

ALIBABA CLOUD

阿里云

私网连接
产品简介

文档版本：20220520

 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> <i>Instance_ID</i>
[] 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

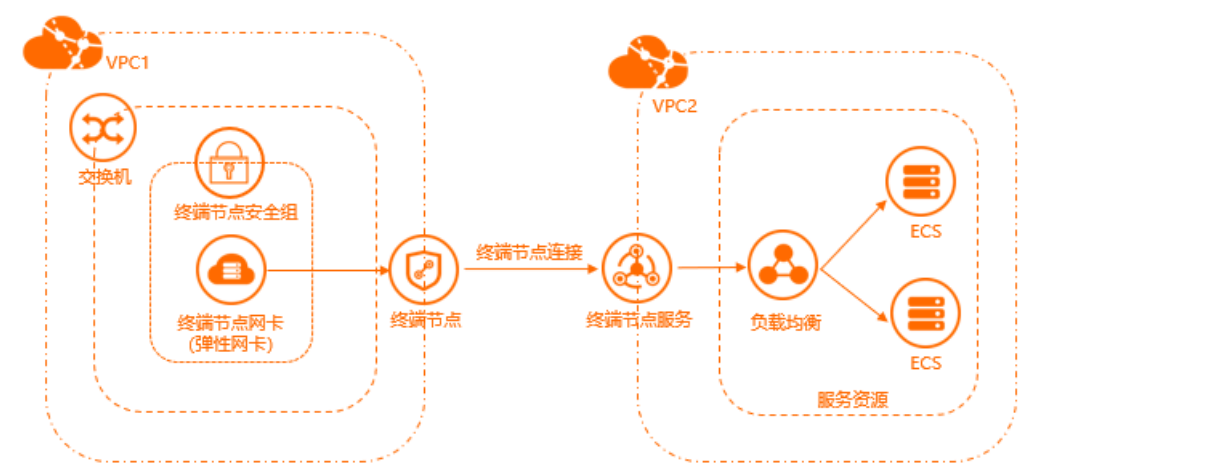
1.什么是私网连接	05
2.使用场景	08
3.基本概念	09
4.使用限制	10
5.支持私网连接的地域和可用区	11

1.什么是私网连接

私网连接（PrivateLink）能够建立专有网络VPC（Virtual Private Cloud）与阿里云上的服务安全稳定的私有连接，简化网络架构，实现私网访问服务，避免通过公网访问服务带来的潜在安全风险。

基本概念

使用私网连接前，您需要了解以下概念。



术语	说明
终端节点（Endpoint）	终端节点可以与终端节点服务相关联，以建立VPC通过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。
终端节点网卡（Endpoint ENI）	终端节点网卡是终端节点访问终端节点服务的入口。
终端节点安全组（Endpoint Security Group）	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。
终端节点服务（Endpoint Service）	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。终端节点服务由服务提供方创建和管理。
服务资源（Service Resources）	服务资源是终端节点服务中可以被终端节点访问的资源。 ❓ 说明 - 终端节点支持将负载均衡作为服务资源，包括传统型负载均衡 CLB（Classic Load Balancer）和应用型负载均衡ALB（Application Load Balancer）。 - 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。

术语	说明
服务白名单 (Service Whitelist)	服务白名单可以控制允许访问服务资源的用户范围。 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访问服务，您需要将该阿里云账号ID添加到服务白名单中。
终端节点连接 (Endpoint Connection)	终端节点与终端节点服务之间建立的连接。

私网连接服务概述

私网连接主要包含服务使用方和服务提供方的相关组件。

相关主体	相关组件
服务使用方	● 终端节点 ● 终端节点可用区和网卡 ● 终端节点安全组
服务提供方	● 终端节点服务 ● 服务资源 ● 服务白名单 ● 终端节点连接

私网连接开通时不产生费用。开通成功后，根据私网连接服务的实际使用量进行计费，按每小时出账。费用包含实例费和流量处理费。更多信息，请参见[计费说明](#)。

私网连接的服务使用方和服务提供方可以是不同的阿里云账号，私网连接也支持将所产生的费用归入服务使用方或者服务提供方的账号进行出账。更多信息，请参见[付费方说明](#)。

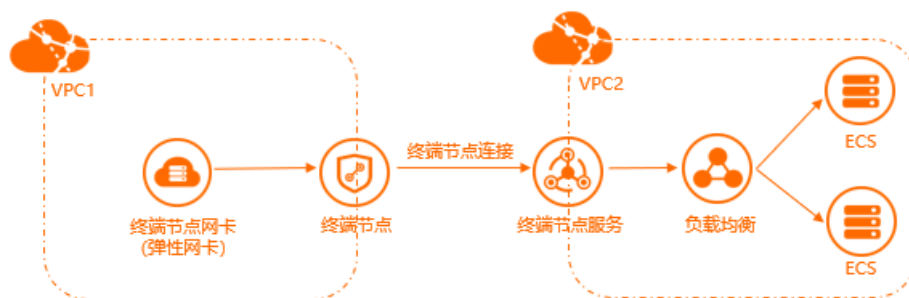
应用场景

私网连接能够实现终端节点所在的VPC与阿里云上的终端节点服务建立安全稳定的私有连接，配置灵活，可以满足不同的应用场景。

将VPC内的云服务共享给其他VPC

您可以使用私网连接服务将一个VPC内的负载均衡服务资源共享给另外一个VPC，实现跨VPC私网访问负载均衡服务资源。

如下图所示，要实现在VPC1中的终端节点私网访问VPC2中部署的负载均衡服务资源，您需要将负载均衡作为服务资源加入到终端节点服务中，然后在VPC1中创建连接该服务的终端节点，实现通过终端节点私网访问负载均衡服务资源。



将VPC内的云服务共享给本地数据中心

您可以使用私网连接服务将一个VPC内的负载均衡的服务资源共享给本地数据中心，实现云下私网访问云上负载均衡服务资源。

如下图所示，要实现在本地数据中心私网访问VPC2中部署的负载均衡服务资源，您需要先将VPC2内的负载均衡服务资源共享给VPC1，然后通过专线、VPN网关或智能接入网关将本地数据中心与VPC1连接起来，实现本地数据中心私网访问云上负载均衡服务资源。



产品优势

- 私网通信

通过私网连接访问终端节点服务，访问流量均在阿里云内网转发，不会通过公网，避免了通过公网访问服务带来的潜在安全风险。

- 安全可控

通过私网连接访问云服务，可以对VPC网络中用于访问服务的弹性网卡添加安全组规则，提供更强的安全保障和控制手段。

- 低延迟和高质量

通过私网连接访问云服务，访问请求会在同可用区内转发，提供最优延时方案。

- 管理简单

灵活的跨账号和跨VPC服务访问方式，避免复杂的路由和安全配置。

2.使用场景

本页面后期将不再维护并下线。更多信息，请参见[应用场景](#)。

3.基本概念

本页面后期将不再维护并下线。更多信息，请参见[基本概念](#)。

4.使用限制

使用私网连接（PrivateLink）功能前，请了解终端节点服务和终端节点的使用限制。

终端节点服务限制

资源	限制	提升配额
单个账号可创建的终端节点服务的数量	100	提交工单
单个终端节点服务可添加的服务资源的数量	500	
单个终端节点服务可添加的服务资源的可用区数量	5	
单个终端节点服务在每个可用区可添加的服务资源的数量	100	
终端节点服务后端服务资源支持的资源类型	专有网络类型且支持PrivateLink功能的负载均衡实例	无法调整
终端节点服务支持的流量	IPv4流量	
终端节点服务支持的协议	TCP协议和UDP协议	

终端节点限制

资源	限制	提升配额
单个账号可创建的终端节点数量	500	提交工单
单个专有网络可创建的终端节点数量	50	
单个终端节点可创建的可用区数量	5	
单个终端节点网卡可支持的带宽	1 Gbps	提交工单，可申请的终端节点网卡最大带宽为10 Gbps
单个终端节点在每个可用区中的弹性网卡数量	1	无法调整
终端节点支持的流量	IPv4流量	
终端节点支持的协议	TCP协议和UDP协议	

5.支持私网连接的地域和可用区

您可以通过私网连接（PrivateLink）访问阿里云上的服务，避免通过公网访问服务带来的潜在安全风险。

地域和可用区

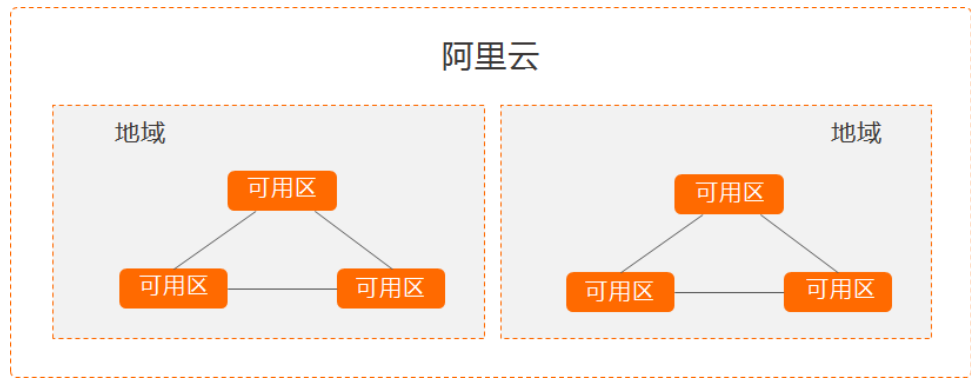
地域是指物理的数据中心。资源创建成功后不能更换地域。而可用区（Availability Zone，简称AZ）是指在同一地域内，电力和网络互相独立的物理区域。同一可用区内实例之间的网络延时更小。

在同一地域内可用区与可用区之间内网互通，可用区之间能做到故障隔离。是否将实例放在同一可用区内，主要取决于对容灾能力和网络延时的要求。

- 如果您的应用需要较高的容灾能力，建议您将实例部署在同一地域的不同可用区内。
- 如果您的应用要求实例之间的网络延时较低，建议您将实例部署在同一可用区内。

每个地域完全独立。每个可用区完全隔离，但同一个地域内的可用区之间使用低时延链路相连。

地域和可用区之间的关系如下图所示。



支持私网连接的地域和可用区

说明 下表中的地域和可用区仅供参考，具体地域和可用区请以购买页为准。

地域	可用区
华东1（杭州）	可用区B、可用区E、可用区F、可用区G、可用区H、可用区I、可用区J、可用区K
华东2（上海）	可用区B、可用区E、可用区F、可用区G、可用区L、可用区M、可用区N、可用区I、可用区H
华东5（南京-本地地域）	可用区A
华北1（青岛）	可用区B、可用区C
华北2（北京）	可用区B、可用区C、可用区D、可用区E、可用区F、可用区G、可用区H、可用区I、可用区K、可用区L
华北3（张家口）	可用区A、可用区B、可用区C
华北5（呼和浩特）	可用区A、可用区B

地域	可用区
华北6（乌兰察布）	可用区A、可用区B、可用区C
华南1（深圳）	可用区D、可用区E、可用区F
华南2（河源）	可用区A、可用区B
华南3（广州）	可用区A
西南1（成都）	可用区A、可用区B
中国（香港）	可用区B、可用区C、可用区D
日本（东京）	可用区A、可用区B
新加坡	可用区A、可用区B、可用区C
澳大利亚（悉尼）	可用区B
马来西亚（吉隆坡）	可用区A、可用区B
印度尼西亚（雅加达）	可用区A、可用区B、可用区C
德国（法兰克福）	可用区A、可用区B
英国（伦敦）	可用区A、可用区B
美国（硅谷）	可用区A、可用区B
美国（弗吉尼亚）	可用区A、可用区B
印度（孟买）	可用区A、可用区B

常见问题

私网连接（PrivateLink）是否支持跨地域连接？

不支持。