VPC 终端节点

用户指南

文档版本 07

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 终端节点服务管理 1
1.1 终端节点服务简介 1
1.2 创建终端节点服务 3
1.3 查看终端节点服务 7
1.4 删除终端节点服务 9
1.5 管理终端节点服务的连接审批 10
1.6 管理终端节点服务的白名单 10
1.7 管理终端节点服务的端口映射 12
1.8 管理终端节点服务的标签 14
2 终端节点管理 16
2.1 终端节点简介 16
2.2 购买终端节点 17
2.3 查询并访问终端节点 24
2.4 删除终端节点 27
2.5 设置终端节点的访问控制 28
2.6 管理终端节点的标签 29
3 访问 OBS 32
4 双端固定 35
4.1 双端固定简介 35
4.2 配置双端固定 35
5 审计 40
5.1 支持审计的关键操作 40
5.2 查看审计日志 41
6 权限管理 42
6.1 创建用户并授权使用 VPCEP 42
7 关于配额 44
A 修订记录 46

1 终端节点服务管理

1.1 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。

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。

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。

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1-1**所示。

表 1-1 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。当“网络类型”选择“IPv4”时可以选择裸金属服务器。 • 一个终端节点服务仅支持对应一个后端资源实例。
查看终端节点服务	介绍如何查看终端节点服务的详细信息。	无
删除终端节点服务	介绍如何删除创建的终端节点服务。	• 终端节点服务删除后无法恢复，请谨慎操作。 • 仅支持删除用户创建的私有服务的终端节点服务。 • 当终端节点服务被“已接受”或者“创建中”状态的终端节点连接时，无法删除。
管理终端节点服务的连接审批	介绍如何设置终端节点服务的连接审批功能，用于控制是否允许终端节点连接终端节点服务。	仅当开启了终端节点服务的“连接审批”功能时，才支持设置是否允许终端节点连接此终端节点服务。
管理终端节点服务的白名单	介绍如何管理终端节点服务的白名单，用于控制跨租户的终端节点连接终端节点服务。	• 终端节点需要与终端节点服务位于同一区域。 • 在设置前，需要获取终端节点所属的账号ID。
管理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。

操作	说明	使用限制
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。

1.2 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。当“网络类型”选择“IPv4”时可以选择裸金属服务器。
- 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。

图 1-1 创建终端节点服务

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 1-2 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。 长度不超过16个字符，允许输入大小写字母、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，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。
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。
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20个标签。 标签的命名规则请参考**表1-3**。 **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。 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 1-3 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。

图 1-2 终端节点服务列表

1.3 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。

图 1-3 终端节点服务详情

终端节点服务详情中涉及的参数如表1-4所示。

表 1-4 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	模式	终端节点服务的模式。
基本信息	网络类型	终端节点服务的网络类型。
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。
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	终端节点创建者的账号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	授权账号ID	连接访问终端节点的授权账号ID或者*。 若“授权账号ID”列为“*”，表示所有用户均可访问该终端节点服务。
权限管理	操作	对连接访问终端节点的授权账号进行操作，支持将授权账号从白名单中删除。
端口映射	协议	终端节点服务与终端节点进行通信支持的协议。
端口映射	服务端口	终端节点服务提供服务的端口。

页签	参数名称	说明
端口映射	终端端口	终端节点访问终端节点服务的端口。
端口映射	操作	对已添加的端口映射信息进行操作。
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。

1.4 删除终端节点服务

操作场景

本节介绍如何删除终端节点服务。

说明

终端节点服务删除后无法恢复，请谨慎操作。

约束与限制

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

操作步骤

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

图 1-4 删除终端节点服务

5. 在“删除终端节点服务”弹框中，单击“确定”，删除终端节点服务。

1.5 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

- 已购买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。

图 1-5 连接管理

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。

1.6 管理终端节点服务的白名单

操作场景

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

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

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

- 如果某一账号未包含在终端节点服务的白名单中，则无法通过该账号创建连接终端节点服务的终端节点。

本节介绍添加或删除终端节点服务白名单记录的操作指导。

约束与限制

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

添加白名单

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

图 1-6 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。

删除白名单

1. 登录管理控制台。
2. 在管理控制台左上角单击“ ”图标，选择区域和项目。

3. 单击“服务列表”中的“网络 > VPC终端节点”，进入“终端节点”页面。
4. 在左侧导航栏选择“VPC终端节点 > 终端节点服务”。
5. 在“终端节点服务”页面，单击需要删除白名单的终端节点服务名称。
6. 在该终端节点服务的“权限管理”页签，单击对应授权账号ID“操作”列下的“删除”，即可删除对应的白名单记录。

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

1.7 管理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，您可以添加端口映射，或者修改、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。

添加端口映射

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。

   进入终端节点服务基本信息页面。
6. 选择“端口映射”，单击“添加端口映射”。

   根据界面提示输入相关参数。

   图 1-7 添加端口映射

7. 单击“确定”。

修改端口映射

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。
   进入终端节点服务基本信息页面。
6. 选择“端口映射”页面，在目标端口映射所在行的操作列单击“修改”。
   根据界面提示输入相关参数。

   图 1-8 修改端口映射

7. 单击“确定”。

删除端口映射

终端节点服务只有一个端口映射时不允许删除。

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。
   进入终端节点服务基本信息页面。
6. 选择“端口映射”页面，在目标端口映射所在行的操作列单击“删除”。

   图 1-9 删除端口映射

7. 确认待删除的端口映射信息，单击“确定”。

1.8 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20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。

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。

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1-5**所示。

表 1-5 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。

参数	规则
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。

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 。

2 终端节点管理

2.1 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，通过购买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。

- 根据终端节点访问的终端节点服务的类型，终端节点分为接口终端节点、网关终端节点。
  - **接口终端节点：**指访问“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。
  - **网关终端节点：**指访问“网关”型终端节点服务的终端节点，是作为一个网关，在其上配置路由，用于将流量指向网关型终端节点服务。
- 终端节点的资源实例类型分为专业型、基础型，不同实例类型的特点如下：
  - **专业型：**新上线终端节点实例类型，目前已在**华东一区域**公测。单实例带宽规格最大支持10Gbps、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。

本章节介绍如何购买并管理终端节点，如表2-1所示。

表 2-1 终端节点管理说明

操作	说明	使用限制
购买终端节点	介绍如何购买连接终端节点服务的终端节点。	• 终端节点属于区域级资源，在购买时需要设置区域和项目。 • 每个租户支持购买50个终端节点。 • 购买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。 • 终端节点按购买时长计费。

操作	说明	使用限制
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： ● 基础型：3000 ● 专业型：1000000
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。
设置终端节点的访问控制	介绍如何开启终端节点的访问控制功能，并通过白名单设置允许访问终端节点的IP地址或网段。	● 只有连接“接口”型终端节点服务的终端节点支持访问控制功能。 ● 如果关闭访问控制功能，表示允许任何IP访问终端节点。
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。

2.2 购买终端节点

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，通过购买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。

说明

仅“拉美-墨西哥城一”、“拉美-圣保罗一”和“拉美-圣地亚哥”区域支持购买访问“网关”型终端节点服务的终端节点。

您可以根据实际需求，购买连接不同终端节点服务类型的终端节点：

- 购买连接“接口”型终端节点服务的终端节点
- 购买连接“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，在购买时需要设置区域和项目。
- 每个租户支持购买50个终端节点。

- 购买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。
- 终端节点按购买时长计费。

购买连接“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“购买终端节点”，进入“购买终端节点”页面。
5. 在“购买终端节点”页面，根据提示配置参数。

图 2-1 购买终端节点（云服务-接口型）

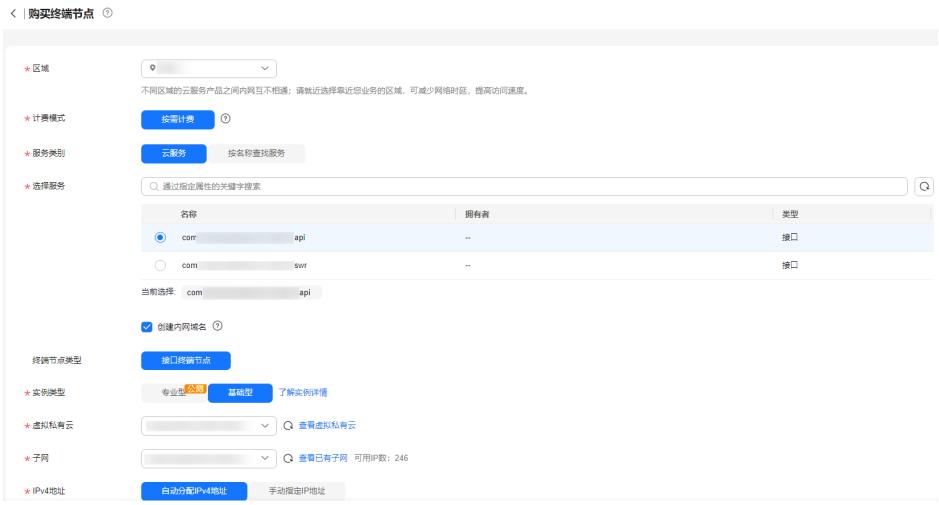


图 2-2 购买终端节点（按名称查找服务-接口型）

表 2-2 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。
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”。
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。
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10Gbps、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。

参数	说明
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	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。
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“选择服务”的“类型”为“接口”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“选择服务”的“类型”为“接口”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“选择服务”的“类型”为“接口”时，打开“访问控制”开关，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。 请输入允许访问的IP地址或网段，不支持格式：0.0.0.0和x.x.x.x/0。
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。 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	终端节点服务描述内容。

表 2-3 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”。

购买连接“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“购买终端节点”，进入“购买终端节点”页面。
5. 在“购买终端节点”页面，根据提示配置参数。

图 2-3 购买终端节点（云服务-网关型）

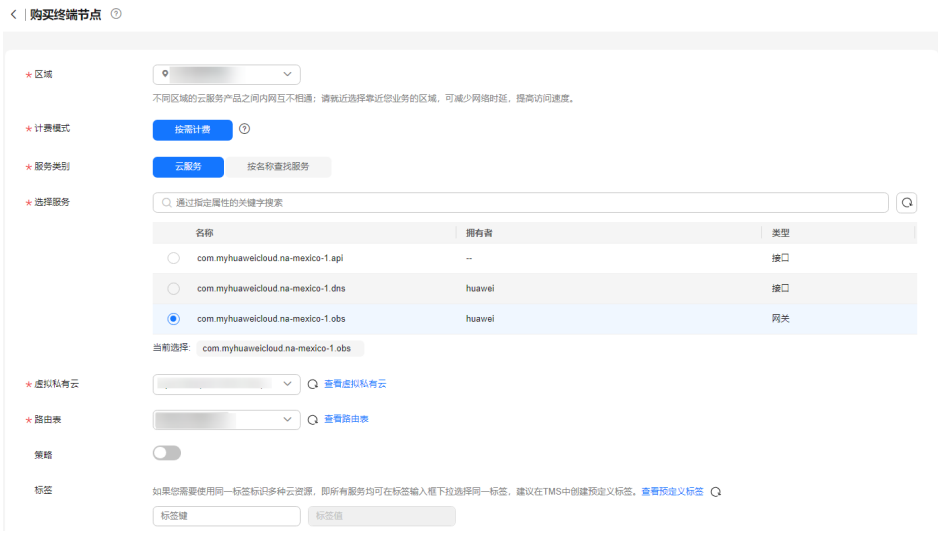


表 2-4 终端节点配置参数

参数	说明
区域	终端节点所在区域。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	仅由系统配置的云服务类别的终端节点服务包括“网关”型。 选择“云服务”。
选择服务	若“服务类别”选择“云服务”，则会出现该参数。 在列表中，选择“类型”列为“网关”类型的终端节点服务。 终端节点服务实例已由运维人员预先创建完成，您可以直接使用。
虚拟私有云	选择终端节点所属的虚拟私有云。
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**”。

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。 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 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”。

2.3 查询并访问终端节点

操作场景

当终端节点购买完成时，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：

- 基础型：3000
- 专业型：1000000

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，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）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 2-4 终端节点详情（接口）

图 2-5 终端节点详情（网关）

表 2-6 参数说明

页签	参数名称	说明
基本信息	ID	终端节点ID。
基本信息	虚拟私有云	终端节点所属VPC。
基本信息	付费方	终端节点的付费方。
基本信息	终端节点服务名称	终端节点所连接的终端节点服务名称。
基本信息	内网域名	终端节点的内网域名。
基本信息	状态	终端节点状态。
基本信息	类型	终端节点所连接的终端节点服务类型。
基本信息	实例类型	终端节点的实例类型。
基本信息	IPv4地址	终端节点的IPv4地址。
基本信息	IPv6地址	终端节点的IPv6地址。
基本信息	创建时间	终端节点的创建时间。
基本信息	访问控制	用于开启或关闭是否通过白名单控制访问终端节点的IP。 ● 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。 **说明** 仅在连接“接口”型终端节点服务的终端节点显示。

页签	参数名称	说明
访问控制	白名单地址	允许访问终端节点的IP地址或网段。 **说明** “访问控制”页签仅在连接“接口”型终端节点服务的终端节点显示。
访问控制	操作	对允许访问终端节点的白名单地址进行操作，仅支持“删除”白名单地址。
路由表	名称	路由表的名称。 **说明** “路由表”页签仅在开放区域可见，且仅在连接“网关”型终端节点服务的终端节点显示。
路由表	虚拟私有云	路由表所属VPC。
路由表	类型	路由表的类型，包括“默认路由表”和“自定义路由表”。
路由表	关联子网	路由表的关联子网数量。
路由表	操作	对终端节点路由表进行操作，可选择“解绑”或“绑定”路由表。 **说明** 当终端节点仅绑定一个路由表时，不支持“解绑”操作。
标签	键	终端节点的标签“键”。
标签	值	终端节点的标签“值”。
标签	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）

当购买终端节点时勾选了“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. 将鼠标悬浮于页面左侧的“ ”，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“域名解析 > 内网解析”。
   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*

2.4 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。

图 2-6 删除终端节点

6. 在“删除终端节点”弹框中，单击“确定”，删除终端节点。

2.5 设置终端节点的访问控制

操作场景

终端节点的访问控制功能支持通过白名单设置允许访问终端节点的IP地址或网段。在购买终端节点时以及购买完成后，均可以开启或关闭终端节点的访问控制功能，也可以添加或删除白名单。

说明

- 只有连接“接口”型终端节点服务的终端节点支持访问控制功能。
- 如果关闭访问控制功能，表示允许任何IP访问终端节点。

购买终端节点时，如何设置访问控制和白名单，请参见**购买终端节点**。

本节介绍在终端节点购买完成后，如何开启并设置访问控制功能。

约束与限制

- 只有连接“接口”型终端节点服务的终端节点支持访问控制功能。
- 如果关闭访问控制功能，表示允许任何IP访问终端节点。

开启访问控制并添加白名单

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. 在终端节点列表中，单击终端节点ID，进入终端节点“基本信息”页签。
5. 在“基本信息”页签，开启“访问控制”。
6. 在“访问控制”页签，单击“添加白名单”。

图 2-7 添加终端节点白名单

7. 在“白名单地址”列，输入允许访问终端节点的IP地址或网段。

   说明

   最多支持添加20个白名单地址。

   输入* 表示全放通，本账号默认在白名单中。

8. 单击“确定”，完成白名单地址的添加。

删除白名单地址

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ID，进入终端节点“基本信息”页签。
5. 选择“访问控制”页签，显示终端节点的白名单列表。
6. 在白名单列表中，单击待删除白名单地址“操作”列的“删除”，删除该地址。

   如果要删除多个白名单地址，可以勾选待删除的白名单地址，单击上方的“删除”。
7. 在“删除白名单”弹框中单击“确定”，删除终端节点的白名单地址。

2.6 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20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。

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。

添加标签

本操作用于为已购买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ID，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2-7**所示。

   表 2-7 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。

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ID，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。

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. 在终端节点列表中，单击终端节点ID，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。

3 访问 OBS

操作场景

虚拟专用网络、云专线线下节点通过终端节点高速访问OBS。

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。

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。

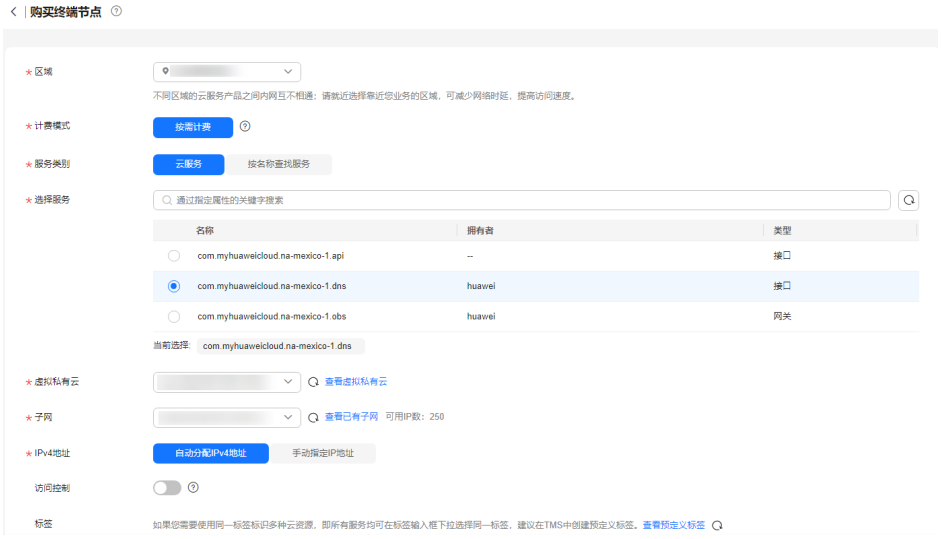
  创建虚拟专用网络，请参考**创建VPN网关**。
- 专线虚拟网关允许访问的VPC子网网段，需要包含OBS的网段，详细请**提交工单**或联系对象存储服务的客户经理获取。

  开通云专线，请参考**开通云专线**。

操作步骤

1. 在管理控制台左上角单击 图标，选择区域和项目。
2. 在“服务列表”中，选择“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”。
4. 在终端节点界面，单击“购买终端节点”，创建连接DNS服务的终端节点。
5. 选择“云服务 > com.myhuaweicloud.na-mexico-1.dns”。
6. 根据界面提示配置参数。

图 3-1 购买终端节点（云服务-接口型）



7. 选择“立即购买 > 提交”，完成创建。
8. 查看连接DNS服务的终端节点创建完成后返回的节点IP。
9. 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为步骤9中的节点IP。

10. 配置线下节点到专线网关或VPN网关的DNS路由。

    DNS终端节点IP的IP地址为xx.xx.xx.xx，所以需要将节点访问DNS的流量指向线下专线网关或VPN网关，然后走专线或VPN访问OBS。在线下节点配置永久路由，指定访问OBS的流量下一跳为线下专线网关或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为步骤9中的节点IP。
    - xxx.xxx.xxx.xxx为线下专线网关或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。

11. 参考步骤5到9，创建连接OBS服务的终端节点。

    说明

    线下节点只能访问终端节点所在区域对应的OBS域名地址。

12. 配置线下节点到专线网关或VPN网关的OBS路由。

    线上OBS的IP地址网段为100.125.0.0/16，所以需要将节点访问OBS的流量指向线下专线网关或VPN网关，然后走专线或VPN访问OBS。

    在线下节点配置永久路由，指定访问OBS的流量下一跳为线下专线网关或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

    - 如果线下节点和线下专线网关或VPN网关网络不通，需要预先打通之间的网络。
    - 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 双端固定

4.1 双端固定简介

操作场景

使用“双端固定”特性，即同时设置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。

一方面，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；另一方面，设置桶策略可以限定OBS中的桶被特定VPC中的服务器访问，从而在请求来源和被访问资源两个角度保障了安全性。

背景信息

VPC终端节点访问控制遵循最小权限原则，如果终端节点策略没有显式“Allow（允许）”，则默认“Deny（拒绝）”。在购买VPC终端节点时，系统将会为该终端节点生成一个默认策略，该策略允许对OBS的完全访问，您可以在创建VPC终端节点时修改默认策略，还可以在创建完成后，根据需要随时调整VPC终端节点策略。VPC终端节点策略的设置规则参见**IAM策略中的Statement标签**。

说明

- VPC终端节点策略与IAM权限存在部分差异：VPC终端节点策略中不含“Condition”标签。
- OBS双端固定的终端节点服务名称：
  - “拉美-墨西哥城一”、“拉美-圣保罗一”和“拉美-圣地亚哥”区域可选择格式为“com.myhuaweicloud.xxx.obs”的终端节点服务。
  - 其余地区endpoint请**提交工单**咨询技术支持。

4.2 配置双端固定

配置示例一：只配置 VPC 终端节点策略

场景描述：

只允许VPC1内的服务器下载账号A的桶mybucket中的对象。

其中VPC1的ID为：4dad1f75-0361-4aa4-ac75-1ffdda3a0fec，账号A的账号ID为：783fc6652cf246c096ea836694f71855。

配置方法：

配置VPC1的终端节点策略如下：

入口：服务列表 > VPC终端节点 > 单击对应VPC终端节点ID > 策略 > 编辑

```
[
  {
    "Action": [
      "obs:object:GetObject"
    ],
    "Resource": [
      "obs:*:783fc6652cf246c096ea836694f71855:object:mybucket/*"
    ],
    "Effect": "Allow"
  }
]
```

配置示例二：只配置 VPC 终端节点策略，禁止指定资源下载

场景描述：

除了账号A的桶mybucket中的对象外，允许VPC1内的服务器下载账号A名下所有其他桶的桶内对象。

其中账号A的账号ID为：783fc6652cf246c096ea836694f71855。

配置方法：

配置VPC1的终端节点策略如下：

入口：服务列表 > VPC终端节点 > 单击对应VPC终端节点ID > 策略 > 编辑

```
[
  {
    "Action": [
      "obs:object:GetObject"
    ],
    "Resource": [
      "obs:*:783fc6652cf246c096ea836694f71855:object:*/*"
    ],
    "Effect": "Allow"
  },
  {
    "Action": [
      "obs:object:GetObject"
    ],
    "Resource": [
      "obs:*:783fc6652cf246c096ea836694f71855:object:mybucket/*"
    ],
    "Effect": "Deny"
  }
]
```

配置示例三：同时配置 VPC 终端节点策略与桶策略

场景描述：

只允许VPC1内的服务器上传/下载账号A的桶mybucket中的对象，并且只允许桶mybucket中的对象被VPC1内的服务器上传/下载。

其中VPC1的ID为：4dad1f75-0361-4aa4-ac75-1ffdda3a0fec，账号A的账号ID为：783fc6652cf246c096ea836694f71855。

配置方法：

1. 配置VPC1的终端节点策略如下：

   入口：服务列表 > VPC终端节点 > 单击对应VPC终端节点ID > 策略 > 编辑

```
[
  {
    "Action": [
       "obs:object:GetObject",
    "obs:object:PutObject"
    ],
    "Resource": [
       "obs:*:783fc6652cf246c096ea836694f71855:object:mybucket/*"
    ],
    "Effect": "Allow"
  }
]
```

2. 配置桶mybucket的桶策略如下：

   配置方法请参见**自定义创建桶策略（JSON视图）**。

   两个桶策略：

   - 桶策略1：允许VPC1内的服务器上传/下载账号A的桶mybucket中的对象。

     其中*statementId*可自定义，*domainId*和*userId*需要设置为允许上传下载的账号ID和用户ID。相关说明请参见**桶策略**。

```
{
  "Statement": [
    {
      "Sid": "statementId",
      "Effect": "Allow",
      "Principal": {
        "ID": ["domain/domainId:user/userId"]
      },
      "Action": ["GetObject", "PutObject"],
      "Resource": ["mybucket/*"],
      "Condition": {
        "StringEquals": {
          "SourceVpc": ["4dad1f75-0361-4aa4-ac75-1ffdda3a0fec"]
        }
      }
    }
  ]
}
```

   - 桶策略2：除了VPC1外的其他VPC内的服务器均不能操作账号A的桶mybucket及桶中的对象。

     其中*DenyReqNotFromVpc*可自定义。

```
{
  "Statement": [
    {
      "Sid": "DenyReqNotFromVpc",
      "Effect": "Deny",
      "Principal": {
        "ID": ["*"]
      },
      "Action": "*",
      "Resource": ["mybucket", "mybucket/*"],
      "Condition": {
        "StringNotEqual": {
          "SourceVpc": ["4dad1f75-0361-4aa4-ac75-1ffdda3a0fec"]
        }
      }
    }
```

```
    ]
}
```

说明

设置上述桶策略后，被授权的IAM用户可以正常通过SDK或API进行上传下载操作。如果希望在控制台或OBS Browser+上进行上传下载，还需要在IAM权限中额外配置obs:bucket:ListAllMyBuckets和obs:bucket:ListBucket权限，否则登录控制台和OBS Browser+时会报错，无法看到桶和桶内对象。

配置示例四：同时配置 VPC 终端节点策略与桶策略后，再授权其他云服务访问桶

场景描述：

当同时设置了VPC1的终端节点策略与账号A的桶mybucket的桶策略后，由于双端固定的限制，其它云服务包括OBS就无法访问桶mybucket。若想要授权其它云服务能够访问桶mybucket，可以通过委托授权的方式。

其中VPC1的ID为：4dad1f75-0361-4aa4-ac75-1ffdda3a0fec，账号A的账号ID为：783fc6652cf246c096ea836694f71855。

配置方法：

1. 配置VPC1的终端节点策略如下：

   只允许VPC1内的服务器上传/下载账号账号A的桶mybucket中的对象。

   入口：服务列表 > VPC终端节点 > 单击对应VPC终端节点ID > 策略 > 编辑

   ```
   [
     {
       "Action": [
           "obs:object:GetObject",
       "obs:object:PutObject"
       ],
       "Resource": [
           "obs:*:783fc6652cf246c096ea836694f71855:object:mybucket/*"
       ],
       "Effect": "Allow"
     }
   ]
   ```

2. **创建IAM委托**，委托其它云服务访问桶mybucket。例如，委托OBS，绑定系统策略OBS FullAccess，也可以创建自定义策略并绑定该委托。

3. 配置桶mybucket的桶策略如下：

   只允许桶mybucket中的对象被VPC1内的服务器或者委托名为testAgencyName所对应授权的云服务访问桶mybucket中的对象。其中委托名以步骤二实际创建的IAM委托名称为准。

   ```
   {
     "Statement": [
       {
           "Effect": "Allow",
           "Principal": {"ID": ["*"]},
           "Action": ["*"],
           "Resource": ["mybucket/*"],
           "Condition": {
               "StringEquals": {
                   "SourceVpc": ["4dad1f75-0361-4aa4-ac75-1ffdda3a0fec"]
               }
           }
       },
       {
           "Effect": "Allow",
           "Principal": {"ID": ["*"]},
           "Action": ["*"],
   ```

```
            "Resource": ["mybucket/*"],
            "Condition": {
                "StringEquals": {
                    "ServiceAgency": ["testAgencyName"]
                }
            }
        }
    ]
}
```

同时，桶策略也可按如下配置达到同样的效果：

```
{
    "Statement": [
        {
            "Effect": "Deny",
            "Principal": {"ID": ["*"]},
            "Action": ["*"],
            "Resource": ["mybucket/*"],
            "Condition": {
                "StringNotEquals": {
                    "SourceVpc": ["4dad1f75-0361-4aa4-ac75-1ffdda3a0fec"],
                    "ServiceAgency": ["testAgencyName"]
                }
            }
        }
    ]
}
```


5 审计

5.1 支持审计的关键操作

操作场景

云平台提供了云审计服务。通过云审计服务，您可以记录与VPCEP服务相关的操作事件，便于日后的查询、审计和回溯。

前提条件

已开通云审计服务。

支持审计的关键操作列表

表 5-1 云审计支持的 VPCEP 服务操作列表

操作名称	资源类型	事件名称
创建终端节点服务	EndpointService	createEndpointService
修改终端节点服务	EndpointService	modifyEndpointService
删除终端节点服务	EndpointService	deleteEndpointService
拒绝/接受终端节点服务连接请求	EndpointService	serviceConnectionsAction
添加/移除终端节点服务的白名单	EndpointService	servicePermissionAction
创建终端节点	vpcEndpoint	createEndpoint
修改终端节点	vpcEndpoint	modifyEndpoint
删除终端节点	vpcEndpoint	deleteEndpoint
修改终端节点路由	vpcEndpoint	modifyEndpointRouteTables

操作名称	资源类型	事件名称
批量修改资源标签	vpcEndpointOrService	batchModifyTag

5.2 查看审计日志

操作场景

在您开启了云审计服务后，系统开始记录云服务资源的操作。云审计服务管理控制台保存最近7天的操作记录。

本节介绍如何在云审计服务管理控制台查看或导出最近7天的操作记录。

操作步骤

1. 登录管理控制台。
2. 在管理控制台左上角单击 ，选择区域和项目。
3. 在页面左上角单击 图标，打开服务列表，选择“管理与监管 > 云审计服务”，进入云审计服务信息页面。
4. 单击左侧导航树的“事件列表”，进入事件列表信息页面。
5. 事件列表支持通过筛选来查询对应的操作事件。当前事件列表支持不同维度的组合查询，详细信息如下：
   - 事件类型：可选项为“管理事件”、“数据事件”。
   - 事件来源、资源类型和筛选类型。

     在下拉框中选择查询条件。

     其中筛选类型选择事件名称时，还需选择某个具体的事件名称。

     选择资源ID时，还需选择或者手动输入某个具体的资源ID。

     选择资源名称时，还需选择或手动输入某个具体的资源名称。
   - 操作用户：在下拉框中选择某一具体的操作用户，此操作用户指用户级别，而非租户级别。
   - 事件级别：可选项为“所有事件级别”、“Normal”、“Warning”、“Incident”，只可选择其中一项。
   - 时间范围：可选择查询“最近1小时”、“最近1天”、“最近1周”以及最近1周内自定义时间段的操作事件。
6. 在需要查看的记录左侧，单击箭头展开该记录的详细信息。
7. 在需要查看的记录右侧，单击“查看事件”，弹出的窗口显示该操作事件结构的详细信息。

6 权限管理

6.1 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，在您的华为账号中，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、高效的其他华为账号或者云服务，这些账号或者云服务可以根据权限进行代运维。

如果华为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。

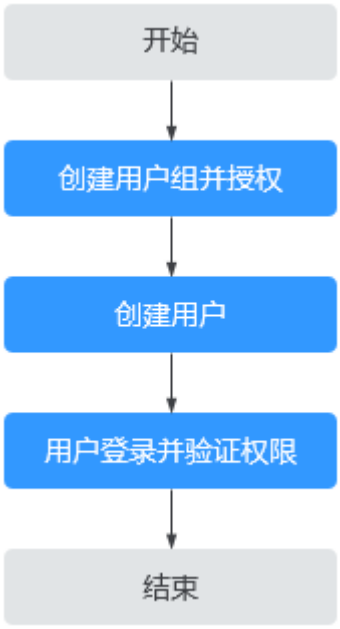
本章节为您介绍对用户授权的方法，操作流程如**图6-1**所示。

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**VPCEP系统权限**。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**系统权限**。

示例流程

图 6-1 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“购买终端节点”，尝试购买终端节点，如果可以购买，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。

7 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. 在页面右上角，选择“资源 > 我的配额”。
   系统进入“服务配额”页面。

   图 7-1 我的配额

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。

图 7-2 我的配额

3. 在页面右上角，单击“申请扩大配额”。

图 7-3 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”。

A 修订记录

版本日期	变更说明
2024-05-10	第十次正式发布。 增加“专业型”终端节点实例类型。
2023-02-16	第九次正式发布。 • 优化快速入门：**配置访问OBS服务内网地址的终端节点**。 • 优化用户指南：**访问OBS**。 • 优化最佳实践：**通过VPC终端节点和云专线服务实现云下IDC访问云上服务**。
2022-09-30	第八次正式发布。 • 优化快速入门：**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）**、**配置访问OBS服务内网地址的终端节点**。 • 优化用户指南：**访问OBS**。
2021-05-08	第七次正式发布。 支持为终端节点添加60条白名单记录，涉及： • **终端节点简介** • **购买终端节点** • **设置终端节点的访问控制**
2020-11-13	第六次正式发布。 新增 • **终端节点服务简介** • **管理终端节点服务的标签** • **终端节点简介** • **设置终端节点的访问控制** • **管理终端节点的标签**

版本日期	变更说明
2019-12-30	第五次正式发布。 更新用户指南：“权限管理”。
2019-11-30	第四次正式发布。 全文更新截图。
2019-07-10	第三次正式发布。 ● 全文更新截图。 ● 新增“权限管理”内容。
2019-02-18	第二次正式发布。 增加配额调整内容。
2018-11-30	第一次正式发布。