



私网连接 用户指南

文档版本: 20220524



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。

- 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。
- 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。
- 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。	大) 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。	⑦ 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 cd /d C:/window 命令,进入 Windows系统文件夹。				
斜体	表示参数、变量。	bae log listinstanceid				
[] 或者 [alb]	表示可选项,至多选择一个。	ipconfig [-all -t]				
{} 或者 {alb}	表示必选项,至多选择一个。	switch {act ive st and}				

目录

1.终端节点	05
1.1. 终端节点概述	05
1.2. 创建和管理终端节点	06
1.3. 加入和管理安全组	09
1.4. 创建和管理终端节点网卡	10
2.终端节点服务	11
2.1. 终端节点服务概述	11
2.2. 管理终端节点服务	12
2.2.1. 创建和管理终端节点服务	12
2.2.2. 创建终端节点服务	18
2.2.3. 修改终端节点服务的基本信息	19
2.2.4. 删除终端节点服务	19
2.3. 管理服务资源	19
2.3.1. 添加和管理服务资源	19
2.3.2. 删除服务资源	20
2.4. 管理终端节点连接	20
2.4.1. 允许和管理终端节点连接	20
2.4.2. 修改终端节点连接带宽	22
2.4.3. 手动接受连接请求	23
2.4.4. 拒绝终端节点连接	23
2.5. 管理服务白名单	23
2.5.1. 添加和管理服务白名单	23
2.5.2. 删除服务白名单	24
3.服务资源调度应用	25
4.服务关联角色	32

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。

概述

终端节点(Endpoint)可以与终端节点服务相关联,以建立VPC1通过私网访问VPC2中部署的负载均衡服务。终端节点由服务使用方创建和管理。



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,交换机的可用区需与负载均衡服务资源所属的主可用区一致。交换机创建成功后, 系统会自动在该交换机下创建一个终端节点网卡,终端节点网卡是终端节点VPC访问终端节点服务的入 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VPC通过私网访问另一个VPC中部署的负载均衡服务。具体操作,请参见创建终端节点。

3. 查看访问服务的域名和IP

创建终端节点后,您可以查看访问服务的域名和IP。具体操作,请参见查看访问服务的域名和IP。

通过终端节点访问终端节点服务
 您可以通过终端节点域名、终端节点可用区域名或IP访问终端节点服务。

1.2. 创建和管理终端节点

终端节点(Endpoint)可以与终端节点服务相关联,以建立通过专有网络VPC(Virtual Private Cloud)私网 访问外部服务的网络连接。本文为您介绍如何创建和管理终端节点。

背景信息

私网连接能够实现VPC与阿里云上的服务建立安全稳定的私有连接,避免通过公网访问服务带来的潜在安全 风险。您可以通过创建终端节点,并且将终端节点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。

使用限制

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。

任务

- 创建终端节点
- 查看访问服务的域名或IP
- 修改终端节点
- 删除终端节点

前提条件

创建终端节点前,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。
- 您已经创建了终端节点服务,且终端节点服务至少添加了一个服务资源。具体操作,请参见创建和管理终端节点服务。
- 您已经创建了用于访问终端节点服务的VPC,且在已创建的终端节点服务对应的可用区创建了交换机。具体操作,请参见创建专有网络和交换机。
- 您已经创建了安全组。
 - 如果终端节点类型为接口终端节点时,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。
 - 可选开放入方向HTTP 80端口和HTTPS 443端口,用于终端节点所在的VPC通过HTTP协议或者HTTPS 协议访问终端节点服务所在的VPC。
 - 如果终端节点类型为反向终端节点时,入方向安全规则必须全部放行,即入方向开放全部协议、任意端口和任意地址段。

具体操作,请参见创建安全组。

创建终端节点

- 1. 登录终端节点控制台。
- 2. 在顶部菜单栏处,选择终端节点所在的地域。
- 3. 在终端节点页面,您可以通过以下两种方式创建终端节点。
 - 单击接口终端节点页签,然后单击创建终端节点。

○ 单击反向终端节点页签,然后单击创建终端节点。

? 说明

- 接口终端节点是指服务使用方通过接口终端节点访问服务提供方提供的服务,反向终端节点 是指服务提供方的服务通过反向终端节点访问服务使用方网络中的资源。
- 。终端节点由服务使用方创建和管理,终端节点服务由服务提供方创建和管理。

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。 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(_)。
终端节点类型	 根据需要输入终端节点类型。终端节点有以下两种类型: 接口终端节点:正向访问,表示服务使用方通过接口终端节点访问服务提供方提供的服务。 反向终端节点:反向访问,表示服务提供方提供的服务通过反向终端节点访问服务使用方网络中的资源。
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,然后输入终端服务的名称。 单击选择可用服务,然后选择目标终端节点服务的ID。 ⑦ 说明 一个终端节点仅支持关联一个终端节点服务。
专有网络	选择需要创建终端节点的VPC。
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。 ⑦ 说明 终端节点网卡是终端节点VPC访问终端节点服务的入口。
安全组 可用区与交换 机	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。 ⑦ 说明 终端节点网卡是终端节点VPC访问终端节点服务的入口。 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。
安全组 可用区与交换机 描述	 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。 ③ 说明 终端节点网卡是终端节点VPC访问终端节点服务的入口。 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。 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 http:// 和 https:// 。

查看访问服务的域名或IP

创建完终端节点后,当终端节点类型为接口终端节点时,您可以通过终端节点域名、终端节点可用区域名或 IP地址访问终端节点服务中的服务资源。

- 1. 登录终端节点控制台。
- 2. 在顶部菜单栏处,选择终端节点所在的地域。
- 3. 在终端节点页面,单击接口终端节点页签。
- 4. 在接口终端节点页签下,找到目标终端节点,单击终端节点的实例ID。
- 5. 在终端节点详情页面,您可以查看访问终端节点服务的终端节点域名、终端节点可用区域名或IP地址。

⑦ 说明 当终端节点类型为反向终端节点时,没有终端节点域名和终端节点可用区域名。

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。
- 在终端节点页面,单击接口终端节点页签或者反向终端节点页签,找到目标终端节点,单击终端节点 的实例ID。
 - 修改实例名称:
 - a. 在基本信息区域, 在实例名称右侧单击编辑。
 - b. 在弹出的对话框中,输入要修改的实例名称,然后单击确定。
 名称长度在2~100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 (_)。
 - 修改描述信息:
 - a. 在基本信息区域,在描述右侧单击编辑。
 - b. 在弹出的对话框中, 输入要修改的描述信息, 然后单击确定。

描述长度为2~256个字符,开头不能为 http:// 和 https:// 。

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。

 ⑦ 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。
- 在终端节点页面,单击接口终端节点页签或者反向终端节点页签,找到目标终端节点,然后在操作列 单击删除。
- 4. 在删除终端节点对话框,单击确定。

- CreateVpcEndpoint: 创建终端节点。
- List VpcEndpoints: 查询终端节点。

- UpdateVpcEndpointAttribute: 修改终端节点的属性。
- DeleteVpcEndpoint:删除终端节点。

1.3. 加入和管理安全组

创建终端节点后,您可以通过加入安全组来管控专有网络VPC(Virtual Private Cloud)到终端节点网卡的数据通信,当您不需要该安全组时,您可以删除终端节点网卡关联的安全组。

任务

- 加入安全组
- 删除安全组

前提条件

- 您已创建了终端节点。具体操作,请参见创建和管理终端节点。
- 您已在该终端节点对应的VPC创建了至少两个安全组,且创建的安全组规则如下:
 - 如果终端节点类型为接口终端节点时,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。
 - 可选开放入方向HTTP 80端口和HTTPS 443端口,用于终端节点所在的VPC通过HTTP协议或者HTTPS 协议访问终端节点服务所在的VPC。
 - 如果终端节点类型为反向终端节点时,入方向安全规则必须全部放行,即入方向开放全部协议、任意端口和任意地址段。

具体操作,请参见创建安全组。

加入安全组

- 1. 登录终端节点控制台。
- 2. 在顶部菜单栏处,选择终端节点所在的地域。
- 在终端节点页面,单击接口终端节点或反向终端节点页签,找到目标终端节点,单击终端节点的实例
 ID。
- 4. 在终端节点详情页面,单击安全组页签,然后单击加入安全组。
- 5. 在加入安全组对话框,选择需要加入的安全组,然后单击确定。

删除安全组

删除安全组前,请确保该终端节点至少加入了一个安全组。

- 1. 登录终端节点控制台。
- 2. 在顶部菜单栏处,选择终端节点所在的地域。
- 在终端节点页面,单击接口终端节点或反向终端节点页签,找到目标终端节点,单击终端节点的实例
 ID。
- 4. 在终端节点详情页面,单击安全组页签,找到目标安全组,在操作列单击删除。
- 5. 在移除安全组对话框,单击确定。

- AttachSecurityGroupToVpcEndpoint:加入安全组。
- DetachSecurityGroupFromVpcEndpoint:删除安全组。

1.4. 创建和管理终端节点网卡

终端节点网卡(Endpoint ENI)是终端节点的专有网络VPC(Virtual Private Cloud)访问终端节点服务的入口。您可以创建终端节点网卡,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。您也可以删除不需要的终端节点网卡。

任务

- 创建终端节点网卡
- 删除终端节点网卡

前提条件

您已经创建了终端节点。具体操作,请参见创建和管理终端节点。

创建终端节点网卡

创建终端节点网卡时,选择的终端节点网卡所属的可用区必须在终端节点服务对应的服务资源部署的可用区内,且在对应的可用区已创建了交换机。具体操作,请参见创建交换机。

- 1. 登录终端节点控制台。
- 2. 在顶部菜单栏处,选择终端节点所在的地域。
- 在终端节点页面,单击接口终端节点或反向终端节点页签,找到目标终端节点,单击终端节点的实例
 ID。
- 4. 在终端节点详情页面,单击可用区与网卡页签,然后单击添加可用区。
- 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。

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,选择终端节点所在的地域。
- 在终端节点页面,单击接口终端节点或反向终端节点页签,找到目标终端节点,单击终端节点的实例
 ID。
- 4. 在终端节点详情页面,单击可用区与网卡页签,找到目标终端节点网卡,在操作列单击删除。
- 5. 在移除可用区对话框中,单击确定。

- AddZoneToVpcEndpoint:为终端节点添加可用区。
- RemoveZoneFromVpcEndpoint:删除终端节点可用区。

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。

概述

终端节点服务(Endpoint Service)是可以通过其他专有网络VPC(Virtual Private Cloud)创建的终端节点建 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。

创建完终端节点服务后,如果您希望其他阿里云账号下的VPC创建的终端节点可以访问终端节点服务,您需 要将该阿里云账号ID添加到终端节点服务的白名单中。未添加到服务白名单中的阿里云账号ID查询不到该终 端节点服务,也不能创建与该终端节点服务连接的终端节点。



配置流程

搭建终端节点服务的流程如下。



1. 创建支持私网连接功能的负载均衡实例

目前,仅可以将支持私网连接功能的传统型负载均衡CLB(Classic Load Balancer)和应用型负载均衡 ALB(Application Load Balancer)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,您需要先创建支持私网连接功能的

CLB

或

ALB

实例。具体操作,请参见创建负载均衡实例。

2. 配置负载均衡实例

创建完

CLB

或

ALB

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。具体操作,请参见配置ALB实 例和配置CLB实例。

3. 创建终端节点服务

创建终端节点服务时,您需要指定提供服务的负载均衡实例。具体操作,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阿里云账号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。如果您希望其他阿里云 账号下的VPC访问服务,您需要将该阿里云账号ID添加到服务白名单中。具体操作,请参见添加和管理 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。具体操作,请参见添加和管理服务资源。

2.2. 管理终端节点服务

2.2.1. 创建和管理终端节点服务

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)和应用型负载 均衡ALB(Application Load Balancer)作为服务资源。本文指导您如何创建一个支持私网连接功能的负载 均衡实例,然后通过创建或管理终端节点服务并将已创建的负载均衡实例作为终端节点服务的服务资源,为 其他专有网络VPC(Virtual Private Cloud)提供私网访问服务。

使用限制

• 创建支持私网连接功能的

CLB

实例时,只支持创建付费模式为按量付费的私网

CLB

实例。

• 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。

• 私网连接支持将

ALB

作为服务资源的功能目前白名单开放,如需体验请提交工单或联系您的客户经理申请。

 选择地域和可用区时,需要选择同时支持私网连接和负载均衡实例的地域和可用区。关于私网连接和负载 均衡实例支持的地域和可用区,请参见

o 私网连接支持的地域和可田区

- CLB支持的地域信息
- ALB支持的地域和可用区
- 创建终端节点服务时选择的可用区必须是

CLB

或

ALB

实例部署的可用区。

任务

- 创建负载均衡实例
- 创建终端节点服务
- 修改终端节点服务的基本信息
- 删除终端节点服务

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。
- 您已经创建了

CLB

或

ALB

实例所属的VPC,并且在该VPC下的对应可用区内创建了交换机。具体操作,请参见创建专有网络和交换 机。

⑦ 说明 确保创建交换机时选择的地域和可用区与创建CLB或

ALB

实例时选择的地域和可用区相同。

创建负载均衡实例

创建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,根据以下信息配置支持私网连接的

CLB

实例,然后单击**立即购买**并完成支付。

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。 ⑦ 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。
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。
实例名称	输入自定义实例名称。 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。更多信息,请参见CLB <mark>实</mark> <mark>例概述</mark> 。
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	选择已创建的VPC和VPC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。

配置	说明					
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。					
	⑦ 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。					
数量	选择购买数量。					
资源组	选择实例所属的资源组。					

创建完

CLB

实例后,您可以为其配置监听并添加后端服务器,用于处理客户端发送的请求。本文只提供与终端节点服务强相关的配置步骤,关于如何配置监听及添加后端服务器,请参见配置实例。

创建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**并完成支付。

配置	说明
地域	选择实例所属的地域。
实例网络类型	选择实例网络类型 <i>,</i> 系统会根据您的选择分配私网或公网服务地址。本文只支持选 择 私网 。
VPC	选择已创建的VPC。
可用区	选择实例所属的可用区。 i. 需要选择至少2个或2个以上的可用区。 ii. 分别在所选可用区内选择已创建的交换机。
IP模式	选择实例的IP地址模式。本文只支持选择固定IP。

配置	说明
功能版本(实例费)	选择实例的功能版本。 • 基础版:包含应用型负载均衡的基本功能,可支持基于域名、URL、HTTP Header 等路由转发。 • 标准版:在基础版的功能基础上,还包含自定义TLS安全策略,重定向、重写等高 级路由功能。 关于基础版和标准版功能差异的更多信息,请参见功能特性。
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。

创建完

ALB

实例后,您可以为其创建后端服务器组并配置监听,用于处理客户端发送的请求。本文只提供与终端节 点服务强相关的配置步骤,关于如何创建后端服务器组并配置监听,请参见创建后端服务器组并配置监 听。

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,选择需要创建终端节点服务所属的地域。
- 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
服务资源类型	选择的终端节点服务的服务资源类型。包括以下两种类型: 负载均衡CLB:将已创建的 CLB 实例作为终端节点服务的服务资源。 应用负载均衡ALB:将已创建的 ALB 实例作为终端节点服务的服务资源。

配置	说明
选择服务资源	 选择要承载流量的可用区,然后选择已创建的与终端节点服务关联的负载均衡实例。 当您需要添加多个可用区的服务资源时,您也可以单击+添加另一可用区资源添加多个服务资源。 ② 说明 一个 CLB 实例只能作为一个可用区的服务资源,即 CLB 所在虚拟交换机的可用区。 一个 ALB 实例可以支持多个可用区,也能同时作为多个可用区的服务资源。
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: 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:终端节点服务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	选择是否支持同可用区优先: • 是: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。 • 否: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。
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 http:// 和 https:// 。

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、是否支持同可用区优先、描述和默 认连接限速。

- 1. 登录终端节点服务控制台。
- 2. 在顶部菜单栏处,选择需要修改终端节点服务所属的地域。
- 3. 在终端节点服务页面,找到目标终端节点服务,单击终端节点服务实例ID。
- 4. 在基本信息区域,根据您的需要修改终端节点服务的基本信息。

修改的配置项	说明
是否自动接受连接	表示终端节点服务是否自动接受终端节点的连接请求。 i. 在是否自动接受连接右侧单击开启或关闭。 ii. 在弹出的对话框中,单击确定。
是否支持同可用区优 先	表示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。 i. 在是否支持同可用区优先右侧单击开启或关闭。 ii. 在弹出的对话框中,单击确定。
描述	i. 在 描述 右侧单击 编辑 。 ii. 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,开头不能为 http:// 和 https:// 。
默认连接限速	表示终端节点服务默认的最大带宽峰值。 i. 在 默认连接限速 右侧单击调整。 ii. 在 设置连接默认限速 对话框,在调整限速调整框中输入新的限速,然后单击确 定。 默认连接限速的取值范围为: 100~10240 Mbps。

删除终端节点服务

您可以删除不需要的终端节点服务,删除终端节点服务不会删除VPC中关联的负载均衡实例。 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终端节点服务的终端节点连接。具体操作,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。具体操作,请参见删除服务资源。
 - 1. 登录终端节点服务控制台。
 - 2. 在顶部菜单栏处,选择需要删除终端节点服务所属的地域。
 - 3. 在终端节点服务页面,找到目标终端节点服务,在操作列单击删除。
 - 4. 在弹出的对话框中,单击确定删除。

相关文档

- CreateVpcEndpointService:调用CreateVpcEndpointService接口创建终端节点服务。
- UpdateVpcEndpointServiceAttribute: 调用UpdateVpcEndpointServiceAttribute接口修改终端节点服务的属性。
- DeleteVpcEndpointService:调用DeleteVpcEndpointService接口删除终端节点服务。

2.2.2. 创建终端节点服务

本页面后期将不再维护并下线。更多信息,请参见创建终端节点服务。

2.2.3. 修改终端节点服务的基本信息

本页面后期将不再维护并下线。更多信息,请参见修改终端节点服务的基本信息。

2.2.4. 删除终端节点服务

本页面后期将不再维护并下线。更多信息,请参见删除终端节点服务。

2.3. 管理服务资源

2.3.1. 添加和管理服务资源

您可以为已创建的终端节点服务添加服务资源。建立终端节点连接后,其他专有网络VPC (Virtual Private Cloud)可以私网访问终端节点服务中的服务资源。您也可以删除终端节点服务中不需要的服务资源。

任务

- 添加服务资源
- 删除服务资源

前提条件

您已创建了终端节点服务。具体操作,请参见创建终端节点服务。

添加服务资源

- 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实例ID。
- 4. 在终端节点服务详情页面,单击服务资源页签,然后单击添加服务资源。
- 5. 在添加服务资源对话框,选择要承载流量的可用区,然后通过以下方式添加服务资源,并单击确定。
 - 如果您在该可用区已经创建了服务资源,您可以单击下拉列表选择已创建的服务资源。
 - 如果您在该可用区未创建过服务资源,您可以单击下拉列表创建服务资源。

关于如何创建服务资源,请参见创建支持私网连接的负载均衡实例。

⑦ 说明 如果您需要在多个可用区添加多个服务资源,您可以单击+添加另一可用区资源添加多个可用区和服务资源。

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	 根据业务需要选择平滑迁移或强制迁移。 ■ 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。 ■ 当选择强制迁移时,待迁移完成后,直接删除 服务资源。
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。

⑦ 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

- AttachResourceToVpcEndpointService:为终端节点服务添加服务资源。
- DetachResourceFromVpcEndpointService:删除终端节点服务中的服务资源。

2.3.2. 删除服务资源

本页面后期将不再维护并下线。更多信息,请参见删除服务资源。

2.4. 管理终端节点连接

2.4.1. 允许和管理终端节点连接

您可以设置终端节点服务是否允许终端节点连接,当设置允许终端节点连接后,终端节点服务可以处理终端 节点发送的连接请求。当您不需要处理终端节点发送的请求时,您可以拒绝终端节点连接。

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或手动接受终端节点连接,也可以修改终端节点连 接的带宽或拒绝终端节点连接,具体操作如下:

- 设置是否自动接受连接
- 手动接受连接请求
- 修改终端节点连接带宽

• 拒绝终端节点连接

前提条件

- 您已经创建了终端节点。具体操作,请参见创建终端节点。
- 您已经创建了终端节点服务。具体操作,请参见创建终端节点服务。

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。

- 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实例ID。
- 4. 在终端节点服务详情页面的基本信息区域,在是否自动接受连接右侧单击开启或关闭。
 - 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终端节点服务中的服务资源。
 - 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已断开的状态, 此时通过该终端节点无法访问终端节点服务中的服务资源。
- 5. 在弹出的对话框中, 单击确定。

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,终端节点才能够通过私网访问终端节点服务中的服务资源。

手动接受连接请求前,请确保:

- 1. 终端节点连接的状态为已断开。
- 2. 终端节点可用区状态为等待连接或者已断开。

服	务资源	终端节点连接	ŧ Ał	股务白名单	监控							
终端节点ID V Q 请输入												
	终端	节点ID		监控		终端节点所在专有网络	终端节点所有智	i 连接修改时间		状态 🖓	连接限速	操作
-	ep-u	fesocrana sawac	c92			vpc-uf6	当前账户	2022年4月14日 17:	36:57	9 已断开	1024 Mbps	允许 调整限速
	可用区		城名			交换机ID	网卡		状态	资源ID	操作	
	上海 可)	HKB 🖸	ep-uf shangi uf6	hai-b.epsrv- w. hai.privatelink.al	en-	vsw-uf6a 1z5b	eni-ufé	rfk36 🖸	✓ 等待	连接 -	分配服	务资源

手动接受连接请求后,终端节点连接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,找到目标终端节点服务,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,找到目标终端节点连接,在操作列单击允许。
- 5. 在允许连接对话框,根据不同情况进行操作。
 - 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。

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。

- 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实例ID。
- 在终端节点服务详情页面,单击终端节点连接页签,找到目标终端节点连接,然后在操作列单击调整 限速。
- 5. 在**设置连接默认限速**对话框,根据您的需要输入调整限速带宽,然后单击**确定**。 连接默认限速的取值范围为:100~10240 Mbps。

拒绝终端节点连接

当终端节点向终端节点服务发送连接请求时,您可以手动拒绝终端节点的连接请求。拒绝后,终端节点无法 访问终端节点服务中的服务资源。

拒绝终端节点连接请求前,请确保:

- 1. 终端节点连接的状态为已连接。
- 2. 终端节点可用区状态为已连接或已断开。

服	务资源	终端节点连续	度 服务	白名单	监控								
终期	尚市点ID	✓ Q 请输〉											
	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	\$	伏态 ₽	连接限速	操作	
_	ep-u	ife contraction of the	:92			vpc-uff ja64	当前账户	2022年5月17日 14	4:12:06	✔ 已连接	1024 Mbps	拒绝	调整限速
	可用区		域名			交换机ID	网卡		状态	资源ID		操作	
	上海可	用区B 🖸	ep-uf(shanghai-b uf6l shanghai.pr	.epsrv- fw. rivatelink.al	ttl2-cn- cn- iyuncs.com	vsw-uf6av z5b	eni-uf6	k36 ⊡	9 已断开	lb- uf6og	SV	分配服 连接服	發行資源 發行資源

拒绝后,终端节点连接的状态变更为已拒绝。

- 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,在操作列单击拒绝。
- 5. 在拒绝连接对话框中, 单击确定。

相关文档

- EnableVpcEndpoint Connection: 调用EnableVpcEndpoint Connection接口接受终端节点连接请求。
- UpdateVpcEndpointConnectionAttribute: 调用UpdateVpcEndpointConnectionAttribute接口修改终 端节点连接带宽。
- DisableVpcEndpointConnection: 调用DisableVpcEndpointConnection接口拒绝终端节点的连接请求。

2.4.2. 修改终端节点连接带宽

本页面后期将不再维护并下线。更多信息,请参见修改终端节点连接带宽。

2.4.3. 手动接受连接请求

本页面后期将不再维护并下线。更多信息,请参见手动接受连接请求。

2.4.4. 拒绝终端节点连接

本页面后期将不再维护并下线。更多信息,请参见拒绝终端节点连接。

2.5. 管理服务白名单

2.5.1. 添加和管理服务白名单

创建终端节点服务后,系统自动将服务所有者的阿里云账号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可 以访问终端节点服务,您需要将该账号ID添加到服务白名单中。

任务

- 添加服务白名单
- 删除服务白名单

前提条件

您已创建终端节点服务。具体操作,请参见创建和管理终端节点服务。

添加服务白名单

- 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实例ID。
- 4. 在终端节点服务详情页面,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。

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。

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,账号查询不到该终端节点服务,也不能创建与该终端节 点服务连接的终端节点。

- 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,单击终端节点服务实例ID。
- 4. 在终端节点服务详情页面,单击服务白名单页签,找到目标白名单账号,在操作列单击删除。
- 5. 在移除白名单账号对话框中, 单击确定。

- AddUserToVpcEndpointService:调用AddUserToVpcEndpointService接口添加服务白名单。
- RemoveUserFromVpcEndpointService: 调用RemoveUserFromVpcEndpointService接口删除服务白名

单。

2.5.2. 删除服务白名单

本页面后期将不再维护并下线。更多信息,请参见删除服务白名单。

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	 VPC网段: 10.10.0.0/16 交换机网段: 10.0.0.0/24 	 VPC网段: 192.168.0.0/16 交换机网段: 192.168.24.0/24

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	ECS01 IP地址: 192.168.24.246ECS02 IP地址: 10.0.0.189

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。 本示例可用区选择Hangzhou Zone H,负载均衡实例选择CLB2的实例ID。
- 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。

服	务资源	终端节点	接	服务白名单	监控								
终端	#节点ID	~ Q 请	入										C
	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	ł	公 恣	连接限速	操作	
-	ep-b	photo a starte	le5c			vpc-bp 1q	当前账户	2022年3月23日 11	:08:00)已断开	1024 Mbps	允许 调整限速	
	可用区		域後	8		交换机ID	网卡		状态	资源ID		操作	
	Hangzho	ou Zone H	ep- har bp har	-bortabilar tala ta nganta-kapan- 1 milayiari ak ige ngatas-privasina	sc-cn-	vsw-bp 642	eni-bp i an an an	• • ;t44 ⊡	9 已断开	lb- bp1	- Wo	分配服务资源	

- 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。

⑦ 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。

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 单指标 。
监控指标	报警的监控指标名称。本示例选择 终端节点服务资 源流入带宽 。
请选择维度	报警作用的地域ID、服务资源ID。 本示例zoneld选择cn-hangzhou- h, resourceld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 警告(Warn)短信+邮件+钉 钉机器人 ,报警条件选择连续1个周期(1周期=1 分钟)平均值>=100Mbit/s,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。

jā	國值报警	事件报警								
ŧ.	建报警规则	请输入进行查询		搜索						
	规则描述/名	称	状态 (全部) 👻	启用	监控項 (全部) ▼	維度 (全部) 👻	报警规则	产品名称 (全部) 👻	通知对象	操作
0	ruiiiist epsrv-bp1ic	b-47ec-8b	♥正常状态	已启用	终端节点服务资源流入带宽	resourceld:lb-bp12glzp , z,instanceld:ep: f5 3f on,zoneld:cn-hangzhou-h	终端节点服务资源流入带宽 >=100Mbit/s Warn 连续1次 就报警	私网连接 终端节点服务	云账号报警联系人 查看	査署 报警历史 修改 禁用 删除
	启用	禁用 劉除							共1条 10 🗸 。	< 1 > »

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。

⑦ 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。

[rootĝiZb
Running 10m test 🖗 http://ep-bp1i965
1 threads and 100 connections
Thread Stats Avg Stdev Max +/- Stdev
Latency 0.92ms 1.76ms 211.09ms 96.73%
Req/Sec 102.69k 32.37k 133.38k 83.00%
60984599 requests in 10.00m, 21.66GB read
Non-2xx or 3xx responses: 60292896
Requests/sec: 101630.81
Transfer/sec: 36.96MB

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。

阈	直报警	事件报警								
esse	投發規則	请输入进行查询		搜索						
	规则描述/名	称	状态 (全部) 👻	启用	监控項 (全部) 👻	維度 (全部) マ	报警规则	产品名称 (全部) ▼	通知对象	操作
	n inist epsrv-bp1ici	b-47ec-8b		已启用	终端节点服务资源流入带宽	resourceld:lb-bp12glz; ,z,instanceld:eps f5 3fon_zoneld:cn-hangzhou-h	终端节点服务资源流入带宽 >=100Mbit/s Warn 连续1次 就报警	私网连接 终端节点服务	云账号报誓联系人 查看	- 査看 报警历史 修改 禁用 删除
	启用	禁用 勤除							共1条 10 🖌 。	< 1 > »

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。

服	务资源	终端节点连接	服务白名单	监控								
緫	尚节点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	Σ	连接限速	操作	
-	ep-b	op aratika na shina late	85c 🖸		vpc-bp	当前账户	2022年3月21日 10:	37:28	已连接	1024 Mbps	拒绝 调整限	速
	可用区	ł	咸名		交换机ID	図卡		状态	资源ID		操作	
	Hangzh 🔄	e ou Zone H h b h	ep-bp hangz bp1ics hangz	HeSc-cn- n- /uncs.com	vsw-bp	eni-bp	tt44 🖸	✓ 已连接	lb- bp19		替换服务资源 断开服务资源	

- 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。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。
- 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。

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。
- 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。
- 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。

? 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	 根据业务需要选择平滑迁移或强制迁移。 ■ 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。 ■ 当选择强制迁移时,待迁移完成后,直接删除服务资源。
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。

⑦ 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。

- 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。
- Det achResourceFromVpcEndpointService: 调用Det achResourceFromVpcEndpointService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。