

ALIBABA CLOUD

阿里云

阿里云最佳实践
网络组网

文档版本：20220402

 阿里云

法律声明

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

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

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.中小企业上云多地域办公组网(SAG)	05
2.基于转发路由器构建企业级组网最佳实践	07
3.中小企业基于SAG APP实现云上移动办公	09
4.通过私网访问云服务	10
5.多账号多vpc企业组网	12
6.应用IPv6改造	13
7.组建多可用区多地域的混合云	14
8.在线教育全球部署网络规划	16
9.互联网业务全球化互通组网	18
10.游戏出海加速	19

1.中小企业上云多地域办公组网(SAG)

企业分布在全国各地的分支机构，使用阿里云建立可靠且易维护的云上内网环境。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

场景描述

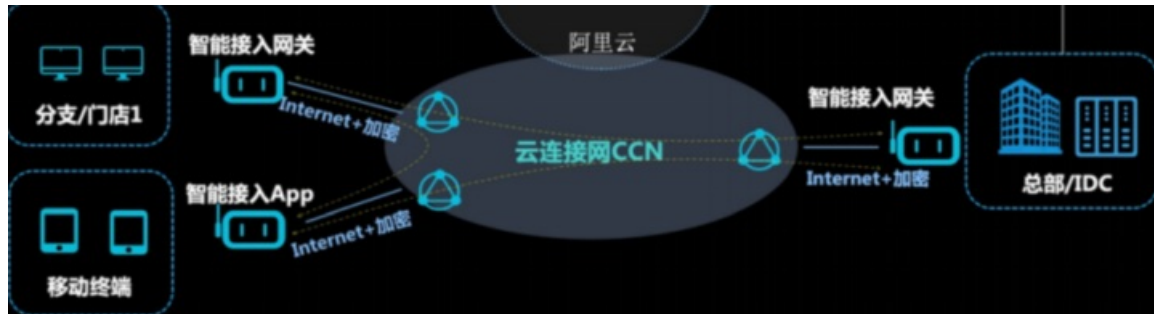
企业存在三个网络：阿里云VPC（北京）、云下北京IDC，云下上海IDC。SAG可就近接入阿里云上海接入点CCN网络，并通过CEN走阿里内网高质量链路连接北京阿里云VPC。

阿里云VPC（北京）、云下北京IDC，云下上海IDC三点可互相通信。如全国有很多分公司，只需每个分公司购买一个SAG即可接入。

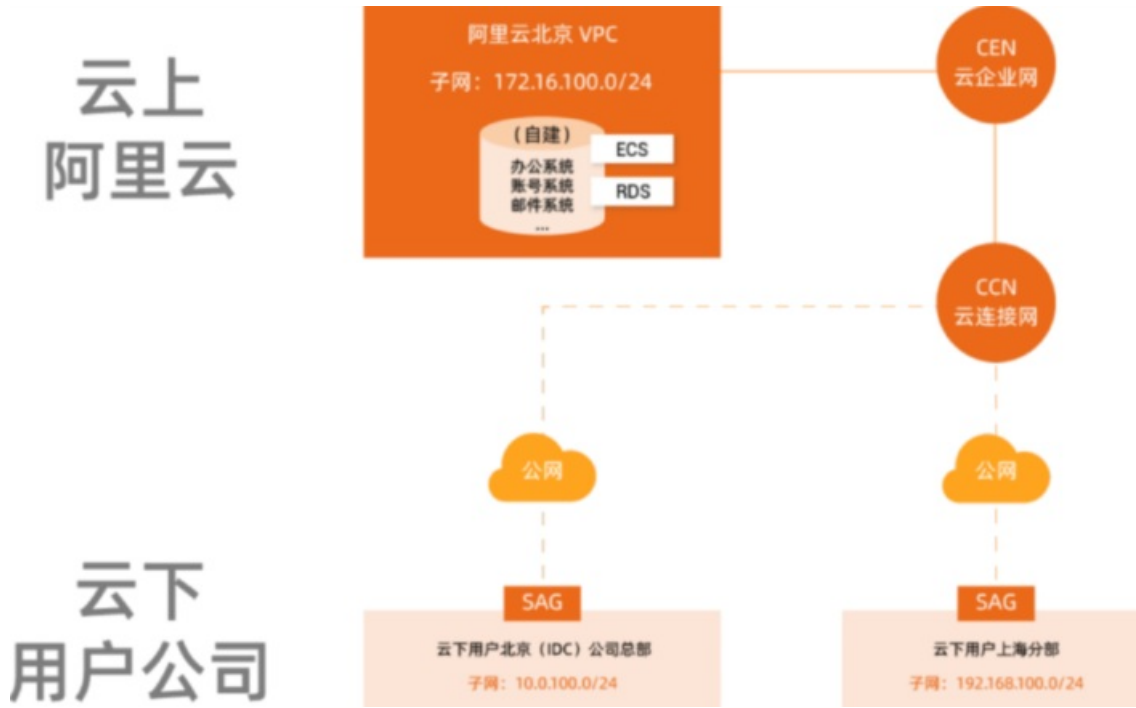
解决问题

- 多地域办公网络通过阿里云互通。
- 较低成本解决稳定高速异地互联。
- 复杂业务场景下软硬件方案结合。

业务架构图



部署架构图



2.基于转发路由器构建企业级组网最佳实践

由于业务需要，客户在云上同地域有多个VPC，希望可以实现多VPC之间的灵活通信，如全部VPC之间可以互相访问、部分VPC隔离、所有流量引流至安全VPC做安全管控、所有VPC统一互联网出口等场景。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多最佳实践](#)

场景描述

本篇最佳实践按照网络规划在中国（香港）地域创建三个VPC以及多个交换机，同时在交换机内部署服务器ECS，通过执行ping命令检查网络连通性。然后再创建云企业网以及转发路由器将这三个VPC加载进来。基于这样的网络环境，通过配置VPC路由和转发路由器路由，实现以下四个场景：

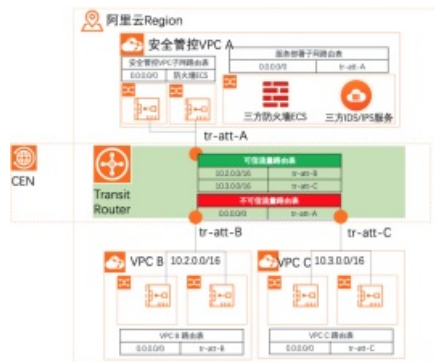
1、多VPC之间互联互通



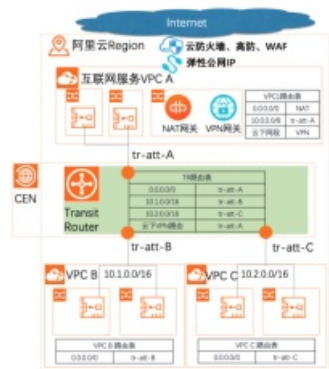
2、部分VPC隔离



3、服务链（东西向安全）



4、统一互联网出口（南北向安全）



解决问题

- 实现灵活的互通、隔离、引流策略
- VPC间的内网互访流量经过三方安全设备管控
- 统一多VPC的互联网访问出口，提高业务安全性

3. 中小企业基于SAG APP实现云上移动办公

公司已在阿里云上部署了应用服务，如OA系统、办公管理后台等，公司员工日常通过办公网络访问云上资源。随着公司的不断发展，移动办公的场景越来越多，如出差、在家办公等。公司运维人员也要求在任何时间和任何地方都能安全访问云资源。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多最佳实践](#)

场景描述

本篇最佳实践会在华东2上海和美西硅谷创建跨地域的VPC，在VPC内部署ECS模拟办公系统应用。购买SAG APP版并挂载到云连接网CCN，通过云企业网CEN将云上跨地域的VPC和云连接网CCN打通，实现内网互联互通。登录SAG客户端之后，就可以通过内网IP访问云上资源。还可以通过PrivateZone解析通过内网域名访问部署在云上的应用。

解决问题

- 客户端一键接入上云，配置自动化
- 城域网Internet就近接入，快速高效
- 数据加密传输，满足安全性要求
- 阿里云控制台统一配置管理

方案架构



4.通过私网访问云服务

阿里云产品服务以OpenAPI的方式对外提供接口调用，默认提供公网接入地址。客户部署在阿里云VPC内的应用由于安全合规或提升访问效率要求通过内网调用OpenAPI。另一方面，客户部署在阿里云VPC内的服务，也希望实现跨VPC甚至跨账号的内网访问。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多最佳实践](#)

场景描述

出于降低公网数据传输风险，提升访问效率降低时延的目的，越来越多的客户倾向通过内网调用阿里云OpenAPI，或者通过内网访问部署在云上VPC的服务。如下图所示，公网访问的实现路径：云服务暴露Internet公网服务入口，用户通过EIP出公网，走公共互联网访问目标服务。

解决问题

- 内网调用阿里云OpenAPI
- 同账号的VPC间私网访问
- 跨账号的VPC间私网访问
- 保障数据传输安全
- 提升访问效率，降低访问时延

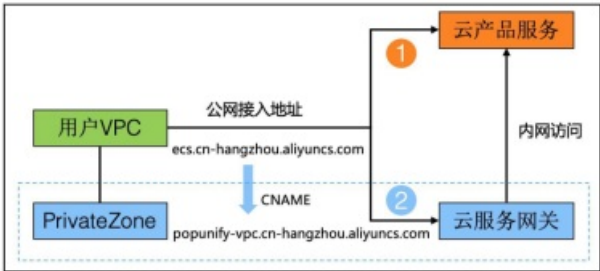
方案架构

内网调用阿里云 OpenAPI

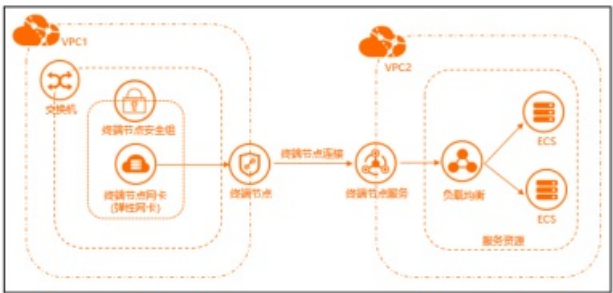
方案一：使用 VPC 接入地址



方案二：PrivateZone 解析互联网域名



内网访问客户 VPC 内服务



5.多账号多vpc企业组网

本篇实践模拟一家集团公司，该公司有多家分公司，结合企业的组织结构，通过资源目录来管理账号体系，多账号下分别创建VPC，根据项目独立分账的要求，对应VSwitch下单独挂载增强型NAT网关。项目之间通过NACL彼此隔离，都以其项目所在VSwitch的NAT网关作为流量出口（典型的分布式部署方式，另外一种典型的部署方式是集中式共享NAT网关），NAT实例通过Tag来做分账，VPC与VPC之间通过CEN组网。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多最佳实践](#)

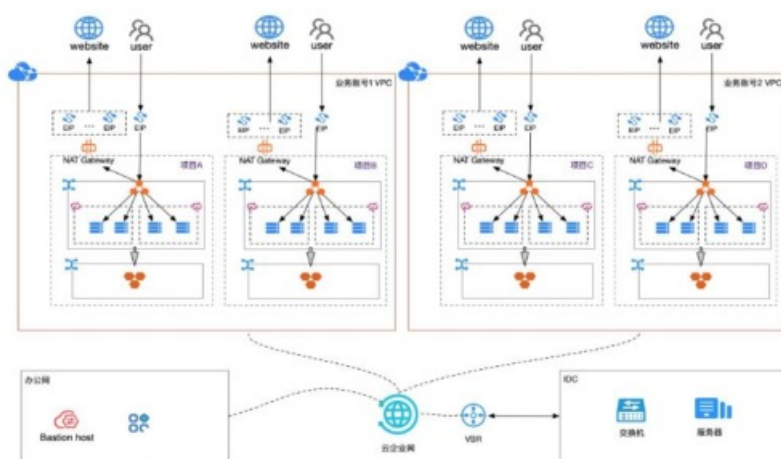
场景描述

针对一些刚开始上云的企业，他们往往业务先行，需要在很短的时间内完成业务系统的搬迁，在迁移过程中，账号体系的设计和网络的规划必不可少。账号是资源的容器，对于有多个法律实体分公司的集团，各个分公司有差异化的结算关系，只有一个账号无法满足集团管理需求，拥有多个阿里云账号，能够很好的应对这些问题。网络架构，关系到企业业务的运行、应用之间的调用、业务的扩展等，我们根据多家企业云上的实践，总结了多账号多VPC企业组网方案。

方案优

- 按照企业组织结构构建账号系统，通过资源目录有效将账号组织起来。
- 典型网络规划，满足企业为了不同业务的发展以及分权分账等诉求。
- 采用增强型NAT网关，支持一个VPC下挂载多个NAT实例。

方案架构



6.应用IPv6改造

使用阿里云服务IPv6能力进行云上业务系统改造。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

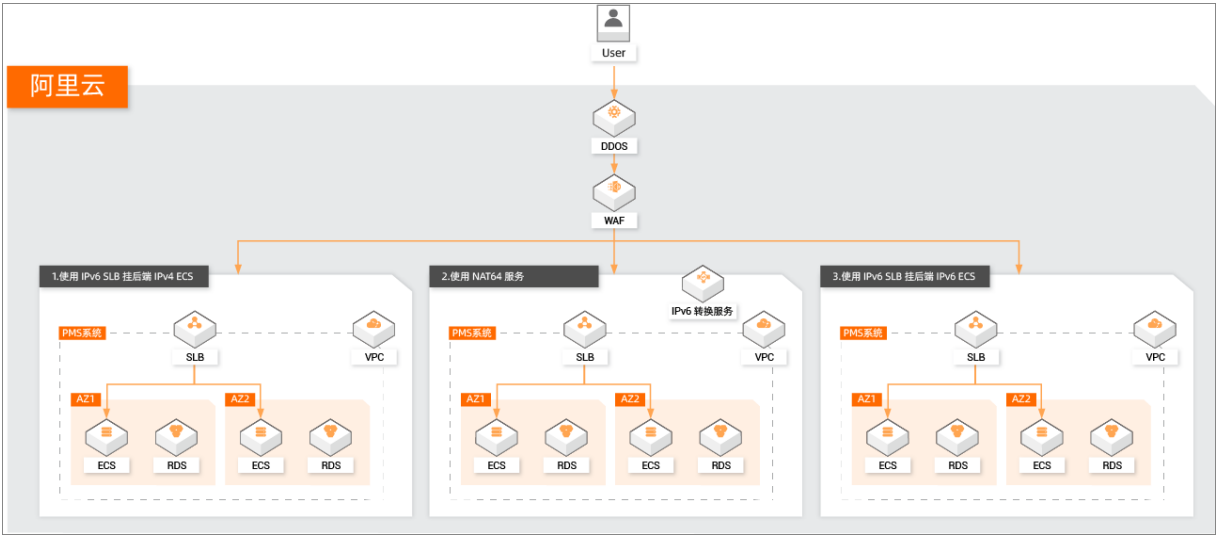
场景描述

- 场景一：对于IPv4-only的云服务器，通过DNS域名解析+IPv6转换服务，快速支持对外提供IPv6 访问能力。
- 场景二：对于双栈云服务器，构建应用环境。

解决问题

- 改造技术复杂度高。
- 改造任务时间紧。
- 改造所需人力和设备成本较高。

部署架构图



7. 组建多可用区多地域的混合云

使用阿里云产品一站式组建多地域混合云，降低用户组网成本。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

场景描述

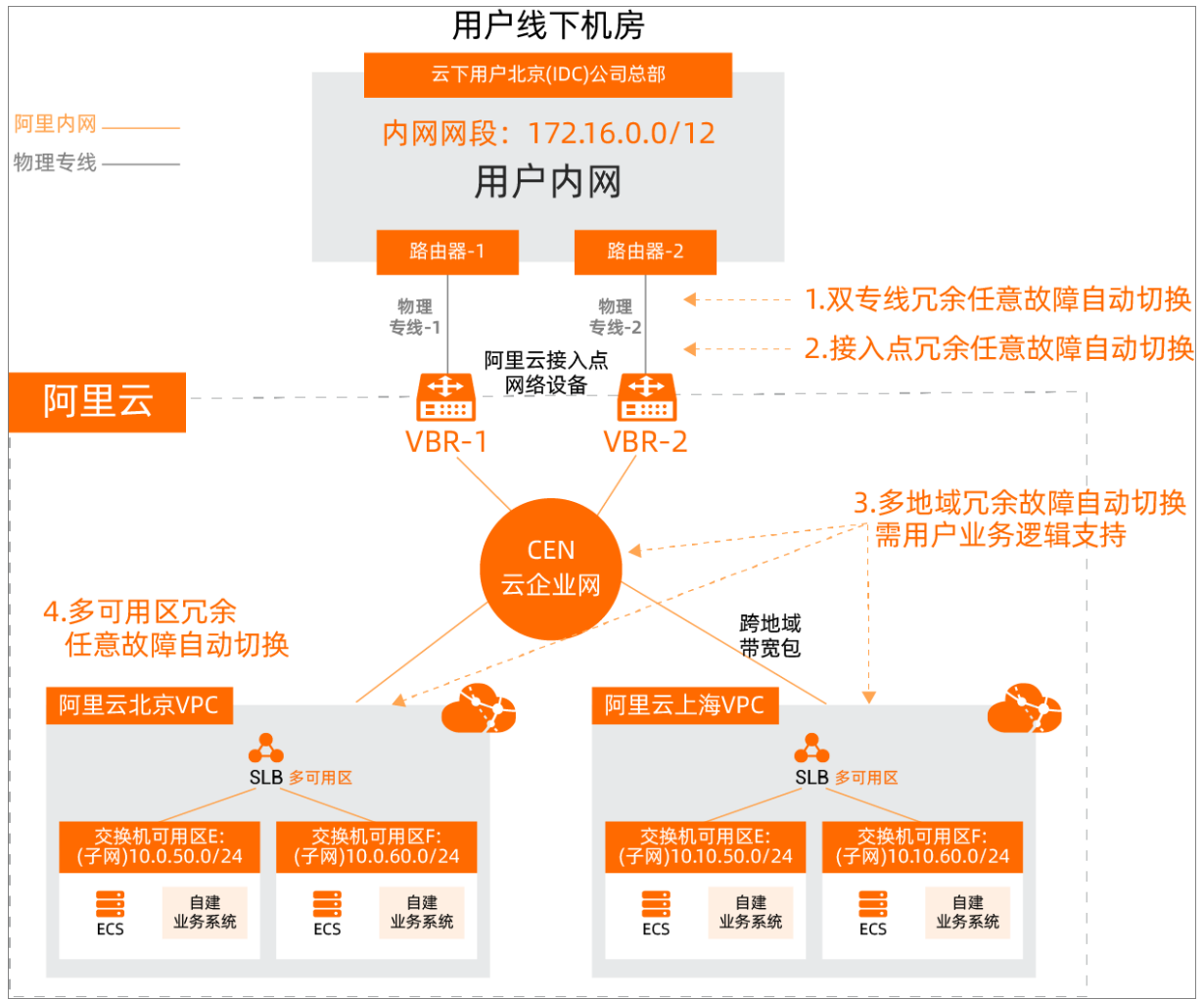
无特定行业属性，对云下有IDC的用户，上云建立多地域多可用区高稳定性的业务架构，组建混合云用户都可适用。

物理专线是打通IDC到云上内网通道的最高质量和稳定性最好方式，但成本较高，交付周期长。

解决问题

- 云下用户IDC应对业务突增弹性扩容能力不足。
- 云下用户IDC业务需要多地域冗余。
- 云上阿里云业务需要多地域冗余。
- 云上阿里云业务需要多可用区冗余。

部署架构图



8.在线教育全球部署网络规划

提供上云第一步的网络规划方案设计与云基础产品操作指导，适用于新上云用户。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践。](#)

场景描述

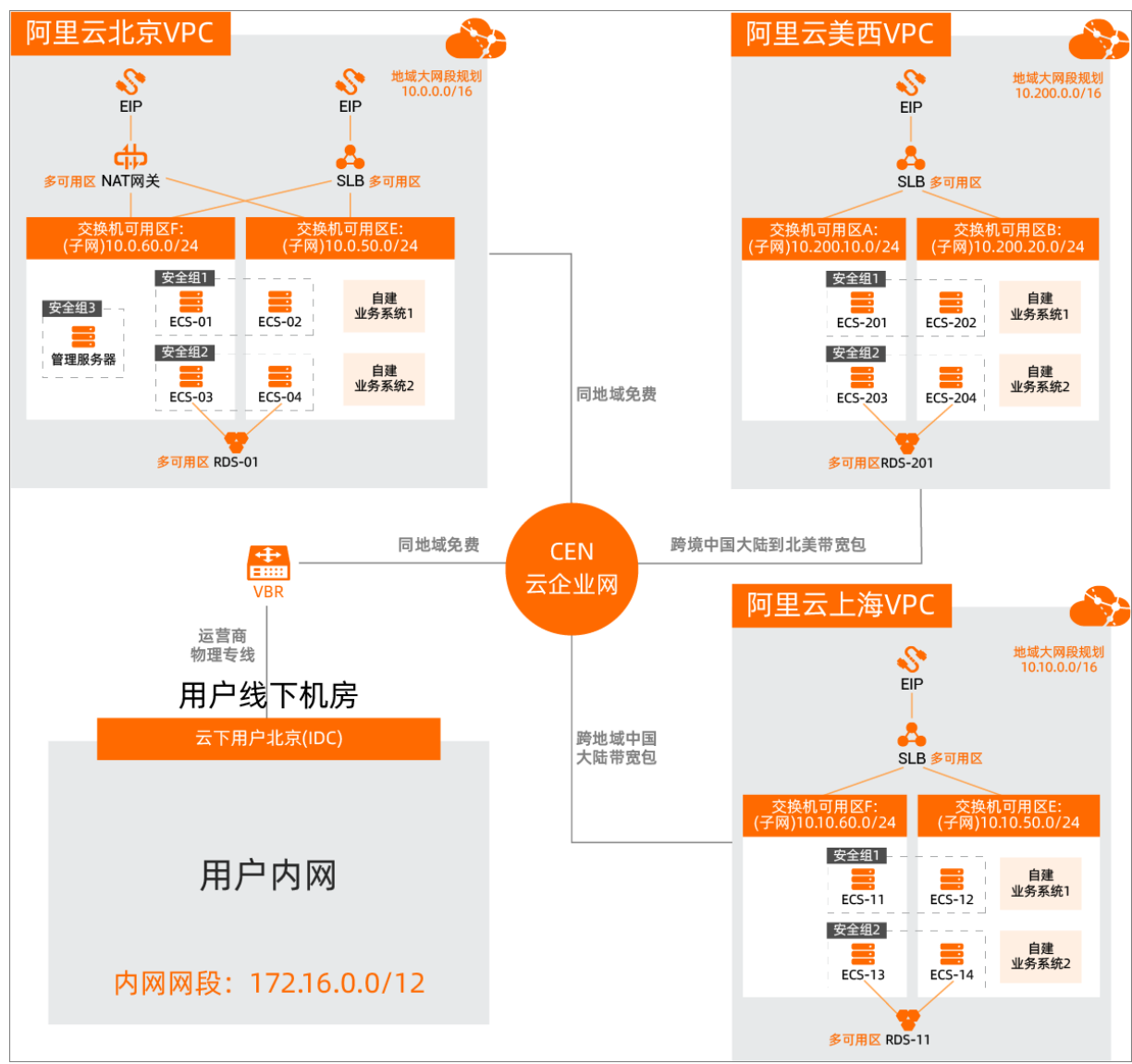
目前国内在线教育行业主流已经演化到移动互联网时代，部分业务已经步入大数据时代。在线教育的教师大部分和学员不在相同区域，设置不在同一个国家。

例如场景的英语类在线教育，教师在北美，学员分布在国内各地区。如何保障跨地区、甚至跨国家的在线教育网络质量，是非常核心的一个技术问题。

解决问题

- 如何架构全球化组网。
- 打通国内混合云和多云环境。
- 复杂网络环境下的安全隔离方案。
- 高品质的视频体验。
- 在线教育学员随时可以查看教学回放录像。

部署架构图



9. 互联网业务全球化互通组网

本方案适用于从事全球化业务的客户借助全球互通的网络，实现多地域的互通，包括网络规划、网络互通和数据互通等。

直达最佳实践

[点击查看最佳实践详情](#)

更多最佳实践

[点击查看更多阿里云最佳实践](#)

场景描述

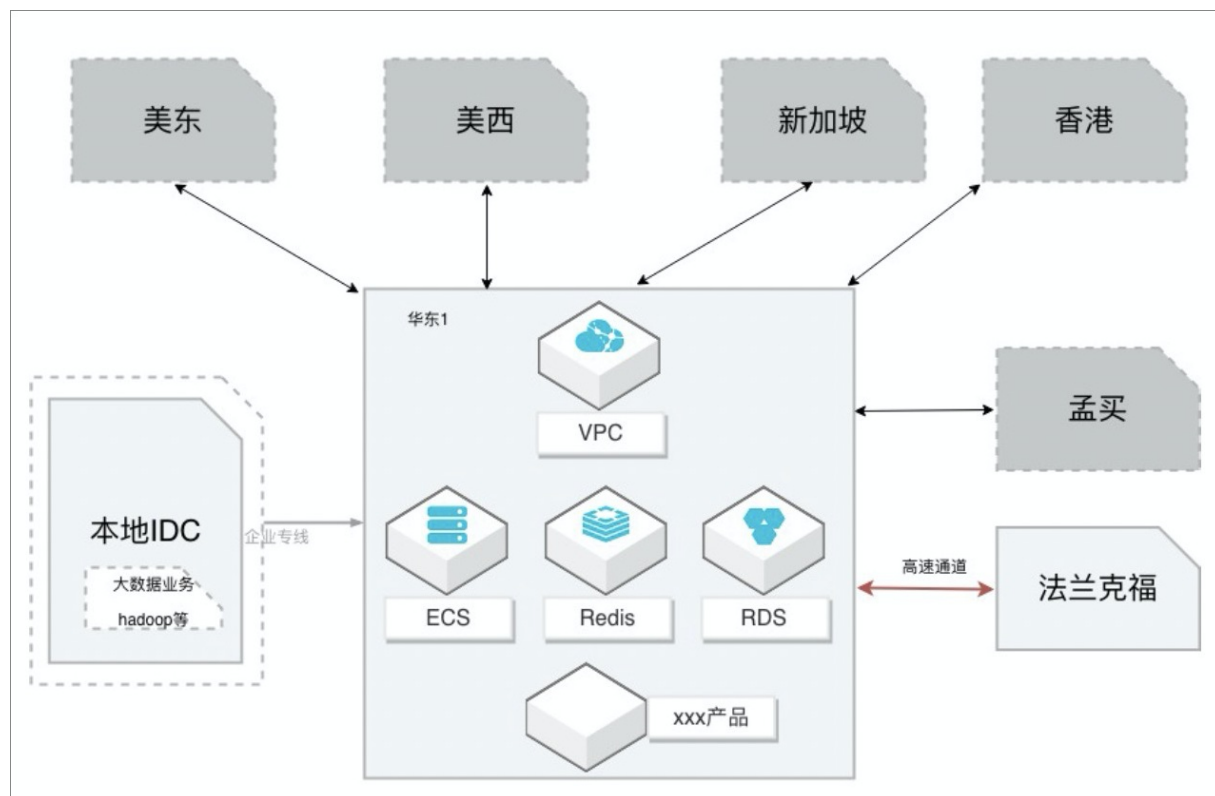
本方案适用从事全球化业务的客户，希望借助全球互通的网络，实现多地域的互通。

同时在全球互联的网络下，搭建应用多地部署。如果业务中涉及到高速通道，提供高速通道迁移云企业网的操作演练；涉及到跨账号多VPC下的数据迁移和同步，本方案提供详细的操作步骤，帮助客户快速完成演练。

解决问题

- 借助云企业网解决网络互通。
- 高速通道到云企业网的平滑迁移。
- RDS的数据互通，特别是跨账号多VPC的数据同步应用的快速部署。

部署架构图



10.游戏出海加速

使用全球加速(GA)及CDN进行游戏出海网络加速以及游戏内容分发加速。

直达最佳实践

[点击查看最佳实践详情](#)

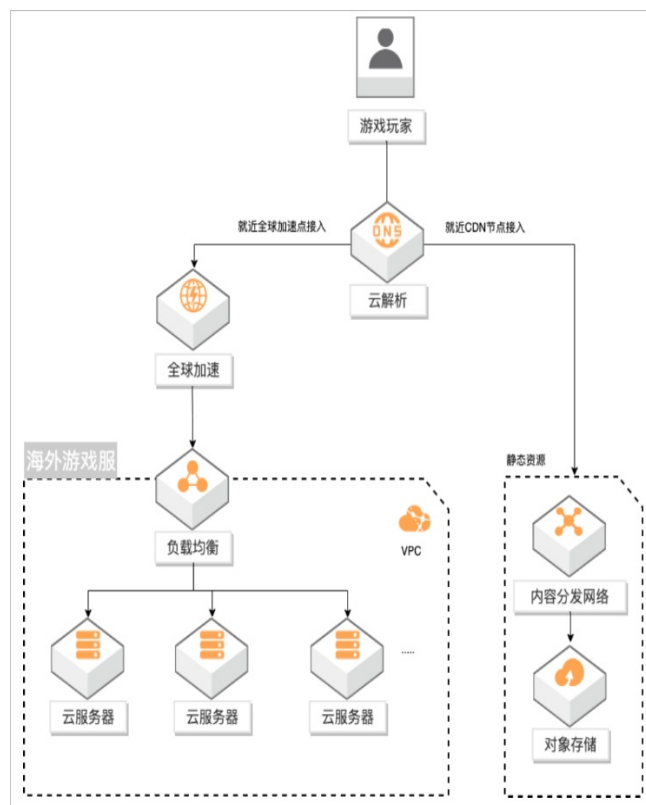
更多最佳实践

[点击查看更多阿里云最佳实践](#)

场景描述

游戏作为应用经济的主要推动力之一，全球游戏下载量、用户支持和参与度持续攀升，全球成熟游戏市场如美国以及新兴游戏市场如印度、印尼、巴西等的游戏市场持续火爆，中国游戏开发商开始拓展全球游戏业务。随之而来的跨国游戏服务会带来游戏时延高、登陆困难、经常掉线等游戏体验差的问题，全球开服成为了出海游戏加速的刚需。出海游戏如何提供稳定游戏访问、灵活快速构建多地就近访问游戏服务器、游戏资源内容安全分发下载，是出海游戏厂商需要具备的核心技术能力。

部署架构



解决问题

- 稳定的跨国游戏访问。
- 游戏玩家多地就近访问游戏服务器。
- 安全快捷的游戏静态内容下载分发。
- 高品质的跨国游戏玩家体验。