VPC 终端节点

快速入门

文档版本 04

发布日期 2024-05-10

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。

目 录

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1-1**。

表 1-1 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购买终端节点，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）**
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 准备工作

在使用VPC终端节点前，您需要完成本文中的准备工作。

- **注册华为云并实名认证**
- **为帐户充值**

注册华为云并实名认证

如果用户已注册华为云，可直接登录管理控制台，访问VPC终端节点。如果用户没有登录管理控制台的账号，请先注册华为云。

说明

VPC终端节点不支持通过华为云APP操作，请通过华为云官网使用VPC终端节点。

1. 登录网站**https://www.huaweicloud.com/**。
2. 单击“注册”。

   进入注册页面，根据提示信息完成注册，详细操作请参见**如何注册华为云管理控制台的用户?**

   注册成功后，系统会自动跳转至您的个人信息界面。
3. 个人或企业账号实名认证请参考：**实名认证**。

注册成功后，该账号可访问华为云的所有服务，包括VPC终端节点。

为账户充值

您需要确保账户有足够金额。

- 关于VPC终端节点资源的价格和计费原则，请参见**计费说明**。
- 关于充值，请参见**账户充值**。

3 配置跨 VPC 通信的终端节点（同一账号）

3.1 简介

操作场景

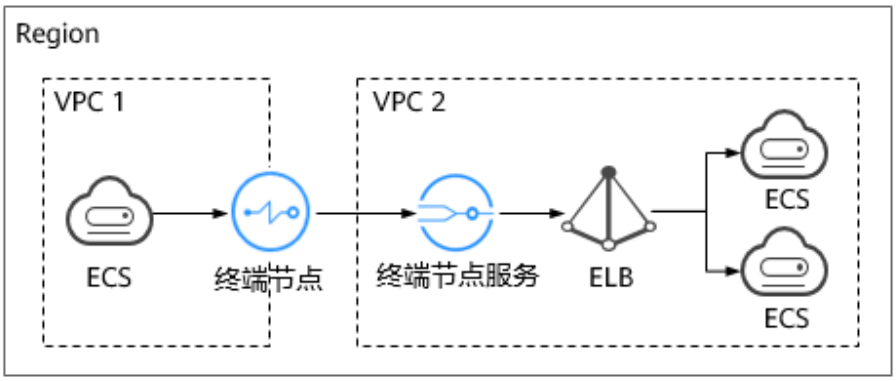
VPC终端节点支持同一区域云资源的跨VPC通信。

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“同账号”的多个VPC中的云资源如何实现跨VPC通信。

如图3-1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中购买终端节点，实现VPC1中的ECS通过私网IP访问VPC2中的ELB。

图 3-1 跨 VPC 通信的终端节点



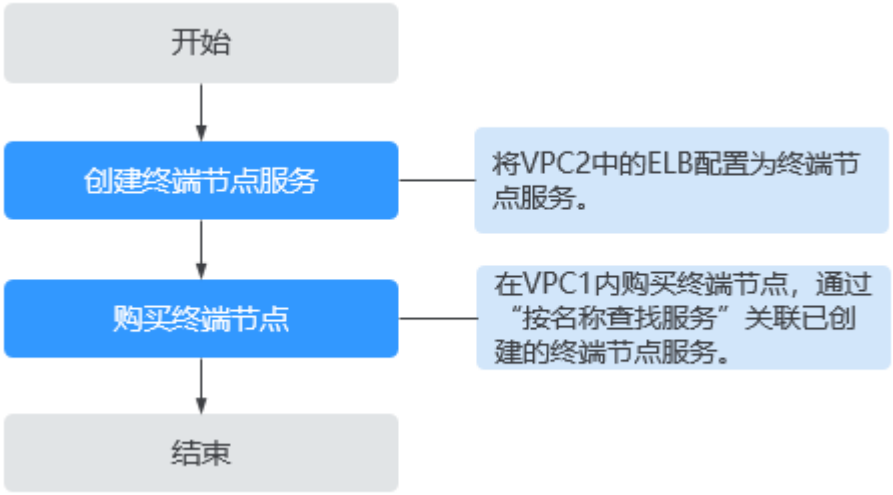
说明

- 如图3-1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3-2所示。

图 3-2 操作流程



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“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 3-3 创建终端节点服务

5. 根据界面提示配置参数。

表 3-1 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。 ● 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}。
网络类型	终端节点服务的网络类型。 支持选择“IPv4”、“IPv6”。 ● IPv4：表示仅支持IPv4网络类型。 ● IPv6：表示仅支持IPv6网络类型。
虚拟私有云	终端节点服务所属虚拟私有云。
子网	终端节点服务所属子网。 当“网络类型”选择“IPv6”时需要配置该参数。
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。 ● 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。 如果您在配置完成后需要通过SSH命令验证连通性，根据SSH协议，此处需要将服务端口设置为22。
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。当“网络类型”选择“IPv4”时可以选择裸金属服务器。 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20个标签。 标签的命名规则请参考**表3-2**。 **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。 预定义标签的详细内容，请参见**预定义标签简介**。 如您的组织已经设定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 3-2 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36个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。
值	• 不能为空。 • 长度不超过43个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。

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。

图 3-4 终端节点服务详情

3.3 步骤二：购买终端节点

操作场景

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

本节指导您购买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“购买终端节点”。
   进入“购买终端节点”页面。

图 3-5 购买终端节点（按名称查找服务-接口型）

5. 根据界面提示配置参数。

表 3-3 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。
计费方式	按需计费是后付费模式，按终端节点的实际使用时长计费，可以随时开通/删除终端节点。 仅支持按需计费。

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。
终端节点类型	根据选择关联的终端节点服务的类型展示。 ● 选择关联接口终端节点服务时，默认展示“接口终端节点”。 ● 选择关联网关终端节点服务时，默认展示“网关终端节点”。
实例类型	选择关联接口终端节点服务时，需要配置该参数。 支持选择“专业型”、“基础型”。 ● **专业型：**新上线终端节点实例类型，目前正在公测中。单实例带宽规格最大支持40Gbps、支持IPv6双栈、组织粒度的策略授权等功能。 ● **基础型：**原终端节点实例类型。
网络类型	选择关联接口终端节点服务且开启高级模式时，需要配置该参数。 支持选择“IPv4”、“双栈”。 ● IPv4：表示仅支持IPv4网络类型。 ● 双栈：表示同时支持IPv4和IPv6网络类型。
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。
IPv4地址	支持自动分配IPv4地址或手动指定IP地址。
IPv6地址	实例类型选择“专业型”，同时网络类型选择“双栈”，需要配置该参数。 支持自动分配IPv6地址或手动指定IP地址。

参数	说明
节点IP	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。 终端节点的私网IP。可选择“自动分配”或“手动分配”。
访问控制	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。 用于设置允许访问终端节点的IP地址或网段。 ● 开启：只允许白名单列表中的IP地址或网段访问终端节点。 ● 关闭：允许任何IP地址或网段访问终端节点。
白名单	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。 用于设置允许访问的IP地址或网段，最多支持添加20个记录。
策略	双端固定策略，即设置VPC终端节点策略与桶策略，可以对OBS的资源提供VPC粒度的权限控制。 当终端节点连接的终端节点服务开启“访问控制策略”时，支持配置终端节点策略。 ● 设置VPC终端节点策略可以限制VPC中的服务器（ECS/CCE/BMS）访问OBS中的特定资源。 ● 设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问。
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20个标签。 标签的命名规则请参考**表3-4**。 **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。 预定义标签的详细内容，请参见**预定义标签简介**。 如您的组织已经设定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 3-4 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36个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。
值	• 不能为空。 • 长度不超过43个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。

6. 参数配置完成，单击“立即购买”，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。

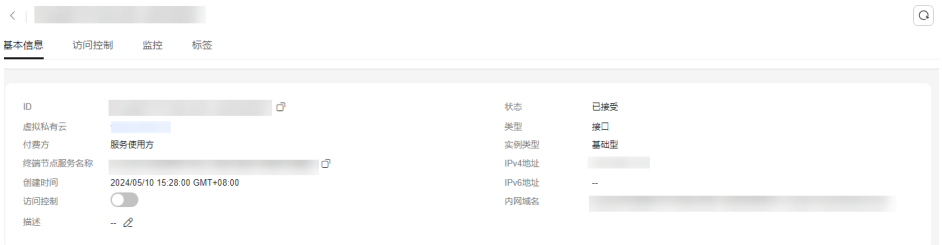
   c. 在终端节点服务详情页面，单击“连接管理”

      - 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 3-6 终端节点详情（接口）



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

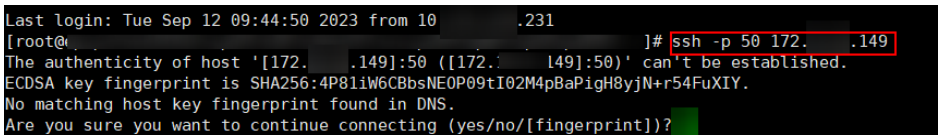
使用SSH命令远程登录VPC1中的弹性云服务器， 访问VPC终端节点的节点IP或内网域名，详细如图3-7所示。

```
ssh -p 终端端口 节点IP
```

⚠ 注意

根据SSH协议，您需要在**创建终端节点服务**时，将服务端口设置为22，否则无法使用SSH命令验证成功。

图 3-7 登录云服务器访问 VPC 终端节点



4 配置跨 VPC 通信的终端节点（不同账号）

4.1 简介

操作场景

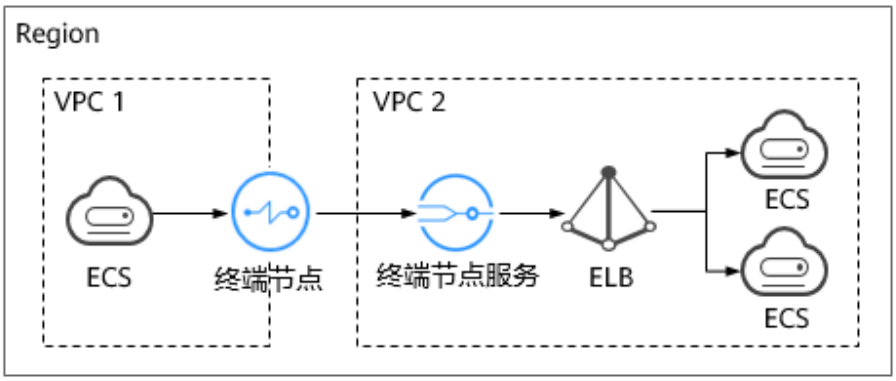
VPC终端节点支持同一区域云资源的跨VPC通信。

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4-1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中购买终端节点，实现VPC1中的ECS通过私网IP访问VPC2中的ELB。

图 4-1 跨 VPC 通信的终端节点



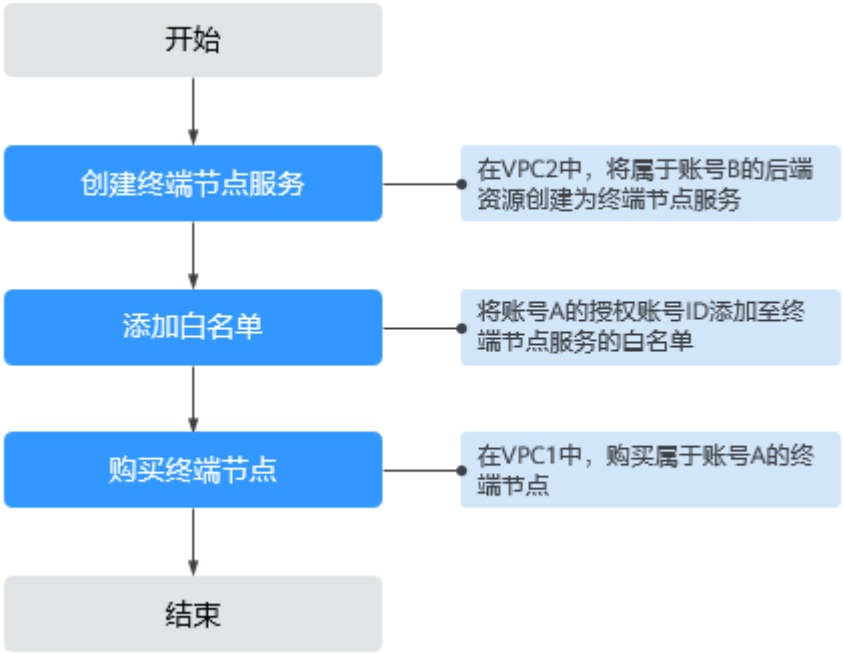
说明

- 如图4-1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。
- 在购买终端节点前，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4-2所示。

图 4-2 操作流程



4.2 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。

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 4-3 创建终端节点服务

5. 根据界面提示配置参数。

表 4-1 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。 • 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}。
网络类型	终端节点服务的网络类型。 支持选择“IPv4”、“IPv6”。 • IPv4：表示仅支持IPv4网络类型。 • IPv6：表示仅支持IPv6网络类型。

参数	说明
虚拟私有云	终端节点服务所属虚拟私有云。
子网	终端节点服务所属子网。 当“网络类型”选择“IPv6”时需要配置该参数。
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。 ● 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。 如果您在配置完成后需要通过SSH命令验证连通性，根据SSH协议，此处需要将服务端口设置为22。
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。当“网络类型”选择“IPv4”时可以选择裸金属服务器。 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20个标签。 标签的命名规则请参考表4-2。 **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。 预定义标签的详细内容，请参见预定义标签简介。 如您的组织已经设定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 4-2 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36个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。
值	• 不能为空。 • 长度不超过43个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。

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。

图 4-4 终端节点服务详情

4.3 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。

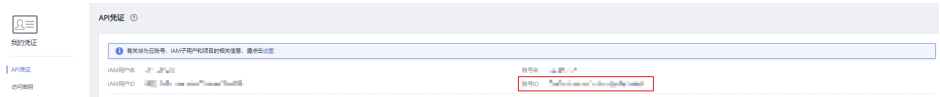
获取被授权的账号 ID

1. 登录管理控制台。
2. 单击账号下的“我的凭证”。

图 4-5 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”，如图4-6所示。

图 4-6 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”。

图 4-7 添加白名单记录

说明

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

4.4 步骤三：购买终端节点

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中购买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“购买终端节点”。
   进入“购买终端节点”页面。

图 4-8 购买终端节点（按名称查找服务-接口型）

5. 根据界面提示配置参数。

表 4-3 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。
计费方式	按需计费是后付费模式，按终端节点的实际使用时长计费，可以随时开通/删除终端节点。 仅支持按需计费。
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。

参数	说明
终端节点类型	根据选择关联的终端节点服务的类型展示。 ● 选择关联接口终端节点服务时，默认展示“接口终端节点”。 ● 选择关联网关终端节点服务时，默认展示“网关终端节点”。
实例类型	选择关联接口终端节点服务时，需要配置该参数。 支持选择“专业型”、“基础型”。 ● **专业型：**新上线终端节点实例类型，目前正在公测中。单实例带宽规格最大支持40Gbps、支持IPv6双栈、组织粒度的策略授权等功能。 ● **基础型：**原终端节点实例类型。
网络类型	选择关联接口终端节点服务且开启高级模式时，需要配置该参数。 支持选择“IPv4”、“双栈”。 ● IPv4：表示仅支持IPv4网络类型。 ● 双栈：表示同时支持IPv4和IPv6网络类型。
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。
IPv4地址	支持自动分配IPv4地址或手动指定IP地址。
IPv6地址	实例类型选择“专业型”，同时网络类型选择“双栈”，需要配置该参数。 支持自动分配IPv6地址或手动指定IP地址。
节点IP	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。 终端节点的私网IP。可选择“自动分配”或“手动分配”。
访问控制	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。 用于设置允许访问终端节点的IP地址或网段。 ● 开启：只允许白名单列表中的IP地址或网段访问终端节点。 ● 关闭：允许任何IP地址或网段访问终端节点。
白名单	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。 用于设置允许访问的IP地址或网段，最多支持添加20个记录。

参数	说明
策略	双端固定策略，即设置VPC终端节点策略与桶策略，可以对OBS的资源提供VPC粒度的权限控制。 当终端节点连接的终端节点服务开启“访问控制策略”时，支持配置终端节点策略。 ● 设置VPC终端节点策略可以限制VPC中的服务器（ECS/CCE/BMS）访问OBS中的特定资源。 ● 设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问。
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20个标签。 标签的命名规则请参考**表4-4**。 **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。 预定义标签的详细内容，请参见**预定义标签简介**。 如您的组织已经设定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 4-4 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36个字符。 ● 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。
值	● 不能为空。 ● 长度不超过43个字符。 ● 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。

6. 参数配置完成，单击“立即购买”，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 4-9 终端节点详情（接口）

   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。

5 配置访问 OBS 服务内网地址的终端节点

5.1 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。

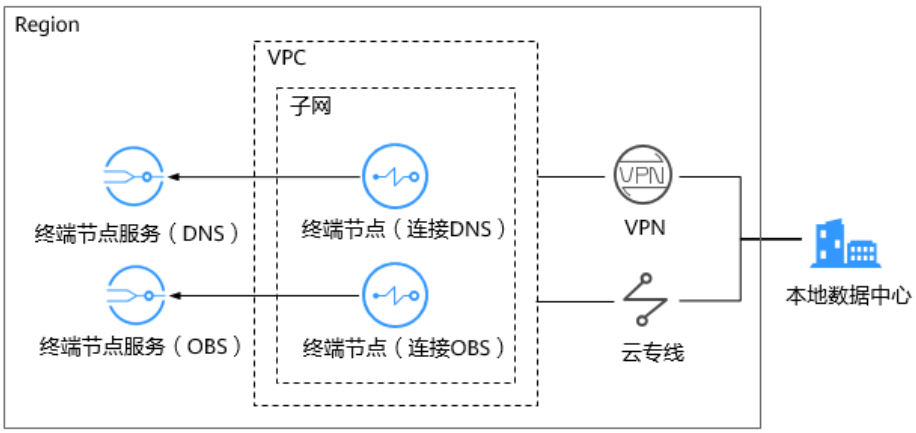
本节介绍线下节点（即本地数据中心）通过内网方式访问云上OBS服务的配置指导。

说明

仅“拉美-墨西哥城一”、“拉美-圣保罗一”和“拉美-圣地亚哥”区域支持通过控制台直接选择“网关”类型的OBS终端节点服务，因此本场景仅适用于这些区域。

其他区域的“网关”类型的OBS终端节点服务目前需要按照名称查找并关联终端节点，终端节点服务名称请**提交工单**或联系OBS服务运维人员获取。

图 5-1 本地数据中心访问 OBS（内网）



如图5-1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内购买终端节点，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，购买终端节点的前提是要连接的终端节点服务已存在。

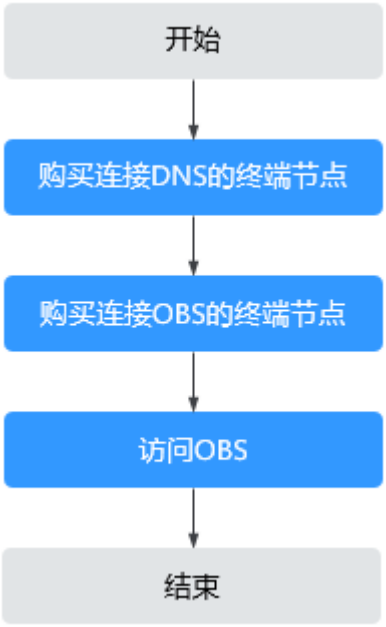
本操作场景涉及两个系统创建的终端节点服务：

- 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。
  以“拉美-墨西哥城一”为例：com.myhuaweicloud.na-mexico-1.dns
- 终端节点服务（OBS）：提供OBS服务，供线下本地数据中心访问。
  以“拉美-墨西哥城一”为例：com.myhuaweicloud.na-mexico-1.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5-2所示。

图 5-2 操作流程



5.2 步骤一：购买连接 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，您需要购买连接DNS服务的终端节点。

前提条件

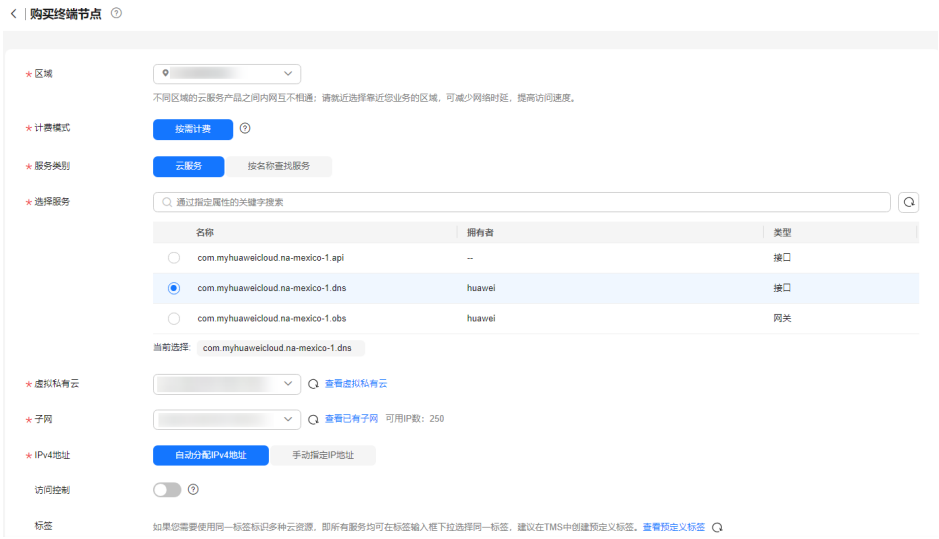
终端节点要连接的终端节点服务已经存在。

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“购买终端节点”。
   进入“购买终端节点”页面。

图 5-3 购买终端节点（云服务-接口型）



5. 根据界面提示配置参数。

表 5-1 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。
计费方式	按需计费是后付费模式，按终端节点的实际使用时长计费，可以随时开通/删除终端节点。 仅支持按需计费。
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”。

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。 此处选择DNS服务实例，即“com.myhuaweicloud.na-mexico-1.dns”。
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。
节点IP	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。 终端节点的私网IP。可选择“自动分配”或“手动分配”。
访问控制	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。 用于设置允许访问终端节点的IP地址或网段。 ● 开启：只允许白名单列表中的IP地址或网段访问终端节点。 ● 关闭：允许任何IP地址或网段访问终端节点。
白名单	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。 用于设置允许访问的IP地址或网段，最多支持添加20个记录。
策略	双端固定策略，即设置VPC终端节点策略与桶策略，可以对OBS的资源提供VPC粒度的权限控制。 当终端节点连接的终端节点服务开启“访问控制策略”时，支持配置终端节点策略。 ● 设置VPC终端节点策略可以限制VPC中的服务器（ECS/CCE/BMS）访问OBS中的特定资源。 ● 设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问。

参数	说明
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20个标签。 标签的命名规则请参考**表5-2**。 **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。 预定义标签的详细内容，请参见**预定义标签简介**。 如您的组织已经设定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。

表 5-2 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36个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。
值	• 不能为空。 • 长度不超过43个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。

6. 参数配置完成，单击“立即购买”，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“com.myhuaweicloud.na-mexico-1.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 5-4 终端节点详情

5.3 步骤二：购买连接 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，需要购买连接OBS服务的终端节点。

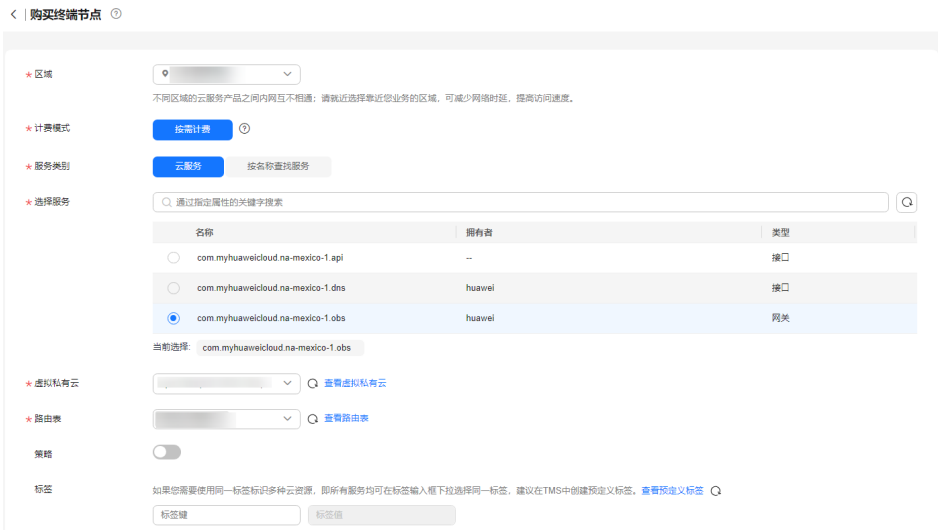
前提条件

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“购买终端节点”。
   进入“购买终端节点”页面。

图 5-5 购买终端节点（云服务-网关型）



5. 根据界面提示配置参数。

表 5-3 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。

参数	说明
计费方式	按需计费是后付费模式，按终端节点的实际使用时长计费，可以随时开通/删除终端节点。 仅支持按需计费。
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，即“com.myhuaweicloud.na-mexico-1.obs”。
虚拟私有云	选择终端节点所属的虚拟私有云。
路由表	当创建连接“网关”类型终端节点服务的终端节点时，则会出现该参数。 **说明** 该参数仅在开放区域可见。 建议选择所有路由表，否则可能导致网络无法访问。 根据实际需求选择终端节点所属的虚拟私有云的路由表。 添加路由的详细操作请参考《虚拟私有云用户指南》中的“**添加自定义路由**”。
策略	双端固定策略，即设置VPC终端节点策略与桶策略，可以对OBS的资源提供VPC粒度的权限控制。 当终端节点连接的终端节点服务开启“访问控制策略”时，支持配置终端节点策略。 • 设置VPC终端节点策略可以限制VPC中的服务器（ECS/CCE/BMS）访问OBS中的特定资源。 • 设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问。
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20个标签。 标签的命名规则请参考**表5-4**。 **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。 预定义标签的详细内容，请参见**预定义标签简介**。 如您的组织已经设定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。

表 5-4 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36个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。
值	• 不能为空。 • 长度不超过43个字符。 • 取值只能包含大写字母、小写字母、数字、中划线、下划线、以及从\u4e00到\u9fff的Unicode字符。

6. 参数配置完成，单击“立即购买”，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“com.myhuaweicloud.na-mexico-1.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。

图 5-6 终端节点详情

5.4 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**提交工单**或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**创建VPN网关**。

- 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**提交工单**或联系对象存储服务的客户经理获取。

  开通云专线，请参考**开通云专线**。

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”。
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：

   方式1：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;};
   };
   ```

   方式2：在/etc/named.rfc1912.zones文件中增加如下内容，“forwarders”为连接DNS服务的终端节点的IP地址。

   以“拉美-墨西哥城一”的OBS的Endpoint地址和所在集群地址为例：

   ```
   zone "obs.na-mexico-1.myhuaweicloud.com" {
   type forward;
   forward only;
   forwarders{ xx.xx.xx.xx;};
   };
   zone "obs.lz01.na-mexico-1.myhuaweicloud.com" {
   type forward;
   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。
   - “obs.na-mexico-1.myhuaweicloud.com”表示OBS在拉美-墨西哥城一区域的终端节点。
   - “obs.lz01.na-mexico-1.myhuaweicloud.com”表示OBS桶所在集群lz01的地址信息。
   - 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 端口号
   ```

   此处的“bucketname.endpoint”表示OBS桶的访问域名，可以在OBS控制台查看桶信息获取，详细请参见**查看桶的信息**。

   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）。
   - 端口号：业务端口，80或443。

   例如，**telnet bucketname.obs.na-mexico-1.myhuaweicloud.com 80**或者**telnet bucketname.obs.na-mexico-1.myhuaweicloud.com 443**

   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。

