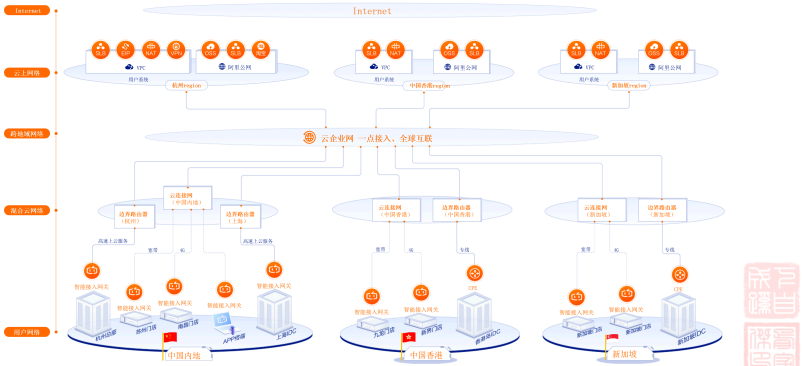
阿里云网络架构设计

之 ACE 认证考试辅导版

目录

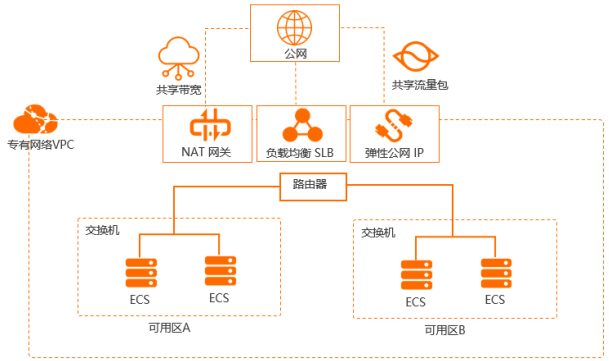
第3页

阿里云网络



第4页

云上网络

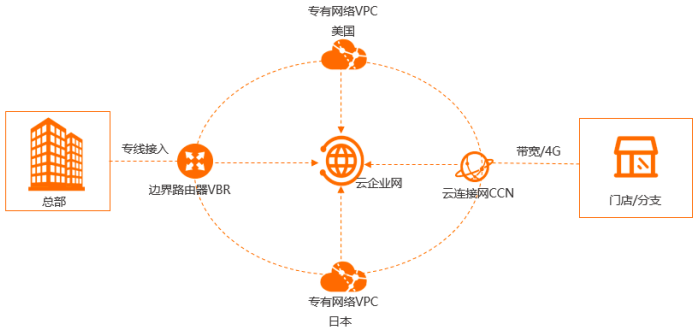


第5页

公网访问

- 您可以通过弹性公网IP、NAT网关、负载均衡使专有网络中的云资源访问公网或被公网访问。
- **弹性公网 IP**：弹性公网IP是独立的公网IP资源，可以绑定到阿里云专有网络类型的ECS、NAT网关、私网负载均衡SLB、弹性网卡等资源。
- **NAT 网关**： NAT网关（NAT Gateway）是一款企业级的公网网关，支持SNAT和DNAT功能，具备Tbps级别的集群转发能力和地域级别的高可用性。
- **负载均衡**：负载均衡（Server Load Balancer）是将访问流量根据转发策略分发到后端多台云服务器（ECS实例）的流量分发控制服务。负载均衡扩展了应用的服务能力，增强了应用的可用性。

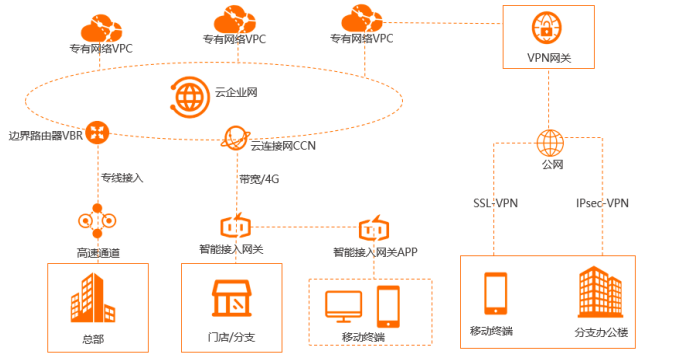
跨地域网络



跨地域互连

- 当您需要将多个专有网络互连汇聚成一个更大的虚拟网络时，您可以通过阿里云提供的云企业网实现全球网络互通，并通过全球加速服务优化跨地域网络访问，减少网路延时、丢包等问题。
- **云企业网**：云企业网可以在VPC间，VPC与本地数据中心间搭建高质量、高安全的私网通信通道，通过自动路由分发及学习，使网络快速收敛，实现全网资源的互通，打造一张具有企业级规模和通信能力的全球互联网络。
- **全球加速**：全球加速（Global Acceleration，简称GA）是一款覆盖全球的网络加速服务，依托阿里巴巴优质BGP带宽和全球传输网络，实现全球网络就近接入和跨地域部署，减少延迟、抖动、丢包等网络问题对服务质量的影响，为全球用户提供高可用和高性能的网络加速服务。

混合云网络



混合云网络

- 随着云计算的普及，企业逐渐将数据中心的业务应用迁移上云。过去以IDC为中心的星形网络结构，正在演进到以云为中心的混合云网络结构，云下和云上之间的网络连接成为关键。您可以使用阿里云提供的网络产品快速构建混合云网络。
- **智能接入网关**：智能接入网关是阿里云SD-WAN网络的终端，协助企业快速构建混合云网络。
- **高速通道**：阿里云高速通道（Express Connect）可在本地数据中心和云上专有网络间建立高速、稳定、安全的私网通信。
- **VPN 网关**： VPN网关是一款基于Internet的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络（VPC）安全可靠的连接。

混合云解决方案

- IDC通过BGP主备链路上云方案
- IDC通过专线和智能接入网关主备方式上云方案
- IDC通过VPN网关上云方案
- IDC双专线静态路由冗余上云方案

目录

什么是 VPC

- 阿里云专有网络（Virtual Private Cloud，简称VPC）是您在云上创建的专用虚拟网络。
- 专有网络类似您在自己的数据中心运营的传统网络，但附带了阿里云基础设施的其他优势，例如可扩展性、隔离性和安全性等。
- 您可以在自己的专有网络内部署、使用云资源，例如云服务器、数据库和容器Kubernetes服务等。
- 您可以完全掌控自己的专有网络，例如选择IP地址范围、配置路由表和网关等。

VPC 的组成

- **私网网段**
  - 在创建专有网络和交换机时，您需要以CIDR地址块的形式指定专有网络使用的私网网段。
- **路由器**
  - 路由器（VRouter）是专有网络的枢纽。作为专有网络中重要的功能组件，它可以连接专有网络内的各个交换机，同时也是连接专有网络和其他网络的网关设备。每个专有网络创建成功后，系统会自动创建一个路由器。每个路由器关联一张路由表。
- **交换机**
  - 交换机（VSwitch）是组成专有网络的基础网络设备，用来连接不同的云资源。创建专有网络后，您可以通过创建交换机为专有网络划分一个或多个子网。同一专有网络内的不同交换机之间内网互通。您可以将应用部署在不同可用区的交换机内，提高应用的可用性。

第14页

地域和可用区规划

- 专有网络和要使用的资源例如云服务器必须部署在同一个地域内，您可以选择将资源部署在同一个地域内的不同可用区。
- 同一个专有网络内的资源可以互通，不同专有网络内的资源无法互通， 但您可以连接不同专有网络的资源。
- 在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。
- 是否将实例放在同一可用区内，主要取决于对容灾能力和网络延时的要求：
  - 如果您的应用需要较高的容灾能力，建议您将实例部署在同一地域的不同可用区内。
  - 如果您的应用要求实例之间的网络延时较低，建议您将实例创建在同一可用区内。

第15页

数量规划

- 您可以为每个地域创建多个专有网络，而每个专有网络内又可创建多个交换机。
- 需要几个专有网络？
  - 如果您没有多地域部署系统的要求且各系统之间也不需要通过专有网络进行隔离，那么推荐使用一个专有网络。
  - 当您有多地域部署系统的需求时，或在一个地域的多个业务系统需要通过专有网络进行隔离，例如生产环境和测试环境，那么就需要使用多个专有网络。
- 需要几个交换机？
  - 首先，即使只使用一个专有网络，也尽量在专有网络内创建至少两个交换机，并且将两个交换机分布在不同可用区，实现跨可用区容灾。
  - 其次，使用多少个交换机还和系统规模、系统规划有关。如果前端系统可以被公网访问并且有主动访问公网的需求，考虑到容灾可以将不同的前端系统部署在不同的交换机下，将后端系统部署在另外的交换机下。

第16页

网段规划

- 在创建专有网络和交换机时，您需要指定专有网络和交换机的网段。网段的大小不仅决定了可部署多少云资源也关系到不同网络之间能否互通。
- **专有网络的网段**：您可以使用192.168.0.0/16、172.16.0.0/12、10.0.0.0/8这三个私网网段及其子网作为专有网络的网络地址。
  - 如果云上只有一个专有网络并且不需要和本地数据中心的网络互通时，可以选择上述私网网段中的任何一个网段或其子网。
  - 如果有多个专有网络，或者有专有网络和本地数据中心构建混合云的需求，推荐使用上面这些标准网段的子网作为专有网络的网段，掩码建议不超过16位。

第17页

网段规划

- 专有网络网段的选择还需要考虑是否使用了经典网络。如果您使用了经典网络，并且计划将经典网络的ECS实例和专有网络连通，那么推荐您选择非10.0.0.0/8作为专有网络的网段，因为经典网络的网段也是10.0.0.0/8。
- 在有多个专有网络的情况下，建议遵循以下网段规划原则：
  - 尽可能做到不同专有网络的网段不同，不同专有网络可以使用标准网段的子网来增加可用的网段数。
  - 如果不能做到不同专有网络的网段不同，则尽量保证不同专有网络的交换机网段不同。
  - 如果也不能做到交换机网段不同，则保证要通信的交换机网段不同。

网段规划

- **交换机的网段**
  - 交换机的网段必须是其所属专有网络网段的子集。
    - 交换机的网段的大小在16位网络掩码与29位网络掩码之间，可提供8~65536个地址。16位掩码能支持部署65532个ECS实例，而小于29位掩码又太小，没有意义。
    - 每个交换机的第一个和最后三个IP地址为系统保留地址。以192.168.1.0/24为例，192.168.1.0、192.168.1.253、192.168.1.254和192.168.1.255这些地址是系统保留地址。
    - ClassicLink功能允许经典网络的ECS实例和192.168.0.0/16、10.0.0.0/8、172.16.0.0/12这三个网段内的ECS实例通信。如果专有网络的网段是10.0.0.0/8，确保和经典网络ECS实例通信的交换机的网段在10.111.0.0/16内。
    - 交换机网段的确定还需要考虑该交换机下容纳ECS的数量。

路由表

- 创建专有网络后，系统会自动为您创建一张系统路由表并为其添加系统路由来管理专有网络的流量。系统会在路由表中自动添加如下系统路由：
  - 以100.64.0.0/10为目标网段的路由条目，用于VPC内的云产品通信。
  - 以交换机网段为目标网段的路由条目，用于交换机内的云产品通信。
- 一个专有网络只有一张系统路由表。该系统路由表在创建专有网络的时候自动为您创建，您不能手动创建也不能删除系统路由表。
- 您可以在专有网络内创建自定义路由表，然后将其和交换机绑定来控制子网路由，更灵活地进行网络管理。每个交换机只能关联一张路由表。
- 路由表采用最长前缀匹配原则作为流量的路由选路规则。
  - 最长前缀匹配是指当路由表中有多条路由条目可以匹配目的IP时，采用掩码最长（最精确）的一条路由作为匹配项并确定下一跳。

VPC访问控制

- **网络ACL**
  - 网络ACL是VPC中的网络访问控制功能。您可以自定义设置网络ACL规则，并将网络ACL与交换机绑定，实现对交换机中ECS实例的流量的访问控制。
- **ECS安全组**
  - 安全组是一种虚拟防火墙，具备状态检测和数据包过滤能力，用于在云端划分安全域。通过配置安全组规则，您可以控制安全组内一台或多台ECS实例的入流量和出流量。
- **RDS白名单**
  - 在VPC中使用云数据库RDS实例，需要将云服务器的IP地址加入到需要访问的RDS的白名单中，云服务器才能访问RDS实例，而其他IP地址将拒绝访问RDS实例。
- **SLB白名单**
  - 负载均衡是将访问流量根据转发策略分发到后端多台云服务器的流量分发控制服务。您可以为负载均衡监听设置允许转发请求的IP地址，适用于只允许特定IP访问应用的场景。

ClassicLink

- 经典网络类型的云产品，统一部署在阿里云的公共基础网络内，由阿里云统一规划和管理，更适合对网络易用性要求比较高的用户。
- 专有网络是指用户在阿里云的基础网络内建立一个可以自定义的专有隔离网络。与经典网络相比，专有网络比较适合有网络管理能力和需求的用户。
- 专有网络提供ClassicLink功能，使经典网络的云服务器ECS实例可以和专有网络（VPC）中的云资源通过内网互通。

第27页

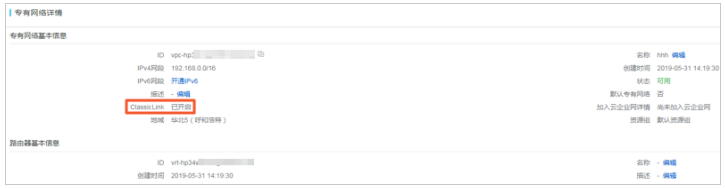
ClassicLink互通原理

- 经典网络是一个网络平面，VPC是另一个网络平面，ClassicLink是通过路由建立这两个网络平面的连接，让其具备互通的条件。
- 使用ClassicLink功能，首先要避免网络地址冲突，做好网络地址规划。
- 阿里云经典网络中使用的地址段是10.0.0.0/8（不包括10.111.0.0/16），因此只要VPC的地址段与经典网络的地址段不冲突，就可以通过ClassicLink功能通信。
- 可以与经典网络互通的VPC地址段有
  - 172.16.0.0/12
  - 10.111.0.0/16
  - 192.168.0.0/16

第28页

ClassicLink互通原则

- 使用ClassicLink功能建立经典网络ECS实例和VPC的私网通信后：
  - 经典网络ECS实例可以访问目标VPC内的云资源。
  - ClassicLink连接成功后，VPC内的ECS实例只能访问已连接到该VPC的经典网络ECS实例，不能访问未连接的经典网络ECS实例，也不能访问经典网络内的其它云资源。



第29页

为什么要迁移至VPC？

- VPC 是你自己独有的的云上私有网络，VPC 具有如下优势：
- 安全的网络环境
  - VPC基于隧道技术，实现数据链路层的隔离，为每个租户提供一张独立、隔离的安全网络。不同专有网络之间网络完全隔离。
- 可控的网络配置
  - 您可以完全掌控自己的虚拟网络，例如选择自己的IP地址范围、配置路由表和网关等，从而可以轻松地实现内网的网络资源规划以及路由表的路径选择。此外，您也可以通过专线或VPN等连接方式将您的专有网络与传统数据中心相连，形成一个按需定制的网络环境，实现应用的平滑迁移上云和对数据中心的扩展。

第30页

如何迁移？

- 阿里云提供以下两种将经典网络迁移到VPC的方案，可以独立使用，也可以组合使用。
- **混访混挂方案**
  - 如果您的服务依赖RDS、SLB等云产品，建议您选择混访混挂的迁移方案。
  - 该方案可以平滑地将系统迁移至专有网络环境中，保证服务的稳定性。即用户通过在VPC中新建ECS等云产品实例，然后将系统平滑迁移到VPC。当所有系统都迁移到VPC后，再将经典网络内的资源释放，从而完成经典网络到VPC的迁移。
- **单ECS迁移方案**
  - 如果您的应用部署在了ECS实例上，且ECS实例重启对系统没有影响，可以选择单ECS迁移方案。

混挂

- 混挂指一个负载均衡实例可以同时添加经典网络和VPC网络的ECS作为后端服务器接收监听转发的请求，且支持虚拟服务器组形式的混挂。
- 公网负载均衡实例和私网负载均衡实例都可开通混挂。

混访

- 云数据库RDS和对象存储OSS等云产品支持混访，即支持同时被经典网络和专有网络中的ECS访问。
- 通常该类产品都提供两个访问域名:
  - 一个是经典网络访问域名，
  - 另外一个是专有网络访问域名。

支持混访的云产品

- 目前支持混访的云数据库类型有：
  - 高安全模式下的云数据库RDS版MySQL、SQL Server、PostgreSQL和PPAS
  - 云数据库Redis/Redis集群版
  - 云数据库Memcache新版
  - 云数据库MongoDB副本集
- 尚未支持混访的云数据库类型有：
  - 标准网络模式下的云数据库RDS版。
  - 云数据库MongoDB集群版。
  - 老版本的云数据库Memcache版

支持混访的云产品

- 存储
  - 对象存储
  - 表格存储
- 应用服务
  - 日志服务
- 中间件
  - 消息服务MNS
  - 消息队列MQ
    - 管控
  - 分布式关系型数据库DRDS:
- 大数据
  - MaxCompute
  - DataHub
- 其它
  - 媒体转码MTS

第35页

单ECS迁移方案

- 单ECS迁移方案，即无需通过创建镜像、重新购买等步骤就能把经典网络的ECS实例迁移到专有网络。
- 在控制台上完成迁移预约后，阿里云会根据您设置的迁移时间进行迁移，迁移完成后，您将收到迁移成功的短信消息提醒。

第36页

单ECS迁移方案 – 注意事项

- 迁移过程中ECS需要进行重启，请关注对系统的影响。
- 迁移后，不需要进行任何特殊配置，ECS实例的公网IP不变。
- 迁移后，所有地域的ECS实例的私网IP会变化。
- 迁移到的目标VPC的交换机的可用区必须和待迁移的ECS的可用区相同。

第37页

目录

第38页

什么是负载均衡

- 负载均衡（Server Load Balancer）是将访问流量根据转发策略分发到后端多台云服务器（ECS实例）的流量分发控制服务。负载均衡扩展了应用的服务能力，增强了应用的可用性。
- 负载均衡通过设置虚拟服务地址，将添加的同一地域的多台ECS实例虚拟成一个高性能、高可用的后端服务池，并根据转发规则，将来自客户端的请求分发给后端服务器池中的ECS实例。
- 负载均衡默认检查云服务器池中的ECS实例的健康状态，自动隔离异常状态的ECS实例，消除了单台ECS实例的单点故障，提高了应用的整体服务能力。此外，负载均衡还具备抗DDoS攻击的能力，增强了应用服务的防护能力。

功能特性

- 调度算法
  - 负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）和一致性哈希（CH）调度算法。
- 健康检查
  - 负载均衡会检查后端服务器的运行状况。当探测到后端服务器运行状况不佳时，会停止向其发送流量，然后将流量转发给其他正常运行的后端服务器。
- 会话保持
- 访问控制
- 安全防护
  - 结合云盾，可提供5Gbps的防DDoS攻击能力。
- 域名URL转发
- 证书管理
- 高可用
  - 负载均衡可以将流量转发给多个可用区的后端服务器。并且，负载均衡已经在大部分地域支持了多可用区部署，当主可用区出现故障时，负载均衡可自动切换到备可用区上提供服务。

应用场景

- **应用于高访问量的业务**
  - 如果您的应用访问量很高，您可以通过配置监听规则将流量分发到不同的ECS实例上。此外，您可以使用会话保持功能将同一客户端的请求转发到同一台后端ECS，提高访问效率。
- **消除单点故障**
  - 您可以在负载均衡实例下添加多台ECS实例。当其中一部分ECS实例发生故障后，负载均衡会自动屏蔽故障的ECS实例，将请求分发给正常运行的ECS实例，保证应用系统仍能正常工作。

组成

- 负载均衡由以下三个部分组成：
- **负载均衡实例**（Server Load Balancer instances）一个负载均衡实例是一个运行的负载均衡服务，用来接收流量并将其分配给后端服务器。
- **监听**（Listeners）监听用来检查客户端请求并将请求转发给后端服务器。监听也会对后端服务器进行健康检查。
- **后端服务器**（Backend Servers）一组接收前端请求的ECS实例。您可以单独添加ECS实例到后端服务器池，也可以通过虚拟服务器组或主备服务器组来批量添加和管理。

实例

- 负载均衡实例是一个运行的负载均衡服务实体。
- 使用负载均衡服务，您必须创建一个负载均衡实例，在实例中添加监听和后端服务器。
- 实例类型
  - 公网负载均衡实例
  - 私网负载均衡实例

监听

- 负载均衡实例监听负责检查连接请求，然后根据调度算法定义的转发策略将请求流量分发至后端服务器。
- 负载均衡提供四层（TCP/UDP协议）和七层（HTTP/HTTPS协议）监听

监听

协议	说明	使用场景
TCP	• 面向连接的协议，在正式收发数据前，必须和对方建立可靠的连接 • 基于源地址的会话保持 • 在网络层可直接看到来源地址 • 数据传输快	• 适用于注重可靠性，对数据准确性要求高，速度可以相对较慢的场景，如文件传输、发送或接收邮件、远程登录 • 无特殊要求的Web应用 详情请参见添加TCP监听。
UDP	• 面向非连接的协议，在数据发送前不与对方进行三次握手，直接进行数据包发送，不提供差错恢复和数据重传 • 可靠性相对低；数据传输快	关注实时性而相对不注重可靠性的场景，如视频聊天、金融实时行情推送。 详情请参见添加UDP监听。
HTTP	• 应用层协议，主要解决如何包装数据 • 基于Cookie的会话保持 • 使用X-Forward-For获取源地址	需要对数据内容进行识别的应用，如Web应用、小的手机游戏等。 详情请参见添加HTTP监听。
HTTPS	• 加密传输数据，可以阻止未经授权的访问 • 统一的证书管理服务，用户可以将证书上传到负载均衡，解密操作直接在负载均衡上完成	需要加密传输的应用。 详情请参见添加HTTPS监听。

调度算法

- 负载均衡支持轮询、加权轮询（WRR）、加权最小连接数（WLC）和一致性哈希（CH）四种调度算法。
- **加权轮询**(WRR)：权重值越高的后端服务器，被轮询到的次数（概率）也越高。
- **轮询**(RR)：按照访问顺序依次将外部请求分发到后端服务器。
- **加权最小连接数**(WLC)：除了根据每台后端服务器设定的权重值来进行轮询，同时还考虑后端服务器的实际负载（即连接数）。当权重值相同时，当前连接数越小的后端服务器被轮询到的次数（概率）也越高。
- **一致性哈希**（CH）：
  - **源IP**：基于源IP地址的一致性hash，相同的源地址会调度到相同的后端服务器。
  - **四元组**：基于四元组的一致性hash（源IP+目的IP+源端口+目的端口），相同的流会调度到相同的后端服务器。

会话保持

- 开启会话保持后，负载均衡监听会把来自同一客户端的访问请求分发到同一台后端服务器上。
- **TCP协议**是基于IP地址的会话保持，即来自同一IP地址的访问请求转发到同一台后端服务器上。
- **HTTP协议**会话保持基于Cookie。负载均衡提供了两种Cookie处理方式：
  - 植入Cookie：客户端第一次访问时，负载均衡会在返回请求中植入Cookie
  - 重写Cookie：负载均衡服务发现用户自定义了Cookie，将会对原来的Cookie进行重写。

第47页

获取客户端真实IP

- 针对四层监听，后端服务器可直接获得来访者的真实IP，无需采用其它手段获取。
- HTTP监听通过 X-Forwarded-For获取客户端真实IP，默认开启。

第48页

HTTP/HTTPS连接的超时时间是如何规定的？

- HTTP长连接的请求数量限定是最多连续发送100个请求，超过限定将关闭这条连接。
- HTTP长连接两个HTTP/HTTPS请求之间的超时时间是可配置的，配置范围为1~60秒（存在误差1~2秒），超过后会关闭TCP连接，如果用户有长连接使用需求请尽量保持在13秒之内发送一个心跳请求。
- 负载均衡与后端一台ECS实例TCP三次握手完成过程的超时时间为5秒，超时后选择下一台ECS实例；查询访问日志的upstream响应时间可以定位。
- 负载均衡等待一台ECS实例回复请求的响应时间是可配置的，配置范围为1~180秒，超过后一般会返回504响应码或408响应码给客户端，查询访问日志的的upstream响应时间可以定位。
- HTTPS session重用超时间为300秒，超过后同一客户端需要重新进行完整的SSL握手过程。

第49页

后端服务器

- 后端服务器，用来接收负载均衡监听转发的请求
- 同一地域的多台ECS实例虚拟成一个高性能、高可用的应用服务池
- 不同的监听可以关联不同的服务器组
- **注意：**
  - 负载均衡不支持跨地域部署，确保ECS实例的所属地域和负载均衡实例的所属地域相同。
  - 负载均衡本身不会限制后端ECS实例使用哪种操作系统，只要您的两台ECS实例中的应用服务部署是相同的且保证数据的一致性即可。
  - 您可以指定后端服务器池内各ECS实例的转发权重。权重越高的ECS实例将被分配到更多的访问请求。
  - 如果您同时开启了会话保持功能，那么有可能会造成后端服务器的访问并不是完全相同的。

第50页

服务器组

- **默认服务器组**
  - 用来接收前端请求的ECS实例。如果监听没有设置虚拟服务器组或主备服务器组，默认将请求转发至默认服务器组中的ECS。
- **主备服务器组**
  - 一个主备服务器组只包括两台ECS实例，一台作为主服务器，一台作为备服务器。
  - 由于备服务器不会做健康检查，所以只要主服务器健康检查失败，系统会直接将流量切到备机。
  - 当主服务器健康检查成功恢复服务后，流量会自动切到主服务器。
- **虚拟服务器组**
  - 当您需要将不同的请求转发到不同的后端服务器上时，或需要通过域名和URL进行请求转发时，可以选择使用虚拟服务器组。

健康检查

- 判断后端服务器的业务可用性，提高前端业务整体可用性
  - 出现异常时，负载均衡会自动将新的请求分发到其它健康检查正常的ECS上
  - 当该ECS恢复正常运行时，负载均衡会将其自动恢复到负载均衡服务中。
- 负载均衡健康检查使用的地址段是100.64.0.0/10，后端服务器务必不能屏蔽该地址段。
- 针对七层监听，健康检查通过HTTP HEAD探测来获取状态信息
- 针对四层TCP监听，健康检查通过定制的TCP探测来获取状态信息
- 针对四层UDP监听，健康检查通过UDP报文探测来获取状态信息

访问日志

- 负载均衡的访问日志功能收集了所有发送到负载均衡的请求的详细信息，包括请求时间、客户端IP地址、延迟、请求路径和服务器响应等。负载均衡作为公网访问入口，承载着海量的访问请求，您可以通过访问日志分析客户端用户行为、了解客户端用户的地域分布、进行问题排查等。
- 在开启负载均衡访问日志后，您可以将访问日志存储在日志服务（SLS）的日志库（Logstore）中，采集分析访问日志。
- 只有七层负载均衡支持访问日志功能

目录

什么是弹性公网IP

- 弹性公网IP EIP（Elastic IP Address）是可以独立购买和持有的公网IP地址资源。目前，EIP可绑定到专有网络类型的ECS实例、专有网络类型的私网SLB实例、专有网络类型的辅助弹性网卡、NAT网关和高可用虚拟IP上。
- EIP是一种NAT IP。它实际位于阿里云的公网网关上，通过NAT方式映射到了被绑定的云资源上。和云资源绑定后，云资源可以通过EIP与公网通信。

第55页

固定公网IP

- 如果需要ECS实例与互联网通信，就必须为ECS实例配置公网IP和公网带宽， 阿里云的公网IP有两种类型。
- **ECS固定公网IP**：当您在创建专有网络（VPC）类型的ECS实例时，可以选择使用系统分配的公网IP，该公网IP无法与ECS实例解绑，称之为ECS实例的固定公网IP。
- **EIP**：EIP是可以独立购买和持有的公网IP地址资源。目前，EIP可绑定到专有网络类型的ECS实例、专有网络类型的私网SLB实例、专有网络类型的辅助弹性网卡、NAT网关和高可用虚拟IP上，还可以使用共享带宽和共享流量包等网络产品，节约公网成本。
- 无论是固定公网IP还是EIP，对外提供公网服务的能力是一样的，都是阿里巴巴优质的多线BGP网络。两者的最大区别为是否可以和ECS实例解绑。EIP可以随时从ECS实例上解绑，在需要时重新绑定；固定公网IP无法从ECS实例上解绑。

第56页

EIP与ECS固定公网IP的区别

比较点	EIP	ECS固定公网IP
支持的网络环境	专有网络	专有网络和经典网络
是否支持单独持有	支持	不支持
是否支持在ECS实例上的弹性插拔	支持	不支持
ECS实例网卡上是否可见该IP	**EIP网卡可见模式**和**多EIP网卡可见模式**下可见	经典网络：可见 专有网络：不可见

第57页

EIP 有何优势

- 独立购买与持有您可以单独持有一个EIP，作为您账号下一个独立的资源存在，无需与其它计算资源或存储资源绑定购买。
- 弹性绑定您可以在需要时将EIP绑定到需要的资源上，在不需要时将之解绑并释放，避免不必要的计费。
- 可配置的网络能力您可以根据业务需要随时调整EIP的带宽峰值，带宽峰值的修改即时生效。

第58页

目录

什么是NAT网关

- NAT网关（NAT Gateway）是一款企业级的公网网关。
- NAT网关作为一个网关设备，需要绑定公网IP才能正常工作。创建NAT网关后，您可以为NAT网关绑定弹性公网IP（EIP）。
- NAT网关支持SNAT和DNAT功能。
  - SNAT可以为VPC内无公网IP的ECS实例提供访问互联网的代理服务。
  - DNAT可以将NAT网关上的公网IP映射给ECS实例使用，使ECS实例能够提供互联网服务。
- 您可以使用共享带宽和共享流量包来降低NAT网关的公网成本。

使用场景

- NAT网关适用于专有网络类型的ECS实例需要主动访问公网和被公网访问的场景。
- **搭建高可用的SNAT网关**
  - 在IT系统中，往往存在一些服务器需要主动访问互联网，但出于安全性考虑需要避免将这些服务器所持有的公网IP暴露在公网上。此时，您可以使用NAT网关的SNAT功能实现这一需求。
- **提供公网服务**
  - 专有网络类型的ECS实例可以通过端口映射和IP映射的方式对外提供服务。
- **共享公网带宽**
  - 如果您的应用需要面向互联网，您需要为该应用购买公网带宽。为了应对业务流量可能发生的变化，在购买带宽时会考虑一定的冗余。当IT系统中同时存在多个面向互联网的应用时，为每个应用购买冗余带宽会造成资源和成本的浪费。
  - 您可以将多个EIP加入到共享带宽中，更好地进行公网带宽资源的管理和成本的控制。另外，多个面向互联网的应用可能存在流量错峰情况，多IP共享带宽功能可以进一步缩减公网带宽总量。

SNAT条目

- 您可以通过在SNAT表中创建SNAT条目，实现代理上网功能。
- SNAT功能提供如下两种粒度，以实现VPC内ECS实例访问互联网。
- **交换机粒度**
  - 选择交换机为粒度创建SNAT条目后，当指定交换机下的ECS实例发起互联网访问请求时，NAT网关会为其提供SNAT服务（代理上网服务），且使用的公网IP为指定的公网IP。默认情况，交换机下的所有ECS实例都可以使用配置的公网IP访问互联网。
- **ECS粒度**
  - 选择ECS为粒度创建SNAT条目后，指定的ECS实例通过配置的公网IP访问互联网。当指定的ECS实例发起互联网访问请求时，NAT网关会为其提供SNAT服务（代理上网服务），且使用的公网IP为指定的公网IP。

DNAT条目

- NAT网关支持DNAT功能，将NAT网关上的公网IP映射给专有网络的ECS实例使用，使ECS实例可以面向互联网提供服务。
- DNAT功能包括端口映射与IP映射：
- **端口映射**
  - 配置端口映射后，NAT网关会将以指定协议和端口访问该公网IP的请求转发到目标ECS实例的指定端口上。
- **IP映射**
  - 配置IP映射后，NAT网关会将任何访问该公网IP的请求都将转发到目标ECS实例上。

第63页

常见问题

- **一个公网IP可以同时设置DNAT和SNAT规则吗？**
  - 不支持。需要分别绑定不同的公网IP来设置DNAT规则和SNAT规则。

第64页

目录

第65页

什么是高速通道

- 阿里云高速通道（Express Connect）可在本地数据中心和云上专有网络间建立高速、稳定、安全的私网通信。高速通道的专线连接绕过您网络路径中的Internet服务提供商，可避免网络质量不稳定问题，同时可免去数据在传输过程中被窃取的风险。
- 高速通道通过专线将您的本地内部网络连接到阿里云的接入点。专线的一端接到您本地数据中心的网关设备，另一端接到高速通道的边界路由器。此连接更加安全可靠、速度更快、延迟更低。
- 将边界路由器和要访问的阿里云专有网络加入同一个云企业网后，本地数据中心便可访问阿里云专有网络内的全部资源，包括云服务器、容器、负载均衡和云数据库等。

第66页

组成部分

- 高速通道由以下部分组成：
- **物理专线连接**：通过高速通道建立的一个您本地IDC机房与阿里云接入点的专用网络连接。您可以通过以下两种方式建立物理专线连接：
  - **自主申请物理专线接口**，企业自主拉通本地数据中心到阿里云接入点的专线，该方式独占一个物理端口。
  - **合作伙伴共享接入**，合作伙伴的接入点已经与阿里云的接入点完成了对接，您只需联系阿里云的合作伙伴，合作伙伴会完成本地IDC机房到合作伙伴接入点的专线部署。该方式，运营商和阿里云之间的连接是多租户共享的。
- **边界路由器**
  - 是本地IDC的CPE设备和阿里云接入点连接的一个路由器，作为数据从本地数据中心到阿里云机房之间的桥梁。

边界路由器

- 基于软件自定义网络SDN（Software Defined Network）架构下的三层Overlay技术和交换机虚拟化技术，阿里云将客户的物理专线接入的端口隔离起来，并抽象成边界路由器VBR（Virtual border router）。VBR是CPE（Customer-premises equipment）设备和VPC之间的一个路由器，作为数据从VPC到本地数据中心的转发桥梁。
- 边界路由器同VPC中的路由器一样，同样管理一个路由表。在该路由表中配置路由条目，可以对边界路由器中的流量转发进行管理。

专线连接和VPN连接对比

- 您可以通过高速通道专线接入也可以通过VPN连接打通本地数据中心和云上网络通信。但专线连接在网络质量、安全性和传输速度等方面都优于VPN连接

对比项	物理专线连接	VPN连接
网络质量	通过专用的物理专线接入阿里云网络，提供内网级通信质量，网络时延和丢包率等极低。	使用共享的公网资源进行通信，网络时延和丢包率等无法保证。
安全性	用户独享物理专线，无数据泄露风险，安全性高。满足金融、政企等对网络安全性要求高的客户需求。	基于公网的加密通信，可以满足一般客户的网络传输安全性需求。
传输带宽	单链路最大支持100Gbps的带宽，可满足大数据量业务的客户。 支持多条专线做ECMP，达到T级别的带宽，在保障服务可用性的基础上叠加扩充带宽上限。	网络带宽受限于公网IP的带宽。

对等连接

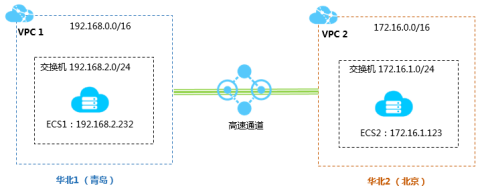
- 高速通道的对等连接功能于2019年6月20日停止售卖。您可以将使用对等连接建立的VPC和VBR迁移至云企业网。
- 用于两个VPC之间，VPC与VBR之间建立对等连接。
- 对等连接的限制
  - 多个VBR和一个VPC连通后，两个VBR之间无法通过VPC互通。
  - 多个VPC和一个VBR连通后，两个VPC之间无法通过VBR互通。

发起端和接收端

- 在建立对等连接时，要连接的两端（VPC或VBR），一个是发起端，另一个是接收端。只有发起端才可以发起连接，接收端只能等待发起端发起连接。发起端和接收端仅用于控制连接建立的过程，在实际进行网络通信时，通信链路是双向的，发起端和接收端没有任何差别。
- 对于同账号VPC互通，高速通道提供了同时创建两端的选项。在这种情况下，您不需要手动发起连接，系统会自动发起并建立连接。对于跨账号VPC互通，您必须手动发起连接。

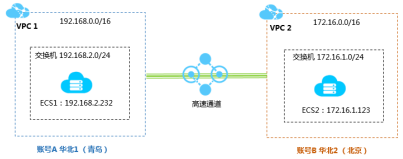
同账号VPC互连

- 步骤一：创建对等连接
- 步骤二：配置路由
  - 配置发起端路由
  - 配置接收端路由
- 步骤三：配置安全组



跨账号VPC互连

- 步骤一：创建发起端
- 步骤二：创建接收端
- 步骤三：添加发起端
- 步骤四：添加接收端并建立对等连接
- 步骤五：配置路由
- 步骤六：配置安全组



目录

什么是智能接入网关

- 智能接入网关（Smart Access Gateway）是阿里云基于云原生的SD-WAN解决方案。企业可以通过智能接入网关实现一站式接入上云，获得更加智能、更加可靠和更加安全的上云体验。
- 智能接入网关分为硬件版和APP版：
  - **硬件版**：硬件CPE设备形态，适用于站点site-to-site接入。
    - SAG-100WM可放在桌面或弱电箱内，适用于小型分支门店快捷接入。
    - SAG-1000可放在机架内，适用于IDC和大型分支接入。
  - **APP版**：APP形态，适用于终端point-to-site接入。

目录

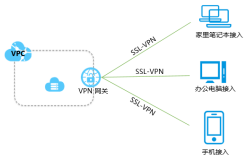
什么是VPN网关

- VPN网关是一款基于Internet的网络连接服务，通过加密通道的方式实现企业数据中心、企业办公网络或Internet终端与阿里云专有网络安全可靠的连接。
- VPN网关提供
  - **IPsec-VPN连接**，您可以使用IPsec-VPN功能将本地数据中心与VPC或不同的VPC之间进行连接。
  - **SSL-VPN连接**，您可以使用SSL-VPN功能从客户端远程接入VPC中部署的应用和服务。

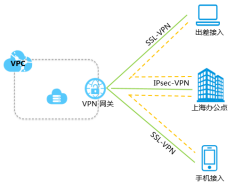
使用场景

VPC到本地数据中心的连接

VPC到VPC的连接



VPC到移动客户端的连接



IPsec-VPN和SSL-VPN组合使用

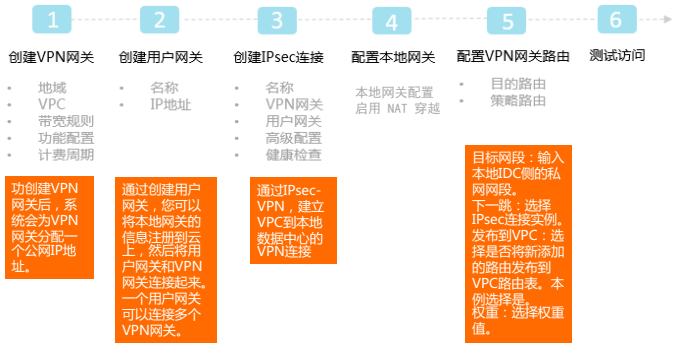
产品优势
安全：使用IKE和IPsec协议对传输数据进行加密，保证数据安全可靠。

高可用：采用双机热备架构，故障时秒级切换，保证会话不中断，业务无感知。

成本低：基于Internet建立加密通道，比建立专线的成本更低。

配置简单：开通即用，配置实时生效，快速完成部署。

VPC到本地数据中心的连接

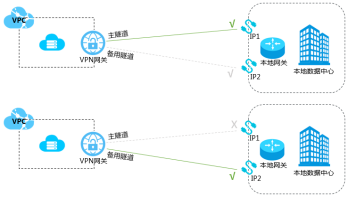


VPC到VPC的连接

- 同一个账号下的两个VPC
  - 步骤一：创建VPN网关
  - 步骤二：创建用户网关
  - 步骤三：创建IPsec连接
  - 步骤四：配置VPN网关路由
  - 步骤五：测试私网通信
- 跨账号VPC互通，操作步骤和同账号VPC互通一样。只是在创建用户网关前，需要获取对方账号的VPN网关的公网IP地址，然后使用获取的对方账号的公网IP地址创建用户网关。

高可用-双IPsec隧道

- 如果您的本地网关有双公网IP，您可以分别与VPN网关建立IPsec隧道，以实现主备隧道冗余。
- 创建用户网关时，创建两个用户网关，将本地网关的两个公网IP地址注册到用户网关中用于建立IPsec连接。
- 创建IPsec连接时，创建两个IPsec连接，将VPN网关分别和两个用户网关连接起来，并开启健康检查。

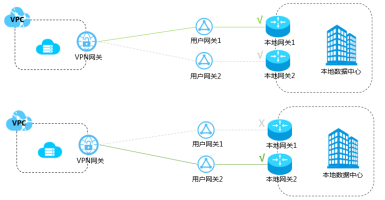


当基于IP1的Internet链路正常时，本地数据中心与VPC之间的所有流量只通过主隧道转发。

当基于IP1的Internet链路异常时，本地数据中心与VPC之间的所有流量切换到备用隧道。

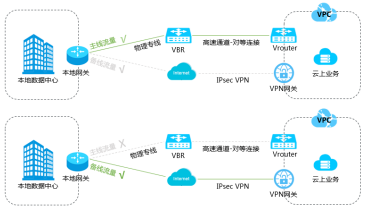
高可用-双用户网关

- 您可以在本地部署两个CPE网关，VPN网关分别与两个用户网关建立IPsec VPN连接，以实现多VPN连接冗余。
- 两个用户网关同时连接一个阿里云VPN网关，每个用户网关与VPN网关建立一条IPsec隧道，并为IPsec连接配置健康检查，两条IPsec隧道均为协商成功状态。当健康检查检测用户网关不可用时，路由自动切换到另外一个用户网关。



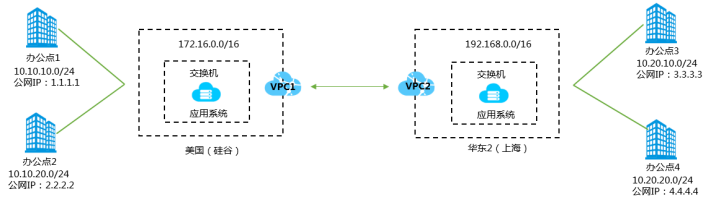
IPsec-VPN配合专线实现主备冗余

- 本地数据中心与VPC既通过物理专线连接，又通过IPsec-VPN连接。
  - 当物理专线正常时，本地数据中心与VPC之间的所有流量只通过物理专线转发。
  - 当物理专线异常时，本地数据中心与VPC之间的所有流量切换至VPN线路。



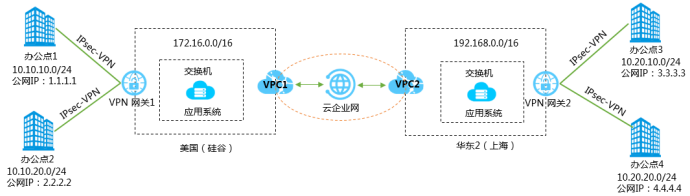
IPsec-VPN配合云企业网搭建高速全球网络

- 某跨国公司在美国硅谷和中国上海均有两个办公点，且该跨国公司在美国（硅谷）和华东2（上海）地域分别创建了VPC1和VPC2，并在两个VPC中部署了应用系统。因业务发展，需要美国硅谷的两个办公点、中国上海的两个办公点、VPC1、VPC2全互通。



IPsec-VPN配合云企业网搭建高速全球网络

- 您可以通过VPN网关1将美国硅谷的办公点1、办公点2与VPC1连接起来，VPN网关2将上海的办公点3、办公点4与VPC2连接起来，然后再将VPC1和VPC2加载到同一云企业网中，实现全球网络全互通。



思考题

1. 如果用高速通道（对等连接）替代云企业网，能否实现全互通？

VPN 常见问题

- 每个VPN网关可以建立多少个IPsec连接？
  - 每个VPN网关最多可以支持10个IPsec连接且无例外。如需要更多数量的IPsec连接，请创建多个VPN网关。
- 是否可以通过VPN网关访问Internet？
  - 不可以。VPN网关仅提供私网接入VPC功能，不提供Internet访问的功能。
- VPC互通流量是否经过Internet？
  - 不经过。通过VPN实现跨地域VPC互访，流量经过阿里云网络，不经过Internet。

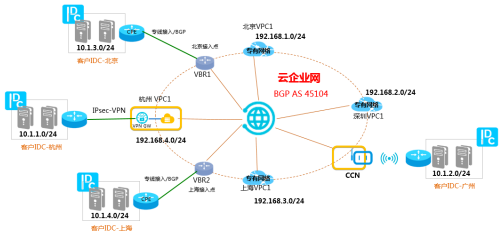
目录

什么是云企业网

- 云企业网（Cloud Enterprise Network）是承载在阿里云提供的高性能、低延迟的私有全球网络上的一张高可用网络。
- 云企业网可帮助您在不同地域VPC间，VPC与本地数据中心间搭建私网通信通道，通过自动路由分发及学习，提高网络的快速收敛和跨网络通信的质量和安全性，实现全网资源的互通，帮助您打造一张具有企业级规模和通信能力的互联网络。

多接入方式构建企业级混合云

- 云企业网致力于为客户提供优质的网络传输环境，通过简化客户的组网过程，帮助客户快速构建一张具有企业级规模和通信能力的混合云网络。
- 通过和高速通道物理专线、VPN网关、智能接入网关组合使用，快速构建一张混合云网络。



组成部分

- **云企业网实例**
  - 云企业网实例是创建、管理一体化网络的基础资源。
  - 创建云企业网实例后，将需要互通的网络实例加载到云企业网实例中，再购买带宽包，设置跨地域互通带宽，便可实现全球网络资源互通。
- **网络实例**
  - 加载到云企业网中的网络实例全互联，网络实例包含专有网络（VPC）、边界路由器（VBR）和云连接网（CCN）。
- **带宽包**
  - 同地域之间网络实例互通，无需购买带宽包。
  - 跨地域之间网络实例互通，必须为要互通的地域所属的区域购买带宽包。

为什么选择云企业网

- **一网通天下**
  - 云企业网打造的是一张能够实现阿里云全球网络资源互联、并能够与接入阿里云的网络资源互联的企业级网络。全网通过IP地址唯一性管理，有效避免了IP地址冲突问题。用户不需要额外配置，网络通过控制器实现多节点、多级路由的自动转发与学习，实现全网的路由快速收敛。
- **就近接入与最短链路互通**
  - 云企业网在全球超过60个地域部署了接入及转发节点，方便全球用户就近接入阿里云，避免绕行公网带来的时延及业务受损。云企业网内部通过最短链路计算方式，快速实现本地IDC与阿里云内资源的互通。
- **链路冗余及容灾**
  - 云企业网具有高可用及网络冗余性，全网任意两点之间存在多组独立冗余的链路。即使部分链路中断，云企业网也可以保证客户的业务正常运行，不会发生抖动及中断。

使用场景

- **同地域网络实例互通**
  - 您只需完成两步便可实现同账号下同地域内的专有网络（VPC）和边界路由器（VBR）互通。首先创建一个云企业网实例，然后将要互通的网络实例（专有网络和边界路由器）加载到云企业网实例中即可。
- **跨地域网络实例互通**
  - 您可以通过云企业网实现任意两个地域下的网络实例互通，例如使北京地域VPC与杭州地域VPC互通。您首先需要创建一个云企业网实例，然后将要互通的网络实例（专有网络和边界路由器）加载到云企业网实例，再购买一个带宽包，设置跨地域互通带宽即可。

云企业网与高速通道的区别

对比点	云企业网	高速通道
网络连接	全网互联 加载到云企业网的网络实例（VPC和VBR）彼此之间全网互联，任何两点间都可以通过云企业网建立安全、可靠、高速的内网通信。	单点连接 高速通道不具有传递性。使用高速通道互通的VPC或本地数据中心只能和对端的VPC互通。
路由管理	动态学习 云企业网基于Fullmesh链路，动态学习并转发路由，提高了路由的快速收敛和网络通信的质量及安全性。	手动配置 高速通道配置过程中需要针对端到端进行路由配置。
带宽管理	跨地域共享带宽包 云企业网提供带宽包，带宽包按区域售卖，方便用户根据业务需要调整跨地域带宽。有利于资源调配和节约成本。	点到点购买 高速通道的带宽需要在购买高速通道时指定互通地域的带宽。购买后可以调整带宽大小，但不可以更改地域。

谢 谢

xujiajie@hotmail.com