

ALIBABA CLOUD

阿里云

私网连接
快速入门

文档版本：20220711

 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
3.私网连接支持将ALB作为服务资源	21

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。

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

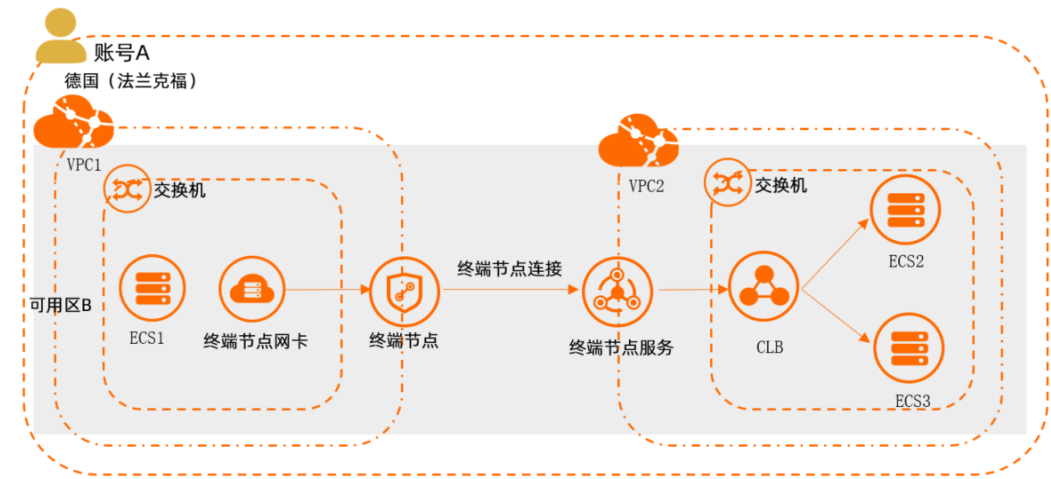
实例，将ECS2实例和ECS3实例添加为

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。



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。
- 创建终端节点服务时，选择地域需要同时支持私网连接和
CLB
实例的地域。关于私网连接和
CLB
实例支持的地域，请参见[私网连接支持的地域](#)和[CLB支持的地域信息](#)。
- 终端节点和终端节点服务需要部署在一个可用区内，且该可用区必须是
CLB
实例部署的可用区。

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部署了不同的Nginx服务。关于如何创建ECS实例和部署Nginx服务，请参见[使用向导创建实例](#)和[手动部署LNMP环境（Alibaba Cloud Linux 2）](#)。
- 您已经在VPC1创建了安全组。您可以根据自己的实际业务和安全要求配置安全组规则。建议配置的安全组规则如下：
 - 默认开放ICMP协议，用于Ping ECS服务器等操作。
 - 默认入方向开放SSH 22端口和RDP 3389端口，用于访问ECS实例。
 - 可选入方向开放HTTP 80端口和HTTPS 443端口，用于VPC1通过HTTP协议或者HTTPS协议访问VPC2。

具体操作，请参见[创建安全组](#)。

 **说明** VPC2中使用的安全组是在创建ECS2和ECS3时，阿里云为您创建的默认安全组。

本文中2个VPC网络规划如下表所示，在您规划网络时，选择的VPC1和VPC2的网段可以重叠且互不影响。

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	- VPC网段：10.10.1.0/16 - 交换机网段：10.0.0.0/24	- VPC网段：192.168.2.0/16 - 交换机网段：192.168.24.0/24
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	- ECS2 IP地址：192.168.20.200 - ECS3 IP地址：192.168.20.12

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。本文只支持选择按量付费。
地域和可用区	选择实例的所属地域，并在可用区下拉列表中选择实例的主可用区，主可用区是当前承载流量的可用区。 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。  说明 确保实例的地域和后端添加的云服务器ECS（Elastic Compute Service）的地域相同。

配置	说明
可用区类型	显示所选地域的可用区类型。系统默认显示 多可用区 。
备可用区	选择实例的备可用区。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	输入自定义实例名称。
实例计费方式	选择实例的一种计费方式。包括以下两种计费方式： - 按规格计费 - 按使用量计费 本文选择 按规格计费 。
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) 。
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，系统会根据您的选择分配公网或私网服务地址。 本文只支持选择 私网 。
网络类型	选择 CLB 实例的网络类型。 系统默认显示 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	选择实例的功能特性。系统默认显示 标准功能 。
公网计费方式	选择一种公网计费方式。公网 CLB 实例支持以下两种公网计费方式： - 按使用流量计费 - 按固定带宽计费 本文系统默认显示 按使用流量计费 。 ② 说明 公网实例会按使用流量计费，本文选择的私网实例不会产生流量费。

配置	说明
数量	选择购买数量。本文选择1。
资源组	选择实例所属的资源组。本文选择默认资源组。

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。

☐	实例名称/ID	服务地址	状态	监控	实例体检	端口/健康检查/后端服务器	操作
☐	aut- lb- 未设置标签	192.168.1.203(专有网络) vpc- gw- vsw- gw-	运行中			TCP: 80 正常 默认服务器组 1	监听配置向导 添加后端服务器

步骤三：创建终端节点服务

1. 登录终端节点服务控制台。

配置	说明
终端节点类型	终端节点选择的节点类型。本文选择接口终端节点。
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ID。 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。
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。 ? 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VPC1中创建的交换机。
描述	输入终端节点的描述信息。

创建完终端节点后，您可以看到生成的终端节点域名、终端节点可用区的域名和IP。如下图所示：

← ep-bp1191ac9cdaa00430b3

基本信息

实例ID

ep-bp1191ac9cdaa00430b3

终端节点类型

接口

服务名称

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

专有网络ID

vpc-bp1191ac9cdaa00430b3

状态

可用

是否支持同可用区优先

是

实例名称

endpoints-st01

所属服务ID

epsrv-bp1191ac9cdaa00430b3

终端节点域名

ep-bp1191ac9cdaa00430b3.cn-hangzhou-bpsrv-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-bp1191ac9cdaa00430b3-cn-hangzhou-bpsrv-bp14... vsw-bp1191ac9cdaa00430b3	vsw-bp1191ac9cdaa00430b3	eni-bp1191ac9cdaa00430b3	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，单击终端节点服务的实例ID。
4. 在终端节点服务详情页面，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，勾选**允许连接并自动分配服务资源**，然后单击**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，表示终端节点服务可以处理终端节点发送的请求了。

服务资源							
终端节点连接		服务白名单		监控			
终端节点ID 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	连接修改时间	状态	连接限速	操作
+ ep-by-  Do3		vpc-by- 	当前账户	2022年3月25日 15:56:02	✓ 已连接	1024 Mbps	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。

本文选择输入**步骤四**创建终端节点后生成的终端节点可用区域名或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）内部署的私网传统型负载均衡 CLB（Classic Load Balancer）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。

配置场景

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，使用阿里云账号B在德国（法兰克福）地域创建了VPC2。在VPC2中创建了ECS2和ECS3，并且在VPC2中的ECS2实例和ECS3实例部署了应用服务。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下创建支持私网连接的

CLB

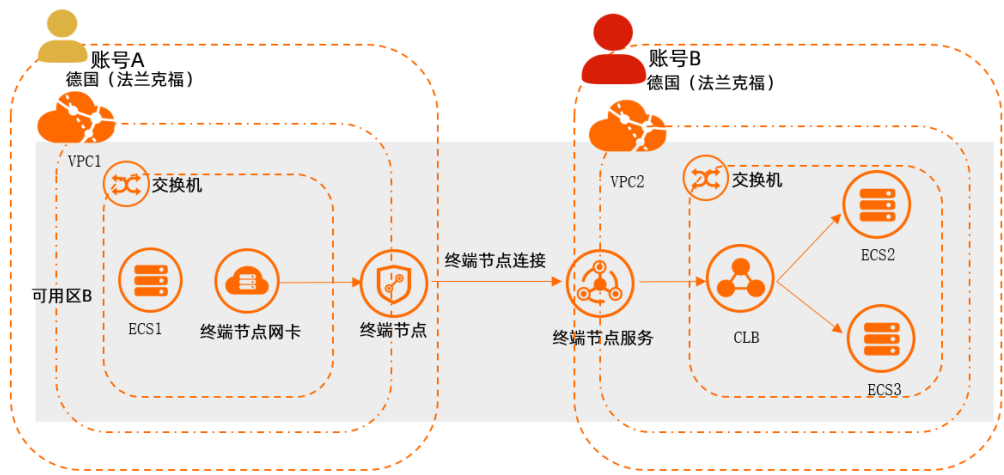
实例，将ECS实例添加为

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，并将账号A的UID添加到终端节点服务的服务白名单中。在VPC1下创建终端节点。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即可跨账号私网访问VPC2下的服务。



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。
- 创建终端节点服务时，选择地域需要同时支持私网连接和
CLB
实例的地域。关于私网连接和
CLB
实例支持的地域，请参见[私网连接支持的地域](#)和[CLB支持的地域信息](#)。
- 终端节点和终端节点服务需要部署在一个可用区内，且该可用区必须是
CLB
实例部署的可用区。

前提条件

- 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。
- 您已使用账号A在德国（法兰克福）地域创建了VPC1，使用账号B在德国（法兰克福）地域创建了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](#)。
- 您已在账号A的VPC1中创建了ECS1实例，在账号B的VPC2中创建了ECS2和ECS3实例，ECS2和ECS3部署了不同的Nginx服务。关于如何创建ECS实例和部署Nginx服务，请参见[使用向导创建实例](#)和[手动部署LNMP环境（Alibaba Cloud Linux 2）](#)。
- 您已经在VPC1创建了安全组。您可以根据自己的实际业务和安全要求配置安全组规则。建议配置的安全组规则如下：
 - 默认开放ICMP协议，用于Ping ECS服务器等操作。
 - 默认入方向开放SSH 22端口和RDP 3389端口，用于访问ECS实例。

- 可選入方向开放HTTP 80端口和HTTPS 443端口，用于VPC1通过HTTP协议或者HTTPS协议访问VPC2。
- 具体操作，请参见[创建安全组](#)。

 **说明** VPC2中使用的安全组是在创建ECS2和ECS3时，阿里云为您创建的默认安全组。

本文中2个VPC网络规划如下表所示，在您规划网络时，选择的VPC1和VPC2的网段可以重叠且互不影响。

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	- VPC网段：10.10.1.0/16 - 交换机网段：10.0.0.0/24	- VPC网段：192.168.2.0/16 - 交换机网段：192.168.24.0/24
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	- ECS2 IP地址：192.168.20.200 - ECS3 IP地址：192.168.20.12

配置步骤



步骤一：创建支持私网连接功能的CLB实例

- 使用账号B登录[传统型负载均衡CLB控制台](#)。
- 在实例管理页面，单击创建传统型负载均衡。
- 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。本文只支持选择按量付费。
地域和可用区	选择实例的所属地域，并在可用区下拉列表中选择实例的主可用区，主可用区是当前承载流量的可用区。 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。  说明 确保实例的地域和后端添加的云服务器ECS（Elastic Compute Service）的地域相同。

配置	说明
可用区类型	显示所选地域的可用区类型。系统默认显示 多可用区 。
备可用区	选择实例的备可用区。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	输入自定义实例名称。
实例计费方式	选择实例的一种计费方式。包括以下两种计费方式： - 按规格计费 - 按使用量计费 本文选择 按规格计费 。
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) 。
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，系统会根据您的选择分配公网或私网服务地址。 本文只支持选择 私网 。
网络类型	选择 CLB 实例的网络类型。 系统默认显示 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	选择实例的功能特性。系统默认显示 标准功能 。
公网计费方式	选择一种公网计费方式。公网 CLB 实例支持以下两种公网计费方式： - 按使用流量计费 - 按固定带宽计费 本文系统默认显示 按使用流量计费 。 ② 说明 公网实例会按使用流量计费，本文选择的私网实例不会产生流量费。

配置	说明
数量	选择购买数量。本文选择1。
资源组	选择实例所属的资源组。本文选择默认资源组。

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ECS2和ECS3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。

☐	实例名称/ID	服务地址	状态	监控	实例体检	端口/健康检查/后端服务器	操作
☐	aut- lb- 未设置标签	192.168.203(专有网络) vpc- gw- vsw- gw-	运行中			TCP: 80 正常 默认服务器组 1	监听配置向导 添加后端服务器

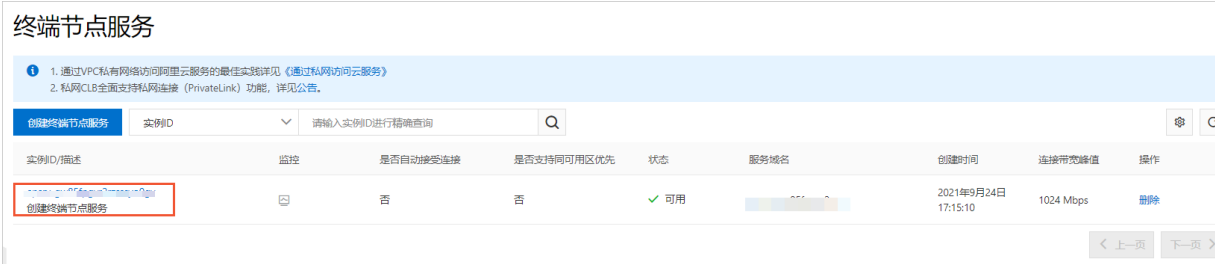
步骤三：创建终端节点服务

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。

1. 使用账号B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	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。 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。
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。本文选择否。 - 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，等待服务使用方进行处理： - 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。 - 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。
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。

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。



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A的UID添加到账号B配置的终端节点服务的服务白名单中。

1. 使用账号B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。
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A的UID，示例图如下：

添加白名单

* 白名单账号

253460731706911258

支持添加一个或多个账号ID，添加多个账号ID时使用英文半角逗号隔开。例如 1234567890123 或 1234567890123,98765432109876

确定

取消

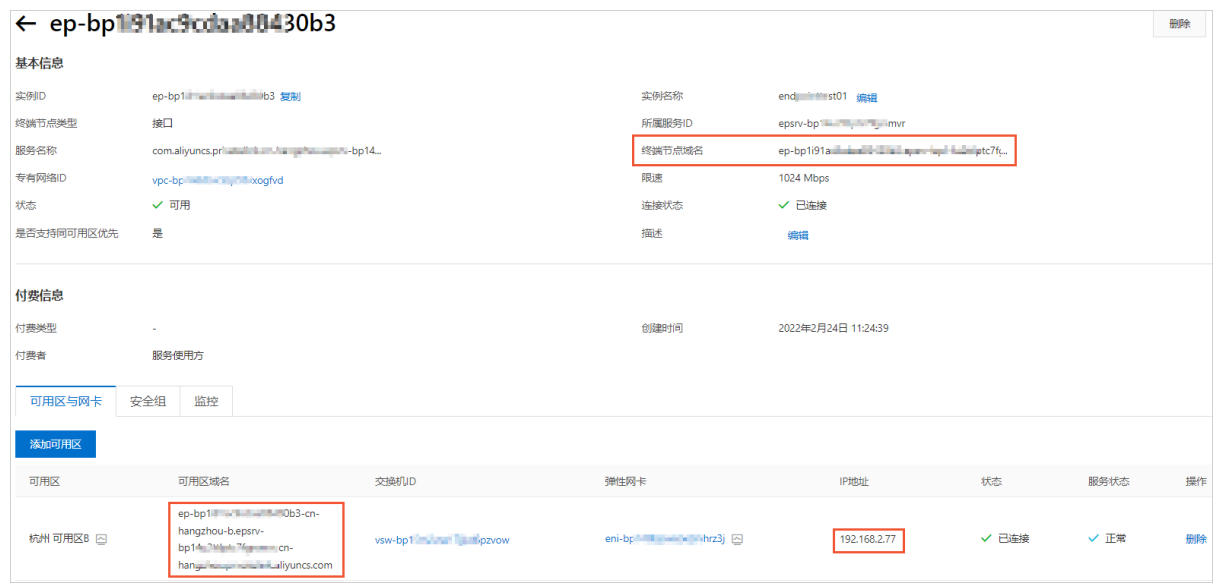
步骤五：创建终端节点

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A[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，单击接口终端节点页签，然后单击**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	输入自定义终端节点的名称。
终端节点类型	终端节点选择的节点类型。本文选择接口终端节点。
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ID。 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。
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。 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VPC1中创建的交换机。
描述	输入终端节点的描述信息。

创建完终端节点后，您可以看到生成的终端节点域名、终端节点可用区的域名和IP。如下图所示：



步骤六：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B的终端节点服务上接受账号A的终端节点连接请求。

1. 使用账号B**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. 在终端节点服务详情页面，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，勾选**允许连接并自动分配服务资源**，然后单击**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**，表示终端节点服务可以处理终端节点发送的请求了。



步骤七：通过终端节点访问服务

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

1. 打开账号A 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VPC2中部署在ECS2上的服务。

本文输入**步骤五**创建终端节点后生成的终端节点可用区域名或IP。

经测试，账号A的VPC1中的ECS1实例可以通过私网访问账号B的VPC2中部署在ECS2上的服务。

3.私网连接支持将ALB作为服务资源

私网连接（PrivateLink）的终端节点服务支持将应用型负载均衡ALB（Application Load Balancer）作为服务资源。

背景信息

ALB

是支持多可用区的服务资源，且拥有超强的业务处理性能，同时提供基于内容的高级路由特性等优势。使用ALB

作为终端节点服务的服务资源时，可以配置一个为多个可用区提供服务的

ALB

服务资源，不需要为每个可用区配置单独的

ALB

服务资源。

本文以下图场景为例。某公司使用阿里云账号A在华东1（杭州）地域创建了VPC1和VPC2，在VPC1中创建了ECS01和ECS02实例，在VPC2中创建了ECS03实例和ECS04实例并部署了不同的Nginx服务。现因业务发展，VPC1的ECS实例需要通过私网访问VPC2中ECS部署的服务。

您需要在VPC2中创建支持私网连接的

ALB

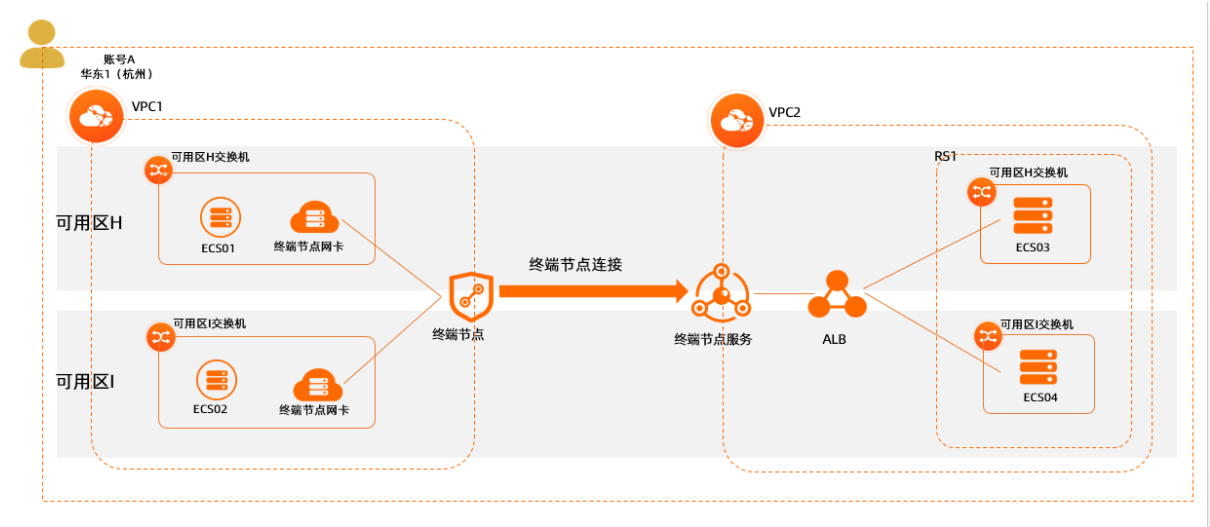
实例，该实例包含华东1（杭州）地域的可用区H和可用区I，然后创建后端服务器组RS1，将ECS03实例和ECS04实例添加到

ALB

的后端服务器组。创建终端节点服务，将

ALB

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的ECS实例即可私网访问VPC2中ECS部署的服务。



使用限制

- 私网连接支持将
ALB
作为服务资源目前白名单开放，如需体验请[提交工单](#)或联系您的客户经理申请。
- 创建支持私网连接功能的
ALB
实例时，只支持创建IP模式为固定IP的私网
ALB
实例。
- 创建终端节点服务时，选择地域需要同时支持私网连接和
ALB
实例的地域。关于私网连接和
ALB
实例支持的地域，请参见[私网连接支持的地域](#)和[支持的地域与可用区](#)。
- 终端节点和终端节点服务需要部署在一个可用区内，且该可用区必须是
ALB
实例部署的可用区。

前提条件

- 您已经在华东1（杭州）地域创建了VPC1和VPC2，并且在VPC1中创建了一个位于可用区H和可用区I的交换机，在VPC2中创建了一个位于可用区H和可用区I的交换机。具体操作，请参见[创建专有网络和交换机](#)。
- 您已经在VPC1中创建了位于可用区H的ECS01和位于可用区I的ECS02，用于发送请求。在VPC2中创建了位于可用区H的ECS03和位于可用区I的ECS04，用于接收和处理请求，且ECS03和ECS04部署了不同的Nginx服务。关于如何创建ECS实例和部署Nginx服务，请参见[使用向导创建实例](#)和[手动部署LNMP环境（Alibaba Cloud Linux 2）](#)。
- 您已经在VPC1创建了安全组。您可以根据自己的实际业务和安全要求配置安全组规则。建议配置的安全组规则如下：
 - 默认开放ICMP协议，用于Ping ECS服务器等操作。
 - 默认入方向开放SSH 22端口和RDP 3389端口，用于访问ECS实例。
 - 可选入方向开放HTTP 80端口和HTTPS 443端口，用于VPC1通过HTTP协议或者HTTPS协议访问VPC2。具体操作，请参见[创建安全组](#)。

 **说明** VPC2中使用的安全组是在创建ECS03和ECS04时，阿里云为您创建的默认安全组。

本文中的2个VPC网络规划如下表所示，在您规划网络时，选择的VPC1和VPC2的网段可以重叠且互不影响。

属性	VPC1	VPC2
网络实例所属的地域	华东1（杭州）	华东1（杭州）

属性	VPC1	VPC2
网络实例的网段规划	- VPC网段：10.0.0.0/8 - 交换机1网段：10.0.10.0/24 - 交换机2网段：10.10.0.0/24	- VPC网段：192.168.0.0/16 - 交换机1网段：192.168.3.0/24 - 交换机2网段：192.168.5.0/24
网络实例交换机的可用区	- 交换机1位于可用区H - 交换机2位于可用区I	- 交换机1位于可用区H - 交换机2位于可用区I
服务器IP地址	- 可用区H下的ECS01 IP：10.0.10.3 - 可用区I下的ECS02 IP：10.0.0.27	- 可用区H下的ECS03 IP：192.168.3.190 - 可用区I下的ECS04 IP：192.168.5.20

配置流程



步骤一：创建支持私网连接功能的ALB实例

- 1. 登录[应用型负载均衡ALB控制台](#)。
- 2. 在实例页面，单击创建应用型负载均衡。
- 3. 在应用型负载均衡（按量付费）购买页面，根据以下信息配置支持私网连接的ALB实例，然后单击立即购买。

配置	说明
地域	选择实例所属的地域。本文选择华东1（杭州）。
实例网络类型	选择实例的网络类型。本文只支持选择私网。
VPC	选择实例所属的VPC。本文选择VPC2。
可用区	实例所在的可用区，需要选择至少2个可用区。本文选择杭州 可用区H以及可用区H下的交换机、杭州 可用区I以及可用区I下的交换机。
IP模式	选择实例的IP地址模式。本文只支持选择固定IP。
功能版本（实例费）	选择实例的功能版本。本文选择基础版。
实例名称	自定义实例名称。
资源组	选择云资源所属的资源组。本文选择默认资源组。

步骤二：创建ALB的后端服务器组

1. 在左侧导航栏，选择**应用型负载均衡ALB > 服务器组**。
2. 在**服务器组**页面，单击**创建服务器组**。
3. 在**创建服务器组**对话框，根据以下信息配置相关参数，然后单击**创建**。

配置	说明
服务器组类型	选择服务器组的类型。本文选择 服务器类型 。
服务器组名称	自定义服务器组的名称。本文输入 RS1 。
VPC	选择后端服务器组所属的VPC。本文选择 VPC2 。
选择后端协议	选择一种后端类型。本文选择 HTTP 。
选择调度算法	选择一种调度算法。本文选择 加权轮询 。
选择资源组	选择云资源所属的资源组。
开启会话保持	是否开启会话保持。本文保持默认配置，既关闭会话保持。
配置健康检查	开启或关闭健康检查。本文保持默认配置，既开启健康检查。
高级配置	开启健康检查后，您可以单击 高级配置 的 修改 展开更多配置信息。本文高级配置保持默认配置。

4. 创建完成后，找到目标后端服务器组**RS1**，单击目标服务器组ID。
5. 单击**后端服务器**页签，然后单击**添加后端服务器**。
6. 在**添加后端服务器**面板，选择已创建的**ECS03**实例和**ECS04**实例，单击**下一步**。
7. 设置已添加的**ECS03**实例和**ECS04**实例的端口和权重，本文端口设置为**80**，权重保持默认值**100**，单击**确定**。

步骤三：配置监听

1. 在左侧导航栏，选择**应用型负载均衡ALB > 实例**。
2. 在**实例**页面，在**实例操作**列单击**创建监听**。
3. 在**配置监听**配置向导，完成以下配置，然后单击**下一步**。

配置	说明
选择负载均衡协议	选择监听的协议类型。本文选择 HTTP 。
监听端口	用来接收和处理请求的监听端口。本文输入 80 。
监听名称	输入自定义监听的名称。
高级配置	单击 修改 进行配置。本文保持默认值。

4. 在**选择服务器组**配置向导，选择**步骤二**中创建的后端服务器组**RS1**，然后单击**下一步**。
5. 在**配置审核**配置向导，确认监听配置信息，然后单击**提交**。

6. 在负载均衡业务配置向导对话框，单击知道了，然后返回实例管理页面。
- 当监听的健康检查状态为正常时，表示后端服务器ECS03和ECS04可以正常处理ALB实例转发的请求了。

创建监听							
监听名称	监听协议/端口	运行状态	健康检查状态	监控	访问控制	监听默认转发规则	操作
HTTP_80 lsn-53gmsa5bafatqma5s	HTTP-80	✓ 运行中	✓ 正常		未开启 启用	转发至 Private:::RS1	查看详情 查看/编辑转发规则 启动 ...

步骤四：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，选择要创建终端节点服务的地域。本文选择华东1（杭州）。
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。

参数	描述
服务资源类型	终端节点服务下的服务资源的类型。本文选择应用负载均衡ALB。
选择服务资源	选择服务资源的可用区及可用区下的服务资源。 本文可用区选择Hangzhou Zone H，然后单击+添加另一可用区资源选择可用区Hangzhou Zone I。可用区H和可用区I的服务资源选择步骤一中创建的支持私网连接的ALB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。本文选择否。
是否支持同可用区优先	终端节点服务是否支持同可用区优先接受终端节点的连接请求。本文选择否。
描述	输入终端节点服务的描述信息。

创建完终端节点服务后，您可以看到一个服务资源类型为ALB的终端节点服务。

创建终端节点服务							
实例ID		请输入实例ID进行精确查询					
实例ID/描述	监控	服务资源类型	是否自动接受连接	状态	创建时间	操作	
epsrv-bp-lbzz1 endpointservices		应用负载均衡ALB	否	✓ 可用	2022年4月18日 15:52:24	删除	

步骤五：创建终端节点

1. 登录终端节点控制台。

2. 在顶部菜单栏，选择要创建终端节点的地域。本文选择华东1（杭州）。
3. 在终端节点页面，单击接口终端节点页签，然后单击创建终端节点。
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。

参数	描述
节点名称	自定义终端节点的名称。
终端节点类型	终端节点选择的节点类型。本文选择接口终端节点。
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，然后输入终端节点服务的名称。 - 单击选择可用服务，然后选择目标终端节点服务ID。 本文先选择选择可用服务，然后选择步骤四创建的终端节点服务。
专有网络	选择终端节点所属的专有网络。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VPC1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。 本文可用区选择Hangzhou Zone H并选择可用区H内的交换机，然后单击+添加交换机选择可用区Hangzhou Zone I并选择可用区I内的交换机。
描述	输入终端节点的描述信息。

创建完终端节点后，您可以看到生成的终端节点可用区的域名和IP。如下图所示：

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
Hangzhou Zone I	ep-bp1- hangzhou-i-epsrv- bp1- hangzhou.privatelink.aliyuncs.com	vsw-bp1- vsw-bp1-					

步骤六：接受连接请求

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终端节点服务。

说明 如果您在步骤四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。本文选择华东1（杭州）。

3. 在终端节点服务页面，找到[步骤四](#)创建的终端节点服务，单击终端节点服务的实例ID。
4. 在终端节点服务详情页面，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，勾选允许连接并自动分配服务资源，然后单击确定。

接受终端节点连接的连接请求后，终端节点连接的状态由已断开变为已连接，表示终端节点服务可以处理终端节点发送的请求了。您可以通过[步骤五](#)生成的终端节点可用区的域名或者IP访问终端节点服务。

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	连接修改时间	状态	连接限速	操作
+ ep-bp1-14ad5		vpc-bp1-14ad5	当前账户	2022年4月19日 10:44:19	已连接	1024 Mbps	拒绝 调整限速

步骤七：测试连通性

完成上述操作后，VPC1和VPC2之间已经可以实现私网通信，以下内容为您展示如何测试VPC1与VPC2之间的连通性。

说明 本文中VPC1的ECS01实例和ECS02实例安装了Windows Server 2012操作系统，VPC2中的ECS03和ECS04实例安装了Alibaba Cloud Linux操作系统，如果您使用的是其他操作系统，如何测试VPC1和VPC2之间的连通性请参见您的操作系统手册。

- 测试VPC1中的ECS01实例是否可以访问VPC2中部署在ECS03中的服务。
 - i. 远程登录VPC1中的ECS01。具体操作，请参见[ECS远程连接操作指南](#)。
 - ii. 打开ECS01的浏览器。
 - iii. 在浏览器中输入[步骤五](#)中创建终端节点后生成的终端节点可用区H的域名或者IP。

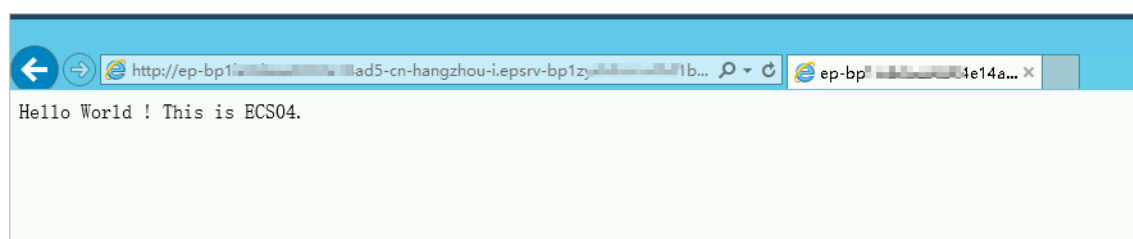
本文选择输入创建终端节点时生成的终端节点可用区H域名的方式进行验证。验证结果如下图所示：



经测试，VPC1中的ECS01实例可以通过私网访问VPC2中部署在ECS03中的服务。

- 测试VPC1中的ECS02实例是否可以访问VPC2中部署在ECS04中的服务。
 - i. 远程登录VPC1中的ECS02。
 - ii. 打开ECS02的浏览器。
 - iii. 在浏览器中输入[步骤五](#)中创建终端节点后生成的终端节点可用区I的域名或者IP。

本文选择创建终端节点时生成的终端节点可用区I域名的方式进行验证。验证结果如下图所示：



经测试，VPC1中的ECS02实例可以通过私网访问VPC2中部署在ECS04中的服务。

相关文档

- [CreateVpcEndpoint](#)：调用CreateVpcEndpoint接口创建终端节点。
- [CreateVpcEndpointService](#)：调用CreateVpcEndpointService接口创建终端节点服务。
- [AttachResourceToVpcEndpointService](#)：调用AttachResourceToVpcEndpointService接口为终端节点添加服务资源。
- [EnableVpcEndpointConnection](#)：调用EnableVpcEndpointConnection接口接受终端节点连接请求。