VPC 终端节点

用户指南（安卡拉区域）

文档版本 01

发布日期 2024-04-12

华为技术有限公司

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


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

 版权所有 © 华为技术有限公司

目 录

1 产品介绍 1
1.1 什么是 VPC 终端节点? 1
1.2 产品优势 1
1.3 应用场景 2
1.4 约束与限制 3
1.5 与其他服务的关系 3
1.6 权限管理 4
1.7 基本概念 6
1.7.1 终端节点服务 6
1.7.2 终端节点 7
1.7.3 用户权限 8
1.7.4 区域和可用区 8
2 快速入门 10
2.1 入门指引 10
2.2 配置跨 VPC 通信的终端节点（同一账号） 10
2.2.1 简介 10
2.2.2 步骤一：创建终端节点服务 12
2.2.3 步骤二：创建终端节点 13
2.3 配置跨 VPC 通信的终端节点（不同账号） 15
2.3.1 简介 15
2.3.2 步骤一：创建终端节点服务 16
2.3.3 步骤二：添加白名单 18
2.3.4 步骤三：创建终端节点 19
3 终端节点服务管理 21
3.1 终端节点服务简介 21
3.2 创建终端节点服务 23
3.3 查看终端节点服务 24
3.4 删除终端节点服务 26
3.5 管理终端节点服务的连接审批 27
3.6 管理终端节点服务的白名单 27
3.7 查看终端节点服务的端口映射 28
4 终端节点管理 30

 版权所有 © 华为技术有限公司

4.1 终端节点简介 30
4.2 创建终端节点 30
4.3 查询并访问终端节点 33
4.4 删除终端节点 34
5 权限管理 35
5.1 创建用户并授权使用 VPCEP 35
5.2 创建 VPCEP 自定义策略 36
6 关于配额 41
7 常见问题 42
7.1 购买终端节点并关联已创建终端节点服务后，无法正常连通如何排查？ 42
7.2 VPC 终端节点和对等连接有什么区别？ 42
7.3 终端节点服务和终端节点有哪些状态？ 43
7.4 VPC 终端节点是否支持跨区域访问？ 44
A 修订记录 45

 版权所有 © 华为技术有限公司

1 产品介绍

1.1 什么是 VPC 终端节点?

VPC终端节点（VPC Endpoint），能够将VPC私密地连接到终端节点服务（云服务、用户私有服务），使VPC中的云资源无需弹性公网IP就能够访问终端节点服务，提高了访问效率，为您提供更加灵活、安全的组网方式。

产品架构

VPC终端节点由“终端节点服务”和“终端节点”两种资源实例组成。

- 终端节点服务：指将云服务或用户私有服务配置为VPC终端节点支持的服务，可以被终端节点连接和访问。
  更多内容，请参考**终端节点服务**。
- 终端节点：用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。
  更多内容，请参考**终端节点**。

更多关于VPC终端节点的组网应用信息，请参见**应用场景**。

如何访问 VPC 终端节点

VPC终端节点提供了Web化的服务管理平台，即管理控制台和基于HTTPS请求的API管理方式。

- 控制台方式
  用户可直接登录管理控制台访问VPC终端节点。
  通过管理控制台上的简单配置，可以快速的使用VPC终端节点。
- API方式
  如果用户需要将VPC终端节点集成到第三方系统，用于二次开发，请使用API方式访问VPC终端节点，具体操作请参见《VPC终端节点API参考》。

1.2 产品优势

- **性能优异**：每个网关节点可提供百万级对话，满足多种应用场景需求。

版权所有 © 华为技术有限公司

- **即创即用**：秒级创建，快速生效，迅速响应，方便用户及时使用。
- **使用灵活**：无需弹性公网IP，直连内网，使用更加灵活。
- **安全性高**：用户能够通过终端节点私密地连接到终端节点服务，避免泄漏服务端相关信息所带来不可知的风险。

1.3 应用场景

在同一区域中，VPC终端节点可以建立终端节点（VPC内云资源）到终端节点服务（用户私有服务、云服务）的便捷、安全、私密连接通道。

基于上述功能，VPC终端节点主要应用于以下场景。

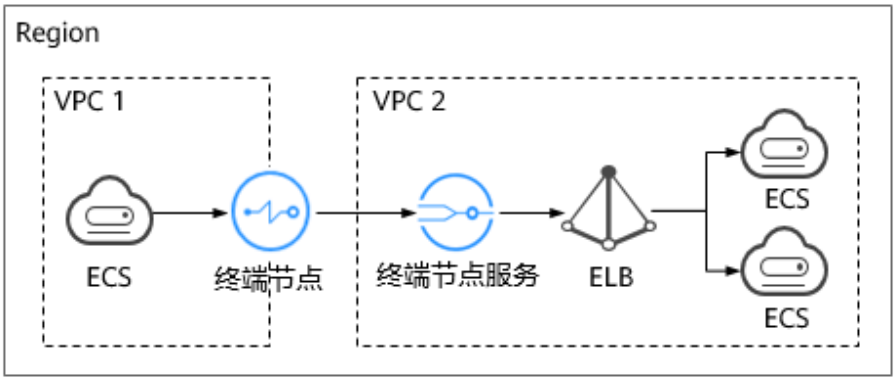
跨 VPC 连接

在同一区域中，由于VPC之间逻辑隔离，不同VPC内的云资源不能直接通信。利用在不同VPC间建立的终端节点到终端节点服务的连接通道，可以实现跨VPC的资源通信。

说明

VPC终端节点的跨VPC通信与VPC的对等连接在安全性、通信方向、路由配置等方面存在差异。详细内容，请参考《VPC终端节点用户指南》的“VPC终端节点和对等连接有什么区别？”。

图 1-1 跨 VPC 连接场景示意图



如图1-1所示，利用终端节点与终端节点服务建立的跨VPC连接通道，实现VPC 1中的云资源（如ECS）通过内网访问VPC 2中的云资源（如ELB）。

这种场景具有以下优势：

- 性能高效
  每个网关节点可支持百万级会话。
- 简化操作
  资源秒级创建，快速生效，操作简单。

具体示例请参考《VPC终端节点快速入门》的：

- 配置跨VPC通信的终端节点（同一账号）
- 配置跨VPC通信的终端节点（不同账号）

版权所有 © 华为技术有限公司

1.4 约束与限制

资源配额

VPC终端节点资源的配额限制如**表1-1**所示。

表 1-1 VPCEP 资源配额

资源	默认限制	如何提升配额
一个用户在单个区域中创建终端节点服务的数量	20个	《VPC终端节点用户指南》的“配额调整”
一个用户在单个区域中创建终端节点的数量	50个	《VPC终端节点用户指南》的“配额调整”

其他限制

- 创建终端节点时，需要确保连接的终端节点服务已经存在，并位于同一区域。
- 一个终端节点仅支持连接一个终端节点服务。
- 一个终端节点支持最大并发连接数为3000。
- 一个终端节点服务可被多个终端节点连接。
- 一个终端节点服务仅支持对应一个后端资源实例。

1.5 与其他服务的关系

VPC终端节点与其他服务的关系如**表1-2**所示。

表 1-2 与其他服务的关系

交互功能	相关服务	相关内容
用户可以将自己VPC中的服务资源配置为终端节点服务。	虚拟私有云	《VPC终端节点快速入门》的： • 配置跨VPC通信的终端节点（同一账号） • 配置跨VPC通信的终端节点（不同账号）
当企业存在多用户访问VPC终端节点服务时，可以使用IAM新建用户，以及控制这些用户账号对企业名下资源具有的操作权限。	统一身份认证服务	-

版权所有 © 华为技术有限公司

交互功能	相关服务	相关内容
由系统配置为“网关”型终端节点服务，可以创建终端节点访问该终端节点服务。	对象存储服务	《VPC终端节点用户指南》的“创建终端节点”
支持将用户私有服务创建为终端节点服务，可以创建终端节点访问该终端节点服务。	弹性负载均衡 云服务器	《VPC终端节点用户指南》的“创建终端节点服务”

1.6 权限管理

如果您需要对云服务平台上创建的VPC Endpoint云资源，为企业中的员工设置不同的访问权限，以达到不同员工之间的权限隔离，您可以使用统一身份认证服务（Identity and Access Management，简称IAM）进行精细的权限管理。该服务提供用户身份认证、权限分配、访问控制等功能，可以帮助您安全的控制云服务的访问。

通过IAM，您可以在账号中为员工创建IAM用户，并授权控制他们对云服务资源的访问范围。例如您的员工中有负责网站维护的人员，您希望他们拥有VPCEP的操作权限，但是不希望他们拥有删除其他云资源实例等高危操作的权限，那么您可以使用IAM为维护人员创建用户，通过授予仅能操作VPCEP，但是不允许操作其他云资源的权限策略，控制他们对云资源的使用范围。

如果账号已经能满足您的要求，不需要创建独立的IAM用户进行权限管理，您可以跳过本章节，不影响您使用VPC终端节点的其它功能。

IAM是云服务提供权限管理的基础服务，无需付费即可使用，您只需要为您账号中的资源进行付费。

关于IAM的详细介绍，请参见《统一身份认证服务用户指南》。

VPCEP 权限

默认情况下，账号管理员创建的IAM用户没有任何权限，需要将其加入用户组，并给用户组授予策略或角色，才能使得用户组中的用户获得对应的权限，这一过程称为授权。授权后，用户就可以基于被授予的权限对云服务进行操作。

VPCEP部署时通过物理区域划分，为项目级服务。授权时，“作用范围”需要选择“区域级项目”，然后在指定区域对应的项目中设置相关权限，并且该权限仅对此项目生效；如果在“所有项目”中设置权限，则该权限在所有区域项目中都生效。访问VPCEP时，需要先切换至授权区域。

根据授权精细程度分为角色和策略。

- 角色：IAM最初提供的一种根据用户的工作职能定义权限的粗粒度授权机制。该机制以服务为粒度，提供有限的服务相关角色用于授权。由于各服务之间存在业务依赖关系，因此给用户授予角色时，可能需要一并授予依赖的其他角色，才能正确完成业务。角色并不能满足用户对精细化授权的要求，无法完全达到企业对权限最小化的安全管控要求。
- 策略：IAM最新提供的一种细粒度授权的能力，可以精确到具体服务的操作、资源以及请求条件等。基于策略的授权是一种更加灵活的授权方式，能够满足企业

 版权所有 © 华为技术有限公司

对权限最小化的安全管控要求。例如：针对VPCEP服务，账号管理员能够控制IAM用户仅能对某一类VPCEP资源进行指定的管理操作。多数细粒度策略以API接口为粒度进行权限拆分，VPCEP支持的API授权项请参见《VPC终端节点接口参考》的“权限策略和授权项”章节。

如表1-3所示，包括了VPCEP的所有系统权限。

表 1-3 VPCEP 系统权限

系统角色/策略名称	描述	类别	依赖关系
VPCEP Administrator	VPC终端节点的所有执行权限。	系统角色	该角色有依赖，需要在同项目中勾选依赖的角色：**Server Administrator**、**VPC Administrator**。
VPCEndpoint FullAccess	VPC终端节点所有权限。	系统策略	无
VPCEndpoint ReadOnlyAccess	VPC终端节点只读权限，拥有该权限的用户仅能查看VPCEP资源。	系统策略	无

表1-4列出了VPCEP常用操作与系统权限的授权关系，您可以参照该表选择合适的系统权限。

表 1-4 常用操作与系统权限的关系

操作	VPCEndpointFullAccess	VPCEndpointReadOnlyAccess	VPCEP Administrator
创建终端节点服务	√	x	√
删除终端节点服务	√	x	√
查询终端节点服务	√	√	√
修改终端节点服务	√	x	√
接受或拒绝终端节点的连接	√	x	√
添加或移除终端节点服务的白名单	√	x	√

版权所有 © 华为技术有限公司

操作	VPCEndpointFullAccess	VPCEndpointReadOnlyAccess	VPCEP Administrator
创建终端节点	√	x	√
删除终端节点	√	x	√
修改终端节点	√	x	√
查询终端节点	√	√	√
设置终端节点的访问控制	√	x	√

相关链接

- 创建用户组、用户并授予VPCEP权限请参考《VPC终端节点用户指南》中“ 创建用户并授权使用VPCEP”章节。

相关参考

- 《统一身份认证服务用户指南》
- 《VPC终端节点用户指南》的“创建VPCEP自定义策略”章节
- 《VPC终端节点接口参考》的“权限策略和授权项”章节

1.7 基本概念

1.7.1 终端节点服务

VPC终端节点支持将云服务或者用户私有服务配置为可被终端节点访问的终端节点服务。

终端节点服务包括“网关”和“接口”两种类型。

- 网关：由系统配置的云服务类别的终端节点服务，用户无需创建，可直接使用。
- 接口：包括由系统配置的云服务类别的终端节点服务，以及由用户私有服务创建的终端节点服务。前者用户无需创建，可直接使用；后者需要用户自行创建。

“网关”型终端节点服务

“网关”型是由系统配置的云服务类别的终端节点服务，用户无需创建，可以直接使用，如表1-5所示。

说明

系统在不同区域支持的云服务不同，具体以管理控制台可配置的“服务列表”为准。

版权所有 © 华为技术有限公司

表 1-5 “网关”型终端节点服务

服务名称	服务类别	终端节点服务类型	终端节点服务示例	说明
对象存储服务	云服务	网关	无	obs：实现通过终端节点访问OBS内网地址。

“接口”型终端节点服务

“接口”型终端节点服务包括：

- 由系统配置的云服务类别的终端节点服务，用户无需创建，可以直接使用。
- 由用户私有服务创建的终端节点服务。

说明

系统在不同区域支持的云服务不同，具体以管理控制台可配置的“服务列表”为准。

表 1-6 “接口”型终端节点服务

服务名称	服务类别	终端节点服务类型	终端节点服务示例	说明
云解析服务	云服务	接口	无	dns：实现通过终端节点访问内网DNS。
弹性负载均衡	用户私有服务	接口	无	弹性负载均衡：适用于高访问量业务和对可靠性和容灾性要求较高的业务。
云服务器	用户私有服务	接口	无	ECS：作为服务器使用。

1.7.2 终端节点

终端节点用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。

在同一区域中，通过创建终端节点可以实现所属VPC内云资源跨VPC访问终端节点服务。

终端节点与终端节点服务一一对应，访问不同类型终端节点服务的终端节点存在差异：

- 访问“接口”型终端节点服务的终端节点：是具备私有IP地址的弹性网络接口，作为接口型终端节点服务的通信入口。
- 访问“网关”型终端节点服务的终端节点：是一个网关，在其上配置路由，用于将流量指向网关型终端节点服务。

版权所有 © 华为技术有限公司

1.7.3 用户权限

系统默认提供两种权限：用户管理权限和资源管理权限。

- 用户管理权限可以管理用户、用户组及用户组的权限。
- 资源管理权限可以控制用户对云服务资源执行的操作。

VPC终端节点的资源包括终端节点服务和终端节点，均属于区域级别的资源，需要在资源所在项目为用户添加权限。

1.7.4 区域和可用区

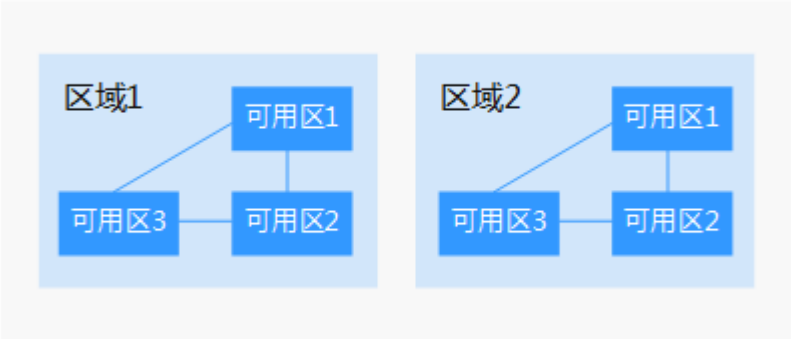
什么是区域、可用区?

区域和可用区用来描述数据中心的位置，您可以在特定的区域、可用区创建资源。

- 区域（Region）指物理的数据中心。每个区域完全独立，这样可以实现最大程度的容错能力和稳定性。资源创建成功后不能更换区域。
- 可用区（AZ，Availability Zone）是同一区域内，电力和网络互相隔离的物理区域，一个可用区不受其他可用区故障的影响。一个区域内可以有多个可用区，不同可用区之间物理隔离，但内网互通，既保障了可用区的独立性，又提供了低价、低时延的网络连接。

图1-2阐明了区域和可用区之间的关系。

图 1-2 区域和可用区



如何选择区域?

建议就近选择靠近您或者您的目标用户的区域，这样可以减少网络时延，提高访问速度。

如何选择可用区?

是否将资源放在同一可用区内，主要取决于您对容灾能力和网络时延的要求。

- 如果您的应用需要较高的容灾能力，建议您将资源部署在同一区域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，则建议您将资源创建在同一可用区内。

版权所有 © 华为技术有限公司

区域和终端节点

当您通过API使用资源时，您必须指定其区域终端节点。有关的区域和终端节点的更多信息，请参阅**地区和终端节点**。

版权所有 © 华为技术有限公司

2 快速入门

2.1 入门指引

本文以VPC终端节点的典型使用场景为例，介绍如何使用VPC终端节点，帮助您更快上手VPC终端节点。

您可以通过控制台使用VPC终端节点，更多介绍请参见**什么是VPC终端节点？**。

选择使用场景

VPC终端节点可以应用在不同的场景下，请参见**表2-1**。

表 2-1 VPC 终端节点使用场景

场景	说明
同一区域云资源的跨VPC通信	VPC终端节点支持同一区域云资源的跨VPC通信，通过创建终端节点服务和终端节点，实现云服务的跨VPC访问，包括： • **配置跨VPC通信的终端节点（同一账号）** • **配置跨VPC通信的终端节点（不同账号）**

2.2 配置跨 VPC 通信的终端节点（同一账号）

2.2.1 简介

操作场景

VPC终端节点支持同一区域云资源的跨VPC通信。

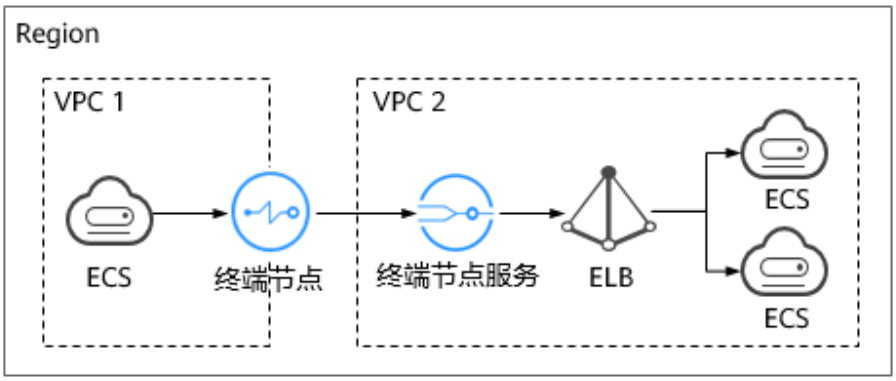
一般情况下，不同VPC内的云资源互相隔离，不支持通过私网IP访问。通过VPC终端节点，您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。

版权所有 © 华为技术有限公司

本章节主要介绍同区域“同账号”的多个VPC中的云资源如何实现跨VPC通信。

如图2-1所示，VPC1和VPC2属于同账号同区域，将VPC2中待访问的后端资源ELB创建为终端节点服务，并在VPC1中创建终端节点，实现VPC1中的ECS通过私网IP访问VPC2中的ELB。

图 2-1 跨 VPC 通信的终端节点



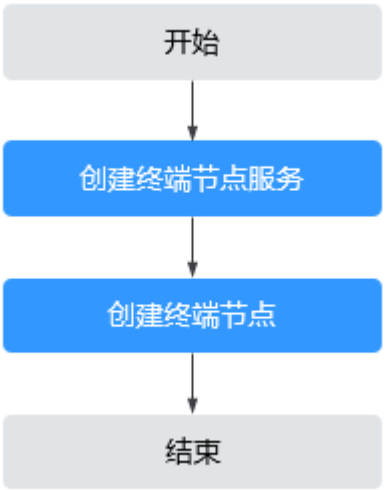
说明

- 如图2-1所示，仅支持终端节点到终端节点服务所在后端资源的单向访问。
- 若两个VPC属于不同账号，请参考**配置跨VPC通信的终端节点（不同账号）**。

操作流程

配置同一账号下的跨VPC通信，具体操作流程如图2-2所示。

图 2-2 操作流程



版权所有 © 华为技术有限公司

2.2.2 步骤一：创建终端节点服务

操作场景

为实现跨VPC通信，您需要将VPC内的云资源（即后端资源）创建为终端节点服务，以便于同一区域其他VPC的终端节点通过私网IP访问该终端节点服务。

本节以“弹性负载均衡”作为后端资源为例，指导您创建终端节点服务。

前提条件

在同一VPC内，已经完成后端资源的创建。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”，单击“创建终端节点服务”。
   进入“创建终端节点服务”页面。
5. 根据界面提示配置参数。

表 2-2 终端节点服务配置参数

参数	说明
区域	终端节点服务所在区域。 不同区域的资源之间内网不互通。请选择靠近您的区域，可以降低网络时延、提高访问速度。
虚拟私有云	终端节点服务所属虚拟私有云。
服务类型	终端节点服务的类型，此处仅支持设置为“接口”类型。
连接审批	连接审批控制的是终端节点与终端节点服务的连接是否需要审批，审批权由终端节点服务控制。 可选择开启或关闭连接审批。 若选择开启连接审批，则与本终端节点服务连接的终端节点需要进行审批，详细操作请查看**连接审批**。

版权所有 © 华为技术有限公司

参数	说明
端口映射	终端节点服务与终端节点建立连接关系，进行通信，支持TCP协议。 ● 服务端口：终端节点服务绑定了后端资源，作为提供服务的端口。 ● 终端端口：终端节点提供给用户，作为访问终端节点服务的端口。 服务端口和终端端口取值范围1～65535，单次操作最多添加50条端口映射。 **说明** 通过“终端端口 → 服务端口”的方式进行访问。
后端资源类型	实际提供服务的后端资源。 可创建为终端节点服务的后端资源包括： ● 弹性负载均衡：适用于高访问量业务和对可靠性和容灾性要求较高的业务。 ● 云服务器：作为服务器使用。 此处选择“弹性负载均衡”。 **说明** ● 终端节点服务配置的后端资源所在安全组，需要添加源地址为198.19.128.0/17的白名单入方向规则，详细操作请参考《虚拟私有云用户指南》中的“添加安全组规则”。 ● 如果终端节点服务配置的后端资源为弹性负载均衡，且弹性负载均衡开通了访问控制策略，也需要放通198.19.128.0/17。
选择负载均衡	“后端资源类型”选择为“弹性负载均衡”时，会出现该参数，在下拉列表中选择需要提供服务的负载均衡。 **说明** 弹性负载均衡作为终端节点服务的后端资源后，不支持获取真实访问客户端的地址。

6. 单击“立即创建”。
7. 返回终端节点服务列表可查看创建的终端节点服务。
8. 单击终端节点服务的“名称”，即可查看终端节点服务的详细信息。

2.2.3 步骤二：创建终端节点

操作场景

将待访问的后端资源创建为终端节点服务后，您还需要创建终端节点用于访问终端节点服务。

本节指导您创建连接终端节点服务的终端节点。

说明

终端节点需要选择与终端节点服务相同的区域和项目。

 版权所有 © 华为技术有限公司

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在“终端节点”页面，单击“创建终端节点”。
   进入“创建终端节点”页面。
5. 根据界面提示配置参数。

   表 2-3 终端节点配置参数

参数	说明
区域	终端节点所在区域，与终端节点服务所在区域保持一致。
服务类别	可选择“云服务”或“按名称查找服务”。 ● 云服务：当您要连接的终端节点服务为云服务时，需要选择“云服务”。 ● 按名称查找服务：当您要连接的终端节点服务为用户私有服务时，需要选择“按名称查找服务”。 此处选择“按名称查找服务”。
服务名称	若“服务类别”选择“按名称查找服务”，则会出现该参数。 输入**查看终端节点服务详情**中记录的终端节点服务名称，单击“验证”： ● 若显示“已找到服务”，继续后续操作。 ● 若显示“未找到服务”，请检查“区域”是否和终端节点服务所在区域一致或输入的“服务名称”是否正确。
虚拟私有云	选择终端节点所属的虚拟私有云。
子网	选择终端节点所属的子网。

6. 参数配置完成，单击“立即创建”，进行规格确认。
   - 规格确认无误，单击“提交”，任务提交成功。
   - 参数信息配置有误，需要修改，单击“上一步”，修改参数，然后单击“提交”。
7. 连接管理。
   如果终端节点状态为“已接受”，表示终端节点已成功连接至终端节点服务；如果终端节点状态为“待接受”，表示要连接的终端节点服务开启了“连接审批”功能，需要先进行审批，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”
      - 如果同意终端节点的连接，在连接管理页面的“操作”栏下，单击“接受”。

 版权所有 © 华为技术有限公司

- 如果不同意终端节点的连接，在连接管理页面的“操作”栏下，单击“拒绝”。

d. 再返回终端节点列表查看终端节点状态变为“已接受”，表示终端节点已成功连接至终端节点服务。

8. 单击终端节点ID，即可查看终端节点的详细信息。

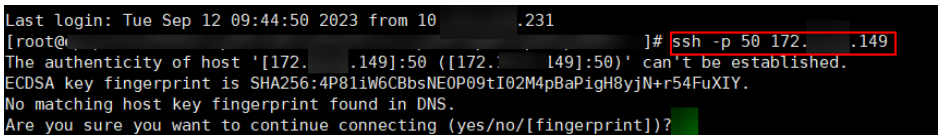
终端节点创建成功后，会生成一个“节点IP”（就是私有IP）。

您可以使用节点IP或内网域名访问终端节点服务，进行跨VPC资源通信。

配置验证

远程登录VPC1中的弹性云服务器， 访问VPC终端节点的节点IP或内网域名，详细如图2-3所示。

图 2-3 登录云服务器访问 VPC 终端节点



2.3 配置跨 VPC 通信的终端节点（不同账号）

2.3.1 简介

操作场景

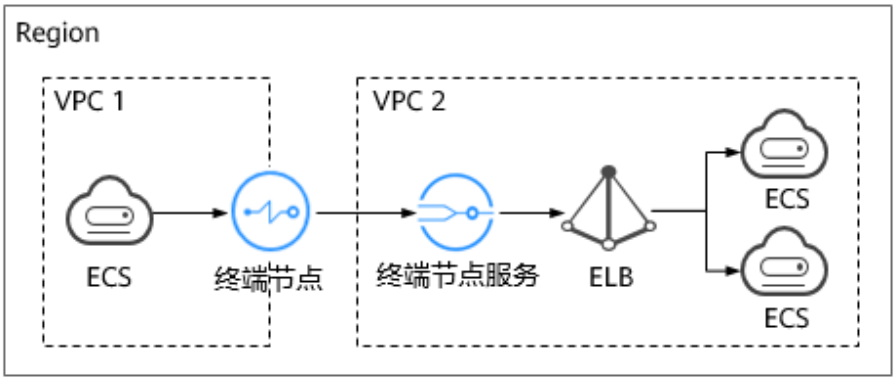
VPC终端节点支持同一区域云资源的跨VPC通信。

一般情况下，不同VPC内的云资源互相隔离，不支持通过私网IP访问。通过VPC终端节点，您可以使用私有IP地址在两个VPC之间进行通信，就像两个VPC在同一个网络中一样。

本章节主要介绍同区域“不同账号”的VPC的云资源如何实现跨VPC通信。

如图2-4所示，VPC1和VPC2分别属于账号A和账号B，将VPC2中待访问的后端资源ELB创建为终端节点服务，并在VPC1中创建终端节点，实现VPC1中的ECS通过私网IP访问VPC2中的ELB。

图 2-4 跨 VPC 通信的终端节点



版权所有 © 华为技术有限公司

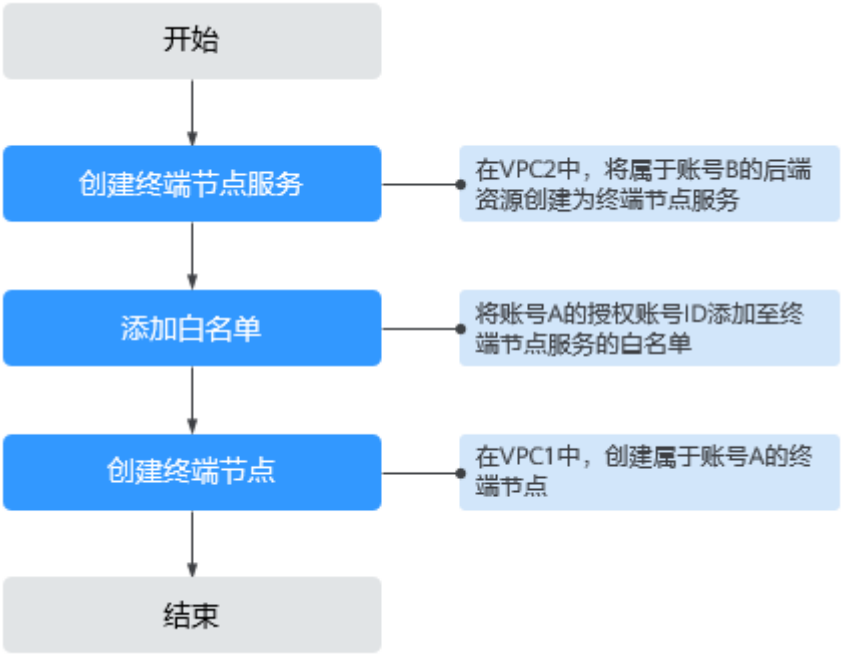
说明

- 如图2-4所示，仅支持终端节点到终端节点服务所在后端资源的单向访问。
- 在创建终端节点前，您需要先将VPC1的授权账号ID添加到VPC2的终端节点服务的白名单中。
- 若两个VPC属于同一账号，请参考**配置跨VPC通信的终端节点（同一账号）**。

操作流程

配置不同账号下的跨VPC通信，具体操作流程如图2-5所示。

图 2-5 操作流程



2.3.2 步骤一：创建终端节点服务

操作场景

为实现跨VPC通信，您需要将VPC内的云资源（即后端资源）创建为终端节点服务，以便于同一区域其他VPC的终端节点通过私网IP访问该终端节点服务。

本节以VPC2中，属于账号B的“弹性负载均衡”作为后端资源为例，指导您创建终端节点服务。

前提条件

在同一VPC内，已经完成后端资源的创建。

操作步骤

1. 登录管理控制台。

版权所有 © 华为技术有限公司

2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”，单击“创建终端节点服务”。
   进入“创建终端节点服务”页面。
5. 根据界面提示配置参数。

表 2-4 终端节点服务配置参数

参数	说明
区域	终端节点服务所在区域。 不同区域的资源之间内网不互通。请选择靠近您的区域，可以降低网络时延、提高访问速度。
虚拟私有云	终端节点服务所属虚拟私有云。
服务类型	终端节点服务的类型，此处仅支持设置为“接口”类型。
连接审批	连接审批控制的是终端节点与终端节点服务的连接是否需要审批，审批权由终端节点服务控制。 可选择开启或关闭连接审批。 若选择开启连接审批，则与本终端节点服务连接的终端节点需要进行审批，详细操作请查看**连接审批**。
端口映射	终端节点服务与终端节点建立连接关系，进行通信，支持TCP协议。 ● 服务端口：终端节点服务绑定了后端资源，作为提供服务的端口。 ● 终端端口：终端节点提供给用户，作为访问终端节点服务的端口。 服务端口和终端端口取值范围1～65535，单次操作最多添加50条端口映射。 **说明** 通过“终端端口 → 服务端口”的方式进行访问。
后端资源类型	实际提供服务的后端资源。 可创建为终端节点服务的后端资源包括： ● 弹性负载均衡：适用于高访问量业务和对可靠性和容灾性要求较高的业务。 ● 云服务器：作为服务器使用。 此处选择“弹性负载均衡”。 **说明** ● 终端节点服务配置的后端资源所在安全组，需要添加源地址为198.19.128.0/17的白名单入方向规则，详细操作请参考《虚拟私有云用户指南》中的“添加安全组规则”。 ● 如果终端节点服务配置的后端资源为弹性负载均衡，且弹性负载均衡开通了访问控制策略，也需要放通198.19.128.0/17。

 版权所有 © 华为技术有限公司

参数	说明
选择负载均衡	“后端资源类型”选择为“弹性负载均衡”时，会出现该参数，在下拉列表中选择需要提供服务的负载均衡。 **说明** 弹性负载均衡作为终端节点服务的后端资源后，不支持获取真实访问客户端的地址。

6. 单击“立即创建”。
7. 返回终端节点服务列表可查看创建的终端节点服务。
8. 单击终端节点服务的“名称”，即可查看终端节点服务的详细信息。

2.3.3 步骤二：添加白名单

操作场景

终端节点服务的权限管理用于控制是否允许跨账号的终端节点连接终端节点服务，通过设置终端节点服务的白名单实现。

在终端节点服务创建完成后，可以通过权限管理设置允许连接该终端节点服务的授权账号ID，支持添加或者移除白名单中的授权账号ID。

本操作指导您获取账号ID，并添加账号ID到终端节点服务的白名单中。

前提条件

终端节点待连接的终端节点服务已经存在。

约束与限制

- 终端节点需要与终端节点服务位于同一区域。
- 在设置前，需要获取终端节点所属的账号ID。

获取被授权的账号 ID

1. 登录管理控制台。
2. 单击账号下的“我的凭证”。
   进入“我的凭证”页面，即可查看到VPC1所属租户的“账号ID”。

添加被授权的账号 ID 至终端节点服务的白名单中

1. 在管理控制台左上角单击“ ”图标，选择区域和项目。
2. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
3. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
4. 在“终端节点服务”页面，单击需要添加白名单的终端节点服务名称。
5. 在该终端节点服务的“权限管理”页签，单击“添加白名单记录”。
6. 根据提示配置参数，输入授权用户的账号ID，添加白名单并单击“确定”。

版权所有 © 华为技术有限公司

说明

- 本账号默认在自身账号的终端节点服务的白名单中。
- 授权账号ID格式为：（iam:domain::domain_id）。
  “domain_id”表示授权用户的账号ID，例如“iam:domain::1564ec50ef2a47c791ea5536353ed4b9”。
- 添加“*”到白名单，表示所有用户可访问。

2.3.4 步骤三：创建终端节点

操作场景

在VPC2中完成终端节点服务的创建，并设置允许连接该终端节点服务的白名单之后，您可以在VPC1中创建连接终端节点服务的终端节点。

说明

终端节点需要选择与终端节点服务相同的区域和项目。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在“终端节点”页面，单击“创建终端节点”。
   进入“创建终端节点”页面。
5. 根据界面提示配置参数。

表 2-5 终端节点配置参数

参数	说明
区域	终端节点所在区域，与终端节点服务所在区域保持一致。
服务类别	可选择“云服务”或“按名称查找服务”。 ● 云服务：当您要连接的终端节点服务为云服务时，需要选择“云服务”。 ● 按名称查找服务：当您要连接的终端节点服务为用户私有服务时，需要选择“按名称查找服务”。 此处选择“按名称查找服务”。
服务名称	若“服务类别”选择“按名称查找服务”，则会出现该参数。 输入**查看终端节点服务详情**中记录的终端节点服务名称，单击“验证”： ● 若显示“已找到服务”，继续后续操作。 ● 若显示“未找到服务”，请检查“区域”是否和终端节点服务所在区域一致或输入的“服务名称”是否正确。
虚拟私有云	选择终端节点所属的虚拟私有云。

版权所有 © 华为技术有限公司

参数	说明
子网	选择终端节点所属的子网。

6. 参数配置完成，单击“立即创建”，进行规格确认。
   - 规格确认无误，单击“提交”，任务提交成功。
   - 参数信息配置有误，需要修改，单击“上一步”，修改参数，然后单击“提交”。
7. 连接管理。

   如果终端节点状态为“已接受”，表示终端节点已成功连接至终端节点服务；如果终端节点状态为“待接受”，表示要连接的终端节点服务开启了“连接审批”功能，需要先进行审批，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”
      - 如果同意终端节点的连接，在连接管理页面的“操作”栏下，单击“接受”。
      - 如果不同意终端节点的连接，在连接管理页面的“操作”栏下，单击“拒绝”。
   d. 再返回终端节点列表查看终端节点状态变为“已接受”，表示终端节点已成功连接至终端节点服务。
8. 单击终端节点ID，即可查看终端节点的详细信息。

   终端节点创建成功后，会生成一个“节点IP”（就是私有IP）。

   您可以使用节点IP或内网域名访问终端节点服务，进行跨VPC资源通信。

 版权所有 © 华为技术有限公司

3 终端节点服务管理

3.1 终端节点服务简介

VPC终端节点支持将云服务或者用户私有服务配置为可被终端节点访问的终端节点服务。

终端节点服务包括“网关”和“接口”两种类型。

- 网关：由系统配置的云服务类别的终端节点服务，用户无需创建，可直接使用。
- 接口：包括由系统配置的云服务类别的终端节点服务，以及由用户私有服务创建的终端节点服务。前者用户无需创建，可直接使用；后者需要用户自行创建。

说明

系统在不同区域支持的云服务不同，具体以管理控制台可配置的“服务列表”为准。

本章节介绍如何创建并管理由用户私有服务创建的“接口型”的终端节点服务，如**表3-1**所示。

版权所有 © 华为技术有限公司

表 3-1 终端节点服务管理说明

操作	说明	使用限制
创建终端节点服务	介绍如何将用户私有服务创建为终端节点服务。	• 终端节点服务属于区域级资源，在创建时需要设置区域和项目。 • 每个租户支持创建20个终端节点服务。 • 支持创建为终端节点服务的用户私有服务包括： – 弹性负载均衡：适用于高访问量业务和对可靠性和容灾性要求较高的业务。 – 云服务器：作为服务器使用。 • 一个终端节点服务仅支持对应一个后端资源实例。
查看终端节点服务	介绍如何查看终端节点服务的详细信息。	无
删除终端节点服务	介绍如何删除创建的终端节点服务。	• 终端节点服务删除后无法恢复，请谨慎操作。 • 仅支持删除用户创建的私有服务的终端节点服务。 • 当终端节点服务被“已接受”或者“创建中”状态的终端节点连接时，无法删除。
管理终端节点服务的连接审批	介绍如何设置终端节点服务的连接审批功能，用于控制是否允许终端节点连接终端节点服务。	仅当开启了终端节点服务的“连接审批”功能时，才支持设置是否允许终端节点连接此终端节点服务。
管理终端节点服务的白名单	介绍如何管理终端节点服务的白名单，用于控制跨租户的终端节点连接终端节点服务。	• 终端节点需要与终端节点服务位于同一区域。 • 在设置前，需要获取终端节点所属的账号ID。
查看终端节点服务的端口映射	介绍如何查看终端节点与终端节点服务通信的端口映射，包括支持的协议、服务端口以及终端端口。	• 在创建终端节点服务时，设置端口映射关系。 • 终端节点服务创建完成后，仅支持查看端口映射。

版权所有 © 华为技术有限公司

3.2 创建终端节点服务

操作场景

终端节点服务包括“网关”和“接口”两种类型。

- 网关：由系统配置的云服务类别的终端节点服务，用户无需创建，可直接使用。
- 接口：包括由系统配置的云服务类别的终端节点服务，以及由用户私有服务创建的终端节点服务。前者用户无需创建，可直接使用；后者需要用户自行创建。

本节介绍将用户私有服务创建为接口型终端节点服务的操作指导。

约束与限制

- 终端节点服务属于区域级资源，在创建时需要设置区域和项目。
- 每个租户支持创建20个终端节点服务。
- 支持创建为终端节点服务的用户私有服务包括：
  - 弹性负载均衡：适用于高访问量业务和对可靠性和容灾性要求较高的业务。
  - 云服务器：作为服务器使用。
- 一个终端节点服务仅支持对应一个后端资源实例。

前提条件

在同一VPC内，已经完成后端资源的创建。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”，单击“创建终端节点服务”。

   进入“创建终端节点服务”页面。
5. 根据界面提示配置参数，参数说明如**表1 终端节点服务配置参数**所示。

表 3-2 终端节点服务配置参数

参数	说明
区域	终端节点服务所在区域。 不同区域的资源之间内网不互通。请选择靠近您的区域，可以降低网络时延、提高访问速度。
虚拟私有云	终端节点服务所属虚拟私有云。
服务类型	终端节点服务的类型，此处仅支持设置为“接口”类型。

版权所有 © 华为技术有限公司

参数	说明
连接审批	连接审批控制的是终端节点与终端节点服务的连接是否需要审批，审批权由终端节点服务控制。 可选择开启或关闭连接审批。 若选择开启连接审批，则与本终端节点服务连接的终端节点需要进行审批，详细内容请参见**管理终端节点服务的连接审批**。
端口映射	终端节点服务与终端节点建立连接关系，进行通信，支持TCP协议。 ● 服务端口：终端节点服务绑定了后端资源，作为提供服务的端口。 ● 终端端口：终端节点提供给用户，作为访问终端节点服务的端口。 服务端口和终端端口取值范围1～65535，单次操作最多添加50条端口映射。 **说明** 通过“终端端口 → 服务端口”的方式进行访问。
后端资源类型	实际提供服务的后端资源。 可创建为终端节点服务的后端资源包括： ● 弹性负载均衡：适用于高访问量业务和对可靠性和容灾性要求较高的业务。 ● 云服务器：作为服务器使用。 此处选择“弹性负载均衡”。 **说明** ● 终端节点服务配置的后端资源所在安全组，需要添加源地址为198.19.128.0/17的白名单入方向规则，详细操作请参考《虚拟私有云用户指南》中的“添加安全组规则”。 ● 如果终端节点服务配置的后端资源为弹性负载均衡，且弹性负载均衡开通了访问控制策略，也需要放通198.19.128.0/17。
选择负载均衡	“后端资源类型”选择为“弹性负载均衡”时，会出现该参数，在下拉列表中选择需要提供服务的负载均衡。 **说明** 弹性负载均衡作为终端节点服务的后端资源后，不支持获取真实访问客户端的地址。
选择云服务器	“后端资源类型”选择为“云服务器”时，会出现该参数，在列表中选择需要提供服务的云服务器。

6. 单击“立即创建”。
7. 返回终端节点服务列表可查看创建的终端节点服务。

3.3 查看终端节点服务

操作场景

本节介绍如何查看终端节点服务的详细信息。

 版权所有 © 华为技术有限公司

通过本操作可以查看终端节点服务的名称、ID、后端资源类型、后端服务名称、虚拟私有云、状态、连接审批、服务类型、创建时间等详细信息。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“  ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”，进入“终端节点服务”页面。
5. 单击要查看的终端节点服务名称，您可以查看终端节点服务的基本信息。
   终端节点服务详情中涉及的参数如**表3-3**所示。

表 3-3 参数说明

页签	参数名称	说明
基本信息	名称	终端节点服务名称。
	ID	终端节点服务ID。
	后端资源类型	提供服务的后端资源类型。
	后端资源名称	提供服务的后端资源名称。
	虚拟私有云	终端节点服务所属VPC。
	状态	终端节点服务状态。
	连接审批	终端节点服务是否开启连接审批。
	服务类型	终端节点服务类型。
	创建时间	终端节点服务创建时间。
连接管理	终端节点ID	终端节点的ID。
	报文标识	终端节点ID的标识，用来识别是哪个终端节点。
	状态	终端节点的状态。 关于终端节点的各个状态，请查看**终端节点服务和终端节点有哪些状态？**。
	拥有者	终端节点创建者的账号ID。
	创建时间	终端节点的创建时间。
	操作	终端节点服务对终端节点的连接审批，可选择“接受”或“拒绝”。

 版权所有 © 华为技术有限公司

页签	参数名称	说明
权限管理	授权账号ID	连接访问终端节点的授权账号ID或者*。 若“授权账号ID”列为“*”，表示所有用户均可访问该终端节点服务。
	操作	对连接访问终端节点的授权账号进行操作，支持将授权账号从白名单中删除。
端口映射	协议	终端节点服务与终端节点进行通信支持的协议。
	服务端口	终端节点服务提供服务的端口。
	终端端口	终端节点访问终端节点服务的端口。

3.4 删除终端节点服务

操作场景

本节介绍如何删除终端节点服务。

说明

终端节点服务删除后无法恢复，请谨慎操作。

约束与限制

- 您只能删除由用户私有服务创建的终端节点服务，无权删除系统配置的终端节点服务。
- 当终端节点服务下存在状态为“已接受”、“创建中”的终端节点时，无法直接删除。
  终端节点服务下终端节点的状态，请参见**终端节点服务和终端节点有哪些状态？**。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 单击待删除的终端节点服务所在行“操作”栏下的“删除”按钮。
5. 在“删除终端节点服务”弹框中，单击“是”，删除终端节点服务。

版权所有 © 华为技术有限公司

3.5 管理终端节点服务的连接审批

操作场景

如果您创建终端节点服务时开启了连接审批功能，则终端节点连接该终端节点服务需要进行审批，审批权由终端节点服务控制。

终端节点服务可以选择接受或拒绝终端节点的访问。

前提条件

- 已创建连接该终端节点服务的终端节点。
- 开启了终端节点服务的“连接审批”功能。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
5. 单击需要操作的终端节点服务名称。
6. 选择“连接管理”页签。
7. 根据实际需求，对列表中的连接审批进行“接受”或“拒绝”操作。
   - 单击“接受”，表示允许终端节点连接终端节点服务。
   - 单击“拒绝”，表示拒绝终端节点连接终端节点服务。

3.6 管理终端节点服务的白名单

操作场景

终端节点服务的权限管理用于控制是否允许跨账号的终端节点连接终端节点服务，通过设置终端节点服务的白名单实现。

在终端节点服务创建完成后，可以通过权限管理设置允许连接该终端节点服务的授权账号ID，支持添加或者移除白名单中的授权账号ID。

- 如果白名单为空，则不支持跨账号的终端节点连接终端节点服务。
- 如果某一账号包含在终端节点服务的白名单中，则可以通过该账号创建连接终端节点服务的终端节点。
- 如果某一账号未包含在终端节点服务的白名单中，则无法通过该账号创建连接终端节点服务的终端节点。

本节介绍添加或删除终端节点服务白名单记录的操作指导。

 版权所有 © 华为技术有限公司

约束与限制

- 终端节点需要与终端节点服务位于同一区域。
- 在设置前，需要获取终端节点所属的账号ID。

添加白名单

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
5. 在“终端节点服务”页面，单击需要添加白名单的终端节点服务名称。
6. 在该终端节点服务的“权限管理”页签，单击“添加白名单记录”。
7. 根据提示配置参数，输入授权用户的账号ID，添加白名单并单击“确定”。

   说明

   - 本账号默认在自身账号的终端节点服务的白名单中。
   - 授权账号ID格式为：（iam:domain::domain_id）。
     “domain_id”表示授权用户的账号ID，例如“iam:domain::1564ec50ef2a47c791ea5536353ed4b9”。
   - 添加“*”到白名单，表示所有用户可访问。

删除白名单

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
5. 在“终端节点服务”页面，单击需要删除白名单的终端节点服务名称。
6. 在该终端节点服务的“权限管理”页签，单击对应授权账号ID“操作”列下的“删除”，即可删除对应的白名单记录。

   如果要删除多个白名单记录，可以勾选待删除的授权账号ID，单击上方的“删除”。
7. 在“删除白名单记录”弹框中，单击“是”，删除终端节点服务的白名单记录。

3.7 查看终端节点服务的端口映射

操作场景

当终端节点服务创建成功后，您可以查看已添加的端口映射。

包括协议、服务端口和终端端口等信息。

 版权所有 © 华为技术有限公司

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
5. 单击需要操作的终端节点服务名称。
6. 选择“端口映射”页签。
   可查看终端节点服务已设置的端口映射。

 版权所有 © 华为技术有限公司

4 终端节点管理

4.1 终端节点简介

终端节点用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。

在同一区域中，通过创建终端节点可以实现所属VPC内云资源跨VPC访问终端节点服务。

本章节介绍如何创建并管理终端节点，如表4-1所示。

表 4-1 终端节点管理说明

操作	说明	使用限制
创建终端节点	介绍如何创建连接终端节点服务的终端节点。	• 终端节点属于区域级资源，在创建时需要设置区域和项目。 • 每个租户支持创建50个终端节点。 • 创建时需要保证所连接的终端节点服务已经存在，且与终端节点服务位于同一区域。
查询并访问终端节点	介绍如何查看终端节点的详细信息。	一个终端节点支持最大连接数为3000。
删除终端节点	介绍如何删除终端节点。	终端节点删除后无法恢复，请谨慎操作。

4.2 创建终端节点

操作场景

终端节点用于在VPC和终端节点服务之间建立便捷、安全、私密的连接通道。

版权所有 © 华为技术有限公司

在同一区域中，通过创建终端节点可以实现所属VPC内云资源跨VPC访问终端节点服务。

终端节点与终端节点服务一一对应，访问不同类型终端节点服务的终端节点存在差异：

- 访问“接口”型终端节点服务的终端节点：是具备私有IP地址的弹性网络接口，作为接口型终端节点服务的通信入口。
- 访问“网关”型终端节点服务的终端节点：是一个网关，在其上配置路由，用于将流量指向网关型终端节点服务。

您可以根据实际需求，创建连接不同终端节点服务类型的终端节点：

- **创建连接“接口”型终端节点服务的终端节点**
- **创建连接“网关”型终端节点服务的终端节点**

约束与限制

- 终端节点属于区域级资源，在创建时需要设置区域和项目。
- 每个租户支持创建50个终端节点。
- 创建时需要保证所连接的终端节点服务已经存在，且与终端节点服务位于同一区域。

创建连接“接口”型终端节点服务的终端节点

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在“终端节点”页面，单击“创建终端节点”，进入“创建终端节点”页面。
5. 在“创建终端节点”页面，根据提示配置参数。

表 4-2 终端节点配置参数

参数	说明
区域	终端节点所在区域。不同区域的资源之间内网不互通。请选择靠近您的区域，可以降低网络时延、提高访问速度。
服务类别	可选择“云服务”或“按名称查找服务”。 ● 云服务：当您要连接的终端节点服务为云服务时，需要选择“云服务”。 ● 按名称查找服务：当您要连接的终端节点服务为用户私有服务时，需要选择“按名称查找服务”。
选择服务	若“服务类别”选择“云服务”，则会出现该参数。 终端节点服务实例已由运维人员预先创建完成，您可以直接使用。

 版权所有 © 华为技术有限公司

参数	说明
服务名称	若“服务类别”选择“按名称查找服务”，则会出现该参数。 在终端节点服务列表的“名称”列，拷贝并输入待访问终端节点服务的名称，单击“验证”： ● 若显示“已找到服务”，继续后续操作。 ● 若显示“未找到服务”，请检查“区域”是否和终端节点服务所在区域一致或输入的“服务名称”是否正确。
虚拟私有云	选择终端节点所属的虚拟私有云。
子网	当“选择服务”的“类型”为“接口”时，则会出现该参数。 选择终端节点所属的子网。

6. 参数配置完成，单击“立即创建”，进行规格确认。
   - 规格确认无误，单击“提交”，任务提交成功。
   - 参数信息配置有误，需要修改，单击“上一步”，修改参数，然后单击“提交”。

创建连接“网关”型终端节点服务的终端节点

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在“终端节点”页面，单击“创建终端节点”，进入“创建终端节点”页面。
5. 在“创建终端节点”页面，根据提示配置参数。

表 4-3 终端节点配置参数

参数	说明
区域	终端节点所在区域。不同区域的资源之间内网不互通。请选择靠近您的区域，可以降低网络时延、提高访问速度。
服务类别	仅由系统配置的云服务类别的终端节点服务包括“网关”型。 选择“云服务”。
选择服务	若“服务类别”选择“云服务”，则会出现该参数。 在列表中，选择“类型”列为“网关”类型的终端节点服务。 终端节点服务实例已由运维人员预先创建完成，您可以直接使用。
虚拟私有云	选择终端节点所属的虚拟私有云。

6. 参数配置完成，单击“立即创建”，进行规格确认。
   - 规格确认无误，单击“提交”，任务提交成功。
   - 参数信息配置有误，需要修改，单击“上一步”，修改参数，然后单击“提交”。

 版权所有 © 华为技术有限公司

4.3 查询并访问终端节点

操作场景

当终端节点创建完成时，可以查询终端节点详情并访问终端节点。

约束与限制

一个终端节点支持最大连接数为3000。

查询终端节点

支持查询终端节点的ID、服务名称、虚拟私有云、状态等详情。

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”，选择“网络 > VPC终端节点”，进入“终端节点”页面。
4. 单击要查看的终端节点ID，即可查看终端节点的基本信息。
   以接口型终端节点为例，创建成功后，会生成一个“节点IP”（即私有IP）。

表 4-4 参数说明

页签	参数名称	说明
基本信息	ID	终端节点ID。
	虚拟私有云	终端节点所属VPC。
	终端节点服务名称	终端节点所连接的终端节点服务名称。
	节点IP	终端节点的IP地址。
	内网域名	终端节点的内网域名。
	状态	终端节点状态。
	类型	终端节点所连接的终端节点服务类型。
	创建时间	终端节点的创建时间。

访问终端节点（节点 IP）

支持通过查询的终端节点的“节点IP”访问终端节点。

1. 在终端节点所属VPC内，登录该终端节点连接的后端资源，例如ECS。
2. 根据后端资源类型，选择不同的命令，通过以下格式访问终端节点：
   命令 节点IP:端口

 版权所有 © 华为技术有限公司

例如，后端资源为ECS，使用如下命令：

curl *节点IP:端口*

4.4 删除终端节点

操作场景

本节介绍如何删除终端节点。

说明

终端节点删除后无法恢复，请谨慎操作。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。
3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点”。
5. 单击待删除的终端节点所在行的“删除”按钮。
6. 在“删除终端节点”弹框中，单击“是”，删除终端节点。

版权所有 © 华为技术有限公司

5 权限管理

5.1 创建用户并授权使用 VPCEP

如果您需要对您所拥有的VPCEP进行精细的权限管理，您可以使用统一身份认证服务（Identity and Access Management，简称IAM），通过IAM，您可以：

- 根据企业的业务组织，在您的账号中，给企业中不同职能部门的员工创建IAM用户，让员工拥有唯一安全凭证，并使用VPCEP资源。
- 根据企业用户的职能，设置不同的访问权限，以达到用户之间的权限隔离。
- 将VPCEP资源委托给更专业、高效的其他账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果账号已经能满足您的要求，不需要创建独立的IAM用户，您可以跳过本章节，不影响您使用VPCEP服务的其它功能。

本章节为您介绍对用户授权的方法，操作流程如**图5-1**所示。

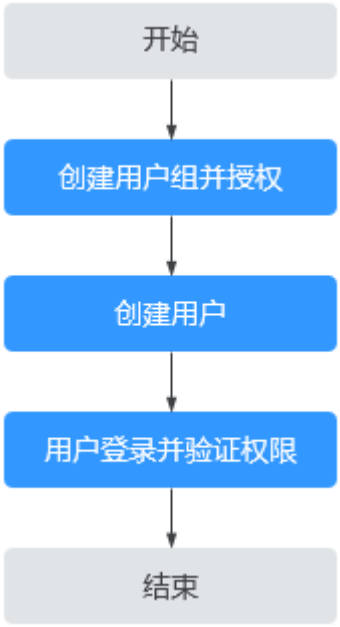
前提条件

给用户组授权之前，请您了解用户组可以添加的VPCEP权限，并结合实际需求进行选择，VPCEP支持的系统权限，请参见**权限管理**。若您需要对除VPCEP之外的其它服务授权，IAM支持服务的所有权限请参见权限集。

 版权所有 © 华为技术有限公司

示例流程

图 5-1 给用户授权 VPCEP 权限流程



1. 创建用户组并授权

   在IAM控制台创建用户组，并在“操作”列下选择“授权”，授予VPC终端节点权限“VPCEP Administrator”。
2. 创建用户并加入用户组

   在IAM控制台创建用户，并在“操作”列下选择“授权”，将其加入1中创建的用户组。
3. 用户登录并验证权限

   新创建的用户登录控制台，切换至授权区域，验证权限：
   - 在“服务列表”中选择“VPC终端节点”，进入VPCEP主界面，单击右上角“创建终端节点”，尝试创建终端节点，如果可以创建，表示“VPCEP Administrator”已生效。
   - 在“服务列表”中选择除VPC终端节点外（假设当前权限仅包含VPCEP Administrator）的任一服务，若提示权限不足，表示“VPCEP Administrator”已生效。

5.2 创建 VPCEP 自定义策略

如果系统策略不满足授权要求，您可以创建自定义策略，并通过给用户组授予自定义策略来进行精细的访问控制，自定义策略是对系统策略的扩展和补充。

目前支持以下两种方式创建自定义策略：

- 可视化视图：通过可视化视图创建自定义策略，无需了解JSON语法，按可视化视图导航栏选择云服务、操作、资源、条件等策略内容，可自动生成策略。
- JSON视图：通过JSON视图创建自定义策略，可以在选择策略模板后，根据具体需求编辑策略内容；也可以直接在编辑框内编写JSON格式的策略内容。

版权所有 © 华为技术有限公司

如下以定制一个用户仅能修改终端节点服务的策略为例。分别采用可视化视图和JSON视图的配置方式创建自定义策略 。

本章为您介绍常用的VPCEP自定义策略样例。

可视化视图配置自定义策略

1. 登录管理控制台。
2. 选择“管理与部署 > 统一身份认证服务”。

   进入“统一身份认证服务”页面。
3. 在“统一身认证服务”页面左侧导航栏中，选择“策略”。
4. 在“策略”页面，单击右上方的“创建自定义策略”。

   进入“创建自定义策略”页面。
5. 输入“策略名称”。
6. 选择“作用范围”，即自定义策略的生效范围，根据服务的部署区域选择。
   - 全局级服务：系统权限中该服务的“所属区域”为“全局区域”，表示该服务为全局级服务。创建全局级服务的自定义策略时，作用范围选择“全局级服务”。给用户组授予该自定义策略时，需要在全局区域中进行。
   - 项目级服务：系统权限中该服务的“所属区域”为“除全局区域外其他区域”，表示该服务为项目级服务。创建项目级服务的自定义策略时，作用范围选择“项目级服务”。给用户组授予该自定义策略时，需要在除全局区域外其他区域中进行。

   因VPCEP是区域级项目，此处选择“项目级服务”。

   说明

   如果一个自定义策略中包含多个服务的授权语句，这些服务必须是同一属性，即都是全局级服务或者项目级服务。如果需要同时设置全局服务和项目级服务的自定义策略，请创建两条自定义策略，“作用范围”分别为“全局级服务”以及“项目级服务”。
7. “策略配置方式”选择“可视化视图”。
8. 在“策略内容”下配置自定义策略。
   a. 选择“允许”或“拒绝”。
   b. 选择“云服务”。

      说明

      此处只能选择一个云服务，如需配置多个云服务的自定义策略，请在完成此条配置后，单击“添加权限”，创建多个服务的授权语句；或使用**JSON视图配置自定义策略**。
   c. 选择“操作”，根据需求勾选产品权限。
   d. （可选）选择资源类型，如选择“特定类型”可以点击“通过资源路径指定”来指定需要授权的资源。
   e. （可选）添加条件，单击“添加条件”，选择“条件键”，选择“运算符”，根据运算符类型填写相应的值。

 版权所有 © 华为技术有限公司

表 5-1 条件参数

名称	说明
条件值	条件键表示策略语句的Condition元素中的键值。分为全局条件键和服务级条件键。 • 全局级条件键：前缀为“g:”，适用于所有操作，如表5-2所示。 • 服务级条件键：前缀为服务缩写，如“vpcep:”，仅适用于对应服务的操作。
运算符	与条件键一起使用，构成完整的条件判断语句。
值	与条件键和运算符一起使用，当运算符需要某个关键字时，需要输入关键字的值，构成完整的条件判断语句。

表 5-2 全局级请求条件

全局条件键	条件类型	说明
g:CurrentTime	时间	接收到鉴权请求的时间。以ISO 8601格式表示，例如：2012-11-11T23:59:59Z。
g:DomainName	字符串	账号名称。
g:MFAPresent	布尔值	是否使用MFA多因素认证方式获取Token。
g:MFAAge	数值	通过MFA多因素认证方式获取的Token的生效时间。该条件需要和g:MFAPresent一起使用。
g:ProjectName	字符串	项目名称。
g:ServiceName	字符串	服务名称。
g:UserId	字符串	IAM用户ID。
g:UserName	字符串	IAM用户名。

9. （可选）在“策略配置方式”选择JSON视图，将可视化视图配置的策略内容转换为JSON语句，您可以在JSON视图中对策略内容进行修改。

 版权所有 © 华为技术有限公司

说明

如果您修改后的JSON语句有语法错误，将无法创建策略，可以自行检查修改内容或单击界面弹窗中的“重置”，将JSON文件恢复到未修改状态。

10. （可选）如需创建多条自定义策略，请单击“添加权限”；也可在已创建的策略最右端单击“+”，复制此权限。
11. （可选）输入“策略描述”。
12. 单击“确定”，完成自定义策略的创建。
13. 参考**创建用户并授权使用VPCEP**将新创建的自定义策略授予用户组，使得用户组中的用户具备自定义策略中的权限。

JSON 视图配置自定义策略

1. 登录管理控制台。
2. 选择“管理与部署 > 统一身份认证服务”。

   进入“统一身份认证服务”页面。
3. 在“统一身认证服务”页面左侧导航栏中，选择“策略”。
4. 在“策略”页面，单击右上方的“创建自定义策略”。

   进入“创建自定义策略”页面。
5. 输入“策略名称”。
6. 选择“作用范围”，即自定义策略的生效范围，根据服务的部署区域选择。
   - 全局级服务：系统权限中该服务的“所属区域”为“全局区域”，表示该服务为全局级服务。创建全局级服务的自定义策略时，作用范围选择“全局级服务”。给用户组授予该自定义策略时，需要在全局区域中进行。
   - 项目级服务：系统权限中该服务的“所属区域”为“除全局区域外其他区域”，表示该服务为项目级服务。创建项目级服务的自定义策略时，作用范围选择“项目级服务”。给用户组授予该自定义策略时，需要在除全局区域外其他区域中进行。

   因VPCEP是区域级项目，此处选择“项目级服务”。

   说明

   如果一个自定义策略中包含多个服务的授权语句，这些服务必须是同一属性，即都是全局级服务或者项目级服务。如果需要同时设置全局服务和项目级服务的自定义策略，请创建两条自定义策略，“作用范围”分别为“全局级服务”以及“项目级服务”。
7. “策略配置方式”选择“JSON视图”。
8. （可选）在“策略内容”区域，单击“从已有策略复制”，例如选择“VPCEndpoint FullAccess”作为模板。
9. 单击“确定”。
10. 修改模板中策略授权语句。
    - 作用（Effect）：允许（Allow）和拒绝（Deny）。
    - 权限集（Action）：写入各服务API授权项列表中“授权项”中的内容，例如："vpcep:epservices:update"，来实现细粒度授权。

    说明

    自定义策略版本号（Version）固定为1.1，不可修改。
11. （可选）输入“策略描述”。

 版权所有 © 华为技术有限公司

12. 单击“确定”后，系统会自动校验语法，如跳转到策略列表，则自定义策略创建成功；如提示“策略内容错误”，请按照语法规范进行修改。
13. 参考**创建用户并授权使用VPCEP**将新创建的自定义策略授予用户组，使得用户组中的用户具备自定义策略中的权限。

 版权所有 © 华为技术有限公司

6 关于配额

什么是配额?

为防止资源滥用，平台限定了各服务资源的配额，对用户的资源数量和容量做了限制。如您最多可以创建多少台弹性云服务器、多少块云硬盘。

如果当前资源配额限制无法满足使用需要，您可以申请扩大配额。

怎样查看我的配额?

1. 登录管理控制台。
2. 单击页面右上角的“My Quota”图标  。
   系统进入“服务配额”页面。
3. 您可以在“服务配额”页面，查看各项资源的总配额及使用情况。
   如果当前配额不能满足业务要求，请参考后续操作，申请扩大配额。

如何申请扩大配额?

目前系统暂不支持在线调整配额大小。如您需要调整配额，请联系运营管理员。

在联系运营管理员之前，请您准备好以下信息：

- 账号名，获取方式如下：
  登录云账户管理控制台，在右上角单击用户名，选择“我的凭证”，在“我的凭证”页面获取“账号名”。
- 配额信息，包括：服务名、配额类别、需要的配额值。

 版权所有 © 华为技术有限公司

7 常见问题

7.1 购买终端节点并关联已创建终端节点服务后，无法正常连通如何排查?

1. 确认弹性云服务器使用的网卡安全组是否正确。
   - 在弹性云服务器详情页面查看网卡使用的安全组。
   - 查看安全组入方向是否已放行198.19.128.0/17网段的地址，如果没有放行，请添加198.19.128.0/17网段的入方向规则，用户可根据自己的实际业务场景添加入方向规则。
2. 确认弹性云服务器网卡所在子网的网络ACL不会对流量进行拦截。

   在虚拟私有云页面左侧如果可以进行网络ACL配置，请确认VPC终端节点涉及的子网已放通。
3. 如果终端节点服务配置的后端资源为弹性负载均衡，且弹性负载均衡开通了访问控制策略，也需要放通198.19.128.0/17。

7.2 VPC 终端节点和对等连接有什么区别?

VPC终端节点与对等连接其他方面的区别请详细参考**表7-1**。

说明

VPC终端节点与对等连接并无直接关系，您可以根据需要进行配置。

表 7-1 VPC 终端节点与对等连接的区别

类别	VPC对等连接	VPC终端节点
安全性	VPC内所有ECS、ELB等均可以被访问。	仅创建了终端节点服务的ECS、ELB等可以被访问。

 版权所有 © 华为技术有限公司

类别	VPC对等连接	VPC终端节点
CIDR重叠	不支持。 如果两个VPC之间的子网网段有重叠或者完全相同，那么建立的对等连接将无效，无法相互通信。	支持。 VPC终端节点完全不受两个VPC子网网段重叠或者完全相同的影响，均可以正常通信。
通信方向	建立对等连接的两个VPC之间支持双向通信。	通过VPC终端节点建立连接的两个VPC之间，仅支持终端节点所在VPC访问终端节点服务所在后端资源的指定端口。
路由配置	两个VPC间创建对等连接后，需要在两端VPC内分别添加对等连接路由信息，才能使两个VPC互通。	通过VPC终端节点服务进行连接的两个VPC，服务已为用户配置好相应的路由信息，用户自己无需再配置。

7.3 终端节点服务和终端节点有哪些状态?

终端节点服务的状态以及每种状态表示的意义如表7-2所示。

表 7-2 终端节点服务的状态

状态	意义
创建中	表示终端节点服务正在创建。
可连接	表示终端节点服务创建成功，可接受终端节点的连接。
失败	表示终端节点服务创建失败。
删除中	表示正在删除终端节点服务。
已删除	表示已删除终端节点服务。

终端节点的状态以及每种状态表示的意义如表7-3所示。

表 7-3 终端节点的状态

状态	意义
待接受	表示终端节点要连接的终端节点服务开启了连接审批功能，正等待终端节点服务的审批。
创建中	表示终端节点正在与终端节点服务进行连接。
已接受	表示终端节点已成功连接至终端节点服务。
已拒绝	表示终端节点服务拒绝了终端节点的连接。

版权所有 © 华为技术有限公司

状态	意义
失败	表示终端节点与终端节点服务的连接失败。
删除中	表示正在删除终端节点。

7.4 VPC 终端节点是否支持跨区域访问?

VPC终端节点服务目前不支持跨区域访问，只支持访问同区域VPC中的云服务或用户私有服务。

版权所有 © 华为技术有限公司

A 修订记录

版本日期	变更说明
2024-04-12	第一次正式发布。

版权所有 © 华为技术有限公司