

ALIBABA CLOUD

# 阿里云

私网连接  
快速入门

文档版本：20220329

 阿里云

## 法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

# 通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <code>Instance_ID</code>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

# 目录

1.同账号VPC间的私网访问服务	05
2.跨账号VPC间的私网访问服务	13

# 1.同账号VPC间的私网访问服务

本文指导您使用私网连接（PrivateLink）服务将一个专有网络VPC（Virtual Private Cloud）内部署的传统型负载均衡CLB（Classic Load Balancer）共享给同账号下的另外一个VPC访问。

## 背景信息

VPC是您独有的云上私有网络，不同VPC之间完全隔离。您可以通过私网连接建立VPC与阿里云服务之间安全稳定的私有连接，简化网络架构，避免通过公网访问服务带来的潜在安全风险。

通过私网连接实现私网访问，您需要创建终端节点服务和终端节点。

- 终端节点服务

终端节点服务是可以与其他VPC的终端节点建立私网连接服务，由服务提供方创建和管理。

- 终端节点

终端节点可以与终端节点服务相关联，以建立通过VPC私网访问外部服务的网络连接。终端节点由服务使用方创建和管理。

相关主体	相关组件
服务提供方	创建和管理终端节点服务。
服务使用方	创建和管理终端节点。

 **说明** 目前，仅部分地域支持私网连接。更多信息，请参见[支持私网连接的地域和可用区](#)。

## 场景示例

本文以下图场景为例。某公司使用阿里云账号A在德国（法兰克福）地域创建了VPC1和VPC2，并且VPC2中的ECS2实例和ECS3实例部署了应用服务。现因业务发展，VPC1需要通过私网访问VPC2中的服务。

您可以在VPC2中创建支持私网连接的

CLB

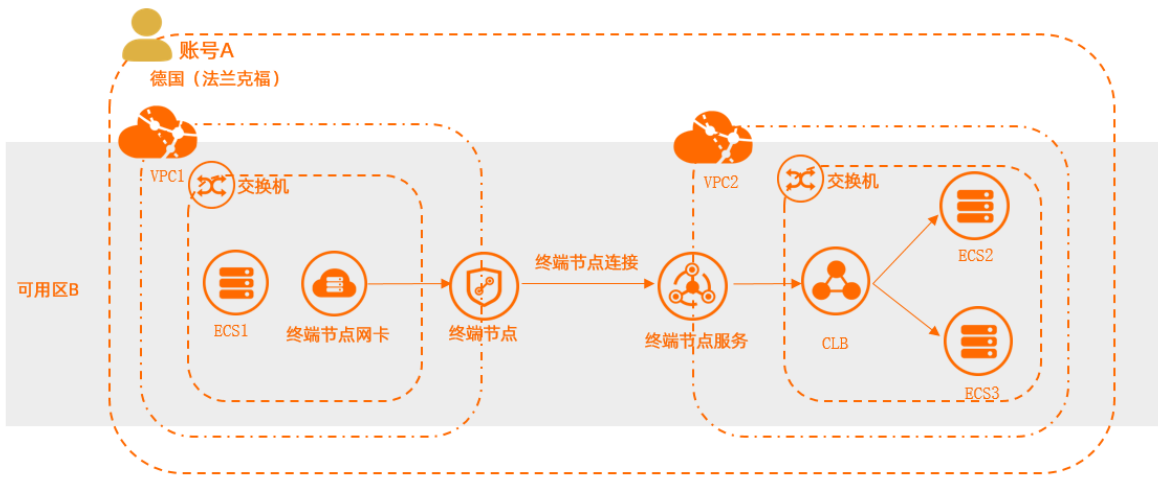
实例，将ECS2实例和ECS3实例添加为

CLB

实例的后端服务器，然后创建终端节点服务，将

CLB

实例添加为服务资源。在VPC1中创建终端节点。创建成功后，终端节点与终端节点服务建立连接且状态正常时，VPC1中的ECS1即可私网访问VPC2中的服务。



本文中2个VPC网络规划如下表所示，在您规划网络时请确保要互通的网段没有重叠。

属性	VPC1	VPC2
网络实例所属地域	德国（法兰克福）	德国（法兰克福）
网络实例的网段规划	<ul style="list-style-type: none"><li>VPC网段：10.10.1.0/16</li><li>交换机网段：10.0.0.0/24</li></ul>	<ul style="list-style-type: none"><li>VPC网段：192.168.2.0/16</li><li>交换机网段：192.168.24.0/24</li></ul>
网络实际交换的可用区	交换机位于可用区B	交换机位于可用区B
服务器IP地址	ECS1 IP地址：10.0.0.182	<ul style="list-style-type: none"><li>ECS2 IP地址：192.168.20.200</li><li>ECS3 IP地址：10.0.0.2</li></ul>

使用限制

- VPC2中的CLB  
服务资源必须是按量付费的私网CLB实例，只有按量付费的私网CLB实例才支持私网连接。
- VPC1中的终端节点、VPC2中的终端节点服务及CLB  
服务资源必须在同一地域的同一可用区内。

前提条件

- 您已经在德国（法兰克福）地域创建了VPC1和VPC2，并且在VPC1和VPC2中分别创建了一个交换机。具体操作，请参见[创建专有网络和交换机](#)。
- 您已在VPC1中创建了ECS1实例，在VPC2中创建了ECS2和ECS3实例，ECS2和ECS3部署了应用服务。具体

- 操作，请参见[使用向导创建实例](#)。
- 您已经在VPC1创建了安全组。具体操作，请参见[创建安全组](#)。

配置步骤



步骤一：创建支持私网连接功能的CLB实例

1. 登录[传统型负载均衡CLB控制台](#)。
2. 在实例管理页面，单击创建传统型负载均衡。
3. 在购买页面，根据以下信息配置

CLB	
实例，然后单击立即购买完成支付。	
配置	说明
付费模式	选择一种付费模式。本文选择按量付费。
地域和可用区	选择 CLB 实例所属的地域和可用区，确保 CLB 实例的地域和后端添加的ECS的地域相同。本文地域选择德国（法兰克福），可用区选择法兰克福 可用区B。
可用区类型	显示所选地域的可用区类型。本文选择多可用区。
备可用区	选择 CLB 实例的备可用区。备可用区默认不承载流量，主可用区不可用时才承载流量。本文选择欧洲中部1 可用区A。
实例名称	自定义 CLB 的实例名称。 长度限制为1~80个字符，允许包含中文、字母、数字、短划线（-）、正斜线（/）、半角句号（.）和下划线（_）等字符。
实例规格	选择一个实例规格。不同的实例规格所提供的性能指标不同。本文选择简约型I（slb.s1.small）。

配置	说明
实例类型	根据业务场景选择配置对外公开或对内私有的CLB实例。本文选择私网。
网络类型	选择CLB实例的网络类型。本文选择专有网络。
专有网络	选择VPC2及VPC2下的交换机。
IP 版本	选择CLB实例的IP版本。本文选择IPv4。
功能特性	选择标准功能。
计费方式	选择按使用流量计费。
数量	选择1。
资源组	选择默认资源组。

步骤二：配置CLB实例

创建

CLB

实例后，您需要至少添加一个监听和一组后端服务器才能实现流量转发。

1. 在实例管理页面，找到步骤一创建的CLB实例，在操作列单击监听配置向导。
2. 在协议&监听配置向导，根据以下信息配置监听规则，其他配置保持默认值，然后单击下一步。
  - 选择负载均衡协议：本文选择TCP协议。
  - 监听端口：用来接收请求并向后端服务器进行请求转发的CLB系统的前端协议和端口。本文端口设置为80。
3. 在后端服务器配置向导，选择默认服务器组，单击继续添加，添加后端服务器。
  - i. 在我的服务器面板，选择已经创建的ECS01和ECS02实例，单击下一步。
  - ii. 配置权重，单击添加。  
权重越大转发的请求越多，默认为100，本文保持默认值。



- iii. 在默认服务器组页签，配置后端协议端口，本文端口设置为80，然后单击下一步。  
ECS实例上开放的用来接收请求的后端端口，在同一个CLB实例内可重复。
- 4. 在健康检查配置向导，配置健康检查，然后单击下一步。本文使用默认值。
- 5. 在配置审核配置向导，检查配置信息，然后单击提交。
- 6. 单击知道了，返回实例管理页面。

当后端ECS实例的健康检查状态为正常时，表示后端ECS实例可以正常处理

CLB

转发的请求了。



步骤三：创建终端节点服务

- 1. 登录终端节点服务控制台。
- 2. 在顶部菜单栏处，选择要创建终端节点服务的地域。本文选择德国（法兰克福）。
- 3. 在终端节点服务页面，单击创建终端节点服务。
- 4. 在创建终端节点服务页面，根据以下信息配置终端节点服务，然后单击确定创建。

配置	说明
选择服务资源	<p>选择要承载流量的可用区，然后选择与终端节点服务关联的CLB实例。</p> <p>本文选择法兰克福 可用区B，然后选择步骤一创建的支持私网连接功能的CLB实例。</p>
自动接受终端节点连接	<p>选择是否自动接受终端节点的连接请求。本文选择否。</p> <ul style="list-style-type: none"><li>是：终端节点服务将自动接受终端节点的连接请求，通过终端节点能够访问服务。</li><li>否：终端节点连接将处于已断开状态，等待服务使用方进行处理：<ul style="list-style-type: none"><li>如果服务使用方接受该终端节点对应的终端节点服务连接，通过终端节点将能够访问服务。</li><li>如果服务使用方拒绝该终端节点对应的终端节点服务连接，通过终端节点无法访问服务。</li></ul></li></ul>
是否支持同可用区优先	本文选择是。

配置	说明
描述	<p>输入终端节点服务的描述信息。</p> <p>描述长度为2~256个字符，但是开头不能为 <code>http://</code> 和 <code>https://</code>。</p>

终端节点服务创建成功后，系统自动将服务所有者的账号ID添加到服务白名单中。

您可以在终端节点服务页面查看服务ID和服务名称。



### 步骤四：创建终端节点

1. [登录终端节点控制台](#)。
2. 在顶部菜单栏处，选择要创建终端节点的地域。本文选择德国（法兰克福）。
3. 在终端节点页面，单击创建终端节点。
4. 在创建终端节点页面，根据以下信息配置终端节点，然后单击确定创建。

配置	说明
节点名称	输入终端节点的名称。 名称长度在2~128个字符之间，以英文字母或中文开头，可包含数字、短划线（-）和下划线（_）。
终端节点服务	您可以通过以下两种方式设置终端节点服务： <ul style="list-style-type: none"><li>单击<b>通过服务名称添加</b>，然后输入终端服务名称。</li><li>单击<b>选择可用服务</b>，然后选择目标终端节点服务ID。</li></ul> 本文先单击 <b>通过服务名称添加</b> ，然后选择 <b>步骤三</b> 中创建的终端节点服务。
专有网络	选择需要创建终端节点的VPC。本文选择已创建的VPC1。
安全组	选择要与终端节点网卡关联的安全组，安全组可以管控VPC到终端节点网卡的数据通信。 <div> <b>说明</b> 确保安全组内的规则开放了客户端对终端节点网卡的访问。</div>
可用区与交换机	选择终端节点服务对应的可用区，然后选择该可用区内的交换机，系统会自动在该交换机下创建一个终端节点网卡。 本文选择 <b>法兰克福 可用区B</b> ，然后选择VPC1中创建的交换机。

配置	说明
描述	输入终端节点的描述信息。 描述长度为2~256个字符，但是开头不能是 <code>http://</code> 和 <code>https://</code> 。

创建终端节点后，您可以查看访问服务的域名或IP。有以下三种方式可以访问终端节点服务：

- 终端节点域名
- IP地址
- 可用区域名

← ep-bp191ac9cdad00430b3

基本信息

实例ID

ep-bp191ac9cdad00430b3

终端节点类型

接口

服务名称

com.aliyuncs.privateconnect.cn-hangzhou-epsnvp-bp14...

专有网络ID

vpc-bp191ac9cdad00430b3

状态

可用

是否支持同可用区优先

是

实例名称

end-test01

所属服务ID

epsnvp-bp191ac9cdad00430b3

终端节点域名

ep-bp191ac9cdad00430b3.ep-bp191ac9cdad00430b3.cn-hangzhou-epsnvp-bp14...

限速

1024 Mbps

连接状态

已连接

描述

付费信息

付费类型

-

付费者

服务使用方

创建时间

2022年2月24日 11:24:39

可用区与网卡

安全组

监控

添加可用区

可用区	可用区域名	交换机ID	弹性网卡	IP地址	状态	服务状态	操作
杭州 可用区B	ep-bp191ac9cdad00430b3-cn-hangzhou-epsnvp-bp14...-cn-hangzhou-epsnvp-bp14...	vsw-bp191ac9cdad00430b3	eni-bp191ac9cdad00430b3	192.168.2.77	已连接	正常	删除

步骤五：接受终端节点连接请求

终端节点发送连接请求后，终端节点服务需要接受终端节点的连接请求。接受后，VPC1才能通过终端节点访问服务。

**说明** 如果您在步骤三创建终端节点服务时设置自动接受连接请求，请忽略此步骤。

1. 在左侧导航栏，单击终端节点服务。

2. 在顶部菜单栏处，选择终端节点服务的地域。本文选择德国（法兰克福）。

3. 在终端节点服务页面，找到步骤三创建的终端节点服务，单击其服务ID链接。

4. 单击终端节点连接页签，找到目标终端节点，在操作列单击允许。

5. 在允许连接对话框，单击确定。

接受连接请求后，终端节点连接的状态由已断开变更为已连接。

服务资源	终端节点连接	服务白名单	监控
终端节点ID	Q 请输入		
终端节点ID	监控	终端节点所在专有网络	终端节点所有者
+	ep-bp191ac9cdad00430b3	vpc-bp191ac9cdad00430b3	当前用户
			连接修改时间
			2022年3月25日 15:56:02
			状态
			已连接
			连接限速
			1024 Mbps
			操作
			拒绝 调整限速

步骤六：通过终端节点访问服务

完成以下操作，测试VPC1中的ECS1实例是否可以通过私网访问VPC2中部署在ECS2上的服务。

1. 打开VPC1中 ECS1实例的浏览器。
2. 在浏览器中输入访问服务的域名或IP，测试是否可以访问VPC2中部署在ECS2上的服务。

本文输入[步骤四](#)创建终端节点后生成的访问域名或IP。

经测试，VPC1 ECS1实例可以通过私网访问VPC2中部署在ECS2上的服务。

## 2.跨账号VPC间的私网访问服务

本文指导您使用私网连接（PrivateLink）服务将一个专有网络（VPC）内部署的私网SLB服务共享给其他账号下的VPC访问。

### 背景信息

VPC是您独有的云上私有网络，不同VPC之间完全隔离。您可以通过私网连接建立VPC与阿里云服务之间安全稳定的私有连接，简化网络架构，避免通过公网访问服务带来的潜在安全风险。

通过私网连接实现私网访问，您需要创建终端节点服务和终端节点。


- 终端节点服务

终端节点服务是可以与其他VPC的终端节点建立私网连接服务，由服务提供方创建和管理。

- 终端节点

终端节点可以与终端节点服务相关联，以建立通过VPC私网访问外部服务的网络连接。终端节点由服务使用方创建和管理。

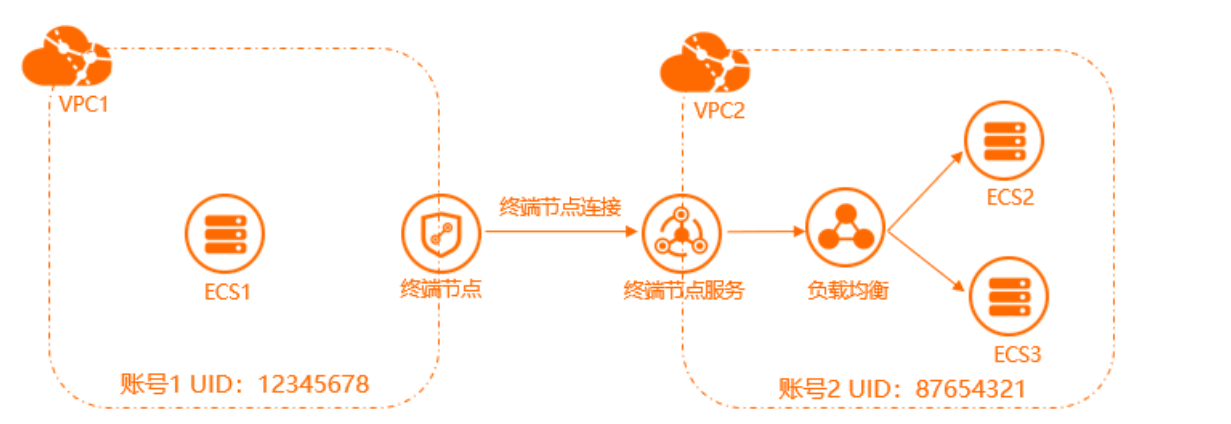
相关主体	相关组件
服务提供方	创建和管理终端节点服务。
服务使用方	创建和管理终端节点。

 **说明** 目前，仅部分地域支持私网连接。更多信息，请参见[支持私网连接的地域和可用区](#)。

### 配置场景

本文以下图场景为例。某公司在阿里云有两个云账号，账号1 UID为12345678，账号2 UID为87654321。该公司在账号1和账号2下分别创建了VPC1和VPC2，VPC2中的ECS实例创建了应用服务。因业务发展，VPC2中的服务需要被VPC1通过私网访问，避免公网访问服务带来的潜在安全风险。

您可以在VPC2下创建支持PrivateLink的负载均衡实例，将ECS实例添加为负载均衡实例的后端服务器，然后创建终端节点服务，将负载均衡实例添加为服务资源，并将账号1的UID添加到终端节点服务的白名单中。在VPC1下创建终端节点。创建成功后，VPC1即可跨账号私网访问VPC2下的服务。



### 前提条件

开始前，请确保满足以下条件：

- 您已经注册了阿里云账号。如还未注册，请先完成[账号注册](#)。
- 首次使用时，请登录[私网连接服务开通页面](#)根据提示开通私网连接服务。
- 您已经在VPC2下创建了ECS实例，并部署了应用服务。详细信息，请参见[使用向导创建实例](#)。
- 您已经在VPC1创建了安全组。详细信息，请参见[创建安全组](#)。

配置步骤



步骤一：创建支持PrivateLink功能的负载均衡实例

目前，仅支持PrivateLink功能的负载均衡实例可以作为终端节点服务的服务资源。通过PrivateLink实现在VPC间私网访问服务前，您需要创建支持PrivateLink功能的负载均衡实例。

完成以下操作，创建支持PrivateLink功能的负载均衡实例。

1. 使用账号2登录[传统型负载均衡CLB控制台](#)。
2. 在实例管理页面，单击创建传统型负载均衡。
3. 在购买页面，根据以下信息配置负载均衡实例。

配置	说明
付费模式	选择一种付费模式。本文选择按量付费。 <div><span>?</span> 说明 仅按量付费模式的传统型负载均衡实例支持PrivateLink功能。</div>
地域和可用区	选择负载均衡实例所属的地域和可用区，确保负载均衡实例的地域和后端添加的云服务器ECS的地域相同。本文地域选择德国（法兰克福），可用区选择法兰克福 可用区B。
可用区类型	显示所选地域的可用区类型。本文选择多可用区。
备可用区	选择负载均衡实例的备可用区。备可用区默认不承载流量，主可用区不可用时才承载流量。本文选择欧洲中部1 可用区A。
实例名称	自定义新建实例名称。 长度限制为1~80个字符，允许包含中文、字母、数字、短划线（-）、正斜线（/）、半角句号（.）和下划线（_）等字符。
实例规格	选择一个实例规格。不同的实例规格所提供的性能指标不同。本文选择简约型l（slb.s1.small）。
实例类型	根据业务场景选择配置对外公开或对内私有的负载均衡服务。本文选择私网。

配置	说明
网络类型	选择负载均衡实例的网络类型。本文选择专有网络。
专有网络	选择VPC2及VPC2下的交换机。
IP 版本	选择负载均衡实例的IP版本。本文选择IPv4。
功能特性	选择标准功能。
计费方式	选择按使用流量计费。
数量	选择1。
资源组	选择默认资源组。

4. 单击立即购买并完成支付。

步骤二：配置负载均衡实例

创建负载均衡实例后，您需要添加至少一个监听和一组后端服务器才能实现流量转发。

1. 在实例管理页面，找到步骤一创建的负载均衡实例，在操作列单击监听配置向导。
2. 在协议&监听页面，根据以下信息配置监听规则。

◦ 选择负载均衡协议：本文选择TCP协议。

◦ 监听端口：用来接收请求并向后端服务器进行请求转发的负载均衡系统的前端协议和端口。  
本文端口设置为80。

其它配置保持默认选项。单击下一步。

3. 在后端服务器页面，选择默认服务器组，单击继续添加，添加后端服务器。

i. 在我的服务器页面，勾选已经创建的ECS实例，单击下一步。

ii. 配置权重，权重越大转发的请求越多，默认为100，保持默认值即可。

iii. 单击添加。

iv. 在后端服务器页面，配置后端协议端口，ECS实例上开放的用来接收请求的后端端口，在同一个负载均衡实例内可重复。本文端口设置为80。

v. 单击下一步。

4. 配置健康检查，本文使用默认值。单击下一步。

5. 进入配置审核页面，确认无误后单击提交。

6. 单击知道了，返回实例管理页面。

当后端ECS实例的健康检查状态为正常时，表示后端ECS实例可以正常处理负载均衡转发的请求了。

步骤三：创建终端节点服务

终端节点服务是可以被其他VPC通过创建终端节点建立私网连接的服务。

> 文档版本：20220329

15

1. 使用账号2[登录终端节点服务控制台](#)。
2. 在顶部菜单栏处，选择要创建终端节点服务的地域。本文选择德国（法兰克福）。
3. 在终端节点服务页面，单击创建终端节点服务。
4. 在创建终端节点服务页面，根据以下信息配置终端节点服务，然后单击确定创建。
  - 选择服务资源：选择要承载流量的可用区，然后选择与终端节点服务关联的负载均衡实例。  
负载均衡实例作为服务资源与终端节点服务关联，关联的负载均衡实例将接受来自您服务的用户的网络访问，终端节点服务的可用区与服务资源所在的主可用区一致。仅支持专有网络类型且支持PrivateLink功能的负载均衡实例作为服务资源。  
本文选择法兰克福 可用区B，然后选择[步骤一](#)创建的支持PrivateLink功能的负载均衡实例。
  - 自动接受终端节点连接：选择是否自动接受终端节点的连接请求。
    - 是：终端节点服务将自动接受终端节点的连接请求，通过终端节点能够访问服务。
    - 否：终端节点连接将处于已断开状态，等待服务管理员进行处理：
      - 如果服务管理员接受该终端节点对应的终端节点服务连接，通过终端节点将能够访问服务。
      - 如果服务管理员拒绝该终端节点对应的终端节点服务连接，通过终端节点无法访问服务。  
本文选择否。
  - 是否支持同可用区优先：本文选择是。
  - 描述：输入终端节点服务的描述信息。  
描述长度为2~256个字符，但是开头不能为 `http://` 和 `https://`。

终端节点服务创建成功后，您可以查看终端节点服务的服务ID和服务名称。

#### 终端节点服务

<div>1. 通过VPC私有网络访问阿里云服务的最佳实践详见<a href="#">《通过私网访问云服务》</a></div> <div>2. 私网CLB全面支持私网连接（PrivateLink）功能。详见<a href="#">公告</a>。</div>								
<div>创建终端节点服务</div> <div>实例ID <input type="text"/> 请输入实例ID进行精确查询 <input type="button" value="Q"/></div>								
实例ID/描述	监控	是否自动接受连接	是否支持同可用区优先	状态	服务名称	创建时间	连接带宽峰值	操作
<a href="#">创建终端节点服务</a>		否	否	✓ 可用	...	2021年9月24日 17:15:10	1024 Mbps	<a href="#">删除</a>

## 步骤四：添加服务白名单

您可以为终端节点服务添加服务白名单，服务白名单中的用户可以创建与终端节点服务连接的终端节点。完成以下操作，将账号1的UID添加到账号2配置的终端节点服务的服务白名单中。

1. 使用账号2[登录终端节点服务控制台](#)。
2. 在左侧导航栏，单击终端节点服务。
3. 在终端节点服务页面，找到[步骤三](#)创建的终端节点服务，单击其服务ID链接。
4. 单击服务白名单页签，然后单击添加白名单。
5. 在添加白名单对话框，输入要添加的白名单账号，然后单击确定。

本文输入账号1的UID，即12345678。





## 步骤五：创建交换机

您需要在VPC1下创建交换机，交换机的可用区必须与**步骤一**创建的负载均衡实例的主可用区一致。创建成功后，系统才能在该交换机下创建终端节点网卡。终端节点网卡是VPC1通过终端节点访问VPC2服务的入口。

1. 在左侧导航栏，单击**交换机**。
2. 在顶部菜单栏处，选择要创建交换机的地域。  
本文选择**德国（法兰克福）**。
3. 在**交换机**页面，单击**创建交换机**。
4. 在**创建交换机**对话框，根据以下信息配置交换机，然后单击**确定**。

- **资源组**：选择交换机的资源组。本文选择**全部**。
- **专有网络**：选择交换机所属的专有网络。本文选择**VPC1**。
- **名称**：输入交换机的名称。

名称长度为2~128个字符，以大小写字母或中文开头，可包含数字、下划线（\_）和短划线（-）。

- **可用区**：选择交换机所属的可用区。本文选择**法兰克福 可用区B**。
- **IPv4网段**：指定交换机的IPv4网段。
- **描述**：输入交换机的描述信息。

描述长度为2~256个中英文字符，开头不能为 `http://` 和 `https://` 。

## 步骤六：创建终端节点

终端节点可以与终端节点服务相关联，以建立通过VPC私网访问外部服务的网络连接。

1. 使用账号1**登录终端节点控制台**。
2. 在顶部菜单栏处，选择要创建终端节点的地域。本文选择**德国（法兰克福）**。
3. 在**终端节点**页面，单击**创建终端节点**。
4. 在**创建终端节点**页面，根据以下信息配置终端节点，然后单击**确定创建**。

- **节点名称**：输入终端节点的名称。

名称长度在2~128个字符之间，以英文字母或中文开头，可包含数字、短划线（-）和下划线（\_）。

- **终端节点服务**：您可以通过以下两种方式设置终端节点服务：

- 单击**通过服务名称添加**，然后输入终端服务名称。
- 单击**选择可用服务**，然后选择目标终端节点服务。

本文先单击通过服务名称添加，然后选择步骤三中创建的终端节点服务。详细信息，请参见[步骤三：创建终端节点服务](#)。

- **专有网络**：选择需要创建终端节点的VPC。本文选择VPC1。
- **安全组**：选择要与终端节点网卡关联的安全组，安全组可以管控VPC到终端节点网卡的数据通信。

 **说明** 确保安全组内的规则开放了客户端对终端节点网卡的访问。

- **可用区与交换机**：选择终端节点服务对应的可用区，然后选择该可用区内的交换机，系统会自动在该交换机下创建一个终端节点网卡。

本文选择法兰克福 可用区B，然后选择步骤五创建的交换机。详细信息，请参见[步骤五：创建交换机](#)。

- **描述**：输入终端节点的描述信息。

描述长度为2~256个字符，但是不能以 `http://` 和 `https://` 开头。

创建终端节点后，您可以查看访问服务的域名或IP。有以下三种方式可以访问终端节点服务：

- 终端节点域名
- IP地址
- 可用区域名

← ep-bp191ac9cdad00430b3

删除

基本信息

实例ID

ep-bp191ac9cdad00430b3

复制

终端节点类型

接口

服务名称

com.aliyuncs.privateconnectivity.cn-hangzhou-b-epsrv-bp14...

专有网络ID

vpc-bp191ac9cdad00430b3

vpc-bp191ac9cdad00430b3

状态

可用

是否支持同可用区优先

是

实例名称

endnode-test01

编辑

所属服务ID

epsrv-bp191ac9cdad00430b3

mvr

终端节点域名

ep-bp191ac9cdad00430b3-7f...

限速

1024 Mbps

连接状态

已连接

描述

编辑

付费信息

付费类型

-

付费者

服务使用方

创建时间

2022年2月24日 11:24:39

可用区与网卡

安全组


监控

添加可用区

可用区	可用区域名	交换机ID	弹性网卡	IP地址	状态	服务状态	操作
杭州 可用区B	ep-bp191ac9cdad00430b3-cn-hangzhou-b-epsrv-bp14...	vsw-bp191ac9cdad00430b3	eni-bp191ac9cdad00430b3	192.168.2.77	已连接	正常	删除

### 步骤七：接受终端节点连接请求

终端节点发送连接请求后，终端节点服务需要接受终端节点的连接请求。接受后，VPC1才能通过终端节点访问服务。

 **说明** 如果您在[步骤三](#)创建终端节点服务时设置自动接受连接请求，请忽略此步骤。

完成以下操作，在账号2的终端节点服务上接受账号1的终端节点连接请求。

1. 使用账号2[登录终端节点服务控制台](#)。
2. 在顶部菜单栏处，选择终端节点服务的地域。  
本文选择德国（法兰克福）。

3. 在终端节点服务页面，找到[步骤三](#)创建的终端节点服务，单击其服务ID链接。
4. 单击终端节点连接页签，找到[步骤六](#)创建的终端节点，在操作列单击允许。
5. 在允许连接对话框，单击确定。

接受连接请求后，终端节点连接的状态由已断开变更为已连接。

服务资源

终端节点连接

服务白名单

终端节点ID

请输入

Q

终端节点ID	终端节点所在专有网络	终端节点所有者	连接修改时间	状态	连接带宽
+ ep-hp33-1p5	vpc-hp33-gg7	当前账户	2020年9月9日 09:40:51	已连接	1024 Mbps

## 步骤八：通过终端节点访问服务

完成以下操作，测试账号1 VPC是否可以通过终端节点访问账号2的服务。

1. 打开账号1 ECS实例的浏览器。
2. 在浏览器中输入访问服务的域名或IP，测试是否可以访问账号2的服务。

本文输入步骤六创建终端节点后生成的访问域名或IP。详细信息，请参见[步骤六](#)。