VPC 终端节点

用户指南

文档版本 01

发布日期 2025-12-02

华为云计算技术有限公司

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云计算技术有限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，华为云计算技术有限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。

华为云计算技术有限公司

地址： 贵州省贵安新区黔中大道交兴功路华为云数据中心 邮编：550029

网址： https://www.huaweicloud.com/

目 录

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

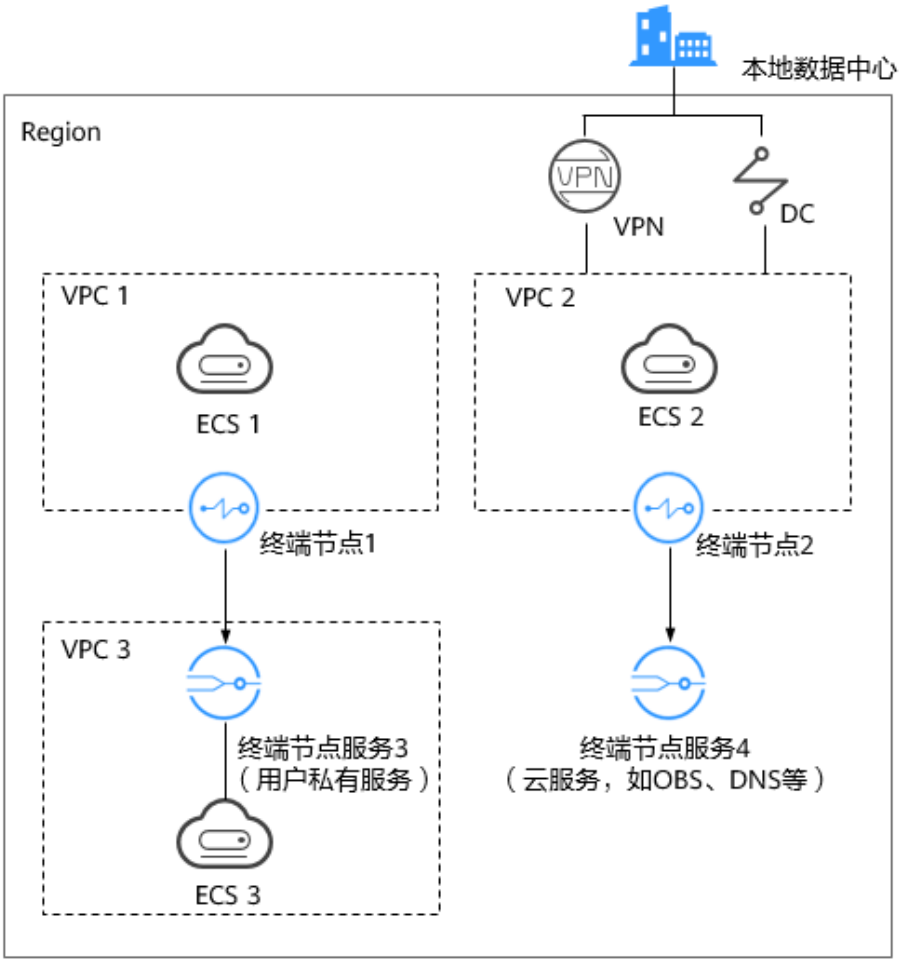
VPC终端节点由“终端节点服务”和“终端节点”两种资源实例组成。

- 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**。

图 1-1 VPC 终端节点组网示意图



如图1-1所示，建立了“终端节点”到“终端节点服务”的访问通道，实现：

- VPC 1中的云资源（ECS 1）通过内网访问VPC 3中的云资源（ECS 3）。
- VPC 2中的云资源（ECS 2）通过内网访问云服务（如OBS、DNS）。
- 本地数据中心（IDC）通过VPN或者DC的方式与VPC 2连通，实现IDC通过内网访问云服务（如OBS、DNS）。

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。
- **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

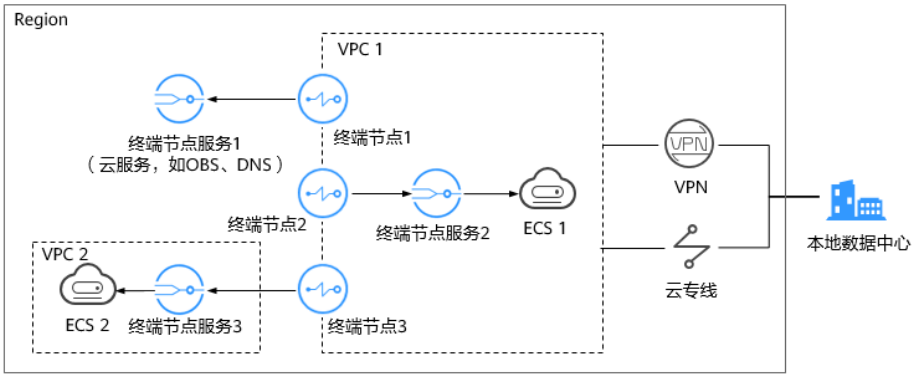
在同一区域中，VPC终端节点可以建立终端节点（VPC内云资源）到终端节点服务（用户私有服务、云服务）的便捷、安全、私密连接通道。

基于上述功能，VPC终端节点主要应用于以下场景。

高速上云

本地数据中心可以通过VPN或者云专线连通VPC，利用建立的终端节点通过内网访问终端节点服务（用户私有服务、云服务）。

图 1-2 高速上云场景示意图



如图1-2所示，本地数据中心通过VPN或者云专线与VPC 1连通，实现：

- 利用终端节点1，通过内网访问云服务（如OBS、DNS等）。
- 利用终端节点2，访问VPC 1的云资源（如ECS 1）。
- 利用终端节点3，跨VPC访问VPC 2的云资源（如ECS 2）。

这种场景具有以下优势：

- 简单快速
  本地数据中心直连终端节点服务，无需经过公网，访问时延小，效率高。
- 成本低廉
  本地数据中心访问云上资源不占用用户的公网资源，降低使用成本。

具体示例请参考**配置访问OBS服务内网地址的终端节点**。

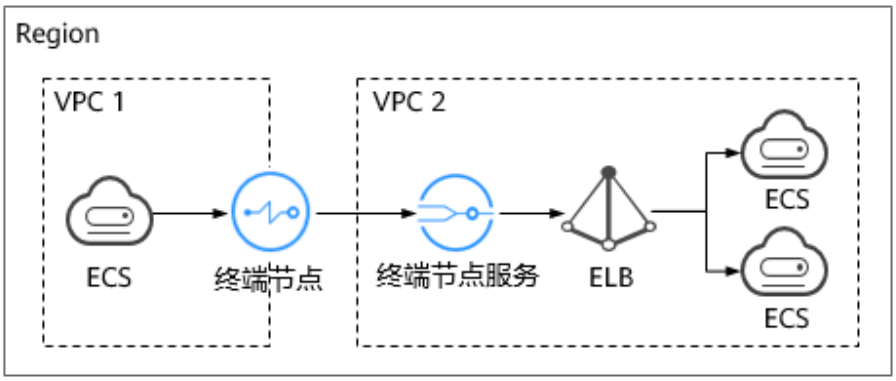
跨 VPC 连接

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终端节点和对等连接有什么区别?** 。

图 1-3 跨 VPC 连接场景示意图



如**图1-3**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：

- **配置跨VPC通信的终端节点（同一）**
- **配置跨VPC通信的终端节点（不同）**

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	**关于配额**

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的数量	50个	关于配额

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	• 配置跨VPC通信的终端节点（同一） • 配置跨VPC通信的终端节点（不同）
本地数据中心可以通过VPN，利用建立的终端节点以内网访问云服务。	虚拟专用网络	配置访问OBS服务内网地址的终端节点
本地数据中心可以通过云专线，利用建立的终端节点以内网访问云服务。	云专线	配置访问OBS服务内网地址的终端节点
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，以及控制这些用户对企业名下资源具有的操作权限。	统一身份认证服务	-
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	创建终端节点
由系统配置为“接口”型终端节点服务，可以创建终端节点访问该终端节点服务。	云解析服务	创建终端节点

交互功能	相关服务	相关内容
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	创建终端节点服务
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。	云服务器	创建终端节点服务
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。	裸金属服务器	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，可以帮助您安全地控制云服务的访问。

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**IAM产品简介**。

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。

如**表1-3**所示，包括了VPCEP的所有系统角色。

表 1-3 VPCEP 系统角色

系统角色	描述	类别	依赖关系
VPCEndpoint 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**和**DNS Administrator**。

表1-4列出了VPCEP服务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	VPCEndpoint Administrator
创建终端节点	√
删除终端节点	√
查询终端节点	√
修改终端节点	√
创建终端节点服务	√
删除终端节点服务	√
查询终端节点服务	√
修改终端节点服务	√

相关链接

- IAM产品简介
- 创建用户组、用户并授予VPCEP权限请参考：创建用户并授权使用VPCEP

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。

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。
裸金属服务器	用户私有服务	接口	无	BMS：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。

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

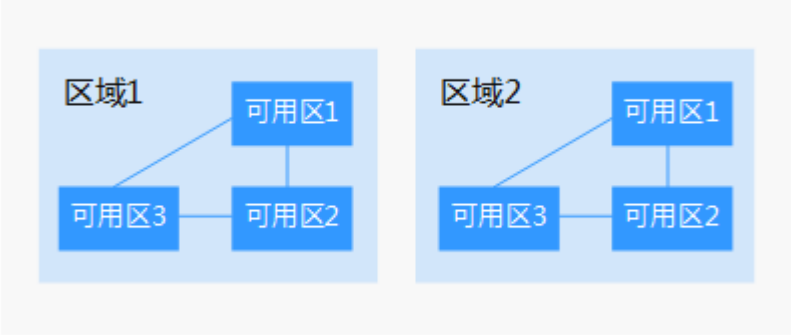
什么是区域、可用区?

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1-4阐明了区域和可用区之间的关系。

图 1-4 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。

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**。

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）** • **配置跨VPC通信的终端节点（不同）**
线下节点访问云上资源	VPC终端节点支持线下节点（即本地数据中心）访问云上资源。包括： **配置访问OBS服务内网地址的终端节点**

2.2 配置跨 VPC 通信的终端节点（同一）

2.2.1 简介

操作场景

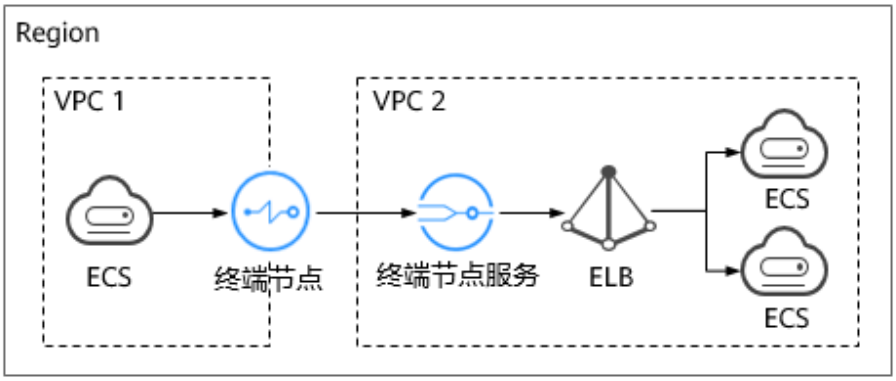
VPC终端节点支持同一区域云资源的跨VPC通信。

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。

本章节主要介绍同区域“同”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



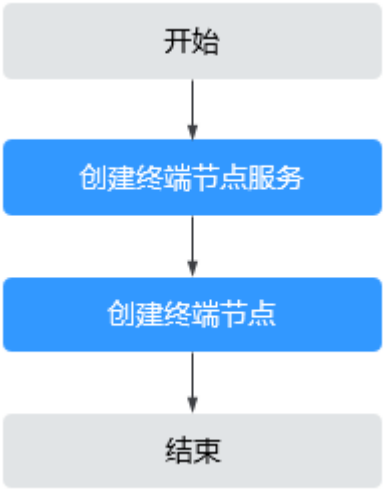
说明

- 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，请参考**配置跨VPC通信的终端节点（不同）**。

操作流程

配置同一下的跨VPC通信，具体操作流程如图2-2所示。

图 2-2 操作流程



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**。

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。 ● 裸金属服务器：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。
标签	可选参数。 终端节点服务的标识，包括键和值。可以为终端节点服务创建10个标签。 标签的命名规则请参考**表2-3**。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点服务添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点服务创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点服务描述内容。

表 2-3 终端节点服务标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

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。

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 2-4 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。

参数	说明
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。
创建内网域名	如果您想要以域名的方式访问终端节点，则选择“创建内网域名”，终端节点创建完成后，即可通过内网域名直接访问终端节点。 关联终端节点服务类型为“接口”时需要在页面设置此选项。
虚拟私有云	选择终端节点所属的虚拟私有云。
子网	当创建连接“接口”类型终端节点服务的终端节点时，则会出现该参数。 选择终端节点所属的子网。
标签	可选参数。 终端节点的标识，包括键和值。可以为终端节点创建10个标签。 标签的命名规则请参考**表2-5**。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点描述内容。

表 2-5 终端节点标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

6. 参数配置完成，单击“立即申请”，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”列，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”列，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前面的“ ”，即可查看终端节点的详细信息。

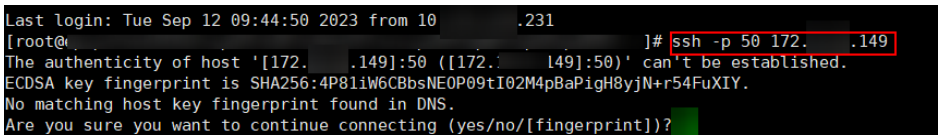
   终端节点创建成功后，会生成一个“节点IP”（就是私有IP）和“内网域名”（如果在创建终端节点时您勾选了“创建内网域名”）。

   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）

2.3.1 简介

操作场景

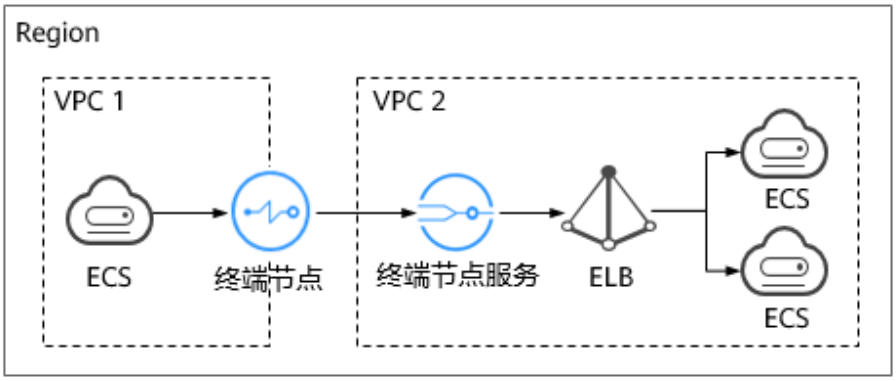
VPC终端节点支持同一区域云资源的跨VPC通信。

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”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A和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



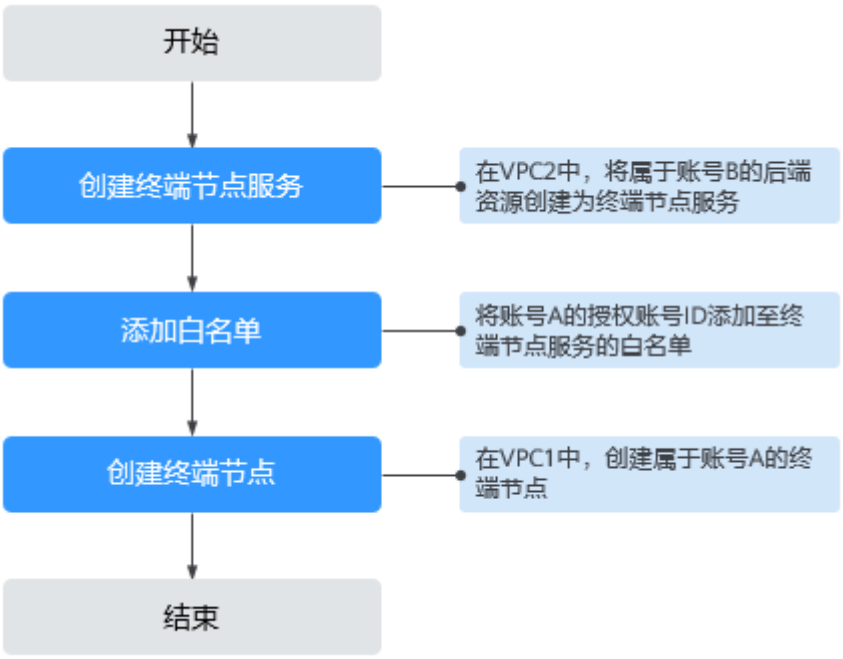
说明

- 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，请参考**配置跨VPC通信的终端节点（同一）**。

操作流程

配置不同下的跨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。
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 2-6 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。 ● 裸金属服务器：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。

参数	说明
标签	可选参数。 终端节点服务的标识，包括键和值。可以为终端节点服务创建10个标签。 标签的命名规则请参考表2-7。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点服务添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点服务创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点服务描述内容。

表 2-7 终端节点服务标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

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ID，支持添加或者移除白名单中的授权ID。

本操作指导您获取ID，并添加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ID。

获取被授权的 ID

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

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ID，添加白名单并单击“确定”。

说明

- 本默认在自身的终端节点服务的白名单中。
- 授权ID格式为：（iam:domain::domain_id）。
  “domain_id”表示授权用户的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 2-8 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。
创建内网域名	如果您想要以域名的方式访问终端节点，则选择“创建内网域名”，终端节点创建完成后，即可通过内网域名直接访问终端节点。 关联终端节点服务类型为“接口”时需要在页面设置此选项。
虚拟私有云	选择终端节点所属的虚拟私有云。
子网	当创建连接“接口”类型终端节点服务的终端节点时，则会出现该参数。 选择终端节点所属的子网。
标签	可选参数。 终端节点的标识，包括键和值。可以为终端节点创建10个标签。 标签的命名规则请参考**表2-9**。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点描述内容。

表 2-9 终端节点标签命名规则

参数	规则
键	● 不能为空。 ● 对于同一资源键值唯一。 ● 长度不超过128个字符。 ● 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	● 可以为空。 ● 长度不超过255个字符。 ● 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

6. 参数配置完成，单击“立即申请”，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”列，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”列，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前面的“ ”，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）和“内网域名”（如果在创建终端节点时您勾选了“创建内网域名”）。

   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。

2.4 配置访问 OBS 服务内网地址的终端节点

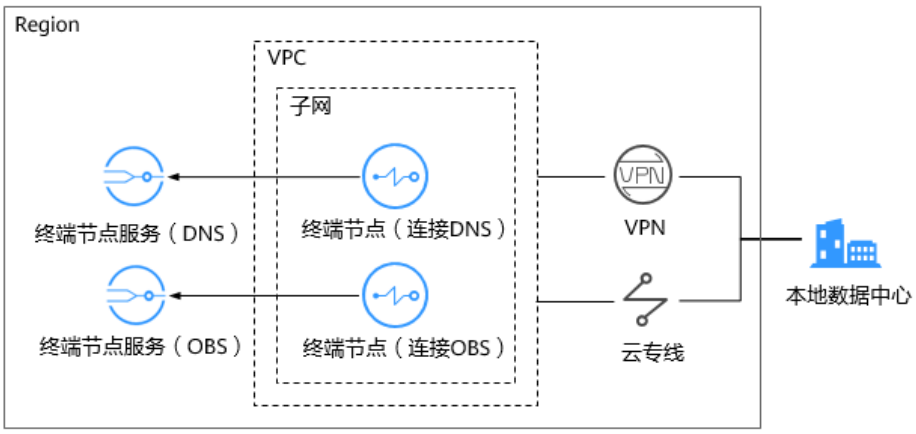
2.4.1 简介

操作场景

如果您希望本地数据中心通过VPN或者云专线以内网方式访问OBS服务，则可以通过终端节点连接终端节点服务实现。

本节介绍线下节点（即本地数据中心）通过内网方式访问云上OBS服务的配置指导。

图 2-6 本地数据中心访问 OBS（内网）



如图2-6所示，线下节点（即本地数据中心）通过VPN或者云专线与VPC连通。在VPC内创建终端节点，与云上的OBS和DNS类型的终端节点服务连接，实现线下节点（即本地数据中心）通过内网访问云上服务。

终端节点不能脱离终端节点服务单独存在，创建终端节点的前提是要连接的终端节点服务已存在。

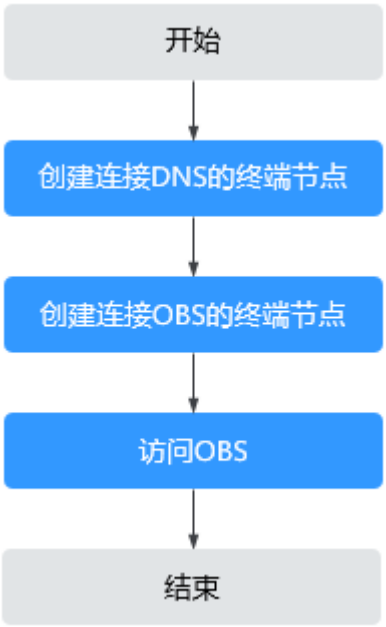
本操作场景涉及两个系统创建的终端节点服务：

- 终端节点服务（DNS）：提供域名解析服务，用于线下本地数据中心解析OBS域名。
- 终端节点服务（OBS）：提供OBS服务，供线下本地数据中心访问。

操作流程

配置本地数据中心通过内网访问OBS，具体操作流程如图2-7所示。

图 2-7 操作流程



2.4.2 步骤一：创建连接 DNS 的终端节点

操作场景

为了将解析OBS域名的请求转发到终端节点，您需要创建连接DNS服务的终端节点。

前提条件

终端节点要连接的终端节点服务已经存在。

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 2-10 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。

参数	说明
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“云服务”。
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。 此处选择DNS服务实例。
创建内网域名	如果您想要以域名的方式访问终端节点，则选择“创建内网域名”，终端节点创建完成后，即可通过内网域名直接访问终端节点。 关联终端节点服务类型为“接口”时需要在页面设置此选项。
虚拟私有云	选择终端节点所属的虚拟私有云。
子网	当创建连接“接口”类型终端节点服务的终端节点时，则会出现该参数。 选择终端节点所属的子网。
标签	可选参数。 终端节点的标识，包括键和值。可以为终端节点创建10个标签。 标签的命名规则请参考**表2-11**。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点描述内容。

表 2-11 终端节点标签命名规则

参数	规则
键	● 不能为空。 ● 对于同一资源键值唯一。 ● 长度不超过128个字符。 ● 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

参数	规则
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

6. 参数配置完成，单击“立即申请”，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. 提交成功后，返回终端节点列表。

   当新创建的终端节点状态为“已接受”时，表示连接dns终端节点服务的终端节点创建成功。
8. 单击终端节点ID前面的“ ”，即可查看终端节点的详细信息。

   接口终端节点创建成功后，会生成一个“节点IP”（就是私有IP）和“内网域名”（如果在创建终端节点时您勾选了“内网域名”）。

2.4.3 步骤二：创建连接 OBS 的终端节点

操作场景

为了实现用户本地数据中心节点通过终端节点访问OBS服务，需要创建连接OBS服务的终端节点。

前提条件

终端节点要连接的终端节点服务已经存在。

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 2-12 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”。 此处选择“云服务”。
选择服务	若“服务类别”选择“云服务”，则会出现该参数。 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。 此处选择OBS服务实例。
虚拟私有云	选择终端节点所属的虚拟私有云。
标签	可选参数。 终端节点的标识，包括键和值。可以为终端节点创建10个标签。 标签的命名规则请参考**表2-13**。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点描述内容。

表 2-13 终端节点标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

参数	规则
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

6. 参数配置完成，单击“立即申请”，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. 任务提交成功，返回终端节点列表。

   当新创建的终端节点状态由“创建中”变为“已接受”时，表示连接obs终端节点服务的终端节点创建成功。
8. 单击终端节点ID前面的“ ”，即可查看终端节点的详细信息。

2.4.4 步骤三：访问 OBS 服务

操作场景

本节介绍如何通过虚拟专用网络或者云专线方式访问OBS服务。

前提条件

您的本地数据中心已通过虚拟专用网络或者云专线与VPC连通。

- 虚拟专用网络VPN网关允许访问的VPC子网网段，需要包含OBS的网段，详细请联系对象存储服务的客户经理获取。

  创建虚拟专用网络，请参考《虚拟专用网络用户指南》。
- 专线虚拟网关允许访问的VPC子网网段，需要包含OBS的网段，详细请联系对象存储服务的客户经理获取。

  开通云专线，请参考《云专线用户指南》。

操作步骤

1. 在“终端节点”列表，单击创建的连接DNS服务的终端节点ID前面的“ ”，查看该终端节点的“节点IP”。
2. 在用户本地数据中心的DNS服务器配置相应的DNS转发规则，将解析OBS域名的请求转发到连接DNS服务的终端节点。

   不同操作系统中配置DNS转发规则的方法不同，具体操作请参考对应DNS软件的操作指导。

   本步骤以Unix操作系统，常见的DNS软件Bind为例介绍：

   在/etc/named.conf文件中增加DNS转发器的配置，“forwarders”为连接DNS服务的终端节点的IP地址。

   ```
   options {
   forward only;
   ```



```
forwarders{ xx.xx.xx.xx;};
};
```

说明

- 用户本地数据中心若无DNS服务器，需要将连接DNS服务的终端节点的节点IP增加到用户本地数据中心节点的/etc/resolv.conf文件中。
- xx.xx.xx.xx为**查看终端节点详情**中连接DNS服务的终端节点IP。

3. 配置用户本地数据中心节点到VPN网关或者专线网关的DNS路由。

   为了通过VPN或者云专线访问DNS，需要将用户本地数据中心节点访问DNS的流量指向用户本地数据中心节点的专线网关或者VPN网关。

   在用户本地数据中心节点配置永久路由，指定访问DNS的流量下一跳为用户本地数据中心节点专线网关或者VPN网关的IP地址。

   ```
   route -p add xx.xx.xx.xx mask 255.255.255.255 xxx.xxx.xxx.xxx
   ```

   说明

   - xx.xx.xx.xx为**查看终端节点详情**中连接DNS服务的终端节点IP。
   - xxx.xxx.xxx.xxx为用户本地数据中心节点专线网关或者VPN网关的IP地址。
   - 不同操作系统的Route命令格式存在差异，请以用户实际操作系统对应的Route命令格式为准。

4. 配置用户本地数据中心节点到VPN网关或者专线网关的OBS路由。

   连接OBS服务的终端节点的IP地址网段为100.125.0.0/16，为了通过VPN或者云专线访问OBS，需要将用户本地数据中心节点访问OBS服务的流量指向用户本地数据中心节点的专线网关或者VPN网关。

   在用户本地数据中心节点配置永久路由，指定访问OBS的流量下一跳为用户本地数据中心节点专线网关或者VPN网关的IP地址。

   ```
   route -p add 100.125.0.0 mask 255.255.0.0 xxx.xxx.xxx.xxx
   ```

   说明

   - xxx.xxx.xxx.xxx为用户本地数据中心节点专线网关或者VPN网关的IP地址。
   - 不同操作系统的Route命令格式存在差异，请以用户实际操作系统对应的Route命令格式为准。

5. 在本地数据中心，通过以下命令验证本地数据中心与OBS的连通性。

   ```
   telnet bucketname.endpoint
   ```

   其中：

   - bucketname：表示OBS的桶名称。
   - endpoint：表示桶所在区域的终端节点（区域域名）。

   例如，**telnet bucketname.obs.my-kualalumpur-1.alphaedge.tmone.com.my**

   说明

   您可以从**地区和终端节点**中查询不同区域OBS的Endpoint信息。

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。

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。 – 裸金属服务器：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。
管理终端节点服务的标签	介绍如何管理终端节点服务的标签，包括查看、添加、编辑和删除标签。	支持为终端节点服务创建10个标签。

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。
  - 裸金属服务器：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。

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。 ● 裸金属服务器：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。
选择裸金属服务器	“后端资源类型”选择为“裸金属服务器”时，会出现该参数，在列表中选择需要提供服务的裸金属服务器。 **说明** 裸金属服务器类型即将废弃，请优先使用弹性负载均衡类型。

参数	说明
标签	可选参数。 终端节点服务的标识，包括键和值。可以为终端节点服务创建10个标签。 标签的命名规则请参考表3-3。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点服务添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点服务创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点服务描述内容。

表 3-3 终端节点服务标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

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。

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。

   在终端节点服务列表右上角的过滤和搜索框可以快速定位终端节点服务：
   - 通过终端节点服务的“名称”或者“ID”进行搜索：
     i. 在过滤框中选择“名称”或者“ID”。
     ii. 在搜索框中输入关键字。
     iii. 单击“ ”开始搜索。

     搜索完成后，终端节点服务列表中显示包含关键字的终端节点服务。
   - 通过终端节点服务预先设置的标签进行搜索：
     i. 在“标签搜索”中单击“ ”展开标签搜索区域。
     ii. 输入标签“键”和“值”。

     直接输入或者在下拉框中选择标签的“键”和“值”。

     最多支持设置10组标签用于搜索终端节点服务。
     iii. 单击“搜索”开始搜索。

     搜索完成后，终端节点服务列表中显示设置了指定标签的终端节点服务。

     若设置多组标签，则显示设置了所有指定标签的终端节点服务。
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3-4所示。

表 3-4 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。
基本信息	ID	终端节点服务ID。
基本信息	后端资源类型	提供服务的后端资源类型。
基本信息	后端资源名称	提供服务的后端资源名称。
基本信息	虚拟私有云	终端节点服务所属VPC。
基本信息	状态	终端节点服务状态。
基本信息	连接审批	终端节点服务是否开启连接审批。
基本信息	服务类型	终端节点服务类型。
基本信息	创建时间	终端节点服务创建时间。

页签	参数名称	说明
连接管理	终端节点ID	终端节点的ID。
连接管理	报文标识	终端节点ID的标识，用来识别是哪个终端节点。
连接管理	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？**。
连接管理	拥有者	终端节点创建者的ID。
连接管理	创建时间	终端节点的创建时间。
连接管理	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”。
权限管理	授权ID	连接访问终端节点的授权ID或者*。 若“授权ID”列为“*”，表示所有用户均可访问该终端节点服务。
权限管理	操作	对连接访问终端节点的授权进行操作，支持将授权从白名单中删除。
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。
端口映射	服务端口	终端节点服务提供服务的端口。
端口映射	终端端口	终端节点访问终端节点服务的端口。
标签	键	终端节点服务的标签“键”。
标签	值	终端节点服务的标签“值”。
标签	操作	对终端节点服务标签进行操作，可选择“编辑”或“删除”标签。

3.4 删除终端节点服务

操作场景

用户不再使用已创建的终端节点服务时，可选择将其删除，终端节点服务删除后无法恢复，请谨慎操作。

本节介绍如何删除终端节点服务。

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. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
5. 单击待删除的终端节点服务所在行“操作”列的“删除”按钮。
6. 在“删除终端节点服务”弹框中，单击“是”，删除终端节点服务。

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ID，支持添加或者移除白名单中的授权ID。

- 如果白名单为空，则不支持跨的终端节点连接终端节点服务。
- 如果某一包含在终端节点服务的白名单中，则可以通过该创建连接终端节点服务的终端节点。
- 如果某一未包含在终端节点服务的白名单中，则无法通过该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。

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ID，添加白名单并单击“确定”。

   说明

   - 本默认在自身的终端节点服务的白名单中。
   - 授权ID格式为：（iam:domain::domain_id）。
     “domain_id”表示授权用户的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。

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。

3.8 管理终端节点服务的标签

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标签，还可以添加、编辑以及删除标签。

标签是终端节点服务的标识，包括键和值。可以为终端节点服务创建10个标签。

说明

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。

如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点服务添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点服务创建失败，请联系组织管理员了解标签策略详情。

添加标签

本操作用于为已创建的终端节点服务添加标签。

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的名称，进入终端节点服务“基本信息”页面。
6. 选择“标签”页签，显示终端节点服务的标签列表。
7. 单击“添加标签”。
8. 在“添加标签”对话框中，输入“标签键”和“标签值”。

   如果您的组织已经设定VPC终端节点服务的相关标签策略，则需按照标签策略规则为终端节点服务添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点服务创建失败，请联系组织管理员了解标签策略详情。

   参数取值如**表3-5**所示。

   表 3-5 终端节点服务标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

9. 单击“确定”，完成终端节点服务标签的添加。

编辑标签

本操作用于修改终端节点服务已添加标签的“值”。

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的名称，进入终端节点服务“基本信息”页面。
6. 选择“标签”页签，显示终端节点服务的标签列表。
7. 在待编辑标签所在行的“操作”列，单击“编辑”。
8. 根据需要修改标签的“值”。

   说明

   仅支持编辑已添加标签的“值”。

9. 单击“确定”，完成标签的编辑。

删除标签

本操作用于删除终端节点服务已添加的标签。

⚠ 注意

删除标签后无法恢复，请谨慎操作。

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的名称，进入终端节点服务“基本信息”页面。
6. 选择“标签”页签，显示终端节点服务的标签列表。
7. 在待删除标签所在行的“操作”列，单击“删除”。
8. 单击“确定”，完成标签的删除 。

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并发连接数为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。
管理终端节点的标签	介绍如何管理终端节点的标签，包括查看、添加、编辑和删除标签。	支持为终端节点创建10个标签。

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。

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”。

参数	说明
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。
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。
创建内网域名	如果您想要以域名的方式访问终端节点，则选择“创建内网域名”，终端节点创建完成后，即可通过内网域名直接访问终端节点。 关联终端节点服务类型为“接口”时需要在页面设置此选项。
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。
标签	可选参数。 终端节点的标识，包括键和值。可以为终端节点创建10个标签。 标签的命名规则请参考表4-3。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点服务描述内容。

表 4-3 终端节点标签命名规则

参数	规则
键	● 不能为空。 ● 对于同一资源键值唯一。 ● 长度不超过128个字符。 ● 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

参数	规则
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

6. 参数配置完成，单击“立即申请”，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 4-4 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。 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。
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。

参数	说明
虚拟私有云	选择终端节点所属的虚拟私有云。
标签	可选参数。 终端节点的标识，包括键和值。可以为终端节点创建10个标签。 标签的命名规则请参考表4-5。 **说明** 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。 如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。
描述	终端节点服务描述内容。

表 4-5 终端节点标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

6. 参数配置完成，单击“立即申请”，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”。

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并发连接数为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。
   在终端节点列表右上角的过滤和搜索框可以快速定位终端节点：
   - 通过终端节点连接的终端节点服务名称或者终端节点ID进行搜索：
     i. 在过滤框中选择“终端节点服务名称”或者“ID”。
     ii. 在搜索框中输入关键字。
     iii. 单击“ ”开始搜索。
     搜索完成后，终端节点列表中显示包含关键字的终端节点。
   - 通过VPC终端节点预先设置的标签进行搜索：
     i. 在“标签搜索”中单击“ ”展开标签搜索区域。
     ii. 输入标签“键”和“值”。
     直接输入或者在下拉框中选择标签的“键”和“值”。
     最多支持设置10组标签用于搜索终端节点。
     iii. 单击“搜索”开始搜索。
     搜索完成后，终端节点列表中显示设置了指定标签的终端节点。
     若设置多组标签，则显示设置了所有指定标签的终端节点。
4. 单击要查看的终端节点ID前面的“ ”，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 4-6 参数说明

参数名称	说明
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。

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

例如，后端资源为ECS，使用如下命令：

curl *节点IP:端口*

访问终端节点（内网域名）

当创建终端节点时勾选了“创建内网域名”时，支持通过查询终端节点的“内网域名”访问终端节点。

系统会自动将生成的“内网域名”添加至云解析服务中，并为该域名添加A类型记录集，实现内网域名到节点IP的解析。

您可以在云解析服务控制台查看内网域名及其解析记录。

查看“内网域名”解析记录

1. 登录管理控制台。
2. 在服务列表中，选择“网络 > 云解析服务”。
   进入“云解析”页面。
3. 在左侧树状导航栏，选择“内网域名”。
   进入“内网域名”页面。
4. 在“内网域名”页面的域名列表中，单击终端节点的“内网域名”的名称。
   进入“解析记录”页面。
5. 在解析记录列表中，可以查看到终端节点“内网域名”到“节点IP”的A类型记录集。
   当“状态”列显示为“正常”时，表示解析生效。

通过“内网域名”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 内网域名:端口
   例如，后端资源为ECS，使用如下命令：
   curl *内网域名: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。

4.5 管理终端节点的标签

操作场景

当终端节点创建成功后，您可以查看已添加的标签，还可以添加、编辑以及删除标签。

标签是终端节点的标识，包括键和值。可以为终端节点创建10个标签。

说明

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。

如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。

添加标签

本操作用于为已创建的终端节点添加标签。

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. 在终端节点列表中，单击终端节点前面的“ ”，进入终端节点“基本信息”页签。
5. 选择“标签”页签，显示终端节点的标签列表。
6. 单击“添加标签”。
7. 在“添加标签”对话框中，输入“标签键”和“标签值”。

   如果您的组织已经设定VPC终端节点的相关标签策略，则需按照标签策略规则为终端节点添加标签。标签如果不符合标签策略的规则，则可能会导致终端节点创建失败，请联系组织管理员了解标签策略详情。

   参数取值如表4-7所示。

表 4-7 终端节点标签命名规则

参数	规则
键	• 不能为空。 • 对于同一资源键值唯一。 • 长度不超过128个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。
值	• 可以为空。 • 长度不超过255个字符。 • 取值为不包含“=”、“*”、“<”、“>”、“\”、“,”、“|”、“/”的所有Unicode字符，且首尾字符不能为空格。

8. 单击“确定”，完成终端节点标签的添加。

编辑标签

本操作用于修改终端节点已添加标签的“值”。

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. 在终端节点列表中，单击终端节点前面的“ ”，进入终端节点“基本信息”页签。
5. 选择“标签”页签，显示终端节点的标签列表。
6. 在待编辑标签所在行的“操作”列，单击“编辑”。
7. 根据需要修改标签的“值”。

   说明

   仅支持编辑已添加标签的“值”。
8. 单击“确定”，完成标签的编辑。

删除标签

本操作用于删除终端节点已添加的标签，标签删除后无法恢复，请谨慎操作。

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. 在终端节点列表中，单击终端节点前面的“ ”，进入终端节点“基本信息”页签。
5. 选择“标签”页签，显示终端节点的标签列表。
6. 在待删除标签所在行的“操作”列，单击“删除”。
7. 单击“确定”，完成标签的删除。

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。

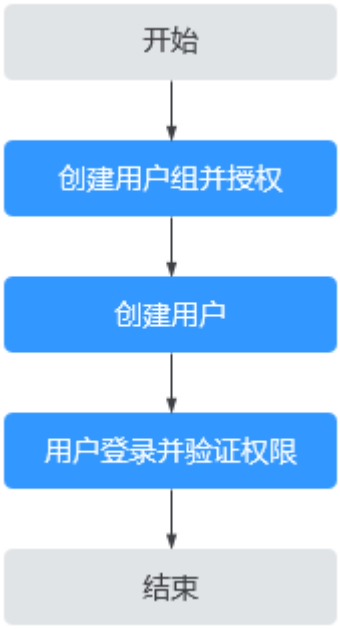
本章节为您介绍对用户授权的方法，操作流程如**图5-1**所示。

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**。

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，并授予VPC终端节点权限“VPCEndpoint Administrator”。

2. **创建用户并加入用户组**

   在IAM控制台创建用户，并将其加入**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“VPCEndpoint 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VPCEndpoint Administrator）的任一服务，若提示权限不足，表示“VPCEndpoint Administrator”已生效。

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. 单击管理控制台左上角的 ，选择区域和项目。
3. 单击页面右上角的“My Quota”图标 。
   系统进入“服务配额”页面。
4. 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?

1. 登录管理控制台。
2. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。
3. 在页面右上角，单击“申请扩大配额”。
4. 在“新建工单”页面，根据您的需求，填写相关参数。
   其中，“问题描述”项请填写需要调整的内容和申请原因。
5. 填写完毕后，勾选协议并单击“提交”。

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。

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。
VPN/DC访问	支持。 本地数据中心可以通过VPN或者云专线，利用建立的对等连接访问云服务。	支持。 本地数据中心可以通过VPN或者云专线，利用建立的终端节点通过内网访问云服务。

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。
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。

A 修订记录

版本日期	变更说明
2024-06-12	第三次正式发布。 变更说明： • **步骤一：创建终端节点服务**、**步骤二：创建终端节点**、**步骤一：创建终端节点服务**、**步骤三：创建终端节点**、**步骤一：创建连接DNS的终端节点**、**步骤二：创建连接OBS的终端节点**、**创建终端节点服务**、**创建终端节点**，更新“标签”参数说明，增加参数“描述”。 • **管理终端节点服务的标签**，更新操作场景。 • **管理终端节点的标签**，更新操作场景。
2022-11-30	第二次正式发布。 变更说明： • 新增**约束与限制** • 新增**与其他服务的关系** • 新增**终端节点服务和终端节点有哪些状态?**
2022-04-12	第一次正式发布。