

ALIBABA CLOUD

阿里云

私网连接  
用户指南

文档版本：20220418

 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. 终端节点	06
1.1. 终端节点概述	06
1.2. 管理终端节点	07
1.2.1. 创建和管理终端节点	07
1.2.2. 查看访问服务的域名或IP	09
1.2.3. 修改终端节点	09
1.2.4. 删除终端节点	10
1.3. 管理终端节点安全组	10
1.3.1. 加入安全组	10
1.3.2. 删除安全组	11
1.4. 管理终端节点网卡	11
1.4.1. 创建终端节点网卡	11
1.4.2. 删除终端节点网卡	11
2. 终端节点服务	13
2.1. 终端节点服务概述	13
2.2. 管理终端节点服务	14
2.2.1. 创建支持私网连接功能的负载均衡实例	14
2.2.2. 创建终端节点服务	16
2.2.3. 修改终端节点服务的基本信息	17
2.2.4. 删除终端节点服务	17
2.3. 管理服务资源	17
2.3.1. 添加服务资源	18
2.3.2. 删除未被关联的服务资源	18
2.4. 管理终端节点连接	18
2.4.1. 设置是否自动接受连接	18
2.4.2. 修改终端节点连接带宽	19

---

2.4.3. 手动接受连接请求	20
2.4.4. 拒绝终端节点连接	20
2.5. 管理服务白名单	20
2.5.1. 添加服务白名单	20
2.5.2. 删除服务白名单	21
3.服务资源调度应用	22
4.服务关联角色	29

# 1. 终端节点

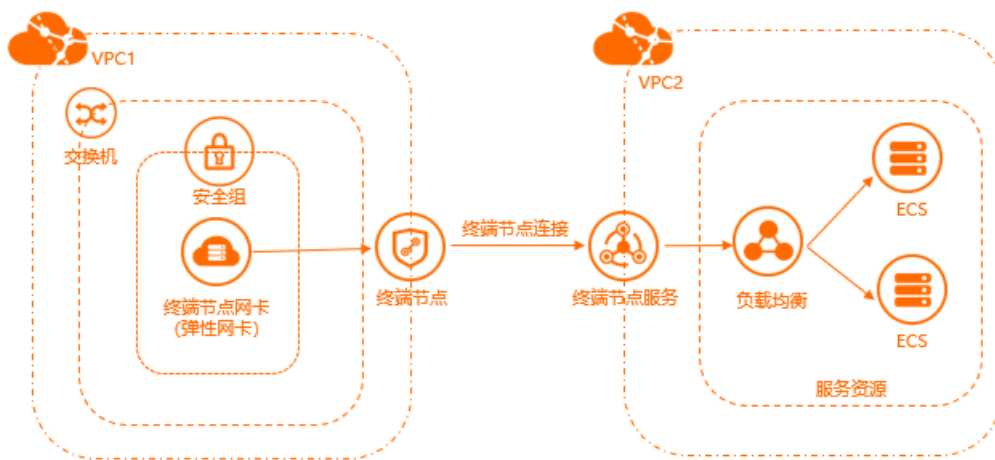
## 1.1. 终端节点概述

本文为您介绍终端节点的概念和创建终端节点并访问终端节点服务的流程。

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

### 概述

终端节点（Endpoint）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。



### 前提条件

创建终端节点前，请确保满足以下条件：

- 您必须了解需要连接的终端节点服务的服务ID或服务名称。
- 您需要联系终端节点服务的管理员，将终端节点所属的账号ID添加到服务白名单中。具体操作，请参见[添加服务白名单](#)。
- 您已经创建了专有网络。具体操作，请参见[创建和管理专有网络](#)。
- 您已经在专有网络中创建了安全组。具体操作，请参见[创建安全组](#)。

### 配置流程

创建终端节点并访问终端节点服务的流程如下：



#### 1. 创建交换机

您需要创建交换机，交换机的可用区须与服务资源所属的主可用区一致。交换机创建成功后，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VPC通过终端节点访问服务的入口。

2. 创建终端节点

您可以创建与终端节点服务关联的终端节点，以建立通过VPC私网访问外部服务的网络连接。具体操作，请参见[创建和管理终端节点](#)。

3. 查看访问服务的域名或IP

创建终端节点后，您可以查看访问服务的域名或IP。更多信息，请参见[查看访问服务的域名或IP](#)。

4. 通过终端节点访问服务

您可以通过终端节点域名、弹性网卡IP或可用区域名访问服务。

# 1.2. 管理终端节点


## 1.2.1. 创建和管理终端节点

您可以创建管理与终端节点服务关联的终端节点，以建立通过VPC私网访问外部服务的网络连接。

### 前提条件

管理终端节点前，请确保满足以下条件：

- 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。


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

- 您已经创建了用于访问终端节点服务的专有网络。具体操作，请参见[创建和管理专有网络](#)。
- 您已经在专有网络中创建了安全组。具体操作，请参见[创建安全组](#)。

### 创建终端节点

您可以创建与终端节点服务关联的终端节点，以建立通过VPC私网访问外部服务的网络连接。

- 登录[终端节点控制台](#)。
- 在顶部菜单栏处，选择终端节点的地域。
- 在终端节点页面，单击[创建终端节点](#)。
- 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<a href="#">通过服务名称添加</a>，然后输入终端服务名称。</li><li>单击<a href="#">选择可用服务</a>，然后选择目标终端节点服务ID。</li></ul> <div> <b>说明</b> 一个终端节点仅支持关联一个终端节点服务。</div>
专有网络	选择需要创建终端节点的专有网络。

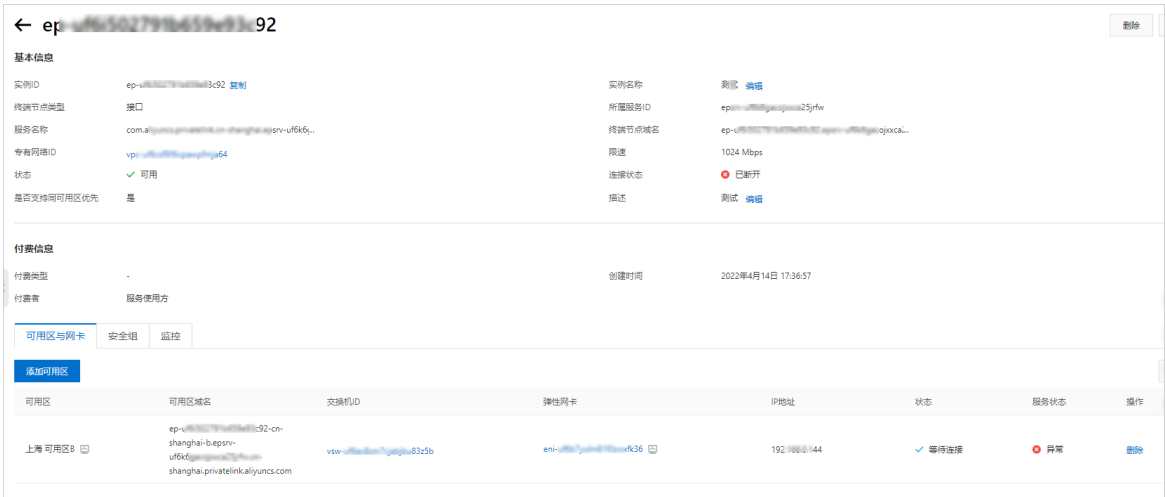
配置	说明
安全组	选择要与终端节点网卡关联的安全组，安全组可以管控VPC到终端节点网卡的数据通信。
可用区与交换机	选择终端节点服务对应的可用区，然后选择该可用区内的交换机，系统会自动在该交换机下创建一个终端节点网卡。
描述	输入终端节点的描述信息。 描述长度为2~256个字符，开头不能为 <code>http://</code> 和 <code>https://</code> 。

查看访问服务的域名或IP

终端节点可以通过终端节点域名、弹性网卡ID和可用区域名访问终端节点服务。

- 1. 登录**终端节点控制台**。
- 2. 终端节点可以通过终端节点域名、弹性网卡IP和可用区域名访问终端节点服务。
- 3. 在**终端节点**页面，找到目标终端节点，单击终端节点ID。
- 4. 在终端节点详情页面，查看访问服务的域名或IP。

您可以通过终端节点域名、弹性网卡ID和可用区域名访问终端节点服务。



修改终端节点

您可以修改终端节点的名称和描述信息。

- 1. 登录**终端节点控制台**。
- 2. 在顶部菜单栏处，选择终端节点的地域。
- 3. 在**终端节点**页面，找到目标终端节点，单击其ID链接。
- 4. 在**基本信息**区域，单击**实例名称**右侧的**编辑**，在弹出的对话框中修改实例名称，然后单击**确定**。  
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（\_）。
- 5. 单击**描述**右侧的**编辑**，在弹出的对话框中修改描述信息，然后单击**确定**。  
描述长度为2~256个字符，不能以 `http://` 和 `https://` 开头。

删除终端节点



您可以删除不需要的终端节点，删除后，终端节点所属VPC将不能通过私网连接访问终端节点服务。

**说明** 删除终端节点前，请先删除终端节点中的终端节点网卡。具体操作，请参见[删除终端节点网卡](#)。

1. 登录[终端节点控制台](#)。
2. 在顶部菜单栏处，选择终端节点的地域。
3. 在终端节点页面，找到目标终端节点，单击操作列下的删除。
4. 在删除终端节点对话框，单击确定。

## 相关文档

- [CreateVpcEndpoint](#)：创建终端节点。
- [ListVpcEndpointConnections](#)：查看终端节点连接。
- [UpdateVpcEndpointAttribute](#)：修改终端节点。
- [DeleteVpcEndpoint](#)：删除终端节点。

## 1.2.2. 查看访问服务的域名或IP

终端节点可以通过终端节点域名、弹性网卡IP和可用区域名访问终端节点服务。

### 操作步骤

1. 登录[终端节点控制台](#)。
2. 在顶部菜单栏处，选择终端节点的地域。
3. 在终端节点页面，找到目标终端节点，单击终端节点ID。
4. 在终端节点详情页面，查看访问服务的域名或IP。

您可以通过终端节点域名、弹性网卡IP和可用区域名访问终端节点服务。

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
上海 可用区8	ep-uf6k6qgms25jrtw-cn-shanghai-b-epsrv-uf6k6qgms25jrtw-shanghai-private-link-aliyuncs.com	vsw-uf6k6qgms25jrtw-cn-shanghai-b-vsw-uf6k6qgms25jrtw	eni-uf6k6qgms25jrtw-cn-shanghai-b-eni-uf6k6qgms25jrtw	192.168.1.144	等待连接	异常	删除

## 相关文档

- [ListVpcEndpointConnections](#)

## 1.2.3. 修改终端节点

您可以修改终端节点的名称和描述信息。

## 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点 > 终端节点**。
3. 在顶部菜单栏处，选择终端节点的地域。
4. 在**终端节点**页面，找到目标终端节点，单击其ID链接。
5. 在**基本信息**区域，单击**实例名称**右侧的**编辑**，在弹出的对话框中修改实例名称，然后单击**确定**。  
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、连字符（-）和下划线（\_）。
6. 单击**描述**右侧的**编辑**，在弹出的对话框中修改描述信息，然后单击**确定**。  
描述长度为2~256个字符，不能以 `http://` 和 `https://` 开头。

## 相关文档

- [UpdateVpcEndpointAttribute](#)

## 1.2.4. 删除终端节点

您可以删除不需要的终端节点，删除后，终端节点所属VPC将不能通过私网连接访问终端节点服务。

### 前提条件

删除终端节点前，请先删除终端节点中的终端节点网卡。详细信息，请参见[删除终端节点网卡](#)。

## 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点 > 终端节点**。
3. 在顶部菜单栏处，选择终端节点的地域。
4. 在**终端节点**页面，找到目标终端节点，单击操作列下的**删除**。
5. 在**删除终端节点**对话框，单击**确定**。

## 相关文档

- [DeleteVpcEndpoint](#)

## 1.3. 管理终端节点安全组

### 1.3.1. 加入安全组

安全组可以管控VPC到终端节点网卡的数据通信，终端节点至少要加入一个安全组。指定安全组后，终端节点下的所有网卡都将加入到安全组中。

## 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点 > 终端节点**。
3. 在顶部菜单栏处，选择终端节点的地域。

4. 在终端节点页面，找到目标终端节点，单击其ID链接。
5. 单击安全组页签，然后单击加入安全组。
6. 在加入安全组对话框，选择要加入的安全组，然后单击确定。

## 相关文档

- [AttachSecurityGroupToVpcEndpoint](#)

### 1.3.2. 删除安全组

您可以删除终端节点网卡关联的安全组，但终端节点至少要加入一个安全组。

## 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击终端节点 > 终端节点。
3. 在顶部菜单栏处，选择终端节点的地域。
4. 在终端节点页面，找到目标终端节点，单击其ID链接。
5. 单击安全组页签，找到目标安全组，单击操作列下的删除。
6. 在弹出的对话框，单击确定。

## 相关文档

- [DetachSecurityGroupFromVpcEndpoint](#)

## 1.4. 管理终端节点网卡

### 1.4.1. 创建终端节点网卡

终端节点网卡是终端节点访问终端节点服务的入口，您可以通过终端节点网卡的私网IP或对应的服务域名访问终端节点服务。

## 背景信息

单个终端节点中可创建的弹性网卡数量不大于终端节点服务的可用区数量。

## 操作步骤

1. 登录[终端节点控制台](#)。
2. 在顶部菜单栏处，选择终端节点的地域。
3. 在终端节点页面，找到目标终端节点，单击终端节点ID。
4. 在可用区与网卡页签，单击添加可用区。
5. 在添加可用区对话框，选择终端节点网卡所属的可用区和交换机，然后单击确定。

## 相关文档

- [AddZoneToVpcEndpoint](#)

### 1.4.2. 删除终端节点网卡

您可以删除不需要的终端节点网卡。

## 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点** > **终端节点**。
3. 在顶部菜单栏处，选择终端节点的地域。
4. 在**终端节点**页面，找到目标终端节点，单击其ID链接。
5. 在**可用区与网卡**页签，找到目标终端节点网卡，单击**操作**列下的**删除**。
6. 在弹出的对话框中，单击**确定**。

## 相关文档

- [RemoveZoneFromVpcEndpoint](#)

## 2.终端节点服务

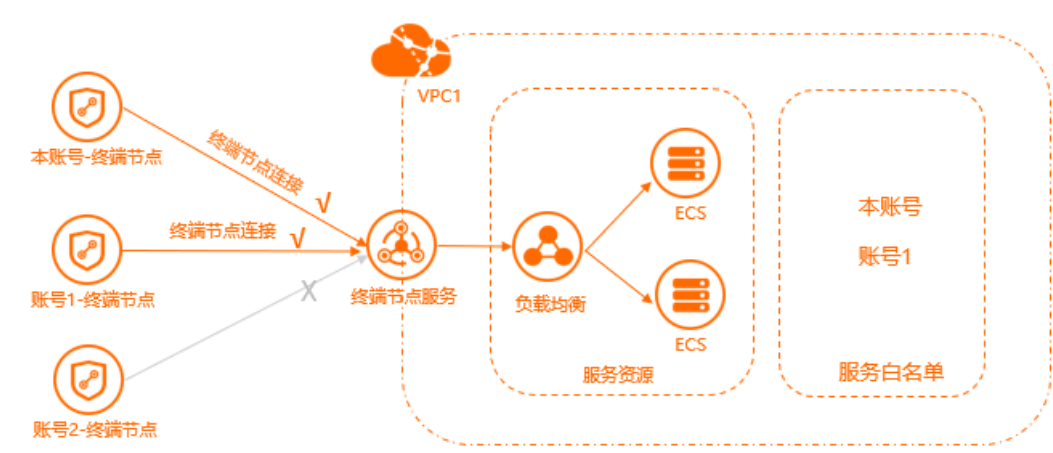
### 2.1. 终端节点服务概述

本文为您介绍终端节点服务的概念和搭建终端节点服务的流程。

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

#### 概述

终端节点服务（EndpointService）是可以被其他VPC通过创建终端节点建立私网连接的服务。终端节点服务由服务提供方创建和管理。



#### 配置流程

搭建终端节点服务的流程如下。



1. 创建支持PrivateLink功能的负载均衡（SLB）实例

目前，仅可以将支持PrivateLink功能的私网SLB实例作为终端节点服务的服务资源，且在创建终端节点服务时需要指定服务资源。所以创建终端节点服务前，您需要创建支持PrivateLink功能的SLB实例。详细信息，请参见[创建支持私网连接功能的负载均衡实例](#)。

2. 配置SLB实例

创建SLB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。详细信息，请参见[配置实例](#)。

3. 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。创建终端节点服务时，您需要指定提供服务的SLB实例。详细信息，请参见[创建终端节点服务](#)。

4. 添加服务白名单

创建终端节点服务后，系统自动将服务所有者的账号ID添加到服务白名单中。服务白名单中的用户可以

查询到该终端节点服务，也可以创建与该终端节点服务连接的终端节点。如果您希望其他账号下的VPC访问服务，您需要将该账号ID添加到服务白名单中。详细信息，请参见[添加服务白名单](#)。

5. （可选）添加服务资源

您可以为终端节点服务添加服务资源。建立终端节点连接后，其他VPC可以私网访问终端节点服务中的服务资源。详细信息，请参见[添加服务资源](#)。

## 2.2. 管理终端节点服务

### 2.2.1. 创建支持私网连接功能的负载均衡实例

本文指引您创建一个支持私网连接（PrivateLink）功能的负载均衡实例，作为终端节点服务的服务资源。

#### 前提条件


创建支持私网连接功能的负载均衡实例前，请确保满足以下条件：

- 目前，仅传统型负载均衡CLB支持私网连接。
- 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](#)。
- 您已经做好了网络规划。更多信息，请参见[准备工作](#)。
- 支持私网连接功能的负载均衡实例必须满足以下条件：

配置	说明
付费模式	按量付费
地域和可用区	选择支持私网连接的地域和可用区。更多信息，请参见 <a href="#">支持私网连接的地域和可用区</a> 。
备可用区	选择支持私网连接的备可用区。更多信息，请参见 <a href="#">支持私网连接的地域和可用区</a> 。
实例类型	私网
网络类型	专有网络

#### 操作步骤

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，根据以下信息配置负载均衡实例。

配置	说明
付费模式	<p>选择一种付费模式。本教程选择按量付费。</p> <div> 说明 仅按量付费模式的负载均衡实例支持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实例的地域相同。

配置	说明
可用区类型	<p>显示所选地域的可用区类型。云产品的可用区指的是一套独立的基础设施，常用数据中心IDC表示。不同的可用区之间具有基础设施（网络、电力、空调等）的独立性，一个可用区的基础设施故障不影响另外一个可用区。可用区是属于某个地域的，一个地域下可能有一个或者多个可用区。负载均衡已经在大部分地域部署了多可用区。</p> <ul style="list-style-type: none"> <li>单可用区：负载均衡实例只部署在一个可用区上。</li> <li>多可用区：负载均衡实例会部署在两个可用区上。默认启用主可用区的实例。当主可用区出现故障时，将会自动切换到备可用区继续提供负载均衡服务，可以大大提升本地可用性。</li> </ul>
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。
实例名称	<p>自定义新建实例名称。</p> <p>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。</p>
实例规格	<p>选择一个实例规格。</p> <p>不同的实例规格所提供的性能指标不同。更多信息，请参见<a href="#">CLB实例概述</a>。</p>
实例类型	<p>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，系统会根据您的选择分配公网或私网服务地址。详细信息，请参见<a href="#">CLB实例概述</a>。</p> <ul style="list-style-type: none"> <li>公网：公网负载均衡实例仅提供公网IP，可以通过Internet访问负载均衡。</li> <li>私网：私网负载均衡实例仅提供阿里云私网IP，只能通过阿里云内部网络访问该负载均衡服务，无法从Internet访问。</li> </ul> <p>本教程选择<b>私网</b>。</p> <div>  <b>说明</b> 仅<b>私网</b>类型的负载均衡实例支持PrivateLink功能。 </div>
网络类型	<p>选择负载均衡实例的网络类型。</p> <p>本教程选择<b>专有网络</b>。</p>
专有网络	选择负载均衡实例所属的专有网络和交换机。
IP 版本	<p>选择负载均衡实例的IP版本。</p> <p>本教程选择<b>IPv4</b>。</p>
功能特性	<p>选择负载均衡实例的功能特性。</p> <p>本教程选择支持<b>PrivateLink</b>。</p>
计费方式	选择一种计费方式。
数量	选择购买数量。
资源组	选择负载均衡实例所属的资源组。

4. 单击**立即购买**，完成支付。

## 2.2.2. 创建终端节点服务

您可以创建终端节点服务，为其他VPC提供私网访问服务。

### 前提条件

开始前，请确保满足以下条件：

- 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](#)。
- 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。
- 您已经创建了支持PrivateLink功能的负载均衡实例。详细信息，请参见[创建支持私网连接功能的负载均衡实例](#)。

### 操作步骤

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。
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负载均衡实例。  如果您还未创建支持PrivateLink功能的负载均衡实例，请参见 <a href="#">创建负载均衡实例</a> ，在负载均衡购买页面创建支持PrivateLink功能的负载均衡实例。您也可以单击 <b>+ 添加</b> 另一可用区资源添加多个服务资源。
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： <ul style="list-style-type: none"><li>◦ <b>是</b>：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>◦ <b>否</b>：终端节点服务连接将处于<b>已断开</b>状态，等待服务管理员进行处理：<ul style="list-style-type: none"><li>■ 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。</li><li>■ 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。</li></ul></li></ul>
是否支持同可用区优先	选择是否支持同可用区优先： <ul style="list-style-type: none"><li>◦ <b>是</b>：终端节点服务支持同可用区优先接受终端节点的连接请求。</li><li>◦ <b>否</b>：终端节点服务不支持同可用区优先接受终端节点的连接请求。</li></ul>
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，开头不能为 <code>http://</code> 和 <code>https://</code> 。

### 相关文档

- [CreateVpcEndpointService](#)



## 2.2.3. 修改终端节点服务的基本信息

您可以修改终端节点服务的基本信息，例如是否自动接受终端节点连接、描述和默认连接带宽峰值。

### 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点 > 终端节点服务**。
3. 在顶部菜单栏处，选择终端节点服务的地域。
4. 在**终端节点服务**页面，找到目标终端节点服务，单击终端节点服务ID链接。
5. 在**基本信息**区域，根据以下信息修改终端节点服务的基本信息。
  - 修改是否自动接收连接  
单击**是否自动接收连接**右侧的**开启**或**关闭**，在弹出的对话框中，单击**确定**。
  - 修改描述信息  
单击**描述**右侧的**编辑**，在弹出的对话框中，修改描述信息，然后单击**确定**。  
描述长度为2~256个字符，不能以 `http://` 和 `https://` 开头。
  - 修改默认连接带宽峰值  
单击**默认连接带宽峰值**右侧的**调整**，在**调整带宽**对话框中输入新的带宽，然后单击**确定**。

### 相关文档

- [UpdateVpcEndpointAttribute](#)

## 2.2.4. 删除终端节点服务

您可以删除终端节点服务，删除终端节点服务不会删除VPC中关联的负载均衡实例。

### 前提条件

删除终端节点服务前，请确保满足以下条件：

- 您必须先拒绝已关联到该服务的终端节点连接。详细信息，请参见[拒绝终端节点连接](#)。
- 您必须删除终端节点服务中包含的服务资源。详细信息，请参见[删除未被关联的服务资源](#)。

### 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点 > 终端节点服务**。
3. 在顶部菜单栏处，选择终端节点服务的地域。
4. 在**终端节点服务**页面，找到目标终端节点服务，单击操作列下的**删除**。
5. 在弹出的对话框中，单击**确定删除**。

### 相关文档

- [DeleteVpcEndpointService](#)

## 2.3. 管理服务资源

## 2.3.1. 添加服务资源

您可以为终端节点服务添加服务资源。建立终端节点连接后，其他VPC可以私网访问终端节点服务中的服务资源。

### 操作步骤

1. [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。
3. 在终端节点服务页面，找到目标终端节点服务，单击终端节点服务ID链接。
4. 在服务资源页签，单击添加服务资源。
5. 在添加服务资源对话框，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。
6. （可选）单击+ 添加另一可用区资源添加多个服务资源。
7. 单击确定。

### 相关文档

- [AttachResourceToVpcEndpointService](#)

## 2.3.2. 删除未被关联的服务资源

当终端节点可用区有未关联的服务资源时，您可以直接删除终端节点服务中不需要提供服务的资源。

### 前提条件

- 您已创建了该可用区的服务资源。具体操作，请参见[创建支持私网连接功能的负载均衡实例](#)。
- 您已添加了该可用区的服务资源。具体操作，请参见[添加服务资源](#)。
- 该服务资源未被可用区关联。

1. [登录终端节点服务控制台](#)。
2. 在顶部菜单栏，选择终端节点服务的地域。
3. 在终端节点服务页面，单击目标终端节点服务的实例ID。
4. 在终端节点服务详情页面，单击服务资源页签，找到目标服务资源，在操作列单击删除。
5. 在移除服务资源对话框，单击确定。

### 相关文档

[DetachResourceFromVpcEndpointService](#)：调用DetachResourceFromVpcEndpointService移除终端节点服务中的服务资源。

## 2.4. 管理终端节点连接

### 2.4.1. 设置是否自动接受连接

您可以根据业务需要，设置是否自动接受连接。如果设置自动接受连接，创建终端节点后，终端节点服务会自动接受终端节点的连接请求。

### 背景信息

创建终端节点时，每个终端节点关联一个终端节点服务。终端节点服务接受了终端节点的连接请求后，终端节点才能与终端节点服务建立连接。您可以设置自动接受终端节点连接，也可以设置手动接受或拒绝终端节点连接，具体如下：

- 开启自动接受连接：创建终端节点后，该终端节点对应的终端节点服务将自动接受终端节点的连接请求，此时通过该终端节点能够访问服务。
- 关闭自动接受连接：创建终端节点后，该终端节点对应的终端节点服务连接将处于连接中状态，等待服务管理员进行处理，此时通过该终端节点无法访问服务。
  - 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。

## 操作步骤

1. 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。
3. 在终端节点服务页面，找到目标终端节点服务，单击终端节点服务的ID链接。
4. 在基本信息区域，单击是否自动接受连接右侧的开启或关闭。



5. 在弹出的对话框，单击确定。

## 相关文档

- [UpdateVpcEndpointServiceAttribute](#)

## 2.4.2. 修改终端节点连接带宽

默认终端节点连接的带宽为1024 Mbps，您可以根据实际业务需要修改终端节点连接带宽。

## 操作步骤

1. 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。
3. 在终端节点服务页面，找到目标终端节点服务，单击其服务ID链接。
4. 单击终端节点连接页签，找到目标终端节点连接，然后在操作列单击调整带宽。
5. 在调整带宽对话框，输入要分配的带宽，然后单击确定。

带宽调整范围为100~1024，单位为Mbps。

## 相关文档

- [UpdateVpcEndpointConnectionAttribute](#)

## 2.4.3. 手动接受连接请求

如果您没有设置自动接受终端节点连接，当终端节点发送连接请求时，您需要手动接受终端节点的连接请求。接受后，终端节点所在的专有网络能够通过终端节点访问服务。

### 前提条件

终端节点连接的状态为已断开，且终端节点可用区状态为等待连接或者已断开时，您可以手动接受该终端节点的连接请求。接收后，终端节点的状态变更为已连接。

1. 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。
3. 在终端节点服务页面，单击目标终端节点服务的实例ID。
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，根据不同情况，单击确定。
  - 当终端节点可用区没有未分配的服务资源时，直接单击确定。
  - 当终端节点可用区有未分配的服务资源时，勾选允许连接并自动分配服务资源，然后单击确定。
  - 当用户需要手动分配服务资源，则取消弹框，在可用区详情页面手动分配可用区的服务资源，完成后单击确定。关于手动分配服务资源，请参见[手动分配可用区服务资源](#)。

### 相关文档

[EnableVpcEndpointConnection](#)：调用EnableVpcEndpointConnection接受终端节点连接请求。

## 2.4.4. 拒绝终端节点连接

当终端节点发送连接请求时，您可以手动拒绝终端节点的连接请求。拒绝后，终端节点所在的专有网络无法通过终端节点访问服务。

### 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击终端节点 > 终端节点服务。
3. 在顶部菜单栏处，选择终端节点服务的地域。
4. 在终端节点服务页面，找到目标终端节点服务，单击其服务ID链接。
5. 单击终端节点连接页签，找到目标终端节点，单击操作列下的拒绝。
6. 在拒绝连接对话框，单击确定。

### 相关文档

- [DisableVpcEndpointConnection](#)

## 2.5. 管理服务白名单

### 2.5.1. 添加服务白名单

创建终端节点服务后，系统自动将服务所有者的账号ID添加到服务白名单中。服务白名单中的用户可以查询到该终端节点服务，也可以创建与该终端节点服务连接的终端节点。如果您希望其他账号下的VPC访问服务，您需要将该账号ID添加到服务白名单中。

## 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点 > 终端节点服务**。
3. 在顶部菜单栏处，选择终端节点服务的地域。
4. 在终端节点服务页面，找到目标终端节点服务，单击其服务ID链接。
5. 单击**服务白名单**页签，然后单击**添加白名单**。
6. 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**。

支持添加一个或多个白名单账号，添加多个白名单账号时使用半角逗号(,) 隔开。

## 相关文档

- [AddUserToVpcEndpointService](#)

## 2.5.2. 删除服务白名单

您可以删除终端节点服务中的白名单账号。删除后，该账号查询不到该终端节点服务，也不能创建与该终端节点服务关联的终端节点连接。

## 操作步骤

1. 登录[专有网络管理控制台](#)。
2. 在左侧导航栏，单击**终端节点 > 终端节点服务**。
3. 在顶部菜单栏处，选择终端节点服务的地域。
4. 在终端节点服务页面，找到目标终端节点服务，单击其服务ID链接。
5. 单击**服务白名单**页签，找到目标白名单账号，单击操作列下的**删除**。
6. 在弹出的对话框，单击**确定**。

## 相关文档

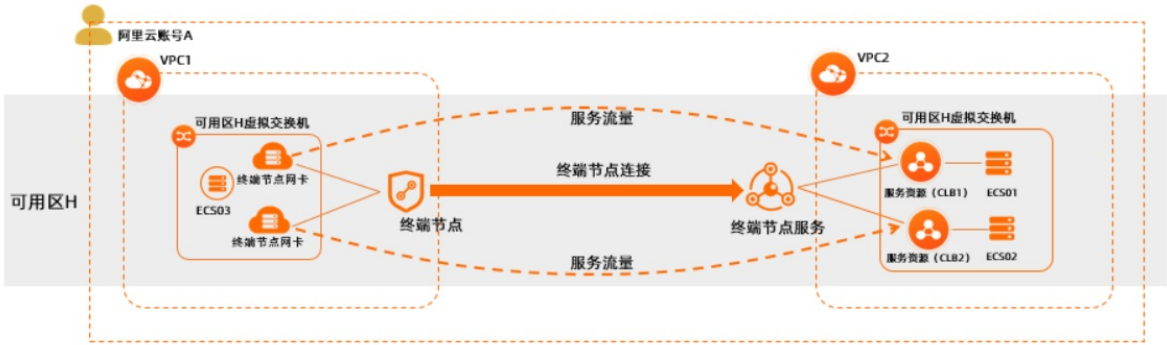
- [RemoveUserFromVpcEndpointService](#)

### 3.服务资源调度应用

目前私网连接（PrivateLink）的终端节点服务支持将传统型负载均衡CLB（Classic Load Balancer）作为服务资源。当终端节点服务接受终端节点连接时，您需要为终端节点所在可用区的终端节点网卡分配指定的CLB服务资源，并与服务资源建立连接。

#### 场景示例

本文以下图场景为例。某公司使用阿里云账号A在华东1（杭州）地域的可用区H创建了专有网络VPC1（Virtual Private Cloud）和VPC2。这两个VPC已实现私网互通，VPC2中使用云服务器ECS（Elastic Compute Service）分别部署了不同的Nginx服务。现因业务发展，需要将VPC2中可用区指定的CLB1服务资源的负载分流一部分到CLB2，避免由于CLB1服务资源负载过高影响业务使用。



#### 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

- 您已经在阿里云华东1（杭州）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](#)。
- 您已经在VPC1中创建了ECS03实例，用于发送请求，并在VPC2中创建了ECS01和ECS02实例，用于接收和处理请求。ECS01和ECS02均部署了不同的Nginx服务。具体操作，请参见[手动部署LNMP环境（Alibaba Cloud Linux 2）](#)。
- 您已经在VPC2中的可用区H创建了服务资源CLB1和CLB2。关于创建支持私网连接的负载均衡，请参见[创建支持私网连接的负载均衡](#)。
- 您已经在服务资源CLB1和CLB2中分别添加了监听和后端服务器ECS01和ECS02。具体操作，请参见[配置负载均衡实例](#)。
- 您已经在VPC1中创建了终端节点，且在VPC2中创建了终端节点服务并绑定了可用区H下的CLB1服务资源。关于创建终端节点和终端节点服务，请参见[创建终端节点和终端节点服务](#)。

本示例中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	华东1（杭州）	华东1（杭州）
网络实例的网段规划	<ul style="list-style-type: none"><li>• VPC网段：10.10.0.0/16</li><li>• 交换机网段：10.0.0.0/24</li></ul>	<ul style="list-style-type: none"><li>• VPC网段：192.168.0.0/16</li><li>• 交换机网段：192.168.24.0/24</li></ul>

属性	VPC1	VPC2
网络实例交换机的可用区	交换机位于可用区H	交换机位于可用区H
服务器IP地址	ECS03 IP地址：10.0.0.190	<ul style="list-style-type: none"><li>ECS01 IP地址：192.168.24.246</li><li>ECS02 IP地址：10.0.0.189</li></ul>

配置流程



步骤一：添加可用区服务资源

- 1. 登录终端节点服务控制台。
- 2. 在顶部菜单栏，选择VPC2中的终端节点服务所属地域。本示例选择华东1（杭州）。
- 3. 在终端节点服务页面，单击目标终端节点服务的实例ID。
- 4. 在服务资源页签，单击添加服务资源。
- 5. 在添加服务资源对话框，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。
- 6. 单击确定。

步骤二：分配并连接可用区服务资源


分配并连接服务资源前，请确保：

- 终端节点连接的状态为已断开。
- 终端节点可用区状态为等待连接或者已断开。
- 终端节点服务在可用区H有可用的服务资源。



- 1. 在终端节点连接页签，找到目标终端节点，在操作列单击允许。
- 2. 在允许连接对话框，根据不同情况进行操作。
  - 如果需要自动分配服务资源：
    - a. 勾选允许连接并自动分配服务资源，单击确定。



- b. 单击目标终端节点前的+图标，在展开的可用区详细信息中选择目标可用区。本示例选择Hangzhou Zone H。
  - c. 在目标可用区的操作列单击连接服务资源。
  - d. 在允许连接对话框，单击确定。
- 如果需要手动分配服务资源，则取消允许连接并自动分配服务资源的弹框：
- a. 单击目标终端节点前的+图标，在展开的可用区详细信息中选择目标可用区。本示例选择Hangzhou Zone H。
  - b. 在目标可用区的操作列单击分配服务资源。
  - c. 在分配服务资源对话框，单击手动分配选择已创建的服务资源CLB1，然后单击确定。
-  **说明** 当终端节点可用区已有指定的服务资源时，选择自动分配会清除已经指定的服务资源。并且在终端节点连接选择允许自动分配可用区服务资源时，该服务资源可以被允许自动分配。
- d. 在目标可用区的操作列单击连接服务资源。
  - e. 在允许连接对话框，单击确定。
3. 远程登录ECS03实例，执行curl命令测试VPC1中的ECS03是否能正常访问部署在VPC2中的ECS01上的服务。关于远程登录ECS实例，请参见[ECS远程连接操作指南](#)。

```
curl https://<终端节点可用区域名>
```

如下图所示，ECS03可以访问到ECS01上的服务。

```
[root@iz1-1-1-1-1 ~]# curl http://ep-bp11965a11a331@link.aliyuncs.com
Hello World ! This is ECS01.
[root@iz1-1-1-1-1 ~]#
```

### 步骤三：创建报警规则

1. 登录[云监控控制台](#)。
2. 在左侧导航栏，选择[云产品监控](#)。
3. 在[云产品监控](#)页面的网络区域下单击[私网连接 终端节点服务](#)。
4. 在[私网连接 终端节点服务](#)监控页面右上角，单击[创建报警规则](#)。
5. 在[创建报警规则](#)面板，配置报警规则相关信息，然后单击[确认](#)。

以下为与终端节点服务实例强相关的报警规则参数说明，其他参数配置，请参见[创建报警规则](#)。

- **产品**：本示例选择**私网连接 终端节点服务**。
- **资源范围**：报警规则的作用范围。本示例选择**实例**。
- **关联资源**：本示例选择VPC2中创建的**终端节点服务**。
- **规则描述**：报警规则的主体。当监控数据满足报警条件时，触发报警规则。

单击添加规则，在添加规则描述面板，完成以下配置，单击确认。

参数	说明
规则名称	自定义规则的名称。



参数	说明
指标类型	阈值报警规则的指标类型。本示例选择 <b>单指标</b> 。
监控指标	报警的监控指标名称。本示例选择 <b>终端节点服务资源流入带宽</b> 。
请选择维度	报警作用的地域ID、服务资源ID。 本示例 <b>zoneId</b> 选择 <b>cn-hangzhou</b> ， <b>resourceId</b> 选择VPC2中的CLB1的实例ID。
阈值及报警级别	报警规则的报警阈值和报警级别。 本示例报警级别选择 <b>警告（Warn）</b> ，短信+邮件+钉钉机器人，报警条件选择 <b>连续1个周期（1周期=1分钟）平均值≥100Mbit/s</b> ，表示报警服务1分钟检查一次终端节点服务资源流入带宽，如果流入带宽检测1次≥100Mbit/s，就上报告警。
监控图表预览	表示指定时间段内监控指标的监控图表。

- 点开高级设置，配置以下参数。
  - 通道沉默周期：报警发生后未恢复正常，间隔多久重复发送一次报警通知。本示例选择30分钟。
  - 生效时间：报警规则的生效时间，报警规则只在生效时间内才会检查监控数据并判断是否需要报警。本示例选择00:00至23:59。
- 报警联系人组：发送报警的联系人通知组。关于创建报警联系人和报警联系人通知组，请参见[创建报警联系人或报警联系组](#)。

阈值报警

事件报警

创建报警策略

请输入进行查询

搜索

<input type="checkbox"/>	规则描述名称	状态(全部)	启用	监控项(全部)	维度(全部)	报警规则	产品名称(全部)	通知对象	操作
<input type="checkbox"/>	rdsinst-epsv-vp-tic@...-47ec-8b-	✔ 正常状态	已启用	跨节点服务器资源流入带宽	resourceId=bp1g2zpmj... ipInstanceId=peo1m...f5 3fa@@nzoneid.cn-hangzhou-h	跨节点服务器资源流入带宽 >= 100Mbit/s 连续1次触发报警	私网连接 跨节点服务	云账号报警联系人查看	<a href="#">设置</a>   <a href="#">报警历史</a> <a href="#">修改</a>   <a href="#">禁用</a>   <a href="#">删除</a>
<input type="checkbox"/>	<div><div>应用</div><div>使用</div><div>删除</div></div>								
共 1 条 <div>10 ▾</div> <div>&lt;=&gt;1&gt;</div>									

#### 步骤四：通过wrk工具进行压测

通过wrk工具对VPC2中终端节点服务的CLB1服务资源进行压测，当CLB1服务资源的后端服务器ECS01达到设置的报警阈值时，触发云监控的报警任务上报告警。

**④ 说明** 本示例中ECS03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，关于如何安装并使用wrk工具请参见您的操作系统手册。

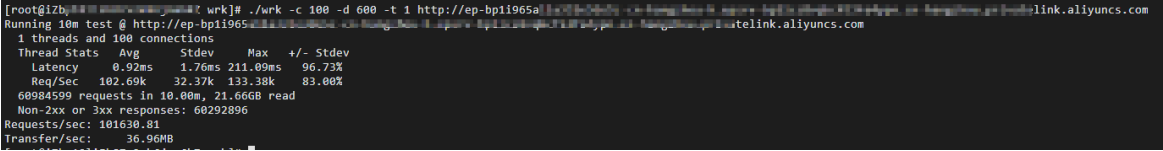
1. 远程登录VPC1的ECS03实例。
2. 在VPC1的ECS03实例中依次执行以下命令，安装wrk工具。

```
yum -y install git make gcc
git clone https://github.com/wg/wrk.git
yum install unzip
cd wrk
make
```

3. 安装完成后，执行以下命令通过wrk工具对ECS01实例进行压测。

```
./wrk -c 100 -d 600 -t 1 http://<终端节点可用区域名>
```

收到如下所示的回复报文，则表示压测已经完成。



4. 返回步骤的报警规则列表页面，等待几分钟后，可以看到报警状态变为红色，表示CLB1服务资源超过报警阈值，您需要将CLB1的负载分流一部分到CLB2服务资源。



步骤五：替换可用区服务资源

替换服务资源前，请确保：

- 终端节点连接的状态为已连接。
- 终端节点可用区状态为已连接或者已断开。
- 终端节点可用区H中除了已经连接的CLB1服务资源外，至少还有1个可用的服务资源。
- 终端节点可用区CLB1服务资源不允许自动分配。具体操作，请参见[允许和禁止服务资源自动分配](#)。



1. 登录终端节点服务控制台。
2. 在顶部菜单栏，选择终端节点服务的地域。本示例选择华东1（杭州）。
3. 在终端节点服务页面，单击目标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，单击目标终端节点前的+图标。
5. 在展开的可用区详细信息中选择目标可用区，在操作列单击替换服务资源。
6. 在替换服务资源对话框，根据业务需要，单击平滑迁移或强制迁移，选择需要替换的服务资源CLB2，单击确认。
7. 待替换完成后，远程登录ECS03实例，执行curl命令测试VPC1中的ECS03是否能正常访问部署在VPC2中的ECS02上的服务。

```
curl https://<终端节点可用区域名>
```

如下图所示，ECS03可以访问到ECS02上的服务。

```
[root@i2b ~]# curl http://ep-bp1i96.cn-hangzhou.aliyuncs.com
Hello World ! This is ECS02.
[root@i2b ~]#
```

## 更多操作

## 允许和禁止服务资源自动分配

选择禁止服务资源自动分配时，请确保一个可用区至少包含一个可以自动分配的服务资源。

1. [登录终端节点服务控制台](#)。
2. 在顶部菜单栏，选择终端节点服务的地域。
3. 在终端节点服务页面，单击目标终端节点服务的实例ID。
4. 在终端节点服务详情页面，单击服务资源页签，找到目标服务资源，在自动分配列根据需要打开或关闭开关。
  - 打开已禁止开关，在是否允许服务资源自动分配？对话框，单击允许。
  - 关闭已允许开关，在是否禁止服务资源自动分配？对话框，单击禁止。

## 断开可用区服务资源

断开可用区服务资源前，请确保：

- 终端节点连接的状态为已连接。
- 终端节点可用区状态为已连接。
- 终端节点可用区有被分配的服务资源。
  1. **登录终端节点服务控制台。**
  2. 在顶部菜单栏，选择终端节点服务的地域。
  3. 在**终端节点服务**页面，单击目标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，单击目标终端节点前的+图标。
  5. 在展开的可用区详细信息中选择目标可用区，在**操作列**根据以下情况单击**断开服务资源**。
    - 在平滑替换场景中，需要先单击**断开旧服务资源**后，再单击**断开服务资源**。
    - 在强制迁移或者未迁移过可用区服务资源场景中，直接单击**断开服务资源**。

② 说明

当迁移方式为平滑迁移时，在可用区中需要展现新的终端节点网卡和旧的终端节点网卡。

6. 在是否断开服务资源?对话框, 单击确认断开。


## 删除服务资源

1. 登录终端节点服务控制台。
2. 在顶部菜单栏，选择终端节点服务的地域。
3. 在终端节点服务页面，单击目标终端节点服务的实例ID。
4. 在终端节点服务详情页面，单击服务资源页签，找到目标服务资源，根据不同情况进行操作。

- 当服务资源没有被任何终端节点可用区关联时：
  - a. 在目标服务资源操作列单击删除。
  - b. 在移除服务资源对话框，单击确定。
- 当服务资源被终端节点可用区关联时：
  - a. 在目标服务资源操作列单击替换资源。
  - b. 在替换服务资源对话框，完成以下配置，单击确定。

配置项	说明
迁移方式	<p>根据业务需要选择平滑迁移或强制迁移。</p> <ul style="list-style-type: none"> <li>■ 当选择平滑迁移时，待迁移完成后，需要在操作列单击清理旧连接，旧连接清理完成后，才能删除服务资源。</li> <li>■ 当选择强制迁移时，待迁移完成后，直接删除服务资源。</li> </ul>
选择目标服务资源	选择需要替换的服务资源。
选择源终端节点连接	勾选源关联的终端节点连接。

- c. 在目标服务资源操作列单击删除。
- d. 在移除服务资源对话框，单击确定。

 **说明** 当需要删除的服务资源被终端节点可用区关联时，需要先在服务资源页签的自动分配列关闭已允许的开关。

## 相关文档

- **UpdateVpcEndpointZoneConnectionResourceAttribute**：调用UpdateVpcEndpointZoneConnectionResourceAttribute接口修改终端节点连接可用区的服务资源。
- **EnableVpcEndpointZoneConnection**：调用EnableVpcEndpointZoneConnection接口接受终端节点在此可用区的连接请求。
- **DisableVpcEndpointZoneConnection**：调用DisableVpcEndpointZoneConnection接口拒绝终端节点在此可用区的连接请求。
- **UpdateVpcEndpointServiceResourceAttribute**：调用UpdateVpcEndpointServiceResourceAttribute接口修改终端节点服务资源的相关属性。
- **DetachResourceFromVpcEndpointService**：调用DetachResourceFromVpcEndpointService接口移除终端节点服务中的服务资源。

## 4. 服务关联角色

本文为您介绍私网连接PrivateLink的服务关联角色（AliyunServiceRoleForPrivatelink）以及如何删除私网连接的服务关联角色。

### 服务关联角色介绍

服务关联角色是指与某个云服务关联的RAM角色。在某些场景下，为了完成云服务的某个功能，需要获取其他云服务的访问权限。通过服务关联角色，您可以更好的创建云服务正常操作所需的权限，避免误操作带来的风险。更多关于服务关联角色的信息，请参见[服务关联角色](#)。

### 创建服务关联角色

创建终端节点时，需要访问其他云资源，您可以通过服务关联角色获取访问其他云资源的权限。如果服务关联角色不存在，系统会自动创建一个名称为AliyunServiceRoleForPrivatelink的服务关联角色，并且为该角色添加名称为AliyunServiceRolePolicyForPrivatelink的权限策略，授予终端节点拥有访问其他云资源的权限，策略内容如下所示：

```
{
  "Version": "1",
  "Statement": [
    {
      "Action": [
        "vpc:DescribeVSwitchAttributes"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:CreateNetworkInterface",
        "ecs:DeleteNetworkInterface",
        "ecs:DescribeNetworkInterfaces",
        "ecs:CreateNetworkInterfacePermission",
        "ecs:DescribeNetworkInterfacePermissions",
        "ecs:DeleteNetworkInterfacePermission"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": "ram:DeleteServiceLinkedRole",
      "Resource": "*",
      "Effect": "Allow",
      "Condition": {
        "StringEquals": {
          "ram:ServiceName": "privatelink.aliyuncs.com"
        }
      }
    }
  ]
}
```

## 删除服务关联角色

如果您要删除私网连接PrivateLink的服务关联角色（AliyunServiceRoleForPrivatelink），请先删除终端节点。详细信息，请参见[删除终端节点](#)。