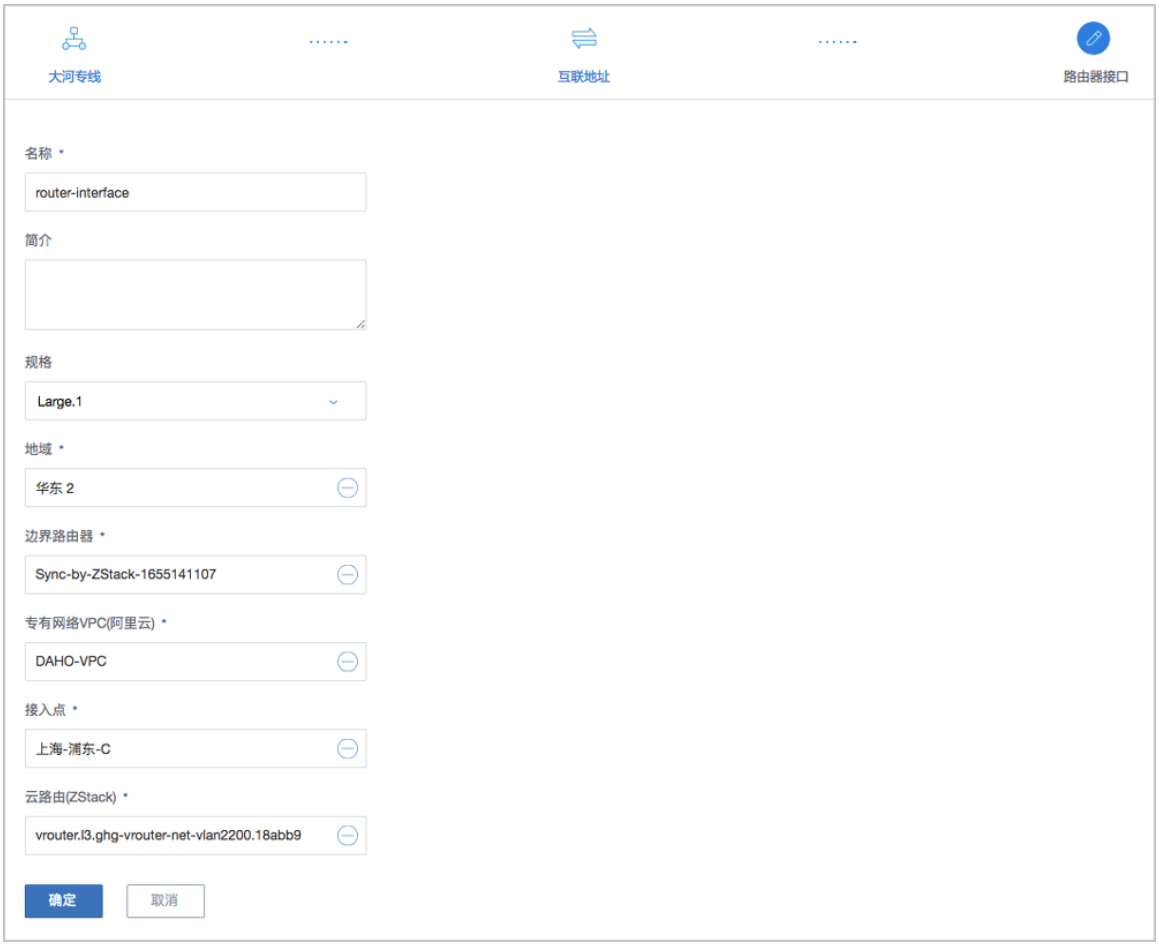
   配置一对路由器接口，即：边界路由器在阿里云侧的路由器接口（VBR接口2），以及相应的阿里云VPC虚拟路由器接口。

   在**路由器接口**界面，可参考以下示例输入相应内容：

   - **名称**：设置这一对路由器接口名称
   - **简介**：可选项，可留空不填
   - **规格**：可选项，设置边界路由器在阿里云侧路由器接口（VBR接口2）的带宽规格
   - **地域**：选择相应的阿里云VPC虚拟路由器所在地域
   - **边界路由器**：选择相应的边界路由器
   - **专有网络VPC(阿里云)**：选择相应的阿里云VPC
   - **接入点**：选择边界路由器在阿里云侧路由器接口（VBR接口2）的接入点
   - **云路由(ZStack)**：选择本地云路由器

如图 *33:* 配置路由器接口所示，点击**确定**，创建大河高速通道。

图 33: 配置路由器接口



创建大河高速通道过程中，ZStack将自动配置以下4条路由：

- VPC虚拟路由器自定义路由：目的地址为ZStack私有网络段，下一跳为VPC虚拟路由器接口；
- 边界路由器自定义路由1：目的地址为ZStack私有网络段，下一跳为边界路由器ZStack侧的路由器接口（VBR接口1）；
- 边界路由器自定义路由2：目的地址为ECS VPC网络段，下一跳为边界路由器阿里云侧的路由器接口（VBR接口2）；
- 本地云路由自定义路由：目的地址为ECS VPC网络端，下一跳为阿里云端网关*10.255.255.222*。

5. 互通验证。

登录本地云主机，检查是否能够ping通ECS云主机。然后再登录ECS云主机，检查是否能够ping通本地云主机。

后续操作

至此，若验证成功，则大河高速通道创建成功，ZStack私有云到阿里云的网络可实现互通。

7 产品

ZStack混合云产品涉及了以下阿里云提供的云计算产品：

- ECS云主机
- 云盘
- 镜像
- 安全组
- 专有网络VPC
- 弹性公网IP
- IPsec VPN
- 高速通道
- 阿里云NAS

7.1 ECS云主机

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

混合云云主机可在ZStack混合云界面创建，也可在阿里云端创建再进行同步。

ECS云主机支持以下操作：

- 创建单个ECS云主机
- 批量创建ECS云主机
- 启动、停止ECS云主机
- 重启ECS云主机
- 打开控制台
- 设置ECS控制台密码
- 修改系统用户密码
- 删除ECS云主机
- 修改ECS云主机名称和简介
- 加载云盘
- 卸载云盘

创建单个ECS云主机

1. 在ZStack混合云主菜单，点击**产品** > **ECS云主机**，进入**ECS云主机**界面，如图 *34: ECS*云主机界面所示：

   图 34: ECS云主机界面

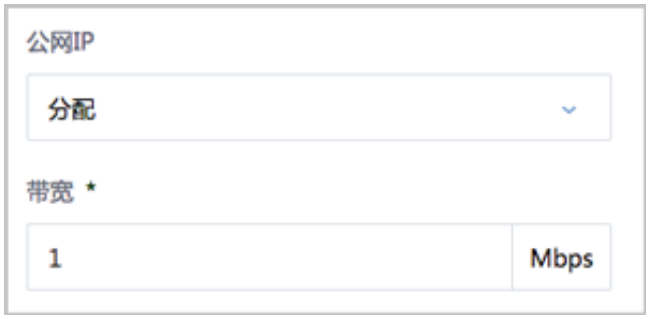
2. 点击**创建ECS云主机**按钮，弹出**创建ECS云主机**界面，可参考以下示例输入相应内容：

- **添加方式**：单个
- **名称**：设置ECS名称
- **简介**：可选项，可留空不填
- **镜像**：此镜像只支持阿里云端镜像，镜像类型包括：阿里云系统镜像和自定义镜像
- **安全组**：指定创建ECS时需要的安全组

  注: 创建ECS时选择的安全组需保证相应的协议或端口允许ZStack私有云端内网通过。
- **虚拟交换机**：指定创建ECS时需要的虚拟交换机
- **计算规格**：选择计算规格，计算规格为从阿里云同步的关于ECS云主机的CPU、内存等规格定义
- **私网IP**：可选项，代表指定静态的私网IP地址
  - 如果指定，则需确定不会与其他ECS IP冲突；
  - 选择交换机后，ZStack列出了当前交换机的CIDR和可用的IP数量，用于提示。
- **公网IP**：可选项，可选择是否给此ECS云主机分配一个公网IP，默认**不分配**

  注: 如果选择**分配**，需设置ECS云主机的网络带宽，如图 *35: 分配公网IP*所示：

  图 35: 分配公网IP



- **控制台密码**：请输入6个字符，包含数字或字母
- **Root密码**：请输入8到30位字符，且同时三种以上的大写、小写字母、数字和特殊字符

> **注:**
>
> Linux云主机的默认指定用户名为root，Windows默认指定的用户名是administrator，在打开控制台后，需输入正确的用户名和此处指定的密码登录ECS云主机。

如图 *36:* 创建单个*ECS*云主机所示：

图 36: 创建单个ECS云主机

注:

- 计算规格只能从阿里云同步

- 若自定义镜像不符合阿里云镜像规范，则使用该自定义镜像创建的ECS云主机无法启动

批量创建ECS云主机

ZStack支持用户批量创建云主机。

在**创建ECS云主机**界面，可参考以下示例输入相应内容：

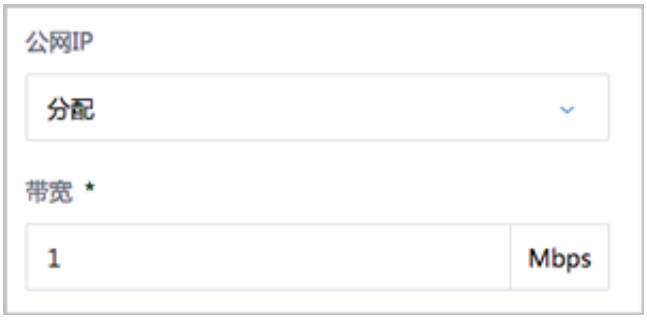
- **添加方式**：多个
- **创建数量**：填写需创建的ECS数量
- **名称**：设置ECS名称
- **简介**：可选项，可留空不填
- **镜像**：此镜像只支持阿里云端镜像，镜像类型包括：阿里云系统镜像和自定义镜像
- **安全组**：指定创建ECS时需要的安全组

  注: 创建ECS时选择的安全组需保证相应的协议或端口允许ZStack私有云端内网通过。

- **虚拟交换机**：指定创建ECS时需要的虚拟交换机
- **计算规格**：选择计算规格，计算规格为从阿里云同步的关于ECS云主机的CPU、内存等规格定义
- **私网IP**：可选项，代表指定静态的私网IP地址
  - 如果指定，则需确定不会与其他ECS IP冲突；
  - 选择交换机后，ZStack列出了当前交换机的CIDR和可用的IP数量，用于提示。
- **公网IP**：可选项，可选择是否给此ECS云主机分配一个公网IP，默认**不分配**

  注: 如果选择**分配**，需设置ECS云主机的网络带宽，如图 *37: 分配公网IP*所示：

  图 37: 分配公网IP



- **控制台密码**：请输入6个字符，包含数字或字母

- **Root密码**：请输入8到30位字符，且同时三种以上的大写、小写字母、数字和特殊字符

  注: Linux云主机的默认指定用户名为root，Windows默认指定的用户名是administrator，在打开控制台后，需输入正确的用户名和此处指定的密码登录ECS云主机。

如图 *38:* 批量创建*ECS*云主机所示：

图 38: 批量创建ECS云主机

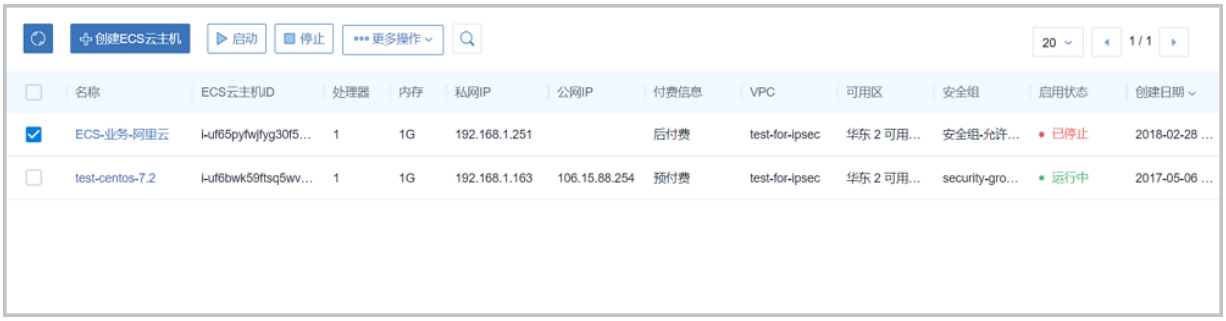

确定
取消
创建ECS云主机
添加方式
单个
多个
创建数量 *
3
名称 *
ECS云主机
简介
镜像 *
ubuntu_14_0405_64_20G_alibase_...
安全组 *
安全组-允许所有
虚拟交换机 *
ecs-for-vpn
计算规格 *
ecs.xn4.small
私网IP
CIDR: 192.168.1.0/24
IP 数量: 246
公网IP
不分配
控制台密码 *
••••••
系统用户密码 *
••••••••••

注: 批量创建ECS云主机时，云主机数量不能超过20个。

启动、停止ECS云主机

在**ECS云主机**界面，选择某一ECS云主机点击 **停止**或**启动**，可管理该ECS云主机实例，如图 *39: 停止或启动ECS云主机*所示：

图 39: 停止或启动ECS云主机



重启云主机

在**ECS云主机**界面，选择某一运行中的ECS云主机，点击 **更多操作** > **重启**，可重启该ECS云主机实例，如图 *40: 重启ECS云主机*所示：

图 40: 重启ECS云主机

打开控制台

在**ECS云主机**界面，选择某一ECS云主机，点击**更多操作** > **打开控制台**，可打开该ECS云主机控制台。

打开控制台后，需输入以下内容才能登录ECS云主机：

1. 控制台密码：输入控制台密码后，点击**Connect**，以连接ECS控制台；

2. 用户名密码：输入创建ECS时的密码。

注:

Linux云主机的默认指定用户名为root，Windows默认指定的用户名是administrator，打开控制台后，需输入正确的用户名和创建ECS时指定的密码登录ECS云主机。

如图 *41:* 输入控制台密码和图 *42:* 输入用户名密码登录*ECS*云主机所示：

图 41: 输入控制台密码

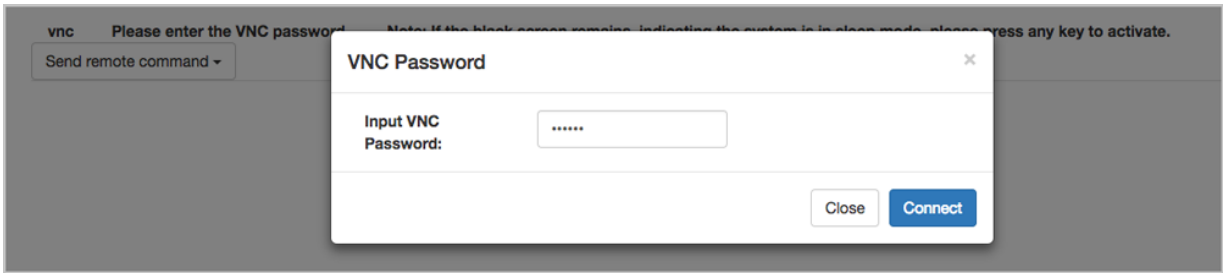
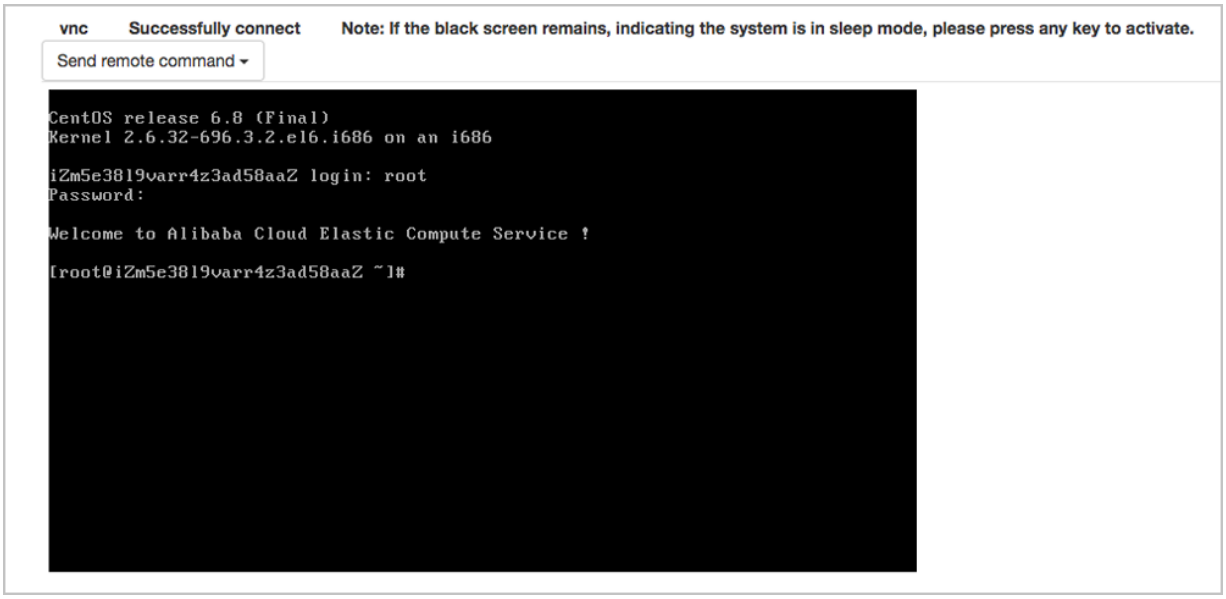


图 42: 输入用户名密码登录ECS云主机



设置控制台密码

在**ECS云主机**界面，选择某一ECS云主机，点击**更多操作** > **设置控制台密码**，可重新设置该ECS云主机控制台密码。修改控制台密码，无须重启，即刻生效。

注: ECS控制台密码为6位字符，包含数字或字母。

如图 *43:* 设置控制台密码所示：

图 43: 设置控制台密码

设置系统用户密码

在**ECS云主机**界面，选择某一ECS云主机，点击 **更多操作** > **设置系统用户密码**，可重新设置该ECS云主机系统用户密码。修改系统用户密码，须重启后生效。

注:

- 修改系统用户密码需重启后生效
- Linux 默认系统用户为：root
- Windows 默认系统用户为：administrator

如图 *44:* 修改系统用户密码所示：

图 44: 修改系统用户密码

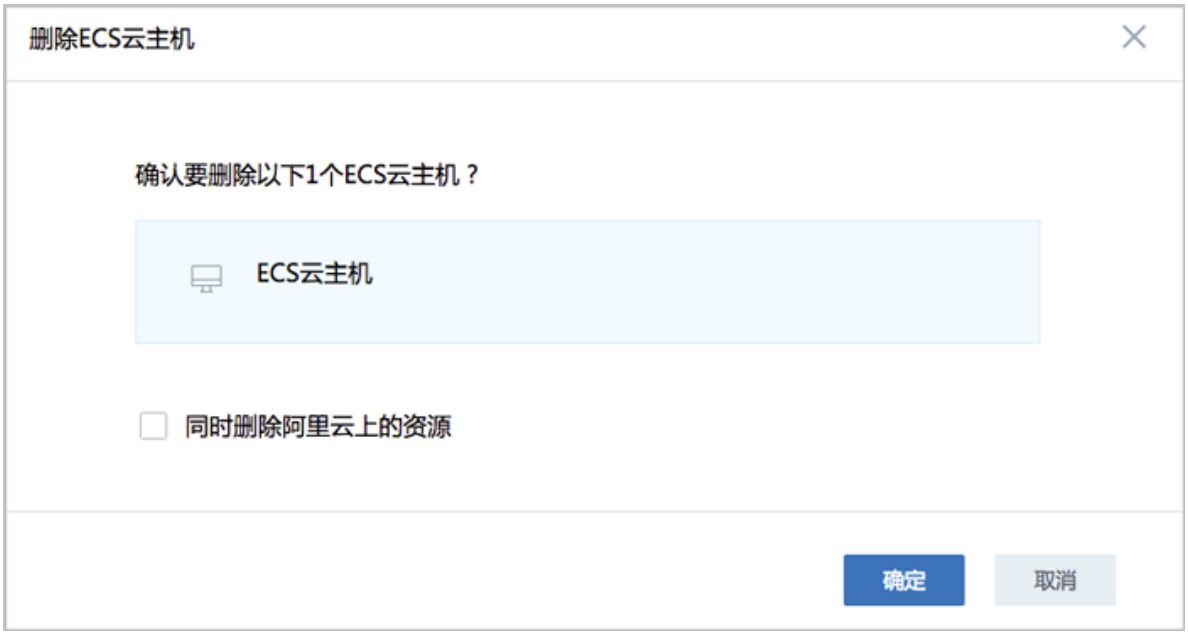
删除ECS云主机

1. 在**ECS云主机**界面，选择要删除的ECS云主机，点击 **更多操作** > **删除**，可删除所选ECS云主机，如图 *45: 删除ECS云主机*所示：

图 45: 删除ECS云主机

2. 弹出**删除ECS云主机**确认窗口，如图 *46: 删除ECS云主机确认窗口*所示：

图 46: 删除ECS云主机确认窗口



注:

- 默认只删除本地记录，如需同时删除阿里云上的ECS云主机，请勾选**同时删除阿里云上的资源**；
- 对于已挂载到ECS云主机的云盘（数据盘），若开启**随主机删除**的开关，删除ECS云主机时，该云盘随ECS云主机一起删除。

修改ECS云主机名称、简介

在**ECS云主机**界面，点击某一ECS云主机，展开详情页，点击**基本属性**，进入**基本属性**子页面，可修改ECS云主机的名称和简介。

加载云盘

在**ECS云主机**界面，点击某一ECS云主机，展开详情页，点击**云盘**，进入**云盘**子页面，点击**操作 > 加载**，可加载云盘（数据盘）到ECS云主机。

如图 *47:* 加载云盘所示：

图 47: 加载云盘

卸载云盘

在ECS云主机详情页，点击**云盘**，进入**云盘**子页面，选择需要卸载的云盘（数据盘），点击**操作 > 卸载**，可将该云盘从ECS云主机卸载。

如图 *48:* 卸载云盘所示：

图 48: 卸载云盘

7.2 云盘

ZStack混合云平台支持阿里云端云盘资源的管理。

目前支持的云盘种类包括：高效云盘和SSD云盘。

1. 高效云盘：采用固态硬盘与机械硬盘的混合介质作为存储介质。

   适用场景：

   - MySQL、SQL Server、PostgreSQL等中小型关系数据库应用
   - 对数据可靠性要求高、中度性能要求的中大型开发测试应用

2. SSD云盘：利用分布式三副本机制，能够提供稳定的高随机 I/O、高数据可靠性的高性能存储

   适用场景：

   - PostgreSQL、MySQL、Oracle、SQL Server等中大型关系数据库应用
   - 对数据可靠性要求高的中大型开发测试环境

云盘属性分为：系统盘和数据盘。系统盘作为ECS云主机必备的一部分，云盘管理主要涉及**数据盘**。

云盘支持以下操作：

- 创建云盘：创建一个阿里云端的云盘（数据盘）
- 同步云盘：同步阿里云端云盘到本地
- 加载云盘：加载云盘到ECS云主机（数据盘）
- 卸载云盘：从ECS云主机卸载云盘（数据盘）
- 删除云盘：默认只删除本地记录，支持同时删除阿里云端的云盘（数据盘）
- 修改云盘名称和简介

创建云盘

云盘（数据盘）可在ZStack混合云界面创建，也可在阿里云端创建再进行同步。

1. 在ZStack混合云主菜单，点击**产品** > **云盘**，进入**云盘**界面，如图 *49:* 云盘界面所示：

   图 49: 云盘界面

2. 点击**创建云盘**按钮，弹出**创建云盘**界面，可参考以下示例输入相应内容：

   - **可用区**：选择云盘所属可用区
   - **名称**：设置云盘名称
   - **简介**：可选项，可留空不填
   - **容量**：按需设置云盘容量，单位为G
   - **云盘种类**：目前支持高效云盘和SSD云盘

   如图 *50:* 创建云盘所示：

   图 50: 创建云盘

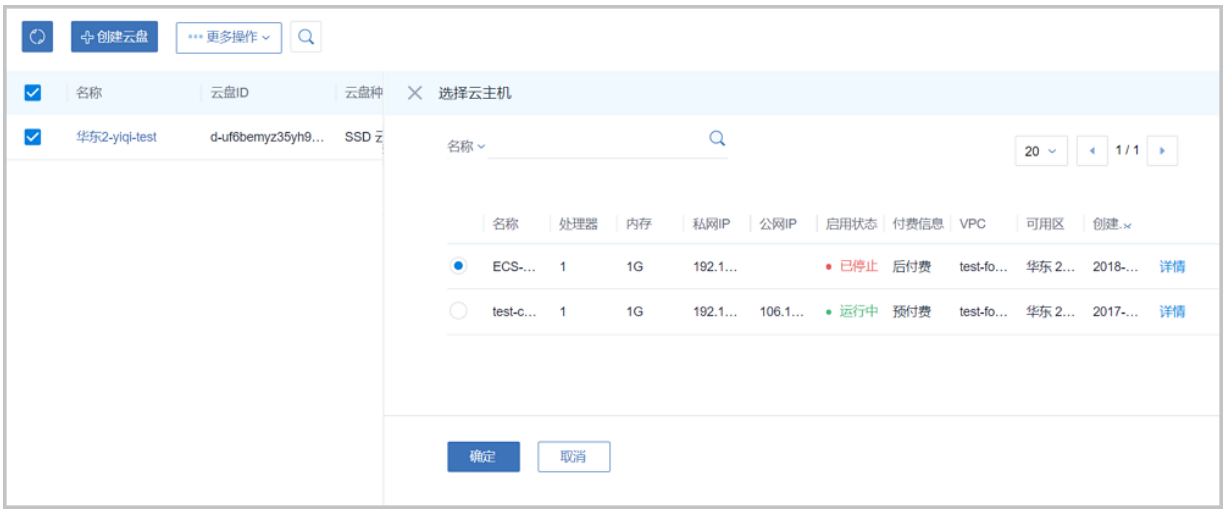
同步云盘

点击左侧的**同步数据**按钮，可将已添加地域和可用区下的阿里云端云盘同步到本地。

加载云盘

在**云盘**界面，选择某一待挂载的云盘（数据盘），点击**更多操作 > 加载** ，弹出**选择云主机**界面，选择加载云盘的ECS云主机，点击**确定**即可，如图 *51: 加载云盘到ECS云主机*所示：

图 51: 加载云盘到ECS云主机



注:

- 加载云盘到ECS云主机，仅支持加载数据盘，不支持加载系统盘
- 处于运行/停止状态的ECS云主机均支持加载云盘
- 云盘加载到ECS云主机后，云盘状态由**待挂载**变为**使用中**

卸载云盘

在**云盘**界面，选择某一使用中的云盘（数据盘），点击 **更多操作** > **卸载**，可从ECS云主机卸载云盘，如图 *52: 从ECS云主机卸载云盘*所示：

图 52: 从ECS云主机卸载云盘

注:

- 从ECS云主机卸载云盘，仅支持卸载数据盘，不支持卸载系统盘
- 处于运行/停止状态的ECS云主机均支持卸载云盘
- 云盘从ECS云主机卸载后，云盘状态由**使用中**变为**待挂载**

删除云盘

1. 在**云盘**界面，选择要删除的云盘（数据盘），点击 **更多操作** > **删除**，可删除所选云盘，如图 *53: 删除云盘*所示：

图 53: 删除云盘

2. 弹出**删除云盘**确认窗口，如图 *54: 删除云盘确认窗口*所示：

图 54: 删除云盘确认窗口

注:

- 默认只删除本地记录，如需同时删除阿里云上的云盘，请勾选**同时删除阿里云上的资源**；
- 仅支持删除数据盘，不支持删除系统盘。

对于已挂载到ECS云主机的云盘（数据盘），可设置云盘是否随ECS云主机删除。

在**云盘**界面，选择某一使用中的云盘（数据盘），打开详情页，在**基本属性**页面，设置**随主机删除**的开关处于启用/停用：

- 启用：删除ECS云主机时，该云盘随ECS云主机一起删除
- 停用：删除ECS云主机时，该云盘保留不释放

如图 *55:* 设置云盘是否随主机删除所示：

图 55: 设置云盘是否随主机删除

修改云盘名称、简介

在**云盘**界面，点击某一云盘，打开详情页，在**基本属性**页面，可修改云盘的名称和简介。

7.3 镜像

创建ECS云主机前需要创建镜像。

ZStack混合云平台目前只支持阿里云端镜像，镜像类型包括：自定义镜像和阿里云系统镜像。

镜像支持以下操作：

- 上传本地镜像到阿里云端
- 同步阿里云端镜像
- 删除镜像
- 修改自定义镜像名称和简介

上传本地镜像到阿里云端

准备工作：

- 上传本地镜像需要本地拥有镜像，如何创建本地镜像请参考用户手册云资源池镜像章节。
- 上传本地镜像前需要添加Bucket并设置为默认，如何添加Bucket请参考添加*Bucket*。

1. 在ZStack混合云主菜单，点击**产品** > **镜像**，进入**镜像**界面，如图 *56:* 镜像界面所示：

图 56: 镜像界面

2. 点击**上传镜像**按钮，弹出**上传镜像**界面，可参考以下示例输入相应内容：

- **名称**：设置镜像名称
- **操作系统**：选择镜像的操作系统
- **操作系统类型**：选择镜像操作系统的类型
- **镜像**：选择本地镜像服务器中的镜像

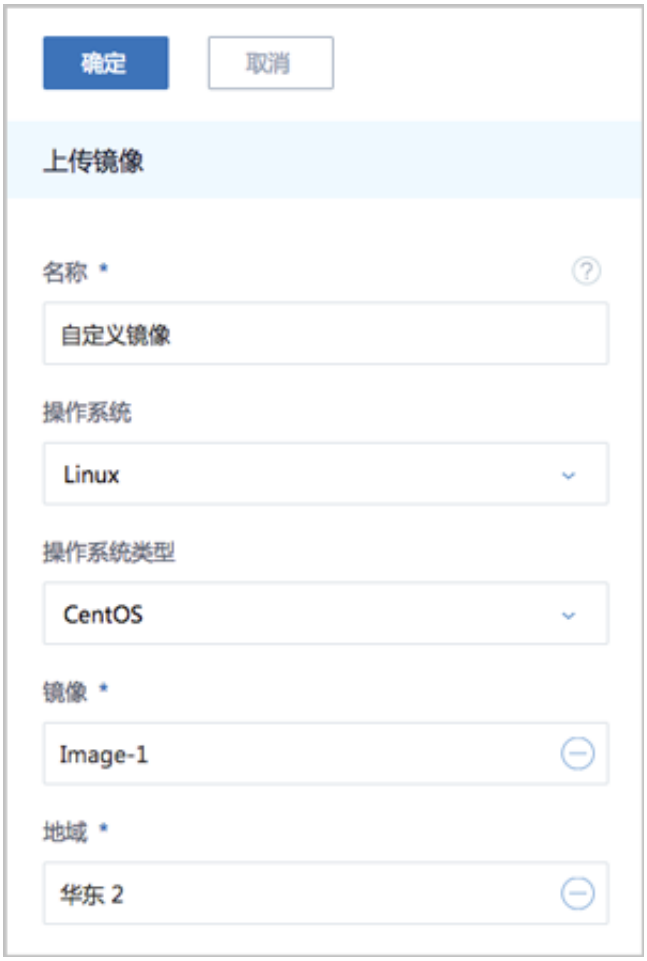
注:

- 镜像需支持在线修改密码（Qemu guest agent）
- 镜像不支持EFI、LVM分区格式

- **地域**：选择镜像上传的地域

如图 *57:* 上传镜像所示：

图 57: 上传镜像



注:

若上传本地镜像前未添加Bucket，操作助手会弹出提示框，如图 *58:* 操作助手提醒添加*Bucket*所示，点击**添加**，即可跳转至**添加Bucket**界面。

图 58: 操作助手提醒添加Bucket

3. 镜像上传可在**镜像**界面中的**上传中**界面查看上传进度，如图 *59:* 镜像上传中所示：

图 59: 镜像上传中

同步阿里云端镜像

点击左侧菜单栏的**同步数据**按钮，可将已添加地域和可用区下的阿里云端镜像同步到本地。

删除镜像

1. 在**镜像**界面，选择要删除的镜像，点击**删除**按钮，可删除所选镜像，如图 *60:* 删除镜像所示：

图 60: 删除镜像

2. 弹出**删除镜像**确认窗口，如图 *61: 删除镜像确认窗口*所示。

注:

- 默认只删除本地记录，如需同时删除阿里云上的镜像，请勾选**同时删除阿里云上的资源**
- 不支持删除阿里云上的系统镜像

图 61: 删除镜像确认窗口

修改自定义镜像名称、简介

在**镜像**界面，点击某一自定义镜像，进入**镜像**详情页，在**基本属性**子页面，可修改镜像的名称和简介。

注: 不支持修改阿里云系统镜像的名称和简介。

7.4 安全组

安全组对应了阿里云对ECS的三层隔离的防火墙约束。

创建阿里云ECS前需先建立安全组。安全组可以在ZStack混合云平台创建，也可在阿里云端创建再进行同步。安全组创建完毕后需要添加相关规则才可使用。

安全组支持以下操作：

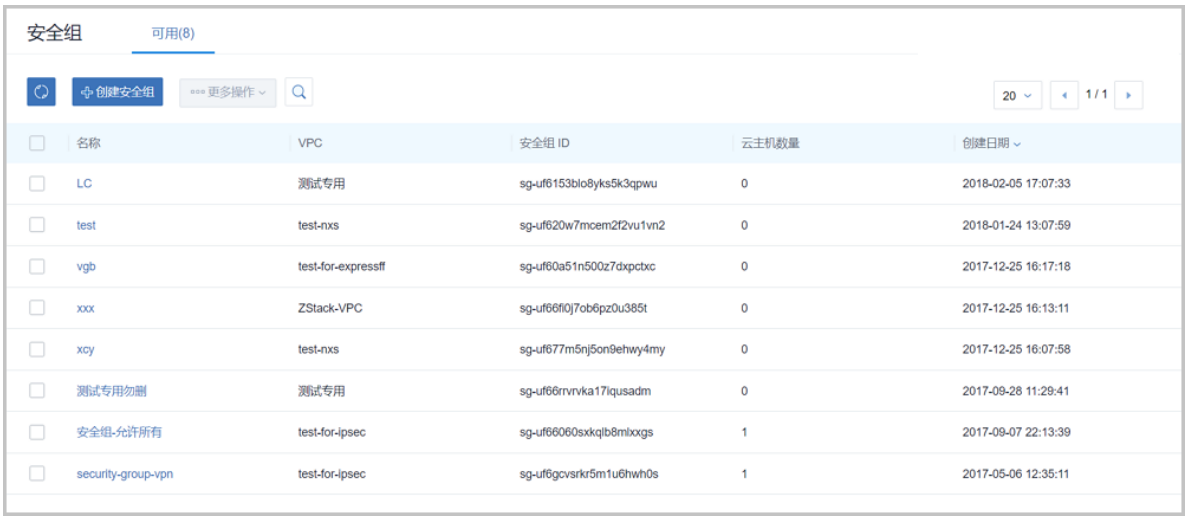
- 创建安全组：新建一个安全组
- 同步安全组：同步阿里云端安全组
- 删除安全组：默认只删除本地记录，支持同时删除阿里云上资源
- 修改安全组名称和简介

- 添加安全组规则：在安全组中添加规则
- 删除安全组规则：默认同时删除本地记录和阿里云上资源

创建安全组

1. 在ZStack混合云主菜单，点击**产品** > **安全组**，进入**安全组**界面，如图 *62:* 安全组界面所示：

图 62: 安全组界面



2. 点击**创建安全组**按钮，弹出**创建安全组**界面，可参考以下示例输入相应内容：

- **名称**：设置安全组名称
- **简介**：可选项，可留空不填
- **专有网络VPC**：选择专有网络
- **初始规则**：选择安全组初始规则，目前支持四种初始规则：
  - **禁止所有**：所有端口的出入规则方向都是拒绝
  - **允许所有**：所有端口的出入规则方向都是允许
  - **禁止部分易受攻击端口**：拒绝135/137/139/42/445等易受攻击端口的入方向（协议为UDP和TCP）
  - **允许基本常用端口**：接受22/23/3389/443/80/6379/8080/3306/1433等基本常用端口的入方向（协议为UDP和TCP）

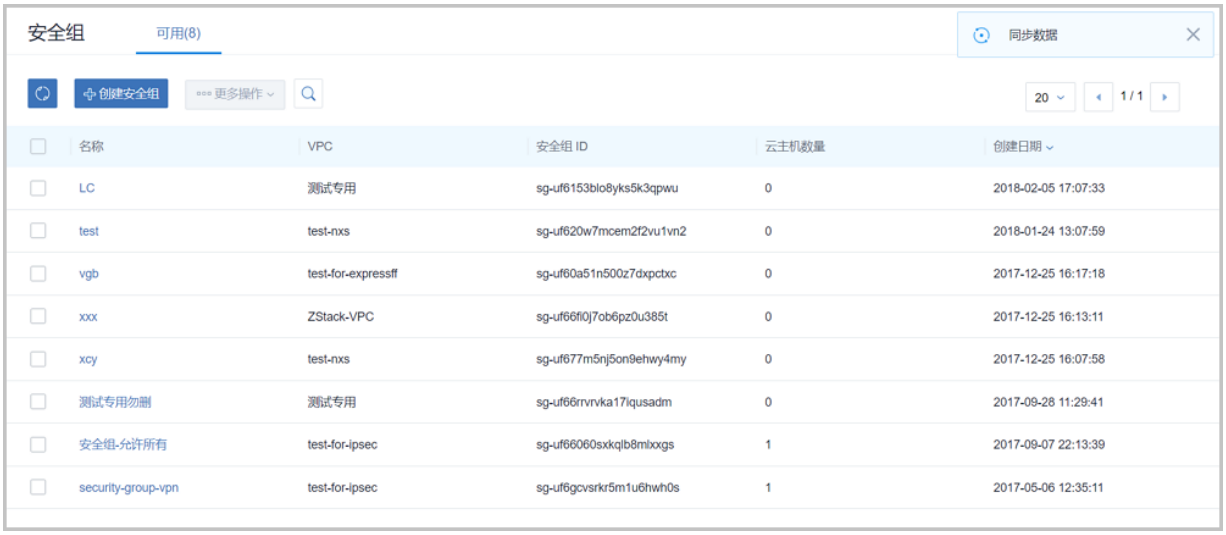
如图 *63:* 创建安全组所示：

图 63: 创建安全组

同步安全组

点击左侧的**同步数据**按钮，可将已添加地域和可用区下的安全组从阿里云端同步到本地，如图 *64: 同步安全组*所示：

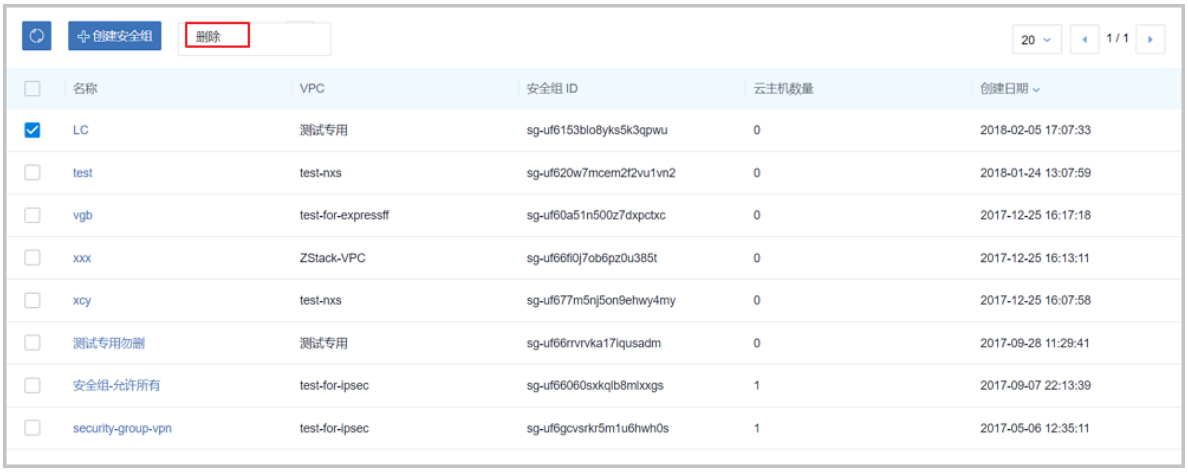
图 64: 同步安全组



删除安全组

1. 在**安全组**界面，选择要删除的安全组，点击**更多操作** > **删除**，可删除所选安全组，如图 *65:* 删除安全组所示：

图 65: 删除安全组

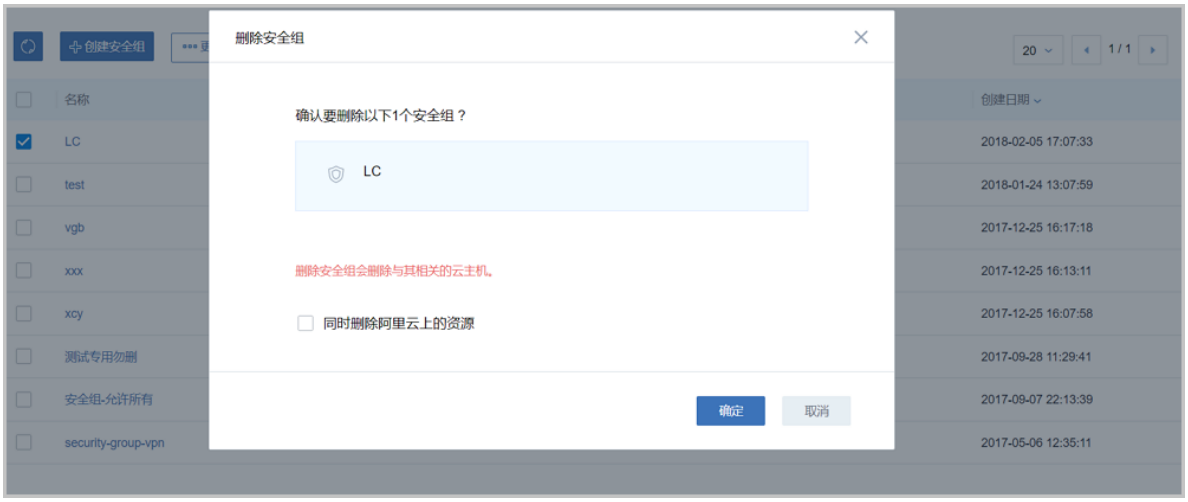


2. 弹出**删除安全组**确认窗口，如图 *66:* 删除安全组确认窗口所示。

注:

- 默认只删除本地记录，如需同时删除阿里云上的安全组，请勾选**同时删除阿里云上的资源**；
- 删除安全组会同时删除与其相关的云主机。

图 66: 删除安全组确认窗口



修改安全组名称、简介

在**安全组**界面，点击某一安全组，进入**安全组**详情页，在**基本属性**子页面，可修改安全组的名称和简介。

添加安全组规则

1. 在**安全组**界面，点击某一安全组，进入**安全组**详情页，点击**安全组规则**，进入**安全组规则**子界面，点击**操作 > 添加规则**，可添加自定义安全组规则，如图 *67: 添加安全组规则1*所示：

图 67: 添加安全组规则1

2. 在弹出的**设置规则**界面，可参考以下示例输入相应内容：

- **网卡类型**：内网（默认）
- **规则方向**：选择安全组规则适用的数据流方向，入或出
- **授权策略**：选择授权策略，允许或拒绝
- **协议**：选择安全组的协议，支持：ALL/TCP/UDP/ICMP/GRE，其中ALL可用于完全互信的场景
- **端口区间**：规则约束的端口范围

注: 安全组协议相关的端口范围说明：

- **ALL**：端口号范围值为-1/-1，不能单独设置，代表不限制端口
- **TCP/UDP**：默认端口号取值范围为1~65535；设置格式例如“1/200”，意思是端口号范围为1~200，若输入值为“200/1”，接口调用将报错
- **ICMP**：端口号范围值为-1/-1，不能单独设置，代表不限制端口
- **GRE**：端口号范围值为-1/-1，不能单独设置，代表不限制端口

- **授权对象**：规则约束的内网网络段

  注:

  - 请根据实际场景设置授权对象的CIDR
  - 如设置0.0.0.0/0，表示允许或拒绝所有IP的访问，设置时请务必谨慎

  ，

- **优先级**：选择安全组优先级，可选范围值为1-100，默认值为1，即最高优先级

如图 *68:* 添加安全组规则2所示：

图 68: 添加安全组规则2

删除安全组规则

在**安全组规则**界面，选择要删除的安全组规则，点击**操作** > **删除规则**，可删除所选安全组规则。

注: 默认同时删除该安全组规则的本地记录和阿里云上资源。

如图 *69:* 删除安全组规则所示：

图 69: 删除安全组规则

7.5 专有网络VPC

1. ZStack混合云网络目前主要用于操作阿里云上的网络资源。
2. ZStack混合云目前只支持VPC网络，不支持经典网络。
3. 专有网络VPC为阿里云的专有网络资源，在VPC中的ECS受二层隔离保护，可以和本地集群通过IPsec隧道打通，因此在ZStack混合云中创建的资源必须在一个VPC中。
4. 专有网络VPC可以在ZStack混合云创建，也可以在阿里云上创建再进行同步。

ZStack混合云专有网络VPC支持以下操作：

- 专有网络VPC管理
- 虚拟交换机管理
- 虚拟路由器管理
- 安全组管理
- VPN网关管理
- 拓扑图

7.5.1 专有网络VPC管理

ZStack专有网络VPC，支持对阿里云端专有网络VPC的管理。

ZStack支持对专有网络VPC进行以下操作：

- 创建专有网络VPC
- 删除专有网络VPC
- 创建高速通道
- 创建阿里云VPN连接
- 修改专有网络VPC名称和简介

创建专有网络VPC

ZStack支持创建阿里云专有网络VPC。

1. 在ZStack混合云主菜单，点击**产品** > **专有网络VPC**，进入**专有网络VPC**界面，如图 *70: 专有网络VPC界面*所示：

图 70: 专有网络VPC界面

2. 点击**创建专有网络VPC**按钮，弹出**创建专有网络VPC**界面，可参考以下示例输入相应内容：

- **地域**：选择VPC所在地域
- **名称**：设置VPC名称
- **简介**：可选项，可留空不填
- **CIDR**：按需选择网络段

注:

选择地域后，ZStack列出了当前地域下VPC可选择的CIDR范围，用于提示。

如图 *71: 创建专有网路 VPC*所示：

图 71: 创建专有网路 VPC

删除专有网络VPC

在**专有网络VPC**界面，选择某一VPC，点击**更多操作** > **删除**，可删除该VPC。

注:

- 默认只删除本地记录，如需同时删除阿里云上的专有网络VPC，请勾选**同时删除阿里云上的资源**；
- 删除专有网络VPC会删除相关ECS云主机；
- 删除阿里云端VPC时，如果该VPC下有付费资源未删除（例如VPN网关、物理专线资源），则删除该VPC时阿里云端会提示依赖性失败，不支持删除。

如图 *72: 删除专有网络VPC*所示：

图 72: 删除专有网络VPC

创建高速通道

1. 在**专有网络VPC**界面，选择某一VPC，点击**更多操作** > **创建高速通道**，可在该VPC下创建高速通道（即阿里云高速通道）。如图 *73: 创建高速通道1*所示：

   图 73: 创建高速通道1

2. 在弹出的**创建高速通道**界面，可参考以下示例输入相应内容：

   - **名称**：设置高速通道名称
   - **简介**：可选项，可留空不填
   - **云路由器(ZStack)**：选择本地云路由器
   - **公有网络(ZStack)**：可以连接本地和边界路由器的公有网络
   - **私有网络(ZStack)**：选择云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网
   - **边界路由器(阿里云)**：选择该VPC下的边界路由器，目前由运营商提供
   - **CPE IP(运营商)**：运营商提供物理专线到ZStack私有云客户端设备IP地址

   如图 *74: 创建高速通道2*所示：

   图 74: 创建高速通道2

注:

- 创建阿里云高速通道需提前配置连接环境，并同步路由器接口。
- 阿里云高速通道配置完成后，终端用户还需在CPE设备上自行配置两条路由，并验证本地云主机与ECS云主机是否可以ping通，至此阿里云高速通道创建成功。
- 阿里云高速通道详细部署教程请参考阿里云高速通道实践。

创建阿里云VPN连接

1. 在**专有网络VPC**界面，选择某一VPC，点击**更多操作** > **创建阿里云VPN连接**，可在该VPC下创建阿里云VPN连接。如图 *75: 创建阿里云VPN连接1*所示：

图 75: 创建阿里云VPN连接1

2. 在弹出的**创建阿里云VPN连接**界面，可参考以下示例输入相应内容：

- **名称**：设置VPN连接名称
- **简介**：可选项，可留空不填
- **VPN网关(阿里云)**：选择已购买的VPN网关

> **注:** 如果该VPC下没有可用的VPN网关，目前必须通过阿里云控制台直接购买。

- **预共享密钥(阿里云)**：建议设置强度高的密钥
- **云路由器(ZStack)**：选择创建本地云主机时自动创建的云路由器
- **公有网络(ZStack)**：选择云路由挂载的公有网络，如果云路由仅挂载一个公网则会默认选中该公网
- **IP地址(ZStack)**：可选项，表示所选择公有网络下可用的IP地址，此IP地址应为互联网公网IP地址。如果留空，系统会自动选择一个可用IP地址
- **私有网络(ZStack)**：选择云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网

如图 *76: 创建阿里云VPN连接2*所示：

图 76: 创建阿里云VPN连接2

注:

- VPN连接配置完成后，系统将自动创建IPsec VPN连接。需验证本地云主机与ECS云主机是否可以ping通，如能ping通，IPsec VPN连接创建成功。
- IPsec VPN详细部署教程请参考*IPsec VPN实践*。

修改专有网络VPC名称、简介

在**专有网络VPC**界面，点击某一VPC，打开详情页，在**基本属性**页面，可修改VPC的名称和简介。

7.5.2 虚拟交换机管理

虚拟交换机对应了阿里云VPC下的虚拟交换机，主要是指机房下可支持创建的虚拟交换机。

虚拟交换机可以在ZStack混合云平台创建，也可以在阿里云创建再进行同步。

ZStack支持对专有网络VPC下的虚拟交换机进行如下操作：

- 创建虚拟交换机
- 删除虚拟交换机
- 修改虚拟交换机名称和简介
- 基于虚拟交换机创建的ECS云主机管理

创建虚拟交换机

1. 在**专有网络VPC**界面，点击某一VPC，进入**专有网络 VPC**详情页，点击**虚拟交换机**，进入**虚拟交换机**页面，点击**操作 > 创建**，可创建虚拟交换机，如图 *77:* 虚拟交换机页面所示：

   图 77: 虚拟交换机页面

2. 在**创建虚拟交换机**页面，可参考以下示例输入相应内容：

   - **可用区**：专有网络VPC所在的可用区
   - **名称**：设置虚拟交换机名称
   - **简介**：可留空不填
   - **CIDR**：虚拟交换机网络段（会提示VPC CIDR范围），虚拟交换机网络段应是专有网络VPC下的一个子网段。例如，如果VPC CIDR为172.16.0.0/12，则虚拟交换机的CIDR可填写172.22.0.0/16

   如图 *78:* 创建虚拟交换机所示：

   图 78: 创建虚拟交换机

删除虚拟交换机

在**专有网络 VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**虚拟交换机**，进入**虚拟交换机**页面，选择要删除的虚拟交换机，并点击**操作** > **删除**，可删除该虚拟交换机。

注:

- 默认只删除本地记录，如需同时删除阿里云上相应资源，请勾选**同时删除阿里云上的资源**；
- 删除虚拟交换机会删除与其相关的ECS云主机。

如图 *79: 删除虚拟交换机*所示：

图 79: 删除虚拟交换机

修改虚拟交换机名称、简介

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**虚拟交换机**，进入**虚拟交换机**页面，点击某一虚拟交换机，进入**虚拟交换机**详情页，在**基本属性**子页面，可修改虚拟交换机的名称和简介。

基于虚拟交换机创建的ECS云主机管理

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**虚拟交换机**，进入**虚拟交换机**页面，点击某一虚拟交换机，进入**虚拟交换机**详情页，在**ECS云主机**子页面，可查看基于该虚拟交换机创建的ECS云主机列表，支持对相关ECS云主机进行以下操作：

- 启动、停止ECS云主机
- 重启ECS云主机
- 打开控制台
- 设置ECS控制台密码
- 删除ECS云主机
- 修改ECS云主机名称和简介
- 加载云盘
- 卸载云盘

如图 *80: ECS云主机管理*所示：

图 80: ECS云主机管理

7.5.3 虚拟路由器管理

虚拟路由器对应了专有网络VPC下的路由器信息。

ZStack支持对专有网路VPC下虚拟路由器进行以下操作：

- 查看虚拟路由器
- 修改虚拟路由器名称和简介
- 添加路由条目
- 删除路由条目

查看虚拟路由器

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**虚拟路由器**，进入**虚拟路由器**页面，可查看当前VPC环境下的虚拟路由器，如图 *81:* 查看虚拟路由器所示：

图 81: 查看虚拟路由器

修改虚拟路由器名称、简介

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**虚拟路由器**，进入**虚拟路由器**页面，点击某一虚拟路由器，进入**虚拟路由器**详情页，在**基本属性**子页面，可修改虚拟路由器的名称和简介。

添加路由条目

1. 在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**虚拟路由器**，进入**虚拟路由器**页面，点击某一虚拟路由器，进入**虚拟路由器**详情页，点击 **路由条目**，进入**路由条目**界面，点击**操作** > **添加**，可添加自定义路由条目，如图 *82: 添加路由条目1*所示：

   图 82: 添加路由条目1

2. 在弹出的**添加路由条目**界面，可参考以下示例输入相应内容：

   - **目标网段**：填写目标网段
   - **下一跳类型**：选择下一跳类型，目前支持ECS实例、路由器接口、VPN网关类型。
   - 选择与类型对应的下一条目标设备。

   如图 *83: 添加路由条目2*所示：

   图 83: 添加路由条目2

删除路由条目

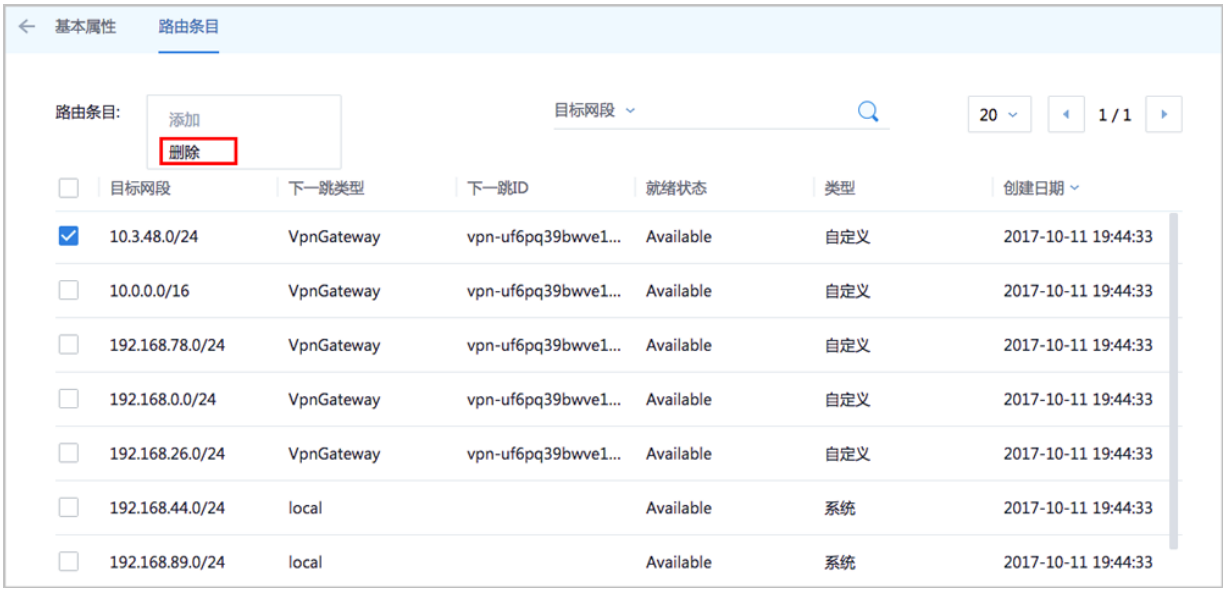
在**路由条目**界面，选择要删除的自定义路由条目，点击**操作** > **删除**，可删除该路由条目。

注:

- 默认同时删除该路由条目的本地记录和阿里云上资源
- 不支持删除系统类型的路由条目

如图 *84:* 删除路由条目所示：

图 84: 删除路由条目



7.5.4 安全组管理

ZStack支持对专有网络VPC下的安全组进行以下操作：

- 创建安全组
- 删除安全组
- 修改安全组名称和简介
- 添加安全组规则
- 删除安全组规则

创建安全组

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**安全组**，进入**安全组**页面，点击**操作** > **创建**，可创建专有网络VPC下的安全组，如图 *86:* 删除安全组所示：

图 85: 创建安全组

删除安全组

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**安全组**，进入**安全组**页面，选择要删除的安全组，点击**操作** > **删除**，可删除该安全组。

注:

- 默认只删除本地记录，如需同时删除阿里云上相应资源，请勾选**同时删除阿里云上的资源**；
- 删除安全组会删除与其相关的ECS云主机。

如图 *86:* 删除安全组所示：

图 86: 删除安全组

修改安全组名称、简介

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**安全组**，进入**安全组**页面，点击某一安全组，进入**安全组**详情页，在**基本属性**子页面，可修改安全组的名称和简介。

添加安全组规则

1. 在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**安全组**，进入**安全组**页面，点击某一安全组，进入**安全组**详情页，点击 **安全组规则**，进入**安全组规则**界面，点击**操作** > **添加规则**，可添加自定义安全组规则，如图 *87: 添加安全组规则1*所示：

   图 87: 添加安全组规则1

2. 在弹出的**设置规则**界面，可参考以下示例输入相应内容：

   - **网卡类型**：内网（默认）
   - **规则方向**：选择安全组规则适用的数据流方向，入或出
   - **授权策略**：选择授权策略，允许或拒绝
   - **协议**：选择安全组的协议，支持：ALL/TCP/UDP/ICMP/GRE，其中ALL可用于完全互信的场景
   - **端口区间**：规则约束的端口范围

     注: 安全组协议相关的端口范围说明：

- **ALL**：端口号范围值为-1/-1，不能单独设置，代表不限制端口
- **TCP/UDP**：默认端口号取值范围为1~65535；设置格式例如“1/200”，意思是端口号范围为1~200，若输入值为“200/1”，接口调用将报错
- **ICMP**：端口号范围值为-1/-1，不能单独设置，代表不限制端口
- **GRE**：端口号范围值为-1/-1，不能单独设置，代表不限制端口

- **授权对象**：规则约束的内网网络段

注:

- 请根据实际场景设置授权对象的CIDR
- 如设置0.0.0.0/0，表示允许或拒绝所有IP的访问，设置时请务必谨慎

，

- **优先级**：选择安全组优先级，可选范围值为1-100，默认值为1，即最高优先级

如图 *88:* 添加安全组规则*2*所示：

图 88: 添加安全组规则2

删除安全组规则

在**安全组规则**界面，选择要删除的安全组规则，点击**操作 > 删除规则**，可删除所选安全组规则。

注: 默认同时删除该安全组规则的本地记录和阿里云上资源。

如图 *89: 删除安全组规则*所示：

图 89: 删除安全组规则

7.5.5 VPN网关管理

ZStack支持对专有网络VPC下的VPN网关进行以下操作：

- 删除VPN网关
- 修改VPN网关名称和简介
- 删除基于VPN网关创建的IPsec VPN连接

删除VPN网关

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**VPN网关**，进入**VPN网关**页面，选择某一VPN网关并点击**操作** > **删除**，可删除该VPN网关。

注: 删除VPN网关，只删除本地记录，不删除阿里云端的VPN网关。

如图 *90: 删除VPN网关*所示：

图 90: 删除VPN网关

修改VPN网关名称、简介

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**VPN网关**，进入**VPN网关**页面，点击某一VPN网关，进入**VPN网关**详情页，在**基本属性**子页面，可修改VPN网关的名称和简介。

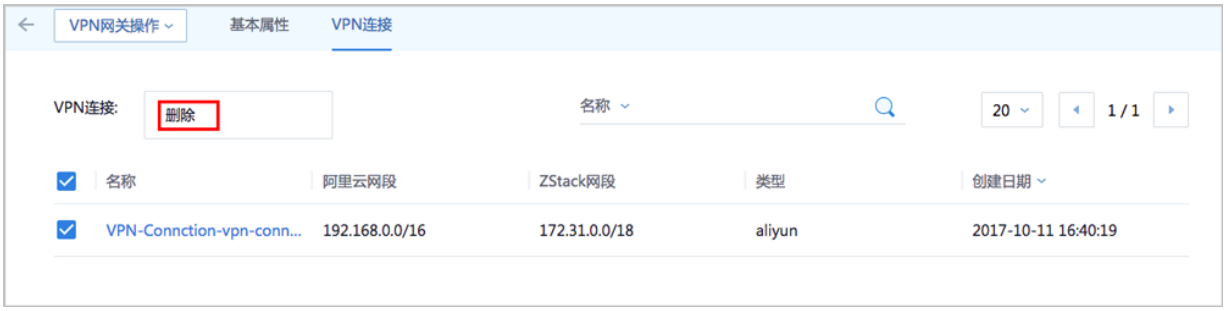
删除基于VPN网关创建的IPsec VPN连接

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**VPN网关**，进入**VPN连接**界面，选择要删除的VPN连接，点击**操作 > 删除**，可删除所选VPN连接。

注： 默认只删除本地记录，如需同时删除阿里云上的VPN连接，请勾选**同时删除阿里云上的资源**。

如图 *91: 删除VPN连接*所示：

图 91: 删除VPN连接



注： 如果IPsec VPN部署过程中发生VPN连接失败，或者两端私网互通验证失败，打算重新配置，仅删除VPN连接是不够的，需全面检查以下资源：

- 本地用于创建IPsec连接的虚拟IP是否已经占用，如果已使用，则需删除此虚拟IP；
- 阿里云VPN连接是否已经存在，如果存在，则需要删除，删除阿里云VPN连接同时需删除远端阿里云资源；
- 阿里云VPN用户网关是否已存在重复的IP，如果存在，则需要删除，删除需同时删除远程阿里云资源；
- VPC的虚拟路由器下是否存在已经指向ZStack私有云对应内网的路由条目，如果存在，则需要删除。

IPsec VPN详细部署教程请参考*IPsec VPN实践*。

7.5.6 拓扑图

阿里云高速通道网络支持网络拓扑图展示。

阿里云高速通道成功搭建后，ZStack会展示网络连接的拓扑结构。

拓扑图

若ZStack私有云端和阿里云端进行了高速通道连接，可查看网络拓扑图。

在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**拓扑图**，进入**拓扑图**页面，可查看网络拓扑，如图 *92:* 拓扑图所示：

图 92: 拓扑图

其中各部件介绍如下：

- **vrouter**：ZStack私有云端的云路由器，用于设置ZStack私有云云主机的私有网络。
- **CPE**：物理专线的客户端设备，用于设置物理专线接入ZStack云平台环境。
- **物理专线**：运营商提供的物理专线。
- **VPC**：阿里云端的VPC网络。

7.6 弹性公网IP

弹性公网IP是指阿里云端公有网络池中的IP，通过创建并绑定弹性公网IP到ECS实例，用户可以通过公网访问ECS实例。

弹性公网IP支持以下操作：

- 创建弹性公网IP
- 绑定弹性公网IP
- 解绑弹性公网IP
- 删除弹性公网IP
- 修改弹性公网IP名称和简介

创建弹性公网IP

1. 在ZStack混合云主菜单，点击**产品** > **弹性公网IP**，进入**弹性公网IP**界面，如图 *93:* 弹性公网*IP*界面所示：

   图 93: 弹性公网IP界面

2. 点击**创建弹性公网IP**按钮，弹出**创建弹性公网IP**界面，可参考以下示例输入相应内容：

   - **地域**：选择弹性公网IP所属地域
   - **名称**：设置弹性公网IP名称
   - **简介**：可选项，可留空不填
   - **带宽**：设置弹性公网IP带宽，单位为M

   如图 *94:* 创建弹性公网*IP*所示：

   图 94: 创建弹性公网IP

绑定弹性公网IP

在**弹性公网IP**界面，选择某一弹性公网IP，点击**更多操作** > **绑定**，可绑定弹性公网IP到ECS实例，如图 *95: 绑定弹性公网IP*所示：

图 95: 绑定弹性公网IP

解绑弹性公网IP

在**弹性公网IP**界面，选择某一弹性公网IP，点击**更多操作** > **解绑**，可将ECS实例上的弹性公网IP解绑，如图 *96: 解绑弹性公网IP*所示：

图 96: 解绑弹性公网IP

删除弹性公网 IP

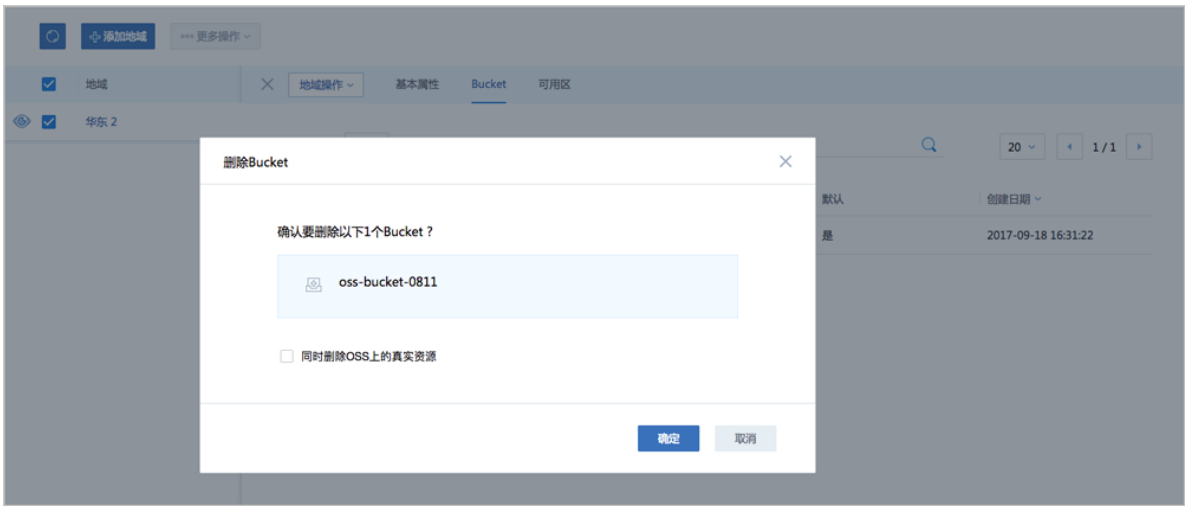
1. 在**弹性公网IP**界面，选择某一弹性公网IP，点击**更多操作** > **删除**，可删除所选弹性公网IP，如图 *97: 删除弹性公网IP*所示：

   图 97: 删除弹性公网IP

2. 弹出**删除弹性公网IP**确认窗口，如图 *98: 删除弹性公网IP确认窗口*所示。

   注: 默认只删除本地记录，如需同时删除阿里云上的弹性公网IP，请勾选**同时删除阿里云上的资源。**

   图 98: 删除弹性公网IP确认窗口



修改弹性公网IP名称、简介

在**弹性公网IP**界面，点击某一弹性公网IP，进入**弹性公网IP**详情页，在**基本属性**子页面，可修改弹性公网IP的名称和简介。

7.7 VPN

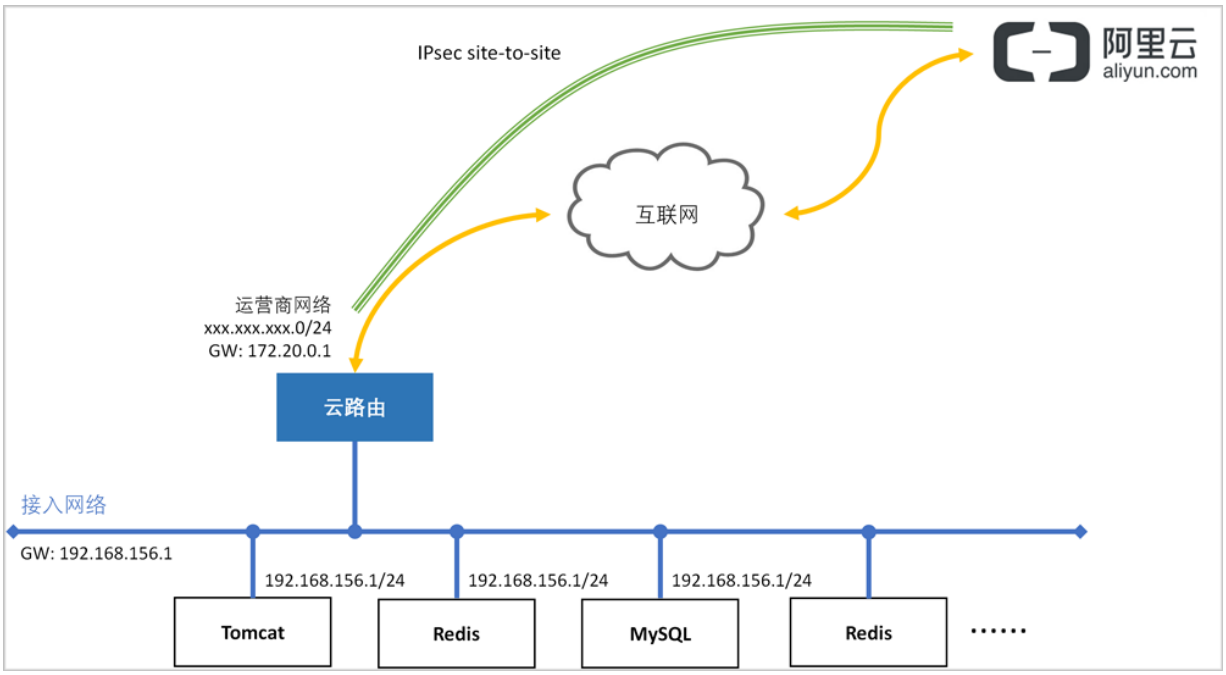
VPN：通过建立点对点的IPsec VPN通道，实现企业本地数据中心的私有网络与阿里云端VPN网络进行通信。

注: 从本地云路由到阿里云端VPN网络，IPsec准备互通的各网络段不可重叠！

典型应用场景

IPsec VPN典型应用场景如图 *99: IPsec VPN*典型应用场景所示：

图 99: IPsec VPN典型应用场景



基本使用流程

ZStack使用IPsec VPN进行互通的基本流程如下：

1. 在ZStack混合云界面按照顺序创建地域、可用区、专有网络VPC和VPC下的虚拟交换机。
2. 在阿里云控制台购买VPN网关。
3. 使用云路由网络创建私有云云主机。
4. 创建ECS云主机。
5. 推荐使用操作向导快速创建阿里云VPN连接。
   a. 选择已购买的VPN网关，可确定该VPN网关所在的地域、可用区、VPC、虚拟交换机等阿里云资源。
   b. 连接配置：选择创建本地云主机时自动创建的云路由器，以及该云路由器挂载的公有网络、私有网络，并填写预共享密钥，其他IPsec各项配置在高级选项中是默认的，不建议修改。
   c. 连接配置完成后，ZStack将自动完成以下操作：
      A. 使用本地云路由器对应的公有网络选择可用的虚拟IP；
      B. 使用此虚拟IP在阿里云端创建VPN用户网关；
      C. 在阿里云端创建VPN连接；
      D. 在阿里云VPC的虚拟路由器下配置路由，路由的目标网段为本地云路由挂载的私有网络*CIDR*，下一跳为*VPN*网关；
      E. 在ZStack私有云端创建IPsec连接。

6. 验证本地云主机与ECS云主机是否可以ping通，如能ping通，IPsec VPN通道创建成功。

注: IPsec VPN详细部署教程请参考*IPsec VPN实践*。

7.7.1 VPN网关

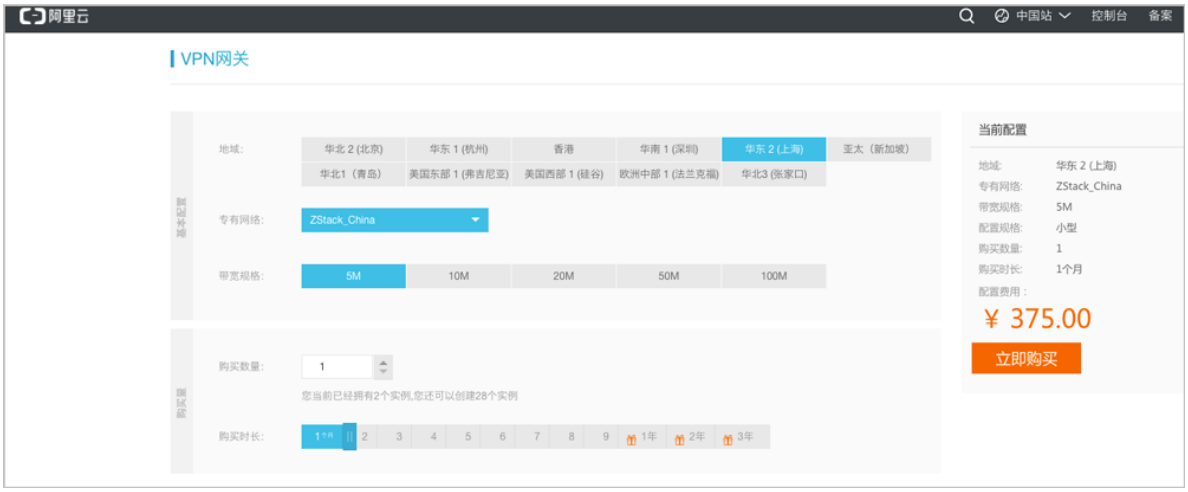
VPN网关是一款基于Internet，通过加密通道将本地数据中心和阿里云专有网络VPC安全可靠连接起来的服务。

- 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网关只能在阿里云VPC中使用，不能在经典网络中使用。

目前VPN网关需在阿里云控制台直接购买。

1. 在阿里云控制台上，选择**专有网络VPC > VPN网关**，点击**创建VPN网关**，选择地域、专有网络VPC、带宽规格等配置信息，并支付。如图 *100: 阿里云端购买VPN网关*所示：

图 100: 阿里云端购买VPN网关



2. 购买成功后，阿里云将在所选VPC下创建VPN网关，并为VPN网关自动分配公网IP。

VPN网关支持以下操作：

- 同步VPN网关到本地
- 删除VPN网关
- 修改VPN网关名称和简介
- 删除基于VPN网关创建的IPsec VPN连接

同步VPN网关到本地

点击左侧菜单栏的**同步数据**按钮，可将已添加地域和可用区下的VPN网关从阿里云端同步到本地。

删除VPN网关

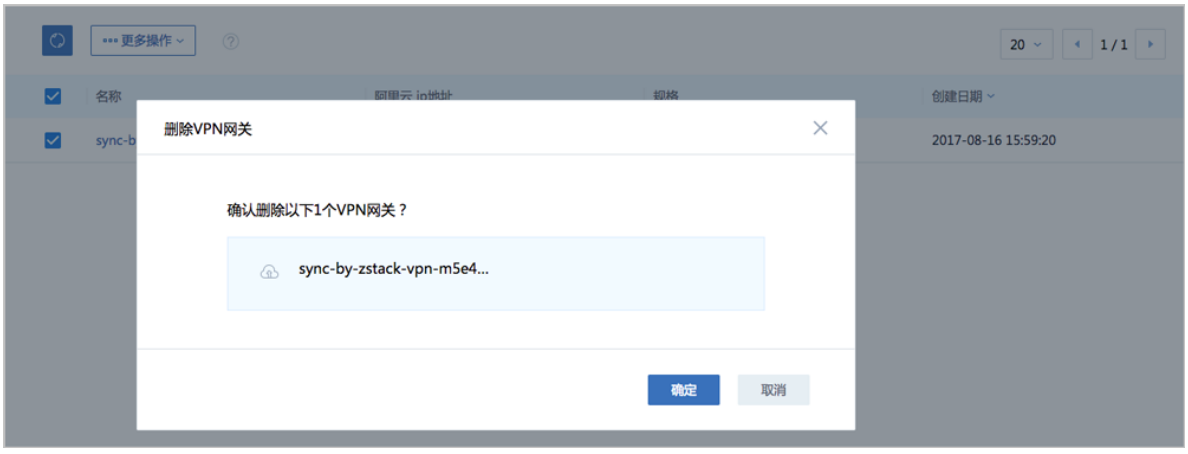
1. 在ZStack混合云主菜单，点击**产品** > **VPN** > **VPN网关**，进入**VPN网关**界面，选择要删除的VPN网关，点击**更多操作** > **删除**，可删除所选VPN网关，如图 *101: 删除VPN网关*所示：

图 101: 删除VPN网关

2. 弹出**删除VPN网关**确认窗口，如图 *102: 删除VPN网关确认窗口*所示。

注: 默认只删除本地记录，不支持删除阿里云上的VPN网关。

图 102: 删除VPN网关确认窗口



修改VPN网关名称、简介

点击ZStack菜单栏的**混合云** > **产品** > **VPN** > **VPN网关**，进入**VPN网关**界面，点击某一VPN网关，进入**VPN网关**详情页，在**基本属性**子页面，可修改VPN网关的名称和简介。

删除基于VPN网关创建的IPsec VPN连接

点击ZStack菜单栏的**混合云** > **产品** > **VPN** > **VPN网关**，进入**VPN网关**界面，点击某一VPN网关，进入**VPN网关**详情页，在**VPN连接**子界面，选择要删除的VPN连接，点击**操作** > **删除**，可删除所选VPN连接。

注: 默认只删除本地记录，如需同时删除阿里云上的VPN连接，请勾选**同时删除阿里云上的资源**。

如图 *103: 删除VPN连接*所示：

图 103: 删除VPN连接

注: 如果IPsec VPN部署过程中发生VPN连接失败，或者两端私网互通验证失败，打算重新配置，仅删除VPN连接是不够的，需全面检查以下资源：

- 本地用于创建IPsec连接的虚拟IP是否已经占用，如果已使用，则需删除此虚拟IP；
- 阿里云VPN连接是否已经存在，如果存在，则需要删除，删除阿里云VPN连接同时需删除远端阿里云资源；
- 阿里云VPN用户网关是否已存在重复的IP，如果存在，则需要删除，删除需同时删除远程阿里云资源；
- VPC的虚拟路由器下是否存在已经指向ZStack私有云对应内网的路由条目，如果存在，则需要删除。

IPsec VPN详细部署教程请参考*IPsec VPN实践*。

7.7.2 VPN用户网关

VPN用户网关是本地数据中心的VPN服务网关，对应了本地云路由网路中的虚拟IP。

VPN用户网关支持以下操作：

- 创建VPN用户网关

- 删除VPN用户网关
- 修改VPN用户网关名称和简介
- 删除基于VPN用户网关创建的IPsec VPN连接

创建VPN用户网关

如前说述，利用操作向导搭建IPsec VPN通道，系统会自动创建VPN用户网关。

ZStack支持手动搭建IPsec VPN通道，需要手动创建VPN用户网关。

1. 在ZStack混合云主菜单，点击**产品** > **VPNVPN用户网关**，进入**VPN用户网关**界面，如图 *104: VPN用户网关界面*所示：

图 104: VPN用户网关界面

2. 点击 **创建VPN用户网关**，弹出 **创建用户网关** 界面，可参考以下示例输入相应内容：

- **名称**：设置VPN用户网关名称
- **简介**：可选项，可留空不填
- **ZStack IP地址**：使用本地云路由器对应的公有网络创建的虚拟IP

> **注:** 该虚拟IP需提前在ZStack私有云界面创建，如何创建虚拟IP请参考用户手册网络虚拟*IP*章节。

- **地域**：选择VPN网关所在地域

如图 *105: 创建VPN用户网关*所示：

图 105: 创建VPN用户网关

删除VPN用户网关

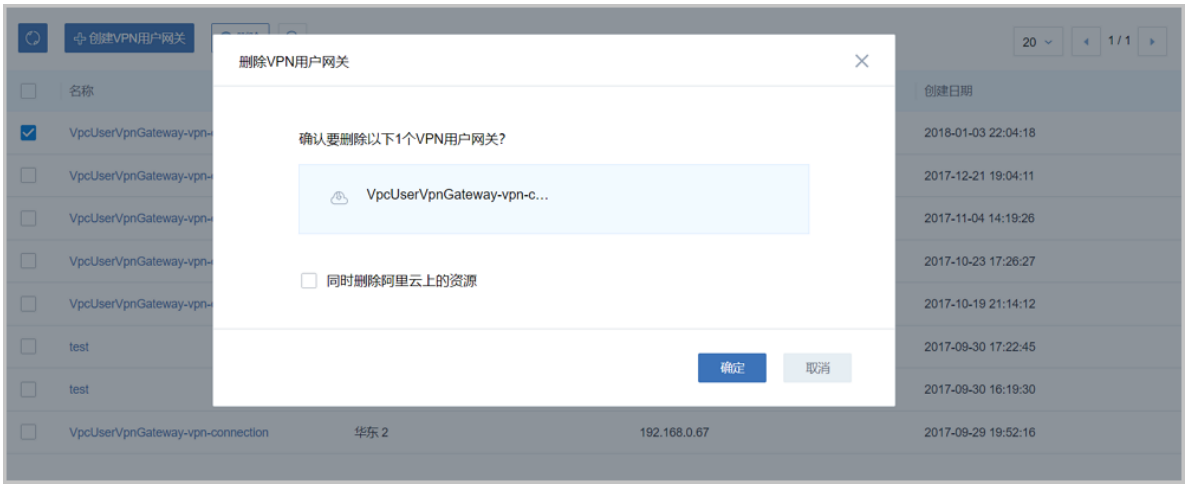
1. 在**VPN用户网关**界面，选择要删除的VPN用户网关，点击**删除**，可删除所选VPN用户网关，如图 *106: 删除VPN用户网关*所示：

   图 106: 删除VPN用户网关

2. 弹出**删除VPN用户网关**确认窗口，如图 *107: 删除VPN用户网关确认窗口*所示。

注: 默认只删除本地记录，如需同时删除阿里云上的VPN用户网关，请勾选**同时删除阿里云上的资源。**

图 107: 删除VPN用户网关确认窗口



修改VPN用户网关名称、简介

在ZStack混合云主菜单，点击**产品** > **VPN** > **VPN用户网关**，进入**VPN用户网关**界面，点击某一VPN用户网关，进入**VPN用户网关**详情页，在**基本属性**子页面，可修改VPN用户网关的名称和简介。

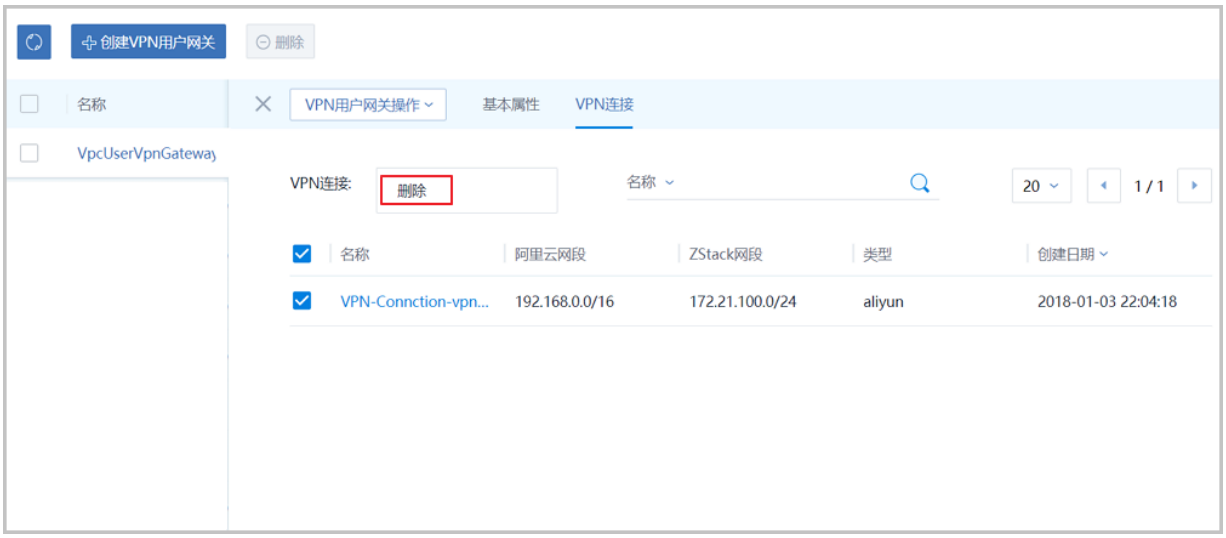
删除基于VPN用户网关创建的IPsec VPN连接

在ZStack混合云主菜单，点击**产品** > **VPN** > **VPN用户网关**，进入**VPN用户网关**界面，点击某一VPN用户网关，进入**VPN用户网关**详情页，在**VPN用户网关**子界面，选择要删除的VPN连接，点击**操作** > **删除**，可删除所选VPN连接。

注: 默认只删除本地记录，如需同时删除阿里云上的VPN连接，请勾选**同时删除阿里云上的资源。**

如图 *108: 删除VPN连接*所示：

图 108: 删除VPN连接



注: 如果IPsec VPN部署过程中发生VPN连接失败，或者两端私网互通验证失败，打算重新配置，仅删除VPN连接是不够的，需全面检查以下资源：

- 本地用于创建IPsec连接的虚拟IP是否已经占用，如果已使用，则需删除此虚拟IP；
- 阿里云VPN连接是否已经存在，如果存在，则需要删除，删除阿里云VPN连接同时需删除远端阿里云资源；
- 阿里云VPN用户网关是否已存在重复的IP，如果存在，则需要删除，删除需同时删除远程阿里云资源；
- VPC的虚拟路由器下是否存在已经指向ZStack私有云对应内网的路由条目，如果存在，则需要删除。

IPsec VPN详细部署教程请参考*IPsec VPN实践*。

7.7.3 VPN连接

VPN连接是VPN网关和VPN用户网关建立连接后的加密VPN通道。

VPN连接支持以下操作：

- 建立VPN连接
- 删除VPN连接
- 修改VPN连接名称和简介

建立VPN连接

搭建IPsec VPN通道的3个入口：

1. 从操作向导搭建IPsec VPN通道。

注： VPN连接配置完成后，系统将自动在阿里云端创建VPN连接。

2. 从专有网络VPC界面搭建IPsec VPN通道。

注： VPN连接配置完成后，系统将自动在阿里云端创建VPN连接。

3. 手动搭建IPsec VPN通道。

注： 手动搭建IPsec VPN通道，需手动创建VPN连接。

手动搭建IPsec VPN通道的基本步骤：

1. 在ZStack混合云界面按照顺序创建地域、可用区、专有网络VPC和VPC下的虚拟交换机。
2. 在阿里云控制台购买VPN网关。
3. 使用云路由网络创建私有云云主机。
4. 创建ECS云主机。
5. 使用本地云路由器挂载的公有网络创建虚拟IP。
6. 基于该虚拟IP手动创建VPN用户网关。
7. 在ZStack私有云界面手动创建IPsec连接。
   a. 在ZStack私有云主菜单，点击**网络服务** > **IPsec隧道**，进入**IPsec隧道**界面，如图 *109: IPsec隧道界面*所示：

图 109: IPsec隧道界面

   b. 点击**创建IPsec隧道**，弹出**创建IPsec隧道**界面，可参考以下示例输入相应内容：

- **名称**：设置IPsec隧道名称
- **简介**：可选项，可留空不填
- **选择虚拟IP**：选择已有虚拟IP，即：已创建的阿里云用户网关的IP地址

- **本地子网**：选择本地云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网
- **远端网络IP**：填写已购买的阿里云VPN网关的IP地址
- **远端网络CIDR**：填写阿里云VPC的CIDR
- **认证密钥**：设置密钥，建议设置强度较高的密钥
- **高级选项**：默认选项为可连通双边私网的选项，不建议修改
  - **认证模式**：psk（默认）
  - **工作模式**：tunnel（默认）
  - **IKE 验证算法**：sha1（默认）
  - **IKE 加密算法**：3des（默认）
  - **IKE 完整前向保密**：2（默认）
  - **传输安全协议**：esp（默认）
  - **ESP 认证算法**：sha1（默认）
  - **ESP 加密算法**：3des（默认）
  - **完全正向保密(PFS)**：dh-group2（默认）

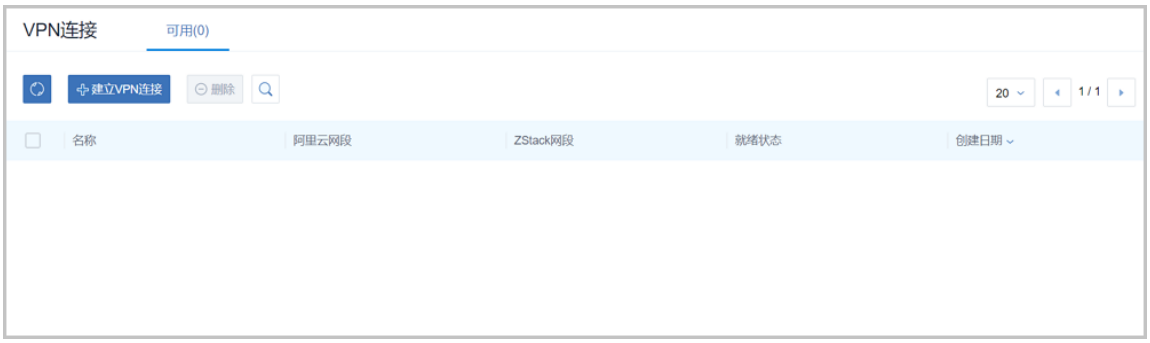
如图 *110: 创建IPsec连接*所示：

图 110: 创建IPsec连接

8. 手动创建VPN连接。

   a. 在ZStack混合云主菜单，点击**产品** > **VPN** > **VPN连接**，进入**VPN连接**界面，如图 *111: VPN连接界面*所示：

图 111: VPN连接界面



b. 点击**建立VPN连接**，弹出**建立VPN连接**界面，可参考以下示例输入相应内容：

- **名称**：设置VPN连接名称
- **简介**：可选项，可留空不填
- **云路由器(ZStack)**：推荐使用云路由网络构建阿里云VPN连接，选择创建本地云主机时自动创建的云路由器
- **私有网络(ZStack)**：选择本地云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网
- **VPN网关(阿里云)**：选择已购买的阿里云VPN网关
- **用户网关(阿里云)**：选择已创建的阿里云用户网关
- **IKE 预共享密钥**：建议设置强度高的密钥
- **高级选项**：默认选项为可连通双边私网的选项，不建议修改
  - **IKE SA生存周期(秒)**：86400（默认）
  - **IKE 阿里云端IP**：已购买的阿里云VPN网关的IP地址（默认自动填充）
  - **IKE ZStack端IP**：已创建的阿里云用户网关的IP地址（默认自动填充）
  - **IKE 版本**：ikev1（默认）
  - **IKE 协商模式**：main（默认）
  - **IKE 加密算法**：3des（默认）
  - **IKE 认证算法**：sha1（默认）
  - **IKE DH分组**：group2（默认）
  - **IPsec SA生存周期**：86400（默认）
  - **IPsec 加密算法**：3des（默认）
  - **IPsec 认证算法**：sha1（默认）
  - **IPsec DH分组**：group2（默认）

如图 *112: 创建VPN连接*所示：

图 112: 创建VPN连接

9. 手动创建VPN连接后，需在阿里云VPC的虚拟路由器下手动配置路由，路由的目标网段为本地云路由挂载的私有网络*CIDR*，下一跳为*VPN*网关。

   如何添加路由条目请参考专有网络VPC虚拟路由器管理章节。

10. 需验证本地云主机与ECS云主机是否可以ping通，如能ping通，IPsec VPN通道手动创建成功。

删除VPN连接

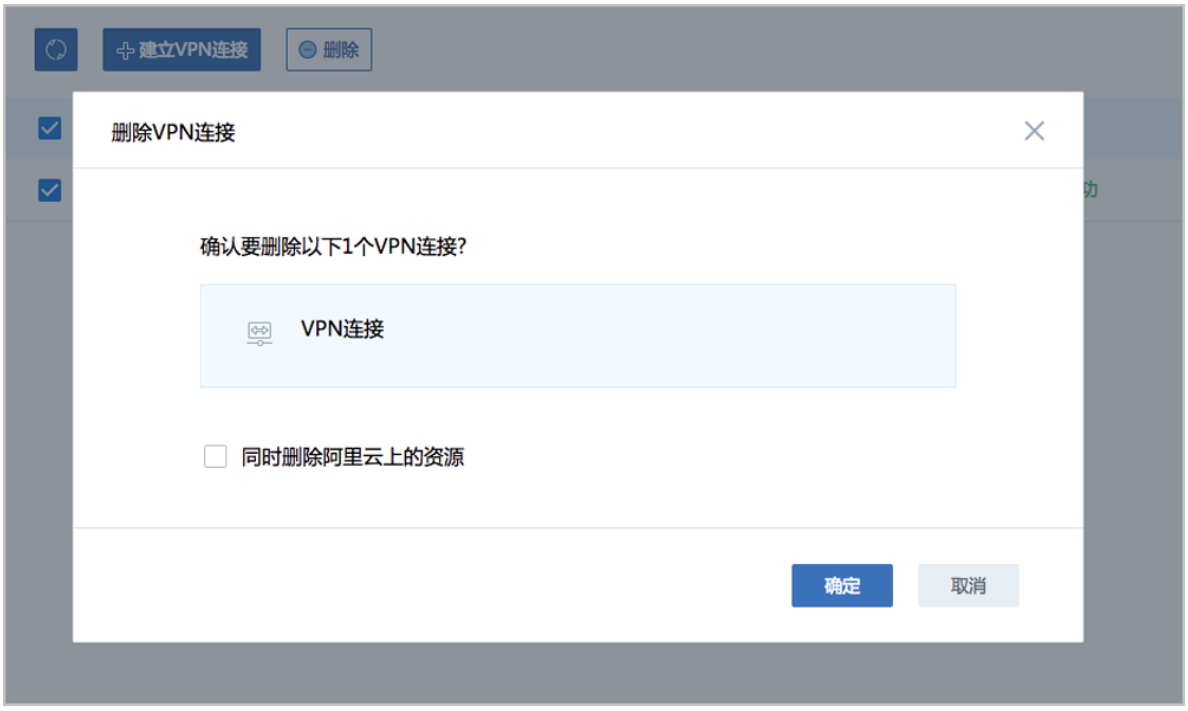
1. 在**VPN连接**界面，选择要删除的VPN连接，点击**删除**，可删除所选VPN连接，如图 *113: 删除VPN连接*所示：

图 113: 删除VPN连接

2. 弹出**删除VPN连接**确认窗口，如图 *114: 删除VPN连接确认窗口*所示。

注: 默认只删除本地记录，如需同时删除阿里云上的VPN连接，请勾选**同时删除阿里云上的资源。**

图 114: 删除VPN连接确认窗口



注: 如果IPsec VPN部署过程中发生VPN连接失败，或者两端私网互通验证失败，打算重新配置，仅删除VPN连接是不够的，需全面检查以下资源：

- 本地用于创建IPsec连接的虚拟IP是否已经占用，如果已使用，则需删除此虚拟IP；

- 阿里云VPN连接是否已经存在，如果存在，则需要删除，删除阿里云VPN连接同时需删除远端阿里云资源；
- 阿里云VPN用户网关是否已存在重复的IP，如果存在，则需要删除，删除需同时删除远程阿里云资源；
- VPC的虚拟路由器下是否存在已经指向ZStack私有云对应内网的路由条目，如果存在，则需要删除。

IPsec VPN详细部署教程请参考*IPsec VPN实践*。

修改VPN连接名称、简介

在ZStack混合云主菜单，点击**产品** > **VPN** > **VPN连接**，进入**VPN连接**界面，点击某一VPN连接，进入**VPN连接**详情页，在**基本属性**子页面，可修改VPN连接的名称和简介。

7.8 高速通道

高速通道，包括阿里云高速通道以及大河高速通道。

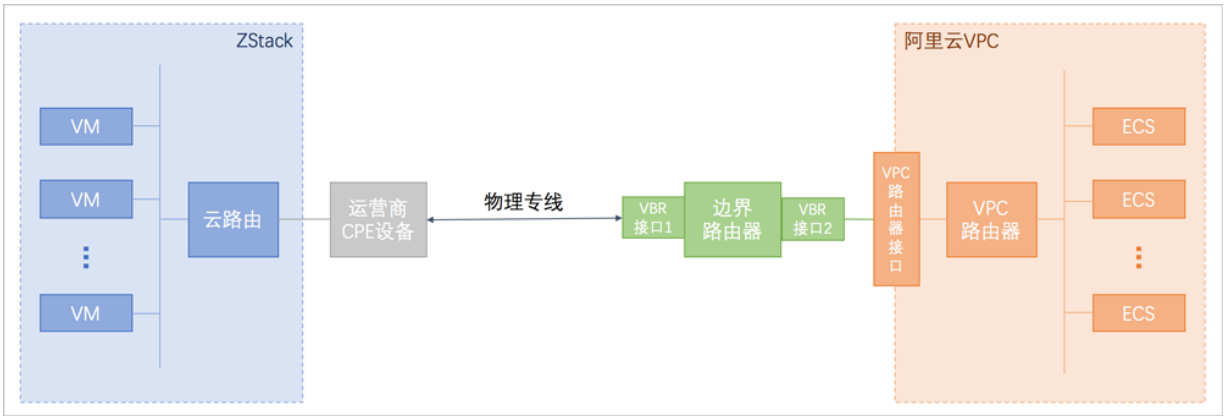
阿里云高速通道

主要是指通过物理专线（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。

注: 从本地云路由到阿里云端VPC网络，阿里云高速通道准备互通的各网络段不可重叠！

阿里云高速通道网络架构如图 *115: 阿里云高速通道网络架构图*所示：

图 115: 阿里云高速通道网络架构图



阿里云高速通道具有以下优点：

- 低延迟、高稳定性
- 具有多种接入方式
- 支持线路冗余
- 安全可靠

大河高速通道

关于大河高速通道的相关介绍请参考*SD-WAN*章节。

高速通道支持的操作

高速通道支持以下操作：

- 同步/本地创建路由器接口：支持从阿里云端同步路由器接口到本地，以及在本地创建路由器接口，实现路由器接口的管理。
- 同步边界路由器：支持从阿里云端同步边界路由器到本地，实现边界路由器的管理。
- 创建高速通道：
  - 创建阿里云高速通道：
    - 支持从操作向导创建阿里云高速通道；
    - 在专有网络VPC下创建阿里云高速通道，配置路由条目，并创建高速通道网络拓扑图。
  - 创建大河高速通道：
    - 首次创建大河高速通道建议使用操作向导方式；
    - 大河高速通道成功创建后，如需修改相关配置，或打算删除重建，建议进入**SD-WAN** > **大河** > **大河专线**界面进行手动创建。

7.8.1 路由器接口

路由器接口是一种虚拟设备，用于搭建通信通道并控制其工作状态。

高速通道将不同网络间搭建内网通信通道的过程抽象为：在两侧路由器上分别创建路由器接口，并进行互连，从而使两个路由器可通过该通道向对方转发消息。

路由器接口通常由运营商或第三方云服务商（例如大河）配置，包括对边界路由器和VPC虚拟路由器创建路由器接口。

ZStack混合云高速通道支持：

- 从阿里云端同步路由器接口到本地
- 在本地创建路由器接口

同步路由器接口

同步路由器接口，即同步在阿里云端创建的路由器接口。

1. 在ZStack混合云主菜单，点击**产品** > **高速通道** > **路由器接口**，进入**路由器接口**界面，如图 *116: 路由器接口界面*所示：

图 116: 路由器接口界面

2. 点击左侧的**同步数据**按钮，可将已添加地域和可用区下的阿里云端路由器接口同步到本地。

创建路由器接口

支持在本地对边界路由器和VPC虚拟路由器创建路由器接口。

- 对边界路由器创建路由器接口

  在**路由器接口**界面，进入**边界路由器**子界面，点击**创建路由器接口**，弹出**创建路由器接口**界面，可参考以下示例输入相应内容：

  - **名称**：设置边界路由器接口名称
  - **简介**：可选项，可留空不填
  - **规格**：可选项，设置边界路由器在阿里云侧路由器接口的带宽规格
  - **地域**：选择相应的阿里云VPC虚拟路由器所在地域
  - **边界路由器**：选择相应的边界路由器
  - **接入点**：选择边界路由器在阿里云侧路由器接口的接入点

  如图 *117: 创建边界路由器接口*所示：

图 117: 创建边界路由器接口

- 对VPC虚拟路由器创建路由器接口

  在**路由器接口**界面，进入**VPC路由器**子界面，点击**创建路由器接口**，弹出**创建路由器接口**界面，可参考以下示例输入相应内容：

  - **名称**：设置VPC虚拟路由器接口名称
  - **简介**：可选项，可留空不填
  - **规格**：可选项，设置VPC虚拟路由器接口的带宽规格
  - **地域**：选择相应的阿里云VPC虚拟路由器所在地域
  - **虚拟路由器**：选择相应的VPC虚拟路由器
  - **接入点**：选择VPC虚拟路由器接口的接入点

如图 *118:* 创建*VPC*路由器接口所示：

图 118: 创建VPC路由器接口

7.8.2 边界路由器

边界路由器是客户申请的物理专线/SD-WAN接入交换机的产品映射。可以看做是本地 CPE（Customer Premise Equipment）设备/本地云路由和阿里云VPC的虚拟路由器之间的一个路由器，作为VPC数据与本地数据之间的转发桥梁。

边界路由器主要提供以下功能：

- 作为云下、云上的中间路由器，交换数据包
- 在三层子接口模式下，可以识别或附加VLAN标签

- 作为专线静态路由的网关，对云下到云上和反向的数据包做路由
- 决定物理专线/SD-WAN专线端口模式：三层路由口或基于VLAN的三层子接口

IP地址分为阿里侧互联IP与客户侧互联IP，分别作为VPC到IDC的路由的网关、IDC到VPC的路由的网关。 这两个IP地址的建议如下：

- 建议使用私有IP（Private IP）中的一段
- 不能与VPC内的IP地址、本地数据中心内的IP地址冲突
- 由于只需要两个可用IP地址，所以掩码不需要太大，可以使用28位、29位等

边界路由器使用限制：

- 目前不支持源地址策略路由
- 目前边界路由器仅支持静态路由
- 每个边界路由器有且只有1个路由表
- 每个路由表支持48条自定义路由条目

边界路由器通常由运营商或第三方云服务商（例如大河）创建并配置路由。

边界路由器支持以下操作：

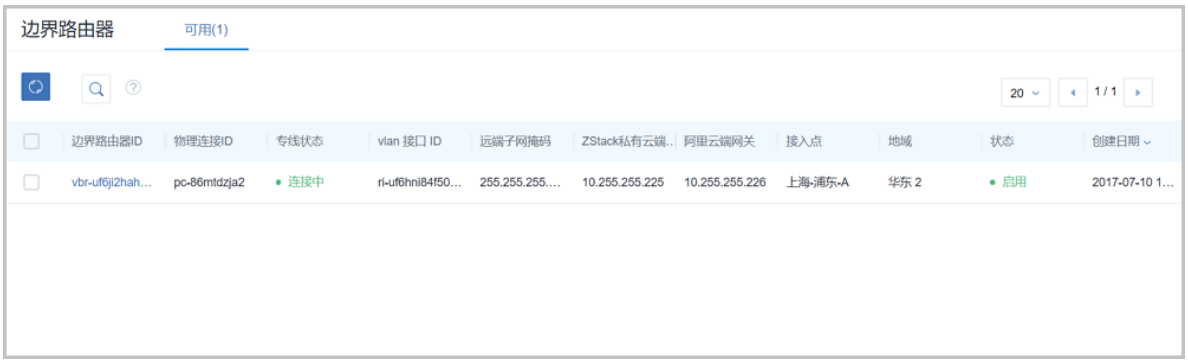
- 同步边界路由器
- 修改边界路由器名称和简介
- 添加路由条目
- 删除路由条目

同步边界路由器

同步边界路由器，可将阿里云端创建的边界路由器及路由条目同步到本地。

1. 在ZStack混合云主菜单，点击**产品** > **高速通道** > **边界路由器**，进入**边界路由器**界面，如图 *119: 边界路由器界面*所示：

   图 119: 边界路由器界面



2. 点击左侧的**同步数据**按钮，可将已添加地域和可用区下的阿里云端边界路由器同步到本地。

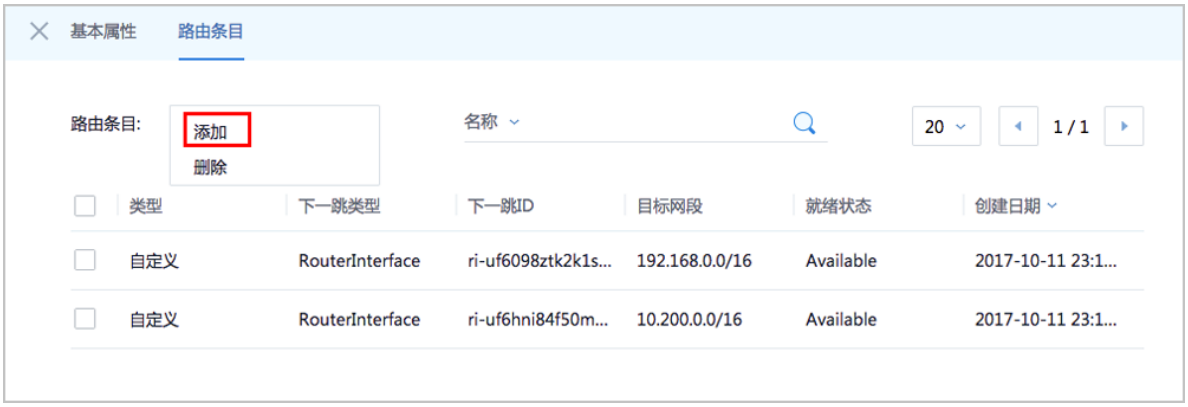
修改边界路由器名称、简介

在ZStack混合云主菜单，点击**产品** > **高速通道** > **边界路由器**，进入**边界路由器**界面，点击边界路由器，进入**边界路由器**详情页，在**基本属性**子页面，可修改边界路由器的名称和简介。

添加路由条目

1. 在**边界路由器**界面，点击边界路由器，进入**边界路由器**详情页，点击 **路由条目**，进入**路由条目**界面，点击**操作** > **添加**，可添加自定义路由条目，如图 *120: 添加路由条目1*所示：

图 120: 添加路由条目1

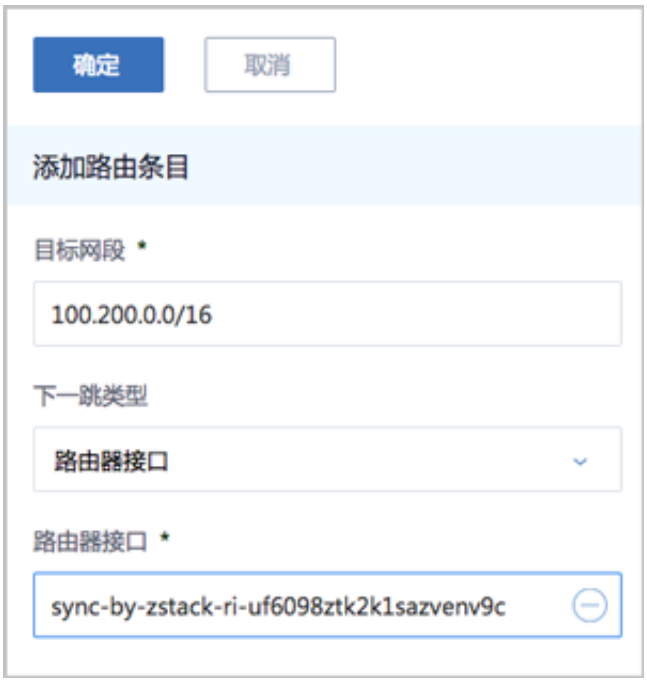


2. 在弹出的**添加路由条目**界面，可参考以下示例输入相应内容：

- **目标网段**：填写目标网段
- **下一跳类型**：选择下一跳类型，目前支持ECS实例、路由器接口、VPN网关类型。
- 选择与类型对应的下一条目标设备。

如图 *121: 添加路由条目2*所示：

图 121: 添加路由条目2



删除路由条目

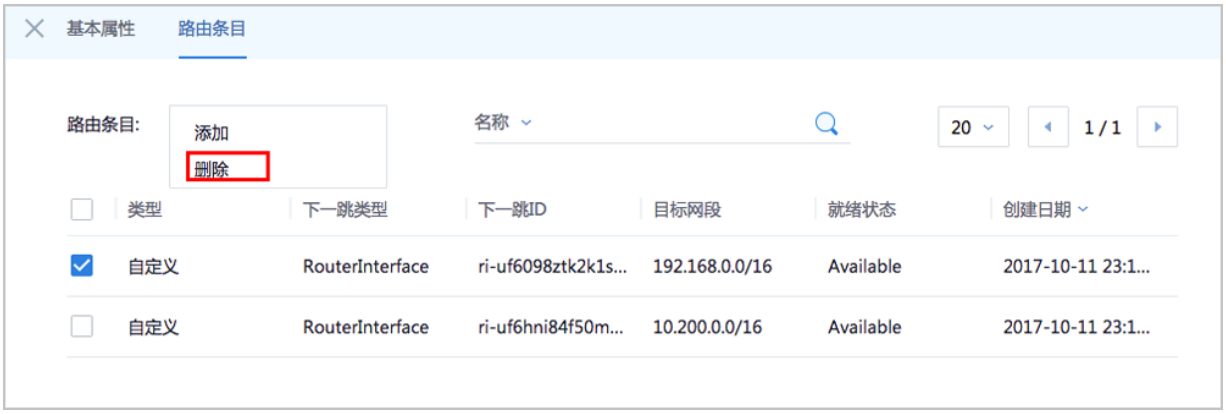
在**路由条目**界面，选择要删除的自定义路由条目，点击**操作 > 删除**，可删除该路由条目。

注:

- 默认同时删除该路由条目的本地记录和阿里云上资源
- 不支持删除系统类型的路由条目

如图 *122: 删除路由条目*所示：

图 122: 删除路由条目



7.8.3 创建高速通道

背景信息

创建高速通道即创建本地数据中心与阿里云之间的物理专线/SD-WAN专线连接。

注:

- 创建高速通道需要提前配置连接环境，详情请参考阿里云高速通道向导或大河高速通道向导。
- 创建高速通道需提前同步或本地创建路由器接口，详情请参考路由器接口。

创建阿里云高速通道的2个入口：

- 支持从操作向导创建阿里云高速通道；
- 在专有网络VPC下创建阿里云高速通道，配置路由条目，并创建高速通道网络拓扑图。

创建大河高速通道的2个入口：

- 首次创建大河高速通道建议使用操作向导方式；
- 大河高速通道成功创建后，如需修改相关配置，或打算删除重建，建议进入**SD-WAN** > **大河** > **大河专线**界面进行手动创建。

关于大河高速通道的相关介绍请参考*SD-WAN*章节。

以下以专有网络VPC界面创建阿里云高速通道为例进行说明。

操作步骤

1. 进入创建高速通道界面。

   在**专有网络VPC**界面，选择某一VPC，点击**更多操作** > **创建高速通道**，可在该VPC下创建高速通道。如图 *123: 创建高速通道1*所示：

   图 123: 创建高速通道1

2. 创建高速通道。

   在弹出的**创建高速通道**界面，可参考以下示例输入相应内容：

   - **名称**：设置高速通道名称
   - **简介**：可选项，可留空不填

- **云路由器(ZStack)**：选择本地云路由器
- **公有网络(ZStack)**：可以连接本地和边界路由器的公有网络
- **私有网络(ZStack)**：选择云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网
- **边界路由器(阿里云)**：选择该VPC下的边界路由器，目前由运营商提供
- **CPE IP(运营商)**：运营商提供物理专线到ZStack私有云客户端设备IP地址

如图 *124:* 创建高速通道2所示：

图 124: 创建高速通道2

3. 点击 **确定**，配置高速通道。

   配置高速通道的过程中，系统将自动配置以下四条路由：

   - **VPC自定义路由1**：

     在VPC的虚拟路由器定义目的地址*ZStack*私有网络段的下一跳为VPC路由器接口；

   - **边界路由器自定义路由1**：

     在边界路由器定义目的地址*ZStack*私有网络段的下一跳为边界路由器ZStack侧的路由器接口；

   - **边界路由器自定义路由2**：

     在边界路由器定义目的地址*ECS VPC*网络段的下一跳为边界路由器阿里云侧的路由器接口；

   - **云路由自定义路由1**：

     在云路由器定义路由的目的地址*ECS VPC*网络段的下一跳为客户端CPE设备的IP地址。

4. 在CPE设备配置两条路由条目。

   高速通道配置完成后，终端用户需在CPE设备上自行配置两条路由：

   - **CPE自定义路由1**：

     目的地址为*ZStack*私有网络段的下一跳为云路由器的物理专线IP；

   - **CPE自定义路由2**：

     目的地址为*ECS VPC*网络段的下一跳为专线的地址。

5. 查看高速通道拓扑图。

   在**专有网络VPC**界面，点击某一VPC，进入**专有网络VPC**详情页，点击**拓扑图**，进入**拓扑图**页面，可查看网络拓扑，如所示：

   图 125: 拓扑图

6. 互通验证。

   登录本地云主机，检查是否能够ping通ECS云主机。然后再登录ECS云主机，检查是否能够ping通本地云主机。

后续操作

至此，若验证成功，则阿里云高速通道创建成功，ZStack私有云数据中心到阿里云的VPC即可实现网络互通。

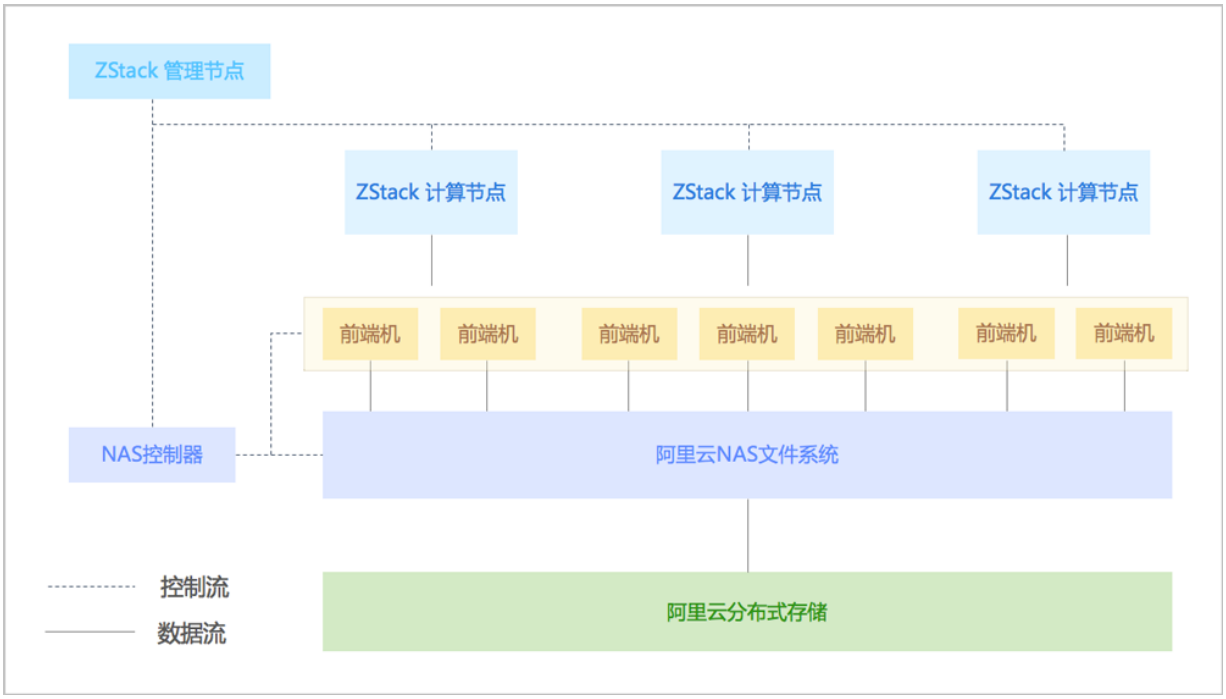
7.9 阿里云NAS

阿里云NAS（Network Attached Storage），是阿里云提供的网络文件存储服务，通过标准的文件访问协议，用户即可使用具备无限容量及性能扩展、单一命名空间、多共享、高可靠和高可用等特性的分布式文件系统。

ZStack无缝对接阿里云NAS，在ZStack私有云环境下，用户可通过添加**AliyunNAS**类型主存储的方式直接采用独立部署的阿里云盘古分布式存储。

ZStack无缝对接阿里云NAS的示意图如图 *126: ZStack无缝对接阿里云NAS*所示：

图 126: ZStack无缝对接阿里云NAS



ZStack通过**IaaS+NAS**的无缝对接，将阿里云分布式存储能力加载到私有云，提供了一种全新的虚拟化分布式存储方案。

AliyunNAS主存储需匹配ImageStore类型镜像服务器使用，并需提前在ZStack混合云界面进行相关配置，包括：设置阿里云服务网关、添加相应AK、创建阿里云NAS文件系统，以及创建权限组和权限规则，为文件系统设置访问白名单机制。

AliyunNAS主存储的优点

AliyunNAS类型主存储具有以下优点：

- **易扩展**

  基于分布式架构特性，计算节点和存储节点可分别按需扩展，支持无限扩容；

- **高性能**

  基于分布式架构特性，整体存储性能支持水平扩展；

- **易用性**

  通过一套UI界面的简单几步操作，快捷添加**AliyunNAS**主存储，添加成功后可以像使用其它主存储一样用于云主机和云盘，无学习成本；

- **高可靠**

  提供11个9的数据可靠性，相比自建文件存储，可大幅节约维护成本，降低数据安全风险。

AliyunNAS主存储的基本部署流程

AliyunNAS主存储的基本部署流程如下：

1. ZStack混合云界面相关配置。

   首次添加**AliyunNAS**主存储，需在ZStack混合云界面进行相关配置：

   1. 设置阿里云服务网关；
   2. 添加阿里专有云AccessKey，添加阿里云NAS文件系统所在阿里专有云地域；
   3. 创建阿里云NAS文件系统，作为**AliyunNAS**主存储的后端存储；
      - 若用户在阿里专有云数据中心已部署阿里云NAS文件系统，可直接添加到ZStack混合云平台；
      - 用户也可在ZStack混合云界面创建阿里云NAS文件系统；
      - 详情请见创建文件系统章节。
   4. 创建权限组和权限组规则，为文件系统设置访问白名单机制。
      - 若用户在阿里专有云数据中心已创建经典网络类型的权限组，并向权限组添加相应规则，可直接将该权限组添加到ZStack混合云平台；
      - 用户也可在ZStack混合云界面创建权限组和权限组规则；
      - 详情请见创建权限组和创建权限组规则章节。
2. ZStack私有云界面添加**AliyunNAS**主存储。
3. 管理**AliyunNAS**主存储。

AliyunNAS主存储的详细部署教程请参考*AliyunNAS主存储 部署实践*章节。

7.9.1 文件系统

阿里云NAS文件系统作为**AliyunNAS**类型主存储的后端存储，用户在添加**AliyunNAS**主存储前，需在ZStack混合云界面创建阿里云NAS文件系统。

创建文件系统

在ZStack混合云主菜单，点击**产品** > **阿里云NAS** > **文件系统**，进入**文件系统**界面，点击**创建文件系统**，弹出**创建文件系统**界面，可参考以下示例输入相应内容：

- **地域**：选择阿里云NAS文件系统所在阿里专有云地域
- **选择方式**：可选择添加已有文件系统或创建文件系统
  - **添加已有**：

若用户在阿里专有云数据中心已部署阿里云NAS文件系统，可直接添加到ZStack混合云平台。

选择添加已有文件系统，需设置以下内容：

- **文件系统**：将已部署的阿里云NAS文件系统添加到ZStack混合云平台
- **名称**：设置文件系统名称
- **简介**：可选项，可留空不填

如图 *127: 添加已有文件系统*所示：

图 127: 添加已有文件系统

- **创建**：

用户也可在ZStack混合云界面创建阿里云NAS文件系统。

选择创建文件系统，需设置以下内容：

- **名称**：设置文件系统名称
- **简介**：可选项，可留空不填
- **存储类型**：可选择容量型（Capacity）或性能型（Performance）
- **协议类型**：支持标准的NFS、SMB文件访问协议

如图 *128:* 创建文件系统所示：

图 128: 创建文件系统

文件系统支持的操作

文件系统支持以下操作：

- 创建文件系统：添加/创建阿里云NAS文件系统，作为**AliyunNAS**主存储的后端存储

- 删除：删除文件系统
  - 若该文件系统已作为**AliyunNAS**主存储的后端存储，不允许删除
  - 若该文件系统未作为**AliyunNAS**主存储的后端存储，可进行删除
  - 删除文件系统，将同时删除本地记录和阿里专有云数据中心部署的真实资源，请谨慎操作
- 修改名称和简介：修改文件系统名称和简介

7.9.2 权限组

权限组是一个白名单机制，通过向权限组内添加规则，来允许指定的IP地址或网段访问文件系统，并可为不同的IP地址或网段授予不同级别的访问权限。

创建权限组

在ZStack混合云主菜单，点击**产品** > **阿里云NAS** > **权限组**，进入**权限组**界面，点击**创建权限组**，弹出**创建权限组**界面，可参考以下示例输入相应内容：

- **地域**：选择阿里云NAS文件系统所在阿里专有云地域
- **选择方式**：可选择添加已有权限组或创建权限组
  - **添加已有**：

    若用户在阿里专有云数据中心已创建权限组，可直接将该权限组添加到ZStack混合云平台。

    注: 仅支持添加经典网络类型的权限组。

    如选择添加已有权限组，需设置以下内容：

    - **权限组**：将已创建的经典网络类型的权限组添加到ZStack混合云平台
    - **名称**：设置权限组名称
    - **简介**：可选项，可留空不填

    如图 *129: 添加已有权限组*所示：

    图 129: 添加已有权限组

- **创建**：

  用户也可在ZStack混合云界面创建权限组。

  注: 仅支持创建经典网络类型的权限组。

  如选择创建权限组，需设置以下内容：

  - **名称**：设置权限组名称
  - **简介**：可选项，可留空不填
  - **网络类型**：默认显示经典网络（classic）

  如图 *130: 创建权限组*所示：

  图 130: 创建权限组

创建权限组规则

- 若用户在阿里专有云数据中心已创建经典网络类型的权限组，并向权限组添加相应规则，将该权限组添加到ZStack混合云平台，权限组内相应规则自动同步到本地。
- 用户也可在ZStack混合云界面创建权限组规则。

在**权限组**界面，选中某一权限组，展开其详情页，进入**权限组规则**子页面，点击权限组规则右侧的**操作** > **创建权限组规则**按钮，弹出**创建权限组规则**界面，可参考以下示例输入相应内容：

- **网络CIDR**：本条规则的授权对象，可指定单个IP地址或网段
- **优先级**：优先级范围为**1-100**，**1**为最高优先级

  注: 当同一个授权对象匹配到多条规则时，高优先级规则将覆盖低优先级规则。

- **读写规则**：允许授权对象对文件系统进行只读操作（RDONLY）或读写操作（RDWR）

如图 *131:* 创建权限组规则所示：

图 131: 创建权限组规则

权限组支持的操作

权限组支持以下操作：

- 创建权限组：添加/创建权限组，为文件系统设置访问白名单机制
- 删除：删除权限组
  - 若该权限组作用的文件系统已作为**AliyunNAS**主存储的后端存储，不允许删除
  - 若该权限组作用的文件系统未作为**AliyunNAS**主存储的后端存储，可进行删除
  - 删除权限组，将同时删除本地记录和阿里专有云数据中心创建的真实资源，请谨慎操作
- 修改名称和简介：修改权限组名称和简介
- 创建权限组规则：向权限组内添加规则，来允许IP地址或网段以不同的权限访问文件系统

  注: 为了最大限度保障数据安全，强烈建议谨慎添加权限组规则，仅为必要的地址授权。
- 删除权限组规则：删除权限组规则，将同时删除本地记录和阿里专有云数据中心创建的真实资源，请谨慎操作

8 数据中心

数据中心涉及了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。

8.1 地域

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。

ZStack地域支持以下操作：

- 地域管理
- Bucket管理
- 可用区管理

8.1.1 地域管理

地域管理支持对地域进行以下操作：

- 添加地域
- 删除地域

添加地域

添加地域，即添加用户想要创建ECS的地区。

所添加的地域与当前AccessKey对应。需添加地域后，才可同步当前AccessKey对应账户的地域下的资源。

ZStack支持多个AccessKey的地域管理。

以下分别介绍添加阿里云地域、阿里专有云地域。

- 添加阿里云地域

  在ZStack混合云主菜单，点击**数据中心** > **地域**，进入**地域**界面，点击**添加地域**，弹出**添加地域**界面，可参考以下示例输入相应内容：

  - **阿里云**：选择添加阿里云地域
  - **地域**：选择阿里云AccessKey中的地域
  - **简介**：所选地域简介（不可留空）

  如图 *132:* 添加阿里云地域所示：

  图 132: 添加阿里云地域

- 添加阿里专有云地域
  - 添加阿里专有云地域-AliyunNAS

    在ZStack混合云主菜单，点击**数据中心 > 地域**，进入**地域**界面，点击**添加地域**，弹出**添加地域**界面，可参考以下示例输入相应内容：

    - **阿里专有云**：选择添加阿里专有云地域
    - **地域**：选择阿里专有云AccessKey中的地域
    - **简介**：所选地域简介（不可留空）
    - **类型**：选择阿里专有云地域的类型：AliyunNAS

    如图 *133: 添加阿里专有云地域-AliyunNAS*所示：

    图 133: 添加阿里专有云地域-AliyunNAS

- 添加阿里专有云地域-AliyunEBS

  在ZStack混合云主菜单，点击**数据中心** > **地域**，进入**地域**界面，点击**添加地域**，弹出**添加地域**界面，可参考以下示例输入相应内容：

  - **阿里专有云**：选择添加阿里专有云地域
  - **地域**：输入阿里专有云AccessKey中的地域
  - **简介**：所选地域简介（不可留空）
  - **类型**：选择阿里专有云地域的类型：AliyunEBS
  - **Endpoint**：输入Ocean对外服务的访问域名

    注:

    - Ocean以HTTP RESTful API形式对外提供服务；
    - 输入格式为：*http://Ocean_Server_Domain:Port/ocean/api*；
    - 访问不同地域时需要不同的域名。

  如图 *134: 添加阿里专有云地域-AliyunEBS*所示：

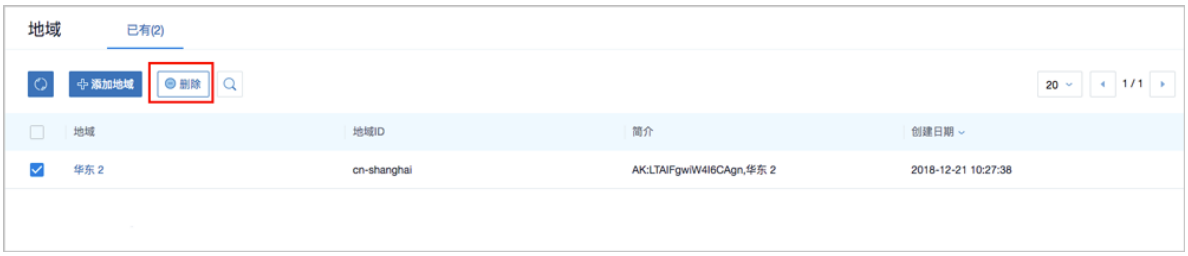
  图 134: 添加阿里专有云地域-AliyunEBS

删除地域

删除地域，表示此地域将不再被ZStack管理，此地域下的所有记录会从本地移除，再次添加可同步回来。

1. 在**地域**界面，选择某一地域，点击**删除**，可删除该地域，如图 *135:* 删除地域所示：

图 135: 删除地域



2. 弹出**删除地域**确认窗口，如图 *136:* 删除地域确认窗口所示。

图 136: 删除地域确认窗口

8.1.2 Bucket管理

对象存储OSS承担了本地私有云云主机镜像到阿里云ECS云主机实例创建前的存储。上传本地镜像依赖OSS里的Bucket作为中转，再上传至阿里云作为自定义镜像。

Bucket支持以下操作：

- 添加Bucket
- 将Bucket设为默认
- 删除Bucket

添加Bucket

1. 在**地域**界面，点击某一地域，进入**地域**详情页，点击**Bucket**，进入**Bucket**页面，点击**操作 > 添加Bucket**，可添加Bucket，如图 *137: Bucket界面*所示：

   图 137: Bucket界面

2. 弹出**添加Bucket**界面，可参考以下示例输入相应内容：

   - 选择已有Bucket：

     - **选择已有**：选择添加该地域下的已有Bucket

- **OSS Domain**：输入OSS对外服务的访问域名

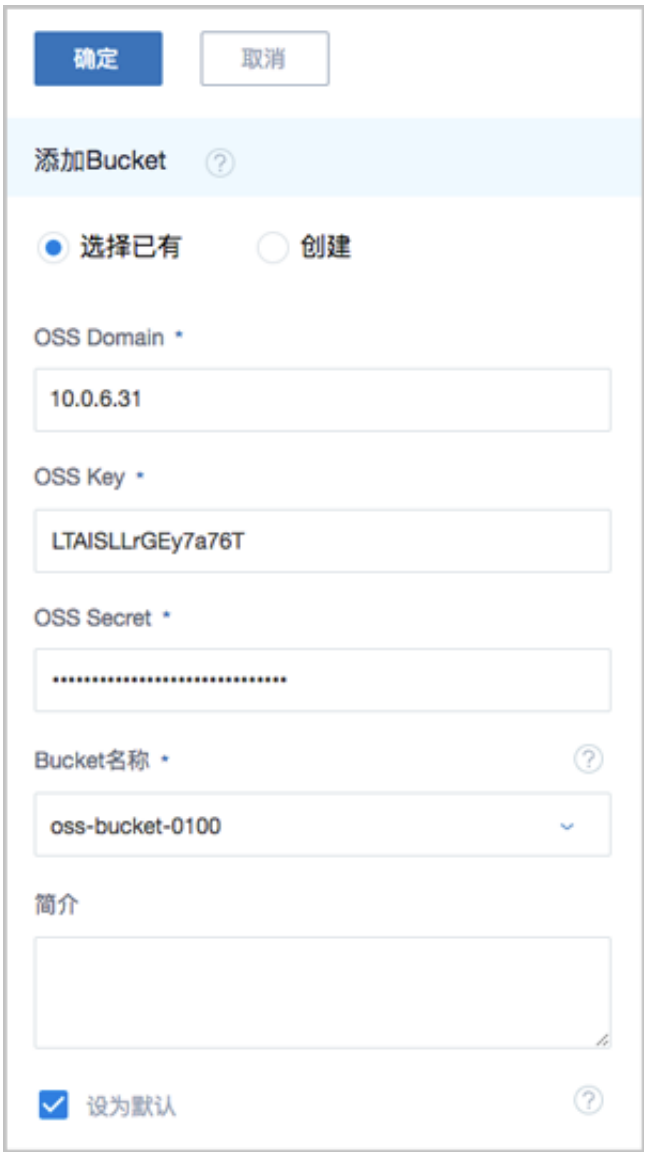
  注:

  - OSS以HTTP RESTful API形式对外提供服务；
  - 输入格式为：*OSS_Server_Domain*；
  - 访问不同地域时需要不同的域名。

- **OSS Key**：输入OSS的AccessKey ID，注意确保正确
- **OSS Secret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确
- **Bucket名称**：下拉菜单显示了所选地域下全部已有Bucket列表，可从中选择一个
- **简介**：可选项，可留空不填
- **设为默认**：是否设为默认，添加Bucket时，默认勾选此项

如图 *138: 选择已有Bucket*所示：

图 138: 选择已有Bucket



- 创建Bucket：
  - **创建**：选择在该地域下创建Bucket
  - **OSS Domain**：输入OSS对外服务的访问域名

    注:

    - OSS以HTTP RESTful API形式对外提供服务；
    - 输入格式为：*OSS_Server_Domain*；
    - 访问不同地域时需要不同的域名。
  - **OSS Key**：输入OSS的AccessKey ID，注意确保正确
  - **OSS Secret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确
  - **Bucket名称**：设置Bucket名称，Bucket名称全局唯一，不可重复

- **简介**：可选项，可留空不填
- **设为默认**：是否设为默认，添加Bucket时，默认勾选此项

如图 *139: 创建Bucket*所示：

图 139: 创建Bucket

将Bucket设为默认

在**地域**界面，点击某一地域，进入**地域**详情页，点击**Bucket**，进入**Bucket**页面，选择某一Bucket，点击**操作** > **设为默认**，可将该Bucket设为默认。

注: 每个地域仅有一个Bucket可被设置为默认，表示默认选择此Bucket来上传本地镜像。

如图 *140: 将Bucket设为默认*所示：

图 140: 将Bucket设为默认

删除Bucket

1. 在**地域**界面，点击某一地域，进入**地域**详情页，点击**Bucket**，进入**Bucket**页面，选择某一Bucket，点击**操作** > **删除**，可删除该Bucket，如图 *141: 删除Bucket*所示：

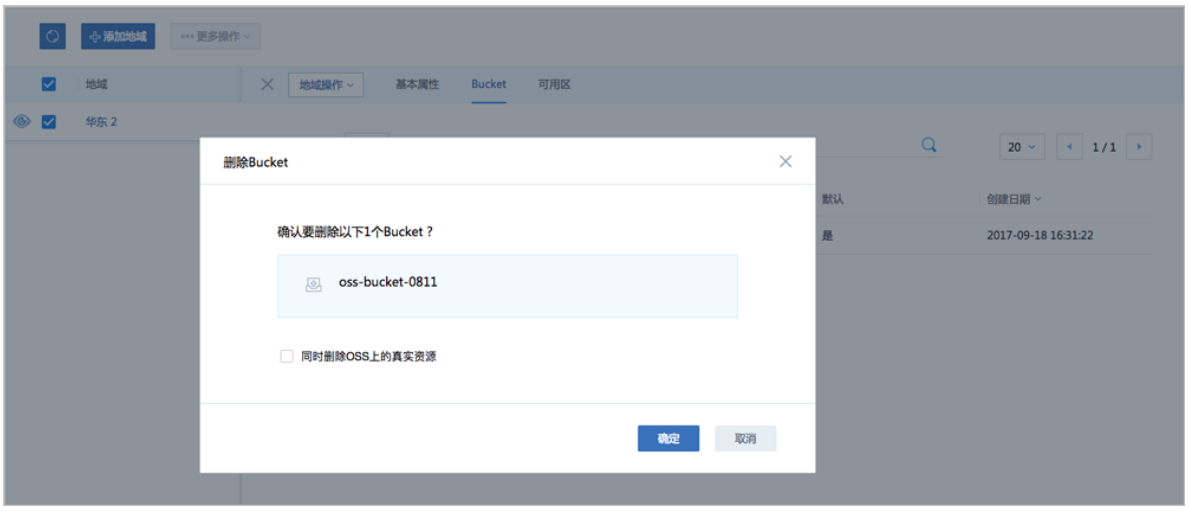
   图 141: 删除Bucket

2. 弹出**删除Bucket**确认窗口，如图 *142: 删除Bucket确认窗口*所示。

   注: 默认只删除本地记录，如需同时删除OSS上的真实Bucket，请勾选同时删除OSS上的真实资源。

   图 142: 删除Bucket确认窗口



8.1.3 可用区管理

ZStack支持对地域中的可用区进行以下操作：

- 将可用区添加到地域
- 删除地域中的可用区

添加可用区

1. 在**地域**界面，点击某一地域，进入**地域**详情页，点击**可用区**，进入**可用区**页面，点击**操作** > **添加**，可添加该地域可用区，如图 *143:* 可用区界面所示：

   图 143: 可用区界面

2. 弹出**添加可用区**界面，可参考以下示例输入相应内容：
   - **可用区**：下拉菜单显示了所选地域下全部可用区列表，可从中选择一个
   - **简介**：所选可用区简介（不可留空）

如图 *144: 添加可用区*所示：

图 144: 添加可用区

删除可用区

删除可用区，表示此可用区将不再被ZStack管理，此可用区下的所有记录会从本地移除，再次添加可同步回来。

在**地域**界面，点击某一地域，进入**地域**详情页，点击**可用区**，进入**可用区**页面，选择某一可用区，点击**操作** > **删除**，可删除该可用区。

如图 *145: 删除可用区*所示：

图 145: 删除可用区

8.2 可用区

可用区对应了阿里云的Zone可用区，主要是指同一地域内，电力和网络互相独立的物理地域。

可用区在ZStack中被定义为一个独立可用区；一个可用区属于唯一的一个数据中心。具体到阿里云中，就是一个独立可用区，它属于唯一的一个地域。

可用区在阿里云中不是对等的，也不是静态的，即：可用区可能增加或减少（库存为0，或可用区搬迁即减少），但终端用户的ECS云主机一定属于某个可用区，因此需要将可用区添加到ZStack中来。

ZStack可用区支持以下操作：

- 添加可用区
- 删除可用区
- 可用区下的虚拟交换机管理
- 可用区下的ECS云主机管理

添加可用区

添加可用区，即添加某个可用区到某个地域。

所添加的可用区与当前AccessKey对应。需添加可用区后，才可同步当前AccessKey对应账户的可用区下的资源。

ZStack支持多个AccessKey的可用区管理。

1. 在ZStack混合云主菜单，点击**数据中心** > **可用区**，进入**可用区**界面，如图 *146:* 可用区界面所示：

   图 146: 可用区界面

2. 点击**添加可用区**，弹出**添加可用区**界面，可参考以下示例输入相应内容：

   - **地域**：选择AccessKey中的地域
   - **可用区**：下拉菜单显示了所选地域下全部可用区列表，可从中选择一个
   - **简介**：所选可用区简介（不可留空）

如图 *147: 添加可用区*所示：

图 147: 添加可用区

删除可用区

删除可用区，表示此可用区将不再被ZStack管理，此可用区下的所有记录会从本地移除，再次添加可同步回来。

在**可用区**界面，点击某个可用区，点击**删除**，可删除该可用区。

如图 *148: 删除可用区*所示：

图 148: 删除可用区

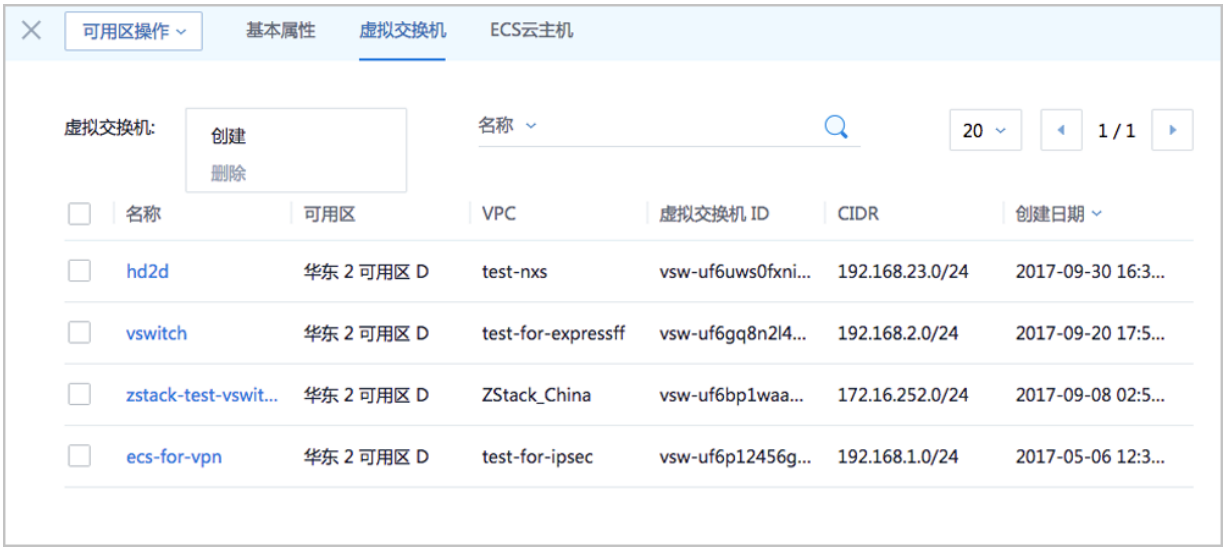
可用区下的虚拟交换机管理

在**可用区**界面，点击某一可用区，进入**可用区**详情页，点击**虚拟交换机**，进入**虚拟交换机**页面，可查看该可用区下的虚拟交换机列表，支持对相关虚拟交换机进行以下操作：

- 创建虚拟交换机
- 删除虚拟交换机
- 修改虚拟交换机名称和简介
- 基于虚拟交换机创建的ECS云主机管理

如图 *149:* 虚拟交换机管理所示：

图 149: 虚拟交换机管理



可用区下的ECS云主机管理

在**可用区**界面，点击某一可用区，进入**可用区**详情页，点击**ECS云主机**，进入**ECS云主机**页面，可查看该可用区下的ECS云主机列表，支持对相关ECS云主机进行以下操作：

- 启动、停止ECS云主机
- 重启ECS云主机
- 打开控制台
- 设置ECS控制台密码
- 删除ECS云主机
- 修改ECS云主机名称和简介
- 加载云盘

- 卸载云盘

如图 *150: ECS云主机管理*所示：

图 150: ECS云主机管理

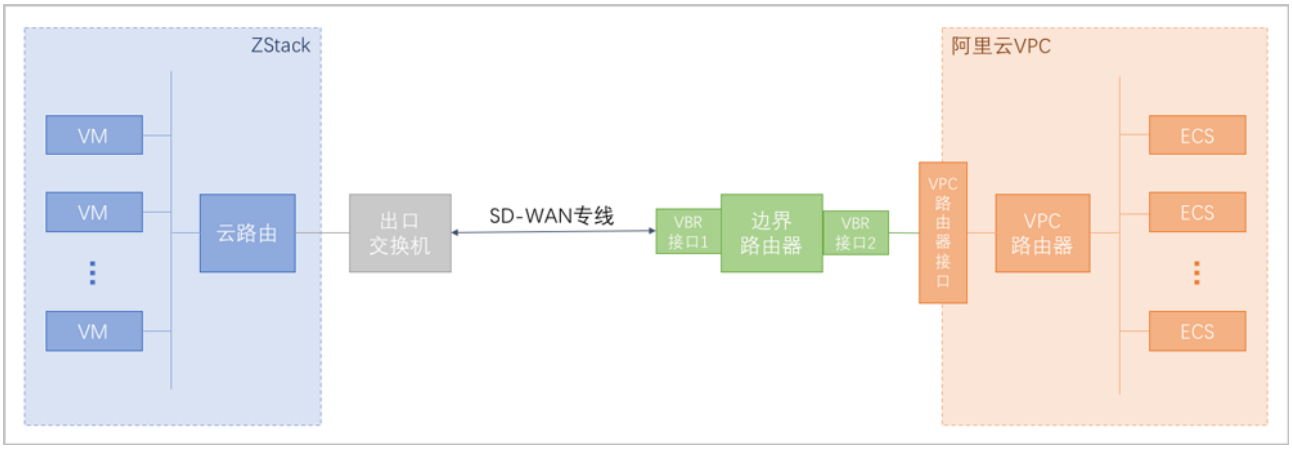
9 SD-WAN

大河高速通道，主要指通过大河专线（即通过集成大河云联提供的标准化开放API，ZStack混合云平台无缝接入DAHO Fabric自服务平台，使用其提供的SD-WAN专线服务），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。

注: 从本地云路由到阿里云端VPC网络，高速通道准备互通的各网络段不可重叠！

大河高速通道网络架构如图 *151:* 大河高速通道网络架构图所示：

图 151: 大河高速通道网络架构图



大河高速通道具有以下优点：

- 快捷部署：通过一套UI界面的简单几步操作，快捷部署全部网络。
- 秒级调整：平台内部自动调度广域网资源，秒级调整带宽以及线路连通性，灵活应对上层业务变动需求。
- 安全可靠：不同用户链路互相隔离，且支持监控网络实时流量和健康状况，某条线路发生故障可自动切换，实现智能调度。
- 灵活计费：根据业务需要可灵活选择带宽和SLA（Service-Level Agreement，服务等级协议），较之传统专线的包年包月计费模式进一步节约用户成本。

SD-WAN支持的操作

SD-WAN支持以下操作：

- 同步大河公网连接：支持从大河端同步大河公网连接到本地，实现大河公网连接的管理。
- 同步大河本地连接：支持从大河端同步大河本地连接到本地，实现大河本地连接的管理。
- 创建/删除大河专线：支持创建、删除大河专线。
  - 首次创建大河高速通道建议使用操作向导方式；
  - 大河高速通道成功创建后，如需修改相关配置，或打算删除重建，建议进入**SD-WAN** > **大河** > **大河专线**界面进行手动创建。

9.1 大河公网连接

大河公网连接：大河端提供的公有云侧连接。

- 通常各大公有云厂商会在全国各地部署一些接入点，例如：阿里云在上海虹桥、上海浦东等地均有接入点，主要用于IDC机房接入公有云环境；
- 当用户网络接入某个接入点后，可视为连通了公有云内部的专线网络；
- 大河将该接入点映射到自己的系统中，成为一个虚拟接入点，即为大河公网连接。

大河公网连接应由大河配置。ZStack混合云SD-WAN支持从大河端同步大河公网连接到本地。

同步大河公网连接

同步大河公网连接，即同步指定地域下大河端提供的公网连接接入点。

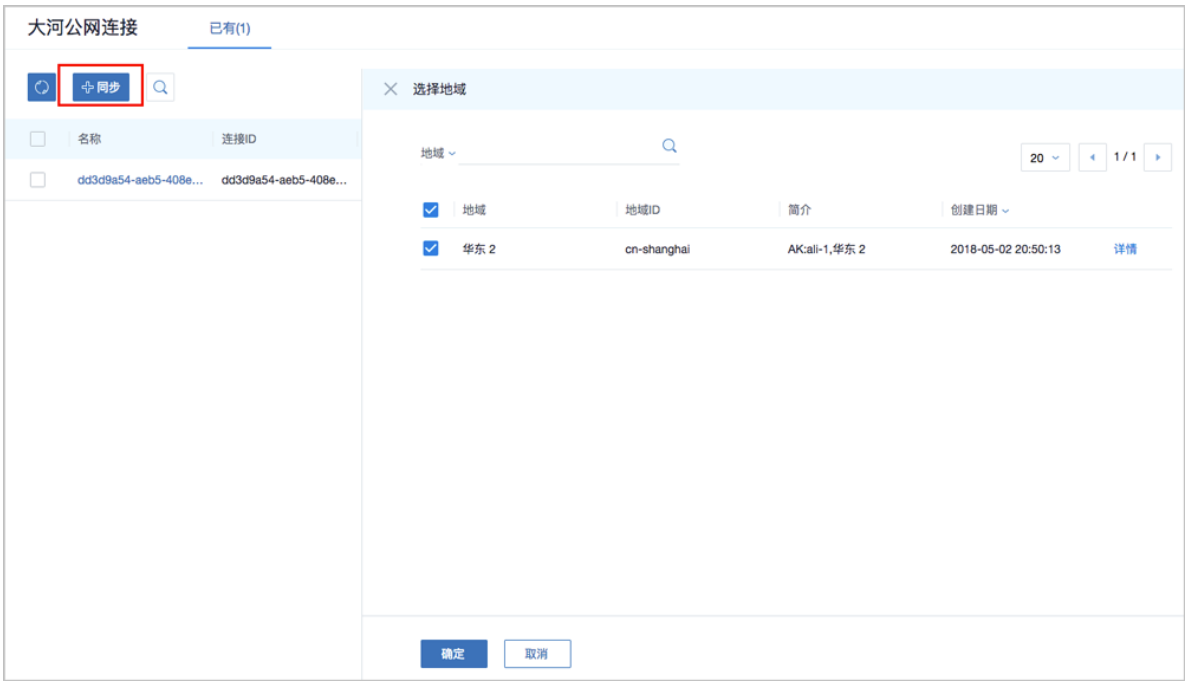
1. 在ZStack混合云主菜单，点击**SD-WAN** > **大河** > **大河公网连接**，进入**大河公网连接**界面，如图 *152:* 大河公网连接界面所示：

   图 152: 大河公网连接界面

2. 点击**同步**按钮，弹出**选择地域**列表，可在阿里云AK相关地域列表中选择目标地域，将指定地域下的大河公网连接同步到本地，如图 *153:* 选择地域所示：

   图 153: 选择地域



修改大河公网连接名称、简介

在**大河公网连接**界面，点击某一大河公网连接，进入**大河公网连接**详情页，在**基本属性**子页面，可修改大河公网连接的名称和简介。

9.2 大河本地连接

大河本地连接：大河端提供的本地侧连接。

- 大河云联在全国各地建设有多个POP接入点，用于用户网络最后一公里的接入；
- 当用户网络接入某个接入点后，可视为连通了大河专线网络，即为大河本地连接。

大河本地连接应由大河配置。ZStack混合云SD-WAN支持从大河端同步大河本地连接到本地。

同步大河本地连接

同步大河本地连接，即同步指定地域下大河端提供的本地连接接入点。

1. 在ZStack混合云主菜单，点击**SD-WAN** > **大河** > **大河本地连接**，进入**大河本地连接**界面，如图 *154: 大河本地连接界面*所示：

图 154: 大河本地连接界面

2. 点击**同步**按钮，可将大河AK相关地域下的大河本地连接同步到本地。

修改大河本地连接名称、简介

在**大河本地连接**界面，点击某一大河本地连接，进入**大河本地连接**详情页，在**基本属性**子页面，可修改大河本地连接的名称和简介。

9.3 大河专线

大河专线：在大河公网连接和大河本地连接之间可搭建一条或多条虚拟专线线路，即为大河专线。

ZStack混合云SD-WAN支持：

- 创建大河专线
- 删除大河专线

注:

- 首次创建大河高速通道建议使用操作向导方式；
- 大河高速通道成功创建后，如需修改相关配置，或打算删除重建，建议进入**SD-WAN** > **大河** > **大河专线**界面进行手动创建。

创建大河专线

在**大河专线**界面，点击**创建大河专线**，弹出**创建大河专线**界面。

1. 创建大河专线。

   可参考以下示例输入相应内容：

   - **名称**：设置大河专线名称
   - **简介**：可选项，可留空不填
   - **VLAN(大河)**：设置VLAN ID号，需与本地出口交换机二层互通
   - **带宽**：设置大河专线的带宽，单位为Mbps
   - **到期策略**：可选项，所购买的大河专线服务到期后是否续期，有两种到期策略可选：shutdown（服务到期后停止续期）、renewal（服务到期后自动续期）

- **大河公网连接**：选择大河端提供的公有云侧连接
- **大河本地连接**：选择大河端提供的本地侧连接

如图 *155:* 创建大河专线所示，点击**下一步**。

图 155: 创建大河专线

大河专线配置完成同时，大河在阿里云端自动购买创建一个边界路由器，以及边界路由器在ZStack侧的路由器接口（VBR接口1），该边界路由器以及路由器接口自动同步至本地。

2. 修改互联地址。

将已准备的一对互联地址：*10.255.255.221*（ZStack私有云端）和*10.255.255.222*（阿里云端）输入边界路由器。可参考以下示例输入相应内容：

- **阿里云端网关**：输入*10.255.255.222*到边界路由器，作为阿里云端网关
- **ZStack私有云端网关**：输入*10.255.255.221*到边界路由器，作为ZStack私有云端网关
- **子网掩码**：设置边界路由器的子网掩码，使阿里云端网关和ZStack私有云端网关可以互通

如图 *156:* 修改互联地址所示，点击**下一步**。

图 156: 修改互联地址

3. 创建路由器接口。

配置一对路由器接口，即：边界路由器在阿里云侧的路由器接口（VBR接口2），以及相应的阿里云VPC虚拟路由器接口。可参考以下示例输入相应内容：

- **名称**：设置这一对路由器接口名称
- **简介**：可选项，可留空不填
- **规格**：可选项，设置边界路由器在阿里云侧路由器接口（VBR接口2）的带宽规格
- **地域**：选择相应的阿里云VPC虚拟路由器所在地域
- **边界路由器**：选择相应的边界路由器
- **专有网络VPC(阿里云)**：选择相应的阿里云VPC

- **接入点**：选择边界路由器在阿里云侧路由器接口（VBR接口2）的接入点
- **云路由(ZStack)**：选择本地云路由器

如图 *157:* 创建路由器接口所示，点击**确定**。

图 157: 创建路由器接口

创建大河高速通道过程中，ZStack将自动配置以下4条路由：

- VPC虚拟路由器自定义路由：目的地址为ZStack私有网络段，下一跳为VPC虚拟路由器接口；
- 边界路由器自定义路由1：目的地址为ZStack私有网络段，下一跳为边界路由器ZStack侧的路由器接口（VBR接口1）；
- 边界路由器自定义路由2：目的地址为ECS VPC网络段，下一跳为边界路由器阿里云侧的路由器接口（VBR接口2）；
- 本地云路由自定义路由：目的地址为ECS VPC网络端，下一跳为阿里云端网关*10.255.255.222*。

4. 互通验证。

   登录本地云主机，检查是否能够ping通ECS云主机。然后再登录ECS云主机，检查是否能够ping通本地云主机。

删除大河专线

在**大河专线**界面，选择某一大河专线，点击**更多操作** > **删除**，可删除该大河专线。

如图 *158: 删除大河专线*所示：

图 158: 删除大河专线

10 设置

在ZStack混合云主菜单，点击**设置**，进入**设置**界面，如图 *159:* 设置所示：

图 159: 设置

ZStack混合云包括以下设置：

- **GC清理时间间隔**：

  默认为3600，单位为秒，用于设置阿里云EBS主存储清理云盘垃圾数据的时间间隔。
- **快照导入导出超时时间**：

  默认为10800000，单位为毫秒，用于设置阿里云EBS主存储快照的导入导出的超时上限。
- **Ping间隔**：

  默认为180，单位为秒，用于设置管理节点在指定的时间间隔去检查阿里云EBS主存储是否连接。
- **GC清理时间间隔**：

  默认为3600，单位为秒，用于设置阿里云NAS主存储清理云盘垃圾数据的时间间隔。
- **Ping间隔**：

  默认为180，单位为秒，用于设置管理节点在指定的时间间隔去检查阿里云NAS主存储是否连接。
- **阿里云控制台访问地址**：

  默认为aliyuncs.com:443，用于设置阿里云控制台访问地址。混合云添加AK时，需要检测用户的管理节点网络是否连通阿里云控制台。
- **阿里云控制台连通检测超时**：

  默认为500，单位为毫秒，用于设置用户的管理节点与阿里云控制台连通检测的超时上限。混合云添加AK时，需要检测管理节点网络是否连通阿里云控制台，如果管理节点在指定时间内没有成功连通阿里云控制台，则添加AK失败。
- **允许接管的阿里云地域列表**

  默认为cn-shenzhen,cn-beijing,cn-shanghai,cn-hangzhou,cn-zhangjiakou,cn-qingdao,cn-huhehaote。用于设置云平台允许接管的阿里云地域（Region）列表，每个地域间用逗号隔开。

- **自定义镜像上传格式**：

  默认为raw，用于设置混合云上传自定义镜像的格式，目前只支持qcow2和raw两种格式。
- **阿里云服务网关**：

  用于设置用户自定义网关，格式为：

  oss::http://oss.api.com,ecs::ecs.api.com,nas::nas.endpoint.com
- **大河服务网关**：

  用于设置大河服务网关，用户设置该网关后，才能够在SD-WAN中创建大河专线。
- **管理节点时区**：

  用于设置管理节点时区，默认为**CHINA**，OpenAPI调用的终端地址的时区。

11 典型场景实践

11.1 混合云互通实践

实现企业本地数据中心的私有云云主机与阿里云ECS云主机互通，才是混合云的精髓。

目前ZStack混合云支持以下两种方式实现**本地-远程**网络互联：

- **IPsec VPN**：使用企业本地的公网IP和阿里云提供的VPN网关进行IPsec VPN互通。
- **高速通道**：使用物理专线/SD-WAN配置高速通道进行网络互通。

11.1.1 IPsec VPN实践

背景信息

ZStack支持IPsec VPN方式实现本地云路由网络与阿里云VPN网络的互通。

搭建IPsec VPN通道的基本流程如下：

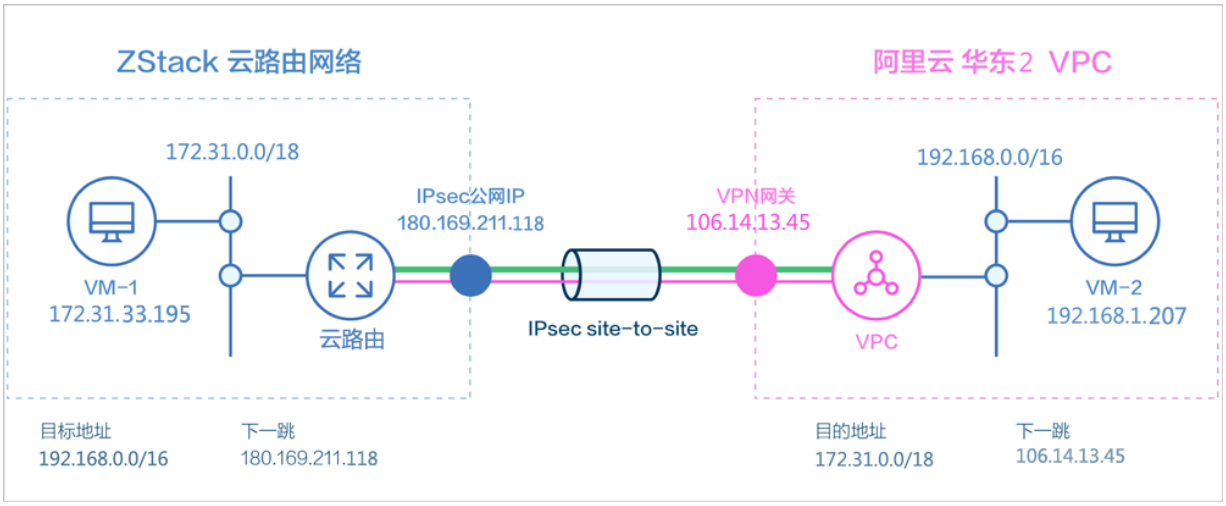
1. 在ZStack混合云界面按照顺序创建地域、可用区、专有网络VPC和VPC下的虚拟交换机。
2. 在阿里云控制台购买VPN网关。
3. 使用云路由网络创建私有云云主机。
4. 创建ECS云主机。
5. 利用操作向导快速创建阿里云VPN连接。
6. 验证本地云主机与ECS云主机是否可以ping通，如能ping通，IPsec VPN通道创建成功。

IPsec VPN通道设计思想：使用IPsec公网IP作为阿里云VPN用户网关，连通到阿里云VPN网关，再连通到阿里云内网。

注: 从本地云路由到阿里云端VPN网络，IPsec准备互通的各网络段不可重叠！

IPsec VPN网络架构如图 *160: IPsec VPN网络架构图*所示：

图 160: IPsec VPN网络架构图



假定客户环境如下：

1. 公有网络

表 1: 公有网络配置信息

公有网络	配置信息
网卡	eth0
VLAN ID	3
IP地址段	*180.169.211.117~180.169.211.118*
子网掩码	*255.255.255.240*
网关	*180.169.211.113*

2. 管理网络

表 2: 管理网络配置信息

管理网络	配置信息
网卡	eth0
VLAN ID	非VLAN
IP地址段	*172.20.58.50~172.20.58.59*
子网掩码	*255.255.0.0*
网关	*172.20.0.1*

3. 私有网络

表 3: 私有网络配置信息

私有网络	值
网卡	eth0
VLAN ID	1982
IP CIDR	*172.31.0.0/18*

4. 已购买的阿里云VPN网关IP地址为*106.14.13.45*
5. 阿里云VPN网关所在的VPC的CIDR为*192.168.0.0/16*

准备工作：

- 在ZStack混合云平台按照顺序创建地域、可用区、专有网络VPC和VPC下的虚拟交换机。详情可参考地域管理、可用区管理、专有网络*VPC*管理和虚拟交换机管理章节。
- ZStack私有云需要完成基本的初始化，包括区域、集群、物理机、镜像服务器、主存储等基本资源的添加。详情可参考用户手册*Wizard*引导设置章节。

以下介绍ZStack云路由环境搭建IPsec VPN通道的实践步骤。

操作步骤

1. 在ZStack私有云界面创建L2-公有网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *1:* 公有网络配置信息填写如下：

   - **名称**：设置L2-公有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2VlanNetwork
   - **Vlan ID**：3
   - **网卡**：eth0
   - **集群**：选择集群，如Cluster-1

   如图 *161:* 创建*L2*-公有网络所示，点击**确定**，创建L2-公有网络。

   图 161: 创建L2-公有网络

2. 在ZStack私有云界面创建L3-公有网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述表 *1:* 公有网络配置信息填写如下：

   - **名称**：设置L3-公有网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-公有网络
   - **网络服务**：选择是否需要DHCP服务

- **添加网络段**：选择网络地址类型和方法添加网络段，网络地址类型包括：IPv4、IPv6；添加方法包括：IP范围、CIDR
  - 若选择IPv4类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
    - **起始IP**：*180.169.211.117*
    - **结束IP**：*180.169.211.118*
    - **子网掩码**：*255.255.240.0*
    - **网关**：*180.169.211.113*

    如图 *162: IPv4*类型通过*IP*范围方式添加网络段所示：

    图 162: IPv4类型通过IP范围方式添加网络段

- 若选择IPv4类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **CIDR**：输入网络段的CIDR。例如：*192.168.1.1/24*
- 若选择IPv6类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP
  - **起始IP**：输入网络段的起始IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2002*
  - **结束IP**：输入网络段的结束IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2200*

- **前缀长度**：输入网络段的前缀长度，范围：64-126
- **网关**：输入网络段的网关。例如：*CDCD:910A:2222:5498:8475:1111:3900:2001*

如图 *163: IPv6类型通过IP范围方式添加网络段*所示：

图 163: IPv6类型通过IP范围方式添加网络段

- 若选择IPv6类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP、Stateless-DHCP、SLAAC
  - **CIDR**：输入网络段的CIDR。例如：*234E:0:2457:3D/64*

- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *164: 创建L3-公有网络*所示，点击**确定**，创建L3-公有网络。

图 164: 创建L3-公有网络

3. 在ZStack私有云界面创建L2-管理网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 2: 管理网络配置信息填写如下：

   - **名称**：设置L2-管理网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork
   - **网卡**：eth0
   - **集群**：选择集群，如Cluster-1

如图 *165: 创建L2-管理网络*所示，点击**确定**，创建L2-管理网络。

图 165: 创建L2-管理网络

4. 在ZStack私有云界面创建L3-管理网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **系统网络**，进入**系统网络**界面，点击**创建系统网络**，在弹出的**创建系统网络**界面，参考上述*表 2: 管理网络配置信息*填写如下：

   - **名称**：设置L3-管理网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-管理网络
   - **添加网络段**：选择网络地址类型和方法添加网络段，网络地址类型包括：IPv4、IPv6；添加方法包括：IP范围、CIDR

- 若选择IPv4类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **起始IP**：*172.20.58.50*
  - **结束IP**：*172.20.58.59*
  - **子网掩码**：*255.255.0.0*
  - **网关**：*172.20.0.1*

  如图 *166: IPv4类型通过IP范围方式添加网络段*所示：

图 166: IPv4类型通过IP范围方式添加网络段

- 若选择IPv4类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **CIDR**：输入网络段的CIDR。例如：*192.168.1.1/24*

- 若选择IPv6类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP
  - **起始IP**：输入网络段的起始IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2002*
  - **结束IP**：输入网络段的结束IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2200*
  - **前缀长度**：输入网络段的前缀长度，范围：64-126
  - **网关**：输入网络段的网关。例如：*CDCD:910A:2222:5498:8475:1111:3900:2001*

  如图 *167: IPv6类型通过IP范围方式添加网络段*所示：

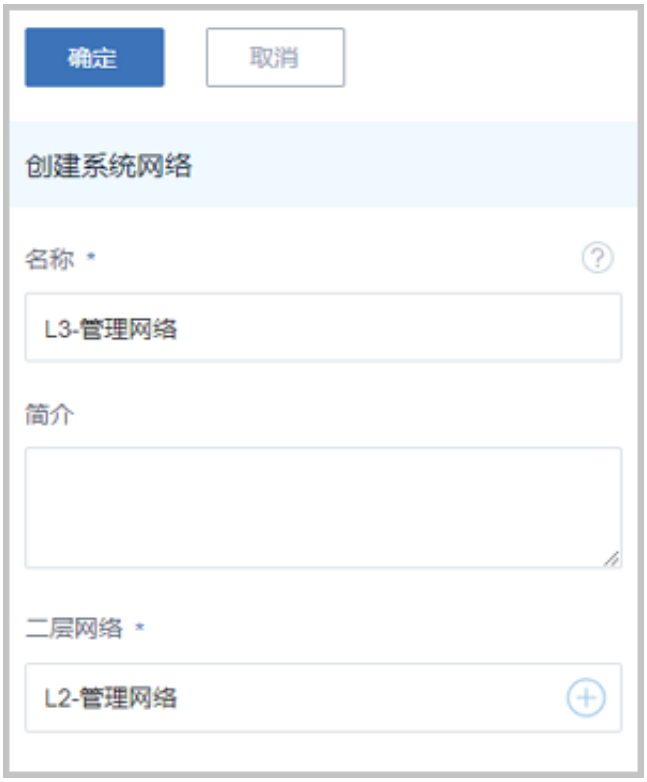
图 167: IPv6类型通过IP范围方式添加网络段

- 若选择IPv6类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP、Stateless-DHCP、SLAAC
  - **CIDR**：输入网络段的CIDR。例如：*234E:0:2457:3D/64*

- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *168:* 创建*L3*-管理网络所示，点击**确定**，创建L3-管理网络。

图 168: 创建L3-管理网络



5. 在ZStack私有云界面创建L2-私有网络（云路由网络）。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *3:* 私有网络配置信息填写如下：

   - **名称**：设置L2-私有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2VlanNetwork
   - **Vlan ID**：1982
   - **网卡**：eth0
   - **集群**：选择集群，如Cluster-1

如图 *169: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 169: 创建L2-私有网络

6. 在ZStack私有云界面创建L3-私有网络（云路由网络）。

   a) 添加云路由镜像。

   在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由镜像**，进入**云路由镜像**界面，点击**添加云路由镜像**，在弹出的**添加云路由镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置云路由镜像名称

- **简介**：可选项，可留空不填
- **镜像服务器**：选择待存放云路由镜像的镜像服务器，如BS-1
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

1. **URL**：输入云路由镜像的可下载路径

   注:

   ZStack提供专用的云路由镜像供用户使用，可在*ZStack*官网下载最新的云路由镜像。

   - 文件名称：zstack-vrouter-3.2.0.qcow2
   - 下载地址：点击这里查看

2. **本地文件**：选择当前浏览器可访问的云路由镜像直接上传

   注:

   - 支持上传到镜像仓库和Ceph镜像服务器；
   - 采用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。

如图 *170:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 170: 添加云路由镜像

b) 创建云路由规格。

在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由规格**，进入**云路由规格**界面，点击**创建云路由规格**，在弹出的**创建云路由规格**界面，可参考以下示例输入相应内容：

- **名称**：设置云路由规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置CPU个数，生产环境中建议个数设置为8以上
- **内存**：设置内存大小，单位包括：M、G、T，生产环境中建议设置为8G以上
- **镜像**：选择已添加的云路由镜像
- **管理网络**：从网络列表中选择已创建的L3-管理网络
- **公有网络**：从网络列表中选择已创建的L3-公有网络

如图 *171:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 171: 创建云路由规格

c) 创建L3-私有网络（云路由网络）。

在ZStack私有云界面，点击**网络资源** > **三层网络** > **私有网络**，进入**私有网络**界面，点击**创建私有网络**，在弹出的**创建私有网络**界面，参考上述*表 3: 私有网络配置信息*填写如下：

- **名称**：设置L3-私有网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-私有网络

- **网络服务**：选择是否需要DHCP服务
- 网络类型选择**云路由**网络
- **云路由规格**：选择已创建的云路由规格
- **添加网络段**：选择CIDR
- **CIDR**：*172.31.0.0/18*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *172: 创建L3-私有网络*所示，点击**确定**，创建L3-私有网络。

图 172: 创建L3-私有网络

7. 使用云路由网络创建ZStack私有云云主机。

   a) 添加镜像。

   在ZStack**私有云**界面，点击 **云资源池** > **镜像**，进入**镜像**界面，点击**添加镜像**，在弹出的**添加镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置镜像名称
   - **简介**：可选项，可留空不填
   - **镜像类型**：选择相应的镜像类型，包括：系统镜像、云盘镜像
   - **镜像格式**：系统镜像支持qcow2、iso、raw格式，云盘镜像支持qcow2、raw格式
   - **平台**：选择相应的平台类型，包括：
     Linux、Windows、WindowsVirtio、Other、Paravirtualization
   - **镜像服务器**：选择已创建的镜像服务器，如BS-1
   - **镜像路径**：支持添加URL路径或本地文件上传两种方式
     - URL路径：支持*HTTP/HTTPS/FTP/SFTP*方式或镜像服务器上的绝对路径*file:///*
       例如：*http://mirrors.aliyun.com/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1804.iso*
     - 本地文件上传：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
   - **BIOS模式**：选择BIOS模式，包括：Legacy和UEFI

注: 模式不匹配可能导致云主机无法正常工作，请谨慎选择。

- 对于qcow2或raw格式的镜像，请选择与封装时一致的BIOS模式
- 对于iso格式的镜像，可自行选择BIOS模式，系统将基于所选模式引导安装
- 对于Windows类型的镜像，建议选择Legacy引导模式
- 对于使用UEFI引导模式的CentOS 7.4及以上版本Linux类型镜像，创建的云主机启动后进入UEFI Shell，需执行以下命令，才能成功启动进入操作系统：

```
Shell> fs0:
FS0:\> cd EFI
FS0:\EFI\> cd centos
FS0:\EFI\centos\> shimx64-centos.efi
```

如图 *173:* 添加镜像所示，点击**确定**，添加镜像。

图 173: 添加镜像


确定
取消
添加镜像
名称 *
Image-1
简介
镜像类型 *
系统镜像
云盘镜像
镜像格式 *
qcow2
平台 *
Linux
镜像服务器 *
BS-1
镜像路径 *
URL
本地文件
http://mirrors.aliyun.com/centos/7/isos/x86_64/Cent
BIOS模式 *
Legacy
请谨慎选择，模式不匹配可能导致云主机无法正常工作
已安装 Qemu guest agent

b) 创建计算规格。

在ZStack**私有云**界面，点击 **云资源池 > 计算规格**，进入**计算规格**界面，点击**创建计算规格**，在弹出的**创建计算规格**界面，可参考以下示例输入相应内容：

- **名称**：设置计算规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置云主机CPU核数
- **内存**：设置云主机内存大小，单位包括：M、G、T，需大于16M，过低规格无法启动云主机
- **物理机分配策略**：选择物理机分配策略，包括：运行云主机数量最少、CPU使用率最低、内存使用率最低、运行云主机最大数量。默认策略为运行云主机数量最少
- **策略模式**：物理机分配策略选择CPU使用率最低或内存使用率最低时需要选择该项，包括非强制和强制两种策略模式

  注:

  - **分配策略(非强制)**：若查询不到物理机负载信息，则随机分配资源足够的物理机创建云主机
  - **分配策略(强制)**：若查询不到物理机负载信息，则无法创建云主机
- **磁盘带宽**：可选项，设置云主机根云盘的IO带宽上限。为空时，代表不限制IO带宽。基本单位包括：MB/s、GB/s、TB/s

  使用磁盘带宽的方法有以下两种：

  - **总速度**：

    如选择总速度，需设置以下内容：

    - **磁盘带宽**：设置云主机根云盘的读写总速度上限

    如图 *174: 总速度*所示：

    图 174: 总速度

- **读写速度**：

  如选择读写速度，需设置以下内容：

  - **读取速度**：设置云主机根云盘的读取速度上限
  - **写入速度**：设置云主机根云盘的写入速度上限

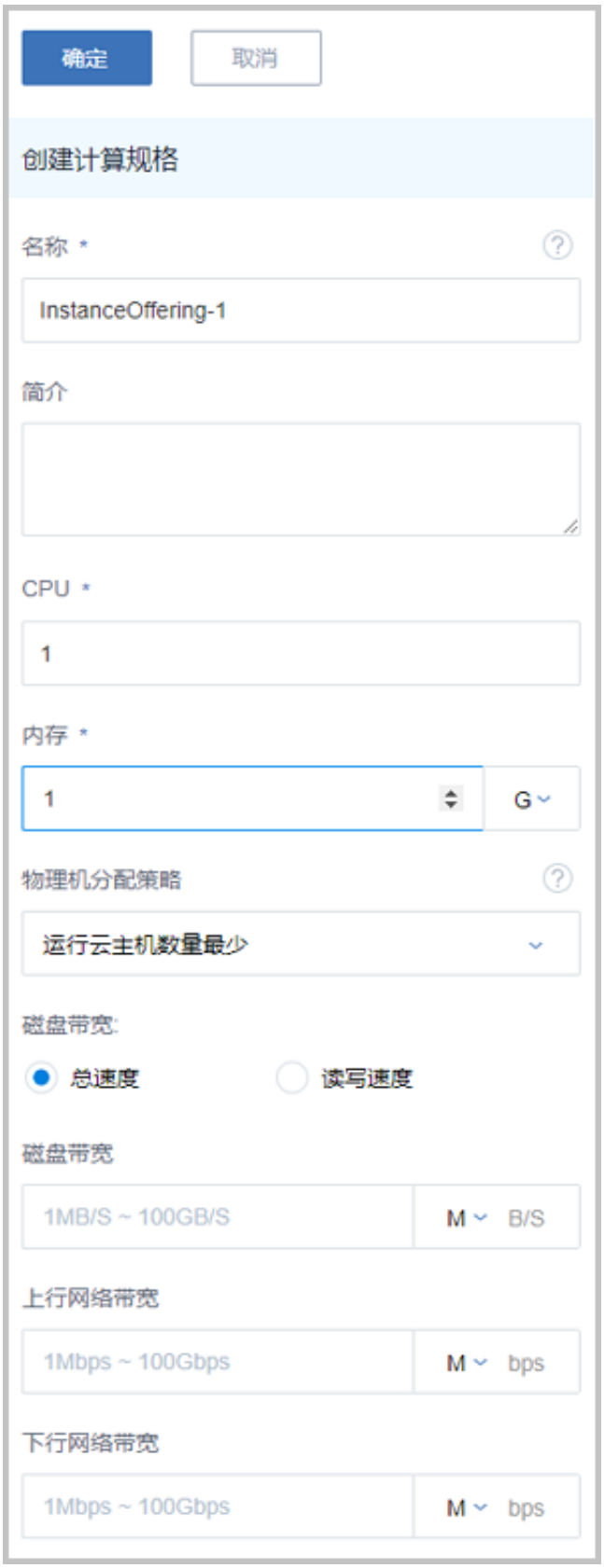
  如图 *175:* 读写速度所示：

  图 175: 读写速度

- **上行网络带宽**：可选项，从云主机上传的网络带宽上限，单位包括：Kbps、Mbps、Gbps，为空时，代表不限制上行网络带宽
- **下行网路带宽**：可选项，从云主机下载的网络带宽上限，单位包括：Kbps、Mbps、Gbps，为空时，代表不限制下行网络带宽。

如图 *176:* 创建计算规格所示，点击**确定**，创建计算规格。

图 176: 创建计算规格



c) 创建ZStack私有云云主机。

在**私有云**界面，点击 **云资源池** > **云主机**，进入**云主机**界面，点击**创建云主机**，在弹出的**创建云主机**界面，可参考以下示例输入相应内容：

- **添加方式**：选择单个
- **名称**：设置私有云云主机名称
- **简介**：可选项，可留空不填
- **计算规格**：选择已创建的计算规格
- **镜像**：选择已添加的镜像
- **网络**：从网络列表中选择已创建的L3-私有网络（云路由网络）

如图 *177:* 创建私有云云主机所示，点击 **确定**，创建私有云云主机。

图 177: 创建私有云云主机

8. 使用云路由网络创建私有云云主机过程中，系统会自动创建云路由器。

9. 创建ECS云主机，详情请参考创建*ECS*云主机。

10. 利用操作向导快速创建阿里云VPN连接。

a) 进入创建阿里云VPN连接向导。

在**操作向导**界面，点击**创建阿里云VPN连接**按钮，可按照向导来创建阿里云VPN连接，如图 *178:* 创建阿里云*VPN*连接所示：

图 178: 创建阿里云VPN连接

b) 选择阿里云网络。

在**阿里云网络**界面，可参照以下示例选择相应内容：

- **VPN网关**：选择已购买的VPN网关

注: 如果选择的地域没有可用的VPN网关，目前必须通过阿里云控制台直接购买。

如图 *179: 选择阿里云网络*所示，点击 **下一步**，进入连接配置。

图 179: 选择阿里云网络

c) 连接配置。

在**连接配置**界面，可参考以下示例输入相应内容：

- **名称**：设置VPN连接名称
- **简介**：可选项，可留空不填
- **预共享密钥**：建议设置强度高的密钥
- **云路由器**：选择创建本地云主机时自动创建的云路由器

- **公有网络**：选择云路由挂载的公有网络，如果云路由仅挂载一个公网则会默认选中该公网
- **IP地址**：可选项，表示所选择公有网络下可用的IP地址，此IP地址应为互联网公网IP地址。如果留空，系统会自动选择一个可用IP地址
- **私有网络**：选择云路由挂载的私有网络，如果云路由仅挂载一个私网则会默认选中该私网
- **高级选项**：默认选项为可连通的选项，不建议修改
  - **SA生存周期（秒）**：86400（默认）
  - **IPsec 加密算法**：3des（默认）
  - **IPsec 认证算法**：sha1（默认）
  - **IPsec DH分组**：group2（默认）
  - **IKE 版本**：ikev1（默认）
  - **IKE 协商模式**：main（默认）
  - **IKE 加密算法**：3des（默认）
  - **IKE 认证算法**：sha1（默认）
  - **IKE DH分组**：group2（默认）

如图 *180:* 连接配置所示，点击**确定**，将自动创建IPsec VPN连接。

图 180: 连接配置

d) 系统在创建IPsec VPN连接过程中，将自动完成以下操作：

1. 使用本地云路由器对应的公有网络选择可用的虚拟IP；
2. 使用此虚拟IP在阿里云端创建VPN用户网关；
3. 在阿里云端创建VPN连接；

4. 在阿里云VPC的虚拟路由器下配置路由，路由的目标网段为本地云路由挂载的私有网络*CIDR*，下一跳为*VPN*网关；
5. 在ZStack私有云端创建IPsec连接。

11. 验证本地云主机与ECS云主机是否可以ping通。

步骤10中，VPN连接的**就绪状态**显示为**第二阶段协商成功**，表示IPsec VPN环境搭建完成，只有互通验证通过，IPsec VPN通道才创建成功。

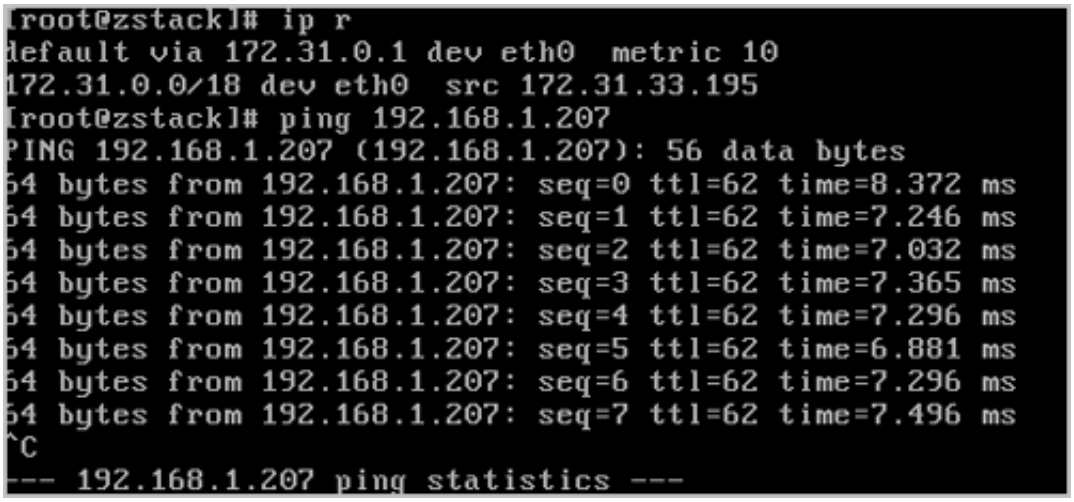
如图 *181: IPsec VPN环境搭建完成*所示：

图 181: IPsec VPN环境搭建完成

a) 登录本地云主机，检查是否能够ping通ECS云主机。

如图 *182: 本地云主机ping通ECS云主机*所示：

图 182: 本地云主机ping通ECS云主机



b) 登录ECS云主机，检查是否能够ping通本地云主机。

如图 *183: ECS云主机ping通本地云主机*所示：

图 183: ECS云主机ping通本地云主机

```
[root@zstack]# ip r
default via 192.168.1.253 dev eth0  metric 10
192.168.1.0/24 dev eth0  src 192.168.1.207
[root@zstack]# ping 172.31.33.195
PING 172.31.33.195 (172.31.33.195): 56 data bytes
64 bytes from 172.31.33.195: seq=0 ttl=62 time=7.624 ms
64 bytes from 172.31.33.195: seq=1 ttl=62 time=7.824 ms
64 bytes from 172.31.33.195: seq=2 ttl=62 time=6.974 ms
64 bytes from 172.31.33.195: seq=3 ttl=62 time=9.536 ms
64 bytes from 172.31.33.195: seq=4 ttl=62 time=7.192 ms
64 bytes from 172.31.33.195: seq=5 ttl=62 time=9.235 ms
64 bytes from 172.31.33.195: seq=6 ttl=62 time=7.173 ms
^C
--- 172.31.33.195 ping statistics ---
```

注:

如果步骤10中VPN连接失败，或者步骤11中互通验证失败，打算重新配置，需检查以下资源：

- 本地用于创建IPsec连接的虚拟IP是否已经占用，如果已使用，则需删除此虚拟IP；
- 阿里云VPN连接是否已经存在，如果存在，则需要删除，删除阿里云VPN连接同时需删除远端阿里云资源；
- 阿里云VPN用户网关是否已存在重复的IP，如果存在，则需要删除，删除需同时删除远程阿里云资源；
- VPC的虚拟路由器下是否存在已经指向ZStack私有云对应内网的路由条目，如果存在，则需要删除。

后续操作

至此，ZStack私有云云主机和阿里云ECS云主机即可使用IPsec VPN的方式实现互通。

11.1.2 阿里云高速通道实践

背景信息

ZStack支持阿里云高速通道方式实现本地云路由网络与阿里云VPC网络的互通。

搭建阿里云高速通道的基本流程如下：

1. 准备物理专线，由运营商创建边界路由器和配置路由器接口。
2. 进行网络规划，需规划：公有网络段、管理网络段、物理专线网络段和私有网络段。其中，公有网络段与管理网络段可为同一网络段。
3. 使用云路由网络创建ZStack私有云云主机。

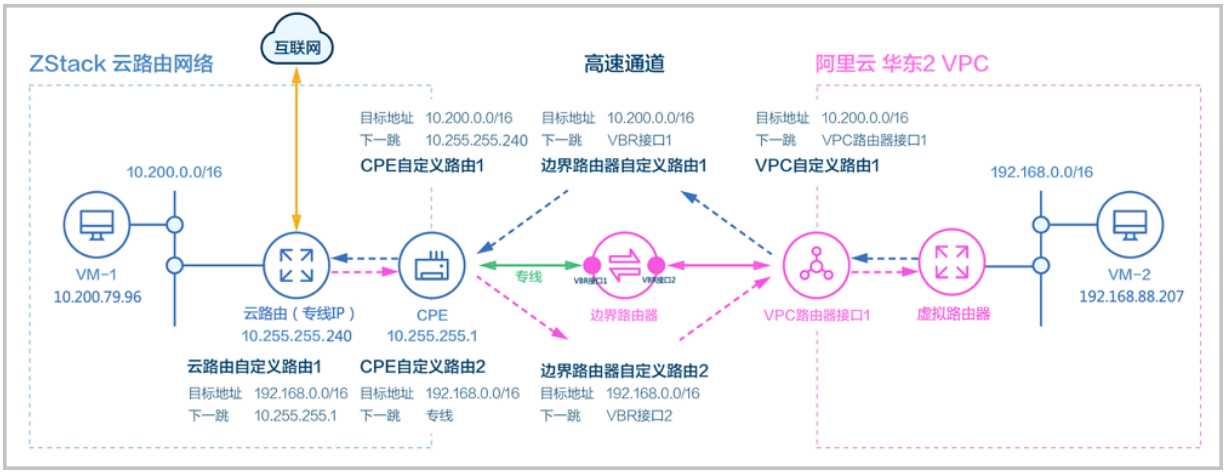
4. 加载物理专线网络到云路由器。
5. 在阿里云端准备VPC环境，并使用VPC下的虚拟交换机创建ECS实例。
6. 在ZStack混合云界面添加AccessKey、添加VPC所在地域和可用区，同步数据。
7. 利用操作向导快速创建阿里云高速通道。
8. 在CPE设备处配置双向路由。
9. 查看高速通道拓扑图。
10. 验证本地云主机与ECS云主机是否可以ping通，如能ping通，高速通道创建成功。

高速通道设计思想：通过物理专线连通本地数据中心到阿里云相应专线接入点，与阿里云VPC环境打通。

注: 从本地云路由到阿里云端VPC网络，高速通道准备互通的各网络段不可重叠！

高速通道网络架构如图 *184:* 高速通道网络架构图所示：

图 184: 高速通道网络架构图



假定客户环境如下：

1. 公有网络

表 4: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	非VLAN
IP地址段	*172.20.58.180~172.20.58.189*

公有网络	配置信息
子网掩码	*255.255.0.0*
网关	*172.20.0.1*
备注	云路由公有网络，私有云云主机可使用此网络访问互联网

2. 物理专线网络

表 5: 物理专线网络配置信息

物理专线网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*10.255.255.230~10.255.255.240*
子网掩码	*255.255.255.0*
网关	*10.255.255.1*
备注	新增网络，私有云云主机可使用此网络访问阿里云ECS

3. 私有网络

表 6: 私有网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2984
IP CIDR	*10.200.0.0/16*

4. 本地私有云端CPE设备IP地址为*10.255.255.1*
5. 边界路由器本地私有云端IP地址为*10.240.1.1*，阿里云端IP地址为*10.240.1.2*
6. 阿里云VPC网络IP地址段为*192.168.0.0/16*

双向路由步骤说明：

1. 本地云主机连通阿里云ECS的路由步骤：

a. 云路由自定义路由1：在云路由器定义路由的目的地址*ECS VPC*网络段*#192.168.0.0/16#*的下一跳为客户端*CPE*设备的*IP*地址*#10.255.255.1##*

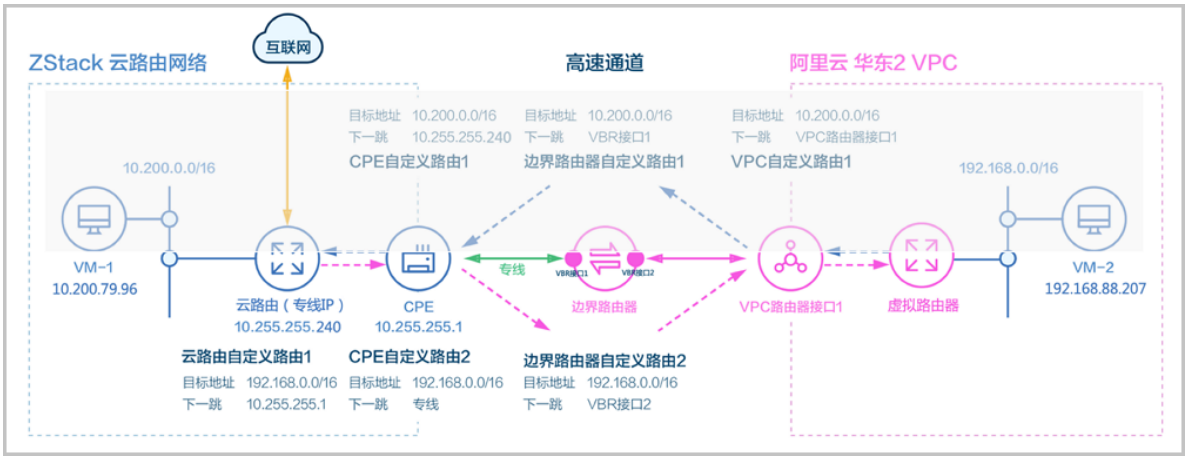
b. CPE自定义路由2：在CPE设备定义路由的目的地址*ECS VPC*网络段*#192.168.0.0/16#*的下一跳为专线的地址；

c. 边界路由器自定义路由2：在边界路由器定义目的地址*ECS VPC*网络段*#192.168.0.0/16#*的下一跳为边界路由器阿里云侧的路由器接口；

d. 路由进入阿里云的虚拟路由器后，由虚拟路由器自动转发路由到阿里云ECS。

如图 *185:* 本地云主机连通阿里云*ECS*的路由步骤所示：

图 185: 本地云主机连通阿里云ECS的路由步骤



2. 阿里云ECS连通本地云主机的路由步骤：

a. VPC自定义路由1：在VPC的虚拟路由器定义目的地址*ZStack*私有网络段*#10.200.0.0/16#*的下一跳为VPC路由器接口1；

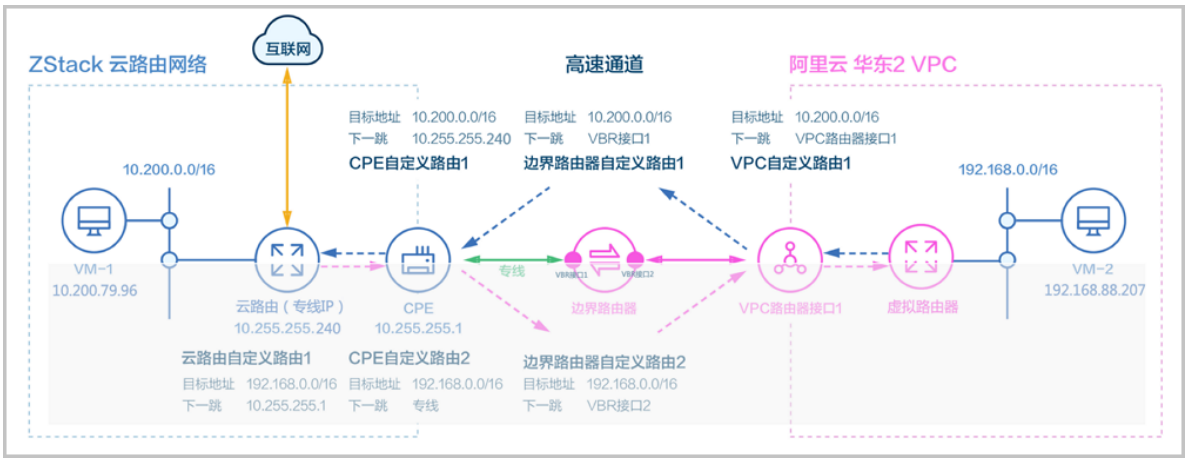
b. 边界路由器自定义路由1：在边界路由器定义目的地址*ZStack*私有网络段*#10.200.0.0/16#*的下一跳为边界路由器ZStack侧的路由器接口；

c. CPE自定义路由1：在CPE设备定义目的地址*ZStack*私有网络段*#10.200.0.0/16#*的下一跳为云路由器的物理专线*IP#10.255.255.240##*

d. 路由进入本地云路由器后，由云路由器自动转发路由到ZStack私有云云主机。

如图 *186:* 阿里云*ECS*连通本地云主机的路由步骤所示：

图 186: 阿里云ECS连通本地云主机的路由步骤



注:

1. 创建高速通道过程中，ZStack将自动配置以下4条路由：
   - VPC自定义路由1（调用阿里云API创建）
   - 边界路由器自定义路由1（调用阿里云API创建）
   - 边界路由器自定义路由2（调用阿里云API创建）
   - 云路由自定义路由1（调用本地API创建）
2. CPE设备的双向路由，应由客户自行创建：
   - CPE自定义路由1
   - CPE自定义路由2

以下介绍ZStack云路由环境搭建高速通道的实践步骤。

注:

- 本实践采用公有网络和管理网络合并的方式；
- 本实践可实现ZStack私有云云主机既能访问互联网，又能访问阿里云ECS云主机。

操作步骤

1. 在ZStack私有云界面创建L2-公有网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网络**，在弹出的**创建二层网络**界面，参考上述表 *4: 公有网络配置信息*填写如下：

   - **名称**：设置L2-公有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork

- **网卡**：em01
- **集群**：选择集群，如Cluster-1

如图 *187: 创建L2-公有网络*所示，点击**确定**，创建L2-公有网络。

图 187: 创建L2-公有网络

2. 在ZStack私有云界面创建L3-公有网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述*表 4: 公有网络配置信息*填写如下：

   - **名称**：设置L3-公有网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-公有网络

- **网络服务**：选择是否需要DHCP服务
- **添加网络段**：选择网络地址类型和方法添加网络段，网络地址类型包括：IPv4、IPv6；添加方法包括：IP范围、CIDR
  - 若选择IPv4类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
    - **起始IP**：*172.20.58.180*
    - **结束IP**：*172.20.58.189*
    - **子网掩码**：*255.255.0.0*
    - **网关**：*172.20.0.1*

    如图 *188: IPv4*类型通过*IP*范围方式添加网络段所示：

    图 188: IPv4类型通过IP范围方式添加网络段

- 若选择IPv4类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **CIDR**：输入网络段的CIDR。例如：*192.168.1.1/24*
- 若选择IPv6类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP
  - **起始IP**：输入网络段的起始IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2002*
  - **结束IP**：输入网络段的结束IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2200*

- **前缀长度**：输入网络段的前缀长度，范围：64-126
- **网关**：输入网络段的网关。例如：*CDCD:910A:2222:5498:8475:1111:3900:2001*

如图 *189: IPv6类型通过IP范围方式添加网络段*所示：

图 189: IPv6类型通过IP范围方式添加网络段

- 若选择IPv6类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP、Stateless-DHCP、SLAAC
  - **CIDR**：输入网络段的CIDR。例如：*234E:0:2457:3D/64*

- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *190: 创建L3-公有网络*所示，点击**确定**，创建L3-公有网络。

图 190: 创建L3-公有网络

3. 在ZStack私有云界面创建L2-物理专线网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网络**，在弹出的**创建二层网络**界面，参考上述*表 5: 物理专线网络配置信息*填写如下：

   - **名称**：设置L2-物理专线网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork
   - **网卡**：em02

- **集群**：选择集群，如Cluster-1

如图 *191: 创建L2-物理专线网络*所示，点击**确定**，创建L2-物理专线网络。

图 191: 创建L2-物理专线网络

4. 在ZStack私有云界面创建L3-物理专线网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述*表 5: 物理专线网络配置信息*填写如下：

   - **名称**：设置L3-物理专线网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-物理专线网络
   - **网络服务**：选择是否需要DHCP服务
   - **添加网络段**：选择网络地址类型和方法添加网络段，网络地址类型包括：IPv4、IPv6；添加方法包括：IP范围、CIDR
     - 若选择IPv4类型网络地址并通过IP范围方式添加网络段，需设置以下内容：

- **起始IP**：*10.255.255.230*
- **结束IP**：*10.255.255.240*
- **子网掩码**：*255.255.255.0*
- **网关**：*10.255.255.1*

如图 *192: IPv4类型通过IP范围方式添加网络段*所示：

图 192: IPv4类型通过IP范围方式添加网络段

- 若选择IPv4类型网络地址并通过CIDR方式添加网络段，需设置以下内容：

- **CIDR**：输入网络段的CIDR。例如：*192.168.1.1/24*

- 若选择IPv6类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP
  - **起始IP**：输入网络段的起始IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2002*
  - **结束IP**：输入网络段的结束IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2200*
  - **前缀长度**：输入网络段的前缀长度，范围：64-126
  - **网关**：输入网络段的网关。例如：*CDCD:910A:2222:5498:8475:1111:3900:2001*

  如图 *193: IPv6类型通过IP范围方式添加网络段*所示：

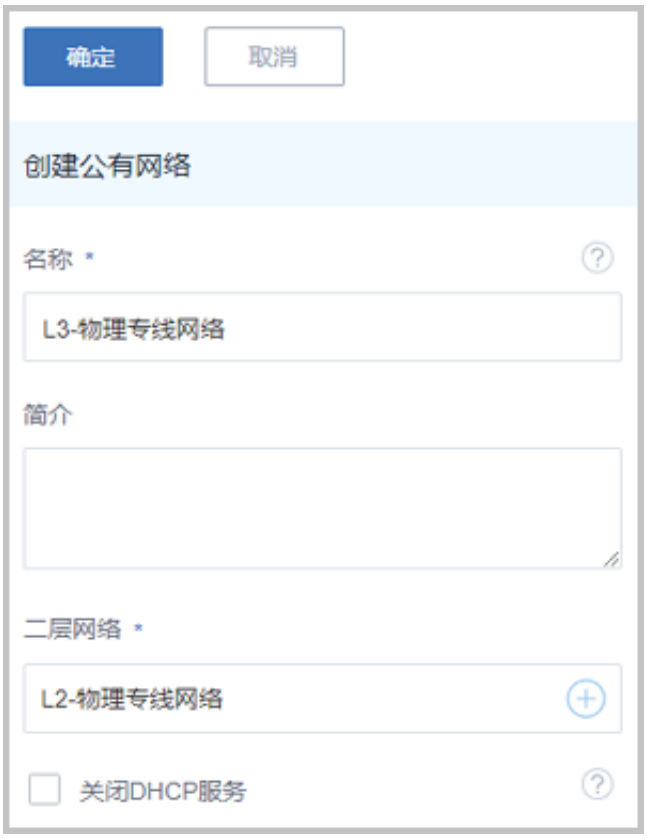
图 193: IPv6类型通过IP范围方式添加网络段

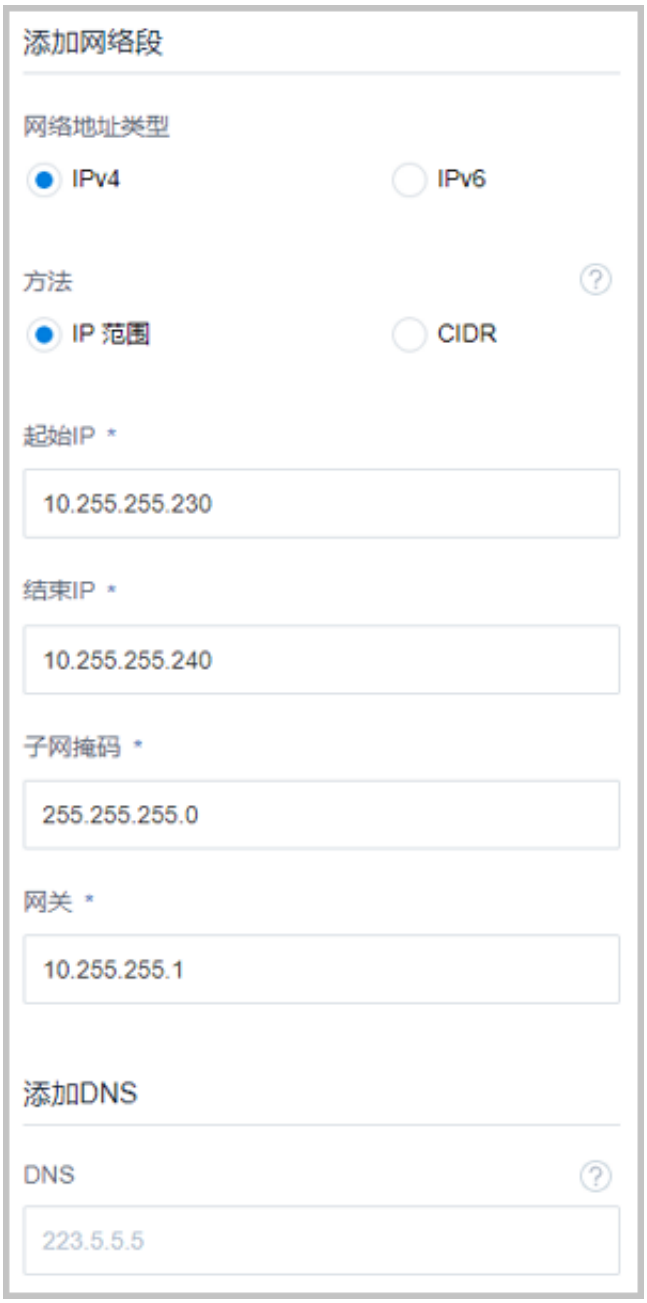
- 若选择IPv6类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP、Stateless-DHCP、SLAAC
  - **CIDR**：输入网络段的CIDR。例如：*234E:0:2457:3D/64*

- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *194: 创建L3-物理专线网络*所示，点击**确定**，创建L3-物理专线网络。

图 194: 创建L3-物理专线网络


确定
取消
创建公有网络
名称 *
L3-物理专线网络
简介
二层网络 *
L2-物理专线网络
关闭DHCP服务



5. 在ZStack私有云界面创建L2-私有网络（云路由网络）。

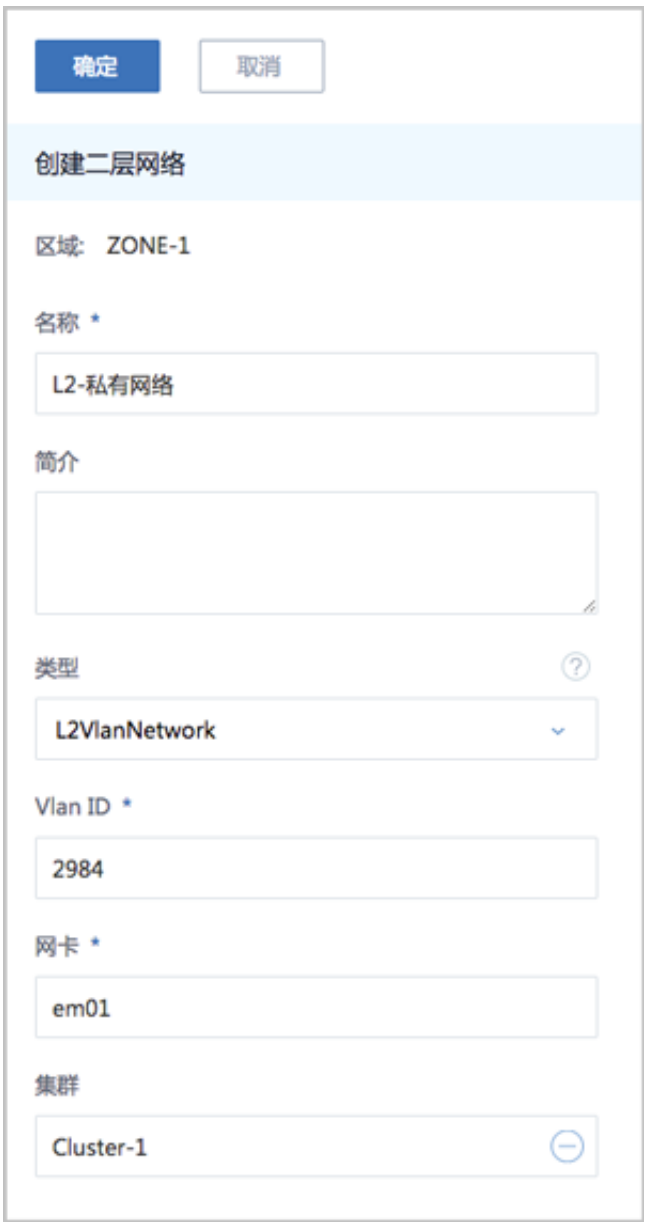
   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *6: 私有网络配置信息*填写如下：

   - **名称**：设置L2-私有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2VlanNetwork
   - **Vlan ID**：2984
   - **网卡**：em01

- **集群**：选择集群，如Cluster-1

如图 *195: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 195: 创建L2-私有网络



6. 在ZStack私有云界面创建L3-私有网络（云路由网络）。

a) 添加云路由镜像。

在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由镜像**，进入**云路由镜像**界面，点击**添加云路由镜像**，在弹出的**添加云路由镜像**界面，可参考以下示例输入相应内容：

- **名称**：设置云路由镜像名称

- **简介**：可选项，可留空不填
- **镜像服务器**：选择待存放云路由镜像的镜像服务器，如BS-1
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

1. **URL**：输入云路由镜像的可下载路径

注:

ZStack提供专用的云路由镜像供用户使用，可在*ZStack*官网下载最新的云路由镜像。

- 文件名称：zstack-vrouter-3.2.0.qcow2
- 下载地址：点击这里查看

2. **本地文件**：选择当前浏览器可访问的云路由镜像直接上传

注:

- 支持上传到镜像仓库和Ceph镜像服务器；
- 采用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。

如图 *196:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 196: 添加云路由镜像

b) 创建云路由规格。

在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由规格**，进入**云路由规格**界面，点击**创建云路由规格**，在弹出的**创建云路由规格**界面，可参考以下示例输入相应内容：

- **名称**：设置云路由规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置CPU个数，生产环境中建议个数设置为8以上
- **内存**：设置内存大小，单位包括：M、G、T，生产环境中建议设置为8G以上
- **镜像**：选择已添加的云路由镜像
- **管理网络**：从网络列表中选择已创建的L3-管理网络
- **公有网络**：从网络列表中选择已创建的L3-公有网络

如图 *197:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 197: 创建云路由规格

c) 创建L3-私有网络（云路由网络）。

在ZStack私有云界面，点击**网络资源** > **三层网络** > **私有网络**，进入**私有网络**界面，点击**创建私有网络**，在弹出的**创建私有网络**界面，参考上述表 *6:* 私有网络配置信息填写如下：

- **名称**：设置L3-私有网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-私有网络

- **网络服务**：选择是否需要DHCP服务
- 网络类型选择**云路由**网络
- **云路由规格**：选择已创建的云路由规格
- **添加网络段**：选择CIDR
- **CIDR**：*10.200.0.0/16*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *198: 创建L3-私有网络*所示，点击**确定**，创建L3-私有网络。

图 198: 创建L3-私有网络

7. 使用云路由网络创建私有云云主机。

   a) 添加镜像。

   在ZStack**私有云**界面，点击 **云资源池** > **镜像**，进入**镜像**界面，点击**添加镜像**，在弹出的**添加镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置镜像名称
   - **简介**：可选项，可留空不填
   - **镜像类型**：选择相应的镜像类型，包括：系统镜像、云盘镜像
   - **镜像格式**：系统镜像支持qcow2、iso、raw格式，云盘镜像支持qcow2、raw格式
   - **平台**：选择相应的平台类型，包括：
     Linux、Windows、WindowsVirtio、Other、Paravirtualization
   - **镜像服务器**：选择已创建的镜像服务器，如BS-1
   - **镜像路径**：支持添加URL路径或本地文件上传两种方式
     - URL路径：支持*HTTP/HTTPS/FTP/SFTP*方式或镜像服务器上的绝对路径*file:///*
       例如：*http://mirrors.aliyun.com/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1804.iso*
     - 本地文件上传：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
   - **BIOS模式**：选择BIOS模式，包括：Legacy和UEFI

注: 模式不匹配可能导致云主机无法正常工作，请谨慎选择。

- 对于qcow2或raw格式的镜像，请选择与封装时一致的BIOS模式
- 对于iso格式的镜像，可自行选择BIOS模式，系统将基于所选模式引导安装
- 对于Windows类型的镜像，建议选择Legacy引导模式
- 对于使用UEFI引导模式的CentOS 7.4及以上版本Linux类型镜像，创建的云主机启动后进入UEFI Shell，需执行以下命令，才能成功启动进入操作系统：

```
Shell> fs0:
FS0:\> cd EFI
FS0:\EFI\> cd centos
FS0:\EFI\centos\> shimx64-centos.efi
```

如图 *199:* 添加镜像所示，点击**确定**，添加镜像。

图 199: 添加镜像


确定
取消
添加镜像
名称 *
Image-1
简介
镜像类型 *
系统镜像
云盘镜像
镜像格式 *
qcow2
平台 *
Linux
镜像服务器 *
BS-1
镜像路径 *
URL
本地文件
http://mirrors.aliyun.com/centos/7/isos/x86_64/Cent
BIOS模式 *
Legacy
请谨慎选择，模式不匹配可能导致云主机无法正常工作
已安装 Qemu guest agent

b) 创建计算规格。

在ZStack**私有云**界面，点击 **云资源池 > 计算规格**，进入**计算规格**界面，点击**创建计算规格**，在弹出的**创建计算规格**界面，可参考以下示例输入相应内容：

- **名称**：设置计算规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置云主机CPU核数
- **内存**：设置云主机内存大小，单位包括：M、G、T，需大于16M，过低规格无法启动云主机
- **物理机分配策略**：选择物理机分配策略，包括：运行云主机数量最少、CPU使用率最低、内存使用率最低、运行云主机最大数量。默认策略为运行云主机数量最少
- **策略模式**：物理机分配策略选择CPU使用率最低或内存使用率最低时需要选择该项，包括非强制和强制两种策略模式

  注:

  - **分配策略(非强制)**：若查询不到物理机负载信息，则随机分配资源足够的物理机创建云主机
  - **分配策略(强制)**：若查询不到物理机负载信息，则无法创建云主机
- **磁盘带宽**：可选项，设置云主机根云盘的IO带宽上限。为空时，代表不限制IO带宽。基本单位包括：MB/s、GB/s、TB/s

  使用磁盘带宽的方法有以下两种：

  - **总速度**：

    如选择总速度，需设置以下内容：

    - **磁盘带宽**：设置云主机根云盘的读写总速度上限

    如图 *200: 总速度*所示：

    图 200: 总速度

- **读写速度**：

  如选择读写速度，需设置以下内容：

  - **读取速度**：设置云主机根云盘的读取速度上限
  - **写入速度**：设置云主机根云盘的写入速度上限

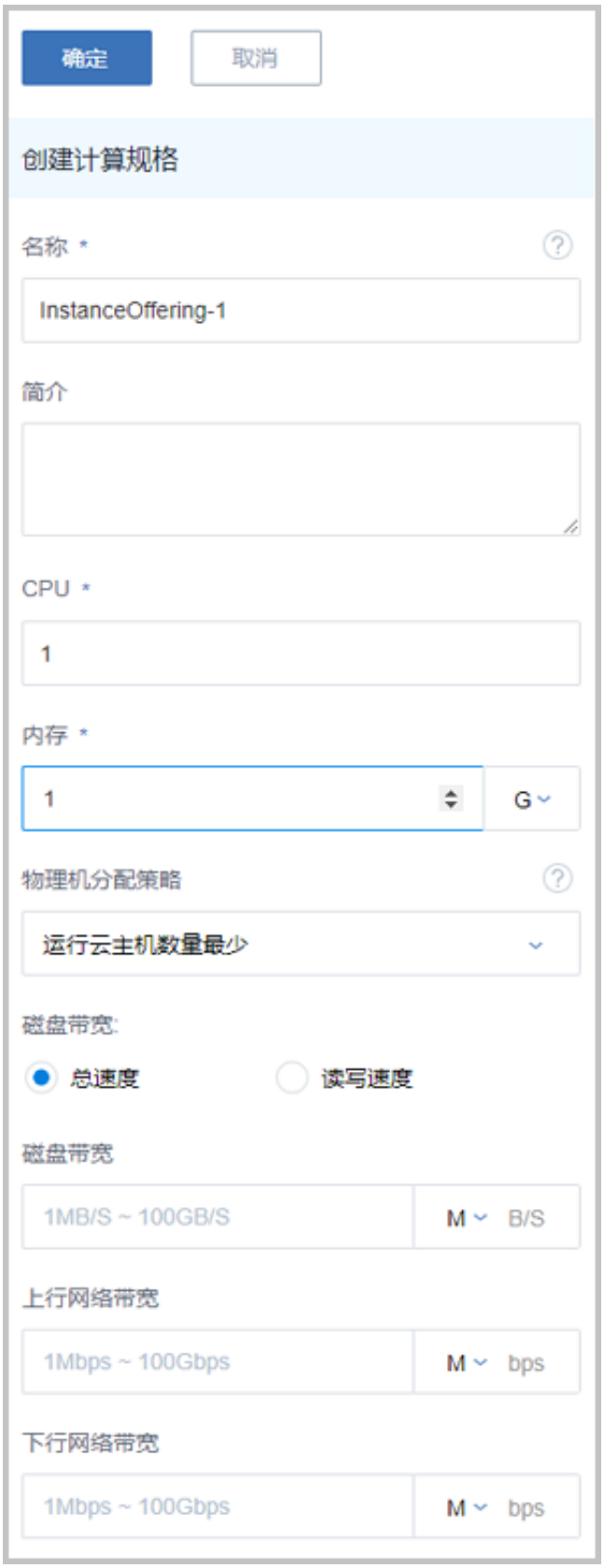
  如图 *201:* 读写速度所示：

  图 201: 读写速度

- **上行网络带宽**：可选项，从云主机上传的网络带宽上限，单位包括：Kbps、Mbps、Gbps，为空时，代表不限制上行网络带宽
- **下行网路带宽**：可选项，从云主机下载的网络带宽上限，单位包括：Kbps、Mbps、Gbps，为空时，代表不限制下行网络带宽。

如图 *202:* 创建计算规格所示，点击**确定**，创建计算规格。

图 202: 创建计算规格



c) 创建ZStack私有云云主机。

在**私有云**界面，点击 **云资源池** > **云主机**，进入**云主机**界面，点击**创建云主机**，在弹出的**创建云主机**界面，可参考以下示例输入相应内容：

- **添加方式**：选择单个
- **名称**：设置私有云云主机名称
- **简介**：可选项，可留空不填
- **计算规格**：选择已创建的计算规格
- **镜像**：选择已添加的镜像
- **网络**：从网络列表中选择已创建的L3-私有网络（云路由网络）

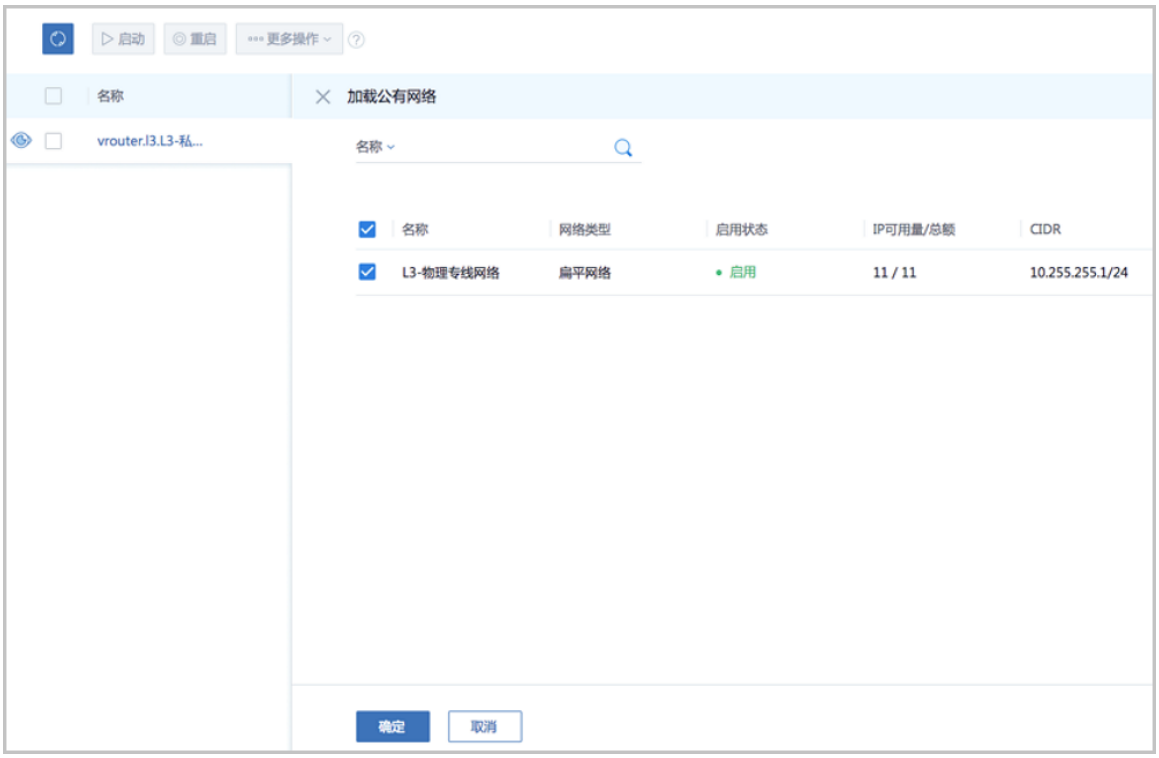
如图 *203:* 创建私有云云主机所示，点击 **确定**，创建私有云云主机。

图 203: 创建私有云云主机

8. 使用云路由网络创建私有云云主机过程中，系统会自动创建云路由器。
9. 加载物理专线网络到云路由器。

   在ZStack**私有云**界面，点击**网络资源** > **路由资源** > **云路由器**，进入**云路由器**界面，选择已创建的云路由器，展开详情页，进入**配置信息**子页面，点击**操作** > **加载**，加载L3-物理专线网络到云路由器，如图 *204:* 加载物理专线网络到云路由器所示：

   图 204: 加载物理专线网络到云路由器



10.在阿里云端准备VPC环境，并使用VPC下的虚拟交换机创建ECS实例。

11.在ZStack混合云界面添加AccessKey、添加VPC所在地域和可用区，同步数据。

添加AccessKey，详情请见添加*AccessKey*。

添加地域和可用区，详情请见添加地域和添加可用区。

在**混合云**界面，点击**同步数据**，可将已添加地域和可用区下的阿里云资源同步至本地，包括在阿里云端创建的专有网络VPC、虚拟交换机、ECS以及边界路由器、路由器接口等信息。

如图 *205:* 同步数据所示：

图 205: 同步数据

12.利用操作向导快速创建阿里云高速通道。

a) 进入创建阿里云高速通道向导。

在**操作向导**界面，点击**创建阿里云高速通道**按钮，可按照向导来创建阿里云高速通道，如图 *206: 创建阿里云高速通道*所示：

图 206: 创建阿里云高速通道

b) 配置ZStack网络。

在**ZStack网络**界面，可参照以下示例输入相应内容：

- **云路由器**：选择本地云路由器
- **公有网络**：选择可以连接本地至边界路由器接口的专线网络
- **私有网络**：选择本地创建的私有网络（云路由网络）

如图 *207: ZStack网络界面*所示，点击 **下一步**，进入配置阿里云网络。

图 207: ZStack网络界面

c) 配置阿里云网络。

在**阿里云网络**界面，可参考以下示例输入相应内容：

- **专有网络VPC**：选择专有网络VPC
- **边界路由器**：选择边界路由器，目前由运营商创建并配置路由
- **CPE IP（运营商）**：运营商提供物理专线接入本地数据中心的客户端设备IP地址

如图 *208:* 配置阿里云网络所示，点击**确定**，创建阿里云高速通道。

图 208: 配置阿里云网络

创建高速通道过程中，ZStack将自动配置以下4条路由：

- VPC自定义路由1：目的地址为*ZStack*私有网络段，下一跳为VPC虚拟路由器接口；
- 边界路由器自定义路由1：目的地址为*ZStack*私有网络段，下一跳为边界路由器ZStack私有云侧的路由器接口；
- 边界路由器自定义路由2：目的地址为*ECS VPC*网络段，下一跳为边界路由器阿里云侧的路由器接口；
- 云路由自定义路由1：目的地址为*ECS VPC*网络段，下一跳为客户端CPE设备的IP地址。

13.在CPE设备处配置双向路由。

CPE设备的两条路由条目，应由客户自行创建：

- 设置CPE自定义路由1：目的地址为*ZStack*私有网络段，下一跳为云路由器的物理专线IP；
- 设置CPE自定义路由2：目的地址为*ECS VPC*网络段，下一跳为专线的地址。

14.查看阿里云高速通道拓扑图。

在**专有网络VPC**界面，点击相应的VPC，进入**专有网络VPC**详情页，点击**拓扑图**，进入**拓扑图**页面，可查看网络拓扑，如图 *209:* 拓扑图所示：

图 209: 拓扑图

15.验证本地云主机与ECS云主机是否可以ping通。

a) 登录本地云主机，检查是否能够ping通ECS云主机。

如图 *210: 本地云主机ping通ECS云主机*所示：

图 210: 本地云主机ping通ECS云主机

```
[root@zstack]# ip r
default via 10.200.0.1 dev eth0  metric 10
10.200.0.0/16 dev eth0  src 10.200.79.96
[root@zstack]# ping 192.168.88.207
PING 192.168.88.207 (192.168.88.207): 56 data bytes
64 bytes from 192.168.88.207: seq=0 ttl=60 time=10.507 ms
64 bytes from 192.168.88.207: seq=1 ttl=60 time=6.674 ms
64 bytes from 192.168.88.207: seq=2 ttl=60 time=8.813 ms
64 bytes from 192.168.88.207: seq=3 ttl=60 time=8.414 ms
64 bytes from 192.168.88.207: seq=4 ttl=60 time=8.134 ms
64 bytes from 192.168.88.207: seq=5 ttl=60 time=6.309 ms
64 bytes from 192.168.88.207: seq=6 ttl=60 time=7.972 ms
^C
--- 192.168.88.207 ping statistics ---
```

b) 登录ECS云主机，检查是否能够ping通本地云主机。

如图 *211: ECS云主机ping通本地云主机*所示：

图 211: ECS云主机ping通本地云主机

后续操作

至此，ZStack私有云云主机和阿里云ECS云主机即可使用阿里云高速通道的方式实现互通。

11.1.3 大河高速通道实践

背景信息

ZStack支持大河高速通道方式实现本地云路由网络与阿里云VPC网络的互通。

搭建大河高速通道的基本流程如下：

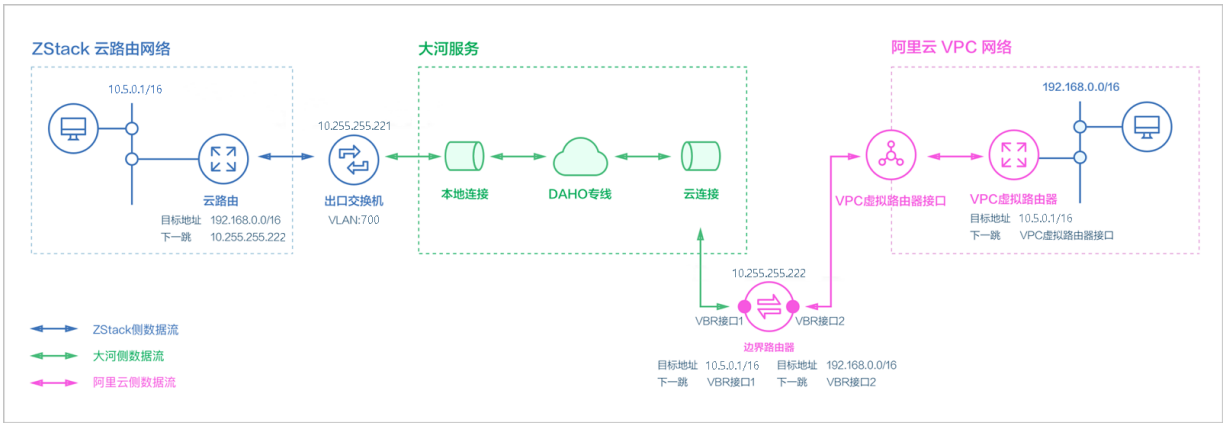
1. 联系大河云联申请大河账号，获取大河提供的AccessKey。
2. 准备一对互联地址，例如：*10.255.255.221*（ZStack私有云端）和*10.255.255.222*（阿里云端），并将这对互联地址绑定到本地出口交换机的某个VLAN上，例如：VLAN ID为700。
3. 进行网络规划，需规划：公有网络段、管理网络段、私有网络段。出于安全和稳定性考虑，建议部署独立的管理网络，并与公有网络隔离。
4. 需关闭私有三层网络的SNAT服务，请咨询ZStack官方技术支持获取帮助。
5. 使用云路由网络创建ZStack私有云云主机。
6. 在阿里云端准备VPC环境，并使用VPC下的虚拟交换机创建ECS实例。
7. 在ZStack混合云界面添加阿里云的AccessKey、添加阿里云VPC所在地域和可用区，同步数据。
8. 在ZStack混合云界面添加大河的AccessKey、同步大河端该账户下所有本地侧连接以及指定地域的所有公有云侧连接。
9. 利用操作向导快速创建大河高速通道。
10. 验证本地云主机与ECS云主机是否可以ping通，如能ping通，大河高速通道创建成功。

大河高速通道设计思想：通过基于SD-WAN的大河专线连通本地数据中心到阿里云相应专线接入点，与阿里云VPC环境打通。

注: 从本地云路由到阿里云端VPC网络，大河高速通道准备互通的各网络段不可重叠！

大河高速通道网络拓扑图如图 *212:* 大河高速通道网络拓扑图所示：

图 212: 大河高速通道网络拓扑图



假定客户环境如下：

1. 公有网络

表 7: 公有网络配置信息

公有网络	配置信息
网卡	em01
VLAN ID	700
IP地址段	*10.255.255.221~10.255.255.221*
子网掩码	*255.255.255.252*
网关	*10.255.255.222*
备注	此处公有网络并非传统意义上的公有网络，仅用于连通大河专线，*10.0.0.0/8*网段本身属于私网地址范围。

2. 管理网络

表 8: 管理网络配置信息

物理专线网络	配置信息
网卡	em02
VLAN ID	非VLAN
IP地址段	*172.16.0.10~172.16.0.20*
子网掩码	*255.255.255.0*
网关	*172.16.0.208*

3. 私有网络

表 9: 私有网络配置信息

私有网络	配置信息
网卡	em01
VLAN ID	2100
IP CIDR	*10.5.0.1/16*

4. 边界路由器本地私有云端IP地址为*10.255.255.221*，阿里云端IP地址为*10.255.255.222*
5. 阿里云VPC网络IP地址段为*192.168.0.0/16*

双向路由步骤说明：

1. 本地云主机连通阿里云ECS的路由步骤：
   a. 本地云路由自定义路由：目的地址为ECS VPC网络端（*192.168.0.0/16*），下一跳为阿里云端网关*10.255.255.222*。
   b. 边界路由器自定义路由2：目的地址为ECS VPC网络段（*192.168.0.0/16*），下一跳为边界路由器阿里云侧的路由器接口（VBR接口2）；
   c. 路由进入阿里云的虚拟路由器后，由虚拟路由器自动转发路由到阿里云ECS。
2. 阿里云ECS连通本地云主机的路由步骤：
   a. VPC虚拟路由器自定义路由：目的地址ZStack私有网络段（*10.5.0.1/16*），下一跳为VPC虚拟路由器接口；
   b. 边界路由器自定义路由1：目的地址ZStack私有网络段（*10.5.0.1/16*），下一跳为边界路由器ZStack侧的路由器接口（VBR接口1）；

c. 路由进入本地云路由后，由云路由自动转发路由到ZStack私有云云主机。

注:

创建大河高速通道过程中，ZStack将自动配置以下4条路由：

- VPC虚拟路由器自定义路由（调用阿里云API创建）
- 边界路由器自定义路由1（调用阿里云API创建）
- 边界路由器自定义路由2（调用阿里云API创建）
- 本地云路由自定义路由（调用本地API创建）

以下介绍ZStack云路由环境搭建大河高速通道的实践步骤。

注:

- 本实践采用公有网络和管理网络分离的方式；
- 本实践可实现ZStack私有云云主机与阿里云ECS云主机间互相访问。

操作步骤

1. 在ZStack私有云界面创建L2-公有网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网络**，在弹出的**创建二层网络**界面，参考上述表 *7:* 公有网络配置信息填写如下：

   - **名称**：设置L2-公有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2VlanNetwork
   - **Vlan ID**：700
   - **网卡**：em01
   - **集群**：选择集群，如Cluster-1

   如图 *213:* 创建*L2*-公有网络所示，点击**确定**，创建L2-公有网络。

   图 213: 创建L2-公有网络

2. 在ZStack私有云界面创建L3-公有网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **公有网络**，进入**公有网络**界面，点击**创建公有网络**，在弹出的**创建公有网络**界面，参考上述表 7: 公有网络配置信息填写如下：

   - **名称**：设置L3-公有网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L2-公有网络
   - **网络服务**：选择是否需要DHCP服务

- **添加网络段**：选择网络地址类型和方法添加网络段，网络地址类型包括：IPv4、IPv6；添加方法包括：IP范围、CIDR
  - 若选择IPv4类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
    - **起始IP**：*10.255.255.221*
    - **结束IP**：*10.255.255.221*
    - **子网掩码**：*255.255.255.252*
    - **网关**：*10.255.255.222*

    如图 *214: IPv4类型通过IP范围方式添加网络段*所示：

    图 214: IPv4类型通过IP范围方式添加网络段

- 若选择IPv4类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **CIDR**：输入网络段的CIDR。例如：*192.168.1.1/24*
- 若选择IPv6类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP
  - **起始IP**：输入网络段的起始IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2002*
  - **结束IP**：输入网络段的结束IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2200*

- **前缀长度**：输入网络段的前缀长度，范围：64-126
- **网关**：输入网络段的网关。例如：*CDCD:910A:2222:5498:8475:1111:3900:2001*

如图 *215: IPv6类型通过IP范围方式添加网络段*所示：

图 215: IPv6类型通过IP范围方式添加网络段

- 若选择IPv6类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP、Stateless-DHCP、SLAAC
  - **CIDR**：输入网络段的CIDR。例如：*234E:0:2457:3D/64*

- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *216:* 创建*L3*-公有网络所示，点击**确定**，创建L3-公有网络。

图 216: 创建L3-公有网络

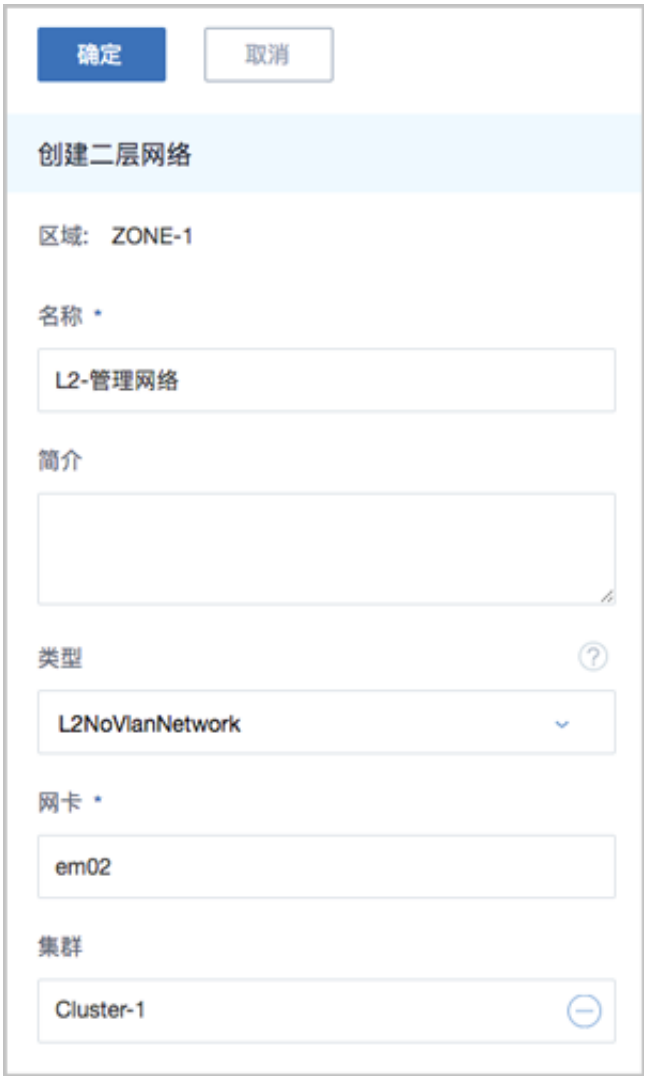
3. 在ZStack私有云界面创建L2-管理网络。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网络**，在弹出的**创建二层网络**界面，参考上述表 *8:* 管理网络配置信息填写如下：

   - **名称**：设置L2-管理网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2NoVlanNetwork
   - **网卡**：em02
   - **集群**：选择集群，如Cluster-1

如图 *217: 创建L2-管理网络*所示，点击**确定**，创建L2-管理网络。

图 217: 创建L2-管理网络



4. 在ZStack私有云界面创建L3-管理网络。

   在ZStack私有云界面，点击**网络资源** > **三层网络** > **系统网络**，进入**系统网络**界面，点击**创建系统网络**，在弹出的**创建系统网络**界面，参考上述*表 8: 管理网络配置信息*填写如下：

   - **名称**：设置L3-管理网络名称
   - **简介**：可选项，可留空不填
   - **二层网络**：选择已创建的L3-管理网络
   - **网络服务**：选择是否需要DHCP服务
   - **添加网络段**：选择网络地址类型和方法添加网络段，网络地址类型包括：IPv4、IPv6；添加方法包括：IP范围、CIDR

- 若选择IPv4类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **起始IP**：*172.16.0.10*
  - **结束IP**：*172.16.0.20*
  - **子网掩码**：*255.255.255.0*
  - **网关**：*172.16.0.208*

  如图 *218: IPv4类型通过IP范围方式添加网络段*所示：

图 218: IPv4类型通过IP范围方式添加网络段

- 若选择IPv4类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
  - **CIDR**：输入网络段的CIDR。例如：*192.168.1.1/24*

- 若选择IPv6类型网络地址并通过IP范围方式添加网络段，需设置以下内容：
  - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP
  - **起始IP**：输入网络段的起始IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2002*
  - **结束IP**：输入网络段的结束IP。例如：*CDCD:910A:2222:5498:8475:1111:3900:2200*
  - **前缀长度**：输入网络段的前缀长度，范围：64-126
  - **网关**：输入网络段的网关。例如：*CDCD:910A:2222:5498:8475:1111:3900:2001*

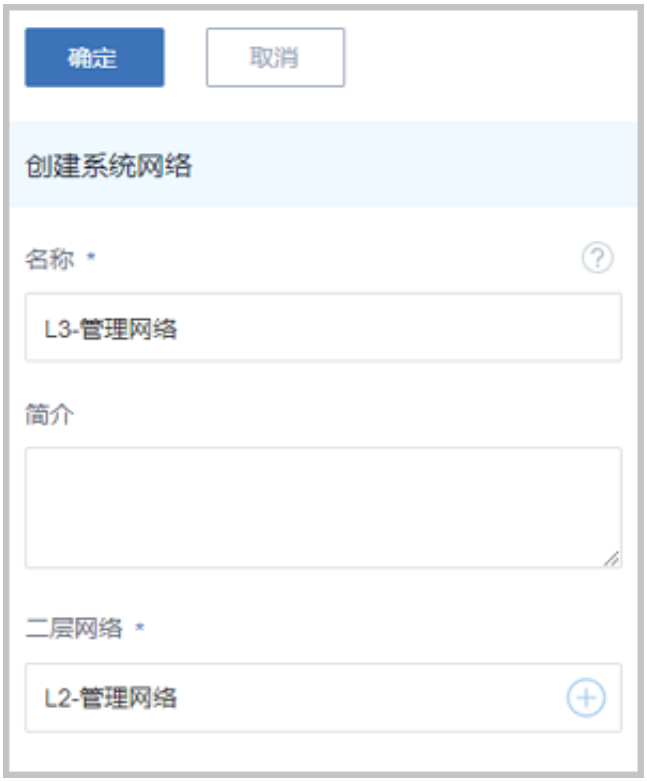
如图 *219: IPv6类型通过IP范围方式添加网络段*所示：

图 219: IPv6类型通过IP范围方式添加网络段

  - 若选择IPv6类型网络地址并通过CIDR方式添加网络段，需设置以下内容：
    - **分配IP模式**：选择分配IP模式，包括：Stateful-DHCP、Stateless-DHCP、SLAAC
    - **CIDR**：输入网络段的CIDR。例如：*234E:0:2457:3D/64*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *220: 创建L3-管理网络*所示，点击**确定**，创建L3-管理网络。

图 220: 创建L3-管理网络



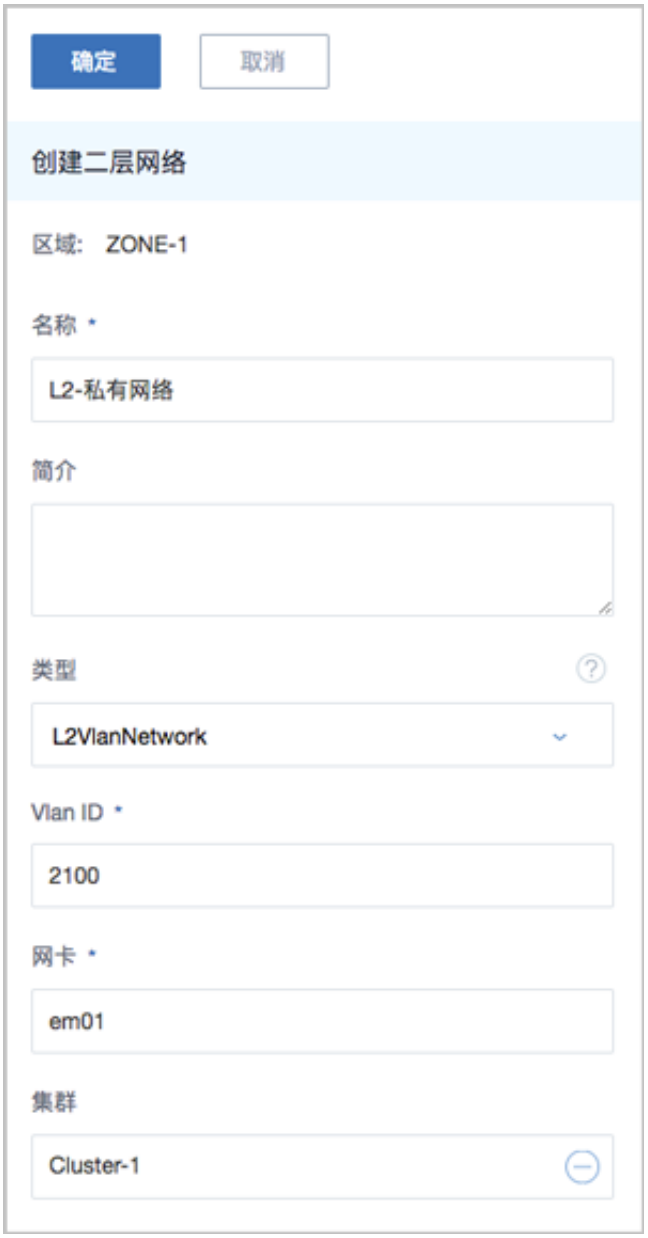
5. 在ZStack私有云界面创建L2-私有网络（云路由网络）。

   在ZStack私有云界面，点击**网络资源** > **二层网络资源** > **二层网络**，进入**二层网络**界面，点击**创建二层网路**，在弹出的**创建二层网络**界面，参考上述表 *9:* 私有网络配置信息填写如下：

   - **名称**：设置L2-私有网络名称
   - **简介**：可选项，可留空不填
   - **类型**：选择L2VlanNetwork
   - **Vlan ID**：2100
   - **网卡**：em01
   - **集群**：选择集群，如Cluster-1

如图 *221: 创建L2-私有网络*所示，点击**确定**，创建L2-私有网络。

图 221: 创建L2-私有网络



6. 在ZStack私有云界面创建L3-私有网络（云路由网络）。

   a) 添加云路由镜像。

   在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由镜像**，进入**云路由镜像**界面，点击**添加云路由镜像**，在弹出的**添加云路由镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置云路由镜像名称
   - **简介**：可选项，可留空不填

- **镜像服务器**：选择待存放云路由镜像的镜像服务器，如BS-1
- **镜像路径**：支持添加URL路径或本地文件上传两种方式

1. **URL**：输入云路由镜像的可下载路径

   注:

   ZStack提供专用的云路由镜像供用户使用，可在*ZStack*官网下载最新的云路由镜像。

   - 文件名称：zstack-vrouter-3.2.0.qcow2
   - 下载地址：点击这里查看

2. **本地文件**：选择当前浏览器可访问的云路由镜像直接上传

   注:

   - 支持上传到镜像仓库和Ceph镜像服务器；
   - 采用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。

如图 *222:* 添加云路由镜像所示，点击**确定**，添加云路由镜像。

图 222: 添加云路由镜像

b) 创建云路由规格。

在ZStack私有云主菜单，点击 **网络资源** > **路由资源** > **云路由规格**，进入**云路由规格**界面，点击**创建云路由规格**，在弹出的**创建云路由规格**界面，可参考以下示例输入相应内容：

- **名称**：设置云路由规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置CPU个数，生产环境中建议个数设置为8以上
- **内存**：设置内存大小，单位包括：M、G、T，生产环境中建议设置为8G以上
- **镜像**：选择已添加的云路由镜像
- **管理网络**：从网络列表中选择已创建的L3-管理网络
- **公有网络**：从网络列表中选择已创建的L3-公有网络

如图 *223:* 创建云路由规格所示，点击**确定**，创建云路由规格。

图 223: 创建云路由规格

c) 创建L3-私有网络（云路由网络）。

在ZStack私有云界面，点击**网络资源** > **三层网络** > **私有网络**，进入**私有网络**界面，点击**创建私有网络**，在弹出的**创建私有网络**界面，参考上述*表 9: 私有网络配置信息*填写如下：

- **名称**：设置L3-私有网络名称
- **简介**：可选项，可留空不填
- **二层网络**：选择已创建的L2-私有网络

- **网络服务**：选择是否需要DHCP服务
- 网络类型选择**云路由**网络
- **云路由规格**：选择已创建的云路由规格
- **添加网络段**：选择CIDR
- **CIDR**：*10.5.0.1/16*
- **DNS**：可选项，可留空不填，也可设置，如*114.114.114.114*

如图 *224: 创建L3-私有网络*所示，点击**确定**，创建L3-私有网络。

图 224: 创建L3-私有网络

7. 需关闭私有三层网络的SNAT服务，请咨询ZStack官方技术支持获取帮助。
8. 使用云路由网络创建私有云云主机。

   a) 添加镜像。

   在ZStack**私有云**界面，点击 **云资源池** > **镜像**，进入**镜像**界面，点击**添加镜像**，在弹出的**添加镜像**界面，可参考以下示例输入相应内容：

   - **名称**：设置镜像名称
   - **简介**：可选项，可留空不填
   - **镜像类型**：选择相应的镜像类型，包括：系统镜像、云盘镜像
   - **镜像格式**：系统镜像支持qcow2、iso、raw格式，云盘镜像支持qcow2、raw格式
   - **平台**：选择相应的平台类型，包括：
     Linux、Windows、WindowsVirtio、Other、Paravirtualization
   - **镜像服务器**：选择已创建的镜像服务器，如BS-1
   - **镜像路径**：支持添加URL路径或本地文件上传两种方式
     - URL路径：支持*HTTP/HTTPS/FTP/SFTP*方式或镜像服务器上的绝对路径*file:///*

       例如：*http://mirrors.aliyun.com/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1804.iso*
     - 本地文件上传：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
   - **BIOS模式**：选择BIOS模式，包括：Legacy和UEFI

注: 模式不匹配可能导致云主机无法正常工作，请谨慎选择。

- 对于qcow2或raw格式的镜像，请选择与封装时一致的BIOS模式
- 对于iso格式的镜像，可自行选择BIOS模式，系统将基于所选模式引导安装
- 对于Windows类型的镜像，建议选择Legacy引导模式
- 对于使用UEFI引导模式的CentOS 7.4及以上版本Linux类型镜像，创建的云主机启动后进入UEFI Shell，需执行以下命令，才能成功启动进入操作系统：

```
Shell> fs0:
FS0:\> cd EFI
FS0:\EFI\> cd centos
FS0:\EFI\centos\> shimx64-centos.efi
```

如图 *225:* 添加镜像所示，点击**确定**，添加镜像。

图 225: 添加镜像


确定
取消
添加镜像
名称 *
Image-1
简介
镜像类型 *
系统镜像
云盘镜像
镜像格式 *
qcow2
平台 *
Linux
镜像服务器 *
BS-1
镜像路径 *
URL
本地文件
http://mirrors.aliyun.com/centos/7/isos/x86_64/Cent
BIOS模式 *
Legacy
请谨慎选择，模式不匹配可能导致云主机无法正常工作
已安装 Qemu guest agent

b) 创建计算规格。

在ZStack**私有云**界面，点击 **云资源池 > 计算规格**，进入**计算规格**界面，点击**创建计算规格**，在弹出的**创建计算规格**界面，可参考以下示例输入相应内容：

- **名称**：设置计算规格名称
- **简介**：可选项，可留空不填
- **CPU**：设置云主机CPU核数
- **内存**：设置云主机内存大小，单位包括：M、G、T，需大于16M，过低规格无法启动云主机
- **物理机分配策略**：选择物理机分配策略，包括：运行云主机数量最少、CPU使用率最低、内存使用率最低、运行云主机最大数量。默认策略为运行云主机数量最少
- **策略模式**：物理机分配策略选择CPU使用率最低或内存使用率最低时需要选择该项，包括非强制和强制两种策略模式

  注:

  - **分配策略(非强制)**：若查询不到物理机负载信息，则随机分配资源足够的物理机创建云主机
  - **分配策略(强制)**：若查询不到物理机负载信息，则无法创建云主机
- **磁盘带宽**：可选项，设置云主机根云盘的IO带宽上限。为空时，代表不限制IO带宽。基本单位包括：MB/s、GB/s、TB/s

  使用磁盘带宽的方法有以下两种：

  - **总速度**：

    如选择总速度，需设置以下内容：

    - **磁盘带宽**：设置云主机根云盘的读写总速度上限

    如图 *226: 总速度*所示：

    图 226: 总速度

- **读写速度**：

  如选择读写速度，需设置以下内容：

  - **读取速度**：设置云主机根云盘的读取速度上限
  - **写入速度**：设置云主机根云盘的写入速度上限

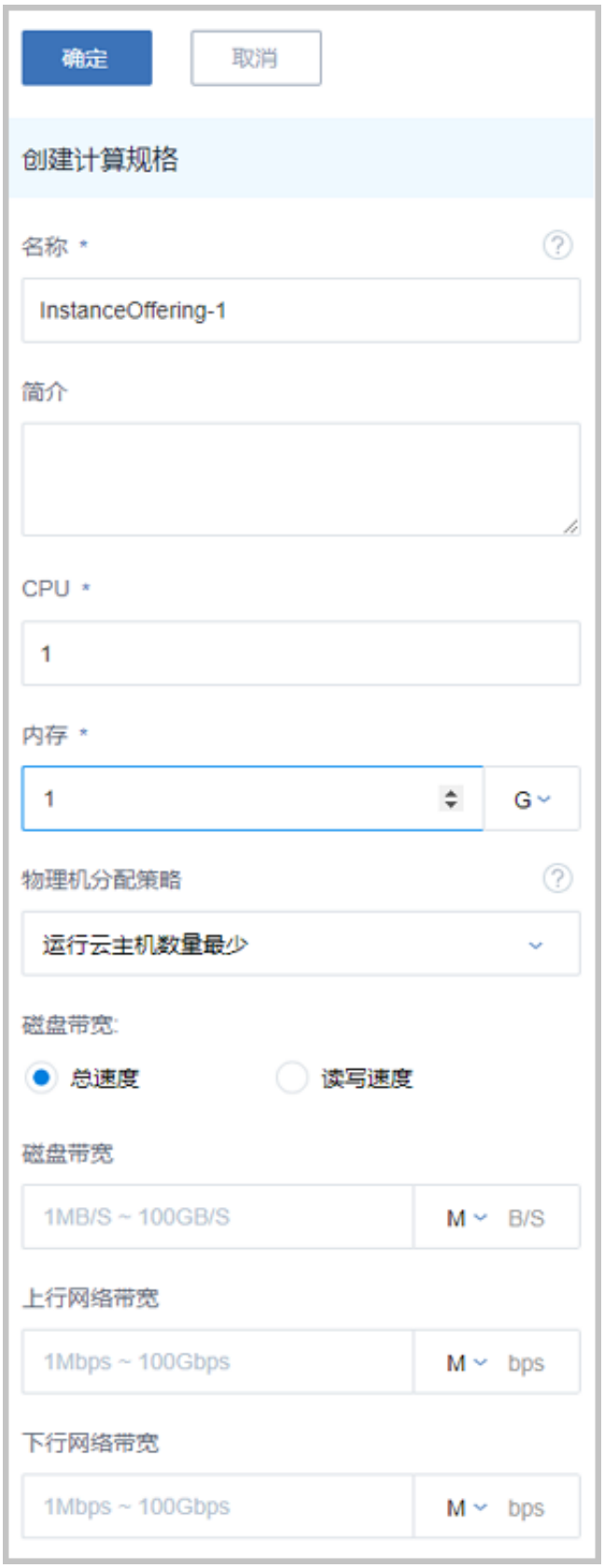
  如图 *227: 读写速度*所示：

  图 227: 读写速度

- **上行网络带宽**：可选项，从云主机上传的网络带宽上限，单位包括：Kbps、Mbps、Gbps，为空时，代表不限制上行网络带宽
- **下行网路带宽**：可选项，从云主机下载的网络带宽上限，单位包括：Kbps、Mbps、Gbps，为空时，代表不限制下行网络带宽。

如图 *228: 创建计算规格*所示，点击**确定**，创建计算规格。

图 228: 创建计算规格



c) 创建ZStack私有云云主机。

在**私有云**界面，点击 **云资源池** > **云主机**，进入**云主机**界面，点击**创建云主机**，在弹出的**创建云主机**界面，可参考以下示例输入相应内容：

- **添加方式**：选择单个
- **名称**：设置私有云云主机名称
- **简介**：可选项，可留空不填
- **计算规格**：选择已创建的计算规格
- **镜像**：选择已添加的镜像
- **网络**：从网络列表中选择已创建的L3-私有网络（云路由网络）

如图 *229:* 创建私有云云主机所示，点击 **确定**，创建私有云云主机。

图 229: 创建私有云云主机

9. 使用云路由网络创建私有云云主机过程中，系统会自动创建云路由器。

10.在阿里云端准备VPC环境，并使用VPC下的虚拟交换机创建ECS实例。

11.在ZStack混合云界面添加阿里云的AccessKey、添加阿里云VPC所在地域和可用区，同步数据。

- 添加阿里云的AccessKey，详情请见《混合云教程》**添加AccessKey**章节。
- 添加地域和可用区，详情请见《混合云教程》**添加地域**和**添加可用区**章节。
- 在**混合云**界面，点击**同步数据**，可将已添加地域和可用区下的阿里云资源同步至本地，包括在阿里云端创建的专有网络VPC、虚拟交换机、ECS实例等信息。

12.在ZStack混合云界面添加大河的AccessKey、同步大河端该账户下所有本地侧连接以及指定地域的所有公有云侧连接。

- 添加大河的AccessKey，详情请见《混合云教程》**添加AccessKey**章节。
- 在**混合云**界面，点击**同步数据**，可将大河端该账户下所有本地侧连接以及指定地域的所有公有云侧连接同步至本地。

13.利用操作向导快速创建大河高速通道。

a) 进入创建大河高速通道向导。

在**操作向导**界面，点击**创建大河高速通道**按钮，可按照向导来创建大河高速通道，如图 *230: 创建大河高速通道*所示：

图 230: 创建大河高速通道

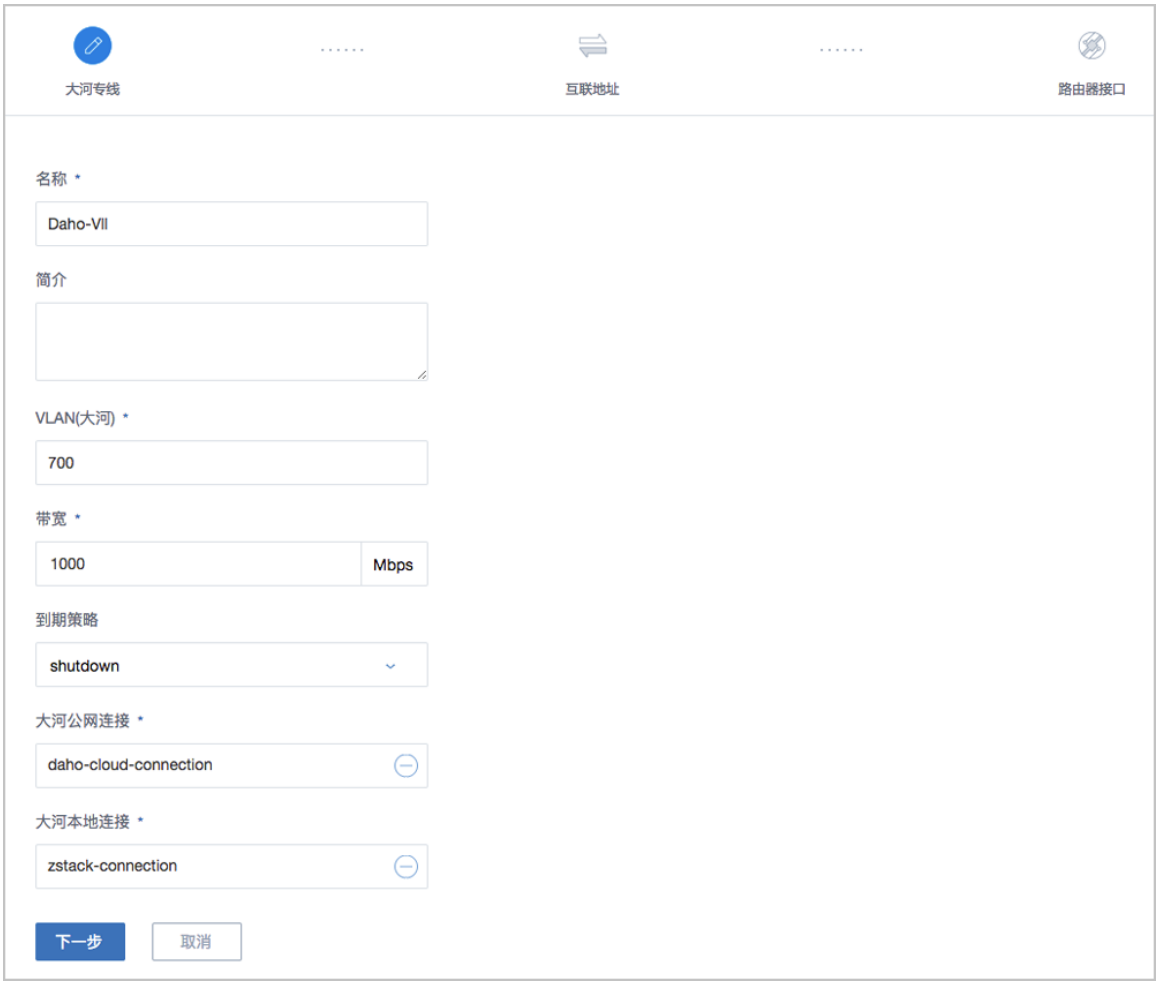
b) 配置大河专线。

在**大河专线**界面，可参考以下示例输入相应内容：

- **名称**：设置大河专线名称
- **简介**：可选项，可留空不填
- **VLAN(大河)**：设置VLAN ID号，需与本地出口交换机二层互通
- **带宽**：设置大河专线的带宽，单位为Mbps
- **到期策略**：可选项，所购买的大河专线服务到期后是否续期，有两种到期策略可选：shutdown（服务到期后停止续期）、renewal（服务到期后自动续期）
- **大河公网连接**：选择大河端提供的公有云侧连接
- **大河本地连接**：选择大河端提供的本地侧连接

如图 *231:* 配置大河专线所示，点击**下一步**，配置互联地址。

图 231: 配置大河专线



大河专线配置完成同时，大河在阿里云端自动购买创建一个边界路由器，以及边界路由器在ZStack侧的路由器接口（VBR接口1），该边界路由器以及路由器接口自动同步至本地。

c) 配置互联地址。

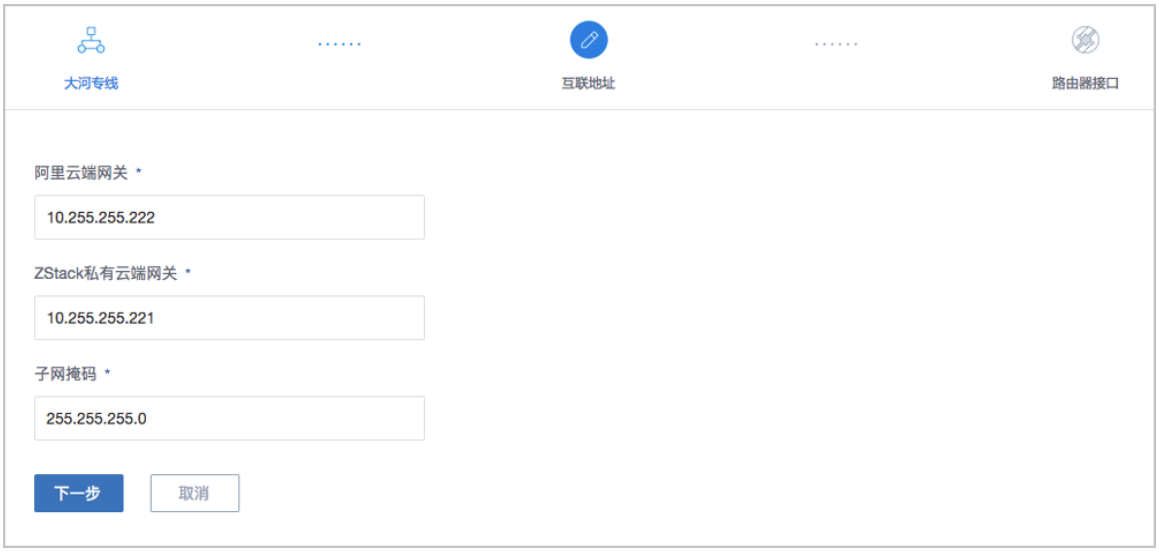
将已准备的一对互联地址：*10.255.255.221*（ZStack私有云端）和*10.255.255.222*（阿里云端）输入边界路由器。

在**互联地址**界面，可参考以下示例输入相应内容：

- **阿里云端网关**：输入*10.255.255.222*到边界路由器，作为阿里云端网关
- **ZStack私有云端网关**：输入*10.255.255.221*到边界路由器，作为ZStack私有云端网关
- **子网掩码**：设置边界路由器的子网掩码，使阿里云端网关和ZStack私有云端网关可以互通

如图 *232: 配置互联地址*所示，点击**下一步**，配置路由器接口。

图 232: 配置互联地址



d) 配置路由器接口。

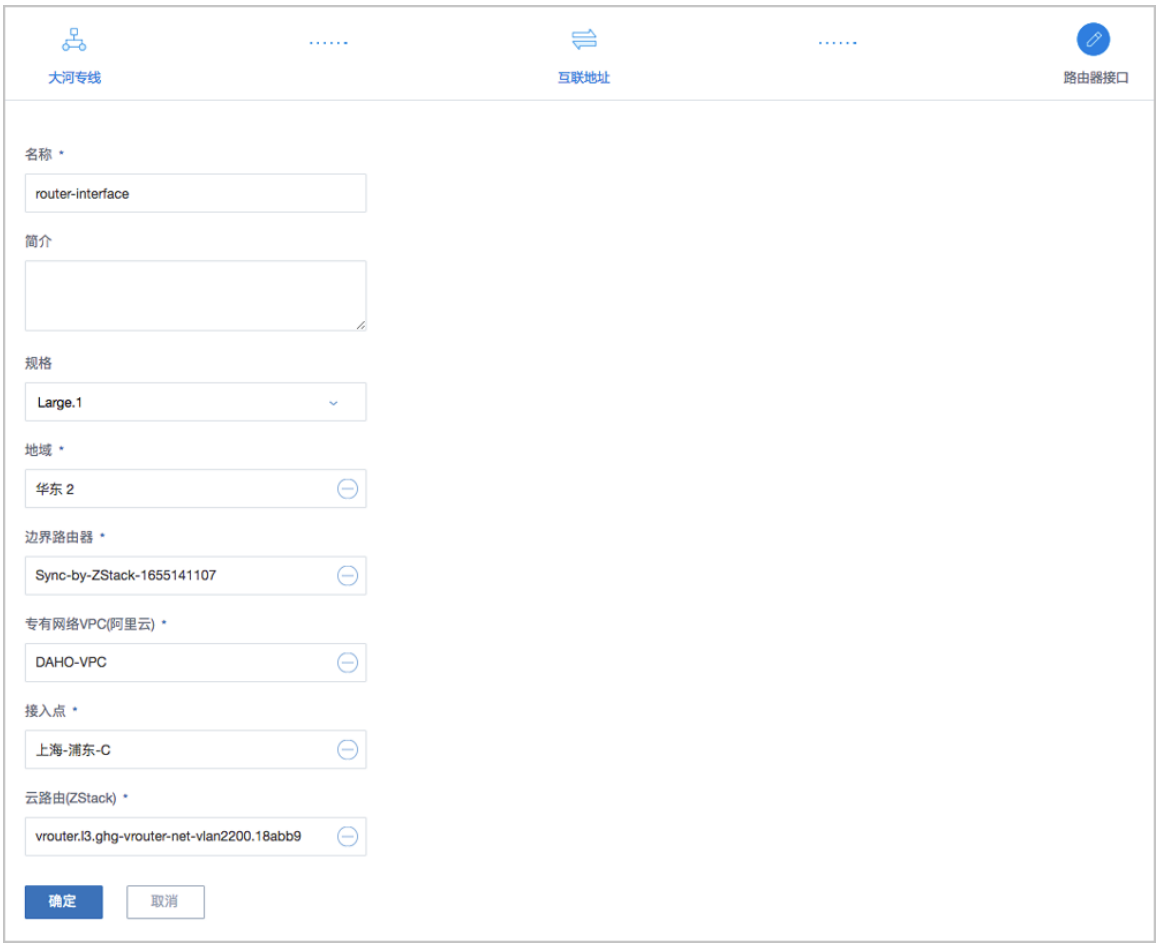
配置一对路由器接口，即：边界路由器在阿里云侧的路由器接口（VBR接口2），以及相应的阿里云VPC虚拟路由器接口。

在**路由器接口**界面，可参考以下示例输入相应内容：

- **名称**：设置这一对路由器接口名称
- **简介**：可选项，可留空不填
- **规格**：可选项，设置边界路由器在阿里云侧路由器接口（VBR接口2）的带宽规格
- **地域**：选择相应的阿里云VPC虚拟路由器所在地域
- **边界路由器**：选择相应的边界路由器
- **专有网络VPC(阿里云)**：选择相应的阿里云VPC
- **接入点**：选择边界路由器在阿里云侧路由器接口（VBR接口2）的接入点
- **云路由(ZStack)**：选择本地云路由器

如图 *233: 配置路由器接口*所示，点击**确定**，创建大河高速通道。

图 233: 配置路由器接口



创建大河高速通道过程中，ZStack将自动配置以下4条路由：

- VPC虚拟路由器自定义路由：目的地址为ZStack私有网络段，下一跳为VPC虚拟路由器接口；
- 边界路由器自定义路由1：目的地址为ZStack私有网络段，下一跳为边界路由器ZStack侧的路由器接口（VBR接口1）；
- 边界路由器自定义路由2：目的地址为ECS VPC网络段，下一跳为边界路由器阿里云侧的路由器接口（VBR接口2）；
- 本地云路由自定义路由：目的地址为ECS VPC网络端，下一跳为阿里云端网关*10.255.255.222*。

14.验证本地云主机与ECS云主机是否可以ping通。

a) 登录本地云主机，检查是否能够ping通ECS云主机。

如图 *234: 本地云主机ping通ECS云主机*所示：

图 234: 本地云主机ping通ECS云主机

```
[root@10-5-0-84 ~]# ip r
default via 10.5.0.1 dev eth0 proto static metric 100
10.5.0.0/16 dev eth0 proto kernel scope link src 10.5.0.84 metric 100
[root@10-5-0-84 ~]# ping 192.168.5.18
PING 192.168.5.18 (192.168.5.18) 56(84) bytes of data.
64 bytes from 192.168.5.18: icmp_seq=1 ttl=62 time=3.65 ms
64 bytes from 192.168.5.18: icmp_seq=2 ttl=62 time=3.52 ms
64 bytes from 192.168.5.18: icmp_seq=3 ttl=62 time=3.65 ms
64 bytes from 192.168.5.18: icmp_seq=4 ttl=62 time=3.49 ms
64 bytes from 192.168.5.18: icmp_seq=5 ttl=62 time=3.24 ms
64 bytes from 192.168.5.18: icmp_seq=6 ttl=62 time=3.51 ms
^C
--- 192.168.5.18 ping statistics ---
```

b) 登录ECS云主机，检查是否能够ping通本地云主机。

如图 *235: ECS云主机ping通本地云主机*所示：

图 235: ECS云主机ping通本地云主机

```
[root@iZbp19kvzy03hnrxlrjieeZ ~]# ip r
default via 192.168.5.253 dev eth0
169.254.0.0/16 dev eth0 scope link metric 1002
192.168.5.0/24 dev eth0 proto kernel scope link src 192.168.5.18
[root@iZbp19kvzy03hnrxlrjieeZ ~]# ping 10.5.0.84
PING 10.5.0.84 (10.5.0.84) 56(84) bytes of data.
64 bytes from 10.5.0.84: icmp_seq=1 ttl=62 time=3.48 ms
64 bytes from 10.5.0.84: icmp_seq=2 ttl=62 time=3.51 ms
64 bytes from 10.5.0.84: icmp_seq=3 ttl=62 time=3.38 ms
64 bytes from 10.5.0.84: icmp_seq=4 ttl=62 time=3.47 ms
64 bytes from 10.5.0.84: icmp_seq=5 ttl=62 time=3.54 ms
64 bytes from 10.5.0.84: icmp_seq=6 ttl=62 time=3.50 ms
64 bytes from 10.5.0.84: icmp_seq=7 ttl=62 time=3.47 ms
64 bytes from 10.5.0.84: icmp_seq=8 ttl=62 time=3.48 ms
^C
--- 10.5.0.84 ping statistics ---
```

注:

- 首次创建大河高速通道建议使用上述操作向导方式。
- 大河高速通道成功创建后，如需修改相关配置，或打算删除重建，建议直接进入**SD-WAN** > **大河** > **大河专线**界面进行手动创建：

  在ZStack**混合云**界面，点击**SD-WAN** > **大河** > **大河专线**，进入**大河专线**界面，点击**创建大河专线**，在弹出的**创建大河专线**界面依次输入相应内容即可。

后续操作

至此，ZStack私有云云主机和阿里云ECS云主机即可使用大河高速通道方式实现互通。

11.2 混合云灾备实践

ZStack以单独的灾备服务功能模块形式提供本地灾备、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。

关于灾备服务的更多介绍，请参考《灾备服务 使用教程》。

11.3 AliyunNAS主存储 部署实践

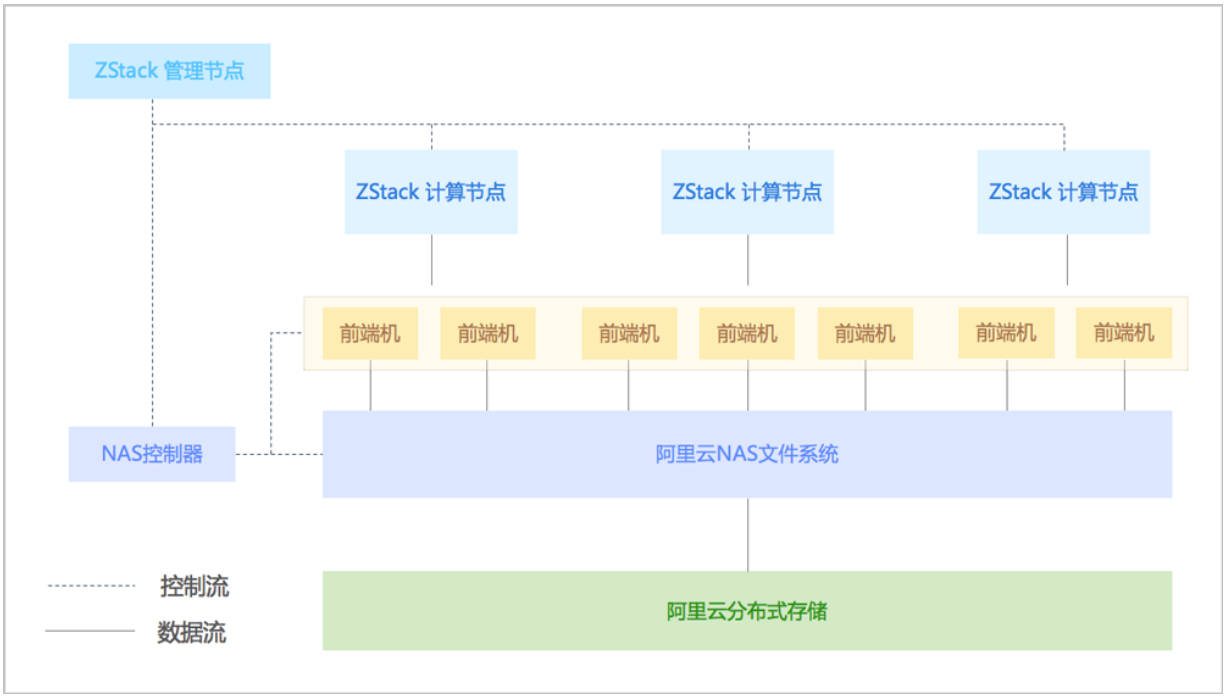
背景信息

ZStack通过无缝对接阿里云NAS，将阿里云的集中式存储还原为分布式存储，并加载到ZStack私有云作为一种新的主存储类型**AliyunNAS**，提供给业务云主机使用。

AliyunNAS主存储需匹配ImageStore类型镜像服务器使用。

ZStack无缝对接阿里云NAS的示意图如图 *236: ZStack无缝对接阿里云NAS*所示：

图 236: ZStack无缝对接阿里云NAS



AliyunNAS主存储的基本部署流程如下：

1. ZStack混合云界面相关配置。

   首次添加**AliyunNAS**主存储，需在ZStack混合云界面进行相关配置：

   1. 设置阿里云服务网关；

2. 添加阿里专有云AccessKey，添加阿里云NAS文件系统所在阿里专有云地域；
3. 创建阿里云NAS文件系统，作为**AliyunNAS**主存储的后端存储；
4. 创建权限组和权限组规则，为文件系统设置访问白名单机制。

2. ZStack私有云界面添加**AliyunNAS**主存储。
3. 管理**AliyunNAS**主存储。

以下为**AliyunNAS**主存储部署实践的具体步骤。

操作步骤

1. ZStack混合云界面相关配置。

a) 设置阿里云服务网关；

在ZStack混合云主菜单，点击**设置**，进入**设置**界面，按实际情况设置阿里云服务网关。

阿里云服务网关的设置格式为：

oss::http://oss.api.com,ecs::ecs.api.com,nas::nas.endpoint.com

本场景下，假定用户部署的阿里专有云数据中心的endpoint为*cn-shanghai-nas.zstack.io*，相应的阿里云服务网关设置为：

NAS::cn-shanghai-nas::cn-shanghai-nas.zstack.io

其中，*cn-shanghai-nas*为阿里专有云数据中心所在地域ID。

b) 添加阿里专有云AccessKey，添加阿里云NAS文件系统所在阿里专有云地域；

1. 添加阿里专有云AccessKey。

在ZStack混合云主菜单，点击**AccessKey**，进入**AccessKey**界面，进入**阿里云**子界面，点击**添加AccessKey**按钮，弹出**添加阿里云AccessKey**界面，可参考以下示例输入相应内容：

- **阿里专有云**：选择添加阿里专有云AccessKey
- **名称**：可自定义输入，用于标识此AccessKey
- **简介**：可选项，可留空不填
- **类型**：选择阿里专有云AccessKey的类型：AliyunNAS
- **AccessKeyID**：输入阿里专有云账户的AccessKey ID，注意确保正确
- **AccessKeySecret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确

注: 首次添加AccessKey会自动设置为默认。

如图 *237: 添加阿里专有云AccessKey界面*所示：

图 237: 添加阿里专有云AccessKey界面

2. 添加阿里专有云地域。

   在ZStack混合云主菜单，点击**数据中心 > 地域**，进入**地域**界面，点击**添加地域**，弹出**添加地域**界面，可参考以下示例输入相应内容：

   - **阿里专有云**：选择添加阿里专有云地域
   - **地域**：选择阿里专有云AccessKey中的地域
   - **简介**：所选地域简介（不可留空）
   - **类型**：选择阿里专有云地域的类型：AliyunNAS

如图 *238: 添加阿里专有云地域-AliyunNAS*所示：

图 238: 添加阿里专有云地域-AliyunNAS

注:

添加阿里专有云AccessKey及相应地域后，无需**同步数据**操作，阿里专有云数据中心的阿里云NAS文件系统相关资源自动同步至本地。

c) 创建阿里云NAS文件系统，作为**AliyunNAS**主存储的后端存储；

在ZStack混合云主菜单，点击**产品** > **阿里云NAS** > **文件系统**，进入**文件系统**界面，点击**创建文件系统**，弹出**创建文件系统**界面，可参考以下示例输入相应内容：

- **地域**：选择阿里云NAS文件系统所在阿里专有云地域
- **选择方式**：可选择添加已有文件系统或创建文件系统
  - **添加已有**：

    若用户在阿里专有云数据中心已部署阿里云NAS文件系统，可直接添加到ZStack混合云平台。

    选择添加已有文件系统，需设置以下内容：

- **文件系统**：将已部署的阿里云NAS文件系统添加到ZStack混合云平台
- **名称**：设置文件系统名称
- **简介**：可选项，可留空不填

如图 *239: 添加已有文件系统*所示：

图 239: 添加已有文件系统

- **创建**：

用户也可在ZStack混合云界面创建阿里云NAS文件系统。

选择创建文件系统，需设置以下内容：

- **名称**：设置文件系统名称
- **简介**：可选项，可留空不填
- **存储类型**：可选择容量型（Capacity）或性能型（Performance）
- **协议类型**：支持标准的NFS、SMB文件访问协议

如图 *240:* 创建文件系统所示：

图 240: 创建文件系统

d) 创建权限组和权限组规则，为文件系统设置访问白名单机制。

1. 创建权限组。

   在ZStack混合云主菜单，点击**产品** > **阿里云NAS** > **权限组**，进入**权限组**界面，点击**创建权限组**，弹出**创建权限组**界面，可参考以下示例输入相应内容：

   - **地域**：选择阿里云NAS文件系统所在阿里专有云地域
   - **选择方式**：可选择添加已有权限组或创建权限组
     - **添加已有**：

若用户在阿里专有云数据中心已创建权限组，可直接将该权限组添加到ZStack混合云平台。

注: 仅支持添加经典网络类型的权限组。

如选择添加已有权限组，需设置以下内容：

- **权限组**：将已创建的经典网络类型的权限组添加到ZStack混合云平台
- **名称**：设置权限组名称
- **简介**：可选项，可留空不填

如图 *241:* 添加已有权限组所示：

图 241: 添加已有权限组

- **创建**：

用户也可在ZStack混合云界面创建权限组。

注: 仅支持创建经典网络类型的权限组。

如选择创建权限组，需设置以下内容：

- **名称**：设置权限组名称
- **简介**：可选项，可留空不填
- **网络类型**：默认显示经典网络（classic）

如图 *242: 创建权限组*所示：

图 242: 创建权限组

2. 创建权限组规则。
   - 若用户在阿里专有云数据中心已创建经典网络类型的权限组，并向权限组添加相应规则，将该权限组添加到ZStack混合云平台，权限组内相应规则自动同步到本地。
   - 用户也可在ZStack混合云界面创建权限组规则。

在**权限组**界面，选中某一权限组，展开其详情页，进入**权限组规则**子页面，点击权限组规则右侧的**操作** > **创建权限组规则**按钮，弹出**创建权限组规则**界面，可参考以下示例输入相应内容：

- **网络CIDR**：本条规则的授权对象，可指定单个IP地址或网段
- **优先级**：优先级范围为**1-100**，**1**为最高优先级

> **注:** 当同一个授权对象匹配到多条规则时，高优先级规则将覆盖低优先级规则。

- **读写规则**：允许授权对象对文件系统进行只读操作（RDONLY）或读写操作（RDWR）

如图 *243:* 创建权限组规则所示：

图 243: 创建权限组规则

2. ZStack私有云界面添加**AliyunNAS**主存储。

在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**界面，点击**添加主存储**按钮，弹出**添加主存储**界面，可参考以下示例输入相应内容：

- **区域**：显示当前区域
- **名称**：输入主存储名称
- **简介**：可选项，可留空不填

- **类型**：选择AliyunNAS
- **文件系统**：选择已在ZStack混合云界面创建好的阿里云NAS文件系统
- **权限组**：选择已在ZStack混合云界面创建好的权限组
- **挂载路径**：挂载路径是物理机上的目录以供挂载阿里云NAS文件系统的挂载点

  注:

  - 如果输入的目录不存在，系统将会自动创建该目录；
  - 不能使用以下系统目录，使用系统目录可能会导致物理机异常。
    - */*
    - */dev/*
    - */proc/*
    - */sys/*
    - */usr/bin*
    - */bin*
- **集群**：选择主存储需要挂载的集群

如图 *244: 添加AliyunNAS主存储*所示：

图 244: 添加AliyunNAS主存储

3. 管理**AliyunNAS**主存储。

   在**主存储**界面，可对已添加的**AliyunNAS**主存储进行管理，支持主存储的启用、停用、重连、加载/卸载集群、进入维护模式、删除等操作，以及对主存储上创建的云主机、云盘资源进行管理，并提供可视化监控、报警和审计功能。

后续操作

至此，**AliyunNAS**主存储部署实践介绍完毕。

11.4 AliyunEBS主存储 | AliyunEBS镜像服务器 部署实践

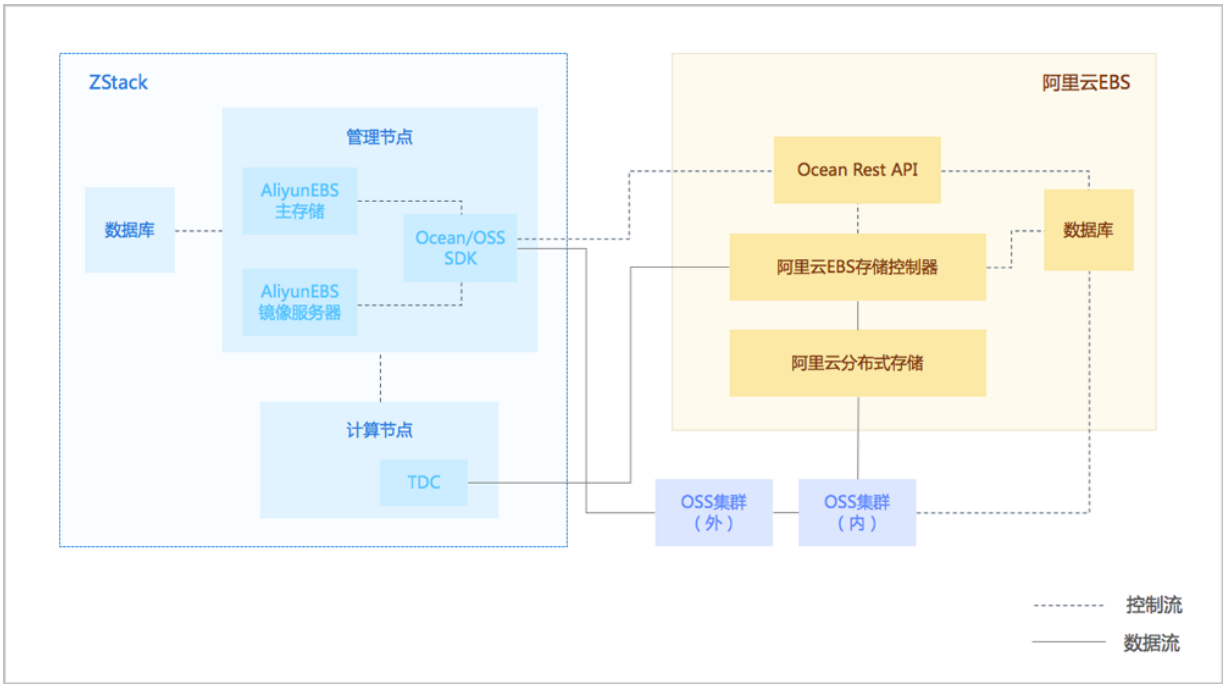
背景信息

ZStack通过无缝对接阿里云EBS，将阿里云的高性能云原生分布式块存储加载到ZStack私有云，作为一种新的主存储类型**AliyunEBS**，提供给业务云主机使用。

ZStack通过无缝对接阿里云OSS，将阿里云的对象存储加载到ZStack私有云，作为一种新的镜像服务器类型**AliyunEBS**，与**AliyunEBS**主存储配合使用，提供镜像存储服务。

ZStack无缝对接阿里云EBS和阿里云OSS的示意图如图 *245: ZStack无缝对接阿里云EBS和阿里云OSS*所示：

图 245: ZStack无缝对接阿里云EBS和阿里云OSS



部署**AliyunEBS**主存储和**AliyunEBS**镜像服务器的基本流程如下：

1. ZStack混合云界面相关配置。

   首次添加**AliyunEBS**主存储和**AliyunEBS**镜像服务器，需在ZStack混合云界面进行相关配置：

   1. 添加阿里专有云AccessKey，类型选择**AliyunEBS**；
   2. 添加阿里云EBS所在阿里专有云地域以及该地域下的可用区；
   3. 添加同一地域下的OSS Bucket。

2. ZStack私有云界面添加**AliyunEBS**主存储。

3. ZStack私有云界面添加**AliyunEBS**镜像服务器。
4. 管理**AliyunEBS**主存储和**AliyunEBS**镜像服务器。

以下为部署**AliyunEBS**主存储和**AliyunEBS**镜像服务器的具体实践步骤。

操作步骤

1. ZStack混合云界面相关配置。

   a) 添加阿里专有云AccessKey，类型选择**AliyunEBS**；

   在ZStack混合云主菜单，点击**AccessKey**，进入**AccessKey**界面，进入**阿里云**子界面，点击**添加AccessKey**按钮，弹出**添加阿里云AccessKey**界面，可参考以下示例输入相应内容：

   - **阿里专有云**：选择添加阿里专有云AccessKey
   - **名称**：可自定义输入，用于标识此AccessKey
   - **简介**：可选项，可留空不填
   - **类型**：选择阿里专有云AccessKey的类型：AliyunEBS
   - **AccessKeyID**：输入阿里专有云账户的AccessKey ID，注意确保正确
   - **AccessKeySecret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确

   注: 首次添加AccessKey会自动设置为默认。

   如图 *246: 添加阿里专有云AccessKey界面*所示：

   图 246: 添加阿里专有云AccessKey界面

b) 添加阿里云EBS所在阿里专有云地域以及该地域下的可用区；

1. 添加阿里云EBS所在阿里专有云地域。

   在ZStack混合云主菜单，点击**数据中心 > 地域**，进入**地域**界面，点击**添加地域**，弹出**添加地域**界面，可参考以下示例输入相应内容：

   - **阿里专有云**：选择添加阿里专有云地域
   - **地域**：输入阿里专有云AccessKey中的地域
   - **简介**：所选地域简介（不可留空）
   - **类型**：选择阿里专有云地域的类型：AliyunEBS
   - **Endpoint**：输入Ocean对外服务的访问域名

   注:

- Ocean以HTTP RESTful API形式对外提供服务；
- 输入格式为：*http://Ocean_Server_Domain:Port/ocean/api*；
- 访问不同地域时需要不同的域名。

如图 *247: 添加阿里专有云地域-AliyunEBS*所示：

图 247: 添加阿里专有云地域-AliyunEBS

2. 添加该地域下的可用区。

   添加阿里专有云地域后，将自动添加该地域下的可用区，若未自动添加，请执行以下手动添加可用区操作。

   在**地域**界面，点击已添加的阿里专有云地域，进入**地域**详情页，点击**可用区**，进入**可用区**页面，点击**操作** > **添加**，弹出**添加可用区**界面，可参考以下示例输入相应内容：

   - **可用区**：下拉菜单显示了所选地域下全部可用区列表，可从中选择一个
   - **简介**：所选可用区简介（不可留空）

如图 *248: 添加可用区*所示：

图 248: 添加可用区

c) 添加同一地域下的OSS Bucket。

在**地域**界面，点击已添加的阿里专有云地域，进入**地域**详情页，点击**Bucket**，进入**Bucket**页面，点击**操作** > **添加Bucket**，弹出**添加Bucket**界面，可参考以下示例输入相应内容：

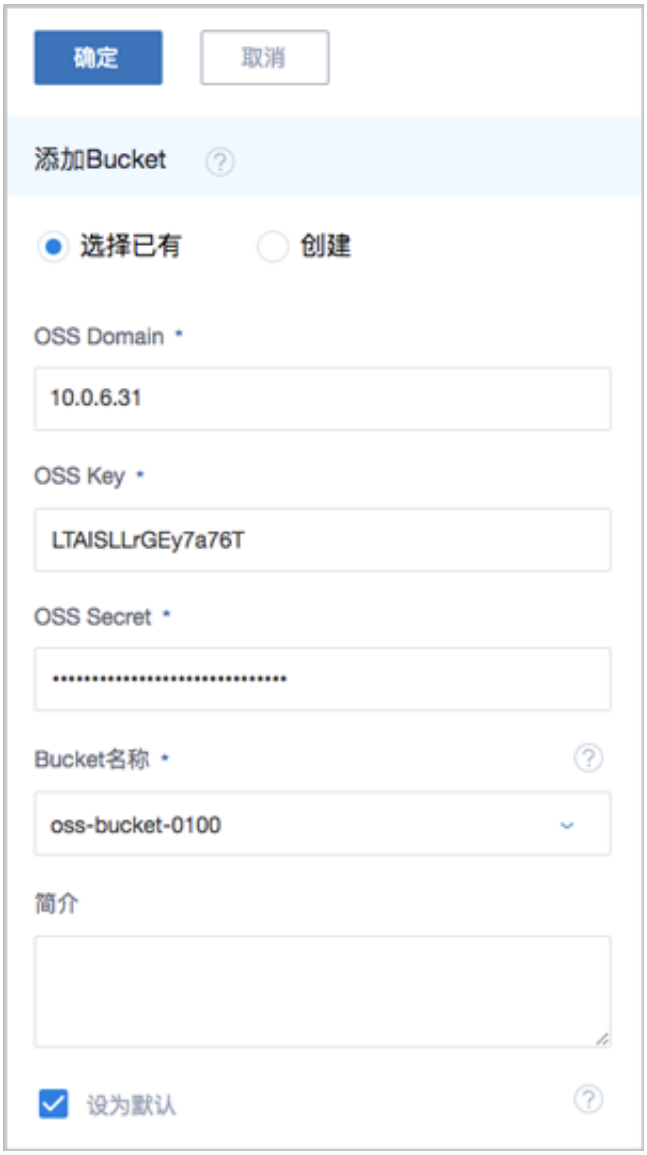
- 选择已有Bucket：
  - **选择已有**：选择添加该地域下的已有Bucket
  - **OSS Domain**：输入OSS对外服务的访问域名

    注:

    - OSS以HTTP RESTful API形式对外提供服务；
    - 输入格式为：*OSS_Server_Domain*；
    - 访问不同地域时需要不同的域名。
  - **OSS Key**：输入OSS的AccessKey ID，注意确保正确
  - **OSS Secret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确
  - **Bucket名称**：下拉菜单显示了所选地域下全部已有Bucket列表，可从中选择一个
  - **简介**：可选项，可留空不填
  - **设为默认**：是否设为默认，添加Bucket时，默认勾选此项

如图 *249: 选择已有Bucket*所示：

图 249: 选择已有Bucket



- 创建Bucket：
  - **创建**：选择在该地域下创建Bucket
  - **OSS Domain**：输入OSS对外服务的访问域名

    注:

    - OSS以HTTP RESTful API形式对外提供服务；
    - 输入格式为：*OSS_Server_Domain*；
    - 访问不同地域时需要不同的域名。

- **OSS Key**：输入OSS的AccessKey ID，注意确保正确
- **OSS Secret**：输入此AccessKey ID对应的AccessKey Secret，注意确保正确
- **Bucket名称**：设置Bucket名称，Bucket名称全局唯一，不可重复
- **简介**：可选项，可留空不填
- **设为默认**：是否设为默认，添加Bucket时，默认勾选此项

如图 *250: 创建Bucket*所示：

图 250: 创建Bucket

2. ZStack私有云界面添加**AliyunEBS**主存储。

   在ZStack私有云主菜单，点击**硬件设施** > **主存储**按钮，进入**主存储**界面，点击**添加主存储**按钮，弹出**添加主存储**界面，可参考以下示例输入相应内容：

- **区域**：显示当前区域
- **名称**：输入主存储名称
- **简介**：可选项，可留空不填
- **类型**：选择AliyunEBS
- **URL**：输入Ocean API的Endpoint

注:

- **AliyunEBS**主存储通过该URL向Ocean Server端发送请求；
- 输入格式为：*http://Ocean_Server_Domain:Port/ocean/api*。

- **可用区**：选择已在ZStack混合云界面添加好的可用区

注:

- 一个**AliyunEBS**主存储仅允许添加一个可用区；
- 一个可用区可添加到多个**AliyunEBS**主存储。

- **TDC配置内容**：对TDC模块进行参数配置

注:

- TDC是安装在计算节点上的程序，用于与阿里云存储节点通信（例如Nuwa），TDC配置是计算节点访问存储节点的相关配置；
- TDC配置参数包括：物理机访问TDC服务的端口、TDC Region、两组River Master（包括URL、Server IP、代理IP）、阿里云EBS所在集群，请按实际情况配置。

  TDC配置示例如下：

```
{
  "tdcPort": "20120",
  "tdcRegion": "region1",
  "riverMaster": "nuwa://ECS-river/sys/houyi/river_master",
  "server": "192.168.0.1:10240,192.168.0.2:10240,192.168.0.3:10240",
  "proxy": "192.168.1.1:10240,192.168.1.2:10240,192.168.1.3:10240",
  "cluster": "ECS-river"
}
```

  可展开编辑器，如图 *251:* 展开编辑器所示：

图 251: 展开编辑器

- **集群**：选择主存储需要挂载的集群

如图 *252: 添加AliyunEBS主存储*所示：

图 252: 添加AliyunEBS主存储


确定
取消
添加主存储
区域: ZONE-1
名称 *
AliyunEBS主存储
简介
类型
AliyunEBS
URL *
http://10.1.0.16:18080/ocean/api
可用区 *
shanghai-az

3. ZStack私有云界面添加**AliyunEBS**镜像服务器。

   在ZStack私有云主菜单，点击**硬件设施** > **镜像服务器**按钮，进入**镜像服务器**界面，点击**添加镜像服务器**按钮，弹出**添加镜像服务器**界面，可参考以下示例输入相应内容：

   - **区域**：显示当前区域
   - **名称**：输入镜像服务器名称
   - **简介**：可选项，可留空不填
   - **类型**：选择AliyunEBS
   - **URL**：输入Ocean API的Endpoint

     注:

     - **AliyunEBS**镜像服务器通过该URL向Ocean Server端发送请求；
     - 输入格式为：*http://Ocean_Server_Domain:Port/ocean/api*。
   - **Bucket**：选择已在ZStack混合云界面添加好的OSS Bucket

如图 *253: 添加AliyunEBS镜像服务器*所示：

图 253: 添加AliyunEBS镜像服务器

4. 管理**AliyunEBS**主存储和**AliyunEBS**镜像服务器。

   - 管理**AliyunEBS**主存储

     在**主存储**界面，可对已添加的**AliyunEBS**主存储进行管理，支持主存储的启用、停用、重连、加载/卸载集群、进入维护模式、删除等操作，以及对主存储上创建的云主机、云盘资源进行管理，并提供可视化监控、报警和审计功能。

   - 管理**AliyunEBS**镜像服务器

     在**镜像服务器**界面，可对已添加的**AliyunEBS**镜像服务器进行管理，支持镜像服务器的启用、停用、重连、删除等操作，以及对镜像服务器上的镜像资源进行管理，并提供可视化监控、报警和审计功能。

后续操作

至此，**AliyunEBS**主存储和**AliyunEBS**镜像服务器部署实践介绍完毕。

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。