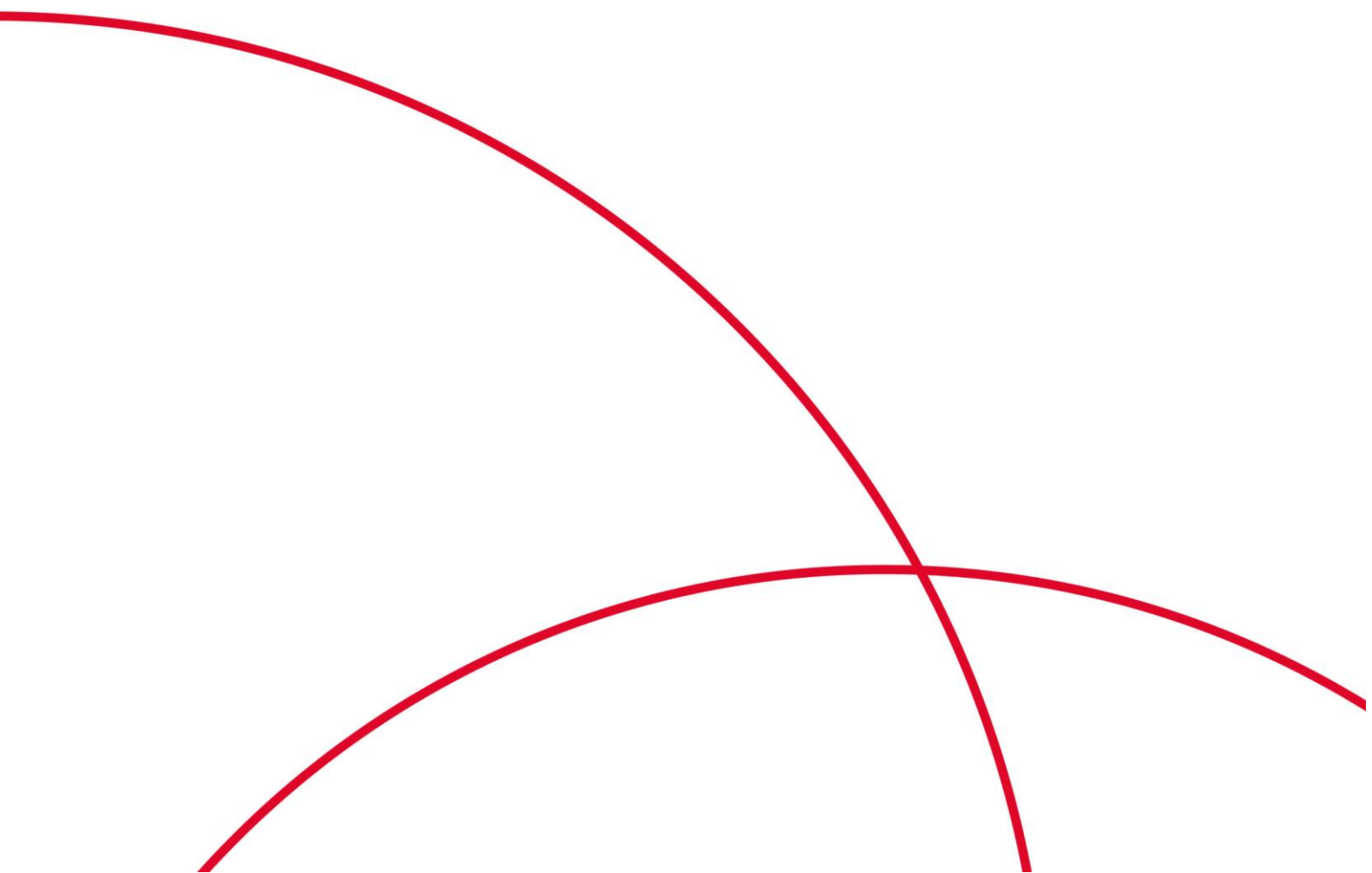




天翼云科技有限公司
VPC 终端节点
用户手册



目 录

1 产品介绍	4
1.1 什么是 VPC 终端节点?	4
1.2 产品优势	6
1.3 应用场景	6
1.4 约束与限制	8
1.5 与其他服务的关系	8
1.6 基本概念	9
1.6.1 终端节点服务	9
1.6.2 终端节点	10
1.6.3 用户权限	11
1.6.4 区域和可用区	11
2 快速入门	13
2.1 入门指引	13
2.2 配置跨 VPC 通信的终端节点（同一帐号）	14
2.2.1 简介	14
2.2.2 步骤一：创建终端节点服务.....	15
2.2.3 步骤二：创建终端节点	17
2.3 配置跨 VPC 通信的终端节点（不同帐号）	20
2.3.1 简介	20
2.3.2 步骤一：创建终端节点服务.....	22
2.3.3 步骤二：添加白名单	24
2.3.4 步骤三：创建终端节点	26
2.4 配置访问 OBS 服务内网地址的终端节点.....	29
2.4.1 简介	29
2.4.2 步骤一：创建连接 DNS 的终端节点.....	30
2.4.3 步骤二：创建连接 OBS 的终端节点.....	32
2.4.4 步骤三：访问 OBS 服务.....	34
3 终端节点服务管理	36
3.1 终端节点服务简介	36
3.2 创建终端节点服务	37

3.3 查看终端节点服务	40
3.4 删除终端节点服务	42
3.5 管理终端节点服务的连接审批.....	42
3.6 管理终端节点服务的白名单	43
3.7 查看终端节点服务的端口映射.....	45
4 终端节点管理.....	46
4.1 终端节点简介	46
4.2 创建终端节点	46
4.3 查询并访问终端节点	50
4.4 删除终端节点	52
5 常见问题.....	53
5.1 什么是配额?	53
5.2 如何检查终端节点服务所在后端弹性云服务器的网络配置?	53
5.3 VPC 终端节点和对等连接有什么区别?	54
5.4 终端节点服务和终端节点有哪些状态?	55
A 修订记录	56

1 产品介绍

1.1 什么是 VPC 终端节点？

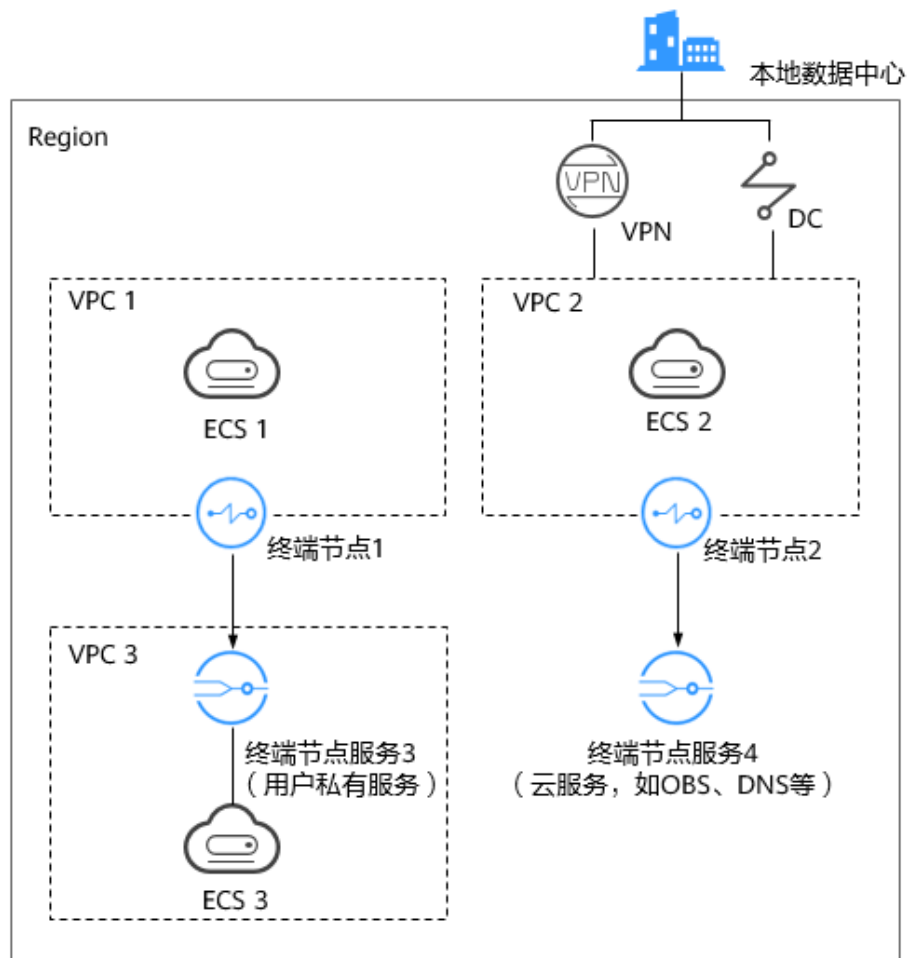
VPC 终端节点 (VPC Endpoint)，能够将 VPC 私密地连接到终端节点服务 (云服务、用户私有服务)，使 VPC 中的云资源无需弹性 IP 就能够访问终端节点服务，提高了访问效率，为您提供更加灵活、安全的组网方式。

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 1.6.1 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 1.6.2 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 1.3 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（Application programming interface）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。
- **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 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

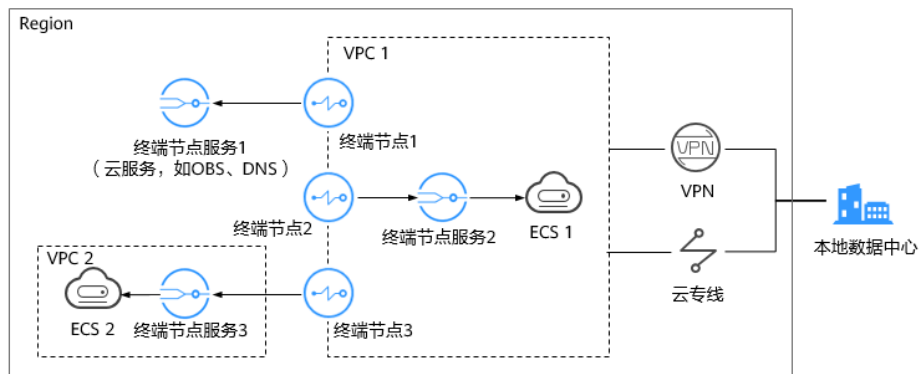
在同一区域中，VPC 终端节点可以建立终端节点（VPC 内云资源）到终端节点服务（用户私有服务、云服务）的便捷、安全、私密连接通道。

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 2.4 配置访问 OBS 服务内网地址的终端节点。

跨 VPC 连接

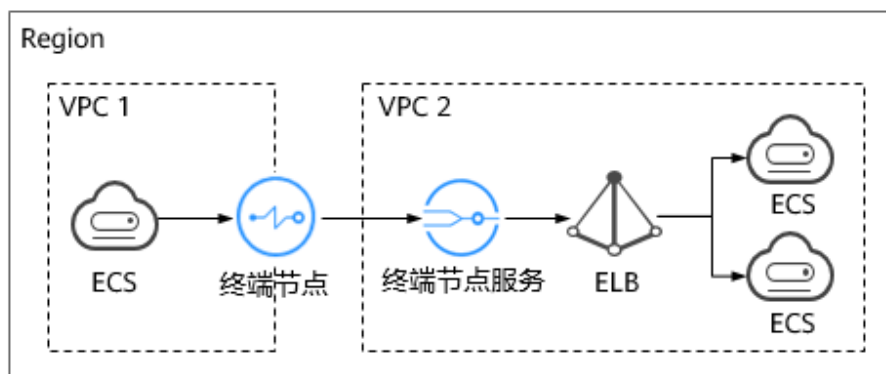
在同一区域中，由于 VPC 之间逻辑隔离，不同 VPC 内的云资源不能直接通信。利用在不同 VPC 间建立的终端节点到终端节点服务的连接通道，可以实现跨 VPC 的资源通信。

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 5.3 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：

- 2.2 配置跨 VPC 通信的终端节点（同一帐号）
- 2.3 配置跨 VPC 通信的终端节点（不同帐号）

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	限制（个）	如何提升配额
一个用户创建终端节点服务的数量	20	5.1 什么是配额？
一个用户创建终端节点的数量	50	

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	<ul style="list-style-type: none">• 2.2 配置跨 VPC 通信的终端节点（同一帐号）• 2.3 配置跨 VPC 通信的终端节点（不同帐号）
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	2.4 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	
当企业存在多用户访问 VPC 终端节点服务时，可	统一身份认证服务	-

交互功能	相关服务	相关内容
以使用 IAM 新建用户，以及控制这些用户帐号对企业名下资源具有的操作权限。		
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	4.2 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	4.2 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	3.2 创建终端节点服务
	云服务器	

1.6 基本概念

1.6.1 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 1-3 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1-3 “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	cn.ctyun.cn-gzt.obs	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1-4 “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	cn.ctyun.cn-gzt.dns	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。

1.6.2 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。

1.6.3 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。

1.6.4 区域和可用区

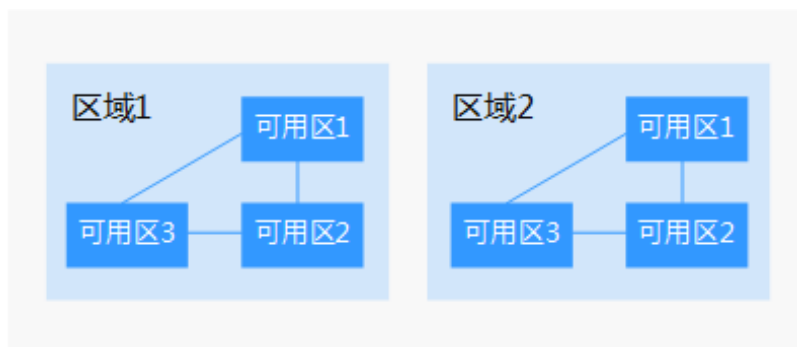
什么是区域、可用区？

我们用区域和可用区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。请向企业管理员获取区域和终端节点信息。

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 1.1 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： <ul style="list-style-type: none">• 2.2 配置跨 VPC 通信的终端节点（同一帐号）• 2.3 配置跨 VPC 通信的终端节点（不同帐号）
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： <ul style="list-style-type: none">2.4 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（同一帐号）

2.2.1 简介

操作场景

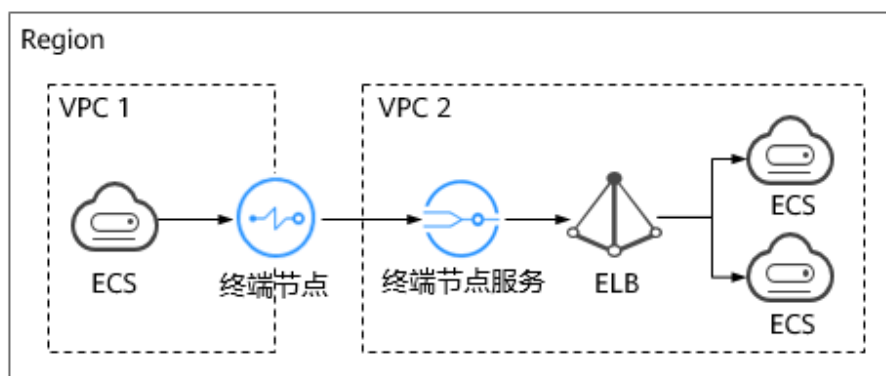
VPC 终端节点支持同一区域云资源的跨 VPC 通信。

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。

这两个 VPC 既可以属于同一帐号，也可以属于不同帐号，本章节以“同一帐号”的跨 VPC 通信为例进行介绍。

例如，VPC1 和 VPC2 属于同一帐号，为 VPC1 创建终端节点，并将 VPC2 中待访问的后端资源 ELB 创建为终端节点服务，实现 VPC1 的 ECS 通过私网 IP 访问 VPC2 的 ELB，如图 2-1 所示。

图2-1 跨 VPC 通信的终端节点



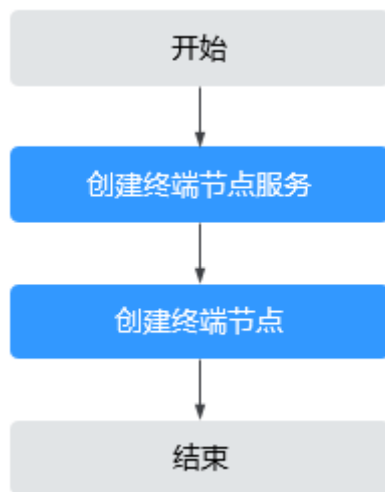
说明

- 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 属于不同帐号，请参考 2.3 配置跨 VPC 通信的终端节点（不同帐号）。

操作流程

配置同一帐号下的跨 VPC 通信，具体操作流程如图 2-2 所示。

图2-2 操作流程



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。

图2-3 创建终端节点服务

创建终端节点服务 < 返回终端节点服务列表

* 区域
不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

名称

* 虚拟私有云 [查看虚拟私有云](#)

服务类型

连接审批 ?

* 端口映射 协议 服务端口 ? 终端端口 ?

+ 添加端口映射 您还可以添加49条

* 后端资源类型

* 选择负载均衡 [查看负载均衡](#)

标签
如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。 [查看预定义标签](#)

您还可以添加10个标签。

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。
名称	可选参数。 终端节点服务的名称。 长度不大于 16，支持大小写字母、数字、下划线、中划线。 <ul style="list-style-type: none">如果您不填写该参数，系统生成的终端节点服务的名称为 {region}.{service_id}。如果您填写该参数，系统生成的终端节点服务的名称为 {region}.{Name}.{service_id}。
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	<p>终端节点服务与终端节点建立连接关系，进行通信，协议可选择 TCP 或 UDP。</p> <ul style="list-style-type: none">• 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。 <p>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。</p> <p>说明</p> <p>通过“终端端口 → 服务端口”的方式进行访问。</p>
后端资源类型	<p>实际提供服务的后端资源。</p> <p>可创建为终端节点服务的后端资源包括：</p> <ul style="list-style-type: none">• 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。 <p>此处选择“弹性负载均衡”。</p> <p>说明</p> <p>安全组添加的规则是白名单。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 198.19.128.0/20 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”。</p>
选择负载均衡	<p>“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，只支持弹性负载均衡。</p> <p>说明</p> <p>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。</p>

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。

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。

图2-4 创建终端节点（按名称查找服务-接口型）



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”。 <ul style="list-style-type: none">• 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。 输入终端节点服务名称，单击“验证”： <ul style="list-style-type: none">• 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
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。 <ul style="list-style-type: none">终端节点服务的类型为“网关”时，该参数不可见；终端节点服务的类型为“接口”时，可选择是否创建内网域名。
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。

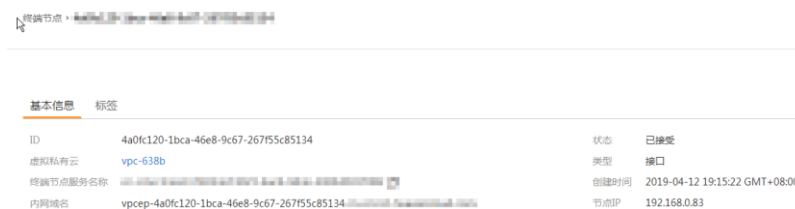
如果终端节点状态为“已接受”，表示终端节点已成功连接至终端节点服务；如果终端节点状态为“待接受”，表示要连接的终端节点服务开启了“连接审批”功能，需要先进行审批，操作如下：

- 在左侧导航栏选择“VPC 终端节点>终端节点服务”。
- 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。
- 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”。
- 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）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”）。

图2-5 终端节点详情



基本信息		标签	
ID	4a0fc120-1bca-46e8-9c67-267f55c85134	状态	已接受
虚拟私有云	vpc-638b	类型	接口
终端节点服务名称	vpcep-4a0fc120-1bca-46e8-9c67-267f55c85134	创建时间	2019-04-12 19:15:22 GMT+08:00
内网域名	vpcep-4a0fc120-1bca-46e8-9c67-267f55c85134	节点IP	192.168.0.83

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 2-6 所示。

图2-6 登录云服务器访问 VPC 终端节点

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1062.1.1.el7.x86_64 on an x86_64

ecs-66a6 login: root
Password:

Welcome to ██████ Service

[root@ecs-66a6 ~]# ssh 192.168.1.114
The authenticity of host '192.168.1.114 (192.168.1.114)' can't be established.
ECDSA key fingerprint is SHA256:HT23UczQ+Oaj0+6zD1gF1rquNks0MJ1aCouueNCn31s.
ECDSA key fingerprint is MD5:2c:56:49:51:b5:f7:f4:b0:16:0c:1d:b4:5c:77:e2:19.
Are you sure you want to continue connecting (yes/no)? no
```

2.3 配置跨 VPC 通信的终端节点（不同帐号）

2.3.1 简介

操作场景

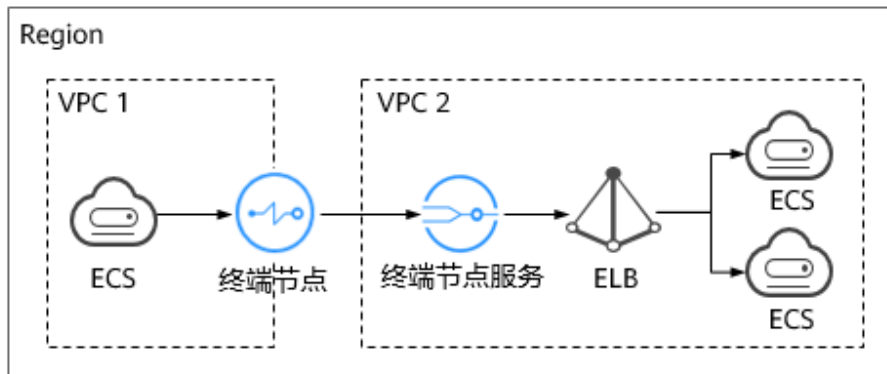
VPC 终端节点支持同一区域云资源的跨 VPC 通信。

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。

这两个 VPC 既可以属于同一帐号，也可以属于不同帐号，本章节以“不同帐号”的跨 VPC 通信为例进行介绍。

例如，VPC1 和 VPC2 分别属于帐号 A 和帐号 B，为 VPC1 创建终端节点，并将 VPC2 中待访问的后端资源 ELB 创建为终端节点服务，实现 VPC1 的 ECS 通过私网 IP 访问 VPC2 的 ELB，如图 2-7 所示。

图2-7 跨 VPC 通信的终端节点



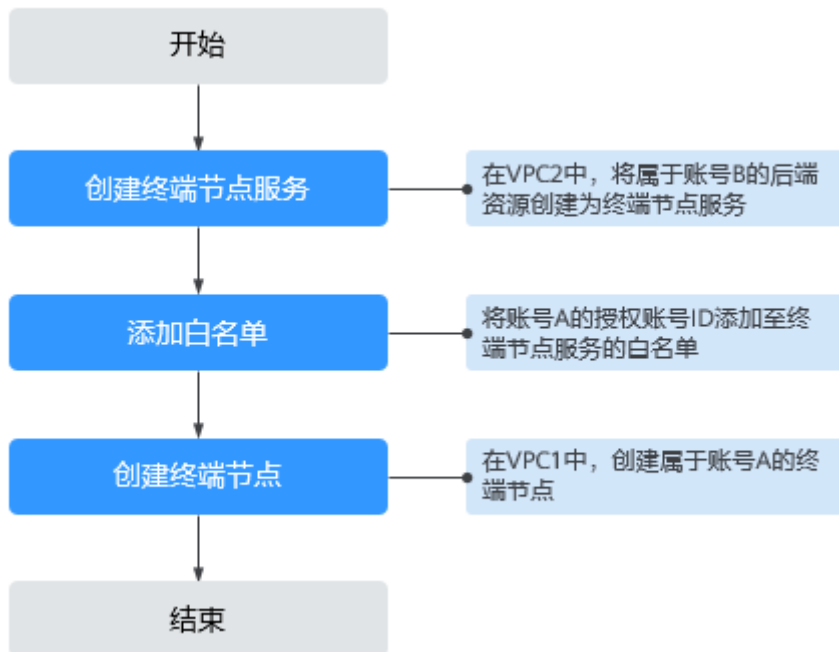
说明

- 如图 2-7 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 的授权帐号 ID 添加到 VPC2 的终端节点服务的白名单中。
- 若两个 VPC 属于同一帐号，请参考 2.2 配置跨 VPC 通信的终端节点（同一帐号）。

操作流程

配置不同帐号下的跨 VPC 通信，具体操作流程如图 2-8 所示。

图2-8 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，属于帐号 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。
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。

图2-9 创建终端节点服务



创建终端节点服务 < 返回终端节点服务列表

* 区域

名称

* 虚拟私有云 vpc-638b(192.168.0.0/20) [查看虚拟私有云](#)

服务类型

连接审批 [?](#)

* 端口映射 协议 TCP 服务端口 终端端口

+ 添加端口映射 您还可以添加49条

* 后端资源类型

* 选择负载均衡 elb-97rn [查看负载均衡](#)

标签

您还可以添加10个标签。

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。
名称	可选参数。 终端节点服务的名称。 长度不大于 16，支持大小写字母、数字、下划线、中划线。 <ul style="list-style-type: none">如果您不填写该参数，系统生成的终端节点服务的名称为 {region}.{service_id}。如果您填写该参数，系统生成的终端节点服务的名称为 {region}.{Name}.{service_id}。
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，协议可选择 TCP 或 UDP。 <ul style="list-style-type: none">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： <ul style="list-style-type: none">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 安全组添加的规则是白名单。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 198.19.128.0/20 的白名单入方向规则，详细操作请参考

参数	说明
	《虚拟私有云用户指南》中的“添加安全组规则”。
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，只支持弹性负载均衡。 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。

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租户的终端节点进行访问。

创建完终端节点服务后，可以设置允许连接该终端节点服务的授权帐号 ID，将授权帐号 ID 添加至终端节点服务的白名单中。

本操作指导您获取帐号 ID，并添加帐号 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。

获取被授权的帐号 ID

1. 登录管理控制台。
2. 单击帐号下的“我的凭证”。

图2-10 我的凭证



进入“我的凭证”页面，即可查看到 VPC1 所属租户的“帐号 ID”，如图 2-11 所示。

图2-11 帐号 ID



添加被授权的帐号 ID 至终端节点服务的白名单中

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，输入授权用户的帐号 ID，添加白名单。

图2-12 添加白名单记录

添加白名单记录

终端节点服务名称

添加授权账号 ?

授权账号ID	操作
iam:domain::domain_id	删除

+ 继续添加 您本次还可以添加49个授权账号

确定 取消

说明

- 本帐号默认在自身帐号的终端节点服务的白名单中。
 - 授权帐号 ID 格式为：(iam:domain::domain_id)。 “domain_id” 表示授权用户的帐号 ID，例如 “iam:domain::1564ec50ef2a47c791ea5536353ed4b9”。
 - 添加 “*” 到白名单，表示所有用户可访问。
8. 单击“确定”，完成白名单的设置。

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

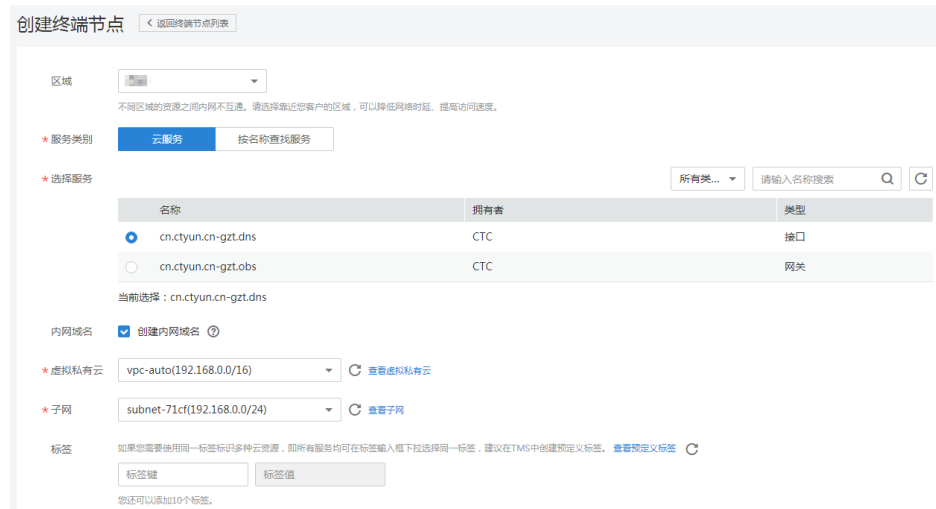
终端节点需要选择与终端节点服务相同的区域和项目。

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。

图2-13 创建终端节点（按名称查找服务-接口型）



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	<p>可选择“云服务”或“按名称查找服务”。</p> <ul style="list-style-type: none"> 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”。 <p>此处选择“按名称查找服务”。</p>
服务名称	<p>若“服务类别”选择“按名称查找服务”，则会出现该参数。</p> <p>输入终端节点服务名称，单击“验证”：</p> <ul style="list-style-type: none"> 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。
内网域名	<p>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。</p> <ul style="list-style-type: none"> 终端节点服务的类型为“网关”时，该参数不可见； 终端节点服务的类型为“接口”时，可选择是否创建内网域名。

参数	说明
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。

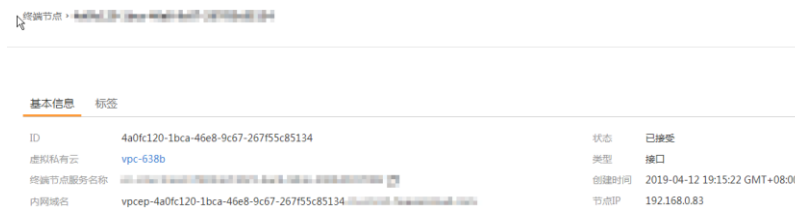
6. 参数配置完成，单击“立即创建”，进行规格确认。
 - 规格确认无误，单击“提交”，任务提交成功。
 - 参数信息配置有误，需要修改，单击“上一步”，修改参数，然后单击“提交”。
7. 连接管理。

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”。
 - 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）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”）。

图2-14 终端节点详情



基本信息		标签	
ID	4a0fc120-1bca-46e8-9c67-267f55c85134	状态	已接受
虚拟私有云	vpc-638b	类型	接口
终端节点服务名称	vpcep-4a0fc120-1bca-46e8-9c67-267f55c85134	创建时间	2019-04-12 19:15:22 GMT+08:00
内网域名	vpcep-4a0fc120-1bca-46e8-9c67-267f55c85134	节点IP	192.168.0.83

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

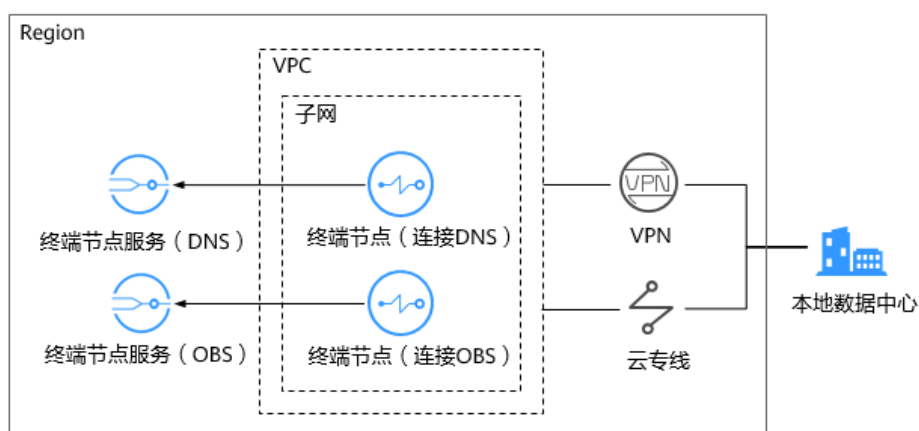
2.4.1 简介

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2-15 本地数据中心访问 OBS（内网）



如图 2-15 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。

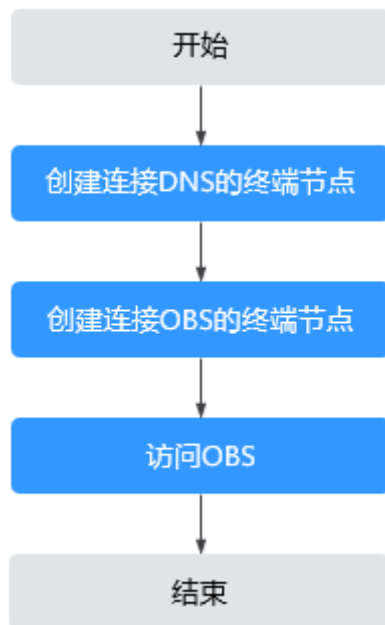
本操作场景涉及两个系统创建的终端节点服务：

- 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。
例如：cn.ctyun.cn-gzt.dns
- 终端节点服务（OBS）：提供 OBS 服务，供线下本地数据中心访问。
例如：cn.ctyun.cn-gzt.obs

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 2-16 所示。

图2-16 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。

图2-17 创建终端节点

创建终端节点 < 返回终端节点列表

区域: [下拉菜单]

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: 云服务 按名称查找服务

* 选择服务: 所有类... 请输入名称搜索 [搜索] [清除]

名称	拥有者	类型
<input checked="" type="radio"/> cn.ctyun.cn-gzt.dns	CTC	接口
<input type="radio"/> cn.ctyun.cn-gzt.obs	CTC	网关

当前选择: cn.ctyun.cn-gzt.dns

内网域名: 创建内网域名

* 虚拟私有云: vpc-auto(192.168.0.0/16) [查看虚拟私有云]

* 子网: subnet-71cf(192.168.0.0/24) [查看子网]

标签: 如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。 [查看预定义标签]

标签键: [输入框] 标签值: [输入框]

您还可以添加10个标签。

5. 根据界面提示配置参数。

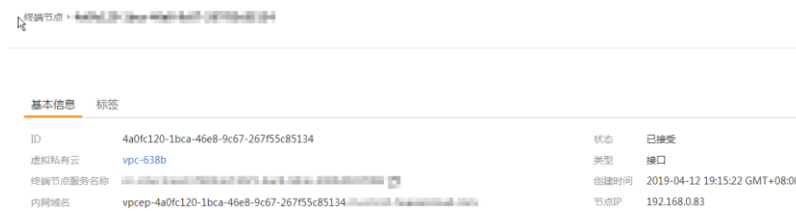
表2-6 终端节点配置参数

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”。 <ul style="list-style-type: none"> 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，即“cn.ctyun.cn-gzt.dns”。
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。 接口终端节点才需在页面设置此选项。 <ul style="list-style-type: none"> 终端节点服务的类型为“网关”时，该参数不可见； 终端节点服务的类型为“接口”时，可选择是否创建内网域名。
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	说明
	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”。
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“cn.ctyun.cn-gzt.dns”的终端节点创建成功。
8. 单击终端节点 ID，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”）。

图2-18 终端节点详情



基本信息		标签
ID	4a0fc120-1bca-46e8-9c67-26755c85134	状态 已接受
虚拟私有云	vpc-638b	类型 接口
终端节点服务名称		创建时间 2019-04-12 19:15:22 GMT+08:00
内网域名	vpcep-4a0fc120-1bca-46e8-9c67-26755c85134	节点IP 192.168.0.83

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。

图2-19 创建终端节点

创建终端节点 < 返回终端节点列表

区域

不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延、提高访问速度。

* 服务类别 云服务 按名称查找服务

* 选择服务 所有类... 请输入名称搜索

名称	所有者	类型
<input type="radio"/> cn.ctyun.cn-gzt.dns	CTC	接口
<input checked="" type="radio"/> cn.ctyun.cn-gzt.obs	CTC	网关

当前选择: cn.ctyun.cn-gzt.obs

* 虚拟私有云

* 路由表

标签 如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。

标签键 标签值

您还可以添加10个标签。

5. 根据界面提示配置参数。

表2-7 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”。 <ul style="list-style-type: none">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，即“cn.ctyun.cn-gzt.obs”。
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”。

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“cn.ctyun.cn-gzt.obs”的终端节点创建成功。

8. 单击终端节点 ID，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 VPN 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 VPN 或者云专线与 VPC 连通。

- VPN 连接对应的需要与本地数据中心互通的 VPC 子网网段，需包含 OBS 的网段 100.125.0.0/16。

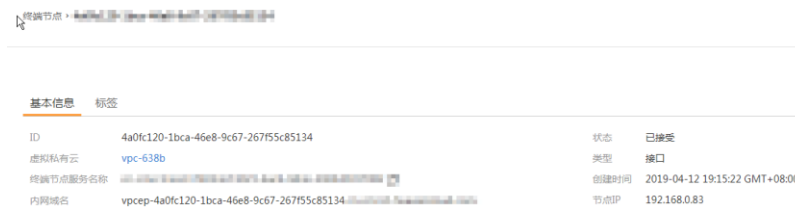
创建虚拟专用网络，请参考《虚拟专用网络用户指南》。

- 专线虚拟网关允许访问的 VPC 子网网段需包含 OBS 的网段 100.125.0.0/16。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，查看该终端节点的“节点 IP”。

图2-20 终端节点详情



基本信息		标签	
ID	4a0fc120-1bca-46e8-9c67-267f55c85134	状态	已接受
虚拟私有云	vpc-638b	类型	接口
终端节点服务名称	vpcep-4a0fc120-1bca-46e8-9c67-267f55c85134	创建时间	2019-04-12 19:15:22 GMT+08:00
内网域名	vpcep-4a0fc120-1bca-46e8-9c67-267f55c85134	节点IP	192.168.0.83

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 内，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](#)中的节点 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。
- 连接 DNS 服务的终端节点的节点 IP 地址为 xx.xx.xx.xx，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](#)中的节点 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。
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。

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 bucket.endpoint
```

其中：

- bucket: 表示 OBS 的桶名。
- endpoint: 表示 OBS 的 Endpoint 信息。

📖 说明

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
3.2 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。	<ul style="list-style-type: none">• 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：<ul style="list-style-type: none">- 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

操作	说明	使用限制
		一个后端资源实例。
3.3 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。
3.4 删除终端节点服务	介绍如何删除创建的终端节点服务。	<ul style="list-style-type: none">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用户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。
3.5 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。
3.6 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。	<ul style="list-style-type: none">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帐号 ID。
3.7 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。	<ul style="list-style-type: none">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。

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3-1 创建终端节点服务



创建终端节点服务 < 返回终端节点服务列表

* 区域

名称

* 虚拟私有云 vpc-638b(192.168.0.0/20) [查看虚拟私有云](#)

服务类型

连接审批

* 端口映射 协议 TCP 服务端口 终端端口

+ 添加端口映射 您还可以添加49条

* 后端资源类型

* 选择负载均衡 elb-97rm [查看负载均衡](#)

标签 如果您需要使用同一标签标识多种云资源，即所有服务均可在标签输入框下拉选择同一标签，建议在TMS中创建预定义标签。 [查看预定义标签](#)

您还可以添加10个标签。

5. 根据界面提示配置参数，参数说明如表 3-2 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。

参数	说明
	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。
名称	可选参数。 终端节点服务的名称。 长度不超过 16 个字符，允许输入大小写字母、数字、下划线、中划线。 <ul style="list-style-type: none">如果您不填写该参数，系统生成的终端节点服务的名称为 {region}.{service_id}。如果您填写该参数，系统生成的终端节点服务的名称为 {region}.{Name}.{service_id}。
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，详细内容请参见 3.5 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，协议可选择 TCP 或 UDP。 <ul style="list-style-type: none">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。 端口映射添加完成后不支持修改或者删除。
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： <ul style="list-style-type: none">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 安全组添加的规则是白名单。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 198.19.128.0/20 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”。

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，只支持弹性负载均衡。 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。

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。

图3-2 终端节点服务基本信息

基本信息	连接管理	权限管理	端口映射	标签
名称	test.e9c186ca-99e4-4a88-9011-8898f1d680c0			
ID	e9c186ca-99e4-4a88-9011-8898f1d680c0			
后端资源类型	增强型负载均衡			
后端资源名称	elb-97m			
虚拟私有云	vpc-638b			
状态	可连接			
连接审批	<input checked="" type="checkbox"/>			
服务类型	接口			
创建时间	2019-05-27 17:09:29 GMT+08:00			

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 5.4 终端节点服务和终端节点有哪些状态？。
	拥有者	终端节点创建者的帐号 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”。
权限管理	授权帐号 ID	连接访问终端节点的授权帐号 ID 或者*。 若“授权帐号 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帐号进行操作，支持将授权帐号从白名单中删除。
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 5.4 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”栏下的“删除”按钮。

图3-3 删除终端节点服务



6. 在弹出的对话框中单击“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。

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。

图3-4 连接管理



终端节点ID	别名标识	状态	所有者	创建时间	操作
4a0fc120-1bca-46e8-9c67-267f5c85134	6723388	已接受	1564ec50e2a47c791ea553635e94b9	2019-04-12 19:15:22 GMT+08:00	接受 拒绝

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帐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帐号 ID，支持添加或者移除白名单中的授权帐号 ID。

- 如果白名单为空，则不支持跨帐号的终端节点连接终端节点服务。
- 如果某一帐号包含在终端节点服务的白名单中，则可以通过该帐号创建连接终端节点服务的终端节点。
- 如果某一帐号未包含在终端节点服务的白名单中，则无法通过该帐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。

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，输入授权用户的帐号 ID，添加白名单。

图3-5 添加白名单记录

添加白名单记录

终端节点服务名称

添加授权账号 ?

授权账号ID	操作
iam:domain::domain_id	删除

+ 继续添加 您本次还可以添加49个授权账号

确定 取消

说明

- 本帐号默认在自身帐号的终端节点服务的白名单中。
- 授权帐号 ID 格式为：(iam:domain::domain_id)。
“domain_id”表示授权用户的帐号 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，单击对应授权帐号 ID “操作”栏下的“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帐号 ID，单击上方的“删除”。
7. 在弹出的对话框中单击“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。

端口映射定义了终端节点与终端节点服务之间通信所支持的协议及端口号，在创建终端节点服务时设置，包括：

- 协议：终端节点与终端节点服务支持的通信协议。
- 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。

说明

不支持修改和删除终端节点服务的端口映射。

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。
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。

图3-6 端口映射



The screenshot shows a console interface with a navigation bar at the top containing tabs: 基本信息, 连接管理, 权限管理, 端口映射 (selected), and 标签. Below the navigation bar is a table with three columns: 协议, 服务端口, and 终端端口. The table contains one row with the following values: TCP, 8989, and 226.

协议	服务端口	终端端口
TCP	8989	226

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
4.2 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。	<ul style="list-style-type: none">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。
4.3 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。
4.4 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。

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](#)

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。

图4-1 创建终端节点（云服务-接口型）



创建终端节点 [返回终端节点列表](#)

区域

不同区域的资源之间内网不互通。请选择靠近您客户的区域，可以降低网络时延，提高访问速度。

* 服务类别 **云服务**

* 选择服务

名称	拥有者	类型
<input checked="" type="radio"/> cn.ctyun.cn-gzt.dns	CTC	接口
<input type="radio"/> cn.ctyun.cn-gzt.obs	CTC	网关

当前选择：cn.ctyun.cn-gzt.dns

内网域名 创建内网域名

* 虚拟私有云

* 子网

标签

您还可以添加10个标签。

图4-2 创建终端节点（按名称查找服务-接口型）

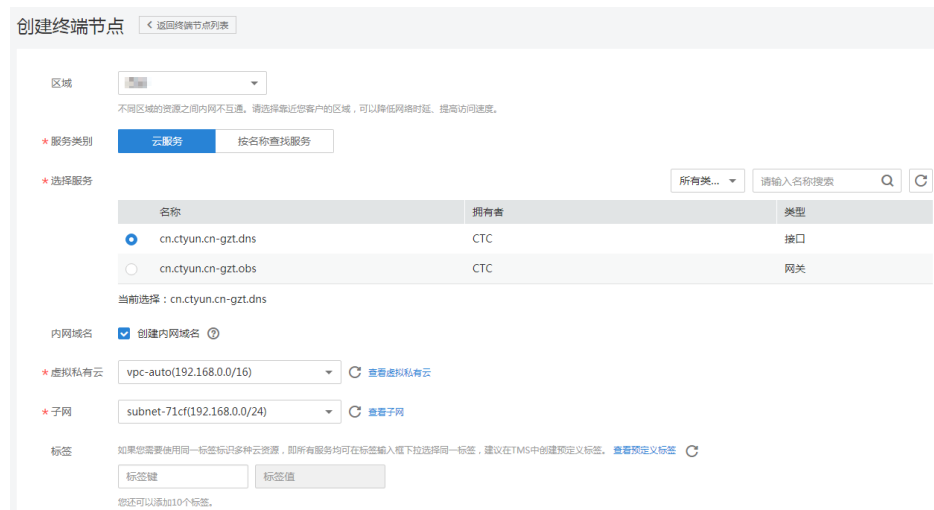


表4-2 终端节点配置参数

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	<p>可选择“云服务”或“按名称查找服务”。</p> <ul style="list-style-type: none"> 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	<p>若“服务类别”选择“云服务”，则会出现该参数。</p> <p>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。</p>
服务名称	<p>若“服务类别”选择“按名称查找服务”，则会出现该参数。</p> <p>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”：</p> <ul style="list-style-type: none"> 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。
内网域名	<p>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。</p> <p>接口类型终端节点才需在页面设置此选项。</p> <ul style="list-style-type: none"> 终端节点服务的类型为“网关”时，该参数不可见； 终端节点服务的类型为“接口”时，可选择是否创建内网域名。

参数	说明
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。

- 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

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

图4-3 创建终端节点（云服务-网关型）



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”。

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。 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。

- 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”。

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。

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。

- 登录管理控制台。
- 在管理控制台左上角单击“📍”图标，选择区域和项目。
- 单击“服务列表”，选择“网络 > VPC 终端节点”，进入“终端节点”页面。
- 单击要查看的终端节点 ID，即可查看终端节点的基本信息。

终端节点创建成功后，会生成一个“节点 IP”（即私有 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”）。

图4-4 终端节点详情

基本信息		标签	
ID	4a0fc120-1bca-46e8-9c67-267f55c85134	状态	已接受
虚拟私有云	vpc-638b	类型	接口
终端节点服务名称	vpccep-4a0fc120-1bca-46e8-9c67-267f55c85134	创建时间	2019-04-12 19:15:22 GMT+08:00
内网域名	vpccep-4a0fc120-1bca-46e8-9c67-267f55c85134	节点IP	192.168.0.83

表4-4 参数说明

页签	参数名称	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。
标签	键	终端节点的标签“键”。
	值	终端节点的标签“值”。
	操作	对终端节点标签进行操作，可选择“编辑”或“删除”标签。

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。

- 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。

- 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

- 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。
- 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

- 登录管理控制台。
- 在管理控制台左上角单击“📍”图标，选择区域和项目。
- 单击“服务列表”中的“网络 > VPC 终端节点”，进入“终端节点”页面。
- 在左侧导航栏选择“VPC 终端节点 > 终端节点”。
- 单击待删除的终端节点所在行的“删除”按钮。

图4-5 删除终端节点



- 在弹出的对话框中单击“是”，删除终端节点。

5 常见问题


5.1 什么是配额？

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个云资源。

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，请拨打热线或发送邮件至客服，客服会及时为您处理配额调整的需求，并以电话或邮件的形式告知您实时进展。

在拨打热线或发送邮件之前，请您准备好以下信息：

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

5.2 如何检查终端节点服务所在后端弹性云服务器器的网络配置？

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 198.19.128.0/20 网段的地址，如果没有放行，请添加 198.19.128.0/20 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。

5.3 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 5-1。

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5-1 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。
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。	而通过 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。

5.4 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 5-2 所示。

表5-2 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 5-3 所示。

表5-3 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。

A 修订记录

版本日期	变更说明
2019-05-10	第一次正式发布。