# 阿里云 云企业网

# 最佳实践

文档版本: 20190910

为了无法计算的价值 | [] 阿里云

# <u>法律声明</u>

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

# 通用约定

格式	说明	样例
•	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。	禁止: 重置操作将丢失用户配置数据。
A	该类警示信息可能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,恢复业务所需 时间约10分钟。
	用于补充说明、最佳实践、窍门等,不 是用户必须了解的内容。	道 说明: 您也可以通过按Ctrl + A选中全部文件。
>	多级菜单递进。	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。	单击 确定。
courier 字体	命令。	执行 cd /d C:/windows 命令,进 入Windows系统文件夹。
##	表示参数、变量。	bae log listinstanceid Instance_ID
[]或者[a b ]	表示可选项,至多选择一个。	ipconfig[-all -t]
{}或者{a b }	表示必选项,至多选择一个。	<pre>swich {stand   slave}</pre>

# 目录

法律责旧	Т
运用幼今	т
· 但用约正	••••I
1 高速通道对等连接迁移方案	1
1.1 迁移介绍	1
1.2 已使用对等连接的VPC迁移至云企业网	2
1.3 已使用对等连接的VBR迁移至云企业网	5
1.4 迁移回滚	9
2 IDC通过BGP主备链路上云方案	.11
3 IDC双专线静态路由冗余上云方案	15
4 IDC通过VPN网关上云方案	18
5 IDC通过专线和智能接入网关主备方式上云方案	25
6 多接入方式构建企业级混合云	. 28
7 路由策略解决方案	.36
7.1 限制VPC间互通	36
7.2 限制网段间互通	43
7.3 不同IDC间通过云企业网实现互通	47
7.4 分支机构与IDC通过云企业网实现互通	52
7.5 同地域VBR通过路由策略实现静态主备路由	

# 1 高速通道对等连接迁移方案

### 1.1 迁移介绍

您可以将已使用高速通道对等连接的专有网络(VPC)和边界路由器(VBR)平滑迁移至云企业 网。云企业网(Cloud Enterprise Network,简称CEN)可以在不同专有网络之间,专有网络与 本地数据中心间搭建私网通信通道。通过自动路由分发及学习,CEN可以提高网络的快速收敛和跨 网络通信的质量,实现全网资源的互通。

### 迁移过程

在完成所需的迁移前准备工作后,您只需要将使用对等连接的VPC和VBR加载到CEN实例中,然后 进行路由管理即可。

CEN会自动学习分发已加载的网络实例的路由。在将使用对等连接的VPC或VBR加载到CEN实 例后,高速通道对等连接配置的静态路由优先于CEN的动态路由。即如果存在高速通道静态路 由,不允许任何比该静态路由更明细或与该静态路由相同的CEN路由学习进来。此时建议您将大 段路由进行拆分,在CEN完成路由学习后再删除拆分的路由,保证平稳迁移。详细迁移过程,请参 见#unique\_5和#unique\_6。

### CEN和高速通道对等连接的差异

CEN可以在不同专有网络之间,专有网络与本地数据中心间搭建私网通信通道。对比高速通道对等 连接功能,CEN的配置更加灵活简单,网络稳定性也更高,具体差异如下表所示。

对比点	云企业网	高速通道
网络连接	全网互联	单点连接
	加载到云企业网的网络实例(VPC	高速通道不具有传递性。使用高速
	和VBR)彼此之间全网互联,任何	通道互通的VPC或本地数据中心只
	两点间都可以通过云企业网建立安	能和对端的VPC互通。
	全、可靠、高速的内网通信。	
路由管理	动态学习	手动配置
	云企业网基于Fullmesh链路,动	高速通道配置过程中需要针对端到
	态学习并转发路由,提高了路由的	端进行路由配置。
	快速收敛和网络通信的质量及安全	
	性。	
		1

对比点	云企业网	高速通道
带宽管理	跨地域共享带宽包	点到点购买
	云企业网提供带宽包,带宽包按区	高速通道的带宽需要在购买高速通
	域售卖, 方便用户根据业务需要调	道时指定互通地域的带宽。购买后
	整跨地域带宽。有利于资源调配和	可以调整带宽大小,但不可以更改
	节约成本。	地域。

### 1.2 已使用对等连接的VPC迁移至云企业网

您可以将已使用高速通道对等连接的专有网络(VPC)平滑迁移至云企业网。云企业网(Cloud Enterprise Network,简称CEN)可以在不同专有网络之间,专有网络与本地数据中心间搭建私 网通信通道。通过自动路由分发及学习,CEN可以提高网络的快速收敛和跨网络通信的质量,实现 全网资源的互通。

🛕 警告:

在将VPC平滑迁移至CEN后,请不要冻结或删除华东1(杭州)地域内建立的同地域对等连接。

准备工作

如果您要使用已有的CEN实例,确保网络重叠功能已开启。

📕 说明:

如果存在未开启网络重叠功能的老实例,请开启网络重叠功能。

一云企业网								
从2018年11月15日起,只有提 云企业网跨境售卖相关说明和》	→ A2018年11月15日紀、只有費交过企业材料信息的客户才可以继续使用和购买完企业购聘機带宽包、如果您还没有要交材料请尽快通过点击元企业网聘機集委会规检查要交。(已参与过高速逐道附值合规改造的客户可忽略此消息) 元企业网聘機集类担关说明和注意事項:点击查看							
基本信息								
	ID cen-vbst	evq9			状态 可用			
	名称 ec2cen-online-ver	编辑			重疊路由功能	巳开启		
描述 - 编辑								
网络实例管理 带宽包管理	跨地域互通带宽管理 路由信息	云服务 PrivateZone F	RouteMap					
加载网络实例 刷新								
实例ID/名称	所属地域	实例类型		所属账号	加载时间	状态	操作	
vpc-gw8 27mbuzo ec2cen-c ation	德国(法兰克福)	专有网络(VPC)		1221 66553	2019-06-13 15:59:00	● 已加载	卸载	

### 迁移操作

参考以下步骤,将已使用对等连接的VPC迁移至云企业网:



### 在迁移前,确保您已经完成所需的准备工作。

- 1. 登录云企业网管理控制台。
- 2. 在云企业网实例页面,单击CEN实例ID链接。
- 3. 在网络实例管理页面,单击加载网络实例加载要迁移的VPC实例。详细说明,请参

见#unique_8。	2
-------------	---

加载	这网络	实例		?	×
	同则	行	跨账号		
	ĺ	)注:	已加载到云企业网的实例不允许重复加载		
			• 实例类型 🕜		
			边界路由器(VBR) ~		
			• 地域 🕐		
			华东1(杭州) ~		
			• 网络实例 🕜		
			≅ \$/∨br-bp17 ✓		

4. 如果需要跨地域互通,请在CEN实例中购买带宽包并配置私网互通带宽。

详细说明,请参见#unique\_9/unique\_9\_Connect\_42\_section\_gtq\_n5n\_tdb。

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CEN中。

16vaol27rmbuzo 🗈
操作
删服

6. 登录云企业网管理控制台,在路由信息页面查看路由配置。确保加载VPC后,不存在冲突路由。 高速通道对等连接配置的静态路由优先于CEN的动态路由。即如果存在高速通道静态路由,不 允许任何比该静态路由更明细或与该静态路由相同的CEN路由学习进来。此时建议您将高速通 道路由进行拆分,在CEN完成路由学习后再删除拆分的路由,保证平稳迁移。

以下图中的CEN路由172.16.1.0/24为例,该路由比指向高速通道的路由172.16.0.0/16更明 细,所以出现了路由冲突。

网络实例管理 带宽包管理 跨	地域互通带宽管理 路由信息 云脈	务 PrivateZone RouteMap			
网络实例 💛 德国(法兰克福):vpc-	gw8o67a16vaol27rmbuzo(VPC) ~ 刷制				
目标网段	发布状态	路由类型	匹配策略	路由属性	状态 下一刻
10.0.0.0/8	未发布	自定义		查看详情	可用 高速通
100.64.0.0/10	未发布	系统		亚看详情	可用 -
172.16.0.0/16	未发布	自定义		查看详情	可用 高速通
172.16.1.0/24		云企业网		查看详情	(冲突) 印度 (
192.168.1.0/24	已发布 撒回 路由冲突	系统		查看详情	可用 —

・如果采用闪断迁移,可以(在VPC控制台上)直接删除高速通道路 由172.16.0.0/16,CEN路由自动生效,完成该路由的迁移。

闪段时长和CEN路由条目数量成正比,对于重要的业务建议您使用平滑迁移方式。

- ・ 如果采用平滑迁移,需要按照比CEN路由172.16.1.0/24更明细的目标拆分,可以将路 由172.16.0.0/16拆分为172.16.1.0/25和172.16.1.128/25两条明细路由。
  - a. 在专有网络管理控制台, 找到要拆分的路由条目所在的路由表。
  - b. 单击添加路由条目分别添加两条目标网段为172.16.1.0/25和172.16.1.128/25, 下一跳 为高速通道路由器接口的路由条目。

路由表							
路由表基本信息							
	路由表ID v 名称 - 创建时间 2	tb-gw8xuys1oc8cl558 编辑 019-01-30 17:43:52	lixuu 🖻		专有网络ID 路由表类型 描述	vpc-gw8o67a16vaol27mbuzo 信 系统 - 编辑	
路由条目列表 已绑定交换	er.						
目标网段		状态	下一跳	类型	CEN中状态	ž	操作
172.16.1.128/25		●可用	ri-gw8328r2s8w9kkp31nik2 🗎 🛈	自定义			删除
172.16.1.0/25		●可用	ri-gw8328r2s8w9kkp31nik2· 📺 🛈	自定义			删除
172.16.0.0/16		●可用	ri-gw8328r2s8w9kkp31nik2 ' @ ①	自定义			删除
10.0.0.0/8 idc		●可用	ri-gw8t4oo7sq7brtvrjkbay 👜 🛈	自定义			删除

c. 添加成功后, 在VPC路由表中单击删除删除高速通道路由172.16.0.0/16。

路由表						
路由表基本信息						
	路由表ID vtb-g 名称 - 编 创建时间 2019	gw8xuys1oc8cl558i # -01-30 17:43:52	bus (B		专有网络D vpc-gw8067a16vaol27mbuzo <sup>(6)</sup> 路由表类型 系统 描述 - 編辑	
路由条目列表 已绑定交换机						
添加路由条目 刷新						
目标网段		状态	下一跳	类型	CEN中状态	操作
172.16.1.128/25		● 可用	ri-gw8328r2s8w9kkp31nik2 🕫 🛈	自定义		删除
172.16.1.0/25		●可用	ri-gw8328r2s8w9kkp31nik2* 🕞 🛈	自定义		删除
172.16.0.0/16		删除中装	ri-gw8328r2s8w9kkp31nik2 1 臣①	自定义		删除
10.0.0/8 idc		● 可用	ri-gw8t4oo7sq7brtvrjkbay 🕞 🛈	自定义		删除

### d. 单击刷新查看CEN路由是否生效。

94++94-64		
<b>珀</b> 田衣 基本信息		
路由表ID vtb-gw8xuys1c8665588kuu lle 名称 - 編編 创趣时间 2019-01-30 17:43:52	专有网络ID vpc-gw8067a16vaol27rmbuzo <sup>(2)</sup> 路由表类型 系統 描述 - 编辑	
路由条目列表 已绑定交换机		
海加港由寺日 附新		
目标网段 状态 下一跳 类型	CEN中状态	操作
172.16.1.128/25 ● 司用 ni-gw8328/289w9kkp31nik2 注① 自定义		删除
172.16.1.025 ● 可用 n-gw8328/2-80/9kbp31nk2: ⑧ 自定义		删除
10.0.0.08 ● 可用 ri-gw814007sq7brtvrjkbay : 图 印 印定义		删除
172.16.1.0/24 ● 可用 vpc-s2dgpn3og3yctty6d3ays ④ ① 云企业网		删除

e. CEN路由生效后,在VPC路由表中删除172.16.1.0/25和172.16.1.128/25两条明细路 由,完成该条路由的平滑迁移。

### 1.3 已使用对等连接的VBR迁移至云企业网

您可以将已使用高速通道对等连接的边界路由器(VBR)平滑迁移至云企业网。云企业网(Cloud Enterprise Network,简称CEN)可以在不同专有网络之间,专有网络与本地数据中心间搭建私 网通信通道。通过自动路由分发及学习,CEN可以提高网络的快速收敛和跨网络通信的质量,实现 全网资源的互通。

准备工作

如果您要使用已有的CEN实例,确保网络重叠功能已开启。



如果存在未开启网络重叠功能的老实例,请开启网络重叠功能。

云企业网	云企业网										
<ul> <li>从2018年11月</li> <li>云企业网跨境1</li> </ul>											
基本信息	基本信息										
		ID cen-v	ibst kv	q9				状态 可用			
		名称 ec2ci	en-online-ver	编辑				重疊路由功能	己开启		
		畑丞 - 踊	H								
网络实例管理	带宽包管理	跨地域互通带宽管理	路由信息	云服务	PrivateZone	RouteMap					
加戴网络实例	加载网络东明 刷新										
实例ID/名称		所属地域		实例类型	2		所属账号	加戴时间	状态	操作	
vpc-gw8 27mmbuzo ec2cen-dation 徳国(法兰克福) 专有网络(VPC)			1221 66553	2019-06-13 15:59:00	• 已加载	卸载					

#### 迁移操作

参考以下步骤,将已使用对等连接的VBR迁移至云企业网:

Ê	说明:
	クレウリ・

在迁移前,确保您已经完成所需的准备工作。

- 1. 如果VBR配置了健康检查,建议您先在高速通道控制台删除健康检查配置。
- 2. 登录云企业网管理控制台。
- 3. 在云企业网实例页面,单击CEN实例ID链接。
- 4. 在网络实例管理页面,单击加载网络实例加载要迁移的VBR和VPC实例。详细说明,请参见#unique\_8。

加载	初络实例		?	$\times$
	同账号	跨账号		
	① 注:	已加载到云企业网的实例不允许重复加载		
		• 实例类型 🕜		
		专有网络(VPC) V		
		• 地域 🕜		
		印度(孟买) >		
		• 网络实例 💿		
		VPC2/vp zcbtqamvmsw V		

5. 如果需要跨地域互通,请在CEN实例中购买带宽包并配置私网互通带宽。

详细说明,请参见#unique\_9/unique\_9\_Connect\_42\_section\_gtq\_n5n\_tdb。

6. 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CEN中。

路由表基本信息	Į.						
	路由表ID	vtb-gw8xuys1oc8cl5	58llxuu 🕒		专有网络	ID vpc-gw8o67a16vaol27mbuzo	Ē
	名称	- 编辑			路由表类	型系统	
	创建时间	2019-01-30 17:43:52	2		揕	述 - 编辑	
路由条目列表	已绑定交换材	TI.					
添加路由条目	刷新						
目标网段		状态	下一跳	类型		CEN中状态	操作
172.16.0.0/16		●可用	i-gw83t :501cw 🗄 🛈	实例ID:i-gw8 fut501cw 实例类型:ECS实例		未发布【发布】	删断

7. 如果本地IDC需要访问云服务例如OSS和PrivateZone等,请在云企业网控制台进行配置。

配置说明,请参见#unique\_11。

8. 登录云企业网管理控制台,在路由信息页面查看路由配置。确保加载VBR和VPC后,不存在冲 突路由。

高速通道对等连接配置的静态路由优先于CEN的动态路由。即如果存在高速通道静态路由,不 允许任何比该静态路由更明细或与该静态路由相同的CEN路由学习进来。此时建议您将高速通 道路由进行拆分,在CEN完成路由学习后再删除拆分的路由,保证平稳迁移。

以下图中的CEN路由192.168.1.0/24为例,该路由比指向高速通道的路由192.168.0.0/16更明 细,所以出现了路由冲突。

	ID cen-vbshh09nil7divq9 名称 ec2cen-online-ver_ 編編 描述 - 編編		11	状态 可用 養路曲功能 已开启		
网络实例管理         带宽色管理         跨地域           网络实例         >         印度 (孟买) xbr-a2dc42kpp	互通带宽管理 <mark>路由信息</mark> 云服务 Priv 6d91584ffdc0(VBR) > 刷新	vateZone RouteMap				
目标网段	发布状态	路由类型	匹配策略	路由属性	状态	下一跳
10.1.0.0/16	已发布 路由冲突	自定义		查看详情	可用	物理专线
172.16.0.0/16	未发布	自定义	14) -	查看详慎	可用	高速通道
192.168.0.0/16	未发布	自定义	9	查看评慎	可用	高速通道
192.168.1.0/24	-	云企业网	×	查看详饰	冲突	德国(法兰克福)

・如果采用闪断迁移可以直接删除高速通道路由192.168.0.0/16, CEN路由自动生效。

闪段时长和CEN路由条目数量成正比,对于重要的业务建议您使用平滑迁移方式。

- ·如果采用平滑迁移,需要按照比CEN路由192.168.1.0/24更明细的目标拆分,可以将高速通 道路由192.168.0.0/16拆分为192.168.1.0/25和192.168.1.128/25两条明细路由。
  - a. 在高速通道管理控制台VBR详情页面,单击路由条目进入VBR路由表页面。
  - b. 单击添加路由条目分别添加两条目标网段为192.168.1.0/25和192.168.1.128/25,下一 跳为专有网络的路由条目。

電通振音 / 边界局曲器 (VBR) / ybr-a3de32mg5d91584ffdc0								
< vbr-a2dc42iqp5d915	84ffdc0							
基本信息							0.00	对等连接 剧情
边界路由器 vbr	-a2dc42iqp5d91584ffdc0			名	称 ec2cen-verify-cer	n		
接入点 印度	建-孟英-A			创建时	间 2019年6月13日 15	:21:08		
状态 •	正常			云企业	cen-vbshh0l9niii7	dkvq9 🛤		
物理专线接口 路由条目 对等连接	宣告BGP网段 BGP组 BGP	邻居 云企业网授权						
<i>隣加路由条目</i> 刷新								
路由表ID	目标网段	状态	下一跳实例		下一跳灵型	路由类型	Cen发布状态	操作
vtb-a2dpygf1waw73gfq85phd	192.168.1.128/25	() 创建中	vpc-gw8o67a16vaol27rmbuzo	]	专有网络	自定义		#1139
vtb-a2dpygf1waw73gfq85phd	192.168.1.0/25	• 可用	vpc-gw8o67a16vaol27rmbuzo		专有网络	自定义		删除
vtb-a2dpygf1waw73gfq85phd	192.168.0.0/16	• 可用	vpc-gw8o67a16vaol27rmbuzo	_	专有网络	自定义	÷	删除
vtb-a2dpygf1waw73gfq85phd	172.16.0.0/16	• 可用	vpc-a2dgpn3og3yctty6d3ays		专有网络	自定义	-	#1189
vtb-a2dpygf1waw73gfq85phd	10.1.0.0/16	<ul> <li>可用</li> <li>冲突</li> </ul>	pc-a2deinish64v31yb6h3i7		物理专线接口	自定义	-	删除

c. 如果是BGP路由, 需要添加192.168.1.0/25和192.168.1.128/25相关的网段宣告。

展建連連 / 边界範曲線 (VBR) / vbr-a2dc42bgb5091584ffdc0						
< vbr-a2dc42iqp5d91584ffdc0						
基本信息		创建对等连接剧制新				
边界路由器 vbr-a2dc42lqp5d91584ffdc0	名称 e	ec2cen-verify-cen				
接入点 印度-孟买-A	创建时间 2	2019年6月13日 15:21:08				
状态 • 正常	云企业网 c	cen-vbshh0l9niii7dkvq9 解倒				
物理专线接口 路击条目 对蒂连接 <b>蓝曲BGP网段</b> BGP组 BGP邻居 云企业网段权						
<b>御奈らGPPN</b> 12 網道						
室告网段		操作				
192.168.1.0/25		BIR .				
192.168.1.128/25		副除				

### d. 删除高速通道路由192.168.0.0/16。

第28曲/ / 记序输出版 (VBR) / vbr-s2dc42ep5d9158416d0									
< vbr-a2dc42iqp5d91584ffdc0									
基本信息						£93#3	时等连接 刷新		
边界路由器	vbr-a2dc42iqp5d91584ffdc0			名称 ec2cen-verify-cen					
接入点	印度-孟买-A			创建时间 2019年6月13日15:21	:08				
状态	<ul> <li>正常</li> </ul>			云企业网 cen-vbshh0l9niii7dk	vq9 1848				
物理专线接口 路由条目 对等连接	宣告BGP网段 BGP组 BGP邻	居 云企业网授权							
<b>淡加路由条目</b> 刷新									
路由表ID	目标网段	状态	下一跳实例	下一跳类型	路由类型	Cen发布状态	操作		
vtb-a2dpygf1waw73gfq85phd	192.168.1.128/25	• 可用	vpc-gw8o67a16vaol27rmbuzo	专有网络	自定义	-	删除		
vtb-a2dpygf1waw73gfq85phd	192.168.1.0/25	• 可用	vpc-gw8o67a16vaol27rmbuzo	专有网络	自定义	-	删除		
vtb-a2dpygf1waw73gfq85phd	192.168.0.0/16	• 可用	vpc-gw8o67a16vaol27rmbuzo	专有网络	自定义	-	#1P8		
vtb-a2dpygf1waw73gfq85phd	172.16.0.0/16	• 可用	vpc-a2dgpn3og3yctty6d3ays	专有网络	自定义	3	删除		
vtb-a2dpygf1waw73gfq85phd	10.1.0.0/16	<ul> <li>可用</li> <li>冲突</li> </ul>	pc-a2deinish64v31yb6h3i7	物理专线接口	自定义		删除		

### e. 单击刷新查看CEN路由是否生效。

高速查道 / 边界题由器 (VBR) / vbr-a2dx42ipp501584ffdc0									
<vbr-a2dc42iqp5d91584ffdc0< th=""></vbr-a2dc42iqp5d91584ffdc0<>									
基本信息						(1)1±	对等连接 剧新		
边界路由署	3 vbr-a2dc42iqp5d91584ffdc0			名称 ec2cen-verify-cen		10			
接入点	图 印度-孟买-A			创建时间 2019年6月13日 15:21:	08				
状态	5. • 正常			云企业网 cen-vbshh019niii7dkw	19 解绑				
物理专线接口 路由条目 对等派	E接 宣告BGP网段 BGP组 BGP领	居 云企业网授权							
添加路由条目 刷新									
路由表ID	目标网段	状态	下一跳实例	下一跳类型	路由类型	Cen发布状态	操作		
vtb-a2dpygf1waw73gfq85phd	192.168.1.128/25	• 可用	vpc-gw8o67a16vaol27rmbuzo	专有网络	自定义	÷	删除		
vtb-a2dpygf1waw73gfq85phd	192.168.1.0/25	• 可用	vpc-gw8o67a16vaol27rmbuzo	专有网络	自定义		BUB		
vtb-a2dpygf1waw73gfq85phd	172.16.0.0/16	• 可用	vpc-a2dgpn3og3yctty6d3ays	专有网络	自定义		删除		
vtb-a2dpygf1waw73gfq85phd	10.1.0.0/16	<ul> <li>可用</li> <li>冲突</li> </ul>	pc-a2deinish64v31yb6h3i7	物理专线接口	自定义	-	删除		
vtb-a2dpygf1waw73gfq85phd	192.168.1.0/24	• 可用	vpc-gw8o67a16vaol27rmbuzo	云企业网	自定义		803		

- f. 在VBR路由表中删除192.168.1.0/25和192.168.1.128/25两条明细路由,并删除宣告 BGP路由。
- g. 在CEN控制台,为已迁移的VBR配置健康检查。配置详情,请参见#unique\_12/ unique\_12\_Connect\_42\_section\_hv3\_qzn\_tdb。

### 1.4 迁移回滚

您可以通过修改路由回滚迁移。

迁移方式不同,回滚方案也不同:

 ・ 闪断迁移:重新添加已删除的高速通道静态路由,比该高速通道静态路由更明细或相等的CEN 路由全部被删除。 · 平滑迁移: 直接添加删除的明细路由进行回滚即可。



如果迁移的VBR配置了BGP路由,VBR的路由宣告也需要同时回滚。

## 2 IDC通过BGP主备链路上云方案

本教程介绍通过专线接入和云企业网组合的方式,实现客户IDC通过主备链路上云,并和云上不同 地域VPC互通的场景。

#### 方案概述

完成以下操作,配置主备选路(主链路优先)接入阿里云:

1. 搭建冗余物理专线

创建冗余物理专线,将本地IDC接入阿里云。本地IDC和边界路由器之间配置BGP路由。

2. 配置健康检查

设置健康检查,是保障等价冗余专线链路中一条链路中断后,流量可以切换到另外一条链路的前提。详情参见#unique\_15。

- 3. 加载网络实例将需要互通的VBR和VPC加载到已创建的云企业网实例中。
- 4. 配置路由

您可以通过设置AS-Path的长度来确定路由选路的优先级。详情参见IDC侧宣告BGP路由并设置 权重。

#### 网络拓扑

本方案中使用的网络拓扑如下:

- ・本地IDC已通过专线双冗余方式连接到阿里云的不同边界路由器(VBR)。IDC和VBR之间采 用BGP路由协议。
- ・分别在北京、香港和上海地域部署了VPC。
- ・本方案中各网络的网段如下表所示。

网络	网段
本地IDC	10.1.1.0/24
北京VPC	192.168.1.0/24
香港VPC	192.168.2.0/24
上海VPC	192.168.3.0/24



### IDC侧宣告BGP路由并设置权重

假设IDC和边界路由器之间分别已经建立起BGP邻居关系(详情参见#unique\_16/ unique\_16\_Connect\_42\_section\_fxm\_rbb\_ydb)。

现在需要在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。



如上图所示,绿色链路(CPE1)为主链路,红色链路(CPE2)为备份链路,则IDC侧分别在两个 CPE的BGP配置如下表所示。

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。

配置	CPE1	CPE2	
Vlan Tag	110	120	
Network	10.1.1.0/24	10.1.1.0/24	
BGP ASN	XXX	XXX	
Interface IP	172.16.1.1/24	172.16.2.1/24	
As-Path	B,A	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。

### ・ 边界路由器BGP路由



如上图所示,在VBR1和VBR2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

0

### ・ 全量路由配置



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,但是路由权重不同,VBR1作为主选路(AS-Path短),VBR2是备选(AS-Path长),那么云企业网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重发布到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侧设置到阿里云业务地址(192.168.X.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.X.0/24 的权重,便可实现从IDC到阿里云的主备选路。

## 3 IDC双专线静态路由冗余上云方案

本教程介绍通过专线接入和云企业网组合的方式,实现客户IDC冗余专线上云,并和云上不同地 域VPC互通的场景。

#### 方案概述

完成以下操作,将本地IDC接入阿里云:

1. 搭建冗余物理专线

创建冗余物理专线,将本地IDC接入阿里云。本地IDC和边界路由器之间配置静态路由。

2. 配置健康检查(必须配置)

设置健康检查,是保障等价冗余专线链路中一条链路中断后,流量可以切换到另外一条链路的前提。在配置健康检查时,您可以将CEN中加载的VPC中任何一个未被使用的私网IP配置为 源IP,将和VBR互联的CPE接口IP配置为目标IP。详情参见#unique\_18。

3. 加载网络实例

将需要互通的VBR和VPC加载到已创建的云企业网实例中。

4. 配置和发布路由

在本地IDC和VPC中分别配置路由,详情参见IDC和VBR静态路由配置。

### 网络拓扑

本方案中使用的网络拓扑如下:

- ・本地IDC已通过专线双冗余方式连接到阿里云的不同边界路由器(VBR)。IDC和VBR之间配 置静态路由。
- ・分别在北京、香港和上海地域部署了VPC。
- 本方案中各网络的网段如下表所示。

网络	网段
本地IDC	10.1.1.0/24
北京VPC	192.168.1.0/24
香港VPC	192.168.2.0/24
上海VPC	192.168.3.0/24



### IDC和VBR静态路由配置



### 本方案中的路由配置如下:

### IDC路由配置

分别在CPE1和CPE2上配置指向阿里云的静态路由,实现IDC到云上的路由。

配置	CPE1	CPE2
目标网段	192.168.0.0/16	192.168.0.0/16
下一跳	172.16.1.2/24 (VBR1)	172.16.2.2/24 (VBR2)

### VBR路由配置

分别在VBR1和VBR2上配置指向本地IDC的静态路由,实现云上到IDC的路由。

配置	VBR1	VBR2
目标网段	10.1.1.0/24	10.1.1.0/24
下一跳	172.16.1.1/24	172.16.2.1/24

・云企业网路由



通过在VBR上进行以上路由配置,云企业网会分别将VBR1和VBR2上配置的静态路由同步到云 企业网内部。从云企业网内部看,两条专线已形成等价路由(ECMP),并且处于双活状态。

冗余容灾



当某条专线断掉后(如VBR1到CPE1),云企业网会对路由进行切换,云上所有到IDC的数据会走 VBR2,从而实现了链路的切换和容灾效果。

# 4 IDC通过VPN网关上云方案

本教程介绍通过VPN网关和云企业网组合的方式,实现客户IDC上云,并和云上不同地域VPC互通的场景。

### 方案概述

完成以下操作,将本地IDC接入阿里云:

1. 配置VPN网关

创建IPSec-VPN连接,将本地IDC接入阿里云。详情参见#unique\_20。

2. 加载网络实例

将需要互通的VBR和VPC加载到已创建的云企业网实例中。

3. 配置和发布路由

您可以将VPC中指向VPN网关的路由发布到CEN中,CEN中其他加载的网络实例便可以学习到 该条路由。

网络拓扑

本方案中使用的网络拓扑如下:

- ·本地IDC已通过VPN网关连接到阿里云。
- ・分别在杭州、北京、香港和上海地域部署了VPC。
- ·本方案中各网络的网段如下表所示,确保各VPC的地址段不冲突。

网络	网段
本地IDC	10.1.1.0/24
北京VPC	192.168.1.0/24
香港VPC	192.168.2.0/24
上海VPC	192.168.3.0/24
杭州VPC	192.168.4.0/24



本地IDC已与阿里云VPN网关之间建立起IPsec-VPN连接,并且已配置指向云上的明细路由或默认 路由:

上海VPC 192.168.3.0/24

### 表 4-1: IDC明细路由配置

目标网段	下一跳
192.168.1.0/24	VPN网关
192.168.2.0/24	VPN网关
192.168.3.0/24	VPN网关
192.168.4.0/24	VPN网关

### 表 4-2: IDC默认路由配置

目标网段	下一跳
0.0.0/0	VPN网关

### VPC路由配置



为了能够让IDC和云上的VPC之间互相通信,需要在连接VPN网关的VPC内,配置一条指向IDC 侧(VPN网关)的路由,并且宣告到CEN。

IDC侧已经配置了指向云上的路由,那么数据流量便可从云下到达云上;在杭州VPC内,配置一条回程路由指向VPN网关,便可实现流量从杭州VPC到达云下IDC。

如下图所示,您需要在杭州VPC内配置指向VPN网关(IDC)的自定义路由:

添加路由条目	3	⑦ 路由表和路由条目
	<ul> <li>● 目标网段</li> <li>10 • 1 • 1 • 0 / 24 ∨</li> <li>● 下一跳类型</li> <li>VPN网关</li> </ul>	~
	• VPN网关 LHW-test1/vpn-bp10ck5rmzhgyod9ggr87	$\sim$

在杭州VPC路由表中可以看到该条指向VPN网关的路由:

路中夷							
APLIAX							
路由表基本信	息						
	路由表ID	vtb-bp1wysoanbb8g	jm8oo7kc		专有网	络ID vpc-bp18c5hiz7xyjesxocrwq	
	名称	- 编辑			路由表	类型 系统	
	创建时间	2018-07-12 14:32:04				描述 - 编辑	
路由条目列表							
添加路由条目	刷新						
目标网段		状态	下一跳	类型		CEN中状态	操作
10.1.1.0/24		●可用	vpn-bp10ck5rmzhgyod9ggr87 ①	自定义	]	未发布 发布	删除
172.16.180.0/24	ł	●可用		系统		已发布 撤回	
100.64.0.0/10		●可用	-	系统			
10.100.0.0/24		●可用	vpc-bp13vqel9jg91c81ootv9 ①	云企业网			
172.16.181.0/24		●可用	vpc-bp1f9dk97zro7segrsoui 🛈	云企业网			

### 在CEN中宣告路由



为了能够让CEN内其他VPC学习到指向IDC的路由,需要在杭州VPC将指向VPN网关的路由发布 到CEN内,其他VPC便可学习到该条路由。

路由发布前

路由表							
路由表基本信息							
	路由表ID 名称	vtb-bp1wysoanbb8g	im8oo7kc		专有网络路由夷类	名ID vpc-bp18c5hiz7xyjesxocrwq	
	创建时间	· 第44     路田表央型 新規       2018-07-12 14:32:04     描述 - 編輯					
路由条目列表							
添加路由条目	刷新						
目标网段		状态	下一跳	类型		CEN中状态	操作
10.1.1.0/24		●可用	vpn-bp10ck5rmzhgyod9ggr87 ①	自定义		未发布发布	删除
172.16.180.0/24		●可用	-	系统		已发布 撤回	

### 路由发布后

路由表							
路由表基本信息							
	路由表ID	vtb-bp1wysoanbb8g	jm8oo7kc		专有网络	名ID vpc-bp18c5hiz7xyjesxocrwq	
	名称	- 编辑			路由表线	芝型 系统	
	创建时间	2018-07-12 14:32:04			Ħ	苗述 - 编辑	
路由条目列表							
添加路由条目	刷新						
目标网段		状态	下一跳	类型		CEN中状态	操作
10.1.1.0/24		●可用	vpn-bp10ck5rmzhgyod9ggr87 ①	自定义	(	已发布 撤回	删除
172.16.180.0/24		● 可用		系统		已发布 撤回	
100.64.0.0/10		● 可用	-	系统		-	

CEN内其他VPC路由表如下图所示。

路由著	長						
路由表望	基本信息						
	路	由表ID v	tb-bp1wuhy9In8id7d	n0edho		专有网络	ID vpc-bp1f9dk97zro7segrsoui
		名称 -	编辑			路由表类	型系统
	创	建时间 2	018-07-12 19:58:21			描	述 - 编辑
路由条[	目列表						
添加	路由条目	刷新					
目标网络	ł		状态	下一跳	类型		CEN中状态
172.16.1	81.0/24		● 可用		系统		已发布 撤回
100.64.0	).0/10		●可用	-	系统		
172.16.1	80.0/24		●可用	vpc-bp18c5hiz7xyjesxocrwq ①	云企业网		
10.100.0	).0/24		●可用	vpc-bp13vqel9jg91c81ootv9 (i)	云企业网		
10.1.1.0	/24		●可用	vpc-bp18c5hiz7xyjesxocrwq ①	云企业网		

通过以上操作,可以看到加载到CEN中的其他VPC已经学习到了该条指向IDC的路由,本地IDC便可和CEN内的任意VPC之间进行通信。

#### CEN发布路由功能说明

以上方案只是对加载到CEN中的网络实例向CEN发布或撤销路由的一种场景,对于加载到CEN中的VPC/VBR,支持如下的路由发布或撤销操作:

路由类型	路由所属实例	是否默认发布到CEN
指向ECS实例的路由	VPC	否
指向VPN网关的路由	VPC	否
指向高可用虚拟IP的路由	VPC	否
VPC系统路由	VPC	是
指向IDC的路由	VBR	是
BGP路由	VBR	是

以上发布到CEN中的路由,均可进行撤销操作。路由撤销后,CEN中将不再存在该路由条目。

对于各条自定义路由,如果已发布到CEN中,在VPC上删除该自定义路由后,该路由也将从CEN中 删除。



目前控制台只支持VPC的路由发布和撤销,VBR路由的发布和撤销操作暂不支持,您可以通过调用#unique\_21发布、撤销VBR路由条目。

# 5 IDC通过专线和智能接入网关主备方式上云方案

本方案指导您如何使用云企业网、高速通道专线和智能接入网关,使本地IDC通过专线和智能接入 网关以主备链路的方式接入阿里云,并和云上不同地域VPC互通。

本地IDC通过专线和智能接入网关两种方式连接到阿里云,实现主备冗余链路。其中,专线作为主 链路使用BGP路由协议连接边界路由器(VBR);智能接入网关通过云连接网(CCN)接入云企业 网作为备用链路。当专线出现故障时,自动切换至智能接入网关的链路,实现高可用。

网络拓扑

本方案的网络架构如下:

- ·本地IDC通过专线和智能接入网关连接到阿里云,实现冗余链路。专线上使用BGP路由协议。
- 分别在北京、香港和上海地域部署了云服务。
- ・确保各地域的VPC网段和本地数据中心的网段都不冲突。本教程中各VPC和本地数据中心 的IP地址段如下表所示。

网络	IP地址段
北京VPC	192.168.1.0/24
香港VPC	192.168.2.0/24
上海VPC	192.168.3.0/24
本地数据中心	10.1.1.0/24

·智能接入网关和专线侧的边界路由器已经加载到云企业网中。



#### 方案概述

### 云企业网内的路由优先级

当连接相同目标网段的专线和智能接入网关同时接入云企业网时,在云企业网内对两者路由的处理 优先级为:专线优于智能接入网关。

1. 专线方向宣告BGP路由

假设IDC和边界路由器之间,分别已经建立起BGP邻居关系。

现在需要在IDC侧配置向阿里云宣告的BGP网段10.1.1.0/24, IDC的CPE1配置如下表所示。

配置	示例值
Vlan Tag	110
Network	10.1.1.0/24
BGP ASN	XXX
Interface IP	172.16.1.1/24



### 2. 智能接入网关配置

1. 在智能接入网关控制台,选择和智能接入网关做主备的专线(专线永远是主链路)。

<	┃ 智能接入网关详情 sa		链路级高可用	$\times$
	基本信息		名称/ID	
	实例ID	sag-ep17ccpeef9b0tac0i	used_by_bvt_dont_delete_l//sag-ep1/ccpeetbb/tacul	
	名称	used_by_bvt_dont 编辑	●高可用方式 ⑦	
	状态	● 高线 ⑦	专线备份	~
	软件版本	1.0.0-20180417211957	⚠ 限制:只有sag-100wm支持双链路备份	
	硬件版本		<ul> <li>● 主用物理专线</li> </ul>	
	SN	sn-cenbvt	请选择	$\sim$
	高可用配置		① 注意:需要将物理专线对应的边界路由器和智能接入网关实例对应的云连接网加入同一个云企业 网实例	
	设备级	未开启 ③		
	当前使用SN			
	备用SN			

### 2. 在智能接入网关控制台, 配置智能接入网关所连接的IDC业务地址。

智能接入网关已经加载到云企业网中,需要在智能接入网关中配置IDC的业务地址 段10.1.1.0/24。

智能接入网关			网络配置	0	$\times$
创建智能接入网关			名称/ID		
实例ID/名称	绑定云连接网	带宽峰值	秋 ・ 私間開路 @		
sag-ep17ccpeef9b0tac0i -	ccn-qqpjwt1aclmxxtpng cbn_test_ccn_02	1000Mbps 变配	10.1.1.0/24		
			新增 私网网段		
			● 绑定云连接网 ⑦		
			to it that four is an up with the time		
			云连接网绑定云企业网 ⑦ 		$\sim$

### ▋ 说明:

在配置专线和智能接入网关的主备链路时,必须按照以上顺序操作。先配置主备专线,再配置智能 接入网关的业务地址。如果配置顺序相反,例如先配置IP地址,由于智能接入网关已经加载到云企 业网中,会出现地址冲突而不能添加IP地址的问题。配置详情参见主备链路配置教程。

### 3. 云企业网内路由处理



本教程中专线侧通过BGP路由协议向云企业网宣告了10.1.1.0/24网段,智能接入网关配置了业务 地址10.1.1.0/24,由于VBR和CCN分别已加载到了云企业网内,那么该地址10.1.1.0/24也会同步 到云企业网内。由于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。那么从云企业网内的其他网络实例看到达10.1.1.0/24目标地址的下一跳是专线方向的 VBR。当专线出现故障,备用链路便生效,从云上到IDC的路径会切换到智能接入网关的链路。

# 6多接入方式构建企业级混合云

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

### 网络拓扑介绍

本教程中以如下网络拓扑为例:

- ・客户分别在北京、上海、杭州和广州部署了云下IDC服务。
- ・客户也在云上部署了服务,包括北京VPC、上海VPC、杭州VPC和深圳VPC。
- ・北京IDC和上海IDC通过专线接入到阿里云接入点,并将对应的边界路由器(VBR)加载到云企 业网内。
- · 杭州IDC通过VPN网关连接到杭州VPC。
- · 广州IDC通过智能接入网关上云,并将智能接入网关所属的云连接网加载到云企业网内。
- ·分别将北京、上海、深圳和杭州的VPC加载到云企业网内。



#### IP地址规划

构建混合云网络时,必须确保所有要互通的网络地址不冲突。本教程中的网段规划如下:

网络	IP地址段
杭州IDC	10.1.1.0/24
广州IDC	10.1.2.0/24
北京IDC	10.1.3.0/24

网络	IP地址段
上海IDC	10.1.4.0/24
北京VPC	192.168.1.0/24
深圳VPC	192.168.2.0/24
上海VPC	192.168.3.0/24
杭州VPC	192.168.4.0/24

接入方式介绍

本教程中客户IDC上云的方式如下:

- ・北京、上海IDC专线接入上云
- · 杭州IDC通过VPN网关接入上云
- ・ 广州IDC通过智能接入网关上云

北京、上海IDC专线接入上云



配置说明:

- 1. 北京、上海的IDC通过专线连接到边界路由器(VBR),并且IDC和边界路由器之间已经建立 起BGP邻居关系。详细信息,请参见#unique\_25。
- 2. 北京IDC和上海IDC的CPE设备,将IDC地址段通过BGP宣告到云企业网。CPE主要配置如下。

配置	北京CPE 上海CPE	
Local BGP ASN	Α	В
Peer BGP ASN	45104	45104

配置	北京CPE	上海CPE
Network	10.1.3.0/24	10.1.4.0/24

IDC和VBR之间建立起BGP邻居关系,IDC和VBR就可以彼此学习到对方的路由信息。

### 杭州IDC通过VPN网关接入上云



### 配置说明:

- 1. 杭州IDC通过IPsec-VPN连接到杭州VPC,接入阿里云。详细信息,请参见#unique\_20。
- 2. 配置指向云上的明细路由或默认路由。

明细路由配置:

目标网段	下一跳
10.1.2.0/24	VPN网关
10.1.3.0/24	VPN网关
10.1.4.0/24	VPN网关
192.168.1.0/24	VPN网关
192.168.2.0/24	VPN网关
192.168.3.0/24	VPN网关
192.168.4.0/24	VPN网关

### 默认路由配置:

目标网段	下一跳
0.0.0.0/0	VPN网关

# 3. 为了能够让IDC和云企业网内加载的各网络实例之间互相通信,需要在连接VPN网关的VPC内,配置一条指向IDC侧(VPN网关)的路由,并且宣告到CEN内。



参考以下步骤配置路由:

a) 在VPC路由表内配置一条目标网段是10.1.1.0/24, 下一跳指向VPN网关的路由。

添加路由条		⑦ 路由表和路由条目
	• 名称 💿	6/128 🕑
	• 目标网段 10 • 0 • 0 • 0 / 24	$\sim$
	● 下一跳类型 VPN网关	$\sim$
	• VPN网关 CL-192/vpn-	$\sim$

b) 在杭州VPC内发布该路由到CEN。

┃ 路由表						
路由表基本信息						
	路由表ID	vtb-t	5 Œ		专有网络ID vpc-ti 10 回	
	名称	- 编辑			路由表类型系统	
	创建时间	2019-04-08 08:05:29			描述 - 編辑	
路由条目列表						
添加路由条目 周	新导出					
目标网段		状态	地一才	类型	CEN中状态	操作
10.1.1.0/24 route1		●可用	vpn-bj 😳 💮	自定义	未发布发布	删除
103.0.0.0/32 ENI		●可用	eni-	自定义	未发布 发布	删除

通过以上操作,CEN内的所有网络实例便可以学习到该条指向IDC的路由,本地IDC就可以和CEN内的任意网络实例互通。详细信息,请参见#unique\_26。



广州IDC通过智能接入网关上云

配置说明:

1. 在智能接入网关控制台,将智能接入网关和广州IDC通过路由对接。

← sag-ik	nduipelle.					
网络配置	基本信息					
设备管理	实例ID	sag-i				
高可用配置	实例名称	- 编辑				
	创建时间	2019年8月7日 16:5	9:50			
监控	硬件类型	SAG-1000				
	线下路由同步方式	绑定网络详情	私网SNAT	DNAT	组网图	
	🔘 动态路由 😰					
< Comparison of the second sec	添加静态路由					

2. 将智能接入网关所绑定的云连接网CCN加载到云企业网中,这样广州IDC便可以和云企业网内任 意加载的网络实例进行互通。

绑定云企业网	
名称/ID	
rre/ccn	
* 绑定云企业网 🕝	
cen1/cen-v	

互联互通

通过以上接入方式:

- ・北京、上海IDC通过专线BGP上云,VBR加载到云企业网中。
- · 杭州IDC通过VPN网关上云, 挂载VPN网关的VPC加载到云企业网中。
- · 广州IDC通过智能接入网关上云,智能接入网关关联的云连接网加载到云企业网中。

在避免路由冲突的情况下, 云企业网动态转发加载到它里面的网络实例路由, 从而构建出一张全互 联的混合云网络。



以北京CPE、北京VBR和深圳VPC为例,查看其路由表。

### 表 6-1: 北京CPE

目标网段	下一跳	路由类型
10.1.1.0/24	BGP邻居(北京VBR)	BGP路由
10.1.2.0/24	BGP邻居(北京VBR)	BGP路由
10.1.4.0/24	BGP邻居(北京VBR)	BGP路由
192.168.1.0/24	BGP邻居(北京VBR)	BGP路由
192.168.2.0/24	BGP邻居(北京VBR)	BGP路由
192.168.3.0/24	BGP邻居(北京VBR)	BGP路由
192.168.4.0/24	BGP邻居(北京VBR)	BGP路由

### 表 6-2: 北京VBR

目标网段	下一跳	路由类型
10.1.3.0/24	BGP邻居(北京CPE)	BGP路由
10.1.1.0/24	杭州VPC	云企业网路由
10.1.2.0/24	CCN	云企业网路由
10.1.4.0/24	上海VPC	云企业网路由
192.168.1.0/24	北京VPC	云企业网路由
192.168.2.0/24	深圳VPC	云企业网路由
192.168.3.0/24	上海VPC	云企业网路由

目标网段	下一跳	路由类型
192.168.4.0/24	杭州VPC	云企业网路由

表 6-3: 深圳VPC

目标网段	下一跳	路由类型
10.1.1.0/24	杭州VPC	云企业网路由
10.1.2.0/24	CCN	云企业网路由
10.1.3.0/24	北京VBR	云企业网路由
10.1.4.0/24	上海VBR	云企业网路由
192.168.1.0/24	北京VPC	云企业网路由
192.168.3.0/24	上海VPC	云企业网路由
192.168.4.0/24	杭州VPC	云企业网路由

# 7路由策略解决方案

### 7.1 限制VPC间互通

本文为您介绍如何通过路由策略功能限制加入到云企业网中的VPC间的互通关系。

前提条件

您已经创建了云企业网实例,并将需要互通的VPC加载到云企业网实例中。详细信息,请参见#unique\_29和#unique\_8。

### 背景信息

默认情况下,云企业网采取VPC与VPC/VBR/CCN间互通的策略,但在特定场景下,您可能需要限 制VPC与VPC/VBR/CCN间的互通关系。



如上图,VPC1、VPC2和VPC3均加入到云企业网中。默认情况下,VPC1、VPC2和VPC3全互 通,如果您不希望VPC1与VPC2间互通,您可以通过路由策略限制VPC1与VPC2之间的互通关 系,VPC1与VPC3、VPC2与VPC3之间依然可以互通。

### 步骤1设置拒绝VPC1访问VPC2的路由策略

完成以下操作,设置拒绝VPC1访问VPC2的路由策略。

- 1. 登录云企业网管理控制台。
- 2. 在左侧导航栏,单击云企业网实例。
- 3. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
- 4. 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。

- 5. 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。
  - ·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。本示例选择出地域网关。
  - ・匹配条件:路由策略的匹配条件。本示例输入源实例ID列表为VPC2实例ID,目的实例ID列 表为VPC1实例ID。
  - ·策略行为:选择策略行为。本示例选择拒绝。

添加路由策略		
■ 优先级 20 + - 描述		
11.1-#		
● 地域 华东1(杭州)		
● 生效方向 RegionOut		
匹配条件		
条件类型	匹配方法	匹配值
实例ID列表	源 🗌 反向匹配	vpc- × bp vpc- ×
十 添加匹配值		
<b>策略行为</b> 〇 允许 <b>ම</b> 拒绝		

### 添加路由策略后,您可以在路由信息页签下查看拒绝VPC1访问VPC2的路由。

网络实例 > 华东1(杭州):vpc-bp1n	(VPC) > 刷新					
目标网段	发布状态	路由类型	匹配策略	路由屬性	状态	下—94
100.64.0.0/10	未发布	系统		宣吾洋情	可用	-
172.16.0.0/24	已发布 撤回	系统		查查洋情	可用	-
192.168.0.0/24		云企业网	查否详情	查若详情	拒绝	华东1(杭州)

### 步骤2设置拒绝VPC2访问VPC1的路由策略

完成以下操作,设置拒绝VPC2访问VPC1的路由策略。

- 1. 在左侧导航栏,单击云企业网实例。
- 2. 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。
- 3. 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。

- 4. 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。
  - ·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。本示例选择出地域网关。
  - ・匹配条件:路由策略的匹配条件。本示例输入源实例ID列表为VPC1实例ID,目的实例ID列 表为VPC2实例ID。
  - ·策略行为:选择策略行为。本示例选择拒绝。

添加路由策略		
■ 优先级 50 + -		
<ul> <li>地域</li> <li>华东1(杭州)</li> <li>生效方向</li> </ul>		
RegionOut <b>匹配条件</b> 条件类型	匹配方法	匹配值
实例ID列表 🗸	源 🔄 反向匹配 目的 🗌 反向匹配	vpc- × b,
+ 添加匹配值 策略行为 ○ 允许 ● 拒绝		

### 添加路由策略后,您可以在路由信息页签下查看拒绝VPC2访问VPC1的路由。

网络实例 > 华东1(杭州):vpc-bp	(VPC) > 周新					
目标网段	发布状态	路由类型	匹配策略	路由屬性	状态	下一跳
0.0.0.00	未发布	自定义		查看详情	可用	NatGateway
10.0.0.0/8	未发布	系统		查香洋博	可用	classicLink
100.64.0.0/10	未发布	系统	•	查看详情	可用	-
172.16.0.0/16	未发布 没布	自定义		登着详情	可用	VpnGateway
172.16.0.0/24		云企业网	查智洋情	查看洋街	拒绝	华东1(杭州)
192.168.0.0/24	已发布 撤回	系统		查看详情	可用	-

#### 步骤3 测试网络连通性

完成以下操作,测试VPC1与VPC2的网络连通性。

- 1. 登录VPC1下的ECS1实例。
- 2. 通过ping命令pingVPC2下的ECS2实例的IP地址,验证通信是否正常。

经验证, ECS1实例不能访问ECS2实例。

```
[root@ ~]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.
^C
--- 192.168.0.1 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 15999ms
```

- 3. 登录VPC2下的ECS2实例。
- 4. 通过ping命令pingVPC1下的ECS1实例的IP地址,验证通信是否正常。

经验证, ECS2实例不能访问ECS1实例。



完成以下操作,测试VPC1与VPC3的网络连通性。

- 1. 登录VPC1下的ECS1实例。
- 2. 通过ping命令pingVPC3下的ECS3实例的IP地址,验证通信是否正常。

经验证, ECS1实例可以正常访问ECS3实例。

C:\Users\Administrator>ping 10.0.0.1
正在 Ping 10.0.0.1 具有 32 字节的数据: 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128
10.0.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = Oms, 最长 = Oms, 平均 = Oms

- 3. 登录VPC3下的ECS3实例。
- 4. 通过ping命令pingVPC1下的ECS1实例的IP地址,验证通信是否正常。

经验证, ECS3实例可以正常访问ECS1实例。

C: Wsers \Administrator>ping 172.16.0.1 正在 Ping 172.16.0.1 具有 32 字节的数据: 来自 172.16.0.1 的回复: 字节=32 时间<1ms ITL=128 172.16.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 <0% 丢失>, 往返行程的估计时间<以毫秒为单位>: 最短 = 0ms, 最长 = 0ms, 平均 = 0ms

完成以下操作,测试VPC2与VPC3的网络连通性。

- 1. 登录VPC2下的ECS2实例。
- 2. 通过ping命令pingVPC3下的ECS3实例的IP地址,验证通信是否正常。

经验证, ECS2实例可以正常访问ECS3实例。

C:\Users\Administrator>ping 10.0.0.1 正在 Ping 10.0.0.1 具有 32 字节的数据: 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 和自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 10.0.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 0ms, 最长 = 0ms, 平均 = 0ms

3. 登录VPC3下的ECS3实例。

4. 通过ping命令pingVPC2下的ECS2实例的IP地址,验证通信是否正常。

经验证, ECS3实例可以正常访问ECS2实例。

C:\Users\Administrator>ping 192.168.0.1 正在 Ping 192.168.0.1 具有 32 字节的数据: 来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=128 192.168.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 <0% 丢失>, 往返行程的估计时间<以毫秒为单位>: 最短 = 0ms, 最长 = 0ms, 平均 = 0ms

### 7.2 限制网段间互通

本文为您介绍如何通过路由策略功能限制VPC与某个网段间的互通关系。

前提条件

配置路由策略前,请确保满足以下条件:

- ・本地IDC已经通过专线与阿里云连接。详细信息,请参见#unique\_31和#unique\_32。
- · 您已经创建了云企业网实例,并将需要互通的网络实例加载到云企业网实例中。详细信息,请参见#unique\_29和#unique\_8。

背景信息

默认情况下,云企业网采取VPC与VPC/VBR/CCN各个网段间互通的策略,但在特定场景下,您可能需要限制VPC与VPC/VBR/CCN某个网段间的互通关系。



如上图,VBR通过BGP从IDC侧学习到网段1和网段2两条路由,VPC、VBR均加入到云企业网中。默认情况下,VPC与IDC网段1/IDC网段2互通。如果您不希望VPC与IDC网段1互通,您可以通过路由策略限制VPC与IDC网段1间的互通关系,VPC与IDC网段2依然可以互通。

步骤1设置拒绝通过VBR网段1路由的路由策略

完成以下操作,设置拒绝通过VBR网段1路由的路由策略。

- 1. 登录云企业网管理控制台。
- 2. 在左侧导航栏,单击云企业网实例。
- 3. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
- 4. 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。

5. 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。

- ·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。本示例添加以下两个匹配条件:
  - 源实例ID列表为VBR实例ID。
  - 路由前缀为192.168.0.0/24,且匹配方法选择精确匹配。

·策略行为:选择策略行为。本示例选择拒绝。

添加路由策略		
■ 优先级 20 + <u>-</u> 描述		
<ul> <li>●地域</li> </ul>		
华东1(杭州)		
● 生效方向		
Regionin		
匹配条件		
条件类型	匹配方法	匹配值
条件类型 实例ID列表 →	匹配方法 源 □ 反向匹配	匹配值 vbr-bp1s×
条件类型 实例ID列表 ~	匹配方法 源 □ 反向匹配 目的 □ 反向匹配	匹配值 vbr-bp1 is × 填入ID, 按回车确认
条件类型 实例ID列表 ✓	<ul> <li>匹配方法</li> <li>源 □ 反向匹配</li> <li>目的 □ 反向匹配</li> </ul>	匹配值 vbr-bp1 is × 填入ID, 按回车确认
<ul> <li>条件类型</li> <li>实例ID列表 </li> <li>路由前缀 </li> </ul>	<ul> <li>匹配方法</li> <li>源 反向匹配</li> <li>目的 反向匹配</li> <li>精确匹配 </li> </ul>	匹配值 vbr-bp1 is × 填入ID, 按回车确认 192.168.0.0/24
<ul> <li>条件类型</li> <li>(实例ID列表 ∨</li> <li>路由前缀 ∨</li> <li>+ 添加匹配値</li> </ul>	匹配方法 源 ② 反向匹配 目的 ③ 反向匹配 精确匹配	匹配值 vbr-bp1 is × 填入ID, 按回车确认 192.168.0.0/24

添加路由策略后,您可以在路由信息页签下查看VPC中已经删除了去往192.168.0.0/24的路由。

配置路由策略前:							
网络实例 > 华东1(杭州):vpc-bp1n	(9(VPC) > 周新						
目标网段	发布状态	路由类型	匹配策略	路由雇性	状态	下一跳	
100.64.0.0/10	未没布	系统		查看详情	可用	-	
172.16.0.0/24	已发布 鄉國	系统		查看洋橋	可用	-	
192.168.0.0/24		云企业网		查看详情	可用	华东1(杭州)	
配置路由策略后:							
目标网段	发布状态	路由类型	匹配策略	路由属性	状	5 下一跳	
100.64.0.0/10	未发布	系统	-	查看洋倚	可用	€ —	
172.16.0.0/24	已发布 撤回	系统		查看洋情	ग	∎ —	

### 步骤2 测试网络连通性

完成以下操作,测试VPC与IDC侧网段1的网络连通性。

- 1. 登录VPC下的ECS实例。
- 2. 通过ping命令pingIDC侧网段1的IP地址,验证通信是否正常。

经验证, ECS实例不能访问IDC侧网段1的IP地址。



完成以下操作,测试VPC与IDC侧网段2的网络连通性。

1. 登录VPC下的ECS实例。

2. 通过ping命令pingIDC侧网段2的IP地址,验证通信是否正常。

经验证, ECS实例可以访问2的IP地址。

C:\Users\Administrator>ping 10.0.0.1 正在 Ping 10.0.0.1 具有 32 字节的数据: 来自 10.0.0.1 的回复: 字节=32 时间<1ms TTL=128 10.0.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失), 往返行程的估计时间(以毫秒为单位): 最短 = 0ms, 最长 = 0ms, 平均 = 0ms

### 7.3 不同IDC间通过云企业网实现互通

本文为您介绍如何通过路由策略功能建立不同IDC间的互通关系。

前提条件

配置路由策略前,请确保满足以下条件:

- ·本地IDC已经通过专线与阿里云连接。详细信息,请参见#unique\_31和#unique\_32。
- · 您已经创建了云企业网实例,并将需要互通的网络实例加载到云企业网实例中。详细信息,请参见#unique\_29和#unique\_8。
- · 您已经购买了带宽包并设置了跨地域互通带宽。详细信息,请参见#unique\_34和#unique\_35。

### 背景信息

系统默认会在云企业网地域网关添加策略优先级为5000、策略行为为拒绝的路由策略,该条路由策略会限制VBR、CCN与加入到云企业网中的其它VBR/CCN间互通。但在特定场景下,您可能需要放通VBR、CCN与加入到云企业网中的其它VBR/CCN间的互通关系。

# (!) 注意:

删除默认路由策略可能造成路由环路,请您谨慎操作。



如上图,IDC1位于北京,通过VBR1接入阿里云;IDC2位于杭州,通过VBR2接入阿里云。VBR1 、VBR2均加入云企业网。默认情况下,IDC1与IDC2间不互通。如果您希望IDC1与IDC2间互 通,您可以通过路由策略建立VBR1与VBR2间的互通关系。

### 步骤1设置允许IDC1访问IDC2的路由策略

完成以下操作,设置允许IDC1访问IDC2的路由策略。

- 1. 登录云企业网管理控制台。
- 2. 在左侧导航栏,单击云企业网实例。
- 3. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
- 4. 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。

5. 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。

- ·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。本示例输入华北2(北京)。
- ·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。本示例添加以下两个匹配条件:
  - 源实例ID列表: VBR2实例ID。
  - 目的实例ID列表: VBR1实例ID。
- ·策略行为:选择策略行为。本示例选择允许。

添加路由策略		
<ul> <li>● 优先级</li> <li>20 ±</li> <li>-</li> <li>描述</li> </ul>		
<ul> <li>● 地域</li> </ul>		
华北2 (北京)		
● 生效方向		
RegionOut		
匹配条件		
条件类型	匹配方法	匹配值
实例ID列表 V	源 🗌 反向匹配 目的 🗌 反向匹配	vbr- bp1s vbr-2
十 添加匹配值		
<b>策略行为</b> ① 允许 ① 拒绝		

### 添加路由策略后,您可以在路由信息页签下查看允许IDC1访问IDC2的路由。

网络实例 > 华北2(北京):vbr-226						
目标网段	发布状态	路由类型	匹配策略	路由屬性	状态	下一跳
172.16.0.0/24	•	云企业网	宣晋洋情	宣吾洋侍	可用	华东1(杭州)
192.168.0.0/24	已发布	自定义		登着详情	可用	物理专线

### 步骤2设置允许IDC2访问IDC1的路由策略

完成以下操作,设置允许IDC2访问IDC1的路由策略。

- 1. 在左侧导航栏,单击云企业网实例。
- 2. 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。
- 3. 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。

4. 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。

- ·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。本示例选择出地域网关。
- ·匹配条件:路由策略的匹配条件。本示例添加以下两个匹配条件:
  - 源实例ID列表: VBR1实例ID。
  - 目的实例ID列表: VBR2实例ID。
- ·策略行为:选择策略行为。本示例选择允许。

添加路由策略		
<ul> <li>● 优先级</li> <li>20 +</li> <li>// -</li> <li>// 描述</li> </ul>		
<ul> <li>地域</li> </ul>		
华东1(杭州)		
● 生效方向		
RegionOut		
匹配条件		
条件类型	匹配方法	匹配值
实例ID列表	源 □ 反向匹配 	vbr-2zedk × vbrx bp1s
十 添加匹配值		
<b>策略行为</b> ① 允许 ① 拒绝		

#### 添加路由策略后,您可以在路由信息页签下查看允许IDC2访问IDC1的路由。

网络实例 > 华东1(杭州):vbr-bp1	a(VBR) 〜 同新					
目标网段	发布状态	路由类型	匹配策略	路由雇性	状态	下一跳
172.16.0.0/24	已发布	自定义		查否详情	可用	物理专线
192:168.0.0/24	-	云企业网	查看详情	查看详情	可用	华北2(北京)

#### 步骤3 测试网络连通性

完成以下操作,测试IDC1与IDC2间的网络连通性。

- 1. 打开IDC1下PC的cmd窗口。
- 2. 通过ping命令pingIDC2下PC的IP地址,验证通信是否正常。

经验证, IDC1下的PC可以访问IDC2下的PC。

C:\Users\Administrator>ping 172.16.0.1 正在 Ping 172.16.0.1 具有 32 字节的数据: 自 172.16.0.1 的回复: 3 **≤†5=32** 日寸旧<1ms TTL=128 4自 172.16.0.1 的回复: 字节=32 时间<1ms TTL=128 百 172.16.0.1 的回复: 字节=32 时间<1ms TTL=128 白 172.16.0.1 的回复: 字节=32 时间<1ms TTL=128 172.16.0.1 的 Ping 统计信 = 4, 手失 = 0 (0% 手失) 己发送 = **4.** F 据句:F 1接收 时间く以る 的估 里位〉: Øms

- 3. 打开IDC2下PC的cmd窗口。
- 4. 通过ping命令pingIDC1下PC的IP地址,验证通信是否正常。

经验证, IDC2下的PC可以访问IDC1下的PC。

C:\Users\Administrator>ping 192.168.0.1 正在 Ping 192.168.0.1 具有 32 字节的数据: 自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=128 字节=32 时间<1ms TTL=128 192.168.0.1 的回复: 3 字节=32 时间<1ms TTL=128 192.168.0.1 的回复: 3 192.168.0.1 的回复: 字节=32 时间<1ms TTL=128 192.168.0.1 的 Ping 统计 句:已 发送 = 4, 丟失 = 0 <0% 丢失> = 4. 8718141 的估 Иms Π Øms

### 7.4 分支机构与IDC通过云企业网实现互通

本文为您介绍如何通过路由策略功能建立企业分支机构与IDC间的互通关系。

### 前提条件

配置路由策略前,请确保满足以下条件:

- · 您已经创建了云连接网,并将分支机构所连接的智能接入网关实例添加到云连接网内。详细信息,请参见#unique\_37和#unique\_38。
- · 您已经创建了云企业网实例,并将需要互通的网络实例加载到云企业网实例中。详细信息,请参见#unique\_29和#unique\_8。

· 您已经购买了带宽包并设置了跨地域互通带宽。详细信息,请参见#unique\_34和#unique\_35。

### 背景信息

系统默认会在云企业网地域网关添加策略优先级为5000、策略行为为拒绝的路由策略,该条路由策略会限制VBR、CCN与加入到云企业网中的其它VBR/CCN间互通。但在特定场景下,您可能需要放通VBR、CCN与加入到云企业网中的其它VBR/CCN间的互通关系。

### <u>!</u>注意:

删除默认路由策略可能造成路由环路,请您谨慎操作。



如上图,IDC位于北京,通过VBR接入阿里云。分支1位于上海,分支2位于杭州,SAG1、SAG2 均添加到CCN,VBR、CCN均加入云企业网。默认情况下,IDC不能与分支1/分支2互通。如果您 希望IDC与分支1互通,您可以通过路由策略建立IDC与分支1间的互通关系。

步骤1设置允许IDC访问分支1的路由策略

完成以下操作,设置允许IDC访问分支1的路由策略。

- 1. 登录云企业网管理控制台。
- 2. 在左侧导航栏,单击云企业网实例。
- 3. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
- 4. 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。

5. 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。

- ·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。本示例输入华北2(北京)。
- ·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。本示例添加以下两个匹配条件:
  - 源实例ID列表: SAG1实例ID。
  - 目的实例ID列表: VBR实例ID。
  - 路由前缀: 172.16.0.0/24。
- ·策略行为:选择策略行为。本示例选择允许。

添加路由策略				
<ul> <li>- 优先级</li> <li>20 <sup>+</sup>/<sub>−</sub></li> <li>描述</li> </ul>				
• <b>地域</b> 华北2 (北京)				
● <b>生效方向</b> RegionOut				
匹配条件				
条件类型		匹配方法		匹配值
实例ID列表	~	源 🔄 反向匹配 目的 🗌 反向匹配		sag-9l2 'p × vbr-2z ×
路由前缀	$\sim$	精确匹配	$\sim$	172.16.0.0/24 ×
<ul> <li>+ 添加匹配值</li> <li>第略行为</li> <li>● 允许 ○ 拒绝</li> </ul>				

### 添加路由策略后,您可以在路由信息页签下查看允许IDC访问分支1的路由。

网络实务管理 帝充包管理 野地域互通帝列 网络实例 ✓ 华北2(北京).vbr-22	管理 新田信息 PrivateZone RouteMap (VBR) / 別新					
目标网段	发布状态	路由类型	匹配策略	路由尾性	状态	下一跳
172.16.0.0/24		云企业网	查看详情	查看洋傳	可用	中国大陆云连接网
192.168.0.0/24	已发布	自定义		查看洋街	可用	物理专线

### 步骤2 设置允许CCN访问IDC的路由策略

完成以下操作,设置允许CCN访问IDC的路由策略。

- 1. 登录云企业网管理控制台。
- 2. 在左侧导航栏,单击云企业网实例。
- 3. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
- 4. 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。

5. 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。

- ·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2(上海)。
- ·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。本示例添加以下两个匹配条件:
  - 源实例ID列表: VBR实例ID。
  - 目的实例ID列表: CCN实例ID。
  - 路由前缀: 192.168.0.0/24。
- ·策略行为:选择策略行为。本示例选择允许。

添加路由策略				
■ 优先级 20 + 一 描述				
<ul> <li>■地域</li> <li>华东2(上海)</li> </ul>				
<ul> <li>生效方向</li> <li>RegionOut</li> <li>匹配条件</li> </ul>				
条件类型		匹配方法		匹配值
实例ID列表	$\sim$	源 🗌 反向匹配 目的 🗌 反向匹配		vbr-2z ×
路由前缀	$\sim$	精确匹配	$\sim$	192.168.0.0/24
<ul> <li>+ 添加匹配值</li> <li>第略行为</li> <li>● 允许 ○ 拒绝</li> </ul>				

### 添加路由策略后,您可以在路由信息页签下查看允许CCN访问IDC的路由。

网络实例 > 中国大陆云连接网:ccn-wfi	↓(CCN) ∨ 刷新					
目标网段	发布状态	路由类型	匹配策略	路由属性	状态	下一跳
172.16.0.0/24	已没布	系统		查看详情	可用	
192.168.0.0/24		云企业网		查看洋情	可用	华北2 (北京

### 步骤3 测试网络连通性

完成以下操作,测试IDC与分支1的网络连通性。

- 1. 打开IDC下PC的cmd窗口。
- 2. 通过ping命令ping分支1下的PC的IP地址,验证通信是否正常。

经验证, IDC可以访问分支1。

C:\Users\Administrator>ping 172.16.0.1	
正在 Ping 172.16.0.1 具有 32 字节的数据: 来自 172.16.0.1 的回复: 字节=32 时间<1ms 来自 172.16.0.1 的回复: 字节=32 时间<1ms 来自 172.16.0.1 的回复: 字节=32 时间<1ms 来自 172.16.0.1 的回复: 字节=32 时间<1ms	TTL=128 TTL=128 TTL=128 TTL=128 TTL=128
172.16.0.1 的 Ping 统计信息: 数据包: 已发送 = 4, 已接收 = 4, 丢失 往返行程的估计时间<以臺秒为单位>: 最短 = Oms, 最长 = Oms, 平均 = Oms	= 0 <0% 丢失>,

- 3. 打开分支1下PC的cmd窗口。
- 4. 通过ping命令pingIDC下的PC的IP地址,验证通信是否正常。

经验证,分支1可以访问IDC。

C:\Users\Administrator>ping 192.168.0.1
止任 Ping 192.168.0.1 具有 32 子下的数据:
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=128
来百 192,168,0,1 的回复: 字节=32 时间<1ms TTL=128
米目 192.168.0.1 的回复: 子卫=32 的间代1ms IIL=128
来自 192.168.0.1 的回复: 字节=32 时间<1ms TTL=128
400 460 g 4 的 piez 统计信息。
172.168.9.1 的 Ping 统计追索
- 数据包:已友诗 = 4、已接收 = 4、丢失 = 0 (0% 丢失)
往返行程的估计时间(以高频为单位);
Ims, 東大 =   Ims, 半均 =   Ims

完成以下操作,测试IDC与分支2的网络连通性。

1. 打开IDC下PC的cmd窗口。

2. 通过ping命令ping分支2下的PC的IP地址,验证通信是否正常。

经验证, IDC不能访问分支2。



### 7.5 同地域VBR通过路由策略实现静态主备路由

本文为您介绍如何通过路由策略实现同地域VBR静态主备路由。

前提条件

配置路由策略前,请确保满足以下条件:

- ·本地IDC已经通过专线与阿里云连接。详细信息,请参见#unique\_31和#unique\_32。
- · 您已经创建了云企业网实例,并将需要互通的网络实例加载到云企业网实例中。详细信息,请参见#unique\_29和#unique\_8。

背景信息

路由策略按照匹配规则允许或拒绝通过被匹配的路由,您可以通过设置路由策略规则修改允许通过 的路由的属性。



如上图,某公司在杭州拥有数据中心,该公司分别向两个运营商各申请一条专线,专线1的端口规 格为10G,专线2的端口规格为1G。VPC、VBR1、VBR2均加入云企业网,前期该公司通过负载的 方式将本地数据中心连接至阿里云,但由于专线2的端口规格较小,需将专线2备用,当专线1出现 线路故障时,流量切换至专线2。

您可以通过路由策略功能设置专线1路由的优先级高于专线2路由的优先级,实现VBR1所在的线路 为主用线路,VBR2所在的线路为备用线路。

步骤1设置VBR1所在的线路为主用线路

完成以下操作,设置VBR1所在的线路为主用线路。

- 1. 登录云企业网管理控制台。
- 2. 在左侧导航栏,单击云企业网实例。
- 3. 在云企业网实例页面,找到目标云企业网实例,单击操作列下的管理。
- 4. 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。
- 5. 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。
  - ·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。

### 🧾 说明:

添加路由策略		
■ 优先级 20 + - 描述		
● <b>地域</b> 华东1(杭州)		
● <b>生效方向</b> RegionIn		
匹配条件		
条件类型	匹配方法	匹配值
条件类型 实例ID列表		匹配值 vbr-bp10q4g8bgsztiwo1x9hs ×
条件类型 实例ID列表 >	匹配方法 源 🗌 反向匹配 目的 🗌 反向匹配	匹配值 vbr-bp10q4g8bgsztiwo1x9hs × 填入ID, 按回车确认
条件类型 实例ID列表 ✓ + 添加匹配值 策略行为 ● 允许 ○ 拒绝	匹配方法 源   反向匹配  目的   反向匹配	匹配值 vbr-bp10q4g8bgsztiwo1x9hs × 填入ID, 按回车确认
条件类型       实例ID列表     ✓       + 添加匹配值       策略行为       ① 允许     拒绝	匹配方法 源 □ 反向匹配 目的 □ 反向匹配 设置方法	匹配值 vbr-bp10q4g8bgsztiwo1x9hs × 填入ID, 按回车确认 参数值

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。

### 步骤2 设置VBR2所在线路为备用线路

完成以下操作,设置VBR2所在线路为备用线路。

- 1. 在左侧导航栏,单击云企业网实例。
- 2. 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。
- 3. 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。

4. 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。

- ·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。



添加路由策略		
<ul> <li>● 优先级</li> <li>30 + -</li> <li>描述</li> </ul>		
• 地域		
华东1(杭州)		
• 生效方向		
RegionIn		
匹配条件		
条件类型	匹配方法	匹配值
条件类型 实例ID列表	匹配方法 源 🗌 反向匹配 目的 🗌 反向匹配	匹配值 vbr-bp13 ************************************
条件类型 实例ID列表 ✓ + 添加匹配值	匹配方法 源 ② 反向匹配 目的 ③ 反向匹配	匹配值 vbr-bp13 **** ● * ● * ● * ● * ● * ● * ● * ● * ●
条件类型 实例D列表 ✓ + 添加匹配值 策略行为 ④ 允许 ○ 拒绝	匹配方法 源 ② 反向匹配 目的 ③ 反向匹配	匹配值 vbr-bp1? ************************************
条件类型       实例ID列表     ✓       + 添加匹配值       策略行为       ① 允许 ○ 拒绝	匹配方法 源 〕 反向匹配 目的 〕 反向匹配 设置方法	匹配值 vbr-bp13 ************************************
条件类型       实例ID列表     ✓       + 添加匹配值       策略行为       ① 允许     拒绝       参数类型       Preference	匹配方法   源 反向匹配   目的 反向匹配	匹配值 vbr-bp13 ************************************

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10.0.0.0/24的两条路由,其中一条为备用 路由。

地域 🗸 华东1(杭州) 🗸 期新							
目标网段	路由类型	匹配策略	路由屬性	状态	16一可	去其他地域策略	去其他地域状态
10.0.0/24	云企业网	查看详情	查看详情	备份	华东1(杭州)		可用
10.0.0/24	云企业网	查看详情	查看洋情	可用	华东1(杭州)		可用
100.64.0.0/10	系统		查看洋街	可用	华东1(杭州)		•
172.16.0.0/24	云企业网	•	查看详情	可用	华东1(杭州)	•	可用