

# 基于VPC网络的 六大场景及解决方案

福郎

- 什么是专有网络
- 专有网络如何规划
- 专有网络中如何使用云产品
- 专有网络中如何进行访问控制
- 专有网络公网出入口管理
- 如何构建混合云
- 经典网络迁移到专有网络

## 专有网络 VPC



帮助您基于阿里云构建出一个**隔离**的网络环境。您可以完全掌控自己的虚拟网络，包括选择**自有的 IP 地址范围**，**划分网段**以及**配置路由表和网关**。此外，您也可以通过**专线/VPN**等连接方式将**专有网络与传统数据中心**组成一个**按需定制的网络环境**，实现应用的平滑迁移上云。



负载均衡



弹性公网IP



NAT网关



高速通道



VPN

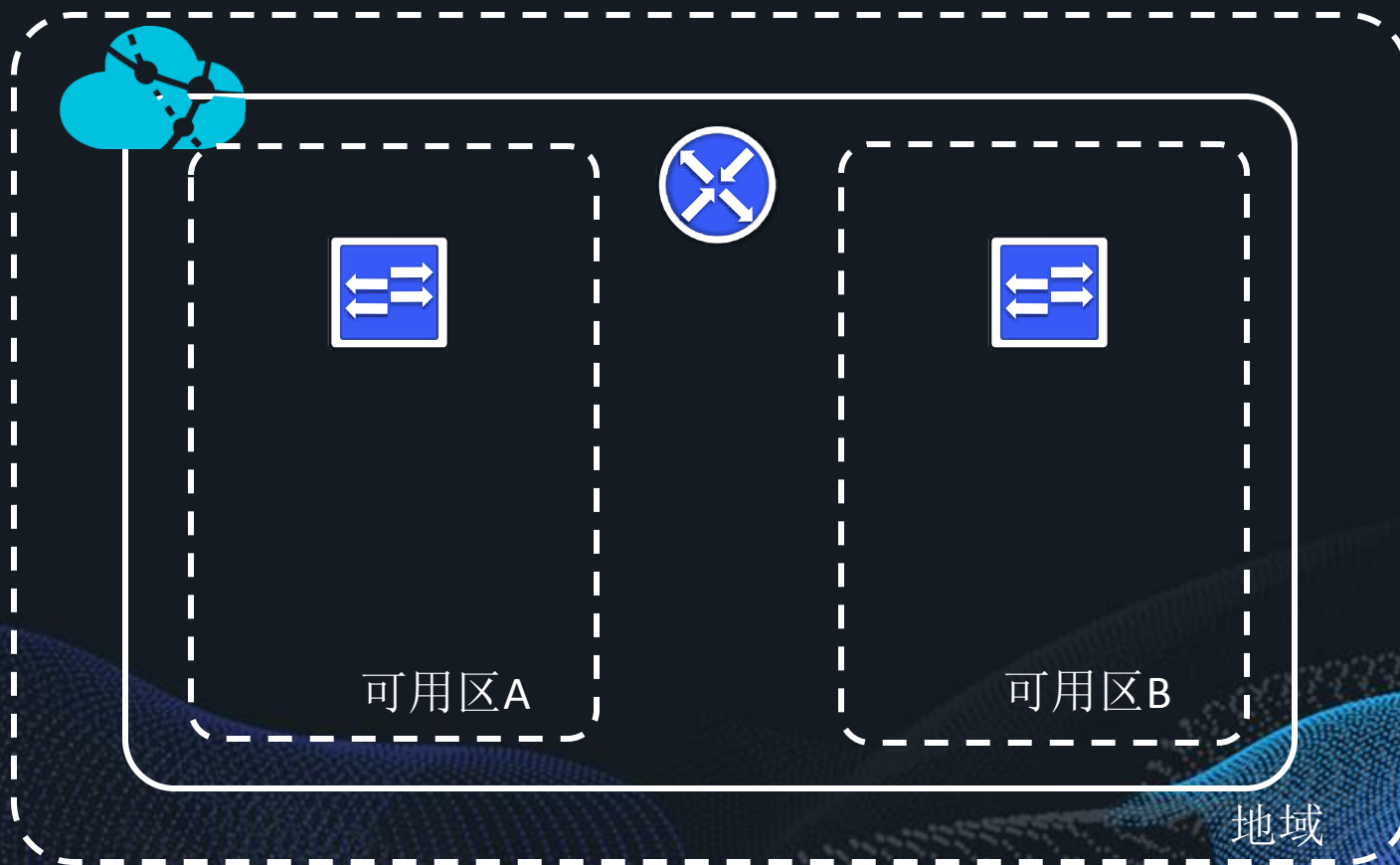


## 专有网络 VPC



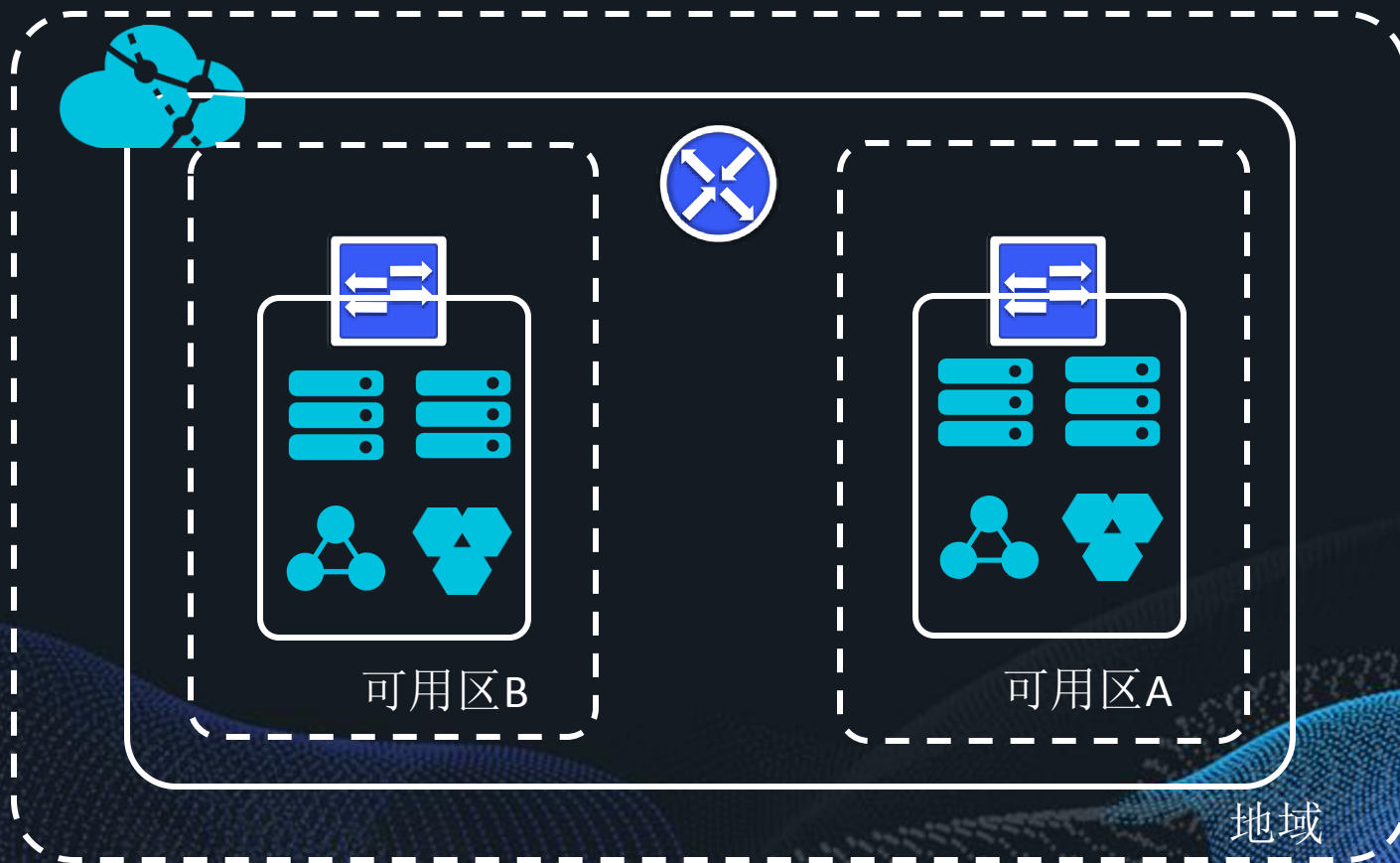
地域级别的二层隔离网络

## 专有网络 VPC



交换机是可用区级别的资源  
用于划分专有网络中子网并管理子网内的流量转发

## 专有网络 VPC



专有网络类型的云产品创建在交换机中

## 专有网络如何规划

- 应该使用几个专有网络
- 应该使用几个交换机
- 应该如何选择网段
- 复杂的业务系统该如何规划网络



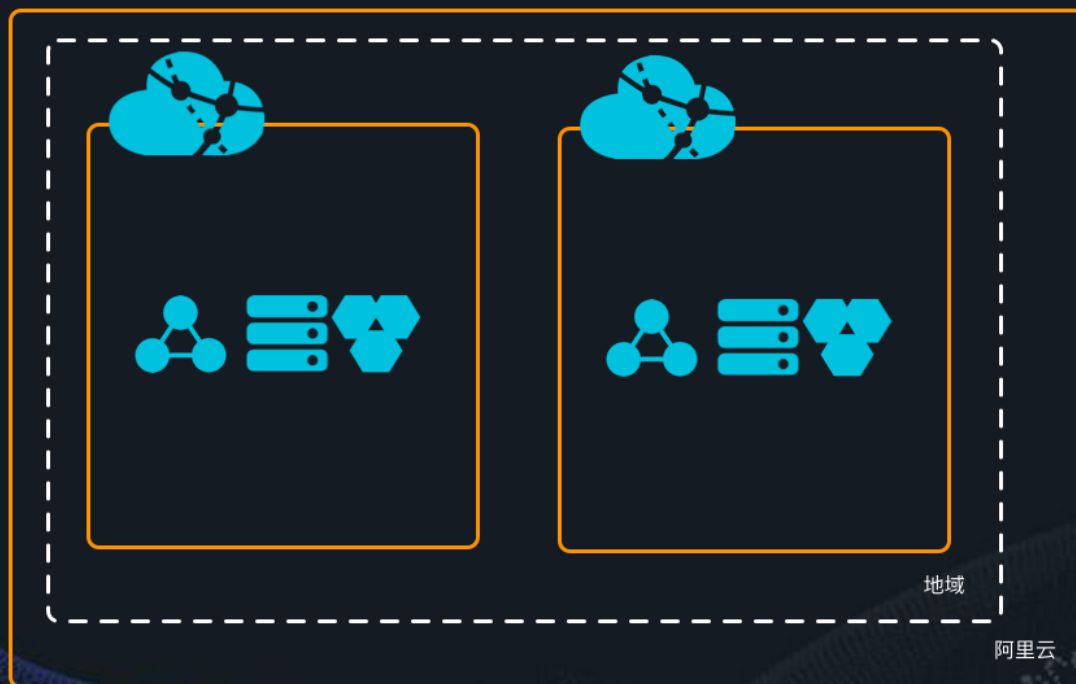
## 使用几个VPC



单个VPC简单部署

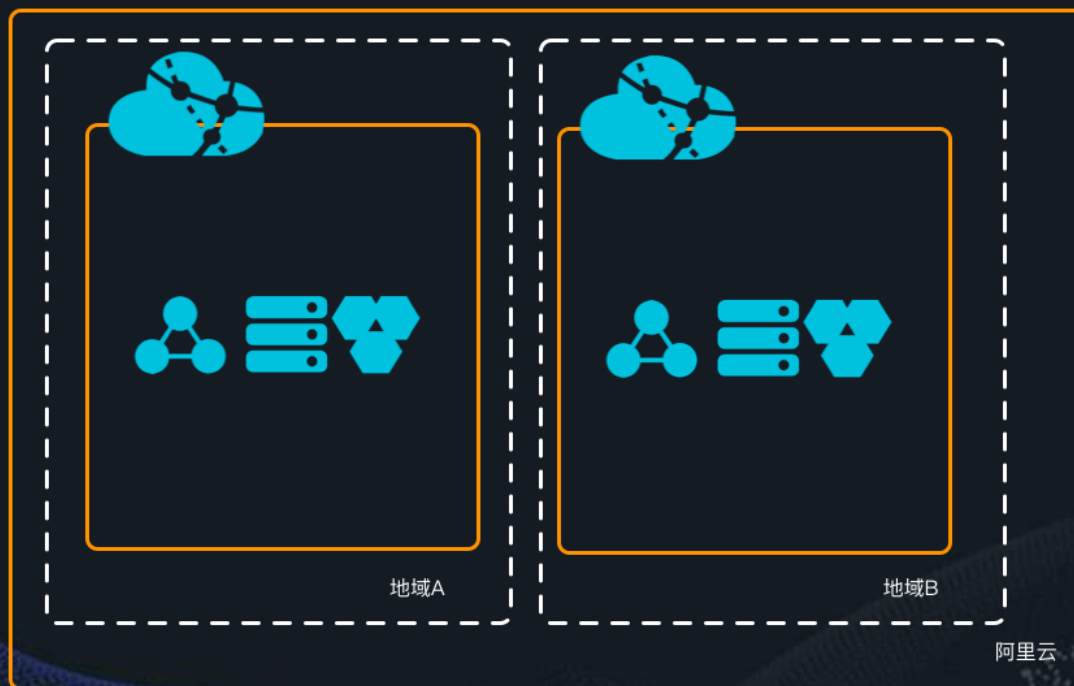


## 使用几个VPC



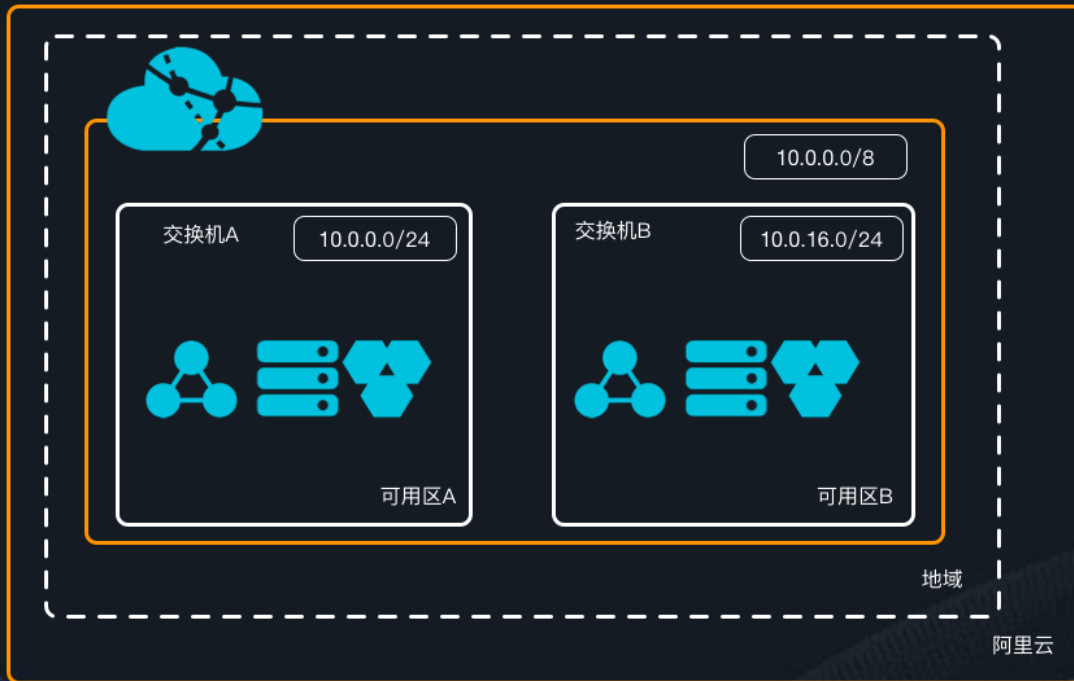
不同应用或同应用不同环境的隔离部署，需要多个VPC

## 使用几个VPC



跨地域部署，需要在多个地域使用VPC

## 交换机创建



尽量使用至少两个交换机，并且两个交换机分布在不同可用区应用的不同部分，如前端服务和数据库服务使用不同的交换机



## VPC地址段的选择

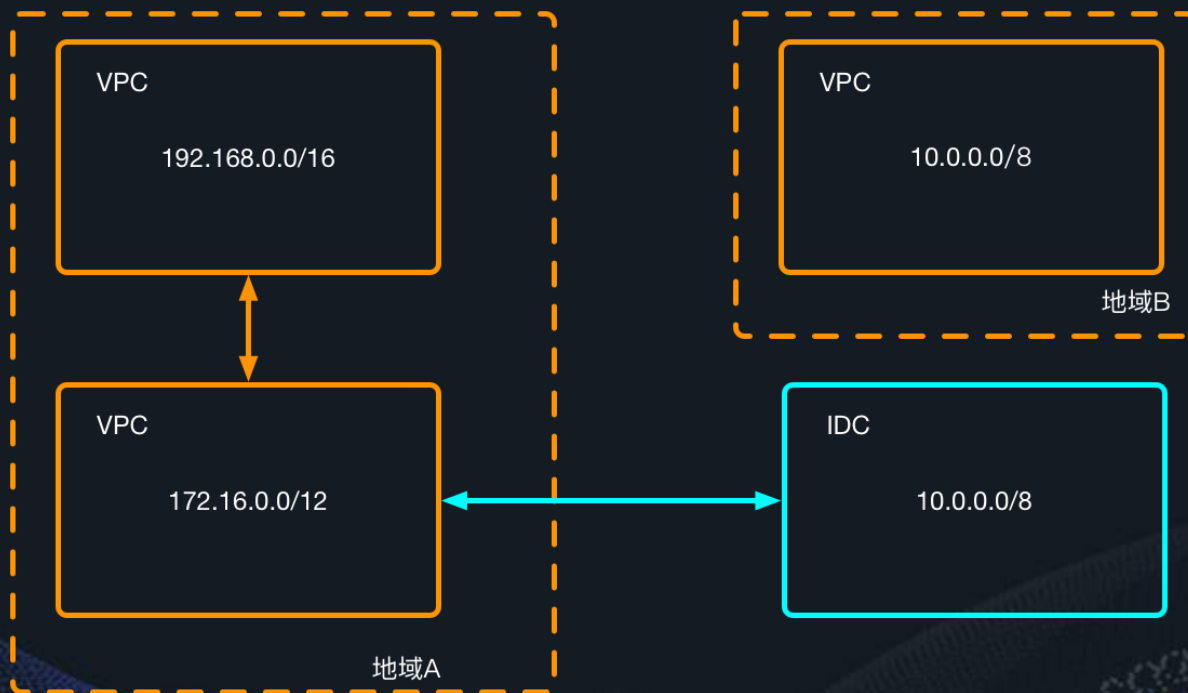
网段	私网IP数量
10.0.0.0/8	16777212
172.16.0.0/12	1048572
192.168.0.0/16	65532

支持三个私网网段及子网，掩码范围 8~24  
如果已经在使用经典网络，谨慎使用10.0.0.0/8

## 交换机地址段的选择

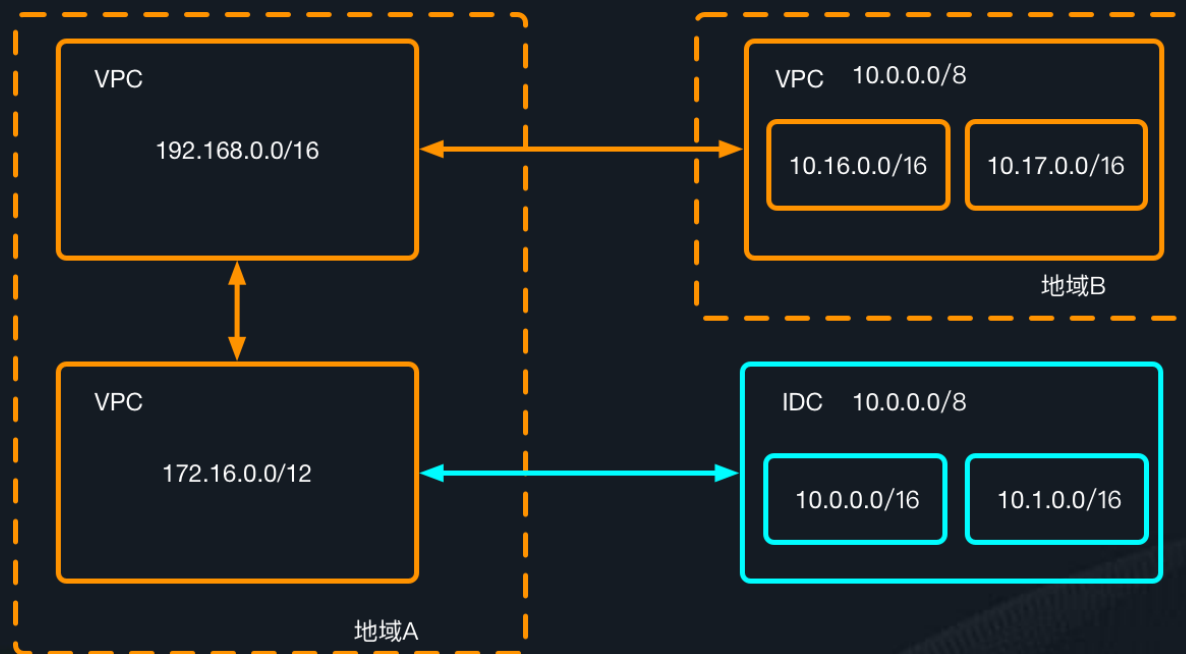
VPC网段的子网，掩码范围 16~29  
根据规划在交换机下的主机容量进行选择

## 混合云的网络规划



需要互通的网络尽量规划不同的地址段

## 混合云的网络规划



不同网络地址段相同时，需要保证需要互通的子网地址段不同



## 专有网络中如何使用云产品

- 专有网络类型的云产品
- 支持专有网络环境使用的云产品

## 专有网络类型的云产品

- 创建时指定网络类型为专有网络
- 选择指定的专有网络和交换机

网络

经典网络

专有网络

?

经典网络与专有网络不能互通，购买后不能更换网络类型，请谨慎选择

请选择专有网络

请选择虚拟交换机

如需使用其他专有网络，请选择已有专有网络，也可以自行到 [控制台创建](#)>>  
当前虚拟交换机所在可用区为：随机分配

实例ID/名称	所在可用区	IP地址	状态(全部)	网络类型(全部)	配置	实例规格族	专有网络属性	付费方式(全部)	操作
实例ID/名称	所在可用区	IP地址	状态(全部)	网络类型(全部)	配置	实例规格族	专有网络属性	付费方式(全部)	操作
实例ID/名称	所在可用区	IP地址	状态(全部)	网络类型(全部)	配置	实例规格族	专有网络属性	付费方式(全部)	操作



## 云服务器 ECS



## 云数据库 RDS



## 负载均衡

## 支持专有网络环境使用的云产品

- 开通对象存储服务
- 创建存储空间
- 提供专有网络的访问方法

VPC网络下Region和Endpoint对照表

在VPC网络下的ECS访问OSS只能使用如下的Endpoint:

Region中文名称	Region英文表示	VPC网络Endpoint
华东 1	oss-cn-hangzhou	vpc100-oss-cn-hangzhou.aliyuncs.com
华东 2	oss-cn-shanghai	vpc100-oss-cn-shanghai.aliyuncs.com
华北 1	oss-cn-qingdao	vpc100-oss-cn-qingdao.aliyuncs.com
华北 2	oss-cn-beijing	vpc100-oss-cn-beijing.aliyuncs.com
华北 3	oss-cn-zhangjiakou	oss-cn-zhangjiakou-internal.aliyuncs.com



对象存储 OSS



日志服务



## 支持专有网络环境使用的云产品

- 开通服务
- 创建实例
- 绑定VPC

绑定VPC

\* 实例名: test1121

\* 选择VPC: test11RouteEntry

\* 选择交换机: aaa-1

\* VPC Name: ccc

网络: 限定VPC访问

确定 取消

test1121

实例访问地址

公网: http://test1121.cn-beijing.ots.aliyuncs.com

私网: http://test1121.cn-beijing.ots-internal.aliyuncs.com

实例网络类型 更改

允许任意网络访问

VPC列表

实例VPC名称	VPC ID	VPC访问IP	VPC访问地址	操作
ccc	vpc-2zsj5kztpa158ev7k7gt	http://192.168.1.227:80/	http://ccc-test1121.cn-beijing.vpc.ots.aliyuncs.com	解除绑定

数据表列表



表格存储



容器服务



文件存储

# 专有网络中的访问控制

## 云服务器 ECS 安全组

添加安全组规则

网卡类型: 内网

规则方向: 入方向

授权策略: 允许

协议类型: 自定义 TCP

\* 端口范围: 例如:22/22或3389/3389

授权类型: 地址段访问

\* 授权对象: 例如:10.x.y.z/32

优先级: 1

描述: 长度为2-256个字符, 不能以http://或https://开头。

确定 取消

## 云数据库 RDS 版白名单

修改白名单分组

1 分组名称: default

组内白名单: 10.10.10.0/24

2 加载ECS内网IP

还可添加999个白名单

IP地址间用英文逗号分隔, 如192.168.0.1,192.168.0.2

3 确定 取消

## 专有网络公网出入口管理



弹性公网IP



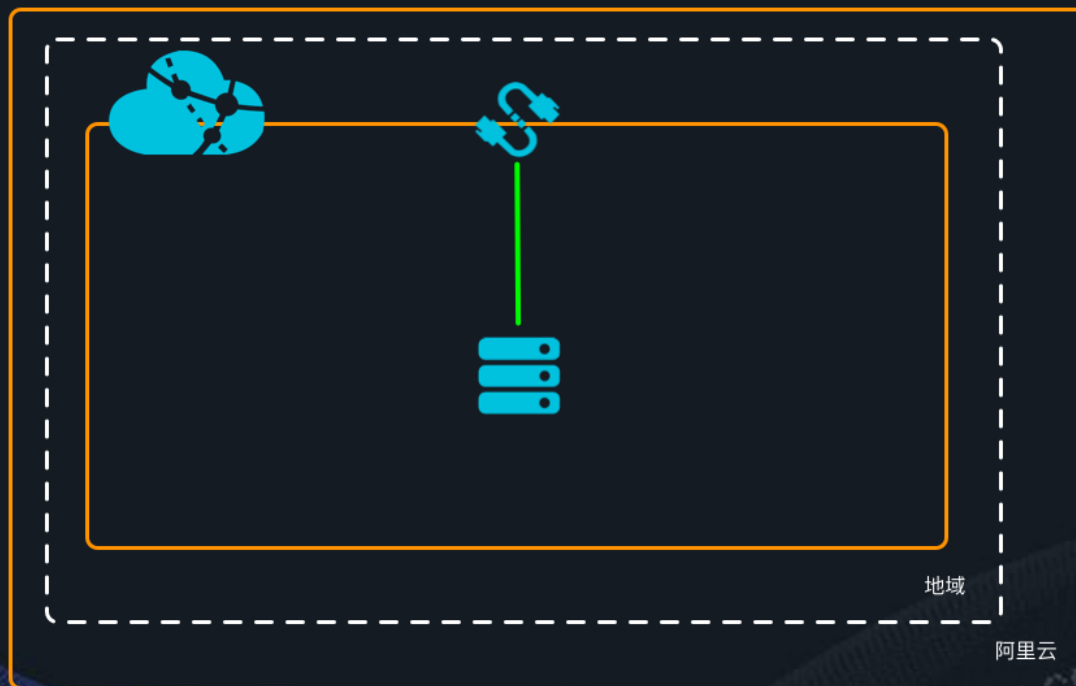
NAT网关



负载均衡

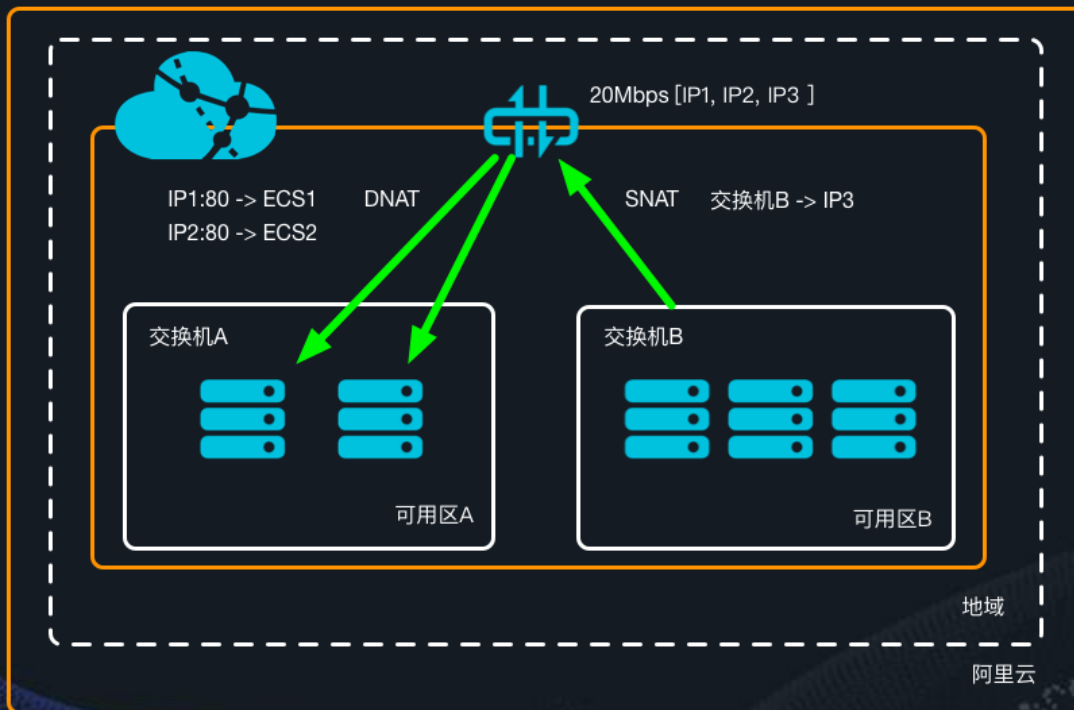


## 弹性公网IP



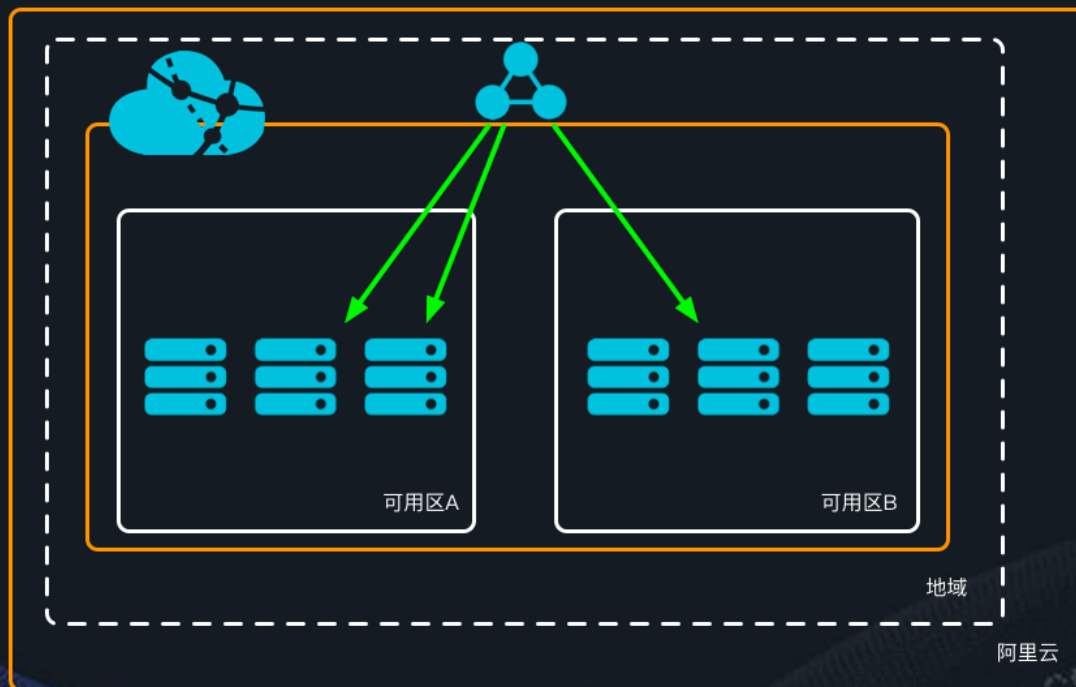
绑定EIP的云服务器可以访问公网  
可以将云服务器配置成为公网网关管理其他云服务器的公网访问

## NAT网关



企业级的公网网关，为专有网络提供统一的公网出入口。提供 NAT 代理（SNAT、DNAT）、10Gbps 级别的转发能力、以及跨可用区的容灾能力，支持多IP共享带宽。

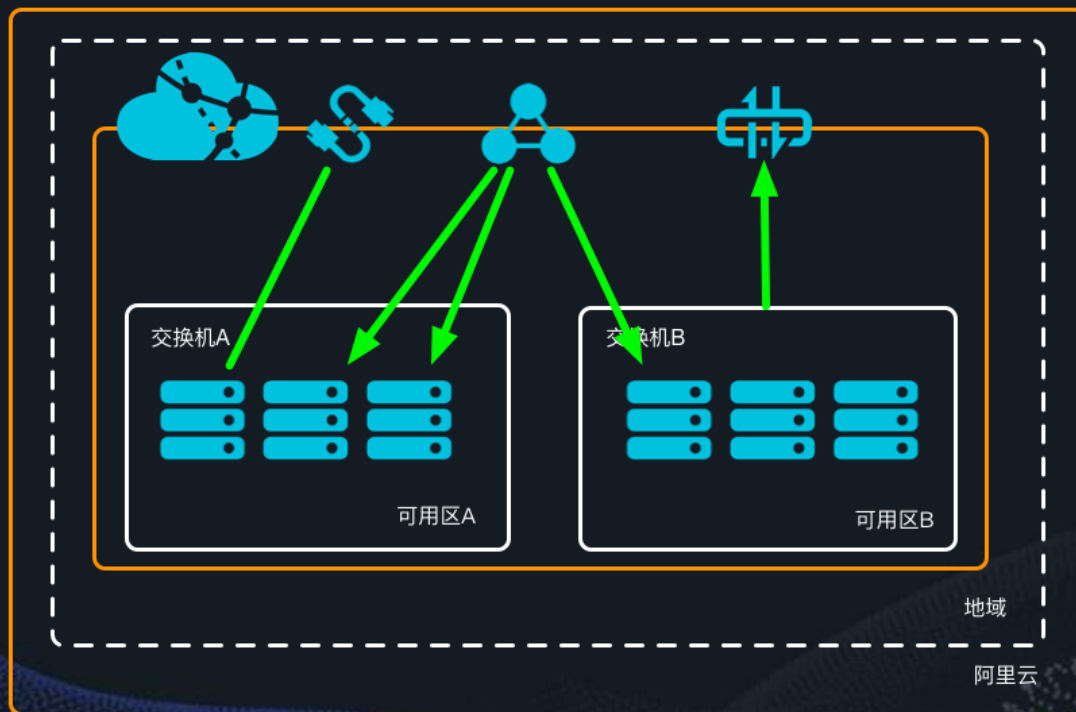
## 负载均衡



对多台云服务器进行四七层流量分发的负载均衡服务，可以通过流量分发扩展应用系统对外的服务能力，通过消除单点故障提升应用系统的可用性。



## 公网出入口管理



## 如何构建混合云——网络融合

VPC互通



专线接入



VPN



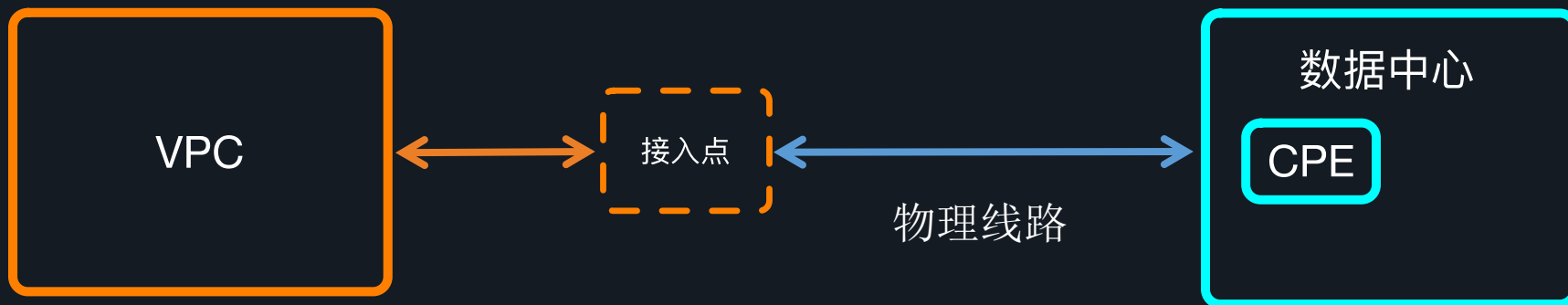
## VPC互通

- 全球13个地域
- 任意两个VPC互通
  - 同账号、跨账号
  - 同地域、跨地域
- 带宽10Mbps-10Gbps





## 专线接入



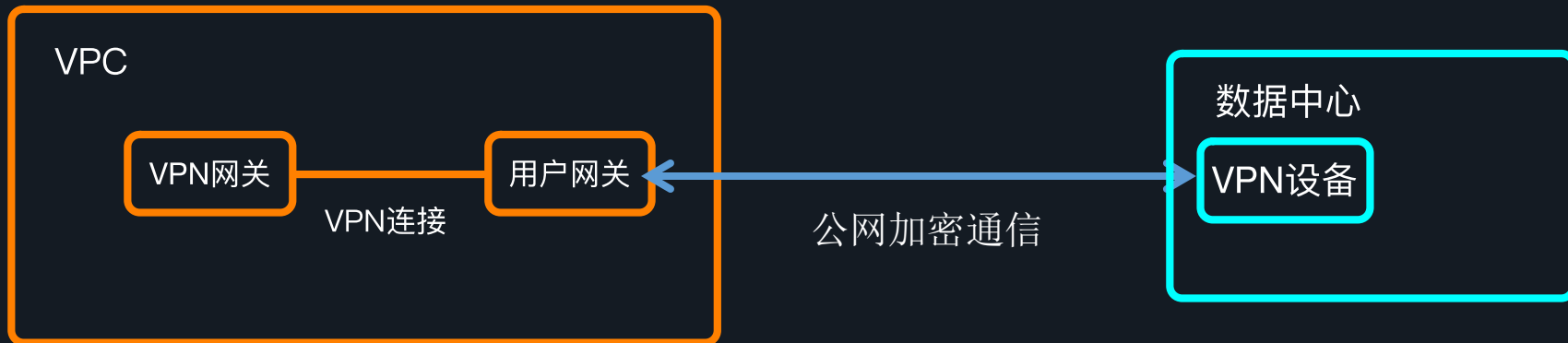
### 接入点

- 每个地域提供2-3个接入点，成都接入点即将开放
- 支持40Gbps线路接入
- 通过一个接入点可以连接到任意地域的VPC

### 物理线路建设

- 联系运营商进行建设
- 通过合作伙伴进行建设

## VPN网关



- 支持IPSec VPN
- 交付周期短，价格低廉 60% Off

### 使用公网的局限

- 延时较长
- 网络抖动
- 传输丢包
- 带宽一般为百兆级别

## 专有网络 vs 经典网络



VS



### 经典网络

- 共享网络地址空间
- 网络由阿里云管理
- 不支持自定义路由
- 不支持混合云网络搭建

### 专有网络

- 独享网络地址空间
- 自定义网络
- 支持自定义路由管理
- 支持混合云网络搭建

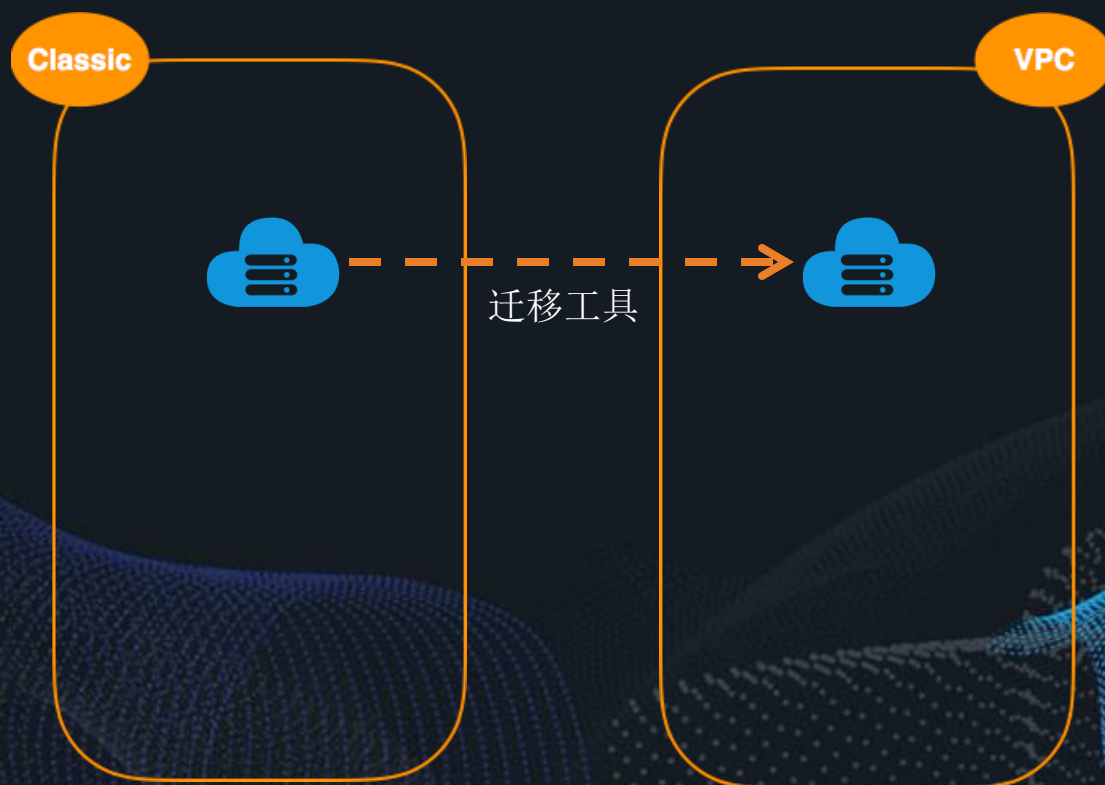


## 经典网络迁移到专有网络

当前应用部署在专有网络中，如何将应用平滑的迁移到专有网络？

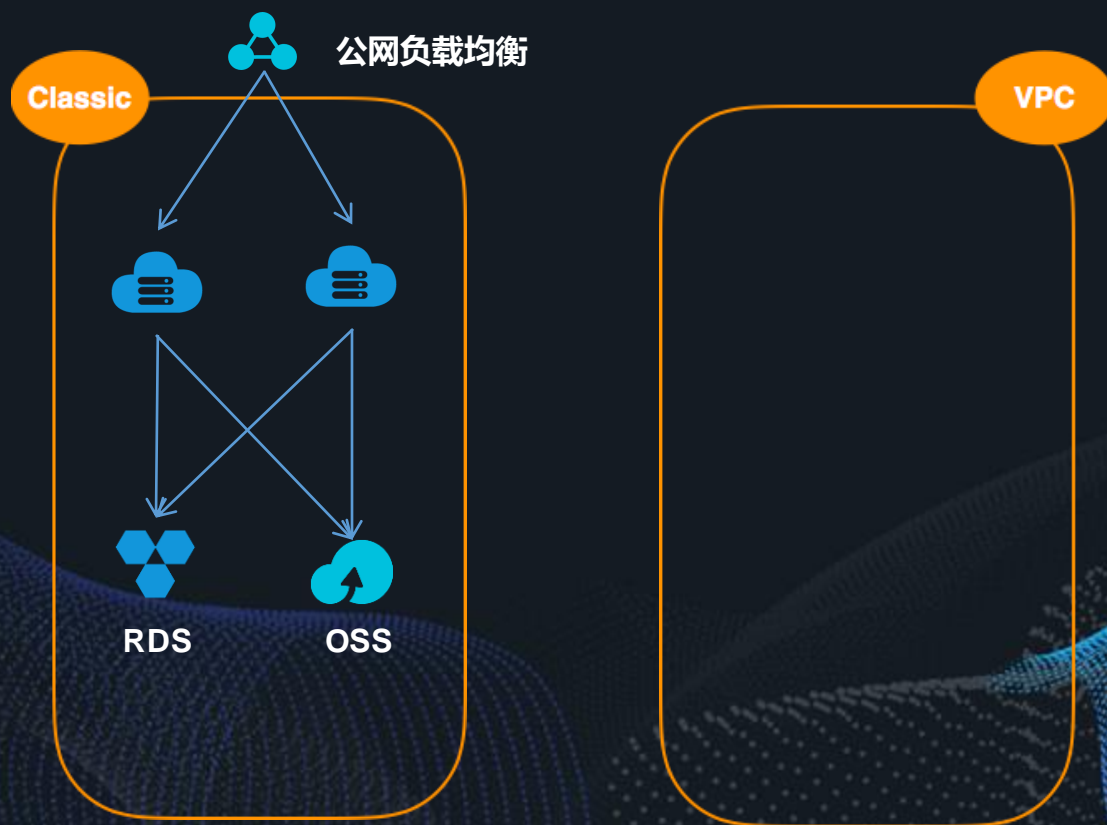
## 经典网络迁移到专有网络

针对于单台 ECS 从经典网络迁移到 VPC 提供直接迁移工具



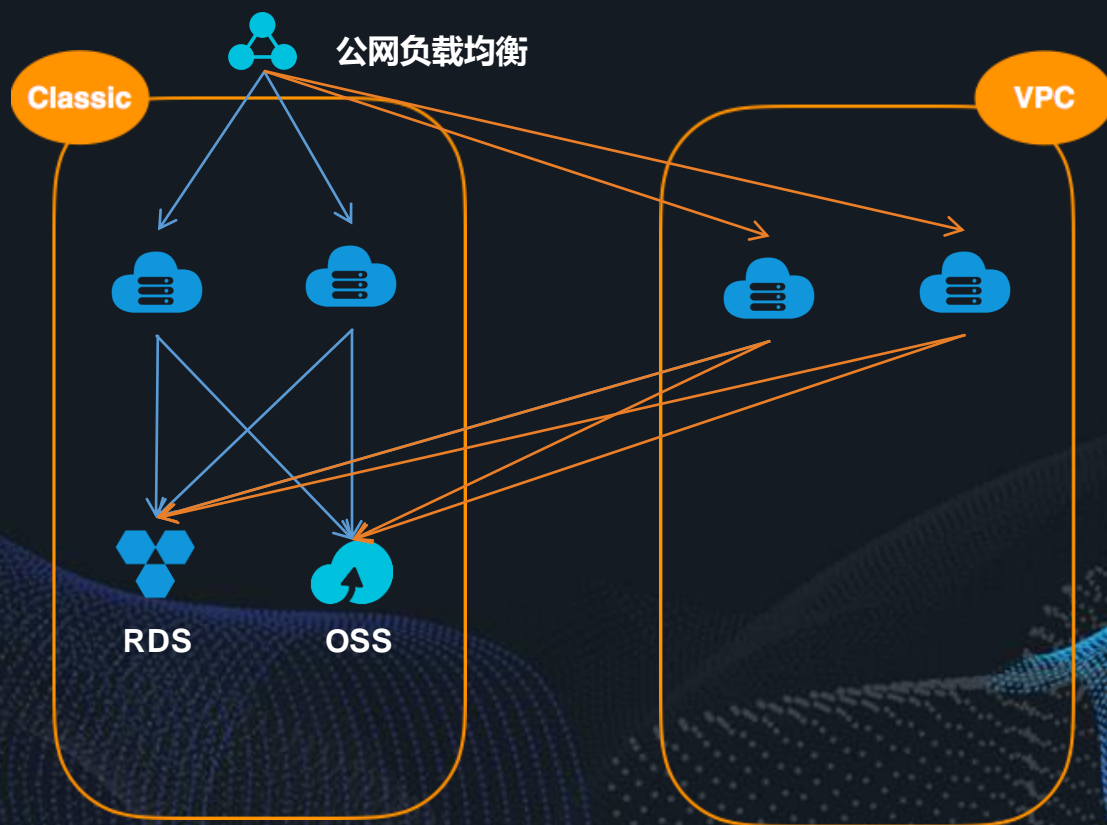
## 经典网络迁移到专有网络

针对在多个云产品之上构建的业务，提供平滑迁移方案



## 经典网络迁移到专有网络

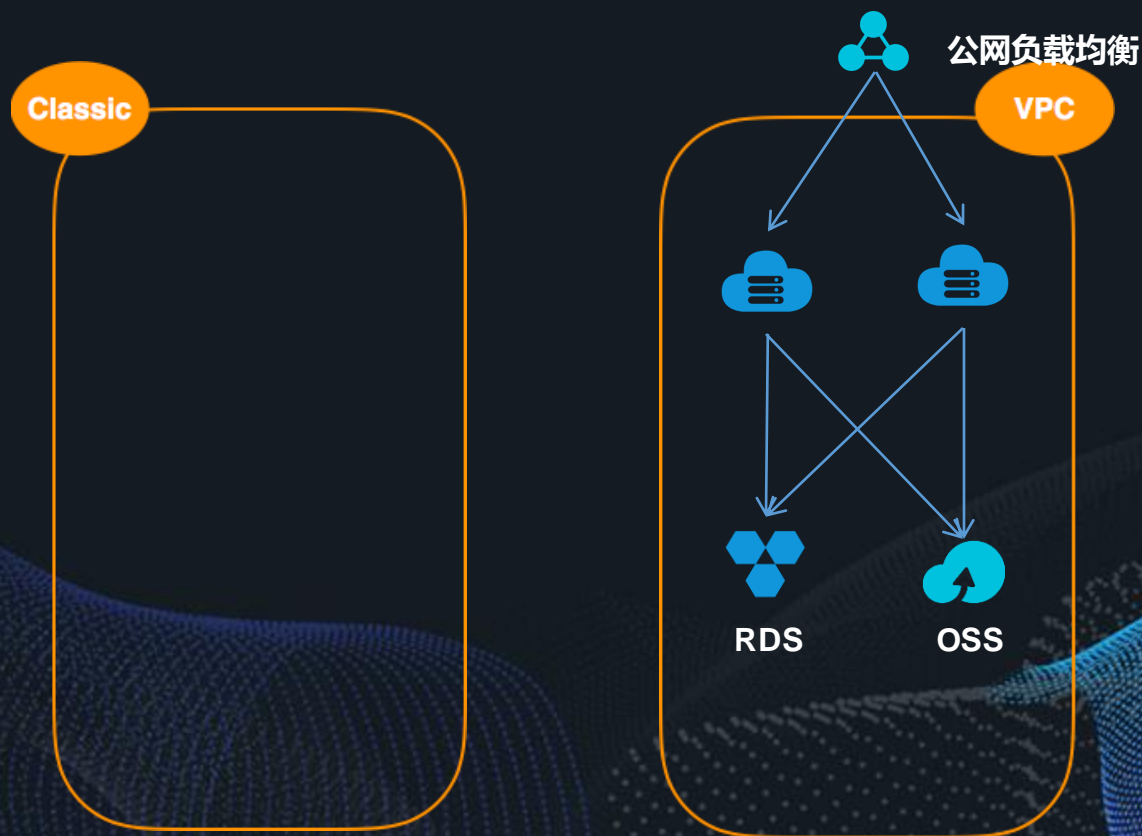
针对在多个云产品之上构建的业务，提供平滑迁移方案





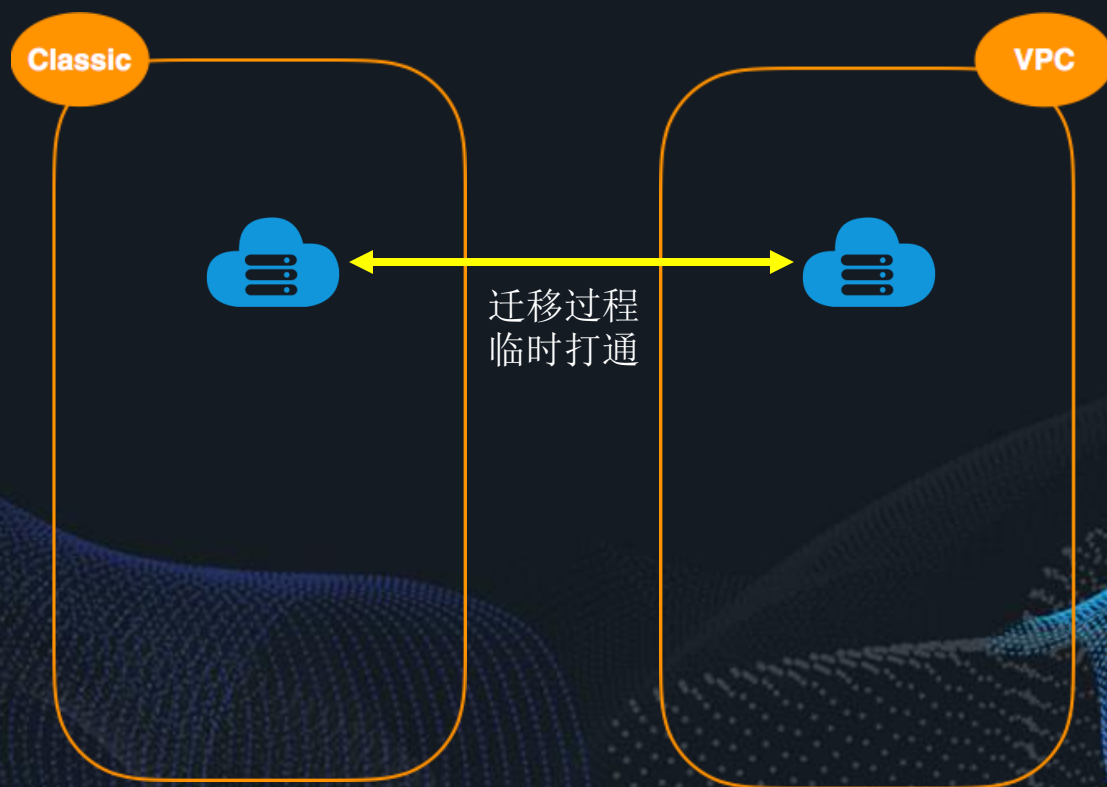
## 经典网络迁移到专有网络

针对在多个云产品之上构建的业务，提供平滑迁移方案



## 经典网络迁移到专有网络

对于更复杂的业务迁移场景，提供ClassicLink功能，允许用户将一台经典网络的ECS直接与指定VPC进行内网通信。



- 专有网络如何规划
- 专有网络中如何使用云产品
- 专有网络中如何进行访问控制
- 专有网络公网出入口管理
- 如何构建混合云
- 经典网络迁移到专有网络

# 谢谢



阿里云

阿里云网络产品技术交流群

279人

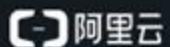


扫一扫群二维码，立刻加入该群。





2017云栖大会·成都峰会  
THE COMPUTING CONFERENCE



云栖社区  
yq.aliyun.com

# 飞天·智能

## APSARA INTELLIGENCE

2017云栖大会·成都峰会

5月23日 成都世纪城天堂洲际大酒店