



网络概述 网络介绍

文档版本: 20220706



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。

- 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。
- 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。
- 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。	大) 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。	⑦ 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 cd /d C:/window 命令,进入 Windows系统文件夹。
斜体	表示参数、变量。	bae log listinstanceid
[] 或者 [alb]	表示可选项,至多选择一个。	ipconfig [-all -t]
{} 或者 {alb}	表示必选项,至多选择一个。	switch {act ive st and}

目录

1.网络介绍	06
1.1. 阿里云网络	06
1.2. 云上网络设计	10
2.网络连接	13
2.1. 公网访问	13
2.2. 跨地域互连	14
2.3. ^{New} 混合云网络	15
3.解决方案	17
3.1. 互动课堂场景网络解决方案	17
3.2. 企业级云上网络解决方案	29
3.2.1. 企业级云上网络解决方案概述	29
3.3. 全球互联	30
3.3.1. 阿里云混合云网络互联	30
3.3.1.1. 阿里云混合云网络互联方案概述	30
3.3.1.2. 云上云下互通	33
3.3.1.2.1. 通过VPN网关(IPsec-VPN)上云方案	33
3.3.1.2.2. SAG双机直挂静态路由上云方案	36
3.3.1.2.3. SAG双机旁挂动态路由上云方案	44
3.3.1.2.4. SAG双机旁挂静态路由上云方案	50
3.3.1.2.5. IPsec-VPN联合物理专线实现主备链路上云方案	57
3.3.1.2.6. SAG联合物理专线实现主备链路上云方案	63
3.3.1.2.7. IDC通过静态路由主备专线链路上云方案	73
3.3.1.2.8. IDC通过BGP主备专线链路上云方案	80
3.3.1.3. 跨地域互通	86
3.3.1.3.1. 跨地域VPC间互通方案	86
3.3.1.3.2. 跨地域IDC上云互通方案	90

3.3.1.4. 多云互通	97
3.3.1.4.1. SAG vCPE实现多云互通	97
3.3.2. 阿里云SD-WAN解决方案	104
3.3.3. 企业级移动办公解决方案	121

1.网络介绍

1.1. 阿里云网络

阿里云在全球24个地域部署了110多个接入点和1500多个边缘节点,可向企业提供优质的全球网络服务。

经过多年的自主研发,阿里云构建了云上网络、跨地域网络、混合云网络一套完整的可满足不同使用场景的 网络解决方案。阿里云的网络产品和服务可单独使用也可搭配使用。



云上网络

阿里云云上网络基于安全隔离的专有网络架构,为您提供优质、功能齐全的云上网络服务。例如网络地址转换、流量分发、公网访问等。同时,提供共享带宽和共享流量包服务,服务器可以共享流量和带宽,优化网络成本。





场景	产品
定义云上网 络	专有网络 专有网络VPC(Virtual Private Cloud)是您在云上创建的专用虚拟网络。您可以在自己的专有网络 内部署、使用云资源,例如ECS实例、RDS数据库和容器Kubernetes服务等。 专有网络类似于您在本地数据中心的传统网络,但附带了很多阿里云基础设施的其他优势,例如可扩 展、安全隔离、访问控制等。
	 负载均衡 负载均衡SLB(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。SLB支持TCP、UDP、HTTP、HTTPS协议的应用流量转发。 负载均衡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。
管理公网流	<mark>弹性公网IP</mark> 弹性公网IP(Elastic IP Address,简称EIP),是可以独立购买和持有的公网IP地址资源。 EIP可绑定到专有网络类型的ECS实例、辅助弹性网卡ENI、专有网络类型的私网SLB实例和NAT网关 上。此外,您可以将EIP加入购买的共享带宽中,节省公网带宽使用成本。
量	NAT网关 NAT网关(NAT Gateway)是一款企业级的VPC网关,提供NAT代理(SNAT、DNAT)、10 Gbps 级别的转发能力、以及跨可用区的容灾能力。NAT网关与共享带宽包配合使用,可以组合成为高性 能、配置灵活的企业级网关。

场景	产品
	IPv6网关 IPv6网关(IPv6 Gateway)是VPC的一个IPv6互联网流量网关。您可以通过配置IPv6公网带宽和仅主 动出规则,灵活定义IPv6互联网出流量和入流量。
公网加速	全球加速 全球加速GA(Global Accelerator)是一款覆盖全球的网络加速服务,依托阿里云优质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。
节约公网成 本	共享带宽 共享带宽提供地域级别的带宽共享和复用能力。购买一个共享带宽可让一个地域下所有EIP复用共享带 宽中的带宽,并提供包括按带宽计费和按增强型95计费等多种计费模式,通过共享带宽可有效节省公 网带宽使用成本。
	<mark>共享流量包</mark> 共享流量包产品是一款流量套餐产品,使用方便,价格实惠。在购买共享流量包产品后会立刻生效, 并自动抵扣按流量计费的EIP、SLB和NAT网关产品产生的流量费用,直到流量包用完为止。

混合云网络

阿里云混合云网络帮助企业打通云上云下系统和数据,消除信息孤岛。为不同规模、不同地域、各行业的企业机构提供云下网络(IDC、总部、分支、门店)到阿里云上安全、可靠、灵活的网络连接。



场景	产品
数据中心IDC 上云	<mark>高速通道</mark> 阿里云高速通道(Express Connect)可在本地数据中心IDC(Internet Data Center)和云上专有网 络VPC(Virtual Private Cloud)间建立高速、稳定、安全的私网通信。高速通道的物理专线数据传 输过程可信可控,避免网络质量不稳定问题,同时可避免数据在传输过程中被窃取。
分支或门店 上云	智能接入网关 智能接入网关(Smart Access Gateway)是阿里云提供的一站式快速上云解决方案。企业可通过智 能接入网关实现互联网就近加密接入,获得更加智能、更加可靠、更加安全的上云体验。 智能接入网关提供不同型号的网关设备供您选择,不同的网关设备可满足不同的上云场景。SAG- 100WM设备适用于小型分支和门店通过直挂组网的方式接入阿里云,SAG-1000设备适用于总部接入 阿里云,满足大型网络组网需求。
	VPN网关 VPN网关是一款基于互联网,通过加密通道将企业数据中心、企业办公网络或互联网终端和阿里云专 有网络(VPC)安全可靠连接起来的服务。您也可以使用VPN网关在VPC之间建立加密内网连接。
移动端上云	<mark>智能接入网关APP</mark> 智能接入网关(Smart Access Gateway)是阿里云提供的一站式快速上云解决方案,智能接入网关 APP支持终端(PC、手机)直接拨号内网加密安全上云,适用于移动办公、远程运维的场景。

跨地域网络

阿里云跨地域网络提供全球跨地域专有网络间互联。帮助您快速构建合法合规的混合云和分布式业务系统网 络。

<mark>云企业网</mark>是您在云上的一张全球网络,您创建云企业网CEN后,只需要把需要通信的VPC加入到CEN即可实现 网络互通,同时云企业网还支持把通过智能接入网关或高速通道接入的云下IDC、门店、分支等和云上VPC构 成全互联网络。



售前咨询

您可以通过以下方式进行网络产品的售前咨询:

- 售前在线咨询: 在帮助文档右侧单击 □图标。
- 云网络解决方案咨询
- 售前电话咨询: 95187转1

1.2. 云上网络设计

在阿里云使用云产品部署服务时,您首先要规划好网络,例如云上网络的网段、交换机部署、路由策略等。

什么是专有网络?

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。专有网络由以下部分组成:

• 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。

您可以使用下表中标准的私网网段及其子网作为专有网络的私网网段。详细信息,请参见网络规划。

网段	可用私网IP数量 (不包括系统保留地址)
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0/8	16,777,212

• 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。

详细信息,请参见路由表概述。

● 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。

详细信息,请参见交换机。



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。

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。以下原则可以帮助您确定需 要多少个专有网络和交换机:

• 需要几个专有网络

专有网络之间互相隔离,您可以通过云企业网打通专有网络间的通信。创建一个还是多个专有网络和您的业务规划相关:

- 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。目前,单个专有网络内运行的云产品实例可达15,000个,这样的容量基本上可以满足您的需求。
- 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。您可以通过使用云企业网实现专有网络互通。
- 需要几个交换机

云资源必须部署在一个指定的交换机内。同一个专有网络内的不同交换机的资源可以互相通信。建议您每 个专有网络至少创建两个交换机: 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。

同一地域不同可用区之间的网络通信延迟很小,但也需要经过业务系统的适配和验证。由于系统调用复 杂加上系统处理时间、跨可用区调用等原因可能产生期望之外的网络延迟。建议您进行系统优化和适 配,在高可用和低延迟之间找到平衡。

 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。

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。在规划专有网络网段时,请注意:

- 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。
- 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。
- 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。例如专有网络的网段是192.168.0.0/16,那么该专有网络下的交换机的网段可以是192.168.0.0/17,一直到192.168.0.0/29。规划交换机网段时,请注意:

- 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。更多详细信息,请参见ClassicLink概述。

设计原则

在创建专有网络时,建议您遵循以下通用设计原则:

- 确保地址空间不重叠。
- 交换机的网段不应涵盖专有网络的整个地址。
- 至少创建两个交换机,并部署在不同可用区内,以确保高可用。

2.网络连接

2.1. 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(Internet)或被公网访问。

下表列举了阿里云提供的专有网络环境下的公网访问服务。这些服务适用于不同的业务场景,例如您的游戏 用户遍布全球,当您需要为海外用户访问加速时便可选择使用全球加速产品。

选项	场景	优势
弹性公网IP (EIP)	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。 适用于以下场景: • 云资源例如ECS实例需要访问公网 • 需要高可用的IP迁移方案 • 需要多个公网IP灵活对外提供服务或主动访问 公网	 灵活,可随时绑定和解绑 BGP多线带宽 配合使用共享带宽和共享流量包可帮您节省公 网成本 更多详情请参见共享带宽和共享流量包。
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。 适用于以下场景: •为无公网的ECS提供上网能力 •让无公网的ECS面向Internet提供服务	 免自建、免维护、高可靠、可弹性扩展 提供SNAT和DNAT功能,无需基于云服务器 搭建公网网关,功能灵活、简单易用、稳定可 靠。 安全 避免ECS的管理端口暴露于公网,更加安全, 更加省心。 高转发性能 NAT网关是基于阿里云自研的分布式网关,是 阿里云使用SDN技术推出的一款虚拟网络硬 件。NAT网关支持10Gbps级别的转发能力, 为大规模公网应用提供支撑。
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。 适用于以下场景: IPv4/IPv6云上公网入口:海量流量分发处理能力 云上云下多活:通过挂载云下IDC服务器,实现云上云下多活 	在DNAT方面,负载均衡是基于端口的负载均 衡,即一个负载均衡的一个端口可以对应多台 ECS。 负载均衡通过对多台ECS进行流量分发,可以扩 展应用系统对外的服务能力,并通过消除单点故 障提升应用系统的可用性。 绑定EIP后,支持使用共享带宽和共享流量包, 可帮您降低公网成本,更多详情请参见共享带 宽和共享流量包。

选项	场景	优势
IPv6网关	IPv6网关是专有网络VPC的一个IPv6互联网网 关,用户可通过IPv6网关管理专有网络的IPv6地 址、为IPv6地址分配IPv6公网带宽、配置IPv6公 网规则。 适用于以下场景: • 搭建IPv6和IPv4双栈环境,支持IPv6和IPv4客 户端访问 • 业务只需要主动访问IPv6终端,但不希望ECS 实例的IPv6地址被外部IPv6终端连接	 高可用 IPv6网关提供跨可用区级的高可用能力,帮您 打造极致稳定的IPv6公网网关服务。 高性能 单个IPv6网关实例可提供万兆级吞吐量,满足 超大业务的IPv6公网需求。 灵活管理公网通信 您可以通过调整公网带宽和设置仅主动出规 则,灵活设置IPv6地址的公网通信能力。

2.2. 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,减少网络延时和丢包等问题。

选项	场景	优势
云企业网	 云企业网CEN (Cloud Enterprise Network)可以在专有网络VPC (Virtual Private Cloud) 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。云企业网通过路由自动分发及学习,使网络快速收敛,实现全网资源互通,帮您打造一张具有企业级规模和通信能力的全球互联网络。 适用于以下场景: 同地域或跨地域VPC互通 本地数据中心上云 在中资出海或外企进中国的场景下,帮助企业快速构建全球互联网络 	 配置简单 您无需额外配置,云企业网通过阿里云控制器 实现路由的自动分发与学习,使全网路由快速 收敛。 低时延高速率 云企业网提供低延迟、高速的网络传输能力。 本地互通最大速率可达到设备端口转发速率。 在全球互通的时延中,整体时延较公网互通时 延有很大提升。 就近接入与最短链路互通 云企业网在全球多个地域部署了接入及转发节 点,方便您的网络就近接入阿里云,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,快速实现本地数据中心 与阿里云内资源的互通。 高可用 云企业网具有高可用及网络冗余性,全网任意 两点之间至少存在4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您的业务 正常运行,不会发生网络抖动及中断。

选项	场景	优势
全球加速	全球加速GA (Global Accelerator) 是一款覆盖 全球的网络加速服务,依托阿里云优质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,为您提供高可用和高性能的网络 加速服务。 适用于以下场景: • 游戏服务加速 • 企业应用加速	 高质量 全球加速拥有遍布全球的网络加速节点,依托 阿里云优质的BGP带宽和全球传输网络,大幅 提升全球公网服务访问体验,减少延迟、丢包 等网络传输问题。 高可用 全球加速支持跨地域流量管理和多终端节点流 量管理,屏蔽单地域和单线路故障,提高网络 的稳定性。 安全 全球加速与云原生的安全能力联动,保护互联 网服务免受攻击,加固对终端节点的安全访 jo. 易部署 全球加速配置简单,能够实现分钟级部署,且 全局资源统一监控运维,业务部署更敏捷。

2.3. New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。

选项	场景	优势
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。 适用于以下场景: • 线下门店或企业多分支互通 • 线下总部和门店上云	 私网连接,可靠安全 内网访问方式,提供更高的安全性,并提供数 据加密能力。 弹性部署,灵活交付 基于Internet接入方式下实现分支需要即开即 用,自动化组网,降低部署成本和资源投入。 全场景覆盖,一站式服务 覆盖企业分支、IDC、移动办公等不同接入场 景,帮企业实现一站式接入上云。

选项	场景	优势
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。 适用于以下场景: • 面向大中型企业的多地容灾高可用网络架构 • 面向大型企业的高弹性、高可用网络架构	 高速互通 依靠阿里云的网络虚拟化技术,可以将不同网 络环境连通,两侧直接进行高速内网通信,不 再需要绕行公网。 支持BGP路由
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。 适用于以下场景: • 本地IDC上云 • 移动客户端上云	 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。

对比

以上三款产品都支持将本地网络连接至专有网络,快速构建混合云。下表列举了这三款产品在质量、成本、 组网方式等方面的差异,便于您选择。

对比项	智能接入网关	高速通道	VPN网关
质量	中 (公网专线)	高(专线)	低 (公网)
组网能力	Full Mesh全网互联	点到点连接	点到点互联
业务应用	企业上云&分支互联	企业上云	企业上云
成本	Ф	高	低

3.解决方案

3.1. 互动课堂场景网络解决方案

对于互动课堂场景,如1对1、双师、小班课、互动大班课,实时音视频质量是影响课程效果的关键因素。互动课堂网络解决方案,依托阿里巴巴优质带宽和全球传输网络,通过SD-WAN技术,构建跨地域高质量实时 通信网络,有效改善网络丢包、减少网络抖动、降低整体网络时延,提升互动直播质量。

方案介绍

目前中国内地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,甚至分布在不同的国家。例如英语类在线教育场景,教师在北美地区,学员分布在国内的各个地区。如何保障跨地区、甚至跨国家的在线教育网络质量,是一个非常核心的技术问题。

本方案以北京、深圳两个固定校区为例,介绍如何通过一系列阿里云产品实现北京、深圳固定校区与跨境复 制转发服务器、跨地域互动后台系统以及跨地域AI系统互通,构建一个跨地域高质量传输网络,提升互动直 播质量。



业务规划

本场景各个区域之间不设置访问控制规则, 各区域路由之间互通。仅在各阿里云专有网络(VPC)区域内的 服务器上设置安全组配置访问规则实现业务流量互通。本场景各区域业务规划如下:

- 阿里云深圳VPC: 国内自建AI后台业务系统,进行流量监控,分析和评估。
- 阿里云北京VPC: 国内自建互动后台服务器区业务系统, 用于转码、录制、美颜等。
- 阿里云美西VPC: 跨境自建业务系统, 接入老师端业务流量, 部署云服务器实现流量复制转发。
- 深圳固定校区:通过智能接入网关设备硬件设备接入本地流量进入阿里云。
- 北京固定校区:通过智能接入网关设备硬件设备接入本地流量进入阿里云。
 北京固定校区网络架构示例图



网段规划

以下为本场景网段规划示例值,如您需要自行规划网段,请确保各个网段地址不冲突。

地域	网段规划
	业务网段: 172.16.0.0/12
	智能接入网关 WAN(端口5):192.168.100.1/30 , 网关192.168.100.2 智能接入网关 LAN(端口4):192.168.50.1/30
北京固定校区	三层交换机G11端口: 192.168.100.2/30
	三层交换机G12端口: 192.168.50.2/30
	出口路由器G1端口: 192.168.80.1/30
	三层交换机G2端口: 192.168.80.2/30
	业务网段: 172.32.0.0/12
	智能接入网关 WAN(端口5):192.168.110.1/30,网关192.168.110.2
	智能接入网关 LAN(端口4): 192.168.60.1/30

深圳固定校区 地域	网段规划
	三层交换机 G11端口:192.168.110.2/30 三层交换机 G12端口:192.168.60.2/30
	出口路由器G1端口: 192.168.90.1/30 三层交换机G2端口: 192.168.90.2/30
阿里云北京VPC(互动后台服务器 区)	10.0.0/16
阿里云深圳VPC(AI系统)	10.200.0.0/16
阿里云美西VPC (复制转发服务器)	10.10.0/16

准备工作

在按照本场景执行操作前,需要完成以下准备工作:

- 注册阿里云账号,并完成实名认证。您可以登录阿里云控制台,并前往实名认证页面查看是否已经完成实 名认证。
- 云企业网CEN跨境互通需要签订法务承诺书,用户已在线完成。详情请参见跨境云专线服务协议。
- 在本文场景中,您需要先在北京、深圳固定校园部署好您的网络,配置好组播服务器。您可以参考本场景 北京固定校区网络架构进行网络部署。

步骤一:搭建云环境

专有网络VPC是您自己独有的云上私有网络。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。您可以创建专有网络,然后在专有网络中使用阿里云资源,例如云服务器ECS、弹性公网IP、云数据库RDS和负载均衡SLB等。

本操作以阿里云美西VPC为例,展示如何创建VPC。请做同样的操作创建阿里云北京VPC和阿里云深圳VPC,为后面资源互访做准备。

- 1. 登录专有网络管理控制台。
- 2. 在顶部状态栏处,选择专有网络的地域。本操作中选择美国(硅谷)。
- 3. 在专有网络页面, 单击创建专有网络。
- 4. 在创建专有网络页面,根据以下信息配置专有网络和交换机,然后单击确定。

类型	配置项	说明
	名称	设置符合要求的名称。
专有网络VPC	IPv4网段	本场景阿里云美西VPC为 10.10.0.0/16。
	名称	设置符合要求的名称。
	可用区	选择目标可用区。
交换机		

类型	配置项	说明
	IPv4网段	10.10.0.0/24。

- 5. 在左侧导航栏, 单击**交换机**。选择刚刚创建的交换机实例ID。
- 6. 在**交换机详情**页面,在基础云资源区域,单击ECS实例后面的添加,创建云服务器ECS实例。详情请参见创建ECS实例。
- 7. 返回到交换机列表页面,在左侧导航栏,单击弹性公网IP,在弹性公网IP页面,单击申请弹性公网 IP。详情请参见申请EIP。
- 8. 在左侧导航栏,单击专有网络,选择刚刚创建的专有网络实例ID。
- 9. 在**专有网络详情**页面,在网络资源区域,单击SLB实例后面的数字,创建负载均衡SLB并挂载创建好的 云服务器ECS,并配置监听访问。请根据您的业务需求进行配置,详情请参见创建实例。

? 说明

本场景中仅阿里云美西VPC环境中选择创建负载均衡SLB、申请弹性公网IP,以便对外网用户提供服务。在阿里云北京VPC、阿里云深圳VPC中无需执行该操作。您可以根据业务需求选择是否执行该操作。

10. 在云服务器ECS上添加安全组规则,允许北京、深圳固定校区访问阿里云上VPC网络资源。详情请参见<mark>添</mark>加安全组规则。

添加安全组规则 ⑦ 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 V
* 嫣囗范围:	1/65535
优先级:	1
授权类型:	IPv4地址段访问 ▼
* 授权对象:	172.16.0.0/12
描述:	
	长鹿为2-256个字符,不能以http://或https://开头。
	确定 取消

下图是本操作中的安全组配置示例。将授权对象配置为北京固定校区的私网网段。

步骤二:购买智能接入网关

在阿里云控制台购买智能接入网关后, 阿里云会将智能接入网关设备寄送给您, 并创建一个智能接入网关实 例方便您管理网络设备。

以下操作是为北京固定校区购买智能接入网关示例,请做同样的操作为深圳固定校区购买智能接入网关。

1. 登录智能接入网关管理控制台。

- 2. 在左侧导航栏,选择智能接入网关。
- 3. 智能接入网关页面, 单击购买智能接入网关, 配置详情请参见购买SAG设备。

本场景中实例类型选择为SAG-1000,购买数量为1。

- 4. 配置智能接入网关后,单击**立即购买**,确认配置信息后,单击确认购买。
- 5. 在弹出的收货地址对话框,填写网关设备的收货地址,然后单击立即购买并完成支付。

您可以在智能接入网关实例页面查看是否下单成功。系统会在下单后两天内发货。如果超期,您可以提交工 单查看物流状态。

创建智能接入网关实例名称	マン 清縮入 Q					
实例ID/名称	网络类型 🕖	状态 🕜	线下路由同步方式 🕜	硬件SN号 🕜	硬件规格 😰	操作
sag Beij	Internet (130M) 👻	 已下単 	静态路由	-	SAG-1000	发货提醒 网络配置 :

步骤三: 激活绑定智能接入网关设备

收到网关设备后,请检查设备配件是否完整配件,详情请参见SAG-1000设备说明,并且请参考本操作激活设备。

- 1. 登录智能接入网关管理控制台。
- 2. 在智能接入网关页面,找到北京固定校区网关实例ID。
- 3. 单击操作列下的激活。
- 4. 单击北京固定校区网关实例ID, 在智能接入网关实例页面, 单击设备管理页签, 输入北京固定校区智 能接入网关设备序列号。

智能接入网关							
← sag-2maid dialowapayant 200							
基本信息	设备管理	网络配置	健康检查	高可用配置	运维监控		
您尚未添加主 硬件类型 SAG	E设备,请添加	加主设备					
设备 39 约 6 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	码						
添加设备							

5. 单击添加设备。

步骤四: 连接智能接入网关设备

绑定智能接入网关后,您还需要将智能接入网关接入到本地固定校区,为将本地固定校区接入到阿里云做准备。

请保持网关设备启动且4G信号正常,已经连接到阿里云。

- 1. 登录智能接入网关管理控制台。
- 2. 在智能接入网关页面,找到北京固定校区网关实例ID。
- 3. 在智能接入网关实例页面,单击设备管理页签。
- 4. 在左侧页签栏,单击端口角色分配。
- 5. 在端口角色分配,单击目标端口的操作列下的修改,修改端口角色。 本场景北京和深圳校区均使用WAN(端口5)、LAN(端口4)。
- 6. 通过网线,将智能接入网关的WAN (端口5)连接到三层交换机的G11端口上。
- 7. 通过网线,将智能接入网关的LAN (端口4)连接到三层交换机的G12端口上。



步骤五: 配置智能接入网关

您可以登录智能接入网关控制台对设备进行配置。

以下操作是对北京固定校区的智能接入网关实例进行配置,请做同样的操作完成深圳固定校区智能接入网关 实例配置。

- 1. 登录智能接入网关管理控制台。
- 2. 在智能接入网关页面,单击北京固定校区网关实例ID。
- 3. 在智能接入网关实例页面,单击设备管理页签。
- 4. 在左侧页签栏,单击LAN口管理。

- 5. 在LAN (端口4)区域,单击编辑。
- 6. 在LAN(端口4)配置页面,连接类型选择静态IP,输入规划好的北京固定校区IP地址信息,然后单击确定。

LAN (端口4) 配置		×
* 连接类型		
○ 动态IP		
● 静态IP		
* LAN地址		
192.168.50.1		
* 掩码地址		
255.255.255.252		
	确定	取消
	WOAE	-WIH

- 7. 在左侧页签栏, 单击WAN口管理。
- 8. 在WAN (端口5) 区域,单击编辑。
- 9. 在WAN(端口5)配置页面,连接类型选择静态IP,输入规划好的北京固定校区IP地址信息,然后单击确定。

WAN (j, 配置	×
* 连接类型	
○ 动态IP	
● 静态IP	
O PPPOE	
* 优先级	
1	
* IP地址	
192.168.100.1	
* 抟码	
255.255.255.252	
* 网关	
192.168.100.2	
确定	财肖

步骤六:配置路由

智能接入网关的WAN口和LAN口配置好后,需要配置线下路由同步方式及静态路由,为实现线下固定校区和 云上网络资源互通做准备。

本操作以北京固定校区为例,请做同样的操作完成深圳校区的配置。

- 1. 在智能接入网关页面,单击北京固定校区网关实例ID。
- 2. 在智能接入网关实例页面,单击网络配置页签。
- 3. 在左侧页签栏,单击线下路由同步方式。
- 4. 选择静态路由,然后单击添加静态路由,然后单击确定。

本操作北京固定校区输入172.16.0.0/12。

添加静态路由			
* 网段 🕝			
172.16.0.0	/	12	
	硝	淀	关闭

- 5. 保持在该智能接入网关实例页面,单击设备管理页签。
- 6. 在左侧导航栏,单击路由管理,然后单击添加静态路由。
- 7. 在添加静态路由页面,添加去往北京固定校区的静态路由。

添加静态路由	×
* 目标网段	
172.16.0.0/12	
* 下—跳IP	
192.168.50.2	
* 端口	
端囗4(LAN)	\sim
	确定取消

步骤七: 配置交换机和出口路由器

以下以北京固定校区为例,为智能接入网关设备对端的交换机和出口路由器添加路由配置,此处以某品牌交换机和路由器为例,由于不同厂商交换机和路由器配置不同,详情请参考厂商设备手册。

互联交换机的路由配置。

三层交换机: interface GigabitEthernet 0/11 no switchport ip address 192.168.100.2 255.255.252 智能接入网关对端交换机的端口IP interfaceGigabitEthernet 0/12 no switchport ip address 192.168.50.2 255.255.252 智能接入网关对端交换机的端口IP ip route 10.0.00 255.255.0.0 192.168.50.1 交换机去往北京VPC的路由 ip route 10.200.0.0 255.255.0.0 192.168.50.1 交换机去往溪圳VPC的路由 ip route 10.10.0.0 255.255.0.0 192.168.50.1 交换机去往美西VPC的路由 ip route 0.0.0.0 0.0.0.0 192.168.80.1 交换机去往公网路由

出口路由器的路由配置。

```
出口路由器:
```

ip route 192.168.100.1 255.255.255.252 192.168.80.2 出口路由器去往智能接入网关的路由

步骤八: 绑定智能接入网关到云连接网

要将智能接入网关实例所连接的线下固定校区接入阿里云,您必须先创建一个云连接网,然后将智能接入网 关实例添加到云连接网内,为实现线下固定校区和云上网络资源互通做准备。

- 1. 登录智能接入网关管理控制台。
- 2. 在左侧导航栏,单击云连接网。
- 3. 在云连接网,单击创建云连接网。
- 4. 在创建云连接网页面, 配置云连接网名称, 然后单击确定。

云连接网名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)或短划线

(-) 。				
智能接入网头 / 云连接网				使用限制 (2 帮助文档
云连接网				
创建云连接网 С				実例ID > 済縮入 Q
实例ID/名称	绑定云企业网	绑定智能接入网关	私网网般	操作
con-		0/0		绑定云企业网 删除

5. 在云连接网页面,单击刚刚创建的云连接网实例ID。

- 6. 在云连接网实例页面, 单击绑定智能接入网关。
- 7. 在绑定智能接入网关页面,选择同账号页签。
- 8. 选择北京固定校区智能接入网关实例,单击确定。
- 9. 请重复上述步骤,将深圳固定校区智能接入网关实例绑定同一个云连接网。

绑定智能接入网关	×
同账号 跨账号	
智能接入网关	
-/sag-	~

您可以在云连接网实例页面查看已经绑定的智能接入网关实例。

已绑定智能接入网关基本信息						绑定智能接入网关
实例ID/名称	带宽峰值	状态	私网网段	到期时间	账号UID	操作
sag- Shenzher , ⇒ ∠		• 可用	10.00		本账号	解掷
sag- Beijing	100	• 可用	1		本账号	解謝

步骤九:添加网络实例到云企业网

在智能接入网关绑定到云连接网后,您还需要创建一个云企业网,将云连接网和专有网络VPC绑定到该云企业网内,为本地固定校区和阿里云上VPC网络资源互通做准备。

- 1. 登录云企业网控制台。
- 2. 在云企业网实例页面,单击创建云企业网实例。
- 3. 在创建云企业网实例页面,将之前步骤中创建的云连接网直接加载到该云企业网实例中。

⑦ 说明 创建云企业网实例详情请参见创建云企业网实例。

创建云台	全业网实例	? ×
云企业		
	• 名称 💿	
	cen-c 10/128	
	描述 💿	
	0/256	
加载网	络实例	
同》	账号	
(i)) 注: 已加载到云企业网的实例不允许重复加载	
	• 实例类型 💿	
	云连接网 (CCN) く	
	• 地域 💿	
	中国 ~	
	 网络实例 ② 	
	ccn-	

- 4. 单击已创建的云企业网实例ID链接,然后单击加载网络实例。
- 5. 在加载网络实例页面,完成以下配置:选择专有网络,选择之前创建的云企业网实例,然后单击确 定。
 - 实例类型:选择专有网络(VPC)。
 - 地域:选择云上应用的VPC地域。
 - 网络实例:选择要互通的VPC。
- 6. 重复上述步骤将阿里云深圳VPC和阿里云美西VPC添加到该云企业网内。
- 7. 在**云企业网**页面,单击**网络实例管理**页签,查看阿里云北京VPC、阿里云美西VPC,阿里云深圳VPC和 云连接网是否已经加入云企业网。

网络实例管理带宽包	19管理 跨地域互通带宽管理	路由信息 云服务	PrivateZone 路由策略			
加載网络实例 刷新						
实例ID/名称	所屬地域	实例类型	所屬账号	加戰时间	状态	操作
ccn-	F	云连接网 (CCN)	100070-100050000	2019-08-15 13:50:00	● 己加載	卸數
vpc-	1911	专有网络 (VPC)	1000	2019-08-15 14:32:00	● 已加載	卸戰
vpc-sal particular	1001	专有网络 (VPC)	1000	2019-08-15 14:48:00	● 已加載	卸戰
vpc-	1911	专有网络 (VPC)	10100-000-0	2019-10-09 15:28:00	●巳加载	卸戰

步骤十:购买带宽包

要实现跨地域网络实例互通,您必须购买带宽包并设置跨地域互通带宽。同地域互通不需要购买带宽包。带 宽包购买说明请参见使用带宽包。

本场景中需要同时购买跨境和非跨境带宽包,以实现云上网络资源互通。

- 1. 登录智能接入网关管理控制台。
- 2. 在左侧导航栏,选择快捷连接 > 云企业网,选择之前创建的云企业网实例ID。
- 3. 在云企业网实例页面,单击带宽包管理页签,然后单击购买带宽包(预付费)。
- 4. 在云企业网(预付费)页面,在跨境页签下配置带宽包信息,然后单击立即购买。
 - **云企业网**:选择VPC和云连接网所加入的云企业网。
 - 区域-A和区域-B:选择本次购买带宽包需要互通的VPC所在的区域。
 本操作选择中国内地和北美。
 - **带宽值**:根据业务需要,选择跨区域互通的带宽。
 - 带宽包名称: 输入该带宽包的名称。

	云企业网	zxtest ▼ 云企业网为必选项。 如果您还没有云企业网,请先 创建云企业网实例。
互通区	区域-A	中国内地
域	区域-B	北美 亚太 欧洲 澳洲
		 选择要互通的区域,购买带宽包后设置两区域间跨地域互通的带宽,可实现两区域内的跨地域互通。(点击查看区域与地域对应关系) 马来西亚,印度,印尼等地分别跨地域互通最大带宽限定50Mbps以内,如需以上地域和其他地域互通,请谨慎选择带宽包带宽值。 互通区域订购后不能修改,请谨慎选择。 云企业网跨地域带宽默认为1kbps,仅供测试连通性。为保证您业务正常运行,请购买完带宽包后设置互通地域带宽。
基	计费方式	按带宽
本配	带宽值	II 2500Mbps 5000Mbps 10000Mbps 2 Mbps \$
直	带宽包名称	
购买量	购买时长	11/2 □自动续费 💩

- 5. 在云企业网实例页面,单击**跨地域互通带宽管理**页签,然后单击**设置跨地域带宽**。
- 6. 设置跨境互通带宽,每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽值。
 - 带宽包:选择已绑定至云企业网实例的带宽包,此处选择中国内地与北美。
 - **互通地域**:选择需要互通的地域,选择中国内地云连接网和美国(硅谷),请以同样的方式创建华
 北2(北京)和美国(硅谷)、华南1(深圳)和美国(硅谷)的互通带宽包。
 - **带宽**:根据业务需要,输入带宽值。

⑦ 说明 每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽值。

- 7. 购买中国内地互通带宽包。在云企业网(预付费)页面,单击**非跨境**页签,然后完成以下配置。
 - **云企业网**:选择VPC和云连接网所加入的云企业网。
 - 区域-A和区域-B: 选择本次购买带宽包需要互通的VPC所在的区域。

此处选择中国内地和中国内地。

- 带宽值:根据业务需要,选择跨区域互通的带宽。
- 带宽包名称: 输入该带宽包的名称。
- 8. 在云企业网实例页面,单击跨地域互通带宽管理页签,然后单击设置跨地域带宽。
- 根据以下信息设置跨地域互通带宽,每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽 值。然后单击确定。
 - 带宽包:选择已绑定至云企业网实例的带宽包,此处选择中国内地与中国内地。
 - **互通地域**:选择需要互通的地域,选择中国内地云连接网和华北2(北京)。请以同样的方式创建华北2(北京)和华南1(深圳)、中国内地云连接网和华南1(深圳)的互通带宽包。
 - **带宽**:根据业务需要,输入带宽值。

步骤十一:访问测试

完成上述配置后,您可以通过在线下固定校区的客户端访问已连接的VPC中部署的云资源验证配置是否生效。

3.2. 企业级云上网络解决方案

3.2.1. 企业级云上网络解决方案概述

随着越来越多的企业用户上云,如何构建一个符合企业管理要求的可管可控的云网络环境,成为企业上云过 程中必须要解决的问题之一。企业级云上组网方案利用专有网络VPC、负载均衡SLB等网络产品,帮助企业用 户构建一个支持多业务部署、安全、可靠的云上网络。

组网方案	方案介绍	使用场景	安全防护
单VPC单账号	使用一个VPC,通过交换机划分 不同功能区	 账号管理要求低(团队规模小) 安全要求低(基本安全防护要求) 可用性要求中(同城双活) 	网络ACL安全组
单VPC多账号	 使用一个VPC,通过交换机划 分不同功能区 使用共享VPC创建多个业务账 号 	 账号管理要求高(团队规模大 且业务多) 安全要求低(基本安全防护要 求) 可用性要求中(同城双活) 	网络ACL安全组

组网方案	方案介绍	使用场景	安全防护
多VPC多账号	 使用多个VPC划分不同功能区 和安全域 使用共享VPC创建多个业务账 号 	 账号管理要求高(团队规模大 且业务多) 安全要求中(需要划分安全 域) 可用性要求中(同城双活) 	 网络ACL 安全组 路由策略 云防火墙
多地域负载/容灾	使用多个地域实现异地容灾和负 载分担,并通过云企业网实现多 地域互通	 账号管理要求高(团队规模大 且业务多) 安全要求中(需要划分安全 域) 可用性要求高(同城双活和异 地容灾) 	 网络ACL 安全组 路由策略 云防火墙
多环境隔离	 使用多个云企业网实现多环境 隔离 利用中转VPC实现不同环境的 数据中转 	 账号管理要求高(团队规模大 且业务多) 安全要求高(不同环境间严格 隔离) 可用性要求中(同城双活) 	 网络ACL 安全组 路由策略 云防火墙 第三方应用/数据 安全能力

3.3. 全球互联

3.3.1. 阿里云混合云网络互联

3.3.1.1. 阿里云混合云网络互联方案概述

阿里云混合云网络互联方案主要介绍了阿里云混合云网络能力,以及如何通过阿里云混合云网络能力帮助企 业构建云上云下的混合云网络,并根据企业用户的业务诉求,从建设成本、网络时延、可靠性和建设周期等 方面,协助您快速决策出一种适合企业上云链路的方案,加速企业上云。

产品组成

阿里云混合云网络能力主要通过以下几个产品实现:

• 专有网络VPC (Virtual Private Cloud)

专有网络是阿里云云上一个隔离的网络环境,可以自定义IP地址范围、网段、路由表和网关等,也可以通 过物理专线、VPN等连接方式实现云上VPC与传统数据中心IDC(Internet Data Center)的互联,构建混 合云业务。更多信息,请参见什么是专有网络。

• 云企业网CEN (Cloud Enterprise Network)

云企业网提供一种能够快速构建混合云和分布式业务系统的全球网络的方法,可帮助您打造一张具有企业 级规模和通信能力的云上网络。更多信息,请参见什么是云企业网。

• 智能接入网关SAG (Smart Access Gateway)

智能接入网关是阿里云的SD-WAN终端,具有多种软硬件的产品形态,可以适应大中小型企业分支和移动 办公场景的需要,快速就近地帮您接入云连接网。部署维护简单方便,可支持集中配置和监控,大大降低 维护难度。更多信息,请参见什么是智能接入网关。

• 云连接网CCN (CloudConnect Network)

云连接网是阿里云SD-WAN终端的接入网络,由分布在各地的接入点构成。云连接网依托阿里云的优质网络和底层网络优化技术,为您提供高质量的广域网接入网络服务。更多信息,请参见云连接网介绍。

• 高速通道EC (Express Connect)

高速通道提供了一种快速安全连接阿里云与本地IDC的方法。您可以通过租用运营商的一条物理专线将本地IDC连接到阿里云接入点,建立物理专线连接。此连接绕过公网,更加安全可靠、速度更快、延迟更低。更多信息,请参见什么是高速通道。

• 边界路由器VBR (Virtual border router)

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,阿里云将您的物理专线接入端口隔离起来,并抽象成边界路由器。边界路由器是CPE(Customerpremisesequipment)设备和VPC之间的一个路由器,作为数据从VPC到本地IDC的转发桥梁。更多信息,请参见什么是边界路由器。

• 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VPC安全可靠的连接。VPN网关提供IPsec-VPN连接和SSL-VPN连接。更多信息,请 参见什么是VPN网关。

混合云网络互联解决方案整体架构



应用场景

混合云网络互联主要分为云上云下互联、跨地域互联及多云互联场景:

- 云上云下互联:企业总部或分支可通过物理专线、SD-WAN、VPN三种不同的上云链路连接至阿里云,实现快速、安全地访问阿里云上服务。针对上云的主备链路方案又可分为双物理专线、物理专线联合SD-WAN、物理专线联合VPN三种场景化方案。
- 跨地域互联:通过阿里云云企业网,企业业务可快速出海,实现海外机构与国内总部互联的网络。

多云互联:随着越来越多的企业选择多云架构的战略方向,快速构建多云互联也成为企业上云的核心诉求。通过阿里云SD-WAN产品,可为企业快速构建多云互联网络。

解决方案特点

在上述应用场景中,您可以通过不同的技术能力构建混合云网络,不同的部署方案有不同的特点,下表从网 络链路的质量、成本、扩展性、建设周期四个方面为您介绍阿里云混合云解决方案并为您介绍各个方案典型 的应用场景。

		网络链	网络链路特点		方案应用场景及说明		
方案分类	解决方案	质量	成本	扩展 性	建设 周期	典型应用场景	方案推荐说明
	通过VPN网关 (IPsec-VPN)上云 方案	低	低	好	天	本类方案话用	 用和定网宽求 心DC 业 学校 心学校 心学校 化 化 化 化 化 化 化 化 化 化 化 化 化 化 化 化 化 化 化
	 SAG双机直挂静态路由上云方案 SAG双机旁挂静态路由上云方案 SAG双机旁挂动态路由上云方案(推荐) 	Ф	Ф	好	Ŧ	不实力案运用 于云下资源有定 期交互,对网 络弹性、带宽 容量有高要求 的场景。	
云上云下 互联	 IDC通过静态路由 主备专线链路上 云方案 IDC通过BGP主备 专线链路上云方 案 	高	高	差	月	本类方案适用 于云上资源互 频繁,且对网 络的时延、可 靠性和强要求的 场景。	
	lPsec-VPN联合物理 专线实现主备链路 上云方案	中	中	好	月	本类方案适用 于云下到云上 的入向流量大	
	SAG联合物理专线实 现主备链路上云方 案(推荐)	言	ф	好	月	于山间流重, 云上和云下资 源交互较为频 繁,对网络的 弹性、可靠性 有强要求的场 景。	
跨地域互 联	跨地域IDC上云互通 方案	高	高	差	月	本方案适用于企业 IDC利用阿里云上 IDC互联的场景。	业快速出海、企业本地 异地资源 <i>,</i> 实现跨地域
多云互联	SAG vCPE实现多云 互通	中	中	好	天	本方案适用于企业 务提供商中,需要	业分支部署在不同云服 要云间互联的场景。

3.3.1.2. 云上云下互通

3.3.1.2.1. 通过VPN网关(IPsec-VPN)上云方案

本文为您介绍如何使用IPsec-VPN建立专有网络VPC(Virtual Private Cloud)到企业的VPN连接,实现云下 企业网络与云上VPC的互通。

方案概述

在企业上云过程中,部分企业会将数据保存在阿里云,其企业总部或分支机构有时会需要从阿里云读取数据,在企业从阿里云读取数据的过程中,会需要一条高弹性和大带宽的上云链路。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可快速为企业数据中心、企业办公网络或Internet终端建立一条安全、高效的上云链路,并可提供多种带宽规格。

场景说明

本文以下图场景为例,为您介绍VPN网关(IPsec-VPN)上云方案。某企业在阿里云华东1(杭州)地域创建 了VPC,其中部署有云服务器ECS(Elastic Compute Service)和对象存储服务OSS(Object Storage Service),企业总部会定期将数据备份到阿里云OSS中,其位于杭州地域的企业分支有时需要从OSS中读取 数据或因业务需求访问ECS。现企业需要为其企业分支部署上云链路,以实现云下企业分支和云上VPC的互 联互通。



准备工作

开始前,请确保您已经满足以下条件:

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经在阿里云华东1(杭州)地域部署了VPC,并部署有ECS服务器和OSS服务。具体操作,请参见创建 和管理专有网络。
- 您已经检查企业分支的网关设备,确保网关设备支持标准的IKEv1和IKEv2协议,以便和阿里云VPN网关建 立连接。例如华为、华三、山石、深信服、Cisco ASA、Juniper、SonicWall、Nokia、IBM和Ixia等厂商的 设备。

本文示例中,企业分支的网关设备,即图中标识的CPE(Customer-premisesequipment)设备,将作为 VPN连接中的用户网关。

- 企业分支的网关设备已经配置了静态公网ⅠP。
- 本文示例中, 网段规划如下表所示。您可以自行规划网段, 请确保您的网段之间没有重叠。

规划目标	网段规划	IP地址
VPC	192.168.0.0/16	服务器地址: 192.168.20.161
企业分支	172.16.0.0/12	客户端地址: 172.16.1.188
企业网关设备	不涉及	公网IP地址: 211.XX.XX.68

配置步骤



步骤一: 创建VPN网关

1.

- 2. 在左侧导航栏,选择VPN > VPN网关。
- 3. 在VPN网关页面,单击创建VPN网关。
- 4. 在购买页面,根据以下信息配置VPN网关,然后单击**立即购买**并完成支付。
 - 实例名称: 输入VPN网关的实例名称。
 - 地域和可用区:选择VPN网关的地域。 请确保已创建VPC的地域和VPN网关的地域相同。本示例选择华东1(杭州)。
 - 网关类型:选择要创建的VPN网关类型。本示例选择普通型。
 - VPC: 选择要连接的VPC。本示例选择华东1(杭州)地域已创建的VPC实例。
 - 指定交换机:是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择否。
 如果您选择了是,您还需要指定具体的虚拟交换机。
 - 带宽规格:选择VPN网关的带宽规格,带宽规格是VPN网关所具备的公网带宽。
 - **IPsec-VPN**:选择开启或关闭IPsec-VPN功能,IPsec-VPN功能可以将本地数据中心与VPC或不同的 VPC之间进行连接。本示例选择**开启**。
 - SSL-VPN: 选择开启或关闭SSL-VPN功能, SSL-VPN功能允许您从任何位置的单台计算机连接到
 VPC。本示例选择关闭。
 - SSL连接数: 选择您需要同时连接的客户端最大规格。

⑦ 说明 本选项只有在选择开启了SSL-VPN功能后才可配置。

- 计费周期:选择购买时长。
- 5. 返回VPN网关页面,查看创建的VPN网关。

刚创建好的VPN网关的状态是**准备中**,约两分钟左右会变成**正常**状态。**正常**状态表明VPN网关完成了初 始化,可以正常使用了。 ⑦ 说明 VPN网关的创建一般需要1~5分钟。

步骤二: 创建用户网关

- 1. 在左侧导航栏,选择VPN > 用户网关。
- 2. 在用户网关页面, 单击创建用户网关。
- 3. 在创建用户网关面板,根据以下信息配置用户网关,然后单击确定。
 - 名称: 输入用户网关的名称。
 - IP地址: 输入VPC要连接的企业分支的网关设备的公网IP。本示例输入211.XX.XX.68。
 - 自治系统号: 输入VPC要连接的企业分支的网关设备的自治系统号。本示例不输入。
 - **描述**: 输入用户网关的描述信息。

更多信息,请参见<mark>创建用户网关</mark>。

步骤三: 创建IPsec连接

- 1. 在左侧导航栏,选择VPN > IPsec连接。
- 2. 在IPsec连接页面,单击创建IPsec连接。
- 3. 在创建IPsec连接页面,根据以下信息配置IPsec连接,然后单击确定。
 - 名称: 输入IPsec连接的名称。
 - VPN网关:选择已创建的VPN网关。
 - **用户网关**:选择已创建的用户网关。
 - 路由模式:选择路由模式。本示例选择目的路由模式。
 - **立即生效**:选择是否立即生效。本示例选择**否**。
 - 是: 配置完成后立即进行协商。
 - 否: 当有流量进入时进行协商。
 - 预共享密钥:输入共享密钥,该值必须与企业分支网关设备的预共享密钥一致。本示例使用默认生成的随机值。

其他选项使用默认配置。

更多信息,请参见创建IPsec连接。

步骤四: 配置VPN网关路由

- 1. IPsec连接创建成功后,在创建成功对话框,单击确定,去往VPN网关中进行路由发布。
- 2. 在左侧导航栏,选择VPN > VPN网关。
- 3. 在VPN网关页面,找到目标VPN网关,单击目标实例ID。
- 4. 在目的路由表页签,单击添加路由条目。
- 5. 在**添加路由条目**面板,根据以下信息配置目的路由,然后单击确定。
 - 目标网段: 输入企业分支的私网网段。本示例输入172.16.0.0/12。
 - 下一跳类型:选择IPsec连接。
 - 下一跳:选择IPsec连接实例。
 - 发布到VPC:选择是否将新添加的路由发布到VPC路由表。本示例选择是。

○ 权重:选择权重值。本示例选择100。

配置完成后,您在VPC控制台可以查看到去往企业分支的路由172.16.0.0/12,其下一跳指向VPN网关。

步骤五: 在网关设备中加载VPN配置

完成以下操作,在企业分支的网关设备中加载VPN配置。

- 1. 在左侧导航栏,选择VPN > IPsec连接。
- 2. 在IPsec连接页面,找到目标IPsec连接,然后选择操作列下的。 > 下载对端配置。
- 3. 根据网关设备的配置要求,将下载的配置添加到网关设备中。具体操作,请参见本地网关配置。

下载配置中的RemotSubnet和LocalSubnet与创建IPsec连接时的本端网段和对端网段是相反的。因为从 阿里云VPN网关的角度看,对端是用户IDC的网段,本端是VPC网段;而从本地网关设备的角度 看,LocalSubnet就是指本地IDC的网段,RemotSubnet则是指阿里云VPC的网段。

步骤六:连通性测试

完成以下操作,测试连通性。

⑦ 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许企业分支访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

- 1. 在企业分支机构中, 打开客户端的命令行窗口。
- 2. 执行 ping 命令, ping 云上VPC 192.168.0.0/16网段下的ECS实例IP地址, 如果能接受到回复报 文, 表示连接成功。

经验证,企业分支可以和云上VPC互通。

[root@iZb; Z ~]# ping 192.168.20.161					
PING 192.168.20.161 (192.168.20.161) 56(84) bytes of data.					
64 bytes from 192.168.20.161: icmp_seq=1 ttl=64 time=2.00 ms					
64 bytes from 192.168.20.161: icmp_seq=2 ttl=64 time=1.88 ms					
64 bytes from 192.168.20.161: icmp_seq=3 ttl=64 time=1.85 ms					
64 bytes from 192.168.20.161: icmp_seq=4 ttl=64 time=1.84 ms					
^Z					
[1]+ Stopped ping 192.168.20.161					
[root@i2 Z ~]# [

3.3.1.2.2. SAG双机直挂静态路由上云方案

本文为您介绍如何通过智能接入网关SAG(Smart Access Gateway)双机直挂模式并使用静态路由将企业接入阿里云,实现云下企业网络与云上VPC(Virtual Private Cloud)的互通。

方案概述

在企业上云过程中,部分大型企业会将数据保存在阿里云,其企业总部及分支机构有时会需要从阿里云读取数据,在企业从阿里云读取数据的过程中,会需要一条高弹性和大带宽的上云链路。智能接入网关是阿里云的SD-WAN终端,具有多种软硬件的产品形态,可将企业快速就近地接入阿里云,部署简单,维护方便,扩展性好。
本文以下图场景为例,为您介绍智能接入网关双机直挂静态路由上云方案。某企业总部在阿里云华北2(北京)地域创建了VPC,其中部署有云服务器ECS(Elastic Compute Service)和对象存储服务OSS(Object Storage Service),企业总部会定期将数据备份到阿里云OSS中,企业有时会需要从阿里云OSS中读取数据并和云上ECS进行交互访问。企业现在需要部署上云链路,以实现云下本地机构和云上VPC的互联互通。其中:

- 智能接入网关采用SAG-1000型号设备并采用直挂模式将企业本地机构接入阿里云。
- 智能接入网关部署为双机模式,两台智能接入网关设备可以互为备份链路,为企业提供高可用的上云链路。
- 企业^{本地机构} 登 数据库 智能接入网关1 CCN 安有网络VPC ECS 智能接入网关2 服务器
- 企业本地机构和智能接入网关之间采用静态路由方式。

准备工作

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经在阿里云华北2(北京)地域创建了VPC。具体操作,请参见创建和管理专有网络。
- 本文示例中SAG-1000运行2.0软件版本。关于设备软件版本支持的功能说明,请参见智能接入网关硬件功能发布记录。
- 以下为本文网段规划示例值以及智能接入网关接入企业本地机构中的网络架构示例图。如您需要自行规划 网段,请确保各个网段地址不冲突。



规划目标	网段及IP地址
VPC	10.0.0/16
山口政由翌	端口G1: 192.168.100.2/30
шцщща	端口G2: 192.168.200.2/30
智能接入网关1	◎ WAN端口5: 192.168.100.1/30, 下一跳: 192.168.100.2 ◎ LAN端口4: 192.168.50.1/24, 启用HA, 且虚IP地址为192.168.50.254
智能接入网关2	◎ WAN端口5: 192.168.200.1/30,下一跳: 192.168.200.2 ◎ LAN端口4: 192.168.50.3/24,启用HA,且虚IP地址为192.168.50.254
三层交换机	 ◎ 端口G11: 划分到VLAN 10下 ◎ 端口G12: 划分到VLAN 10下 ◎ VLAN 10: 192.168.50.2/24
本地机构	172.16.0.0/12

配置步骤



步骤一:购买智能接入网关

在智能接入网关控制台购买智能接入网关设备后, 阿里云会将智能接入网关设备寄送给您, 并创建一个智能 接入网关实例方便您管理设备。

⑦ 说明 如果您要使用智能接入网关的区域非中国内地时,您需要通过第三方公司购买硬件。具体操作,请参见购买SAG设备。

1. 登录智能接入网关管理控制台。

- 2. 在智能接入网关页面,选择购买智能接入网关 > 创建智能接入网关(硬件版)。
- 3. 在购买页面,根据以下信息配置智能接入网关,然后单击**立即购买**。
 - 区域:智能接入网关使用区域。本示例选择中国内地。
 - 实例类型:选择智能接入网关设备规格。本示例选择SAG-1000。
 - 已有SAG硬件:选择是否已有智能接入网关硬件设备。本示例选择否。
 - 版本:智能接入网关设备版本。本示例使用默认值标准版。
 - 购买数量:智能接入网关设备购买数量。本示例选择2。
 - 区域:智能接入网关使用的带宽区域。该区域类型和智能接入网关设备使用区域保持一致,且无法修改。
 - **实例名称**:智能接入网关实例名称。
 名称长度为2~128个字符,以大小写字母或中文开头,可包含数字、半角句号(.)、短划线(-)和下划线(_)。
 - 带宽峰值:选择通信网络的带宽峰值。本示例选择30 Mbps。
 - 购买时长:选择购买时长。
- 4. 确认订单信息并勾选服务协议,然后单击确认购买。
- 5. 在弹出的收货地址对话框,填写网关设备的收货地址,然后单击**立即购买**。
- 6. 在弹出的支付页面,选择支付方式,然后完成支付。

您可以在智能接入网关实例页面查看是否下单成功。系统会在下单后两个工作日内发货。如果超期,您可以提交工单查看物流状态。

智能接入网关											
随时随地安全上云,智能 合作伙伴可提供一站式。	能接入网关APP免费试用活动中。 点击 上门安装、售后服务。 服务详情 >>	查看									
购买智能接入网关 🗸	実例名称 > 清輸入	Q									\$ C
宾例ID/名称	绑定云连接网ID/名称	接入点	带宽峰值	状态 😰	SN号 🕑	規格 🙆	购买时间	到期时间	资源组	操作	
sag- g8s68 /53 testco	绑定网络		50M	🖻 待发货		SAG-1000	2020年8月19日 16:05:15	2020年9月20日 00:00:00	default resource group	发货提醒 网络配置	È) I

7. 收到网关设备后,请检查设备配件是否完整。关于设备配件信息,请参见SAG-1000设备说明。

步骤二: 激活智能接入网关

收到设备后,您还需要按照以下操作,激活绑定设备。

- 1. 登录智能接入网关管理控制台。
- 2. 在顶部菜单栏,选择目标区域。
- 在智能接入网关页面,找到目标实例。将设备与智能接入网关实例进行绑定。具体操作,请参见添加设备。

您需要将两台设备绑定到一个实例中,最先绑定的设备为主设备,另一个台设备为备设备。本示例中智能接入网关1为主设备,智能接入网关2为备设备。

4. 绑定后,返回到智能接入网关页面。选择目标实例操作列下的:>激活。

5. 在激活对话框,单击确定。

步骤三: 连接智能接入网关

激活、绑定智能接入网关设备后,您还需要将智能接入网关连接到您的本地机构中。

在您执行以下操作前,请保持设备启动且4G信号正常,已经连接到阿里云。本操作以智能接入网关1为例进行配置,请根据网络规划和以下步骤配置智能接入网关2。

- 1. 在智能接入网关页面,找到目标网关实例ID。
- 2. 在智能接入网关实例详情页面,单击设备管理页签,选择目标设备。
- 3. 在页签左侧区域,单击端口角色分配。
- 4. 在端口角色分配页面,单击目标端口操作列下的修改,修改端口角色,然后单击确定。
 本示例中智能接入网关1使用WAN(端口5)和LAN(端口4)。具体操作,请参见分配端口角色。

⑦ 说明 仅SAG-1000型号设备的2.0版本支持端口角色分配功能。

- 5. 通过网线,将智能接入网关1的WAN (端口5)与出口路由器的G1端口连接。
- 6. 通过网线,将智能接入网关1的LAN (端口4) 与三层交换机的G11端口连接。

步骤四:配置端口

连接好网关设备后,您可以在智能接入网关管理控制台分别对智能接入网关1和智能接入网关2进行端口配置。

- 1. 登录智能接入网关管理控制台。
- 2. 在智能接入网关页面,单击目标实例ID。
- 3. 在智能接入网关实例详情页面,单击设备管理页签,然后选择目标设备。
- 4. 在页签左侧区域,单击LAN口管理。
- 5. 在LAN (端口4) 区域, 单击编辑。
- 6. 在LAN (端口4) 配置对话框,根据以下信息配置端口,然后单击确定。

智能接入网关1:

- 连接类型:选择静态IP。
- 接口地址: LAN端口IP地址。本示例输入192.168.50.1。
- 掩码地址: LAN端口IP地址掩码。本示例输入255.255.255.0。

智能接入网关2:

- 连接类型:选择静态IP。
- 接口地址: LAN端口IP地址。本示例输入192.168.50.3。
- 掩码地址: LAN端口IP地址掩码。本示例输入255.255.255.0。
- 7. 在页签左侧区域,单击WAN口管理。
- 8. 在WAN (端口5) 区域,单击编辑。
- 在WAN(端口5)配置对话框,根据以下信息配置端口,然后单击确定。 智能接入网关1:
 - 连接类型:选择静态IP。

- IP地址: WAN端口IP地址。本示例输入192.168.100.1。
- 掩码: WAN端口IP地址掩码。本示例输入255.255.255.252。
- 网关: 网关IP地址。本示例输入192.168.100.2。

智能接入网关2:

- 连接类型:选择静态ⅠP。
- IP地址: WAN端口IP地址。本示例输入192.168.200.1。
- 掩码: WAN端口IP地址掩码。本示例输入255.255.255.252。
- 网关: 网关IP地址。本示例输入192.168.200.2。

⑦ 说明 配置网关IP地址后,智能接入网关设备自动会生成一条默认路由。

步骤五:配置路由

智能接入网关设备的端口配置完成后,您需要配置线下路由同步方式将本地机构的路由同步到云上,同时在 设备上配置静态路由为云上流量去往本地机构指定出口。

- 1. 在智能接入网关页面,单击目标网关实例ID。
- 2. 在智能接入网关实例详情页面,单击网络配置页签。
- 3. 在页签左侧区域,单击线下路由同步方式。
- 4. 选择静态路由,然后单击添加静态路由并配置静态路由信息,然后单击确定。

静态路由添加为本地机构要和云上互通的网段: 172.16.0.0/12。

添加静态路由			
* 网段 👔			
172.16.0.0	/	12	
	确	定	关闭

- 5. 保持在该智能接入网关实例页面,单击设备管理页签,并选择目标设备。 请根据步骤和步骤分别为智能接入网关1和智能接入网关2添加静态路由。
- 6. 在页签左侧区域,单击路由管理,然后单击添加静态路由。
- 7. 在添加静态路由对话框,添加去往本地机构的静态路由。

参数	说明
目标网段	智能接入网关1: 172.16.0.0/12 智能接入网关2: 172.16.0.0/12
下一跳IP	智能接入网关1: 192.168.50.2 智能接入网关2: 192.168.50.2
端口	两台智能接入网关均选择 端口4(LAN)

参数		说明
添加静态路由	×	
*目标网段		
172.1		
* 下—BK		
192.10 x		
"」」而口		

步骤六:配置HA

端口)

请根据以下操作分别为智能接入网关1和智能接入网关2配置HA功能,使两台智能接入网关设备互为主备设备,为企业上云提供高可用链路。

 \sim

取消

1. 在智能接入网关实例详情页面,单击设备管理页签,并选择目标设备。

确定

- 2. 在设备管理页签左侧区域,单击HA管理。
- 3. 在HA信息区域, 单击 ∠ 图标。
- 4. 在HA配置对话框,根据以下信息进行配置。

配置	说明
HA模式	两台智能接入网关设备均选择 静态 。
端口	两台智能接入网关设备均选择LAN4(LAN)。
虛IP	智能接入网关的虚拟IP地址。本示例中两台智能接入网关设备均使用 192.168.50.254。

更多信息,请参见配置设备级高可用。

5. 单击**保存**。

步骤七:本地机构配置

您需要为智能接入网关设备对端的交换机添加端口和路由配置。此处以某品牌交换机为例,由于不同厂商交换机配置不同,详情请参见厂商设备手册。

interface GigabitEthernet 0/12	#将连接智能接入网关1 LAN口的端口划分到VLAN 10下
switchport access vlan 10	
interface GigabitEthernet 0/14	#将连接智能接入网关2 LAN口的端口划分到VLAN 10下
switchport access vlan 10	
interface vlan 10	
ip address 192.168.50.2 255.255.255.0	#客户端网关地址
ip route 0.0.0.0 0.0.0.0 192.168.50.254	#默认路由

步骤八:配置网络连接

在配置好网关设备后,您需要配置网络连接,将本地机构接入阿里云。

- 1. 创建云连接网。
 - i. 登录智能接入网关管理控制台。
 - ii. 在左侧导航栏, 单击云连接网。
 - iii. 在云连接网页面, 单击创建云连接网。
 - iv. 在创建云连接网面板, 配置云连接网名称, 然后单击确定。

云连接网名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)和短划线 (-)。

智能接入网关 / 云连接网				使用限制 🔮 帮助文档
云连接网				
创建云连接网 C				実例D > 溶組入 Q
实例ID/名称	绑定云企业网	鄉定智能接入网关	私网网段	操作
ccn-		0/0		御垣云企业网 删除

2. 配置网络连接。

- i. 在左侧导航栏, 单击智能接入网关。
- ii. 在智能接入网关页面,单击目标实例操作列的网络配置。
- iii. 单击绑定网络详情页签, 然后单击添加网络。
- iv. 在**添加网络**对话框,选择**云连接网**类型并选择已创建的云连接网实例,然后单击确定。

3. 绑定云企业网。

i. 创建云企业网实例。具体操作, 请参见创建云企业网实例。

在您创建云企业网实例过程中,您需要加载一个网络实例,您从已创建的VPC或云连接网实例中,选择一个即可。

ii. 云企业网加载网络实例。具体操作,请参见加载网络实例。

本示例中需要将**华北2(北京)**地域的VPC和云连接网实例加载到同一云企业网中。加入后,VPC和云连接网实例的路由条目会自动发布到云企业网中,VPC和云连接网实例能从云企业网中学习对 方的路由,实现云下本地机构和云上VPC的互联互通。

步骤九:连通性测试

完成上述配置后,您可以通过本地机构中的客户端访问VPC中部署的云资源,验证网络的连通性。

② 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许本地机构访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

- 1. 在本地机构中, 打开客户端的命令行窗口。
- 2. 执行 ping 命令, ping 云上VPC 10.0.0.0/16网段下的ECS实例IP地址, 如果能接受到回复报文, 则 表示网络已经连通。

经验证,企业本地机构可以和云上VPC正常通信。

[root@iZZ ~]# ping 10.0.2.210
PING 10.0.2.210 (10.0.2.210) 56(84) bytes of data.
64 bytes from 10.0.2.210: icmp_seq=1 ttl=64 time=0.345 ms
64 bytes from 10.0.2.210: icmp_seq=2 ttl=64 time=0.237 ms
64 bytes from 10.0.2.210: icmp_seq=3 ttl=64 time=0.155 ms
64 bytes from 10.0.2.210: icmp_seq=4 ttl=64 time=0.161 ms
^Z
[1]+ Stopped ping 10.0.2.210
[root@iZZ ~]# []

3.3.1.2.3. SAG双机旁挂动态路由上云方案

本文为您介绍如何通过智能接入网关SAG(Smart Access Gateway)双机旁挂模式并使用动态路由将企业接入阿里云,实现云下企业网络与云上VPC(Virtual Private Cloud)的互通。

方案概述

在企业上云过程中,部分大型企业会将数据保存在阿里云,其企业总部及分支机构有时会需要从阿里云读取数据,在企业从阿里云读取数据的过程中,会需要一条高弹性和大带宽的上云链路。智能接入网关是阿里云的SD-WAN终端,具有多种软硬件的产品形态,可将企业快速就近地接入阿里云,部署简单,维护方便,扩展性好。

本文以下图场景为例,为您介绍智能接入网关双机旁挂动态路由上云方案。某企业总部在阿里云华北2(北京)地域创建了VPC,其中部署有云服务器ECS(Elastic Compute Service)和对象存储服务OSS(Object Storage Service),企业的总部会定期将数据备份到阿里云OSS中,企业有时会需要从OSS中读取数据并和 云上ECS进行交互访问。企业现在需要部署上云链路,以实现云下本地机构和云上VPC的互联互通。其中:

- 智能接入网关采用SAG-1000型号设备并采用旁挂模式将企业本地机构接入阿里云,无需改变企业本地机构的现有网络架构。
- 智能接入网关部署为双机模式,两台智能接入网关设备可以互为备份链路,为企业提供高可用的上云链路。
- 企业本地机构和智能接入网关之间采用OSPF动态路由方式,降低路由维护难度。



准备工作

您已经注册了阿里云账号。如未注册,请先完成账号注册。

- 您已经在阿里云华北2(北京)地域创建了VPC。具体操作,请参见创建和管理专有网络。
- 本文示例中SAG-1000运行2.0软件版本。关于设备软件版本支持的功能说明,请参见智能接入网关硬件功能发布记录。
- 以下为本文网段规划示例值以及智能接入网关接入企业本地机构中的网络架构示例图。如您需要自行规划 网段,请确保各个网段地址不冲突。



规划目标	网段及IP地址
VPC	10.0.0/16
出口路由器	端口G1: 192.168.80.1/30
智能接入网关1	WAN端口5: 192.168.100.1/30, 下一跳: 192.168.100.2
智能接入网关2	WAN端口5: 192.168.200.1/30, 下一跳: 192.168.200.2
三层交换机	 端口G2: 192.168.80.2/30 端口G11: 192.168.100.2/30 端口G13: 192.168.200.2/30 环回口: 192.168.100.3/32
本地机构	172.16.0.0/12

配置步骤



步骤一:购买智能接入网关

在智能接入网关控制台购买智能接入网关设备后, 阿里云会将智能接入网关设备寄送给您, 并创建一个智能 接入网关实例方便您管理设备。 ⑦ 说明 如果您要使用智能接入网关的区域非中国内地时,您需要通过第三方公司购买硬件。具体操作,请参见购买SAG设备。

1. 登录智能接入网关管理控制台。

- 2. 在智能接入网关页面,选择购买智能接入网关 > 创建智能接入网关(硬件版)。
- 3. 在购买页面,根据以下信息配置智能接入网关,然后单击**立即购买**。
 - 区域:智能接入网关使用区域。本示例选择中国内地。
 - 实例类型:选择智能接入网关设备规格。本示例选择SAG-1000。
 - 已有SAG硬件:选择是否已有智能接入网关硬件设备。本示例选择否。
 - 版本:智能接入网关设备版本。本示例使用默认值标准版。
 - **购买数量**:智能接入网关设备购买数量。本示例选择2。
 - 区域:智能接入网关使用的带宽区域。该区域类型和智能接入网关设备使用区域保持一致,且无法修改。
 - **实例名称**:智能接入网关实例名称。

名称长度为2~128个字符,以大小写字母或中文开头,可包含数字、半角句号(.)、短划线(-)和 下划线(_)。

- 带宽峰值:选择通信网络的带宽峰值。本示例选择30 Mbps。
- 购买时长:选择购买时长。
- 4. 确认订单信息并勾选服务协议,然后单击确认购买。
- 5. 在弹出的收货地址对话框,填写网关设备的收货地址,然后单击立即购买。
- 6. 在弹出的支付页面,选择支付方式,然后完成支付。

您可以在智能接入网关实例页面查看是否下单成功。系统会在下单后两个工作日内发货。如果超期,您可以<mark>提交工单</mark>查看物流状态。

智能接入网关												
随时随地安全上云,智能 合作伙伴可提供一站式。	能接入网关APP免费试用活动中。 点目 上门安装、售后服务。 服务详情 >>	達著										
购买智能接入网关 🗸	実例名称 > 清縮入	Q									۲	С
实例ID/名称	绑定云连接网ID/名称	接入点	带宽峰值	状态 🕜	SN号 @	規格 🙆	购买时间	到期时间	资源组	操作		
sag- g8s68 /53 testco	鄉定网络		50M	🖻 待发贷		SAG-1000	2020年8月19日 16:05:15	2020年9月20日 00:00:00	default resource group	发货提醒 网络配	E i	

7. 收到网关设备后,请检查设备配件是否完整。关于设备配件信息,请参见SAG-1000设备说明。

步骤二: 激活智能接入网关

收到设备后,您还需要按照以下操作,激活绑定设备。

- 1. 登录智能接入网关管理控制台。
- 2. 在顶部菜单栏,选择目标区域。
- 在智能接入网关页面,找到目标实例。将设备与智能接入网关实例进行绑定。具体操作,请参见添加设备。

您需要将两台设备绑定到一个实例中,最先绑定的设备为主设备,另一个台设备为备设备。本示例中智能接入网关1为主设备,智能接入网关2为备设备。

- 4. 绑定后,返回到智能接入网关页面。选择目标实例操作列下的:>激活。
- 5. 在激活对话框,单击确定。

步骤三: 连接智能接入网关

激活、绑定智能接入网关设备后,您还需要将智能接入网关连接到您的本地机构中。

在您执行以下操作前,请保持设备启动且4G信号正常,已经连接到阿里云。本操作以智能接入网关1为例进行配置,请根据网络规划和以下步骤配置智能接入网关2。

- 1. 在智能接入网关页面,找到目标网关实例ID。
- 2. 在智能接入网关实例详情页面,单击设备管理页签,选择目标设备。
- 3. 在页签左侧区域,单击端口角色分配。
- 在端口角色分配页面,单击目标端口操作列下的修改,修改端口角色,然后单击确定。
 本示例中智能接入网关1使用WAN(端口5)。关于端口的更多信息,请参见分配端口角色。

⑦ 说明 仅SAG-1000型号设备的2.0版本支持端口角色分配功能。

5. 通过网线,将智能接入网关1的WAN (端口5)连接到三层交换机的G11端口上。

步骤四:配置端口

连接好网关设备后,您可以在智能接入网关管理控制台分别对智能接入网关1和智能接入网关2进行端口配置。

- 1. 在智能接入网关页面,单击目标网关实例ID。
- 2. 在智能接入网关实例详情页面,单击设备管理页签,然后选择目标设备。
- 3. 在页签左侧区域,单击WAN口管理。
- 4. 在WAN (端口5) 区域, 单击编辑。
- 5. 在WAN (端口5) 配置对话框,根据以下信息配置端口,然后单击确定。

智能接入网关1:

- 连接类型:选择静态IP。
- IP地址: WAN端口IP地址。本示例输入192.168.100.1。
- 掩码: WAN端口IP地址掩码。本示例输入255.255.255.252。
- 网关: 网关IP地址。本示例输入192.168.100.2。

智能接入网关2:

- 连接类型:选择静态ⅠP。
- IP地址: WAN端口IP地址。本示例输入192.168.200.1。
- 掩码: WAN端口IP地址掩码。本示例输入255.255.255.252。
- 网关: 网关IP地址。本示例输入192.168.200.2。

⑦ 说明 配置网关IP地址后,智能接入网关设备自动会生成一条默认路由。

步骤五:配置路由

端口配置完成后,请按照以下操作,分别对智能接入网关1和智能接入网关2进行OSPF路由配置并完成线下 路由同步方式的配置。

1. 在智能接入网关页面,单击目标网关实例ID。

- 2. 在智能接入网关实例详情页面,单击设备管理页签,然后选择目标设备。
- 3. 在页签左侧区域,单击路由管理。
- 4. 在OSPF协议配置区域,单击编辑。
- 5. 在配置OSPF路由协议对话框, 输入以下配置信息, 然后单击确定。

关于参数的说明,请参见<mark>配置OSPF路由</mark>。

参数	说明
Area ID	OSPF路由协议区域ID。 两台设备的区域ID均设置为1。
Hello Time	发送Hello报文的时间间隔。 两台设备的Hello Time时间均设置为3秒。
Dead Time	OSPF邻居失效时间。 两台设备的Dead Time时间均设置为10秒 。
认证类型	OSPF路由协议认证方式。 两台设备均选择 不认证 。
Router ID	路由器ID。 • 智能接入网关1路由器ID: 192.168.100.1。 • 智能接入网关2路由器ID: 192.168.200.1。
Area Type	OSPF路由协议区域类型。默认为 NSSA 。

- 6. 在动态路由配置详情区域,选择启用OSPF协议。
- 7. 在切换路由协议对话框,单击确定。
- 8. 在端口展示区域,选择目标端口5(WAN),单击端口操作列的编辑,选择启用OSPF,然后单击确 定。
- 9. 配置线下路由同步方式。具体操作,请参见线下路由同步方式。

本示例选择添加静态路由。静态路由添加为本地机构要和云上互通的网段: 172.16.0.0/12。

步骤六:本地机构配置

您需要为智能接入网关设备对端的交换机和出口路由器添加端口以及路由配置。此处以某品牌交换机和路由 器为例,由于不同厂商设备配置命令不同,详情请参见厂商设备手册。

1. 三层交换机配置。

```
#a. 配置端口IP及OSPF参数:
interface GigabitEthernet 0/11
no switchport
ip ospf network point-to-point #端口网络类型必选为p2p
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.100.2 255.255.252 #智能接入网关1对端交换机的端口IP
interface GigabitEthernet 0/13
no switchport
ip address 192.168.200.2 255.255.255.252 #智能接入网关2对端交换机的端口IP
ip ospf network point-to-point     #端口网络类型必须为</mark>p2p
ip ospf dead-interval 10
ip ospf hello-interval 3
#b.配置交换机的环回口地址及路由通告信息:
interface Loopback 0
ip address 192.168.100.3 255.255.255.255
                                    #交换机的环回口IP地址
router ospf 1
router-id 192.168.100.3
                             #交换机OSPF路由协议的路由器ID
network 172.16.0.0 0.15.255.255 area 0
                                    #宣告本地机构私网网段
network 192.168.100.0 0.0.0.4 area 1
                                   #宣告交换机连接智能接入网关1的端口网段
                                  #宣告交换机环回口地址
network 192.168.100.3 0.0.0.0 area 0
network 192.168.200.0 0.0.0.4 area 1
                                  #宣告交换机连接智能接入网关2的端口网段
                                         #OSPF路由协议区域类型
area 1 nssa
```

2. 出口路由器的路由配置。

#添加出口路由器去往智能接入网关的回程路由:

```
ip route 192.168.100.0 255.255.255.252 192.168.80.2 #出口路由器去往智能接入网关1的回程路由
ip route 192.168.200.0 255.255.255.252 192.168.80.2 #出口路由器去往智能接入网关2的回程路由
```

步骤七:配置网络连接

在配置好网关设备后,您需要配置网络连接,将本地机构接入阿里云。

- 1. 创建云连接网。
 - i. 登录智能接入网关管理控制台。
 - ii. 在左侧导航栏, 单击云连接网。
 - iii. 在云连接网页面, 单击创建云连接网。
 - iv. 在创建云连接网面板, 配置云连接网名称, 然后单击确定。

云连接网名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)和短划线 (-)。

智能接入网关 / 云连接网				使用限制 📀 幕助文档
云连接网				
创建云连接网 C				案例ID ~ 请输入 Q
实例ID/名称	绑定云企业网	鄉定智能接入网关	私网网段	操作
ccn-		0/0		御喧云企业网 删除

- 2. 配置网络连接。
 - i. 在左侧导航栏, 单击智能接入网关。

ii. 在智能接入网关页面,单击目标实例操作列的网络配置。

iii. 单击绑定网络详情页签, 然后单击添加网络。

iv. 在添加网络对话框,选择云连接网类型并选择已创建的云连接网实例,然后单击确定。

- 3. 绑定云企业网。
 - i. 创建云企业网实例。具体操作, 请参见创建云企业网实例。

在您创建云企业网实例过程中,您需要加载一个网络实例,您从已创建的VPC或云连接网实例中, 选择一个即可。

ii. 云企业网加载网络实例。具体操作,请参见加载网络实例。

本示例中需要将**华北2(北京)**地域的VPC和云连接网实例加载到同一云企业网中。加入后,VPC和云连接网实例的路由条目会自动发布到云企业网中,VPC和云连接网实例能从云企业网中学习对方的路由,实现云下本地机构和云上VPC的互联互通。

步骤八: 连通性测试

完成上述配置后,您可以通过本地机构中的客户端访问VPC中部署的云资源,验证网络的连通性。

⑦ 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许本地机构访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

- 1. 在本地机构中, 打开客户端的命令行窗口。
- 2. 执行 ping 命令, ping 云上VPC 10.0.0.0/16网段下的ECS实例IP地址, 如果能接受到回复报文, 则 表示网络已经连通。

经验证,企业本地机构可以和云上VPC正常通信。

[root@iZ J Z ~]# ping 10.0.2.210						
PING 10.0.2.210 (10.0.2.210) 56(84) bytes of data.						
64 bytes from 10.0.2.210: icmp_seq=1 ttl=64 time=0.345 ms						
64 bytes from 10.0.2.210: icmp_seq=2 ttl=64 time=0.237 ms						
64 bytes from 10.0.2.210: icmp_seq=3 ttl=64 time=0.155 ms						
64 bytes from 10.0.2.210: icmp_seq=4 ttl=64 time=0.161 ms						
^Z						
[1]+ Stopped ping 10.0.2.210						
[root@iZ Z ~]# []						

3.3.1.2.4. SAG双机旁挂静态路由上云方案

本文为您介绍如何通过智能接入网关SAG(Smart Access Gateway)双机旁挂模式并使用静态路由将企业接入阿里云,实现云下企业网络与云上VPC(Virtual Private Cloud)的互通。

方案概述

在企业上云过程中,部分大型企业会将数据保存在阿里云,其企业总部及分支机构有时会需要从阿里云读取数据,在企业从阿里云读取数据的过程中,会需要一条高弹性和大带宽的上云链路。智能接入网关是阿里云的SD-WAN终端,具有多种软硬件的产品形态,可将企业快速就近地接入阿里云,部署简单,维护方便,扩展性好。

本文以下图场景为例,为您介绍智能接入网关双机旁挂静态路由上云方案。某企业总部在阿里云华北2(北京)地域创建了VPC,其中部署有云服务器ECS(Elastic Compute Service)、对象存储服务OSS(Object Storage Service)以及其他云服务,企业的总部会定期将数据备份到阿里云OSS中,企业有时会需要从OSS中读取数据并和云上ECS进行交互访问。企业现在需要部署上云链路,以实现云下本地机构和云上VPC的互联互通。其中:

- 智能接入网关采用SAG-1000型号设备并采用旁挂模式将企业本地机构接入阿里云,无需改变企业本地机构的现有网络架构。
- 智能接入网关部署为双机模式,两台智能接入网关设备可以互为备份链路,为企业提供高可用的上云链路。
- 企业本地机构和智能接入网关之间采用静态路由。



准备工作

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经在阿里云华北2(北京)地域创建了VPC。具体操作,请参见创建和管理专有网络。
- 本文示例中SAG-1000运行2.0软件版本。关于设备软件版本支持的功能说明,请参见智能接入网关硬件功能发布记录。
- 以下为智能接入网关接入企业本地机构中的网络架构示例图以及网段规划示例值。



↓ 注意

- 如您需要自行规划网段,请确保要互通的网段之间没有重叠。
- 请确保智能接入网关1的WAN□IP地址、智能接入网关2的WAN□IP地址、虚IP地址、交换机 VLAN IP地址之间互不相同。

规划目标	网段及IP地址
VPC	10.0.0/16
出口路由器	端口G1: 192.168.80.1/30
智能接入网关1	。 WAN端口5: 192.168.100.1/30, 下一跳: 192.168.100.4 。 WAN端口5开启静态HA模式, 虚IP地址: 192.168.100.3
智能接入网关2	○ WAN端口5: 192.168.100.2/30, 下一跳: 192.168.100.4 ○ WAN端口5开启静态HA模式, 虚IP地址: 192.168.100.3
三层交换机	 端口G2: 192.168.80.2/30 端口G11: 划分到VLAN 11下 端口G12: 划分到VLAN 11下 VLAN 11: 192.168.100.4/30
本地机构	172.16.0.0/12

配置步骤



步骤一:购买智能接入网关

在智能接入网关控制台购买智能接入网关设备后, 阿里云会将智能接入网关设备寄送给您, 并创建一个智能 接入网关实例方便您管理设备。

⑦ 说明 如果您要使用智能接入网关的区域非中国内地时,您需要通过第三方公司购买硬件。具体操作,请参见购买SAG设备。

1. 登录智能接入网关管理控制台。

2. 在智能接入网关页面,选择购买智能接入网关 > 创建智能接入网关(硬件版)。

- 3. 在购买页面,根据以下信息配置智能接入网关,然后单击**立即购买**。
 - 区域:智能接入网关使用区域。本示例选择中国内地。
 - **实例类型**:选择智能接入网关设备规格。本示例选择SAG-1000。

○ 已有SAG硬件:选择是否已有智能接入网关硬件设备。本示例选择否。

- 版本:智能接入网关设备版本。本示例使用默认值标准版。
- 购买数量:智能接入网关设备购买数量。本示例选择2。
- 区域:智能接入网关使用的带宽区域。该区域类型和智能接入网关设备使用区域保持一致,且无法修改。
- **实例名称**:智能接入网关实例名称。
 名称长度为2~128个字符,以大小写字母或中文开头,可包含数字、半角句号(.)、短划线(-)和下划线()。
- 带宽峰值:选择通信网络的带宽峰值。本示例选择30 Mbps。
- 购买时长:选择购买时长。
- 4. 确认订单信息并勾选服务协议,然后单击确认购买。
- 5. 在弹出的收货地址对话框,填写网关设备的收货地址,然后单击**立即购买**。
- 6. 在弹出的支付页面,选择支付方式,然后完成支付。

您可以在智能接入网关实例页面查看是否下单成功。系统会在下单后两个工作日内发货。如果超期,您可以提交工单查看物流状态。

智能接入网关											
随时随地安全上云,智前 合作伙伴可提供一站式」	8接入网关APP免费试用活动中。 点击 E门安装、售后服务。 服务详情 >>	22									
购买智能接入网关 🗸	実例名称 > 清輸入	Q									\$ C
实例ID/名称	鄉定云連接网ID/名称	接入点	带宽峰值	状态 😰	SN쿡 🕝	規格 😡	购买时间	到期时间	资源组	操作	
sag- g8s68 /53 testco	绑定网络		50M	🖻 待发贷		SAG-1000	2020年8月19日 16:05:15	2020年9月20日 00:00:00	default resource group	发货提醒 网络配置	: I I

7. 收到网关设备后,请检查设备配件是否完整。关于设备配件信息,请参见SAG-1000设备说明。

步骤二: 激活智能接入网关

收到设备后,您还需要按照以下操作,激活绑定设备。

- 1. 登录智能接入网关管理控制台。
- 2. 在顶部菜单栏,选择目标区域。
- 在智能接入网关页面,找到目标实例。将设备与智能接入网关实例进行绑定。具体操作,请参见添加设备。

您需要将两台设备绑定到一个实例中,最先绑定的设备为主设备,另一个台设备为备设备。本示例中智能接入网关1为主设备,智能接入网关2为备设备。

4. 绑定后,返回到智能接入网关页面。选择目标实例操作列下的:>激活。

5. 在激活对话框,单击确定。

步骤三: 连接智能接入网关

激活、绑定智能接入网关设备后,您还需要将智能接入网关连接到您的本地机构中。

在您执行以下操作前,请保持设备启动且4G信号正常,已经连接到阿里云。本操作以智能接入网关1为例进行配置,请根据网络规划和以下步骤配置智能接入网关2。

- 1. 在智能接入网关页面,找到目标网关实例ID。
- 2. 在智能接入网关实例详情页面, 单击设备管理页签, 选择目标设备。
- 3. 在页签左侧区域,单击端口角色分配。
- 4. 在端口角色分配页面,单击目标端口操作列下的修改,修改端口角色,然后单击确定。

本示例中智能接入网关1使用WAN(端口5)。关于端口的更多信息,请参见分配端口角色。

⑦ 说明 仅SAG-1000型号设备的2.0版本支持端口角色分配功能。

5. 通过网线,将智能接入网关1的WAN (端口5)连接到三层交换机的G11端口上。

步骤四:配置端口

连接好网关设备后,您可以在智能接入网关管理控制台分别对智能接入网关1和智能接入网关2配置端口。

- 1. 在智能接入网关页面,单击目标网关实例ID。
- 2. 在智能接入网关实例详情页面,单击设备管理页签,然后选择目标设备。
- 3. 在页签左侧区域,单击WAN口管理。
- 4. 在WAN (端口5) 区域,单击编辑。
- 5. 在WAN (端口5) 配置对话框,根据以下信息配置端口,然后单击确定。

配置项	说明	智能接入网关1参数值	智能接入网关2参数值
连接类型	端口连接类型。	选择静态IP	选择静态IP
IP地址	WAN端口IP地址。	192.168.100.1	192.168.100.2
掩码	WAN端口IP地址掩码。	255.255.255.252	255.255.255.252
网关	网关IP地址。	192.168.100.4	192.168.100.4

⑦ 说明 配置网关IP地址后,智能接入网关设备自动会生成一条默认路由。

6. 开启HA模式。

您分别需要将智能接入网关1和智能接入网关2的WAN口开启HA模式。

i. 在智能接入网关实例详情页面, 单击**设备管理**页签, 并选择目标设备。

- ii. 在设备管理页签左侧区域,单击HA管理。
- ⅲ. 在HA信息区域, 单击 ∠ 图标。
- iv. 在HA配置对话框,根据以下信息进行配置,然后单击保存。

配置	说明
HA模式	两台智能接入网关设备均选择静态。
端口	两台智能接入网关设备均选择WAN(端口5)。
虚IP	智能接入网关WAN口的虚拟IP地址。本示例中两台智能接入网关设备均使用 192.168.100.3。

更多信息,请参见配置设备级高可用。

步骤五:配置路由

智能接入网关设备的端口配置完成后,您需要配置线下路由同步方式将本地机构的路由同步到云上,同时在 设备上配置静态路由为云上流量去往本地机构指定出口。

- 1. 在智能接入网关页面,单击目标网关实例ID。
- 2. 在智能接入网关实例详情页面,单击网络配置页签。
- 3. 在页签左侧区域,单击线下路由同步方式。
- 4. 选择静态路由,然后单击添加静态路由,配置静态路由信息,然后单击确定。

静态路由添加为本地机构要和云上互通的网段: 172.16.0.0/12。

添加静态路由	
* 网段 🕖	
172.16.0.0	/ 12
	确 定 关闭

5. 保持在该智能接入网关实例页面,单击**设备管理**页签,并选择目标设备。

请根据以下操作分别为智能接入网关1和智能接入网关2添加静态路由。

- i. 在页签左侧区域, 单击路由管理, 然后单击添加静态路由。
- ii. 在**添加静态路由**对话框,添加去往本地机构的静态路由。

配置项	智能接入网关1参数值	智能接入网关2参数值
目标网段	172.16.0.0/12	172.16.0.0/12
下一跳IP	192.168.100.4	192.168.100.4
端口	选择 端口5(WAN)	选择 端口5(WAN)

步骤六:配置本地机构

您需要为智能接入网关设备对端的交换机和出口路由器添加端口以及路由配置。由于不同厂商设备配置不同,以下内容仅供参考,具体配置命令请参见您的厂商设备手册。

1. 三层交换机配置。

#a. **配置端口**IP

```
#创建SVI端口VLAN11,并为端口配置IP地址
vlan 11
interface vlan 11
ip address 192.168.100.4 255.255.255.252
                                        #将端口G11加入VLAN11
interface GigabitEthernet 0/11
switchport
switchport mode access
switchport access vlan 11
interface GigabitEthernet 0/12
                                       #将端口G12加入VLAN11
switchport
switchport mode access
switchport access vlan 11
#b.为交换机配置去往VPC的静态路由:
ip route 10.0.0.0 255.255.0.0 192.168.100.3 #去往VPC的路由的下一跳指向虚IP地址
```

2. 出口路由器的路由配置。

#添加出口路由器去往智能接入网关的回程路由:

ip route 192.168.100.0 255.255.255.252 192.168.80.2 #出口路由器去往智能接入网关的回程路由

步骤七:配置网络连接

在配置好网关设备后,您需要配置网络连接,将本地机构接入阿里云。

- 1. 创建云连接网。
 - i. 登录智能接入网关管理控制台。
 - ii. 在左侧导航栏, 单击云连接网。
 - iii. 在云连接网页面, 单击创建云连接网。
 - iv. 在创建云连接网面板, 配置云连接网名称, 然后单击确定。

云连接网名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)和短划线 (-)。

智能接入网关 / 云连接网				使用限制 🛛 😵 帮助文档
云连接网				
创建云连接网 C				実例ID ~ 清縮入 Q
实例ID/名称	绑定云企业网	鄉定智能接入网关	私网网段	操作
con-	-	0 / 0		御還云企业网 删除

- 2. 配置网络连接。
 - i. 在左侧导航栏, 单击智能接入网关。
 - ii. 在智能接入网关页面, 单击目标实例操作列的网络配置。
 - iii. 单击绑定网络详情页签, 然后单击添加网络。
 - iv. 在添加网络对话框,选择云连接网类型并选择已创建的云连接网实例,然后单击确定。
- 3. 绑定云企业网。
 - i. 创建云企业网实例。具体操作,请参见云企业网实例。

ii. 云企业网加载网络实例。具体操作,请参见创建VPC连接或创建CCN连接。

本示例中需要将**华北2(北京)**地域的VPC和云连接网实例加载到同一云企业网中。加入后,VPC和云连接网实例的路由条目会自动发布到云企业网中,VPC和云连接网实例能从云企业网中学习对方的路由,实现云下本地机构和云上VPC的互联互通。

⑦ 说明 在您将VPC加入云企业网中时,请选择开启所有高级功能。

步骤八:连通性测试

完成上述配置后,您可以通过本地机构中的客户端访问VPC中部署的云资源,验证网络的连通性。

② 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许本地机构访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

- 1. 在本地机构中, 打开客户端的命令行窗口。
- 2. 执行 ping 命令, ping 云上VPC 10.0.0.0/16网段下的ECS实例IP地址, 如果能接受到回复报文, 则 表示网络已经连通。

3.3.1.2.5. IPsec-VPN联合物理专线实现主备链路上云方案

本文为您介绍如何组合使用IPsec-VPN和物理专线,实现本地数据中心IDC(Internet Data Center)通过主备链路上云并和云上专有网络VPC(Virtual Private Cloud)互通。

方案概述

在企业上云过程中,一些企业的IDC数据、云上业务数据会统一汇聚到阿里云大数据平台,通过云计算能力 进行数据挖掘、分析、开发数据应用。在此场景下,企业至阿里云通常是入向流量大于出向流量,业务交互 也比较频繁,企业需要高可靠、高弹性的上云链路。

针对上述网络诉求, 阿里云为您提供以下两种解决方案:

- IPsec-VPN联合物理专线实现主备链路上云方案
- SAG联合物理专线实现主备链路上云方案

在上述方案中,本地IDC与VPC通过物理专线连接,作为上云的主链路,保障日常数据交互的可靠性。VPN网 关或智能接入网关SAG (Smart Access Gateway)作为备用链路,解决网络弹性连接的诉求。

- 当物理专线正常时,本地IDC与VPC之间的所有流量只通过物理专线进行转发。
- 当物理专线异常时,本地IDC与VPC之间的所有流量将切换至VPN链路或SAG链路进行转发。

场景示例

本文以下图场景为例,为您介绍IPsec-VPN联合物理专线实现主备链路上云方案。某企业在杭州拥有一个本地IDC,且企业已经在阿里云华东1(杭州)地域部署了业务VPC1,VPC1中通过云服务器ECS(Elastic Compute Service)等云产品部署了应用业务和数据分析服务,用于后续业务交互和数据分析。企业现在需要部署上云的主备链路,以实现云下IDC和云上VPC1的互联互通。链路说明如下:

- VPN网关将关联至一个独立的VPC(VPC2)。VPC2中不部署任何业务,仅作为中转VPC为本地IDC和云上 搭建VPN链路。
- 在物理专线和VPN链路都正常的情况下,本地IDC与VPC1之间的所有流量只通过物理专线进行转发;当物 理专线异常时,本地IDC与VPC1之间的所有流量将切换至VPN链路进行转发。



准备工作

- 您需要为本地IDC和网络实例规划路由协议。本文路由协议规划如下:
 - 本地IDC网关设备与VPN网关之间配置静态路由。
 - 本地IDC网关设备与边界路由器VBR(Virtual border router)之间运行BGP动态路由协议。
 - ⑦ 说明 在VPN网关作为物理专线备份链路的场景下,路由协议说明如下:
 - 如果VPN网关关联至一个独立的VPC(例如本文的VPC2)中,则VBR必须使用BGP动态路由 协议,VPN网关可以使用静态路由或BGP动态路由协议。
 - 如果VPN网关关联至业务VPC(例如本文的VPC1)中,则VBR和VPN网关均需要使用BGP动态路由协议。
- 您需要为本地IDC和网络实例规划网段,请确保网段之间没有重叠。本文网段规划如下。

配置目标	网段规划	IP地址
VPC1	192.168.0.0/16	云服务器地址: 192.168.20.161
VPC2	10.0.0/16	不涉及
VBR	10.1.0.0/30	 VLAN ID: 0 阿里云侧IPv4互联IP: 10.1.0.1/30 客户侧IPv4互联IP: 10.1.0.2/30 本文中客户侧指本地IDC的网关设备
本地IDC	172.16.0.0/16	客户端地址: 172.16.1.188
本地IDC的网关设备	10.1.0.0/30	 公网IP地址: 211.XX.XX.68 与物理专线连接的端口IP地址: 10.1.0.2/30 BGP AS号: 65530

您已经在阿里云华东1(杭州)地域创建了VPC1和VPC2。其中,VPC1部署有应用业务和数据分析服务;
 VPC2暂不部署业务,仅关联VPN网关,作为中转VPC为云下和云上搭建VPN链路。具体操作,请参见创建

和管理专有网络。

- 请检查本地IDC网关设备,确保网关设备支持标准的IKEv1和IKEv2协议,以便和阿里云VPN网关建立连接。
 关于网关设备是否支持标准的IKEv1和IKEv2协议,请咨询网关设备厂商。
- 您已经为本地IDC网关设备配置了静态公网IP。
- 您已经了解VPC1中的ECS实例所应用的安全组规则,并确保安全组规则允许本地IDC访问VPC1中的ECS实例。具体操作,请参见查询安全组规则和添加安全组规则。

配置流程



步骤一: 部署物理专线

1. 创建物理专线。

您需要在华东1(杭州)地域申请一条物理专线。具体操作,请参见创建和管理独享专线连接或共享专 线连接概述。

- 2. 创建VBR。
 - i. 登录高速通道管理控制台。
 - ii. 在左侧导航栏,单击边界路由器(VBR)。
 - iii. 在顶部状态栏,选择要创建的VBR的地域。

本示例选择**华东1(杭州)**地域。

- iv. 在边界路由器 (VBR) 页面, 单击创建边界路由器。
- v. 在创建边界路由器面板,根据以下信息进行配置,然后单击确定。
 - 账号类型:本示例选择当前账号。
 - 名称:本示例输入VBR。
 - 物理专线接口:选择已申请的物理专线接口。
 - VLAN ID: 0。
 - 阿里云侧IPv4互联IP: 10.1.0.1。
 - 客户侧IPv4互联IP: 10.1.0.2。
 - IPv4子网掩码: 255.255.255.252。
- 3. 配置BGP组。
 - i. 在边界路由器 (VBR) 页面, 单击目标实例ID。
 - ii. 在边界路由器实例详情页面,单击BGP组页签,然后单击创建BGP组。
 - iii. 在创建BGP组面板,根据以下信息配置BGP组,然后单击确定。
 - 名称: BGP组的名称。本示例输入test。
 - Peer AS号:本地IDC侧网关设备的AS号。本示例输入65530。
 - BGP密钥: BGP组的密钥。本示例不配置该项。
 - 描述: BGP组的描述信息。本示例输入test。

- 4. 配置BGP邻居。
 - i. 在边界路由器实例详情页面,单击BGP邻居页签,然后单击创建BGP邻居。
 - ii. 在创建BGP邻居面板, 配置BGP邻居信息, 然后单击确定。
 - BGP组:选择要加入的BGP组。本示例选择已创建的BGP组。
 - BGP邻居IP: BGP邻居的IP地址。本示例输入本地IDC侧网关设备的端口IP地址10.1.0.2。

步骤二:部署VPN网关

- 1. 创建VPN网关。
 - i. 登录VPN网关管理控制台。
 - ii. 在顶部菜单栏,选择**华东1(杭州)**地域。
 - iii. 在VPN网关页面,单击创建VPN网关。
 - iv. 在购买页面,根据以下信息配置VPN网关,然后单击**立即购买**并完成支付。
 - 实例名称: 输入VPN网关的实例名称。
 - 地域和可用区:选择VPN网关的地域。

- 网关类型:选择要创建的VPN网关类型。本示例选择普通型。
- VPC: 选择要连接的VPC。本示例选择VPC2。
- 指定交换机:是否指定VPN网关创建在VPC中的某一个交换机下。本示例选择否。 如果您选择了是,您还需要指定具体的虚拟交换机。
- 带宽规格:选择VPN网关的带宽规格,带宽规格是VPN网关所具备的公网带宽。
- IPsec-VPN: 选择开启或关闭IPsec-VPN功能, IPsec-VPN功能可以在本地IDC与VPC之间或不同 VPC之间建立连接。本示例选择**开启**。
- SSL-VPN: 选择开启或关闭SSL-VPN功能, SSL-VPN功能允许您从任何位置的单台计算机连接 到VPC。本示例选择关闭。
- 计费周期:选择购买时长。
- v. 返回VPN网关页面,查看创建的VPN网关并记录VPN网关公网IP地址,用于后续本地IDC侧路由配置。

刚创建好的VPN网关的状态是**准备中**,约1~5分钟会变成**正常**状态。**正常**状态表明VPN网关完成了 初始化,可以正常使用。

- 2. 创建用户网关。
 - i. 在左侧导航栏,选择网间互联 > VPN > 用户网关。
 - ii. 在用户网关页面, 单击创建用户网关。
 - iii. 在创建用户网关面板,根据以下信息配置用户网关,然后单击确定。
 - 名称: 输入用户网关的名称。
 - IP地址: 输入VPC2要连接的本地IDC的网关设备的公网IP。本示例输入211.XX.XX.68。
 - 自治系统号:本地IDC网关设备的自治系统号。本示例无需配置该参数。
 - 描述: 输入用户网关的描述信息。
- 3. 创建IPsec连接。

本示例将VPN网关关联到VPC2上,确保VPC2和VPN网关的地域相同。本示例选择**华东1(杭 州)**。

i 在左侧旦航栏 选择网间百联 > VPN > IPsec连接

- ii. 在IPsec连接页面,单击创建IPsec连接。
- iii. 在创建IPsec连接页面,根据以下信息配置IPsec连接,然后单击确定。
 - 名称: 输入IPsec连接的名称。
 - VPN网关:选择已创建的VPN网关。
 - 用户网关:选择已创建的用户网关。
 - 路由模式:选择路由模式。本示例选择目的路由模式。
 - **立即生效**:选择是否立即生效。本示例选择否。
 - 是: 配置完成后立即进行协商。
 - 否:当有流量进入时进行协商。
 - 预共享密钥:输入共享密钥,本地IDC网关设备的预共享密钥必须与该值一致。本示例使用默认 生成的随机值。

其他选项使用默认配置。

更多信息,请参见创建IPsec连接。

4. 配置VPN网关路由。

您需要在VPN网关中将本地IDC的路由发布到VPC2中。

- i. IPsec连接创建成功后,在创建成功对话框,单击确定,去往VPN网关实例中进行路由发布。
- ii. 在左侧导航栏,选择网间互联 > VPN > VPN网关。
- iii. 在VPN网关页面,找到目标VPN网关,单击目标实例ID。
- iv. 在目的路由表页签, 单击添加路由条目。
- v. 在添加路由条目面板,根据以下信息配置目的路由,然后单击确定。
 - 目标网段: 输入本地IDC的网段。本示例输入172.16.0.0/16。
 - 下一跳类型:选择IPsec连接。
 - 下一跳:选择已创建的IPsec连接实例。
 - 发布到VPC:选择是否将新添加的路由发布到VPC2路由表。本示例选择是。
 - 权重:选择路由的权重值。本示例使用默认值100,表示高优先级。

⑦ 说明 若VPN网关中存在相同目标网段的目的路由,目的路由的权重值不支持同时设置为100。

- 5. 在本地IDC网关设备中加载VPN配置。
 - i. 在左侧导航栏,选择网间互联 > VPN > IPsec连接。
 - ii. 在IPsec连接页面,找到目标IPsec连接,然后在操作列选择。 > 下载对端配置。
 - iii. 根据本地IDC网关设备的配置要求,将下载的配置添加到本地IDC网关设备中。具体操作,请参见本地网关配置。

步骤三:配置云企业网

VBR和VPN网关配置完成后,您需要将VPC1、VPC2和VBR加入到云企业网中,云企业网可帮您实现本地IDC 和VPC1间的互连互通。

- 1. 创建云企业网实例。
 - i. 登录云企业网管理控制台。
 - ii. 在云企业网实例页面, 单击创建云企业网实例。
 - iii. 在创建云企业网实例面板,根据以下信息配置云企业网实例,然后单击确定。
 - 名称: 输入云企业网实例的名称。
 - 描述: 输入云企业网实例的描述。
 - **实例类型**:选择要加载的网络实例类型。本示例选择专有网络(VPC)。
 - 地域:选择网络实例所属的地域。本示例选择**华东1(杭州)**。
 - 网络实例:选择网络实例。本示例选择VPC2。
- 2. 在云企业网实例中加载VPC1、VBR实例。
 - i. 在云企业网实例页面, 找到目标云企业网实例, 单击目标实例ID。
 - ii. 在网络实例管理页签, 单击加载网络实例。
 - iii. 在加载网络实例页面,单击同账号页签。
 - iv. 根据以下信息选择要加载的网络实例, 然后单击确定。
 - 实例类型:选择要加载的网络实例类型。本示例选择专有网络(VPC)。
 - 地域:选择网络实例所属地域。本示例选择**华东1(杭州)**。
 - 网络实例:选择网络实例。本示例选择VPC1。
 - v. 重复上述步骤,将VBR实例加载至该云企业网实例。
- 3. 发布VPC2中的本地IDC路由至云企业网。

您在VPN网关中将本地IDC路由发布到VPC2中后,VPC2中本地IDC的路由默认是未发布状态。您需要手动将VPC2中的本地IDC路由发布到云企业网中,以便VPC1也能从VPC2学习到本地IDC的路由。

- i. 登录云企业网管理控制台。
- ii. 在云企业网实例页面,找到目标云企业网实例,单击实例ID。
- iii. 在云企业网实例详情页面, 单击路由信息页签。
- iv. 在路由信息页签下,选择查看VPC2网络实例的路由条目,找到本地IDC的路由,在发布状态列单 击发布。
- v. 在发布路由对话框, 单击确定。
- 4. 为物理专线配置健康检查。

您需要为物理专线配置健康检查,健康检查会以您指定的发包时间间隔发送探测报文,当连续发送的所 有探测报文(即您指定的探测报文个数)都丢包时,云企业网会主动将流量切换到VPN链路。

- i. 登录云企业网管理控制台。
- ii. 在左侧导航栏, 单击健康检查。
- iii. 选择VBR的地域,然后单击设置健康检查。

iv. 在设置健康检查面板,根据以下信息配置健康检查,然后单击确定。

- 云企业网实例:选择VBR加载的云企业网实例。
- 边界路由器 (VBR): 选择要监控的VBR实例。
- 源IP: 本示例选择自动生成源IP。

使用自动生成源IP,系统将自动分配100.96.0.0/16地址段内的IP地址,探测链路的连通性。

- 目标IP: 输入VBR实例中客户侧IP地址。
- **发包时间间隔(秒)**:指定健康检查时发送连续探测报文的时间间隔。单位:秒。本示例使用 默认值。
- 探测报文个数(个):指定健康检查时发送探测报文的个数。单位:个。本示例使用默认值。

步骤四:配置本地IDC网关设备

以下配置示例仅供参考。不同厂商的设备,配置命令可能会有所不同。具体命令,请咨询相关设备厂商。

```
#配置BGP动态路由协议,与VBR建立BGP邻居关系,同时宣告本地IDC私网网段至云上
interface GigabitEthernet 0/12
                                #该端口为本地IDC网关设备与物理专线连接的端口
no switchport
                               #端口的IP地址,需和VBR客户侧IPv4互联IP地址一致
ip address 10.1.0.2 255.255.255.252
router bgp 65530
bgp router-id 10.1.0.2
                               #宣告本地IDC私网网段
network 172.16.0.0 mask 255.255.0.0
                               #和VBR建立BGP邻居关系
neighbor 10.1.0.1 remote-as 45104
exit.
#配置通过VPN网关去往VPC1的静态路由,使其优先级低于BGP路由
ip route 192.168.0.0 255.255.0.0 <VPN网关公网IP地址> preference 255
#配置健康检查探测报文的回程路由
ip route <健康检查源IP地址> 255.255.255.255 10.1.0.1
```

步骤五:测试连通性

- 1. 在本地IDC下,打开客户端的命令行窗口。
- 执行 ping 命令,访问云上VPC1 192.168.0.0/16网段下的ECS实例IP地址,如果接收到回复报文,则 表示本地IDC和VPC1连接成功。
- 3. 在本地IDC网关设备上,关闭连接物理专线的端口,切断物理专线连接。在客户端再次执行 ping 命 令,测试本地IDC和VPC1的连通性,如果接收到回复报文,则表示备份VPN链路可用。

3.3.1.2.6. SAG联合物理专线实现主备链路上云方案

本文为您介绍如何组合使用智能接入网关SAG(Smart Access Gateway)和物理专线,实现本地数据中心 IDC(Internet Data Center)通过主备链路上云并和云上专有网络VPC(Virtual Private Cloud)互通。

方案概述

在企业上云过程中,一些企业的IDC数据、云上业务数据会统一汇聚到阿里云大数据平台,通过云计算能力 进行数据挖掘、分析、开发数据应用。在此场景下,企业至阿里云通常是入向流量大于出向流量,业务交互 也比较频繁,企业需要高可靠、高弹性的上云链路。

针对上述网络诉求, 阿里云为您提供以下两种解决方案:

- IPsec-VPN联合物理专线实现主备链路上云方案
- SAG联合物理专线实现主备链路上云方案

在上述方案中,本地IDC与VPC通过物理专线连接,作为上云的主链路,保障日常数据交互的可靠性。VPN网 关或智能接入网关SAG (Smart Access Gateway)作为备用链路,解决网络弹性连接的诉求。

- 当物理专线正常时,本地IDC与VPC之间的所有流量只通过物理专线进行转发。
- 当物理专线异常时,本地IDC与VPC之间的所有流量将切换至VPN链路或SAG链路进行转发。

场景说明

本文以下图场景为例,为您介绍智能接入网关联合物理专线实现主备链路上云方案。某企业在北京地域拥有 一个本地IDC,且企业已经在阿里云华北2(北京)地域创建了一个VPC,其中已通过云服务器ECS(Elastic Compute Service)等云产品部署了应用业务和数据分析服务,用于后续业务交互和数据分析。企业现在需 要部署上云链路,以实现云下IDC和云上VPC的互联互通。



准备工作

在开始操作前,请确保您已经满足以下条件:

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经在阿里云华北2(北京)地域创建了VPC,其中部署有应用业务和数据分析服务。具体操作,请参见创建和管理专有网络。
- 您已经完成网络规划。以下为本文示例中本地IDC的网络规划以及智能接入网关接入企业本地IDC中的网络 架构示例图。



- 企业将智能接入网关和物理专线均接入到同一台三层交换机上。其中,智能接入网关通过云连接网将本地IDC接入阿里云,物理专线通过边界路由器VBR(Virtual border router)将本地IDC接入阿里云。
- 智能接入网关采用SAG-1000型号设备并采用旁挂模式将本地IDC接入阿里云,无需改变本地IDC的现有 网络架构。
- 本地IDC、智能接入网关和边界路由器实例之间均通过BGP路由协议进行路由学习传递,方便网络管理和运维。
 - ⑦ 说明 在智能接入网关作为物理专线备份链路的场景中,物理专线需使用BGP路由协议。
- 智能接入网关同时关联云连接网实例和边界路由器实例,并加入到同一个云企业网实例中,通过云企业 网和云上VPC互通。

在智能接入网关同时关联云连接网和边界路由器的情况下,云企业网默认物理专线优先。云企业网会优 先通过物理专线学习发布路由,物理专线故障时,则通过云连接网学习发布路由,即上云流量和去往云 下的流量优先通过物理专线进行传输,在物理专线故障时,流量则会通过云连接网进行传输。

 本文示例中SAG-1000运行2.0软件版本。关于设备软件版本支持的功能说明,请参见智能接入网关硬件 功能发布记录。 ○ 以下为本文网段规划示例值。请您根据实际业务情况规划网段,并确保各个网段地址不冲突。

项目	网段规划			
	私网网段: 172.16.0.0/12			
本地IDC	 三层交换机G11端口: 192.168.100.2/30 三层交换机G12端口: 192.168.110.1/30 三层交换机G2端口: 192.168.80.2/30 三层交换机BGP路由协议: AS号: 65430 Router ID: 192.168.1.1 			
	出口路由器G1端口: 192.168.80.1/30			
	WAN口(端口5):192.168.100.1/30,网关192.168.100.2			
智能接入网关	BGP路由协议: AS号: 65435 Router ID: 192.168.2.2 Keep Alive: 60秒 Hold Time: 180秒 自用BGP的端口: WAN口			
边界路由器	 阿里云侧IP: 192.168.110.2/30 客户侧IP(本示例为三层交换机侧): 192.168.110.1/30 VLAN: 0 			
VPC	云上网段: 10.0.0/16			

配置流程



步骤一: 创建物理专线

您需要在华北2(北京)地域申请一条物理专线。具体操作,请参见创建和管理独享专线连接或共享专线连接概述。

步骤二:配置边界路由器

边界路由器是本地IDC设备和阿里云接入点连接的一个路由器,作为数据从本地IDC到阿里云机房之间的桥梁。物理专线的一端连接到您本地IDC的设备上,另一端连接到边界路由器。您需要在高速通道控制台创建 边界路由器实例,并和三层交换机建立BGP邻居关系。

1. 创建边界路由器。

i. 登录高速通道管理控制台。

- ii. 在左侧导航栏,单击边界路由器(VBR)。
- iii. 在顶部状态栏,选择要创建的边界路由器的地域。
 本示例选择华北2(北京)地域。
- iv. 在边界路由器 (VBR) 页面, 单击创建边界路由器。
- v. 在创建边界路由器面板,根据以下信息进行配置,然后单击确定。
 - 账号类型:本示例选择当前账号。
 - 名称:本示例输入VBR。
 - 物理专线接口:选择已申请的物理专线接口。
 - VLANID: 0。
 - 阿里云侧互联IP: 192.168.110.2。
 - 客户侧互联IP: 192.168.110.1。
 - 子网掩码: 255.255.255.252。
- 2. 配置BGP组。
 - i. 在边界路由器 (VBR) 页面, 单击目标边界路由器实例ID。
 - ii. 在边界路由器实例详情页面,单击BGP组页签。
 - iii. 在BGP组页签下,单击创建BGP组,并根据以下信息进行BGP组配置。
 - 名称: BGP组的名称。本示例输入test。
 - Peer AS号: 三层交换机侧AS号。本示例输入65430。
 - BGP密钥: BGP组的密钥。本示例不配置该项。
 - 描述: BGP组的描述信息。本示例输入 SAGtest。
 - iv. 单击确定。
- 3. 配置BGP邻居。
 - i. 在边界路由器实例详情页面,单击BGP邻居页签。
 - ii. 在BGP邻居页签下, 单击创建BGP邻居。
 - iii. 在创建BGP邻居面板,配置BGP邻居信息,然后单击确定。
 - BGP组: 要加入的BGP组。本示例选择已创建的BGP组。
 - BGP邻居IP: BGP邻居的IP地址。本示例输入三层交换机G12端口IP地址 192.168.110.1。

BGP邻居	BGP组	BGP邻居IP	网络类型	BGP密钥	Peer AS号	状态	Bgp邻居底层状态
bgp-bp [*] qisnm	bgpg dqx	192.168.110.1	ipv4		65430	• 可用	• Idle

步骤三:购买智能接入网关设备

在智能接入网关控制台购买智能接入网关设备后, 阿里云会将智能接入网关设备寄送给您, 并创建一个智能 接入网关实例方便您管理设备。

⑦ 说明 如果您要使用智能接入网关的区域非中国内地时,您需要通过第三方公司购买硬件。具体操作,请参见购买SAG设备。

1. 登录智能接入网关管理控制台。

- 2. 在左侧导航栏,单击智能接入网关。
- 3. 在智能接入网关页面,选择购买智能接入网关 > 创建智能接入网关(硬件版)。

- 4. 在智能接入网关页面,根据以下信息配置智能接入网关设备,然后单击立即购买。
 - 区域:智能接入网关设备使用区域。本示例选择中国内地。
 - **实例类型**:选择智能接入网关设备规格。本示例选择SAG-1000。
 - 已有SAG硬件:选择是否已有智能接入网关硬件设备。本示例选择否。
 - 版本:智能接入网关设备版本。本示例使用默认标准版。
 - 购买数量:智能接入网关设备购买数量。本示例选择1。
 - 区域:智能接入网关设备使用的带宽区域。该区域类型和智能接入网关设备使用区域保持一致,且无法修改。
 - **实例名称**:智能接入网关实例名称。

名称长度为2~128个字符,以大小写字母或中文开头,可包含数字、半角句号(.)、短划线(-)和 下划线(_)。

- 带宽峰值:选择通信网络的带宽峰值。本示例选择50 Mbps。
- 购买时长:选择购买时长。
- 5. 确认订单信息并勾选服务协议,然后单击确认购买。
- 6. 在弹出的**收货地址**对话框,填写网关设备的收货地址,然后单击**立即购买**。
- 7. 在弹出的支付页面,选择支付方式,然后完成支付。

您可以在智能接入网关实例页面查看是否下单成功。系统会在下单后两个工作日内发货。如果超期,您可以提交工单查看物流状态。

智能接入网关											
● 随时間地安全上去、智能接入风风ADPG集成(用后动中、角曲重音 合作改体可通供一Add、LF)安装、曲局服务、服务評構 >>											
购买智能接入网关 🗸	実例名称 > 清縮入	Q									\$ C
宾例ID/名称	绑定云连接网ID/名称	援入点	带宽峰值	状态 🕝	SN号 @	規格 🙆	购买时间	到期时间	资源组	操作	
sag- g8s68 /53 testcom	继定网络		50M	🖻 待发货		SAG-1000	2020年8月19日 16:05:15	2020年9月20日 00:00:00	default resource group	发货提醒 网络配置	11-1

步骤四: 激活并连接智能接入网关设备

收到智能接入网关设备后,请检查设备配件是否完整。更多信息,请参见SAG-1000设备说明。

设备检查完成后,您需要激活连接设备。

- 1. 登录智能接入网关管理控制台。
- 2. 在顶部菜单栏,选择目标区域。
- 在智能接入网关页面,找到目标实例。将设备与智能接入网关实例进行绑定。具体操作,请参见添加设备。
- 4. 绑定后,返回到智能接入网关页面。在目标实例操作列下,单击:>激活。
- 5. 在激活对话框,单击确定。
- 6. 激活设备后,您还需要将智能接入网关设备按照拓扑所示接入到本地机构中。 通过网线,将智能接入网关设备的WAN口连接到三层交换机的G11端口上。 本示例使用WAN口(端口5)。如果您的端口5不是WAN口,您可以修改端口角色。具体操作,请参见分配端口角色。

? 说明

- 仅SAG-1000型号设备的2.0版本支持端口角色分配功能。
- 在您分配端口角色前,请保持网关设备启动且4G信号正常,已经连接到阿里云。

步骤五: 配置智能接入网关设备

连接好设备后,您需要在智能接入网关管理控制台对设备进行配置。 在执行此操作前,请保证设备4G信号正常且已经连接到阿里云。

- 1. WAN口配置。
 - i. 登录智能接入网关管理控制台。
 - ii. 在顶部菜单栏,选择目标区域。
 - iii. 在智能接入网关页面,单击目标网关实例ID。
 - iv. 在智能接入网关实例详情页面, 单击**设备管理**页签。
 - v. 在页签左侧区域,单击WAN口管理。
 - vi. 在WAN (端口5) 区域, 单击编辑。
 - vii. 在WAN(端口5)配置对话框,根据以下信息配置端口,然后单击确定。
 - 连接类型:选择静态IP。
 - IP地址: WAN口IP地址。本示例输入192.168.100.1。
 - 掩码: WAN口IP地址掩码。本示例输入255.255.255.252。
 - 网关: 网关IP地址。本示例输入192.168.100.2。

⑦ 说明 配置网关后,智能接入网关设备会生成一条默认路由。

2. 配置BGP路由协议。

- i. 在页签左侧区域, 单击路由管理。
- ii. 在BGP协议配置区域,单击编辑。
- iii. 在配置BGP路由协议对话框,根据网络规划,配置BGP路由协议,然后单击确定。
 - 本端AS: 本示例输入65435。
 - Router ID:本示例输入192.168.2.2。
 - Hold Time: 本示例输入180秒。
 - Keep Alive:本示例输入60秒。

更多信息,请参见配置BGP路由。

- 3. 启用BGP路由协议并为WAN口启用BGP。
 - i. 在动态路由配置详情区域,单击启用BGP协议。
 - ii. 在**切换路由协议**对话框,单击确定。
 - iii. 在端口展示区域,选择目标端口5(WAN),单击操作列的编辑。

- iv. 在BGP动态路由配置修改对话框,选择启用BGP,并配置对端IP和对端AS,然后单击确定。 本示例中对端IP和对端AS为WAN口连接的对端交换机的BGP AS号以及G11端口IP地址。
 - 对端AS: 本示例输入65430。
 - 对端IP: 本示例输入192.168.100.2。

BGP协议配置 🖉 编辑							
本端AS	65435			Router ID 192.1	68.2.2		
Hold Time	180			Keep Alive 60			
 动态路由配置详 自用OSPF协议 自用SPF协议 	请 义						
 ○ 不启用 端□ 		IDH05F	¥—7	连接分本	マム時行の	路中坊心	操作
			1 100	ALLINGVEN		不自用	(c):R
						Ten	370428
● 第□4 (LAN)	•		-		不屈用	编辑
● 端口5 (WA1	4)	192.168.100.1	192.168.100.2		65430	启用BGP	编辑

- 4. 配置线下路由同步方式。
 - i. 在智能接入网关实例详情页面, 单击网络配置页签。
 - ii. 在页签左侧区域,单击线下路由同步方式。
 - iii. 选择静态路由,然后单击添加静态路由,然后单击确定。

静态路由添加为本地IDC要和云上互通的网段: 172.16.0.0/12。

添加静态路由					
* 网段 👔					
172.16.0.0	1	12			
	确定	关闭			

步骤六:本地IDC配置

您需要为智能接入网关设备对端的三层交换机和出口路由器添加路由配置,此处以某品牌交换机和路由器为例。由于不同厂商交换机和路由器配置命令不同,详情请参见相关厂商的设备手册。

1. 三层交换机的路由配置。

```
interface GigabitEthernet 0/11
no switchport
ip address 192.168.100.2 255.255.255.252 #智能接入网关对端交换机的端口IP
interface GigabitEthernet 0/12
no switchport
ip address 192.168.110.1 255.255.255.252 #边界路由器对端交换机的端口IP
router bgp 65430
bgp router-id 192.168.1.1
network 172.16.0.0 mask 255.240.0.0
                                     #宣告本地IDC私网网段
neighbor 192.168.100.1 remote-as 65435
                                      #和智能接入网关建立BGP邻居关系
neighbor 192.168.100.1 timers 60 180
                                      #配置BGP路由协议的Keep Alive和Hold Time
neighbor 192.168.110.2 remote-as 45104
                                      #和边界路由器建立BGP邻居关系
exit
```

⑦ 说明 以上交换机路由配置为本示例内容。请根据您网络实际情况进行路由配置和网段宣告。

例如: 您本地IDC中包含多台三层交换机,交换机之间通过运行OSPF动态路由协议学习本地IDC私网 网段,您需要在和智能接入网关连接的三层交换机中进行OSPF和BGP路由协议的路由重分布操作,以便您本地IDC的所有三层交换机均能够通过OSPF路由协议学习到云上VPC网段,同时边界路由器实 例也能通过BGP协议学习到您本地IDC的所有私网网段。具体命令请参考您相应的厂商设备手册。

2. 出口路由器的路由配置。

ip route 192.168.100.0 255.255.255.252 192.168.80.2 #出口路由器去往智能接入网关的回程路由

步骤七: 配置云上网络连接

在配置好设备后,您需要配置云上网络连接,将本地IDC接入阿里云。

- 1. 创建云连接网。
 - i. 登录智能接入网关管理控制台。
 - ii. 在顶部菜单栏,选择**中国内地**区域。

云连接网区域需和智能接入网关设备使用区域保持一致。

- iii. 在左侧导航栏, 单击云连接网。
- iv. 在云连接网页面, 单击创建云连接网。
- v. 在创建云连接网面板, 配置云连接网名称, 然后单击确定。

云连接网名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)和短划线 (-)。

智能接入网关 / 云连接网				使用限制 (2 帮助文档
云连接网				
创建云连接网 C				実例ID ~ 清縮入 Q
实例ID/名称	绑定云企业网	鄉定智能接入网关	私网网段	操作
con-		0 / 0		御宠云企业网 删除

2. 绑定边界路由器和云连接网实例。

⑦ 说明 在智能接入网关作为物理专线备份链路的场景中,智能接入网关需先绑定边界路由器实例,然后再绑定云连接网实例,以防止路由冲突。

- i. 在左侧导航栏, 单击智能接入网关。
- ii. 在智能接入网关页面, 单击目标实例操作列的网络配置。
- iii. 在页签左侧区域,单击**绑定网络详情**。
- iv. 在绑定网络详情页签下,单击添加网络,选择边界路由器类型并在指定地域选择已创建的边界路 由器实例,然后单击确定。
- v. 请重复上述绑定步骤, 将已经创建的云连接网实例绑定到智能接入网关实例中。具体操作, 请参见 ^绑定网络实例。

在智能接入网关同时绑定云连接网实例和边界路由器实例的情况下,本地IDC优先通过物理专线和 云上进行互通。物理专线故障时,本地IDC则会通过云连接网和云上进行互通,即通过互联网加密 接入阿里云。

3. 创建云企业网。具体操作,请参见创建云企业网实例。

在您创建云企业网实例过程中,您需要加载一个网络实例,从已创建的VPC实例、云连接网实例或边界 路由器实例中选择一个即可。

4. 云企业网加载网络实例。具体操作,请参见加载网络实例。

本示例中需要将**华北2(北京)**地域的VPC实例、云连接网实例和边界路由器实例加载到同一云企业网中。加入后,VPC实例、云连接网实例和边界路由器实例的路由条目会自动发布到云企业网中,VPC实例、云连接网实例和边界路由器实例也能从云企业网中学习到其它实例的路由。

步骤八:配置健康检查

您需要为物理专线配置健康检查,健康检查会以您指定的发包时间间隔发送探测报文,当连续发送的所有探测报文(即您指定的探测报文个数)都丢包时,云企业网会主动将流量切换至SAG链路。

- 1. 登录云企业网管理控制台。
- 2. 在左侧导航栏, 单击健康检查。
- 3. 选择边界路由器的地域, 然后单击设置健康检查。

本示例选择华北2(北京)。

- 4. 在设置健康检查面板,根据以下信息配置健康检查,然后单击确定。
 - **云企业网实例**:选择边界路由器实例加载的云企业网实例。
 - 边界路由器 (VBR): 选择已创建的边界路由器实例。
 - 源IP: 本示例选择自动生成源IP。

使用自动生成源IP,系统将自动分配100.96.0.0/16地址段内IP地址,探测链路的连通性。

- 目标IP: 输入边界路由器实例中客户侧ⅠP地址。
- **发包时间间隔(秒)**:指定健康检查时发送连续探测报文的时间间隔。单位:秒。本示例使用默认值。

探测报文个数(个):指定健康检查时发送探测报文的个数。单位:个。本示例使用默认值。
 更多信息,请参见健康检查。

步骤九:连通性测试

完成以下操作,测试网络的连通性:

⑦ 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许本地IDC访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

- 1. 在本地IDC下, 打开客户端的命令行窗口。
- 2. 执行 ping 命令, ping 云上VPC 10.0.0.0/16网段下的ECS实例IP地址, 如果能接受到回复报文, 则 表示网络已经连通。

经验证,本地IDC和VPC可以正常通信。

[root@iZ	Z ~]# ping 10.0.2.210				
PING 10.0.2.210 (10.0.2.21	10) 56(84) bytes of data.				
64 bytes from 10.0.2.210:	icmp_seq=1 ttl=64 time=0.345 ms				
64 bytes from 10.0.2.210:	icmp_seq=2 ttl=64 time=0.237 ms				
64 bytes from 10.0.2.210:	icmp_seq=3 ttl=64 time=0.155 ms				
64 bytes from 10.0.2.210: ^Z	icmp_seq=4 ttl=64 time=0.161 ms				
[1]+ Stopped ping_10.0.2.210					
[root@iz	z ~]# [
3. 在本地IDC网关设备上,关闭物理专线端口,切断物理专线链接。再次执行 ping 命令,测试本地IDC 和VPC的连通性。

经验证,本地IDC和VPC仍可以正常通信。

[root@iZ	j iZ ~]# pir	ng 10.0.2.210	
PING 10.0.2.210 (10	.0.2.210) 56(84) b	bytes of data.	
64 bytes from 10.0.	2.210: icmp_seq=1	ttl=64 time=0.345	ms
64 bytes from 10.0.	2.210: icmp_seq=2	ttl=64 time=0.237	ms
64 bytes from 10.0.	2.210: icmp_seq=3	ttl=64 time=0.155	ms
64 bytes from 10.0.	2.210: icmp_seq=4	ttl=64 time=0.161	ms
^Z			
[1]+ Stopped	ping 10	0.0.2.210	
[root@iz	Z ~]# []		

3.3.1.2.7. IDC通过静态路由主备专线链路上云方案

本文介绍如何组合使用物理专线和云企业网CEN(Cloud Enterprise Network),实现本地数据中心 IDC(Internet Data Center)通过静态路由主备物理专线链路上云并和云上专有网络VPC(Virtual Private Cloud)互通。

方案概述

在企业上云过程中,一些企业会将复杂数据库集群、专业设备、高安全要求系统放在本地IDC中,前端应用 部署在阿里云上。在这种部署场景下,本地IDC和前端应用交互频繁,通常会对上云链路的时延、可靠性和 带宽容量有较高要求。

针对上述网络诉求, 阿里云为您提供以下两种解决方案:

- IDC通过静态路由主备专线链路上云方案
- IDC通过BGP主备专线链路上云方案

两种方案均通过主备物理专线将您本地IDC接入阿里云,在为您提供高可靠,低延迟连接的同时,可以有效 避免上云链路单点故障的问题。您可以根据本地IDC侧路由配置情况灵活选择使用静态路由或BGP动态路由上 云;同时,云企业网和物理专线均能提供多种带宽规格,满足您对带宽容量的高要求。

场景说明

本文以下图场景为例,为您介绍IDC通过静态路由主备物理专线链路上云方案。某企业在杭州拥有一个IDC, 其中部署有数据库集群等高级别业务系统;同时该企业已在阿里云华东1(杭州)地域创建了一个VPC,其中 通过云服务器ECS(Elastic Compute Service)等云服务部署了一些应用业务。现企业为实现云上云下平稳 互通,计划购买两条物理专线,分别连接到本地IDC不同的CPE设备和边界路由器VBR(Virtual border router)上,然后通过云企业网实现本地IDC和云上VPC的互通。其中本地IDC侧和VBR之间通过静态路由互 通,两条物理专线分别为主备链路将本地IDC接入阿里云。



准备工作

在您执行本文操作前,请先完成以下准备工作:

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经在阿里云华东1(杭州)地域部署了VPC。具体操作,请参见创建和管理专有网络。
- 本文示例中的网段规划如下表所示。您可以自行规划网段,请确保您的网段之间没有重叠。

项目	网段规划	服务器或客户端地址
本地IDC	10.1.1.0/24	客户端地址: 10.1.1.1
VPC	192.168.20.0/24	服务器地址: 192.168.20.161
VBR1	 ◇ VLAN ID: 0 ◇ 阿里云侧IPv4互联IP: 172.16.1.2/30 ◇ 客户侧IPv4互联IP: 172.16.1.1/30 	不涉及
VBR2	 ◇ VLAN ID: 0 ◇ 阿里云侧IPv4互联IP: 172.16.2.2/30 ◇ 客户侧IPv4互联IP: 172.16.2.1/30 	不涉及

配置流程



步骤一: 创建物理专线

您需要在华东1(杭州)地域申请两条物理专线,与本地CPE1连接的物理专线的名称为leasedline1,与本地 CPE2连接的物理专线的名称为leasedline2。具体操作,请参见创建和管理独享专线连接或共享专线连接概述。

• 如果第二个物理专线接口的接入点和第一个物理专线接口的接入点相同,选择第一条物理专线的专线ID作

为冗余物理专线(确保第一条物理专线的初装费已支付),可以避免两条物理专线接入同一台物理接入设备。

 如果第二个物理专线接口的接入点和第一个物理专线接口的接入点不同,两条线路默认形成冗余链路,不 需要再选择物理专线接口。

本示例使用独享专线连接,且两条物理专线的接入点不同。

步骤二: 创建VBR

完成以下操作,分别为两条物理专线创建VBR,作为数据从VPC到本地IDC的转发桥梁。

- 1. 登录高速通道管理控制台。
- 2. 在左侧导航栏,单击边界路由器(VBR)。
- 在顶部状态栏处,选择要创建的边界路由器的地域。
 本示例选择**华东1(杭州)**地域。
- 4. 在边界路由器 (VBR) 页面, 单击创建边界路由器。
- 5. 在创建边界路由器面板,根据以下信息配置边界路由器,然后单击确定。
 - 账号类型:本示例选择当前账号。
 - 名称:本示例输入VBR1。
 - 物理专线接口:选择申请的leasedline1接口。
 - $\circ~$ VLAN ID: 0.
 - 设置VBR带宽值:不限速
 - 阿里云侧IPv4互联IP: 172.16.1.2。
 - 客户侧IPv4互联IP: 172.16.1.1。
 - IPv4子网掩码: 255.255.255.252。
- 6. 重复上述步骤,为第二条物理专线创建边界路由器。

配置参数如下:

- 账号类型:本示例选择当前账号。
- 名称:本示例输入VBR2。
- 物理专线接口:选择申请的leasedline2接口。
- $\circ~$ VLAN ID: 0.
- 设置VBR带宽值:不限速
- 阿里云侧IPv4互联IP: 172.16.2.2。
- 客户侧IPv4互联IP: 172.16.2.1。
- IPv4子网掩码: 255.255.255.252。

步骤三: 配置VBR路由

您需要在VBR上配置指向本地IDC的路由。

- 1. 在边界路由器 (VBR) 页面, 单击目标边界路由器的ID。
- 2. 单击路由条目页签, 然后单击添加路由条目。
- 3. 在添加路由条目面板,根据以下信息配置路由条目,然后单击确定。

下一跳类型:选择物理专线接口。

- 目标网段: 输入本地IDC的网段。本示例输入10.1.1.0/24。
- 下一跳:选择物理专线leasedline1接口。
- 4. 重复上述步骤,为另一个VBR配置指向本地IDC的路由。

配置参数如下:

- 下一跳类型:选择物理专线接口。
- 目标网段: 输入本地IDC的网段。本示例输入10.1.1.0/24。
- 下一跳:选择物理专线leasedline2接口。

VBR路由如下表所示:

路由表项	VBR1	VBR2
目标网段	10.1.1.0/24	10.1.1.0/24
地一不	leasedline1接口	leasedline2接口

步骤四:加入云企业网

完成物理专线接入后,您需要将物理专线关联的VBR和要互通的VPC加入同一个云企业网中。

⑦ 说明 本教程使用云企业网的旧版控制台。关于如何进入旧版控制台,请参见旧版控制台使用说明。

- 1. 登录云企业网管理控制台。
- 2. 在云企业网实例页面,创建云企业网实例。具体操作,请参见创建云企业网实例。
- 3. 在云企业网实例页面,找到已创建的云企业网实例,在操作列单击管理。
- 4. 单击网络实例管理页签, 然后单击加载网络实例加载物理专线关联的VBR和要互通的VPC。

本示例中需要将VBR1、VBR2、VPC加载到同一云企业网中。加入后,VPC和VBR实例的路由条目会自动 发布到云企业网中,VPC和VBR实例能从云企业网中学习对方的路由。具体操作,请参见加载网络实 例。

5. 如果VPC中存在指向ECS实例、VPN网关、HAVIP等路由条目,请根据连通性需求,在VPC控制台将这些路由发布到云企业网中。

具体操作,请参见发布路由至云企业网。

云企业网路由如下表所示:

目标网段	下一跳
10.1.1.0/24	VBR1
10.1.1.0/24	VBR2

步骤五: 配置路由策略

完成以下步骤,设置VBR1所在连接的物理专线为主用线路,VBR2所连接的物理专线为备用线路。

1. 在云企业网实例页面,找到目标云企业网实例,在操作列单击管理。

2. 在云企业网页面,单击路由策略页签,然后单击添加路由策略。

3. 在添加路由策略页面,根据以下信息配置路由策略,然后单击确定。

添加路由策略	?	\times
* 策略优先级 ⑦ 20 描述 ⑦		
* 地域 ⑦		
华东1 (杭州) 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇 〇〇		
* 应用方向 ⑦ 入地域网关		
匹 配条件		
iii iii iii iii iii iii iii iii iii ii		
* 策略行为 ⑦ ● 允许 〇 拒绝		
路由优先级 > ⑦		
10		
▋ 添加策略值		
关联策略优先级 ⑦		

- 策略优先级:路由策略的优先级。优先级数字越小,优先级越高。本示例输入20。
- 地域:选择路由策略应用的地域。本示例输入**华东1(杭州)**。
- 应用方向:选择路由策略应用的方向。本示例选择入地域网关。
- 匹配条件:路由策略的匹配条件。本示例设置源实例ⅠD列表为VBR1实例ⅠD。
- **策略行为**:选择策略行为。本示例选择**允许**。
- 执行动作:设置允许通过的路由的优先级。本示例设置路由优先级为10。

默认情况下,允许通过的路由的优先级为50。您可以设置路由的优先级,取值范围为1~100,取值越小,优先级越高。

4. 重复上述步骤,为第二个VBR配置路由策略。

添加路由策略	?	\times
* 策略优先级 ⑦ 30		
描述 ⑦		
* 地域 ⑦		
华东1 (杭州) ~		
* 应用方向 ⑦ 入地域网关		
匹配条件		
源实例ID列表 ∨ ^⑦ □ 排除匹配		
vbr.		
 ■ 添加匹配条件 * 策略行为 ⑦ ● 允许 ○ 拒绝 		
路由优先级 V ^⑦ 20		
关联策略优先级 ⑦		

- 策略优先级:路由策略的优先级。优先级数字越小,优先级越高。本示例输入30。
- 地域:选择路由策略应用的地域。本示例输入**华东1(杭州)**。
- **应用方向**:选择路由策略应用的方向。本示例选择入地域网关。
- 匹配条件:路由策略的匹配条件。本示例设置源实例ⅠD列表为VBR2实例ⅠD。
- **策略行为**:选择策略行为。本示例选择**允许**。
- 执行动作:设置允许通过的路由的优先级。本示例设置路由优先级为20。

⑦ 说明 默认情况下,允许通过的路由的优先级为50。您可以设置路由的优先级,取值范围为 1~100,取值越小,优先级越高。

添加路由策略后,您可以在路由信息页签下查看去往10.1.1.0/24的两条路由,其中一条为备用路由。

地域 > 华东1 (杭州)	✓ 刷新				
目标网段	路由类型	匹配策略	路由属性	状态	下一跳
10.1.1.0/24	云企业网	查看详情	查看详情	可用	华东1 (杭州)
10.1.1.0/24	云企业网	查看详情	查看详情	Standby	华东1 (杭州)
100.64.0.0/10	系统	-	查看详情	可用	华东1 (杭州)
192.168.20.0/24	云企业网	-	查看详情	可用	华东1(杭州)

步骤六:配置健康检查

主备物理专线接入时,您需要配置健康检查。健康检查会以您指定的发包时间间隔发送探测报文,当连续发送的所有探测报文(即您指定的探测报文个数)都丢包时,云企业网会主动将流量切换至另一条物理专线。

- 1. 返回到云企业网实例页面。
- 2. 在左侧导航栏, 单击健康检查。
- 3. 选择VBR的地域,然后单击设置健康检查。
- 4. 在设置健康检查面板,根据以下信息配置健康检查,然后单击确定。
 - 云企业网实例:选择边界路由器加载的云企业网实例。
 - 边界路由器 (VBR): 选择要监控的边界路由器。
 - 源IP: 本示例选择自动生成源IP。

使用自动生成源IP,系统将自动分配100.96.0.0/16地址段内IP地址,探测链路的连通性。

- 目标IP: 输入本地IDC网络设备的接口IP。
- **发包时间间隔(秒)**:指定健康检查时发送连续探测报文的时间间隔。单位:秒。本示例使用默认值。
- 探测报文个数(个):指定健康检查时发送探测报文的个数。单位:个。本示例使用默认值。
- 5. 重复上述步骤,为第二个VBR配置健康检查。

步骤七:本地IDC侧配置

您需要在本地IDC侧完成以下配置,实现主备物理专线接入。以下配置示例仅供参考,不同厂商的设备配置 命令可能会有所不同。具体命令,请咨询相关设备厂商。

#设置本地IDC去往云上的路由的优先级,使流量优先走物理专线leasedline1,物理专线leasedline2为备用链路 ip route 192.168.0.0/16 172.16.1.2 preference 10 ip route 192.168.0.0/16 172.16.2.2 preference 20 #配置健康检查探测报文的回程路由 ip route 100.96.0.0 255.255.0.0 172.16.1.2 #在CPE1上配置健康检查探测报文的回程路由 ip route 100.96.0.0 255.255.0.0 172.16.2.2 #在CPE2上配置健康检查探测报文的回程路由

步骤八: 连通性测试

完成以下操作,测试主备物理专线的连通性:

⑦ 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许本地IDC访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

1. 在本地IDC下, 打开客户端的命令行窗口。

2. 执行 ping 命令, ping 云上VPC 192.168.20.0/24网段下的ECS实例IP地址,如果能接受到回复报 文,则表示网络能正常连通。

经验证,本地IDC可以与VPC正常通信。

[root@iZbj Z	~]# ping 192.168.20.161
PING 192.168.20.161 (192.168.2	20.161) 56(84) bytes of data.
64 bytes from 192.168.20.161:	<pre>icmp_seq=1 ttl=64 time=2.00 ms</pre>
64 bytes from 192.168.20.161:	<pre>icmp_seq=2 ttl=64 time=1.88 ms</pre>
64 bytes from 192.168.20.161:	<pre>icmp_seq=3 ttl=64 time=1.85 ms</pre>
64 bytes from 192.168.20.161:	<pre>icmp_seq=4 ttl=64 time=1.84 ms</pre>
^Z	
[1]+ Stopped	ping 192.168.20.161
[root@iZZ	~]# [

3. 在本地IDC网关设备上,关闭一个物理专线端口(如VBR1到CPE1),再次执行 ping 命令,测试本地 IDC和VPC的连通性。

经验证,本地IDC和VPC仍可以正常通信。

[root@iZbj Z	~]# ping 192.168.20.161
PING 192.168.20.161 (192.168.2	20.161) 56(84) bytes of data.
64 bytes from 192.168.20.161:	<pre>icmp_seq=1 ttl=64 time=2.00 ms</pre>
64 bytes from 192.168.20.161:	<pre>icmp_seq=2 ttl=64 time=1.88 ms</pre>
64 bytes from 192.168.20.161:	icmp_seq=3 ttl=64 time=1.85 ms
64 bytes from 192.168.20.161:	icmp_seq=4 ttl=64 time=1.84 ms
^Z	
[1]+ Stopped	ping 192.168.20.161
[root@iZZ	~]# [

4. 您也可以执行 tracert 命令,通过路由跟踪可以查看到云企业网会对路由进行切换,本地IDC通过 VBR2和云上VPC互通。

不同的设备,路由追踪命令会有所不同,具体请咨询相关设备厂商。

3.3.1.2.8. IDC通过BGP主备专线链路上云方案

本文介绍如何组合使用物理专线和云企业网CEN(Cloud Enterprise Network),实现本地数据中心 IDC(Internet Data Center)通过BGP主备专线链路上云并和云上专有网络VPC(Virtual Private Cloud)互通。

方案概述

在企业上云过程中,一些企业会将复杂数据库集群、专业设备、高安全要求系统放在本地IDC中,前端应用 部署在阿里云上。在这种部署场景下,本地IDC和前端应用交互频繁,通常会对上云链路的时延、可靠性和 带宽容量有较高要求。

针对上述网络诉求, 阿里云为您提供以下两种解决方案:

- IDC通过静态路由主备专线链路上云方案
- IDC通过BGP主备专线链路上云方案

两种方案均通过主备物理专线将您本地IDC接入阿里云,在为您提供高可靠,低延迟连接的同时,可以有效 避免上云链路单点故障的问题。您可以根据本地IDC侧路由配置情况灵活选择使用静态路由或BGP动态路由上 云;同时,云企业网和物理专线均能提供多种带宽规格,满足您对带宽容量的高要求。

场景说明

本文以下图场景为例,为您介绍IDC通过BGP主备专线链路上云方案。某企业在杭州拥有一个IDC,其中部署 有数据库集群等高级别业务系统;同时该企业已在阿里云华东1(杭州)地域创建了一个VPC,其中通过云服 务器ECS(Elastic Compute Service)等云服务部署了一些应用业务。现企业为实现云上云下平稳互通,计 划购买两条物理专线,分别连接到本地IDC不同的CPE(Customer-premisesequipment)设备和边界路由器 VBR(Virtual border router)上,然后通过云企业网实现本地IDC和云上VPC的互通。其中两条专线分别为主 备链路将本地IDC接入上云,本地IDC侧和VBR之间通过BGP动态路由互通并开启双向转发检测 BFD(Bidirectional Forwarding Detection)功能,实现本地IDC与VPC之间路由的快速收敛,提高网络的可 用性。



准备工作

在您执行本文操作前,请先完成以下准备工作:

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经部署了专有网络VPC,且已部署了业务应用。具体操作,请参见创建和管理专有网络。
- 您已提交工单申请并获得使用BFD功能的权限。
- 本文示例中的网段规划如下表所示。您可以自行规划网段,请确保您的网段之间没有重叠。

机构	网段规划	服务器或客户端地址
本地IDC	10.1.1.0/24	客户端地址: 10.1.1.1
VPC	192.168.20.0/24	服务器地址: 192.168.20.161
VBR1	 VLAN: 110 阿里云侧IPv4互联IP: 172.16.1.2/30 客户侧IPv4互联IP: 172.16.1.1/30 	不涉及
VBR2	 VLAN: 120 阿里云侧IPv4互联IP: 172.16.2.2/30 客户侧IPv4互联IP: 172.16.2.1/30 	不涉及

配置流程





步骤一: 创建物理专线

您需要在华东1(杭州)地域申请两条物理专线,与本地CPE1连接的物理专线的名称为leasedline1,与本地 CPE2连接的物理专线的名称为leasedline2。具体操作,请参见创建和管理独享专线连接或共享专线连接概述。

- 如果第二个物理专线接口的接入点和第一个物理专线接口的接入点相同,选择第一条物理专线的专线ID作为冗余物理专线(确保第一条物理专线的初装费已支付),可以避免两条物理专线接入同一台物理接入设备。
- 如果第二个物理专线接口的接入点和第一个物理专线接口的接入点不同,两条线路默认形成冗余链路,不 需要再选择物理专线接口。

本示例使用独享专线连接,且两条物理专线的接入点不同。

步骤二: 创建VBR

完成以下操作,分别为两条物理专线创建VBR,作为数据从VPC到本地IDC的转发桥梁。

- 1. 登录高速通道管理控制台。
- 2. 在左侧导航栏,单击边界路由器 (VBR)。
- 在顶部菜单栏,选择要创建的VBR的地域。
 本示例选择**华东1(杭州)**地域。
- 4. 在边界路由器 (VBR) 页面, 单击创建边界路由器。
- 5. 在创建边界路由器面板,根据以下信息配置VBR,然后单击确定。
 - 账号类型:本示例选择当前账号。
 - 名称:本示例输入VBR1。
 - 物理专线接口:选择申请的其中一个专线接口。
 - VLANID: 110.
 - 阿里云侧IPv4互联IP: 172.16.1.2。
 - 客户侧IPv4互联IP: 172.16.1.1。
 - IPv4子网掩码: 255.255.255.252。
- 6. 重复上述步骤,为第二条物理专线创建VBR实例。

配置参数如下:

- 账号类型:本示例选择当前账号。
- 名称:本示例输入VBR2。
- 物理专线接口:选择申请的另一个专线接口。
- VLANID: 120.
- **阿里云侧IPv4互联IP**: 172.16.2.2。
- 客户侧IPv4互联IP: 172.16.2.1。
- IPv4子网掩码: 255.255.255.252。

步骤三:加入云企业网

完成物理专线接入后,您需要将物理专线关联的VBR和要互通的VPC加入同一个云企业网中。

⑦ 说明 本文中关于云企业网的配置均在旧版控制台操作。

- 1. 登录云企业网管理控制台。
- 2. 在云企业网实例页面,创建云企业网实例。具体操作,请参见创建云企业网实例。
- 3. 在云企业网实例页面,找到目标云企业网实例,在操作列单击管理。
- 4. 在**云企业网**页面,单击网络实例管理页签,然后单击加载网络实例加载专线关联的VBR和要互通的 VPC。

本示例中需要将VBR1、VBR2、VPC加载到同一云企业网中。加入后,VPC和VBR实例的路由条目会自动 发布到云企业网中,VPC和VBR实例能从云企业网中学习对方的路由。具体操作,请参见加载网络实 例。

5. 如果VPC中存在指向ECS实例、VPN网关、HAVIP等路由条目,请根据连通性需求,在VPC控制台将这些路由发布到云企业网中。

具体操作,请参见发布路由至云企业网。

步骤四:配置路由

您需要在本地IDC和VBR之间配置BGP,并且您可以在本地IDC侧通过设置AS-Path的长度来确定路由选路的优先级。

1. 在IDC和VBR之间分别建立起BGP邻居关系并宣告路由。具体操作,请参见配置和管理BGP。

阿里云侧BGP ASN (Autonomous System Number)为45104,可接受本地IDC侧传递2字节或4字节的ASN。

2. IDC侧配置向阿里云宣告的BGP路由(10.1.1.0/24),并通过设置AS-Path来确定选路权重,实现阿里云 到IDC路由的主备模式。

设置CPE1所连接的专线为主链路,CPE2所连接的专线为备份链路。您可以通过设置AS-Path的长度来确定路由选路的优先级。AS-Path长度越短,优先级越高。IDC侧分别在两个CPE的BGP配置如下表所示,具体命令请咨询相应厂商。

配置	CPE1	CPE2
Vlan Tag	110	120
Network	10.1.1.0/24	10.1.1.0/24
BGP ASN	6***3	6***4
Interface IP	172.16.1.1/24	172.16.2.1/24
AS-Path	В, А	С, В, А

云企业网具备自动学习分发路由的能力,在配置好路由后,云企业网会基于选路权重等信息,将路由同步到 云企业网内部,各节点路由学习说明如下。

● VBR的BGP路由信息

路由表项	VBR1	VBR2
目标网段	10.1.1.0/24	10.1.1.0/24
下一跳	172.16.1.1	172.16.2.1

如上表所示,在VBR1和VBR2中可以看到从对端邻居学到的路由信息和下一跳。由于VBR已经加载到云企业网中,所以VBR会将从IDC侧学来的BGP路由信息发送到云企业网,包括AS-Path。

● 全量路由配置说明

CPE路由配置			
配置	CPE1	CPE2	
Vlan Tag	110	120	
Network	10.1.1.0/24	10.1.1.0/24	
BGP ASN	6***3	6***4	
Interface IP	172.16.1.1/24	172.16.2.1/24	
AS-Path	В, А	С, В, А	
VBR路由条目			
配置	VBR1	VBR2	
目标网段	10.1.1.0/24	10.1.1.0/24	
下一跳	172.16.1.1	172.16.2.1	
IDC路由条目			
目标网段	192.168.20.0/24		
下一跳	i. 172.16.1.2 ii. 172.16.2.2		
CEN路由条目			
目标网段	10.1.1.0/24		
下一跳	VBR1		

由于VBR和VPC均已加载到云企业网中,那么从VBR上学来的BGP路由也会发布到云企业网中,云企业网会基于选路权重等信息,将路由同步到云企业网内部。

两个VBR从IDC侧学习到的BGP路由目标网段一致,但路由权重不同,VBR1作为主链路(AS-Path 短),VBR2是备链路(AS-Path长)。云企业网学习到该路由后,会将该路由的属性通知到云企业网中的 其他网络实例,例如VPC。从VPC的路由表中就可以看到去往10.1.1.0/24的路由均指向VBR1。 云企业网也会将云企业网内系统路由发布到BGP中,所以在IDC的BGP路由表中就可以看到学习到的云企业 网中的路由信息,并且下一跳分别指向与IDC建立邻居的两个VBR的接口IP。

同理,如果想从IDC侧设置到阿里云VPC的地址192.168.20.0/24的主备链路,同样可以通过BGP选路属性,在IDC侧分别设置从不同邻居VBR1、VBR2学习到的路由192.168.20.0/24的权重,便可实现从IDC到阿里云的主备选路。

步骤五: 配置健康检查

主备物理专线接入时,您需要配置健康检查。健康检查会以您指定的发包时间间隔发送探测报文,当连续发送的所有探测报文(即您指定的探测报文个数)都丢包时,云企业网会主动将流量切换至另一条物理专线。

- 1. 返回到云企业网实例页面。
- 2. 在左侧导航栏,单击健康检查。
- 3. 选择VBR的地域,然后单击设置健康检查。
- 4. 在设置健康检查面板,根据以下信息配置健康检查,然后单击确定。
 - 云企业网实例:选择VBR实例加载的云企业网实例。
 - 边界路由器 (VBR): 选择要监控的VBR实例。
 - 源IP:选择自定义源IP,输入所连接的VPC中交换机下的一个空闲IP。
 - 目标IP: 输入本地IDC网络设备的接口IP。
 - 发包时间间隔(秒):采用默认值2秒。
 - 探测报文个数(个):采用默认值8个。
- 5. 重复上述步骤,为第二个VBR配置健康检查。

步骤六: VBR开启BFD

通过在VBR上配置BFD, 实现路由的快速收敛。

- 1. 登录高速通道管理控制台。
- 2. 在左侧导航栏,单击边界路由器(VBR)。
- 3. 在边界路由器(VBR)页面,在目标VBR实例操作列单击编辑。
- 4. 在修改边界路由器面板,根据以下信息设置BFD参数,然后单击确定。
 - 发送间隔: BFD报文的发送间隔, 单位: ms。本示例使用默认值1000ms。
 - 接收间隔: BFD报文的接收间隔, 单位: ms。本示例使用默认值1000ms。
 - 检测时间倍数:指接收方允许发送方发送报文的最大连接丢包个数。本示例使用默认值3。
- 5. 返回边界路由器(VBR)页面,单击目标VBR实例ID。
- 6. 在VBR实例详情页面,单击BGP邻居页签。
- 7. 单击目标BGP邻居操作列下的编辑。
- 8. 在修改BGP邻居面板,选中启用BFD复选框并配置BFD跳数,然后单击确定。

⑦ 说明 BFD功能支持自定义单跳或多跳会话。您可以根据真实的物理链路因素来配置不同的跳数。

步骤七:连通性测试

完成以下操作,测试主备物理专线的连通性。

② 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许本地IDC访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

- 1. 在本地IDC下, 打开客户端的命令行窗口。
- 2. 执行 ping 命令, ping 云上VPC 192.168.20.0/24网段下的ECS实例IP地址,如果能接受到回复报 文,则表示网络能正常连通。

经验证,本地IDC可以与VPC正常通信。

[root@iZbpZ	~]# ping 192.168.20.161
PING 192.168.20.161 (192.168.2	20.161) 56(84) bytes of data.
64 bytes from 192.168.20.161:	<pre>icmp_seq=1 ttl=64 time=2.00 ms</pre>
64 bytes from 192.168.20.161:	<pre>icmp_seq=2 ttl=64 time=1.88 ms</pre>
64 bytes from 192.168.20.161:	<pre>icmp_seq=3 ttl=64 time=1.85 ms</pre>
64 bytes from 192.168.20.161:	<pre>icmp_seq=4 ttl=64 time=1.84 ms</pre>
^Z	
[1]+ Stopped	ping 192.168.20.161
[root@iZZ	~]# [

3. 在本地IDC网关设备上,关闭一个物理专线端口(如VBR1到CPE1),再次执行 ping 命令,测试本地 IDC和VPC的连通性。

经验证,本地IDC和VPC仍可以正常通信。

[root@iZb; Z ~]# ping 192.168.20.161	
PING 192.168.20.161 (192.168.20.161) 56(84) bytes of data.	
64 bytes from 192.168.20.161: icmp_seq=1 ttl=64 time=2.00 ms	
64 bytes from 192.168.20.161: icmp_seq=2 ttl=64 time=1.88 ms	
64 bytes from 192.168.20.161: icmp_seq=3 ttl=64 time=1.85 ms	
64 bytes from 192.168.20.161: icmp_seq=4 ttl=64 time=1.84 ms	
^Z	
[1]+ Stopped ping 192.168.20.161	
[root@iZZ ~]# [

4. 您也可以执行 tracert 命令,通过路由跟踪可以查看到云企业网会对路由进行切换,本地IDC通过 VBR2和云上VPC互通。

不同的设备,路由追踪命令会有所不同,具体请咨询相关设备厂商。

3.3.1.3. 跨地域互通

3.3.1.3.1. 跨地域VPC间互通方案

本文为您介绍如何使用云企业网CEN(Cloud Enterprise Network),实现跨地域专有网络VPC(Virtual Private Cloud)间互通。

方案概述

在企业上云过程中,可能会需要在海外地域部署云服务,实现业务出海;同时,也会需要海外云服务可以和 国内云服务互通。云企业网提供一种能够快速构建混合云和分布式业务系统的全球网络的方法,帮助您打造 一张具有企业级规模和通信能力的云上网络。

本文以下图场景为例,为您介绍跨地域VPC间互通方案。某企业已经在阿里云华东1(杭州)地域创建了两个 VPC,其中已在VPC的云服务器ECS(Elastic Compute Service)上部署了应用业务系统。企业因业务扩展, 也已在华北1(青岛)地域和美国(硅谷)地域创建了VPC,实现业务出海。现企业需要国内VPC与海外VPC 可以全互通。



准备工作

开始前,请确保您已经满足以下条件:

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经在阿里云华东1(杭州)地域部署了两个VPC、华北1(青岛)地域部署了一个VPC以及美国(硅谷)地域部署了一个VPC,且其中均已部署有ECS服务器。具体操作,请参见创建和管理专有网络。
- 您已经通过跨境产品售卖合规检查。更多信息,请参见【售卖迁移】云企业网跨境带宽包售卖迁移公告。
- 本文示例中, 网段规划如下表所示。您可以自行规划网段, 请确保您的网段之间没有重叠。

规划目标	网段规划	IP地址
华东1(杭州)VPC1	 ○ 主网段: 192.168.0.0/16 ○ 交换机1网段: 192.168.20.0/24 ○ 交换机2网段: 192.168.21.0/24 	192.168.20.161
华东1(杭州)VPC2	 ○ 主网段: 172.16.0.0/16 ○ 交换机3网段: 172.16.0.0/24 ○ 交换机4网段: 172.16.1.0/24 	172.16.1.188
华北1(青岛)VPC	∘ 主网段: 10.0.0.0/16 ∘ 交换机5网段: 10.0.1.0/24	10.0.1.106
美国(硅谷)VPC	 ○ 主网段: 192.168.0.0/16 ○ 交换机6网段: 192.168.0.0/24 ○ 交换机7网段: 192.168.1.0/24 	192.168.1.227

⑦ 说明 本教程使用的为云企业网旧版控制台。更多信息,请参见旧版控制台使用说明。

配置步骤



步骤一: 创建云企业网实例

- 1. 登录云企业网管理控制台。
- 2. 在云企业网实例页面,单击创建云企业网实例。
- 3. 在创建云企业网实例面板,根据以下信息配置云企业网实例,然后单击确定。
 - 名称: 输入云企业网实例的名称。

名称在2~128个字符之间,以英文字母或中文开始,可包含数字、短划线(-)和下划线(_),但不能以 http:// 和 https:// 开始。

• 描述: 输入云企业网实例的描述。

描述在2~256个字符之间,不能以 http:// 或者 https:// 开头,只能以中文或者英文大小写字 母开始,可包含数字、短划线(-)、半角句号(.)和下划线(_)。

- 加载网络实例:在您创建云企业网实例的过程中,您可以将您当前账号下的一个网络实例直接加载 到云企业网实例中。云企业网支持加载VPC实例、边界路由器实例和云连接网实例。本示例首先将 VPC1加载到云企业网中。
 - 实例类型:选择要加载的实例类型。本示例选择专有网络(VPC)。
 - 地域:选择目标实例所在的地域。本示例选择**华东1(杭州)**。
 - 网络实例:选择目标实例。本示例选择VPC1。

步骤二:加载VPC网络实例

创建云企业网实例后,您需要将要互通的网络实例都加入到云企业网实例中,云企业网实例可帮您构建一张 云上互通网络。

- 1. 在云企业网实例页面,单击已创建的云企业网实例ID。
- 2. 在网络实例管理页签, 单击加载网络实例。
- 3. 在加载网络实例面板的同账号页签下,根据以下信息加载网络实例,然后单击确定。
 - **实例类型**:选择要加载的实例类型。本示例选择专有网络(VPC)。
 - 地域:选择目标实例所在的地域。本示例选择**华东1(杭州)**。
 - 网络实例:选择目标实例。本示例选择VPC2。
- 4. 请重复步骤,将华北1(青岛)地域的VPC和美国(硅谷)地域的VPC加入到已创建的云企业网中。

步骤三:购买带宽包

加入云企业网中的网络实例,同地域网络实例可直接互通,跨地域网络实例需购买带宽包并设置跨地域带宽才能互通。请完成以下操作,购买带宽包。

- 1. 在云企业网实例页面,单击目标云企业网实例ID。
- 2. 在云企业网页面,单击带宽包管理页签,然后单击购买带宽包(预付费)。
- 3. 在购买页面,选择带宽包的类型。本示例选择跨境。

• 非跨境:指中国内地到中国内地的带宽包或境外区域到境外区域的带宽包,例如北美到亚太。

○ **跨境**:指中国内地到境外区域的带宽包,例如中国内地到北美。

注意 涉及跨境(中国内地至境外、中国内地至中国香港)的云企业网带宽包由中国联通运营,购买后只支持续费降配,不支持退款,请提前做好规划和测试。

- 4. 根据以下信息配置带宽包,然后单击**立即购买**并完成支付。
 - 云企业网: 系统自动选择当前的云企业网实例。
 - 区域-A:选择参与互通的网络实例所在区域。本示例选择中国内地。
 - 区域-B:选择参与互通的网络实例所在区域。本示例选择北美。

↓ 注意 带宽包创建后,无法修改互通区域。

- **计费方式**:带宽包的计费方式。默认值**按带宽**。关于计费的更多信息,请参见计费说明。
- 带宽值:请根据业务需要,选择区域互通的带宽,最小为2 Mbps。
- 带宽包名称: 输入带宽包的名称。
- **购买时长:**选择预付费带宽包的购买时长。默认值为1个月,您可以选中到期自动续费开启预付费
 带宽包的自动续费功能。
- 资源组:选择带宽包所属的资源组。仅购买非跨境的带宽包时,支持配置该项。

带宽包购买完成后,会自动绑定到当前云企业网实例上。

步骤四:设置跨地域带宽

- 1. 在云企业网实例页面,单击目标云企业网实例ID。
- 2. 在云企业网页面,单击跨地域互通带宽管理页签,然后单击设置跨地域带宽。
- 3. 在设置跨地域带宽面板,根据以下信息配置跨地域互通带宽,然后单击确定。
 - 带宽包:选择已绑定至云企业网实例的带宽包。本示例选择中国内地与中国内地。
 - 互通地域:选择需要互通的地域。本示例选择华东1(杭州) ⇒华北1(青岛)。
 - 带宽:选择跨地域互通带宽的带宽值。单位: Mbps。
- 4. 请重复步骤,分别设置华东1(杭州)至美国(硅谷)和华北1(青岛)至美国(硅谷)的互通带宽。

⑦ 说明 每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽值。

例如,一个云企业网实例绑定了一个带宽值为20 Mbps,互通区域为中国内地和北美的带宽包。您可以在该带宽包内设置美国(硅谷)到华东1(杭州)、华北1(青岛)等地域的跨地域互通带宽, 但所有跨地域互通带宽之和不大于20 Mbps。

步骤五: 连通性测试

完成以下操作,测试网络的连通性:

② 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许VPC中的ECS实例可以互访。具体操作,请参见查询安全组规则。

- 1. 登录VPC1中的ECS实例。具体操作,请参见连接方式概述ECS远程连接操作指南。
- 2. 执行 ping 命令, ping VPC2的服务器172.16.1.188, 如果能接收到回复报文, 则表示网络连接成

功。

经验证, VPC1和VPC2可正常通信。

[root@iZb; 5Z ~]# ping 172.16.1.188
PING 172.16.1.188 (172.16.1.188) 56(84) bytes of data.
64 bytes from 172.16.1.188: icmp_seq=1 ttl=64 time=2.16 ms
64 bytes from 172.16.1.188: icmp_seq=2 ttl=64 time=2.06 ms
64 bytes from 172.16.1.188: icmp_seq=3 ttl=64 time=2.08 ms
64 bytes from 172.16.1.188: icmp_seq=4 ttl=64 time=2.08 ms
72
[4]+ Stopped ping 172.16.1.188
[root@iZb; 5Z ~]# []

3. 保持在VPC1的ECS实例中,执行 ping 命令, ping 华北1(青岛) VPC的服务器地址10.0.1.106,如 果能接收到回复报文,则表示网络连接成功。

经验证, VPC1和华北1(青岛) VPC可正常通信。

[root@iZbp252	~]# ping 10.0.1.106
PING 10.0.1.106 (10.0.1.106)	56(84) bytes of data.
64 bytes from 10.0.1.106: icm	p_seq=1 ttl=64 time=24.3 ms
64 bytes from 10.0.1.106: icm	p_seq=2 ttl=64 time=24.3 ms
64 bytes from 10.0.1.106: icm	p_seq=3 ttl=64 time=24.2 ms
64 bytes from 10.0.1.106: icm	p_seq=4 ttl=64 time=24.2 ms
^Z	
[5]+ Stopped	ping 10.0.1.106
[root@iZbp14\Lfj25Z	:~]# []

4. 依旧在VPC1的ECS实例中,执行 ping 命令, ping 美国(硅谷)VPC的服务器地址192.168.1.227, 如果能接收到回复报文,则表示网络连接成功。

经验证, VPC1和美国(硅谷) VPC可正常通信。

[root@iZbp25Z	. ~]# ping 192.168.1.227
PING 192.168.1.227 (192.168.1	227) 56(84) bytes of data.
64 bytes from 192.168.1.227:	<pre>icmp_seq=1 ttl=64 time=140 ms</pre>
64 bytes from 192.168.1.227:	<pre>icmp_seq=2 ttl=64 time=140 ms</pre>
64 bytes from 192.168.1.227:	icmp_seq=3 ttl=64 time=140 ms
64 bytes from 192.168.1.227:	<pre>icmp_seq=4 ttl=64 time=140 ms</pre>
^Z	
[7]+ Stopped	ping 192.168.1.227
[root@iZbp14\25Z	:~]# []

5. 登录华北1(青岛) VPC的ECS实例中,执行 ping 命令, ping 美国(硅谷) VPC的服务器地址 192.168.1.227,如果能接收到回复报文,则表示网络连接成功。

经验证, 华北1(青岛) VPC和美国(硅谷) VPC可正常通信。

3.3.1.3.2. 跨地域IDC上云互通方案

本文为您介绍如何使用云企业网CEN(Cloud Enterprise Network),实现跨地域的本地数据中心 IDC(Internet Data Center)上云互通。

方案概述

在企业发展过程中,企业可能会需要在海外创建分支机构,实现业务出海。同时,也会需要海外机构可以和 国内总部互通。云企业网提供一种能够快速构建混合云和分布式业务系统的全球网络的方法,帮助您打造一 张具有企业级规模和通信能力的云上网络。

本文以下图场景为例,为您介绍跨地域IDC上云互通方案。某企业在杭州拥有一个IDC,且企业已经在阿里云 华东1(杭州)地域创建了一个专有网络VPC(Virtual Private Cloud),其中已在云服务器ECS(Elastic Compute Service)上部署了应用业务系统。现企业因业务扩展,已在海外创建了一个IDC作为海外总部。企 业需要国内IDC、海外总部与云上VPC可以全互通,其中企业计划通过物理专线分别将杭州IDC和新加坡IDC接 入阿里云,物理专线可为企业IDC提供高可靠的上云链路。



准备工作

在您执行本文操作前,请先完成以下准备工作:

- 您已经注册了阿里云账号。如未注册,请先完成账号注册。
- 您已经在阿里云华东1(杭州)地域部署了VPC。具体操作,请参见创建和管理专有网络。
- 您已经通过跨境产品售卖合规检查。更多信息,请参见【售卖迁移】云企业网跨境带宽包售卖迁移公告。
- 本文示例中的网段规划如下表所示。您可以自行规划网段,请确保您的网段之间没有重叠。

配置项	网段规划	服务器IP地址
IDC1	10.2.1.0/24	10.2.1.204
IDC2	10.2.2.0/24	10.2.2.200
VBR1	 ◇ VLAN: 0 ◇ 阿里云侧IPv4互联IP: 172.16.1.2/30 ◇ 客户侧IPv4互联IP: 172.16.1.1/30 	不涉及
VBR2	 ◇ VLAN: 0 ◇ 阿里云侧IPv4互联IP: 172.16.2.2/30 ◇ 客户侧IPv4互联IP: 172.16.2.1/30 	不涉及

配置项	网段规划	服务器IP地址
VPC	192.168.20.0/24	192.168.20.161

配置流程



步骤一: 创建物理专线

您需要在华东1(杭州)地域和新加坡地域分别申请一条物理专线,与杭州IDC的CPE1(Customerpremisesequipment)设备连接的物理专线的名称为leasedline1,与新加坡地域CPE2连接的物理专线的名称 为leasedline2。具体操作,请参见创建和管理独享专线连接或共享专线连接概述。

步骤二: 创建VBR

边界路由器VBR(Virtual border router)是IDC中CPE设备和阿里云接入点连接的一个路由器,作为数据从 IDC到阿里云机房之间的桥梁。物理专线的一端连接到您IDC的CPE设备,另一端连接到边界路由器。

- 1. 登录高速通道管理控制台。
- 2. 在左侧导航栏,单击边界路由器(VBR)。
- 3. 在顶部状态栏,选择要创建的VBR的地域。

本示例选择华东1(杭州)地域。

- 4. 在边界路由器 (VBR) 页面, 单击创建边界路由器。
- 5. 在创建边界路由器面板,根据以下信息配置边界路由器,然后单击确定。
 - 账号类型:本示例选择当前账号。
 - 名称:本示例输入VBR1。
 - 物理专线接口:选择申请的leasedline1接口。
 - VLANID: 0.
 - **阿里云侧互联IP**: 172.16.1.2。
 - 客户侧互联IP: 172.16.1.1。
 - 子网掩码: 255.255.255.252。
- 6. 重复上述步骤,为新加坡的物理专线创建VBR实例。

配置参数如下:

- 账号类型:本示例选择当前账号。
- 名称:本示例输入VBR2。
- 物理专线接口:选择申请的leasedline2接口。
- \circ VLANID: 0.
- 阿里云侧互联IP: 172.16.2.2。
- 客户侧互联IP: 172.16.2.1。
- 子网掩码: 255.255.255.252。

步骤三: 配置VBR路由

您需要在VBR上分别添加指向IDC的路由。

- 1. 在边界路由器 (VBR) 页面, 单击VBR1实例的ID。
- 2. 单击路由条目页签, 然后单击添加路由条目。
- 3. 在添加路由条目面板,根据以下信息配置路由条目,然后单击确定。
 - 下一跳类型:选择物理专线接口。
 - 目标网段: 输入IDC1中业务系统的网段。本示例输入10.2.1.0/24。
 - 下一跳:选择物理专线leasedline1接口。
- 4. 重复上述步骤,为VBR2配置指向本地IDC的路由。

配置参数如下:

- 下一跳类型:选择物理专线接口。
- 目标网段: 输入IDC2的网段。本示例输入10.2.2.0/24。
- 下一跳:选择物理专线leasedline2接口。

VBR指向IDC的路由如下表所示:

实例	目标网段	下一跳
VBR1	10.2.1.0/24	leasedline1接口
VBR2	10.2.2.0/24	leasedline2接口

步骤四:加入云企业网

完成物理专线接入后,您需要将物理专线关联的VBR和要互通的VPC加入同一个云企业网中。

- 1. 登录云企业网管理控制台。
- 在云企业网实例页面,创建云企业网实例。具体操作,请参见创建云企业网实例。
 在您创建云企业网实例过程中,您需要加载一个网络实例,您从已创建的VPC或VBR实例中,选择一个 即可。
- 3. 在云企业网实例页面,找到已创建的云企业网实例,单击操作列下的管理。
- 4. 单击网络实例管理页签, 然后单击加载网络实例加载物理专线关联的VBR和要互通的VPC。

本示例中需要将VBR1、VBR2、VPC加载到同一云企业网中,本操作请将剩余的VPC或VBR网络实例加载 到云企业网中。具体操作,请参见<mark>加载网络实例</mark>。

网络实例加载完成后, VBR1、VBR2、VPC的路由条目会自动发布到云企业网中。

5. 如果VPC中存在指向ECS实例、VPN网关、HAVIP等路由条目,请根据连通性需求,在VPC控制台将这些路由发布到云企业网中。

具体操作,请参见发布路由至云企业网。

步骤五: 配置路由策略

为避免在双物理专线场景下,VBR发布同样的本地IDC路由到阿里云上,造成路由环路的风险,系统默认会在 云企业网出地域网关方向添加优先级为5000、策略行为为拒绝的路由策略。该条路由策略会限制VBR、云连 接网与加入到云企业网中的其它VBR、云连接网互通。在本文示例中,您需要分别在华东1(杭州)地域和新 加坡地域添加高优先级的路由策略,允许VBR1和VBR2可以学习到对方的路由。

- 1. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
- 2. 在云企业网页面,单击路由策略页签,然后单击添加路由策略。
- 3. 在添加路由策略页面,根据以下信息配置路由策略,然后单击确定。
 - 本操作在华东1(杭州)地域添加路由策略,允许VBR2的路由传递到VBR1中。
 - 策略优先级:路由策略的优先级。优先级数字越小,优先级越高。本示例输入50。
 - 地域:选择路由策略应用的地域。本示例选择**华东1(杭州)**。
 - **应用方向**:选择路由策略应用的方向。本示例选择出地域网关。
 - **匹配条件**:路由策略的匹配条件。本示例设置**源实例ⅠD列表**为VBR1实例ⅠD和VBR2的实例ⅠD;**目的实 例ⅠD列表**为VBR1实例ⅠD和VBR2的实例ⅠD。
 - 策略行为:选择策略行为。本示例选择允许。
 - 更多信息,请参见路由策略概述。
- 4. 请重复步骤,在新加坡地域配置路由策略,允许VBR1的路由传递到VBR2中。
 - 策略优先级:路由策略的优先级。优先级数字越小,优先级越高。本示例输入50。
 - 地域:选择路由策略应用的地域。本示例选择新加坡。
 - **应用方向**:选择路由策略应用的方向。本示例选择出地域网关。
 - 匹配条件:路由策略的匹配条件。本示例设置源实例ID列表为VBR1实例ID和VBR2的实例ID;目的实例ID列表为VBR1实例ID和VBR2的实例ID。
 - 策略行为:选择策略行为。本示例选择允许。

配置完成后,云企业网、VPC和VBR中的路由条目如下所示:

○ 云企业网华东1(杭州)地域和新加坡地域下的路由条目

目标网段	下一跳
10.2.1.0/24	VBR1
10.2.2.0/24	VBR2
192.168.20.0/24	VPC

○ VPC中IDC的路由条目

目标网段	下一跳
10.2.1.0/24	VBR1
10.2.2.0/24	VBR2

○ VBR1中的路由条目

目标网段	下一跳
10.2.1.0/24	物理专线
10.2.2.0/24	VBR2
192.168.20.0/24	VPC

○ VBR2中的路由条目

目标网段	下一跳
10.2.1.0/24	VBR1
10.2.2.0/24	物理专线
192.168.20.0/24	VPC

步骤六:设置跨地域带宽

网络实例加载完成后,您还需要设置跨地域带宽,实现华东1(杭州)和新加坡地域的互通。

- 购买并绑定带宽包。具体操作,请参见使用带宽包和绑定带宽包。
 本示例中购买中国内地区域至亚太区域的带宽包。
- 2. 设置跨地域互通带宽。
 - i. 登录云企业网管理控制台。
 - ii. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
 - iii. 单击**跨地域互通带宽管理**页签,然后单击**设置跨地域带宽**。
 - iv. 在**设置跨地域带宽**面板,根据以下信息配置跨地域互通带宽,然后单击**确定**。
 - 带宽包:选择已购买的带宽包。
 - **互通地域**:选择需要互通的地域。

本示例选择华东1(杭州) ≒新加坡。

■ 带宽: 输入跨地域互通带宽的带宽值。

每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽值。更多信息,请参见<mark>跨地域互通带宽。</mark>

步骤七: 配置健康检查

您需要分别为两条物理专线配置健康检查,探测链路的连通性。健康检查会以您指定的发包时间间隔发送探测报文,当连续发送的所有探测报文(即您指定的探测报文个数)都丢包时,则判断健康检查失败。如果健康检查失败,请检查您的物理专线链路是否正常。具体操作,请参见故障排查。

- 1. 返回到云企业网实例页面。
- 2. 在左侧导航栏, 单击健康检查。
- 3. 选择VBR的地域,然后单击设置健康检查。

本示例选择华东1(杭州)。

- 4. 在设置健康检查面板,根据以下信息配置健康检查,然后单击确定。
 - 云企业网实例:选择VBR加载的云企业网实例。
 - 边界路由器 (VBR): 选择VBR1。
 - 源IP: 本示例选择自动生成源IP。

使用自动生成源IP,系统将自动分配100.96.0.0/16地址段内IP地址,探测链路的连通性。

- 目标IP: 输入VBR1实例中客户侧IP地址。
- 发包时间间隔(秒):指定健康检查时发送连续探测报文的时间间隔。单位:秒。本示例使用默认

值。

探测报文个数(个):指定健康检查时发送探测报文的个数。单位:个。本示例使用默认值。
 更多信息,请参见健康检查。

5. 重复上述步骤,为新加坡的物理专线配置健康检查。

步骤八:本地IDC侧配置

完成上述配置后,您可以分别在杭州IDC和新加坡IDC的CPE设备上,查看从云上学来的路由,同时您需要分别为两个IDC的CPE设备配置健康检查的回程路由。

● 为CPE设备配置健康检查的回程路由。

以下配置示例仅供参考,不同厂商的设备配置命令可能会有所不同。具体命令,请咨询相关设备的厂商。

#IDC1配置 ip route 100.96.0.0 255.255.0.0 172.16.1.2 #健康检查探测报文的回程路由 #IDC2配置 ip route 100.96.0.0 255.255.0.0 172.16.2.2 #健康检查探测报文的回程路由

• IDC从云上学习到的路由如下所示。

o IDC1

目标网段	下一跳
10.2.2.0/24	172.16.1.2
192.168.20.0/24	172.16.1.2

IDC2

目标网段	下一跳
10.2.1.0/24	172.16.2.2
192.168.20.0/24	172.16.2.2

步骤九: 连通性测试

完成以下操作,测试网络的连通性:

⑦ 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许IDC中的设备访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

- 1. 登录阿里云VPC中的ECS实例。具体操作,请参见连接方式概述ECS远程连接操作指南。
- 2. 执行 ping 命令, ping 杭州IDC的服务器10.2.1.204, 如果能接收到回复报文, 则表示网络连接成 功。

经验证, VPC和杭州IDC可正常通信。

[root@iZt	$Z \sim]$ # ping 10.2.1.204
LING 10.2.1.26	(10.2.1.204) 30(84) Dyles of uala.
64 bytes from	10.2.1.204: icmp_seq=1 ttl=64 time=2.06 ms
64 bytes from	10.2.1.204: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from	10.2.1.204: icmp_seq=3 ttl=64 time=1.97 ms
64 bytes from	10.2.1.204: icmp_seq=4 ttl=64 time=1.97 ms
^Z	
[1]+ Stopped	ping 10.2.1.204
[root@iZbp	Z ~]# [

- 3. 在新加坡IDC下,打开客户端的命令行窗口。
- 4. 执行 ping 命令, ping 杭州IDC的服务器地址, 如果能接收到回复报文, 则表示新加坡IDC和杭州 IDC可正常通信。

经验证,新加坡IDC和杭州IDC可正常通信。

[ro	ot@iZ		and the second second	Z ~]# pin	ng 10.2.	1.204	
PIN	G 10.2	2.1.20	94 (10.2.1.20	94) 56(84) b	oytes of	⁻ data.	
64	bytes	from	10.2.1.204:	<pre>icmp_seq=1</pre>	ttl=64	time=2.06	ms
64	bytes	from	10.2.1.204:	<pre>icmp_seq=2</pre>	ttl=64	time=1.97	ms
64	bytes	from	10.2.1.204:	<pre>icmp_seq=3</pre>	ttl=64	time=1.97	ms
64	bytes	from	10.2.1.204:	<pre>icmp_seq=4</pre>	ttl=64	time=1.97	ms
^Z							
[1]	+ Sto	opped		ping 10	9.2.1.20	94	
[ro	ot@iZł		engen not Die	z ~]# [

5. 依旧在新加坡客户端下,执行 ping 命令, ping 云上VPC的服务器IP地址192.168.20.161,如果能 接收到回复报文,则表示网络连接成功。

经验证, VPC和新加坡IDC可以正常通信。

[root@iZb; Z	~]# ping 192.168.20.161
PING 192.168.20.161 (192.168.2	20.161) 56(84) bytes of data.
64 bytes from 192.168.20.161:	icmp_seq=1 ttl=64 time=2.00 ms
64 bytes from 192.168.20.161:	icmp_seq=2 ttl=64 time=1.88 ms
64 bytes from 192.168.20.161:	icmp_seq=3 ttl=64 time=1.85 ms
64 bytes from 192.168.20.161:	icmp_seq=4 ttl=64 time=1.84 ms
^Z	
[1]+ Stopped	ping 192.168.20.161
[root@iz Z	~]# [

3.3.1.4. 多云互通

3.3.1.4.1. SAG vCPE实现多云互通

本文为您介绍如何通过智能接入网关SAG(Smart Access Gateway)vCPE将已经部署在亚马逊云计算服务 (AWS)平台中的云服务接入阿里云实现多云互通。

方案概述

在企业上云过程中,企业可能会因分支机构服务不同、境内和境外部署业务不同选择不同的云服务提供商, 企业总部和分支机构之间要相互通信,则需要云间互联技术。SAG vCPE是智能接入网关的软件镜像版,可为 您提供云间互联技术。SAG vCPE突破了物理的限制,支持多种形态的网络加密接入阿里云。您可以将SAG vCPE镜像部署在AWS的云服务器中,部署后,SAG vCPE作为一个虚拟CPE设备帮您提供服务,实现AWS云服 务和阿里云服务的互连互通。

场景说明

本文以下图场景为例,为您介绍SAG vCPE如何实现多云互通。某新加坡企业在AWS平台部署有业务系统, 在阿里云平台部署有安全服务系统。出于安全考虑,企业希望员工在访问互联网时,其流量能够先通过阿里 云平台的安全服务系统进行过滤,然后再进行通信。基于上述期望,企业需要AWS云服务和阿里云服务能够 互联互通,企业计划使用SAG vCPE产品实现AWS云服务和阿里云服务之间互联互通的需求。



准备工作

在您开始操作前,请确保您已经满足以下条件:

- 您已经在AWS中部署了业务系统。部署详情请咨询相关云服务提供商。
- 您已经注册了阿里云账号。如未注册,请先完成<mark>账号注册</mark>。
- 您已经在阿里云中创建了专有网络VPC(Virtual Private Cloud)并部署了相关服务。具体操作,请参见创 建和管理专有网络。
- 本文示例中, 网段规划如下表所示。您可以自行规划网段, 请确保您的网段之间没有重叠。

配置目标	网段规划	服务器IP地址
阿里云VPC	192.168.0.0/24	192.168.20.161
AWS	10.0.2.0/24	10.0.2.210

配置流程



步骤一:购买SAG vCPE设备

您需要在智能接入网关管理控制台,购买SAG vCPE设备和带宽,购买后系统会为您创建一个SAG vCPE实例,以便您管理SAG vCPE设备并对其进行网络配置。

1. 登录智能接入网关管理控制台。

- 2. 在智能接入网关页面,单击购买智能接入网关。
- 3. 选择创建智能接入网关(VCPE),根据以下信息配置SAG vCPE购买信息,然后单击立即购买。
 - 区域:选择SAG vCPE使用的区域。本示例选择亚太东南1(新加坡)。
 - 实例名称:输入SAG vCPE的实例名称。
 实例名称为非必填参数,长度为2~128个字符,以大小写字母或中文开头,可包含数字,半角句号
 (.),下划线(_)或短划线(-)。
 - **实例类型**:选择SAG vCPE的实例类型。默认为SAG-vCPE。
 - 版本:选择SAG vCPE的版本。默认为基础版。
 - **使用方式**:选择SAG vCPE的使用方式。默认为**双机**。

购买两台SAG vCPE,共享上云接入带宽,主设备故障时可切换到备用设备。本示例中只使用主设备。

- 带宽峰值:选择网络通信的带宽峰值。单位: Mbps。
- 购买数量:选择您需要购买的SAG vCPE实例的数量。本示例输入1。
- 购买时长:选择购买时长。

您可以选中下方的到期自动续费进行自动续费。

- 在确认订单页面,确认订单信息并选中我已阅读并同意《智能接入网关vCPE软件版服务协议》,单 击去支付。
- 5. 返回智能接入网关管理控制台,在顶部菜单栏,选择已创建实例的区域。
- 6. 在智能接入网关页面,单击已创建的实例ID。
- 7. 在智能接入网关详情页面,单击设备管理,查看并记录当前SAG vCPE主设备的序列号和密钥。

 ○ #定网络 ● 设置域下路由同步方式 認応需要设置域下路由同步方式。 例关加し引気症接例中。 ● 已成功绑定 ● 已成功绑定
● 已成功绑定
VPN状态 · 异常
管控状态: ● 异常
远程登陆IP -
秘钥 ***** 显示

步骤二: 部署SAG vCPE镜像

为实现AWS和阿里云的云服务互通,您需要在已创建的AWS云服务的VPC网络中新建一个实例,用于部署 SAG vCPE镜像。部署完成后,AWS SAG vCPE实例可作为AWS云服务与阿里云云服务互通的桥梁。

新建实例的详细步骤请参见云服务提供商相关文档,在新建过程中请注意以下步骤说明。

1. 为实例选择系统镜像时,请选择SAG vCPE的镜像进行启动。

当前SAG vCPE的镜像处于私有状态,请您提交工单给阿里云团队,提供AWS账号后SAG vCPE的镜像可 被分享到您的账号。

1. 遗择 AMI 2. 遗释实例类型 步骤 1: 选择一个 An AMI 是一种模板,其中包含启动实	3. 配置实例 Nazon 系统 例所需的软件配置	4. 质如府语 5. 质如病法 6. 配置安全组 7. 编辑 映像 (AMI) 硬作系统、应用程序服务器和应用程序),您可以选择 AWS、我们的用户社区或 AWS Marketplace 提供的 AMI;或者您也可以选择自己的 AMI 之一。	取得并源出
Q, 通过输入搜索词来搜索 AMI,	例如"Windows"		×
			按 SSM 參数搜索
快速启动			< < 1到2,共2个AMI > >
我的 AMI AWS Marketplace	۵	帝定義型 eba (251)(25型 hnn) 病者者 50 1018 日間用 ENA 国	逃择 64 位 (x86)
社区 AMI ▼ 所有权 ◎ 我拥有的	۵	aws-docker-vcpe-2.1.0-release06 - ami-0ct 2a [Copied ami	选择 64 位 (x86)

2. 选择实例类型时, 推荐您选择2核vCPU, 4 GB内存的实例规格。

SAG vCPE镜像在2核vCPU, 4 GB内存的实例规格下,加密私网带宽可达300 Mbps以上(1024字节)。 SAG vCPE镜像也支持1核vCPU, 2 GB内存的实例规格,在此规格下系统性能会降低30%以上,您可根据 业务需要进行选择。

1.选择/ 步骤 ^{当前选}	2. 法得实制关型 3. 配置实制 2: 选择一个实例类型 择的实例类型: 12.medium (变量 ECU, 2 vCF)	4. 添加存储 5. 添加标记 PU, 2.3 GHz, Intel Broadwel	些 <u>6. 配置安全组 7. 审</u> I E5-2686v4, 4 GiB 内存, 仅限	被 表于 EBS)				
	派列 ▼	类型 🗸	vCPU (j)	内存 (GiB) -	实例存储 (GB) (i)	可用的优化EBS() 。	Maatan (i) •	IPv6支持()。
	通用型	t2.nano	1	0.5	仅限于 EBS	-	低到中等	是
	通用型	t2.micro 符合条件的免费参考	1	1	仅限于 EBS	-	低到中等	是
	通用型	t2.small	1	2	仅限于 EBS	-	低到中等	是
	通用型	t2.medium	2	4	仅限于 EBS	-	低到中等	是
	通用型	t2.large	2	8	仅限于 EBS	-	低到中等	是
	通用型	t2.xlarge	4	16	仅限于 EBS	-	中等	是

3. 配置实例时,请将SAG vCPE设备的序列号和密钥与实例进行绑定并保证实例分配了公网IP地址。

序列号和密钥绑定示例如下所示:

{"sn":"sage6m2ph5sit******	***","key":"y7y7LUWqnbc4fCpIJnxRQ2c1nOYtW************}
1. 选择 AMI 2. 选择实例类型 3. 配置实例 步骤 3: 配置实例详细信息	4. 添加存储 5. 添加标签 6. 配置安全组 7. 审核
Elastic Inference (j)	Additional charges may apply when launching Dedicated instances. □ 添加 Elastic Inference 加速器 将收取额外费用。
T2/T3 无限 (ì	□ 启用 可能收取额外费用
文件系统 (1)	添加文件系统 C 新建文件系统
▼ 高级详细信息	
Metadata accessible (j)	Enabled
Metadata version (j)	V1 and V2 (token optional)
Metadata token response hop limit 🧃	1
用户数据 ()	◉ 以文本形式 ○ 以文件形式 □ 输入已采用 base64 编码
	{"sn": "sagexxxxxx", "key":"xxxxxxx"}

4. 配置安全组时,您需要允许阿里云云服务私网网段和AWS云服务私网网段可以访问SAG vCPE实例。

5. 实例启动后, 您需要关闭源、目标检查。

启动实例 ▼ 连接 操作 ▼	L -> + 0
Q、按标签和属性筛选,或者按关键字搜索	❷ К < 1到3, 3 > >
Name - 实例 ID - 实例类型	▼ 可用区
i-0c 2 t2.micro	ap-northeast-1c 🧅 running 🥝 2 项检查已 无 🍃 ec2-3- 💷 🗰 🐂 -nor 3.1 💶 73
实例: i-0c	启用源/目标检查 ×
描述 状态检查 监控 标签	
实例 ID i-0c	您确定要对包含以下详细信息的实例禁用源/目标检查吗? 2-3-112-57-73.ap-northeast-
实例状态 running 实例类型 t2.micro 正在查找 选择使用 AWS Com	文例: i-0c8 网络接口: eni-0 状态 已启用
私有 DNS ip-172-31-2-137.ap	-northeast-1c
私有 IP 172.3 137 辅助私有 IP 172.3 199	取消 是,请禁用 计划事件 ##### 如 ##### 201052011-¥86.64-on2

步骤三: SAG vCPE设备网络配置

AWS SAG vCPE实例部署完成后,该实例可作为一个虚拟的CPE设备帮您提供服务。您还需要在智能接入网关管理控制台对该虚拟设备进行网络配置,以便AWS SAG vCPE实例能正常接入阿里云并访问其云服务。

- 1. 配置线下路由同步方式。
 - i. 登录智能接入网关管理控制台。
 - ii. 在顶部菜单栏,选择目标区域。
 - iii. 在智能接入网关页面,找到目标实例,单击操作列的网络配置。
 - iv. 在线下路由同步方式页面, 单击添加静态路由。
 - v. 在添加静态路由对话框,输入您AWS云服务所在的私网网段,单击确定。

基本信息 设备管	理 网络剧查 高可用配置 监控	
线下路由同步方式 绑定网络详情 私网SNAT	 静态路由 ○ 动态路由 添加静态路由 	
DNAT	网段	攝作
组网图	10	删除

2. 绑定云连接网。

云连接网是智能接入网关的重要组成部分,智能接入网关通过云连接网将您的网络接入阿里云。更多信息,请参见云连接网介绍。

如果您未创建过云连接网,请先创建云连接网实例,再进行下面的绑定操作。具体操作,请参见创建云 连接网。

- i. 在智能接入网关页面, 找到目标实例, 单击操作列的网络配置。
- ii. 单击绑定网络详情页签。
- iii. 单击添加网络,在添加网络对话框,选择目标云连接网实例,然后单击确定。

iv. 在您绑定网络后,在设备管理页签下, SAG vCPE设备的VPN状态和管控状态均变为正常。

← sag-cr	← sag-cr								
请开始您的	0 約配置 <u>約</u> 自	激活设备 买的实例将赠送15天有效期,并 动从下单日开始计费。			○ 绑定网络 您还需要在网络配置中将智能接入 网关加入到云连接网中。			○ 设置线下路 您还需要设置线	由同步方式 缆下路由同步方式。
	•	已成功激活			已成功绑定			⊘ 已成功配置	
基本信息 设备管	理网络配置	高可用配置 监控							
sage	2(±) sage	буź							
C 同步配置到云端	更新版本	远程登录 远程重启	重置秘钥 刷新						
设备信息	设备信息					_			
WAN口管理	当前版本	2.1.0					VPN状态	 正常 	
HA管理	设备类型	sag-vcpe				L	管控状态	 正常 	
< 路由管理	设备启动时间 公网IP	2020-08-06 10:32:17					远程登时IP 秘钥	- *****	
一键诊断									

3. 配置云企业网。

云企业网可让SAG vCPE设备和阿里云上VPC资源互通。更多信息,请参见什么是云企业网。

您需要参考以下操作将SAG vCPE设备绑定云企业网,并在云企业网中加载已创建的VPC实例,操作完成后,SAG vCPE和阿里云上VPC实例可学习到对方的路由。

- i. 在左侧导航栏, 单击云连接网。
- ii. 在云连接网页面,找到目标云连接网实例,单击操作列的绑定云企业网。
- iii. 在**绑定云企业网**页面,选择要绑定的云企业网实例,然后单击确定。

您可以通过以下两种方式选择目标云企业网实例,本示例选择新建CEN。

- 选择现有CEN:如果您已经创建了云企业网,您可以单击下方文本框,选择已创建的云企业网实 例进行绑定。
- 新建CEN:如果您未创建过云企业网,您可以在下方文本框中,输入云企业网实例名称,系统会为您新建云企业网实例并自动进行绑定。

云企业网实例名称长度为2~100个字符,以大小字母或中文开头,可包含数字、下划线(_)或 短划线(-)。

iv. 将您已经创建的阿里云VPC实例,绑定到此云企业网中。具体操作,请参见加载网络实例。

v. 将VPC加载到云企业网后,您需要为VPC下的云服务器ECS(Elastic Compute Service)配置安全组,允许AWS云服务实例的私网网段访问VPC资源。具体操作,请参见添加安全组规则。

编辑安全组规则 ⑦ 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:	全部					
* 端口范围:	-1/-1					
优先级:	1					
授权类型:	IPv4地址頁 ▼					
*授权对象:	10.0.2.0/24	● 教我设置				
描述:						
	上 长度为2~256个字符,不能以http://或 https://开头。					
	确定	取消				

步骤四: AWS云服务实例配置

为实现AWS和阿里云资源互通,您还需要执行以下步骤完成对AWS云服务实例的配置,步骤中需要执行的具体命令请咨询相应云服务提供商。

- 1. 登录AWS云服务中要访问阿里云云服务的实例。
- 2. 为实例配置路由。

在AWS的VPC中配置路由,将要访问的阿里云云服务网段的下一跳指向VPC中SAG vCPE实例,由SAG vCPE实例帮您完成和阿里云云服务的互通。

êJJJ	踏由表 操作	•							Ð	۰	?
Q	路由表 ID: rtb-a	ai c 💿 添加	筛选条件					K < 13	則1, 1	> >	
	Name	→ 路由表 ID	*	显式关联对象	Edge associations	主路由表	VPC ID	- Owner		Ŧ	
		rtb-aa cc		-	-	是	vpc-ba dc	191 84			
路由	表: rtb-aad9acco	2			000						
	摘要	路由	子网关联	Edge Associations	路由传播标签						
	始大日時中										
	細相印日										
			查看所有规则	J -							
	Destination			Target		Status		Propagated			
	1 0/16			local		active		No			
	0.0			igw-a	cf	active		No			
	17: .0.0/20			eni-0	f6	active		No			
	192.168.0.0/24			eni-0 =	1 1 1 1 1 1 1 1 1 1	active		No			

3. 为实例配置安全组。

允许阿里云云服务私网网段和SAG vCPE私网网段访问AWS云服务。

- 4. 路由配置完成后,测试网络连通性。
 - i. 登录阿里云VPC中的ECS实例。具体操作,请参见连接方式概述ECS远程连接操作指南。
 - ii. 通过ping命令, ping AWS云服务实例的私网IP地址,测试AWS云服务和阿里云云服务之间的连通 性。

经验证,AWS云服务和阿里云云服务之间可以正常通信。

```
[root@iZk]
PING 10.0.2.210 (10.0.2.210) 56(84) bytes of data.
64 bytes from 10.0.2.210: icmp_seq=1 ttl=64 time=1.96 ms
64 bytes from 10.0.2.210: icmp_seq=2 ttl=64 time=1.97 ms
64 bytes from 10.0.2.210: icmp_seq=3 ttl=64 time=1.96 ms
64 bytes from 10.0.2.210: icmp_seq=4 ttl=64 time=1.96 ms
64 bytes from 10.0.2.210: icmp_seq=4 ttl=64 time=1.96 ms
72
[6]+ Stopped ping 10.0.2.210
[root@iZb]
```

3.3.2. 阿里云SD-WAN解决方案

阿里云SD-WAN解决方案,依托于阿里巴巴优质的全球传输网络,通过SDN技术应用到广域网络,结合智能 接入网关,企业总部及各分支能够就近接入阿里云POP点,快速、安全、简单地帮助企业构建广域互联网 络,为客户提供了一站式云-网-端的云原生SD-WAN解决方案。

方案介绍

随着企业新兴业务的爆发、迅速增长,以昂贵MPLS专线为主的传统广域网互联难以支撑企业WAN的流量激增,SD-WAN逐渐成为企业总部分支互联在云时代的优选。阿里云SD-WAN为企业总部各分支提供基于专线/Internet/4G等混合链路广域网互联接入服务,基于阿里云全球高质量传输网络优势,进一步平衡并优化企业应用,从而提高企业WAN网络的可靠性、灵活性和运维效率。

本方案以某企业各机构上云为例,介绍如何通过部署智能接入网关SAG(专线+互联网)将该企业的分支机构,上海分支、深圳IDC、北京门店和北京移动办公区就近接入阿里云POP点并与企业总部互通,为该企业快速构建总部与分支互联的网络,并且通过云企业网CEN实现全球跨境跨地域高速互联。

方案咨询

方案咨询,请访问SD-WAN解决方案咨询。

部署结构图



本方案涉及的产品说明:

● 智能接入网关SAG

通过Internet就近加密接入,智能、可靠、安全的一站式上云服务。了解更多产品信息,请参见智能接入 网关。

• 高速通道

帮助不同网络环境间实现高速、稳定、安全的私网通信。物理专线连接实现云下IDC专线接入云上,提高 网络拓扑灵活性和跨网通信质量。了解更多产品信息,请参见高速通道。

● 云企业网CEN

提供全球网互联能力,帮助用户打造一张具有企业级规模和通信能力的云上网络。了解更多产品信息,请 参见云企业网。

业务规划

本方案企业各机构上云规划如下:

- 云上网络:已经部署了阿里云北京VPC、阿里云美西VPC。
- 上海总部:已经部署了上云物理专线。
- 上海分支: 将通过智能接入网关双机旁挂模式接入阿里云。智能接入网关采用宽带和4G双链路上云方式。
- 深圳IDC:将通过物理专线和智能接入网关接入阿里云。智能接入网关采用单机旁挂,宽带和4G双链路上 云方式,作为物理专线的备份链路接入阿里云。
- 北京门店: 将通过智能接入网关直挂模式接入阿里云。智能接入网关采用宽带和4G双链路上云方式。
- 北京移动办公区:将通过智能接入网关APP接入阿里云。

本方案企业各机构购买智能接入网关规格说明:

分支机构	智能接入网关规格	设备数量
上海分支	SAG-1000	2

分支机构	智能接入网关规格	设备数量
深圳IDC	SAG-1000	1
北京门店	SAG-100WM	1
北京移动办公区	智能接入网关APP版	无

网段规划

以下为本方案网段规划示例值,如您需要自行规划网段,请确保各个网段地址不冲突。

分支机构	项目	网段规划	
	出口路由器	端口G1: 192.168.80.1/30	
	三层交换机上行接口	端口G2: 192.168.80.2/30	
	智能接入网关1	WAN端口5: 192.168.100.1/30, 下 一跳: 192.168.100.2 LAN端口4: 192.168.50.1/30	
上海分支	智能接入网关2	WAN端口5: 192.168.200.1/30, 下 一跳: 192.168.200.2 LAN端口4: 192.168.60.1/30	
	三层交换机	端口G11: 192.168.100.2/30 端口G12: 192.168.50.2/30 端口G13: 192.168.200.2/30 端口G14: 192.168.60.2/30 环回口: 192.168.100.3/32	
	业务网段	172.16.0.0/12	
	智能接入网关	WAN端口3: 192.168.110.1/30 , 下一跳: 192.168.110.2	
深圳IDC	三层交换机	端口G11: 192.168.110.2/30 端口G2: 192.168.90.2/30	
	出口路由器地址	端口G1: 192.168.90.1/30	
	业务网段	172.32.0.0/12	
北京门店	业务网段	192.168.10.0/24	
北京移动办公区	业务网段	192.168.20.0/24	
上海总部	业务网段	192.168.30.0/24	

分支机构	项目	网段规划
阿里云美西VPC	业务网段	10.10.0.0/16
阿里云北京VPC	业务网段	10.0.0/16

部署流程

本方案部署流程如下:



步骤一:购买智能接入网关

您在阿里云控制台购买智能接入网关后,阿里云会将智能接入网关设备寄送给您,并创建一个智能接入网关 实例方便您管理网络配置。

请根据企业各分支规划,完成以下操作,购买智能接入网关。

- 1. 登录智能接入网关管理控制台。
- 2. 在智能接入网关页面,单击创建智能接入网关。
- 3. 配置智能接入网关,然后单击**立即购买**,确认配置信息后,选择**《智能接入网关设备服务协议》**,然 后单击**确认购买**。
- 4. 在弹出的**收货地址**对话框,填写网关设备的收货地址,然后单击**立即购买**并完成支付。

步骤二:北京门店接入智能接入网关

北京门店收到网关设备后,请按照部署模式检查配件。



- 1. 激活绑定智能接入网关设备。
 - i. 登录智能接入网关管理控制台。
 - ii. 在智能接入网关页面,找到北京门店网关实例ID。
 - iii. 单击操作列下的激活。
 - iv. 单击北京门店网关实例ID, 在**智能接入网关实例**页面, 单击**设备管理**页签, 输入北京门店智能接入网关设备序列号。

智能接入网关							
← sag-2 mid-0 u0 + qc, gc > 00							
基本信息	设备管理	网络配置	健康检查	高可用配置	运维监控		
您尚未添加主设备,请添加主设备 ^{硬件类型} SAG							
设备编码							
请输入设备编码							
添加设备							

v. 单击添加设备。
- 2. 连接网关设备。
 - i. 启动网关设备后,将WAN口和Modem相连,LAN口和本地客户端相连。
 - ii. 北京门店本地客户端可直接通过网关设备接入,使用默认的网关配置即可。如果需要配置WAN口和 LAN口,请参见SAG-100WM Web配置和SAG-100WM Web配置。
- 3. 配置网络路由。
 - i. 登录智能接入网关管理控制台。
 - ii. 在左侧导航栏,单击智能接入网关,在智能接入网关页面,单击需要进行网络配置的网关实例操 作列下的网络配置。
 - iii. 单击线下路由同步方式。
 - iv. 选择静态路由,然后单击添加静态路由。

本操作输入192.168.10.0/24。因为北京门店智能接入网关设备使用了默认网关配置,所以本地客 户端的IP地址从192.168.10.0/24中分配。

添加静态路由		×
* 网段 🕐		
192.168.10.0	/ 24	
	确定	关闭

v. 单击确定。

步骤三:上海分支接入智能接入网关

上海分支收到网关设备后,请按照SAG-1000设备说明检查配件。

在执行此操作前,请保持网关设备启动且4G信号正常,已经连接到阿里云。本操作以智能接入网关1为例进行配置,请根据同样的步骤和网络规划配置智能接入网关2。



- 1. 激活智能接入网关实例,将两台智能接入网关绑定到同一智能接入网关实例。详细步骤请参见。
- 2. 连接网关设备。
 - i. 在智能接入网关实例页面,单击设备管理页签,选择目标主设备。
 - ii. 在左侧页签栏, 单击**端口角色分配**。
 - iii. 在端口角色分配页面,单击目标端口的操作列下的修改,修改端口角色。
 上海分支使用WAN(端口5), LAN(端口4)。
 - iv. 通过网线,将智能接入网关的WAN (端口5)连接到三层交换机的G11端口上。
 - v. 通过网线,将智能接入网关的LAN (端口4)连接到三层交换机的G12端口上。
- 3. 端口配置。
 - i. 在智能接入网关实例页面, 单击设备管理页签。
 - ii. 在左侧页签栏, 单击LAN口管理。
 - iii. 在LAN(端口4)区域,单击编辑。

iv. 在LAN(端口4)配置页面,连接类型选择静态IP,输入规划好的IP地址信息,然后单击确定。

LAN (端口4) 配置	×
* 连接类型	
○ 动态IP	
● 静态IP	
* LAN地址	
192.168.50.1	
* 掩码地址	
255.255.255.252	
确定	取消
	0.12

- v. 在左侧页签栏,单击WAN口管理。
- vi. 在WAN (端口5)区域,单击编辑。
- vii. 在WAN(端口5)配置页面,连接类型选择静态IP,输入规划好的IP地址信息,然后单击确定。

WAN (讀,, 配置	×
* 连接类型	
○ 动态IP	
● 静态P	
O PPPoE	
* 优先级	
1	
* IPt地址	
192.168.100.1	
* 掩码	
255.255.255.252	
* 网关	
192.168.100.2	
确定即	消

4. 配置路由。

- i. 在智能接入网关实例页面, 单击设备管理页签。
- ii. 在左侧页签栏, 单击路由管理。
- iii. 在OSPF协议配置区域,单击编辑。
- iv. 在配置OSPF路由协议页面,输入规划好的配置信息,然后单击确定。

参数	说明
Area ID	主设备区域ID: 1 备设备区域ID: 1
Hello_time	两台设备Hello_time时间均为3秒。
Dead_time	两台设备Dead_time时间均为10秒。
认证方式	两台设备均选择不认证。
Router ID	主设备路由器ID: 192.168.100.1 备设备路由器ID: 192.168.200.1
Area Type	区域类型默认为NSSA。

- v. 在WAN/LAN动态路由配置详情区域,选择启用OSPF协议。
- vi. 单击目标端口端口4(LAN)的操作列的编辑,选择启用OSPF,单击确定。
- 5. 配置线下路由同步方式。
 - i. 登录智能接入网关管理控制台。
 - ii. 在智能接入网关页面,单击需要进行网络配置的网关实例操作列下的网络配置。
 - iii. 在线下路由同步方式页签下,选择动态路由。
- 6. 配置三层交换机和出口路由器。

由于不同厂商的交换机配置命令有所区别,具体请参考厂商的配置手册。本文仅以某厂商交换机和路由 器举例说明。

○ 交换机配置

■ 配置端口IP及OSPF参数:

⑦ 说明 同一个智能接入网关设备运行OSPF协议接口的网络类型需要配置为p2p, 否则不能 正确地计算路由。

```
interface GigabitEthernet 0/11
no switchport
ip address 192.168.100.2 255.255.255.252 智能接入网关1对端交换机的端口IP
interface GigabitEthernet 0/12
no switchport
                                     网络类型必须为p2p
ip ospf network point-to-point
ip ospf hello-interval 3
ip ospf dead-interval 10
ip address 192.168.50.2 255.255.252 智能接入网关1对端交换机的端口IP
interface GigabitEthernet 0/13
no switchport
ip address 192.168.200.2 255.255.255.252 智能接入网关2对端交换机的端口IP
!
interface GigabitEthernet 0/14
no switchport
ip address 192.168.60.2 255.255.255.252
                                      智能接入网关2对端交换机的端口IP
ip ospf network point-to-point
                                       网络类型必须为p2p
ip ospf dead-interval 10
ip ospf hello-interval 3
1
```

■ 配置交换机的Loopback地址及路由通告信息:

⑦ 说明 OSPF需要配置为NSSA区域,且自动产生默认路由发布给智能接入网关。

```
interface Loopback 0
ip address 192.168.100.3 255.255.255.255
                                          交换机的loopback地址
1
router ospf 1
                                            交换机的routerID
router-id 192.168.100.3
network 172.16.0.0 0.15.255.255 area 0
                                           本地服务器网段
network 192.168.50.0 0.0.0.4 area 1
                                           交换机连接智能接入网关1的接口网段
network 192.168.100.3 0.0.0.0 area 0
                                            交换机本身的loopback地址
network 192.168.60.0 0.0.0.4 area 1
                                            交换机连接智能接入网关2的接口网段
area 1 nssa default-information-originate no-summary
1
```

○ 出口路由器路由配置

配置静态路由

ip route 192.168.100.1 255.255.255.252 192.168.80.2 出口路由器去往智能接入网关1的路由 ip route 192.168.200.1 255.255.255.252 192.168.80.2 出口路由器去往智能接入网关2的路由

步骤四:深圳IDC接入智能接入网关和物理专线

深圳IDC收到网关设备后,请按照SAG-1000设备说明检查配件。





- 1. 激活绑定智能接入网关实例。详细步骤请参见。
- 2. 连接网关设备。
 - i. 在智能接入网关实例页面, 单击设备管理页签。
 - ii. 在左侧页签栏, 单击端口角色分配。
 - iii. 在端口角色分配,单击目标端口的操作列下的修改,修改端口角色。深圳IDC使用WAN(端口3)。
 - iv. 通过网线,将智能接入网关的WAN (端口3)连接到三层交换机的G11端口上。
- 3. 端口配置。
 - i. 在智能接入网关实例页面, 单击设备管理页签。
 - ii. 单击WAN口管理页签。
 - iii. 在WAN (端口3)区域,单击编辑。

iv. 在WAN(端口3)配置页面,连接类型选择静态IP,输入规划好的IP地址信息,然后单击确定。

WAN () 配置	\times
○ 动态IP	
● 静态IP	
O PPPoE	
* IP地址	
192.168.110.1	
* 掩码	
255.255.255.252	
* 网关	
192.168.110.2	
确定取	消

- 4. 配置路由。
 - i. 配置线下路由同步方式。详情请参见。

深圳IDC选择添加静态路由172.32.0.0/12。

ii. 保持在该智能接入网关实例页面,单击设备管理页签。

iii. 在左侧导航栏,单击路由管理,然后单击添加静态路由。

iv. 在添加静态路由添加静态路由页面,添加去往本地机构的静态路由。

添加静态路由		\times
172.32.0.0/12		
* 下—跳IP		
192.168.110.2		
* 端口		
端口3(WAN)		\sim
	确定	取消

5. 配置三层交换机和出口路由器。

由于不同厂商的交换机配置命令有所区别,具体请参考厂商的配置手册。本文仅以某厂商交换机和路由 器举例说明。

互联交换机的路由配置。

三层交换机:

interface GigabitEthernet 0/11 no switchport ip address 192.168.110.2 255.255.252 智能接入网关对端交换机的端口IP ip route 10.0.0.0 255.255.0.0 192.168.110.1 255 交换机去往阿里云北京VPC的路由 ip route 10.10.0.0 255.255.0.0 192.168.110.1 255 交换机去往阿里云美西VPC的路由 ip route 192.168.30.0 255.255.255.0 192.168.110.1 255 交换机去往上海总部的路由 ip route 0.0.0.0 0.0.0.0 192.168.90.1 交换机去往公网路由。

出口路由器的路由配置。

出口路由器:

ip route 192.168.110.1 255.255.255.252 192.168.90.2 出口路由器去往智能接入网关的路由

6. 搭建物理专线。

- i. 在自主申请专线接入前,您需要完成接入点确认、运营商工勘等准备工作。详细信息,请参见<u>独享</u> 专线连接前准备。
- ii. 开通上云物理专线。详情请参见创建和管理独享专线连接。
- iii. 登录高速通道管理控制台。
- iv. 在左侧导航栏, 单击边界路由器(VBR) > 边界路由器(VBR)。
- v. 在顶部状态栏处,选择要创建的边界路由器的地域。
 - 深圳IDC选择华南1(深圳)地域。
- vi. 在边界路由器 (VBR) 页面, 单击创建边界路由器。

vii. 在创建边界路由器对话框,根据以下信息配置边界路由器,然后单击确定。

- 账号类型:当前账号。
- 名称: 深圳VBR。
- 物理专线接口:选择申请的物理专线接口。
- VLANID: 0。
- 阿里云侧互联IP: 192.168.150.2/30。
- 客户侧互联IP: 192.168.150.1/30。
- 子网掩码: 255.255.255.252。
- 7. 在深圳IDC和边界路由器之间分别建立起BGP邻居并宣告相应路由。深圳IDC配置请咨询相应厂商, 阿里 云上配置请参见配置和管理BGP。
- 8. 智能接入网关绑定边界路由器。
 - i. 登录智能接入网关管理控制台。
 - ii. 在智能接入网关页面, 单击需要进行网络配置的网关实例操作列下的网络配置。

iii. 在**绑定网络详情**页签下,单击添加网络,选择刚刚创建的边界路由器网络实例,单击确定。

⑦ 说明 云企业网对相同网段的专线路由和智能接入网关路由处理优先级是:专线路由优先处理。

步骤五:北京移动办公区接入智能接入网关APP

- 1. 购买智能接入网关APP。详情请参见购买SAG App。
- 在智能接入网关控制台添加要进行云上访问的私网网段。详情请参见网络配置。
 北京移动办公区添加私网网段192.168.20.0/24。
- 3. 在智能接入网关控制台为移动用户添加账号。详情请参见创建客户端账号。
 - 用户名: 非必填参数, 默认为邮箱账号。此处输入test。
 - 邮箱地址:此参数必填。普通用户的邮箱地址,此处输入username@example.com。
 - 设置带宽峰值:当前账号可以使用的带宽峰值。此处保持默认值。

可设置带宽范围为1Kbps-2Mbps,默认为2Mbps。

- · 设置密码: 非必填参数。此处不输入。
- 4. 移动用户安装客户端。详情请参见安装客户端。
- 5. 移动用户可通过下发的账户信息连接内网。详情请参见连接内网。

步骤六: 绑定智能接入网关到云连接网

要将智能接入网关实例所连接的线下分支接入阿里云,您必须先创建一个云连接网,然后将智能接入网关实 例添加到云连接网内,为实现线下分支和云上网络资源互通做准备。

- 1. 登录智能接入网关管理控制台。
- 2. 在左侧导航栏,单击云连接网。
- 3. 在云连接网, 单击创建云连接网。
- 在创建云连接网页面,配置云连接网名称,然后单击确定。
 云连接网名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)或短横线

(-) 。				
智能接入网美 / 云连接网				使用限制 🕐 帮助文档
云连接网				
创建云连接网 C				案例ID × 清細入 Q
实例ID/名称	绑定云企业网	绑定智能接入网关	私网网段	操作
con-		0/0		柳垣云企业网 删除

5. 在云连接网页面,单击刚刚创建的云连接网实例ID。

6. 在云连接网实例页面,单击绑定智能接入网关。

7. 在绑定智能接入网关页面,选择同账号页签。

- 8. 选择北京门户智能接入网关实例,单击确定。
- 9. 请重复上述步骤,将深圳IDC、上海分支和北京移动办公区APP实例绑定同一个云连接网。

绑定智能接入网关	×
同账号 跨账号	
智能接入网关	
-/sag-	\sim

您可以在云连接网实例页面查看已经绑定的智能接入网关实例。

已绑定智能接入网关基本信息						绑定智能接入网关
实例ID/名称	带宽峰值	状态	私网网段	到期目时间	账号UID	操作
sag- Shenzher , ⇒ ∠	-	• 可用	10100100	1040 Aug 100	本账号	解绑
sag- Beijing	10.0	• 可用	1		本账号	解謝

步骤七:添加网络实例到云企业网

在智能接入网关绑定到云连接网后,您还需要创建一个云企业网,将云连接网CCN、专有网络VPC和边界路 由器VBR绑定到该云企业网内,为企业分支机构、阿里云上VPC网络和企业总部互通做准备。

- 1. 登录云企业网控制台。
- 2. 在云企业网实例页面, 单击创建云企业网实例。
- 3. 在创建云企业网实例页面,将之前步骤中创建的云连接网CCN直接加载到该云企业网实例中。

⑦ 说明 创建云企业网实例详情请参见创建云企业网实例。

创建云企	业网实例		?	\times
云企业网				
	• 名称 🕗			
	cen-c	10/128		
	描述 💿			
		0/256		
加载网络	实例			
同账号	1			
 注 	E: 已加载到云企业网的实例不允许重复加载			
	• 实例类型 ②			
	云连接网 (CCN)	\sim		
	• 地域 💿			
	中国	\sim		
	• 网络实例 ②			
	ccn-	\sim		

- 4. 登录智能接入网关管理控制台。
- 5. 在左侧导航栏,选择快捷连接 > 云企业网,选择之前创建的云企业网实例ID。
- 6. 在网络实例管理页签, 单击加载网络实例。
- 7. 单击同账号页签, 添加网络实例。

将之前创建的阿里云北京VPC、阿里云美西VPC、上海总部边界路由器VBR和深圳IDC边界路由器VBR绑 定到该云企业网内。

- **实例类型**:选择要加载的实例类型。
- 地域:选择所选实例类型的所属地域。
- 网络实例:选择要加载的网络实例。

步骤八:购买带宽包

要实现跨地域网络实例互通,您必须购买带宽包并设置跨地域互通带宽。同地域互通不需要购买带宽包。带 宽包购买说明请参见使用带宽包。

本方案中需要同时购买跨境和非跨境带宽包,以实现云上网络资源互通。

1. 登录智能接入网关管理控制台。

- 2. 在左侧导航栏,选择快捷连接 > 云企业网,选择之前创建的云企业网实例ID。
- 3. 在云企业网实例页面,单击带宽包管理页签,此处以单击购买带宽包(预付费)。
- 4. 在云企业网(预付费)页面,在跨境页签下配置带宽包信息,然后单击立即购买。
 - **云企业网**:选择VPC、VBR和云连接网所加入的云企业网。
 - 区域A和区域B:选择本次购买带宽包需要互通的网络实例所在的区域。
 此处选择中国内地和北美。
 - **带宽值**:根据业务需要,选择跨区域互通的带宽。
 - 带宽包名称: 输入该带宽包的名称。

	云企业网	zxtest ▼ 云企业网为 <mark>必选项。</mark> 如果您还没有云企业网,请先 创建云企业网实例 。
互通区	区域-A	中国内地
域	区域-B	北美 亚太 欧洲 澳洲
		 选择要互通的区域,购买带宽包后设置两区域间跨地域互通的带宽,可实现两区域内的跨地域互通。(点击查看区域与地域对应关系) 马来西亚,印度,印尼等地分别跨地域互通最大带宽限定50Mbps以内,如需以上地域和其他地域互通,请谨慎选择带宽包带宽值。 互通区域订购后不能修改,请谨慎选择。 <u>石企业网跨地域带宽默认为1kbps,仅供测试连通性。为保证您业务正常运行,请购买完带宽包后设置互通地域带宽。</u>
Ħ	计费方式	按带宽
華本配	带宽值	11 2500Mbps 5000Mbps 10000Mbps 2 Mbps 🜩
置	带宽包名称	
购买量	购买时长	179 □自动续费 💩

- 5. 在云企业网实例页面,单击跨地域互通带宽管理页签,然后单击设置跨地域带宽。
- 6. 设置跨境互通带宽,每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽值。
 - 带宽包:选择已绑定至云企业网实例的带宽包,此处选择中国内地与北美。
 - 互通地域:选择需要互通的地域,此处选择中国内地云连接网和美国(硅谷)。请以同样的方式创建华北2(北京)和美国(硅谷)、华南1(深圳)和美国(硅谷)、华东2(上海)和美国(硅谷)的互通带宽包。
 - 带宽: 根据业务需要, 输入带宽值。

⑦ 说明 每个带宽包下的跨地域互通带宽的总和不能大于该带宽包的带宽值。

- 7. 购买中国内地互通带宽包。在云企业网(预付费)页面,单击非跨境页签,然后完成以下配置。
 - **云企业网**:选择VPC、VBR和云连接网所加入的云企业网。
 - 区域A和区域B:选择本次购买带宽包需要互通的网络实例所在的区域。

此处选择中国内地和中国内地。

- **带宽值**:根据业务需要,选择跨区域互通的带宽。
- 带宽包名称: 输入该带宽包的名称。
- 8. 设置跨地域互通带宽, 然后单击确定。
 - 带宽包:选择已绑定至云企业网实例的带宽包,此处选择中国内地与中国内地。
 - 互通地域:选择需要互通的地域,此处选择中国内地云连接网和华北2(北京)。请以同样的方式 创建中国内地云连接网和华南1(深圳)、中国内地云连接网和华东2(上海)、华北2(北 京)和华南1(深圳)、华北2(北京)和华东2(上海)、华东2(上海)和华南1(深圳)的互 通带宽包。
 - **带宽**: 根据业务需要, 输入带宽值。

步骤九:配置安全组

您需要在阿里云北京VPC、阿里云美西VPC内分别为上海分支、深圳IDC、北京门户和北京移动办公区进行访问授权,以便分支机构访问云上资源。

本操作以阿里云北京VPC为例为上海分支进行访问授权,请以同样的操作为其余分支授权。

- 1. 登录ECS管理控制台。
- 2. 在左侧导航栏,单击实例。
- 3. 找到阿里云北京VPC内的ECS实例,然后单击更多 > 网络和安全组 > 安全组配置。
- 4. 单击配置规则,然后单击添加安全组规则。
- 5. 配置一条允许上海分支访问阿里云北京VPC的安全组规则。

入方向 出方向						
手动滚加 快速	添加 へ 輸入講	口或者授权对象进行搜索				
授权策略 优	抗叛 ①	协议类型	靖口范園 ③	授权对象 ①	描述	操作
	1	自定义 TCP V	* 目的: HTTP (80) ×	★源: 10.10.0.0/12 ×	cesishiy	保存:预览:删除

步骤十:访问测试

完成上述配置后,您可以通过在各个分支的客户端访问已连接的VPC中部署的云资源验证配置是否生效。

3.3.3. 企业级移动办公解决方案

阿里云提供一站式快速上云解决方案,通过智能接入网关APP、VPN网关产品,可实现终端(电脑端和手机)直接拨号通过内网加密安全上云,适用于企业移动办公、远程运维场景。本文为您介绍如何使用智能接入网关APP直接拨号连接内网,实现和云上应用互访。

场景说明

本文以下图场景为例,为您介绍如何部署企业级移动办公网络。某企业总部在阿里云华东2(上海)、华北 2(北京)地域创建了VPC,其中部署有云服务器ECS(Elastic Compute Service)和对象存储服务 OSS(Object Storage Service),企业的总部会定期将数据备份到阿里云OSS中,企业有时会需要从OSS中 读取数据并和云上ECS进行交互访问。企业现在需要部署移动办公网络,实现终端(电脑端和手机)直接拨 号通过内网加密安全上云。

- 企业总部通过物理专线接入阿里云。
- 企业IDC利用SAG硬件通过公网就近加密接入阿里云。
- 针对长期出差在外的商务人士移动办公场景,利用智能接入网关APP就近加密接入阿里云访问业务系统。

• 关于图中涉及的办公网络部署,请参见SAG双机旁挂静态路由上云方案。



方案组成

企业级移动办公解决方案主要通过以下产品实现:

• 云企业网CEN (Cloud Enterprise Network)

云企业网提供一种能够快速构建混合云和分布式业务系统的全球网络的方法,可帮助您打造一张具有企业 级规模和通信能力的云上网络。更多信息,请参见什么是云企业网。

• 云连接网CCN (CloudConnect Network)

云连接网是阿里云SD-WAN终端的接入网络,由分布在各地的接入点构成。云连接网依托阿里云的优质网络和底层网络优化技术,为您提供高质量的广域网接入网络服务。更多信息,请参见云连接网介绍。

● 智能接入网关SAG (Smart Access Gateway)

智能接入网关是阿里云的SD-WAN终端,具有多种软硬件的产品形态,可以适应大中小型企业分支和移动 办公场景的需要,快速就近地帮您接入云连接网。部署维护简单方便,可支持集中配置和监控,大大降低 维护难度。更多信息,请参见什么是智能接入网关。

● 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VPC安全可靠的连接。VPN网关提供IPsec-VPN连接和SSL-VPN连接。更多信息,请 参见什么是VPN网关。

方案优势

• 一站式解决方案

一套方案解决多种场景需要。

● 网络资源优势

能够提供灵活可靠且合规的组网服务。

• 云网融合能力

可以与阿里云的其它云服务无缝扩展集成。

准备工作

开始前,请确保您已经满足以下条件:

您已经注册了阿里云账号。如未注册,请先完成账号注册。

您已经在阿里云华东2(上海)、华北2(北京)地域创建了VPC。具体操作,请参见创建和管理专有网络。

配置步骤



步骤一: 创建云连接网

要将智能接入网关实例所连接的线下分支机构接入阿里云,您必须先创建一个云连接网,然后将智能接入网 关实例添加到云连接网内,再将云连接网和云企业网绑定,实现线下分支机构和云上互通。

- 1. 登录智能接入网关管理控制台。
- 2. 在左侧导航栏,单击云连接网。
- 3. 单击创建云连接网。
- 4. 在创建云连接网面板, 配置云连接网名称。

云连接网名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)或短划线 (-)。

5. 单击确定。

步骤二: 创建CEN实例

在使用云企业网进行网络互通前,您需要先创建一个云企业网实例。

1. 规划网络。

要互连的网络实例(专有网络VPC、本地数据中心关联的边界路由器VBR、本地分支或总部加入的云连 接网CCN)的所属地域和账号决定了网络互通所需的步骤。在开始使用CEN配置互连网络前,您需要明 确要互通的网络实例及所属账号和地域情况。

本示例中的网络实例信息如下所示。



- 2. 创建CEN实例。
 - i. 登录云企业网控制台。
 - ii. 在云企业网实例页面, 单击创建云企业网实例。

iii. 在创建云企业网实例面板, 配置云企业网。

创建云企业网实例			?	\times
云企业网 • 名称 ②				
test	4/128			
• 描述 📀				
	0/256			
加载网络实例				
同账号				
① 注: 已加载到云企业网的实例不允许重复加载				
 ● 实例类型 ⑦ 				
专有网络(VPC)	\sim	/		
• 地域 ⊘				
华东1(杭州)	\sim	/		
●网络实例 ②				
ye-vpc) be the second se	\sim	/		

- 名称:输入实例名称。
 名称长度为2~128个字符,以英文字母或中文开头,可包含数字、下划线()和短划线(-)
- 描述:(可选)输入实例描述信息。
 描述可以为空;或填写2~256个字符,不能以 http:// 和 https:// 开头,只能以中文或大小写英文字母。
- 加载网络实例:加载同账号下的网络实例。加载后, CEN实例内的网络实例可私网互通。
 - **实例类型**:选择要互通的实例,支持加载专有网络(VPC)、边界路由器(VBR)和云连接网 (CCN)。
 - 地域:选择所选实例的地域。
 - 网络实例:选择要加载的实例。

⑦ 说明 确保要加载的网络实例没有加入到其他的云企业网实例中。

iv. 单击**确定**。

步骤三:加载网络实例

您可以将要互通的网络实例(专有网络VPC、边界路由器VBR和云连接网CCN)连接到同一CEN实例中。连接 后,CEN会自动学习发布已连接的网络实例的路由,实现私网互通。 ⑦ 说明 确保要加载的网络实例没有加入到其他的云企业网实例中。

- 1. 登录云企业网控制台。
- 2. 在云企业网实例页面,单击已创建的CEN实例ID。
- 3. 在网络实例管理页签, 单击加载网络实例。
- 4. 在同账号页签, 配置网络实例。

同账号 跨账号
 注:已加载到云企业网的实例不允许重复加载
专有网络(VPC) ····································
• 地域 🕜
华东1(杭州) 🗸 🗸
• 网络实例 ②
ye-vpc

- **实例类型**:选择要互通的实例,支持加载专有网络(VPC)、边界路由器(VBR)和云连接网 (CCN)。
- **地域**:选择所选实例类型的所属地域。
- 网络实例:选择要加载的网络实例。
- 5. 单击确定。

步骤四:购买智能接入网关APP实例

在您使用智能接入网关APP产品前,您需要先购买一个智能接入网关APP实例。购买实例后,您可以通过实 例统一管理网络和客户端。

- 1. 登录智能接入网关管理控制台。
- 2. 在左侧导航栏,选择智能接入网关App > App实例管理。
- 3. 在智能接入网关APP页面,单击创建智能接入网关APP,根据以下信息进行购买配置。

区域	中国 其它
	中国内地中国香港
客户端账号数量	- 10 +
每账号流量套餐	5GB
超套计费方式	按使用流量计费
购买时长	1个月 2个月 3个月 4个月 5个月 6个月 更多时长 ↓ 到期自动续费
资源组	默认资源组 ▼ ② 如需创建新的资源组,您可以点击 去创建>

- 区域:智能接入网关客户端的使用地域。本示例选择中国内地。
- 客户端账号数量:客户端账号数规格,购买后可创建相应数量的账号,一般为每个需要登录的员工 创建一个账号。本示例保持默认值10。

⑦ 说明 系统默认支持购买5~1000个客户端,不同账号数规格按阶梯计费,具体请参见SAG APP计费说明。

- 每账号流量套餐:每个账号每月赠送的流量套餐规格,赠送的流量多个账号间不可共享,不支持结算到次月。默认为5 GB/月。
- 超套计费方式:每个账号实际使用流量超过赠送的流量套餐后,超出的部分按流量后付费。
- 购买时长:每个账号下套餐的使用时长,按月计算,支持自动续费。本示例保持默认值1个月。
- 资源组:每个账号下统一管理一组相关资源的容器,根据不同的业务场景,资源组可以映射为项目、 应用或组织等概念。一个资源只能归属于一个资源组。
- 4. 单击立即购买,确认订单后,完成支付。

步骤五: 配置智能接入网关APP

购买实例后,您需要在实例中进行网络配置、云企业网配置和客户端账号创建。

- 1. 在APP实例管理页面,找到已创建的APP实例,在目标实例操作列单击快捷配置。
- 2. 在快捷配置页面,根据以下信息配置网络,然后单击下一步:配置云企业网(可选)。

您需要通过网络配置,指定客户端私网网段和要绑定的云连接网(CCN)。

云连接网是智能接入网关的一个重要组成部分,将智能接入网关APP实例关联到云连接网后,实例所关 联的客户端便可以和其他已绑定到此云连接网中的网关设备互通。云连接网更多详情请参见云连接网介 绍。

实例名称/ID	
-/sag-:	
* 云连接网 🕐	
ccn-4	
主备DNS 🕜	
* 私网网段 2	
10.10.10/24	
新増 私网网段	

- 云连接网:您可通过以下两种方式选择要绑定的云连接网。本示例选择新建云连接网。
 - 选择现有云连接网:如果您已经创建了云连接网,您可以单击下方文本框,选择已创建的云连接 网实例进行绑定。
 - 新建云连接网:如果您未创建过云连接网,您可以在下方文本框中,输入云连接网实例名称,系 统会为您在本地域新建云连接网实例并自动进行绑定。

云连接网实例名称长度为2~100个字符,以大小写字母或中文开头,可包含数字、下划线(_)或 短划线(-)。

○ **主备DNS**: 非必填参数。您可以自定义智能接入网关APP实例客户端连接私网时使用的主备DNS配置。在您配置DNS后,系统会自动向客户端推送DNS配置。本示例无需填写。

0

3. 根据以下信息配置云企业网,然后单击下一步:创建客户端账号。

您可以将实例与云企业网CEN(Cloud Enterprise Network)绑定,绑定后,实例所在网络便可与云企业 网中已加载的云资源进行互访。云企业网更多信息,请参见什么是云企业网。

您可以通过以下两种方式绑定云企业网,本示例选择现有CEN进行绑定,以便客户端与云上资源互通。

实例名称/ID	
Default/ccn-	
* 绑定云企业网 ❷ ● 选择现有CFN ○ 新建CFN	
doctest/cen-	\sim

- 选择现有CEN:如果您已经创建了云企业网,您可以单击下方文本框,选择已创建的云企业网实例进行绑定。
- 新建CEN:如果您未创建过云企业网,您可以在下方文本框中,输入云企业网实例名称,系统会为您 新建云企业网实例并自动进行绑定。

云企业网实例名称长度为2~100个字符,以大小字母或中文开头,可包含数字、下划线(_)或短划线(-)。

4. 创建客户端账号。

网络配置完成后,您还需要创建客户端账号,您可以通过已创建的账号信息登录客户端,进而连接内 网。

用户名 🕐	
ta na hairte	
*邮箱地址 🕢	
1 P P a a	
是否固定IP 2	
设置带宽峰值 ❷ 2000 Kbps	
设置密码 🕢	
③ 客户端账号创建完成后,系统会自动将智能接入网关实例ID、用户名、密码以及软件APP下载安装方式发送到您指定的邮箱,请注意查收。	

5. 单击确定创建。

步骤六:使用客户端连接上云

1. 下载并安装智能接入网关APP客户端。

智能接入网关APP客户端支持部署在Windows、Android、macOS、iOS四种系统中。客户端适配详情和 获取方式请参见<mark>客户端安装说明</mark>。

2. 登录智能接入网关APP客户端。

登录时,需要输入智能接入网关APP实例ID、用户名和密码,内容如下图所示。该信息在管理员发送的邮件中可获取,如果没有收到,请联系管理员。

尊敬的阿里云用户:	
您好,感谢您使用阿里云智能接入网关软件版产品,您的管理员已为您创建了一个账号或修改了您的密码,请您妥善保管好您的账号	雪密码。
智能接入网关实例ID: sag-gf: 14g	
企业码: z) ¹ 3	
用户名: zx 67	
密码: Ⅳ 22u	
您可以 <mark>点击</mark> 下载安装阿里云网络客户装,您可以通过上述账号登录客户请修改密码,若在使用过程中忘记密码,您可以联系您的网络 或重置密码,更多帮助请获系您的管理员或参考 <mark>操作指导</mark> 。	皆理员咨询

3. 单击连接内网,连接内网。

系统显示内网已连接,表示连接成功。

步骤七:测试网络连通性

完成上述配置后,您可以通过iPerf工具,验证移动办公网络的连通性。

⑦ 说明 在您执行以下步骤前,请您先了解您VPC中的ECS实例所应用的安全组规则,确保安全组规则允许企业分支访问VPC中的ECS实例。具体操作,请参见查询安全组规则。

1. 分别在终端(PC和手机)和ECS服务器上下载并安装对应版本的iPerf工具。

2. 参考如下命令示例,使用iPerf工具检测客终端(PC和手机)和ECS服务器的网络吞吐量,如果接收到回 复报文,则表示连接成功。

⑦ 说明 单击下载iPerf工具,下载对应版本的iPerf工具。

以下命令示例仅供参考。不同厂商的设备,命令可能会有所不同。具体命令,请咨询相关设备厂商。

ECS服务器执行: iperf -s -i 1 -w 1M 终端 (PC和手机) 执行: iperf -c host -i 1 -w 1M

⑦ 说明 其中,-w表示TCP window size, host需替换成ECS实例IP地址。