Tencent Cloud

Private Link

Getting Started

Product Documentation

Getting Started

Last updated：2023-11-28 16:41:35

This document guides you through the steps to create a private link and share the cloud services deployed in your VPC with other VPCs in the same region under the same account.

Overview

VPCs are your own private network resources on the cloud, and they are isolated from each other by default. With Private Link, you can establish secure and stable connection between Tencent Cloud VPCs to simplify the network architecture, and avoid security risks caused by public network access.
A Private Link connection involves a VPC endpoint and an endpoint service. To create an endpoint service, you need to create a private L4 CLB instance and create a listener to associate with the CVM instance where your service is deployed. Then, associate the endpoint service with the CLB instance when creating the service. The endpoint service serves as the service entry point of the service provider. The service consumer initiates a connection request from their VPC endpoint, After the connection is established, the service consumer can access the resources deployed by the service provider.

Sample Scenario

Assume that a company deploys their applications in VPC2, and hopes to share the resources in VPC2 with VPC1 owned by another account. To avoid security risks caused by public network access, they decide to connect VPC1 and VPC2 over the private network using Tencent Cloud Private Link.
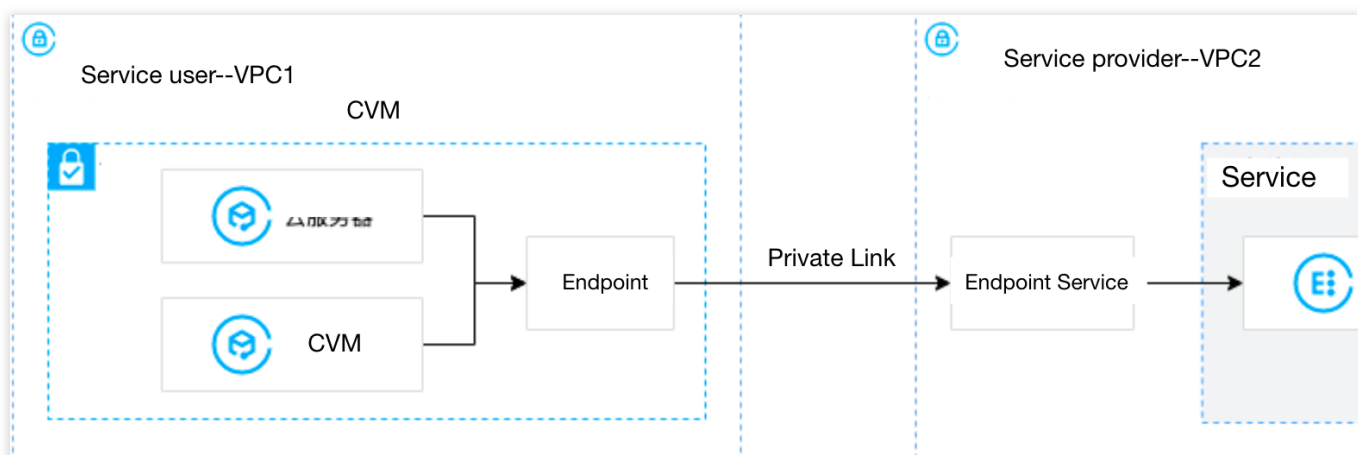
Prerequisites

Create VPC2 (service provider) and VPC1 (service consumer). For details, see Creating a VPC.

Create a private L4 CLB instance in VPC2. Deploy related service resources on the backend CVM of the CLB. Ensure that the backend CVM can process requests forwarded by the CLB instance normally. For details, see Getting Started with CLB.

****Please ensure that the IP range 11.163.0.0/16 is allowed in the security group associated with the backend CVM of CLB in VPC2.** For details, see Adding Security Group Rules.

Directions

Step 1. (Service provider) Create an endpoint service

Note

In this example, a private network Layer-4 CLB instance has been created in VPC2, relevant service resources have been deployed in the CLB backend CVM instance, and the IP range 11.163.0.0/16 is allowed in the security group associated with the CVM instance.

1. Log in to the VPC console.

2. Click **Private Link** > **VPC Endpoint Service** in the left sidebar.

3. Click **Create** to configure the relevant parameters.

Name	Description
Service name	The custom name of the endpoint service.
Region	The region where the endpoint service is located.
Network	Select the VPC. In this example, VPC2 is selected.
Load balancing	Select a CLB instance in the related VPC. In this example, select the CLB instance in VPC2.
Accept endpoint connection requests	Specify whether the endpoint service automatically accepts the connection requests initiated by endpoints. In this example, **No** is selected. **Yes**: The endpoint service accepts requests from all connected endpoints by default. After an endpoint is successfully created, it is in **Available** status. **No**: The connection status of the endpoint is **Pending**. You need to manually **Accept** the request to make the connection available.

4. After setting the parameters, click **OK**.

Step 2. (Service consumer) Create an endpoint

Note

In this example, the two VPCs are under the same account, so there is no need to add the account of the service consumer to the allowlist. If the VPCs are owned by different accounts, the service provider needs to get the account UIN of the service consumer, and add it to the allowlist. For details, see Sharing Services Between VPCs of Different Accounts.

1. Click **VPC Endpoint** in the left sidebar.

2. Click **Create** to configure relevant parameters.

Parameter	Description
Name	The custom name of the endpoint.
Region	The region where the endpoint is located.
Network	Select the VPC where the endpoint is located. In this example, VPC1 is selected.
Subnet	Select the subnet of the endpoint.
IP address	IP address of the endpoint. You can specify an IP address in VPC1, or get an auto-assigned IP.
Peer account type	Select the account to which the endpoint service to be connected belongs. In this example, we select **My account**: For access between VPCs under the same account, select **My account**. For access between VPCs under different accounts, select **Other Tencent Cloud account**.
Service type	Enter the endpoint service ID and click **Verify**. Connections can only be established for verified services.

3. When the parameters are configured, click **OK**. In Step 1 of this example, **Yes** is set for the endpoint service, that is, the endpoint service accepts connection requests from all connected endpoints by default. When the endpoint is created, the status is **Available**.

Step 3. (Service consumer) Verify the connection

1. Log in to a CVM in VPC1 and access the backend service of the service provider through VIP+VPORT.

2. In this example, we use telnet to verify the connection. Run telnet *VIP VPORT*.

If the following message appears, the connection is succeeded.

Note

If the connection is abnormal, record the configuration information and contact us immediately.

If telnet is not installed, run `yum install telnet` to install it first.

```
[root@VM-2-15-centos ~]# telnet 172.16.2
Trying 172.██ ██ .16...
Connected to 172. █ .16.
Escape character is '^]'.
```