

VPC 终端节点

最佳实践

文档版本 01
发布日期 2024-03-15



版权所有 © 华为技术有限公司 2024。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目录

1 通过 VPC 终端节点和云专线服务实现云下 IDC 访问云上服务	1
1.1 方案概述.....	1
1.2 资源和成本规划.....	3
1.3 云下 IDC 通过华为云内网访问云上资源总流程.....	4
1.4 配置步骤.....	4

1 通过 VPC 终端节点和云专线服务实现云下 IDC 访问云上服务

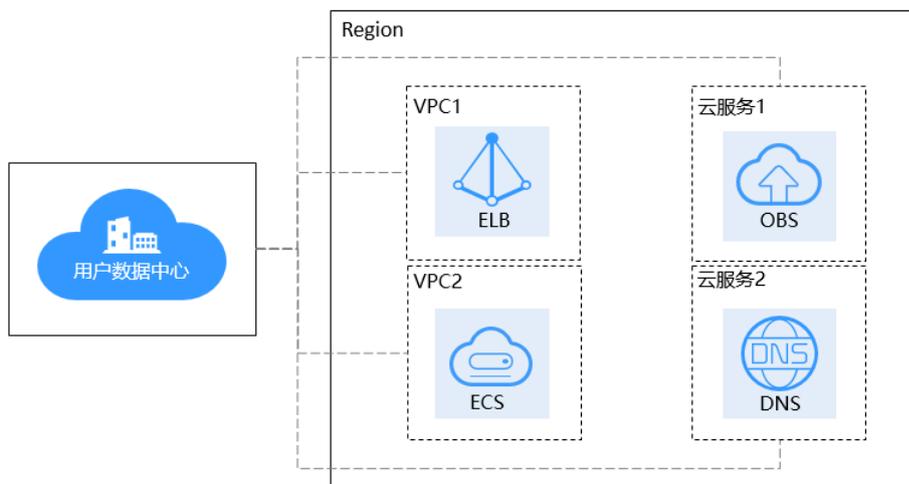
1.1 方案概述

应用场景

在企业IDC上云的过程中，用户云下IDC长期保持复杂的混合云架构：云下IDC生产、云下IDC测试、云上华为云生产、云上华为云测试、云上其他云的生产测试等等，因此经常存在云下IDC通过内网（专线或VPN）上云访问云上业务的功能需求，而单纯依赖专线或VPN上云后很多云上资源和云服务依然无法访问。

如图1-1所示，云下IDC希望通过公网的方式访问云上VPC1、VPC2内的资源（ELB、ECS）以及其他云服务（OBS、DNS）。

图 1-1 云下 IDC 访问华为云服务（业务需求）



方案架构

结合用户业务需求分析，不仅需要实现云下用户数据中心与华为云上互通，同时要不借助公网访问云上VPC内的资源和其他云服务。

本实践中主要用到以下两个服务来实现用户业务需求：

- **云专线**（Direct Connect），用于搭建用户本地数据中心与华为云VPC之间高速、低时延、稳定安全的专属连接通道，充分利用华为云服务优势的同时，继续使用现有的IT设施，实现灵活一体，可伸缩的混合云计算环境。

云专线服务在本方案中主要用于实现云下用户数据中心与华为云VPC上互通

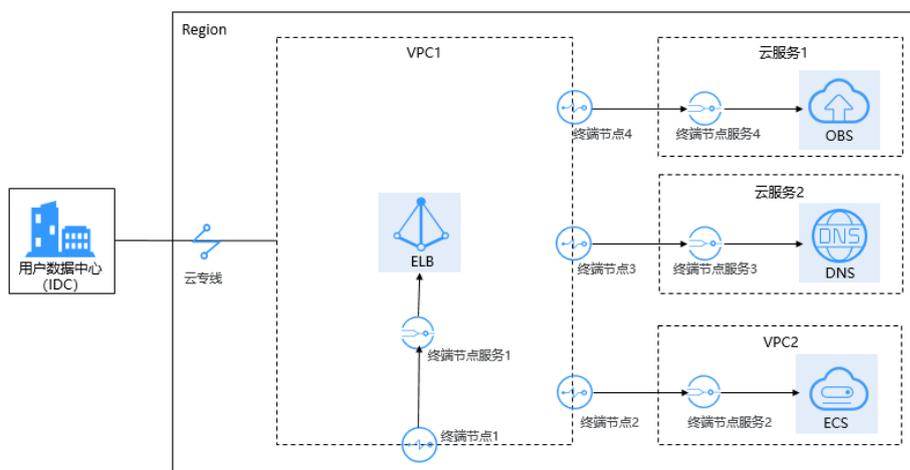
- **VPC终端节点**（VPC Endpoint），可以在VPC内提供便捷、安全、私密的通道与终端节点服务（华为云服务、用户私有服务）进行连接，该服务使用华为云内部网络，无需弹性公网IP。

VPC终端节点服务在本方案中主要用于实现通过华为云内网访问云上VPC内的资源和其他云服务。

如图1-2所示：

- 通过云专线实现云下IDC与云上VPC1互通。
- 通过终端节点1，IDC可以访问VPC1内的云资源ELB。
- 通过终端节点2，IDC可以跨VPC访问VPC2内的云资源ECS。
- 通过终端节点3，IDC可以通过内网访问云服务DNS。
- 通过终端节点4，IDC可以通过内网访问云服务OBS。

图 1-2 通过云专线和 VPC 终端节点实现云下 IDC 访问华为云服务



⚠ 注意

并非所有的云服务都支持用户云下通过VPCEP走内网访问，仅支持提供了VPCEP的服务可以通过内网访问云上资源和云服务。

方案优势

- 创建简易，响应迅速，敏捷高效。
- 无需弹性公网IP，直连内网，使用方便灵活。
- 避免泄漏服务端相关信息所带来不可知的风险，安全私密。

约束与限制

- 已拥有华为账号，并且华为账号已配置相关服务操作权限。
- 华为账号未欠费，并且有足够的金额可以购买本最佳实践所涉及的资源。
- 确定专线接入点地址并完成运营商工勘。详细请参见[准备工作](#)。
- 用户需要访问的云上资源或云服务按照VPCEP的标准开发流程已开发相关能力并上线至对应区域。

1.2 资源和成本规划

本节介绍最佳实践中资源规划情况，包含以下内容：

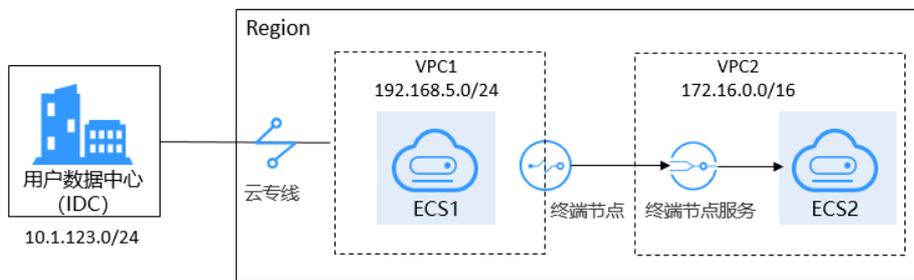
表 1-1 跨区域 VPC 互通组网规划说明

区域	资源	资源说明	数量	费用
中国-香港	VPC	VPC1子网：192.168.0.0/16 VPC2子网：172.16.0.0/16	2	免费
	物理连接	<ul style="list-style-type: none">• 虚拟网关的本端子网：192.168.5.0/24• 虚拟接口的本端网关：10.0.0.1/30• 虚拟接口的远端网关：10.0.0.2/30• 虚拟接口的远端子网：10.1.123.0/24	1	详细请参见 云专线产品价格详情 。
	弹性云服务器	自动分配IP地址。	2	详细请参见 弹性云服务器产品价格详情 。
	VPC终端节点	自动分配IP地址。	1	详细请参见 VPC终端节点产品价格详情 。

场景网络拓扑如下：

- 云下用户数据中心（IDC）通过云专线与云上VPC1建立连接。
- 云上VPC1通过终端节点访问VPC2中的云服务ECS（终端节点服务）。
- 云下IDC通过云上VPC1访问VPC2中的云服务ECS（终端节点服务）。

图 1-3 场景拓扑



1.3 云下 IDC 通过华为云内网访问云上资源总流程

本实践以云下 IDC 访问云上 VPC 内的云服务器为例。

根据用户业务需求，云下 IDC 与云上 VPC 通过云专线互通后，需要在不使用公网的情况下，实现云下 IDC 访问云上 VPC 内的云服务器。

本最佳实践的操作流程请参见图 1-4。

图 1-4 操作流程



1.4 配置步骤

步骤 1 创建云专线

1. 购买物理连接。
 - a. 登录管理控制台。
 - b. 在系统首页，单击管理控制台左上角的 ，选择区域和项目。
 - c. 在系统首页，单击管理控制台左上角的 ，选择“网络 > 云专线”。进入物理连接页面。
 - d. 在物理连接页面，单击“创建物理连接”，进入物理连接的端口购买页面。
 - e. 根据界面提示，在物理连接购买页面配置机房地址、华为云接入点、物理连接端口等信息，可参照表 1-2 输入相关参数。

表 1-2 购买物理连接参数

参数	说明
计费模式	专线服务付费方式，目前仅支持包年/包月方式付费。
请选择区域	物理连接开通的区域。用户可以在管理控制台左上角或购买页面切换区域。
物理连接名称	用户将要创建的物理连接的名称（可自定义）。
华为云接入点	物理连接接入点的位置。
运营商	提供物理连接的运营商。
端口类型	物理连接接入端口的类型：1GE，10GE、40GE、100GE。
专线带宽	物理连接的带宽大小，请在下拉框中选择对应的带宽。仅作为运营商接入带宽描述。
您的机房地址	用户填写机房地址，可精确到楼层。
标签	<p>云专线服务的标识，包括键和值。可以为云专线服务创建10个标签。标签的命名规则请参考表1-3。</p> <p>说明</p> <p>如果已经通过TMS的预定义标签功能预先创建了标签，则可以直接选择对应的标签键和值。</p> <p>预定义标签的详细内容，请参见预定义标签简介。</p> <p>如您的组织已经设定云专线服务的相关标签策略，则需按照标签策略规则为物理连接添加标签。标签不符合标签策略的规则，则可能会导致物理连接创建失败，请联系组织管理员了解标签策略详情。</p>
描述	用户可以对物理连接添加备注信息。
联系人姓名/手机/Email	用户可以在此提供用户侧专线负责人信息。
购买时长	购买服务的时长。
自动续费	自动续费时长与购买时长相同。 例如：用户购买时长为三个月，当勾选该项后，将自动续费三个月，以此类推。

参数	说明
企业项目	企业项目是一种云资源管理方式，企业项目管理服务提供统一的云资源按项目管理，以及项目内的资源管理、成员管理。

表 1-3 物理连接标签命名规则

参数	规则
键	<ul style="list-style-type: none">不能为空。对于同一资源键值唯一。长度不超过36个字符。取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。
值	<ul style="list-style-type: none">可以为空。长度不超过43个字符。取值只能包含大写字母、小写字母、数字、点、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。

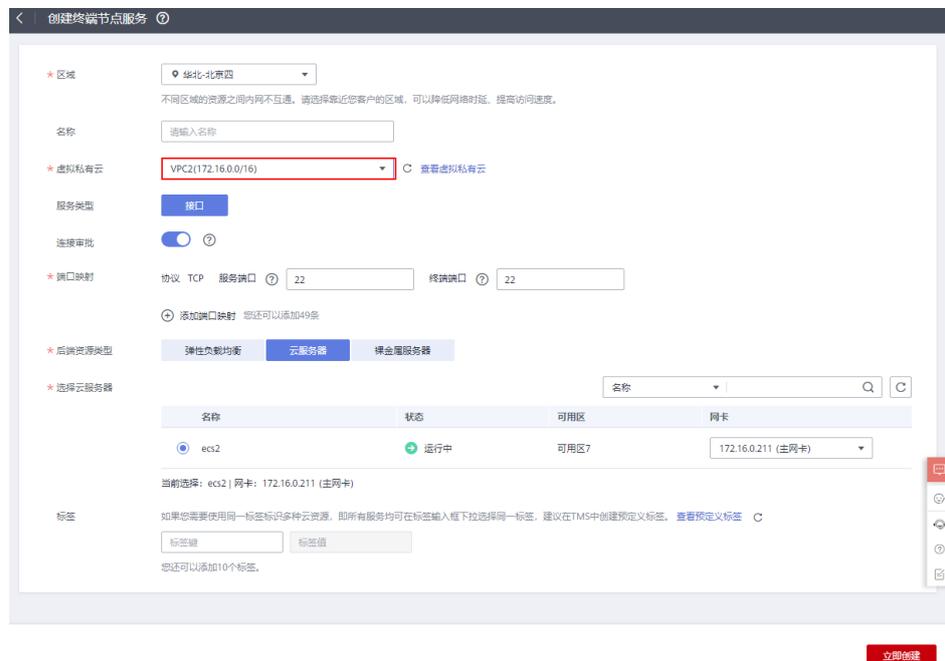
- f. 单击“确认配置”。
 - g. 确认物理连接信息，单击“去支付”。
 - h. 确认订单信息，选择付款方式，单击“确认”。
2. 开始物理连接接入。
 - a. 购买成功后，系统会为您自动分配物理连接ID，物理连接控制台会有相应的资源信息，此时您的物理连接状态为“创建中”，将会有专线经理与您联系确认施工计划和相关信息（包括公司名称、入场施工单位、期望入场时间和施工人员信息）。
 - b. 施工计划确认后，您可以根据施工计划，安排物理连接运营商部署专线，并接入机房。
 - c. 正常情况下，物理线路接入后两个工作日内，华为驻场工程师会根据客户信息将专线对接到华为云的网关端口。
 - d. 施工完成后，物理连接状态变为“正常”时，表示完成物理连接接入。
 3. 创建虚拟网关
 - a. 在左侧导航栏，选择“云专线 > 虚拟网关”。
 - b. 在虚拟网关页面，单击右上角“创建虚拟网关”。
 - c. 根据界面提示，配置相关参数。
 - d. 单击“确定”。
 4. 创建虚拟接口

- a. 在左侧导航栏，选择“云专线 > 虚拟接口”。
- b. 在虚拟接口页面，单击右上角“创建虚拟接口”。
- c. 根据界面提示，配置相关参数。
- d. 单击“立即创建”。

步骤2 创建终端节点服务

1. 在系统首页，单击管理控制台左上角的 ，选择“网络 > VPC终端节点”。
2. 在左侧导航栏，选择“VPC终端节点 > 终端节点服务”。
3. 在终端节点服务页面，单击“创建终端节点服务”。
4. 根据界面提示，配置相关参数。

图 1-5 创建终端节点服务



5. 单击“立即创建”。

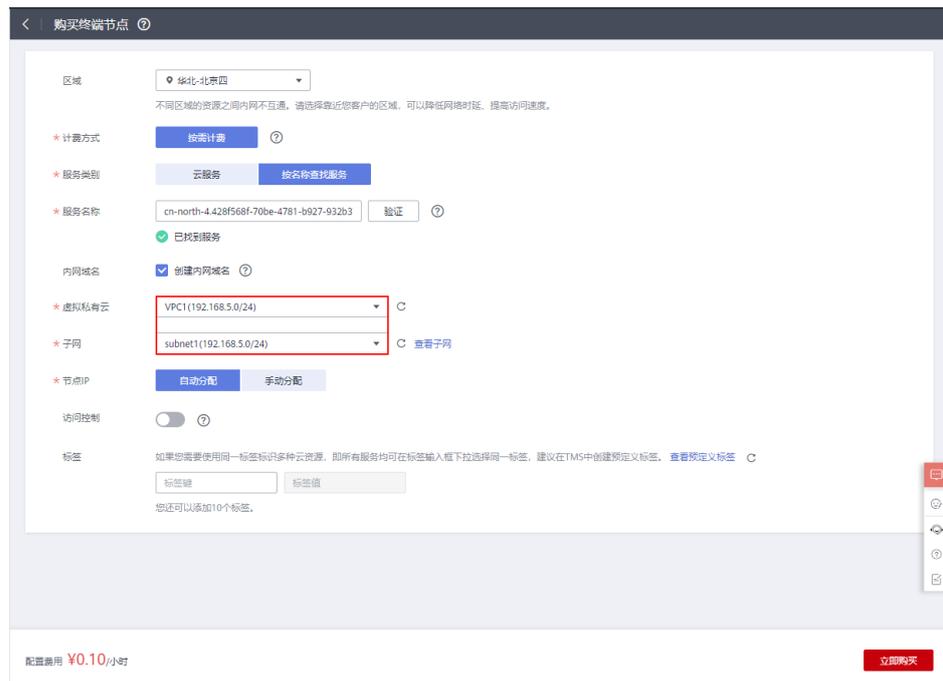
说明

在本实践中，因为创建终端节点服务时打开了“连接审批”开关，所以购买终端节点后，需要接受连接。

步骤3 创建终端节点

1. 在左侧导航栏，选择“VPC终端节点 > 终端节点”。
2. 在终端节点页面，单击“购买终端节点”。
3. 根据界面提示，配置相关参数。

图 1-6 购买终端节点



4. 单击“立即购买”。
5. 确认订单详情，单击“提交”。
6. 连接审批。

因为在步骤**步骤2**创建终端节点服务时打开了“连接审批”开关，查看终端节点状态为“待接受”，需要进行审批，操作如下：

- a. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
- b. 单击对应的终端节点服务名称，进入终端节点服务详情页面。
- c. 在终端节点服务详情页面，单击“连接管理”。
- d. 在连接管理页面的“操作”栏下，单击“接受”。

步骤4（可选）配置验证

- VPC1中的云服务器ECS1可以成功访问云下IDC

```
Authorized users only. All activities may be monitored and reported.
ecs1 login: root
Password:
Last login: Wed Nov 10 16:24:52 on tty1

Welcome to Huawei Cloud Service

[root@ecs1 ~]# ping 10.1.123.1
PING 10.1.123.1 (10.1.123.1) 56(84) bytes of data:
64 bytes from 10.1.123.1: icmp_seq=1 ttl=255 time=255 ms
64 bytes from 10.1.123.1: icmp_seq=2 ttl=255 time=5.41 ms
64 bytes from 10.1.123.1: icmp_seq=3 ttl=255 time=5.27 ms
64 bytes from 10.1.123.1: icmp_seq=4 ttl=255 time=5.42 ms
64 bytes from 10.1.123.1: icmp_seq=5 ttl=255 time=5.70 ms
^C
--- 10.1.123.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 5.274/55.320/254.793/99.736 ms
[root@ecs1 ~]#
```

- 通过终端节点IP可以成功访问VPC2中的云服务器ECS2

```
Authorized users only. All activities may be monitored and reported.
ecs1 login: root
Password:
Last login: Wed Nov 10 15:04:33 on tty1

Welcome to Huawei Cloud Service

[root@ecs1 ~]# ssh 192.168.5.111
The authenticity of host '192.168.5.111 (192.168.5.111)' can't be established.
ED25519 key fingerprint is SHA256:X3pUwri0B/u08UHJ0E2wPggjIz+uEoa7USf6Ix/nH4g.
No matching host key fingerprint found in DNS.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.5.111' (ED25519) to the list of known hosts.
Authorized users only. All activities may be monitored and reported.
root@192.168.5.111's password:
Welcome to Huawei Cloud Service

Last login: Wed Nov 10 14:54:59 2021 from 198.19.131.4
[root@ecs2 ~]#
```

----结束