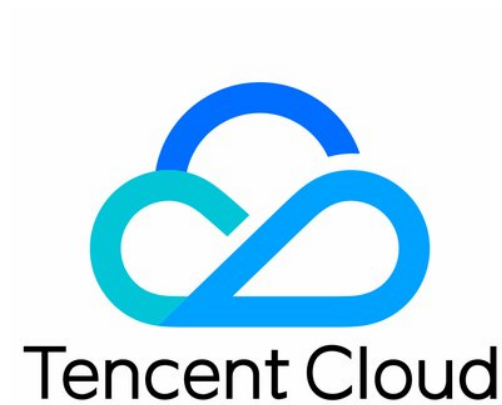


Private Link Best Practice



Copyright Notice

©2013–2023 Tencent Cloud. All rights reserved.

Copyright in this document is exclusively owned by Tencent Cloud. You must not reproduce, modify, copy or distribute in any way, in whole or in part, the contents of this document without Tencent Cloud's the prior written consent.

Trademark Notice



All trademarks associated with Tencent Cloud and its services are owned by Tencent Cloud Computing (Beijing) Company Limited and its affiliated companies. Trademarks of third parties referred to in this document are owned by their respective proprietors.

Service Statement

This document is intended to provide users with general information about Tencent Cloud's products and services only and does not form part of Tencent Cloud's terms and conditions. Tencent Cloud's products or services are subject to change. Specific products and services and the standards applicable to them are exclusively provided for in Tencent Cloud's applicable terms and conditions.

Contents

Best Practice

Cross-Region VPC Service Sharing

Cross-Account VPC Service Sharing

Best Practice

Cross-Region VPC Service Sharing

Last updated: 2023-08-31 22:06:25

If your cloud services deployed in a VPC need to be shared with VPCs in other regions, you can use Private Connection and Cloud Connect Network services.

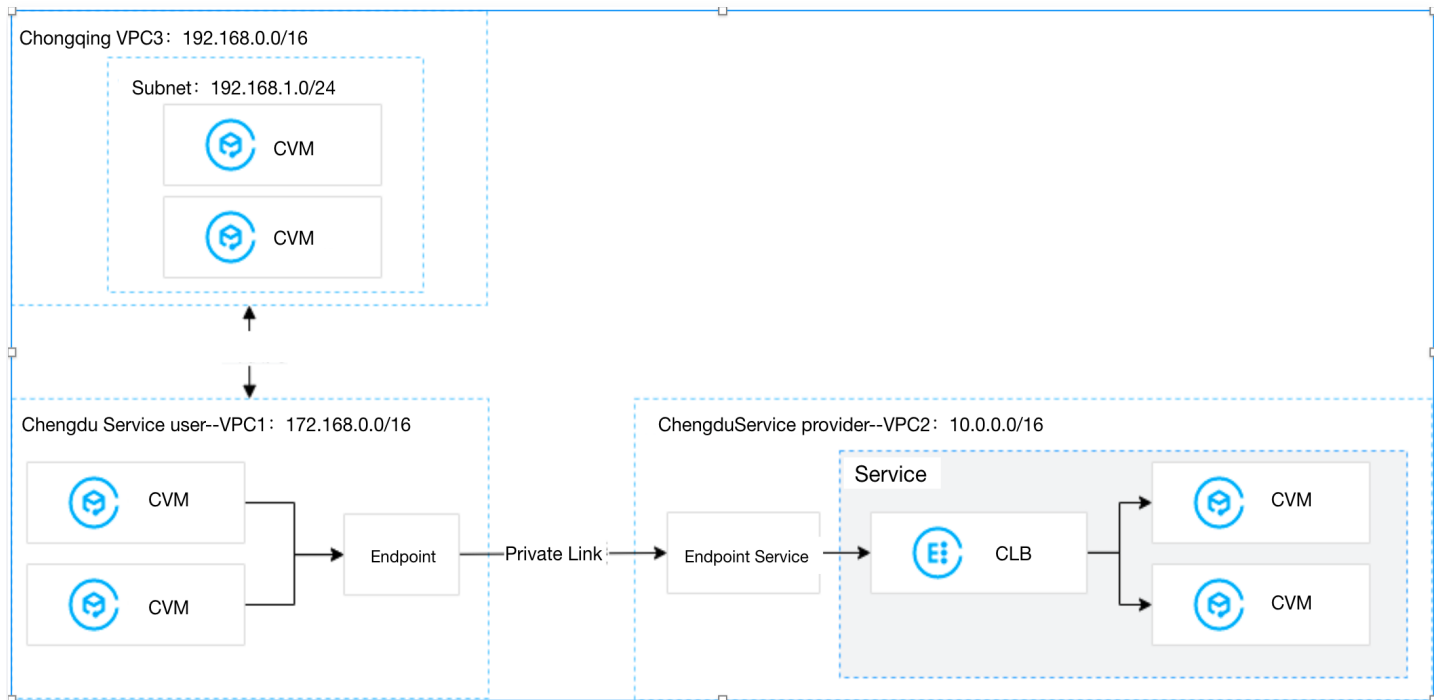
Background Information

A Virtual Private Cloud (VPC) is your exclusive cloud-based network, and different VPCs are completely isolated by default. You can use Private Link service to establish secure and stable connections between Tencent Cloud VPCs and other VPCs in the same region, simplifying network architecture and avoiding potential security risks associated with public network access. If you need to share VPC services across regions, you can use Cloud Connect Network to enable cross-regional VPC communication, and then use the Private Link service with the endpoint in the consumer VPC to access services in the provider VPC.

To use Private Link, you need to create an Endpoint Service and an Endpoint. Before creating the Endpoint Service, you need to create an internal Layer 4 Cloud Load Balancer instance and a listener associated with the Cloud Virtual Machine instance where your service is deployed. Then, when creating the Endpoint Service, associate it with the Cloud Load Balancer instance. At this point, the Endpoint Service will serve as the access point for the service provider's business, allowing the consumer to create an Endpoint to request a connection. Once the connection is established, the service consumer can access the business services deployed by the service provider.

Scenario Example

In this document, we will use the following business scenario as an example. A company has its services deployed in the Chengdu region's VPC2 and needs to share these services with clients in the same region's VPC1 network and the Chongqing region's VPC3 network. To avoid potential security risks associated with public network access, Tencent Cloud Private Link and Cloud Connect Network are used to implement this communication solution.



Note

This article assumes that the three VPCs are under the same account.

Preparations

- Service provider VPC2 and service consumer VPC1 have been created, as well as cross-regional service consumer VPC3.
- In the service provider's VPC2, an internal Layer 4 CLB instance has been created, and related service resources are deployed in the backend Cloud Virtual Machine instances. Please ensure that the backend Cloud Virtual Machine instances can properly handle requests forwarded by the Cloud Load Balancer. For more information, refer to the [Cloud Load Balancer Quick Start Guide](#).
- Please ensure that the security group associated with the Cloud Virtual Machine in the service provider's VPC2 has allowed the 11.163.0.0/16 address range, as shown in the following diagram.

Add rule

Import rule

Sort by priority

Edit all

Delete

Open all common ports

How to Set

Separate keywords with "|"; press Enter to separate filter

Q

↓

<input type="checkbox"/> Source ⓘ	Protocol+Port ⓘ	Policy	Remark	Modification time	Operation
<input type="checkbox"/> 11.163.0.0/16	ALL	Allow		2023-08-25 16:13:08	Edit Insert Delete

Instructions

Step 1: Service provider creates an Endpoint Service

Note

In this example, the service provider's VPC2 has created a Layer 4 private network CLB, with the backend Cloud Virtual Machine instances already deployed with the relevant business services. The security group of the Cloud Virtual Machine instances has allowed the 11.163.0.0/16 IP address range.

1. Log in to the [Virtual Private Cloud Console](#).
2. Click **Private Link** > **Endpoint Services** in the left sidebar.
3. Click **Create**, and in the pop-up window for creating a new Endpoint Service, configure the relevant parameters.


Create VPC endpoint service

Service name


Region

Southwest China (Chengdu)


Network

Please select 

Service type

Please select 

Backend instance

Please select 

Accept endpoint connection request

☒ No ☐ Yes

OK

Cancel

Parameter name	Description
----------------	-------------

Service name	Customize the Endpoint Service name.
Region	Endpoint service region.
Network	Select the associated VPC; in this example, choose VPC2.
Cloud Load Balancer	Select the Cloud Load Balancer instance that has been created in the VPC. In this example, choose the CLB instance already created in VPC2.
Accept endpoint connection request	<p>Specify whether the Endpoint Service will or will not automatically accept connection requests initiated by the Endpoint. In this example, we choose yes:</p> <ul style="list-style-type: none">• When Yes is selected for automatic acceptance, the Endpoint Service will accept all connection requests from Endpoints by default. After the Endpoint is created successfully, its status will be Available.• When selecting No for not accepting automatic connections, the Endpoint connection status will be Pending Acceptance. The Endpoint Service needs to manually perform Accept Connection to change the status from Pending Acceptance to Available.

4. After completing the parameter settings, click **OK** to finish creating the Endpoint Service.

Step 2: Service consumer creates a VPC endpoint

Note

In this example, the access is between VPCs under the same account, so there is no need to add the service consumer's whitelist account in the Endpoint Service. If it is a cross-account VPC access, the service consumer needs to inform the service provider of their UIN account in advance. The service provider's Endpoint Service should add the whitelist first, and then proceed with this step. For more information, see [Service Sharing between Cross-Account VPCs](#).

1. In the left sidebar, click **Endpoint**.
2. Click **Create** and, in the pop-up window for creating a new Endpoint, configure the relevant parameters.

Create VPC endpoint

Name

Region

Southwest China (Chengdu)

Network

Please select

Subnet

Please select

IP address

Automatic assignment

Get an auto-assigned IP

Service type

☒ Custom service

Destination account type

☒ My account ☐ Other Tencent Cloud Account

Enter the endpoint node service ID, such as vpcs

Verify

OK

Cancel

Parameter name	Description
Name	Specify a custom name for the endpoint.
Region	Endpoint node region.
Network	Select the VPC where the Endpoint is located; in this example, choose VPC1.
Subnet	Select the subnet where the Endpoint is located.
IP Addresses	Endpoint IP address: You can specify an IP address, which should be a private IP within VPC1, or you can choose to have the IP address automatically assigned.
Destination	Select the account to which the Endpoint Service to be connected belongs. In this example, choose My Account : <ul style="list-style-type: none">For access between VPCs under the same account, select My

account type	Account. <ul style="list-style-type: none">For cross-account VPC access, select Other Account.
Select a service	Enter the endpoint node service ID and click Verify ; only verified services can establish a connection.

3. After completing the parameter configuration, click **Confirm**. In this example, since the Endpoint Service in [Step 1](#) is set to automatically accept connections, it will accept connection requests from all Endpoints by default. Therefore, once the Endpoint is created successfully, its status will be **Available**.

ID/Name	Monitoring	Status	Network	Subnet	IP address	Elastic IP	Service	Operation
VPC8-vpc-00000001 test-...		Available	vpc-...	subnet-...	10.0.0.11	-	vpcsvc-...	Delete

Step 3: Create a Cloud Connect Network to connect VPC3 and VPC1 networks

- Log in to the [CCN console](#).
- Click **Create** to create a Cloud Connect Network instance, associate cross-regional VPC1 and VPC3, and click **Confirm** to enable interconnectivity between VPC1 and VPC3.

Create CCN instance

Name

Up to 60 characters ([a-z], [A-Z], [0-9], [-_] and Chinese characters).

Bandwidth billing mode ⓘ

☐ Monthly subscription ☒ Pay-as-you-go by monthly 95th percentile

The default bandwidth cap is 1 Gbps. It's billed based on the actual bandwidth usage of the current month on a [95th percentile basis](#)

Service level ⓘ

☐ Platinum ⓘ ☐ Gold ⓘ ☐ Silver ⓘ

Bandwidth limit mode ⓘ

☒ Inter-region bandwidth cap

Description

Optional

Associated to

Virtual Private Cloud ▼

Please select ▼

Search for VPC name or ID ▼

Remarks (Optional) ✕

[Add](#)

Advanced options ▶

Fee

Network connections fee ⓘ

Chinese mainland ⓘ

Outside Chinese mainland ⓘ

Inbound traffic process fee ⓘ

1. To purchase bandwidth packages, please complete the creation. Then go the details page of the instance and select <1>Bandwidth Management</1>.

2. Make sure that your account balance is enough. Otherwise the resource may be isolated or the data transfer speed is limited.

3. Starting from now till April 1, 2024, a free tier of two network instances and 100 TB/month of inbound traffic is provided for each account.

For more information, see [Billing Overview](#) [Expiration Reminder](#)

☒ Read and Agreed [Cross-Region Internet Service Agreement](#)

OK

Close

Note

For more detailed information, please see [Getting Started with Cloud Connect Network](#).

Step 4: Service consumer initiates access request to verify the connection

- Verify that the service consumer VPC1 in Chengdu region can access VPC2:

- a. Log in to a CVM in the service consumer's VPC1 and access the service provider's backend services using VIP + VPORT.
- b. In this example, use telnet to verify connectivity by running *telnet VIP VPORT*.

Note

If the server does not have telnet installed, please run `yum install telnet` to install telnet first.

Obtain the Endpoint VIP:

VPC endpoint Chengdu All VPCs Help of VPC endpoint

Private Link has been commercialized since August 15, 2022 with the price of 0.07CNY/instance/hour and 0.07CNY/GB. [Learn more](#)

Create ID/Name Q + -

ID/Name	Monitoring	Status	Network	Subnet	IP address	Elastic IP	Service	Operation
vpc-		Available	vpc-	subnet-	10.0.1.1	-	vpcsvc-	Delete

Obtain the CLB VPort:

HTTP/HTTPS listener(Configured1)

Create

+

80(HTTP:80)

+

Click the left node to view details

If the following message is returned, it indicates a successful access:

```
[root@VM-2-15-centos ~]# telnet 172.16.2.16 1044
Trying 172.16.2.16...
Connected to 172.16.2.16.
Escape character is '^['.
```

- Verify that VPC3 in Chongqing region accesses the service provider VPC2 through the endpoint in the service consumer VPC1 in Chengdu region:
 - a. Log in to a CVM under VPC3 and access the service provider's backend service via VIP + VPORT. The VIP is the one obtained from the Endpoint in VPC1, in this case, 172.16.2.16, and the VPORT is the listener port of the CLB in VPC2, which is 1044 in this example.

b. Continue using telnet to verify connectivity by executing *telnet VIP VPORT*.

ⓘ **Note**

If the server does not have telnet installed, please run `yum install telnet` to install telnet first.

The following message indicates a successful access:

```
Add rule</a> |                         | <a href="#">Import rule</a>                                                             | <a href="#">Sort by priority</a> | <a href="#">Edit all</a> | <a href="#">Delete</a> | <a href="#">Open all common ports</a> <a href="#">How to Set</a>   |
|                          |                         | <input type="text" value="Separate keywords with ' '; press Enter to separate filter"/> |                                  |                          |                        |                                                                    |
| <input type="checkbox"/> | Source <small>i</small> | Protocol+Port <small>i</small>                                                          | Policy                           | Remark                   | Modification time      | Operation                                                          |
| <input type="checkbox"/> | 11.163.0.0/16           | ALL                                                                                     | Allow                            |                          | 2023-08-25 16:13:08    | <a href="#">Edit</a> <a href="#">Insert</a> <a href="#">Delete</a> |

## Instructions

### Step 1: Service provider creates an Endpoint Service

#### Note

In this example, the service provider's VPC2 has created a Layer 4 private network CLB, with the backend Cloud Virtual Machine instances already deployed with the relevant business services. The security group of the Cloud Virtual Machine instances has allowed the 11.163.0.0/16 IP address range.

1. Log in to the [Virtual Private Cloud Console](#).
2. Click **Private Link** > **Endpoint Services** in the left sidebar.
3. Click **Create**, and in the pop-up window for creating a new Endpoint Service, configure the relevant parameters.

### Create VPC endpoint service ✕

Service name

Region

South China (Guangzhou)

Network

Please select ▼

Service type

Please select ▼

Backend instance

Please select ▼

Accept endpoint connection request

☒ No ☐ Yes

OK

Cancel

| Parameter name                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Service name                       | Customize the Endpoint Service name.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Region                             | Endpoint Service Region.                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Network                            | Select the associated VPC; in this example, choose VPC2.                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cloud Load Balancer                | Select the Cloud Load Balancer instance that has been created in the VPC. In this example, choose the CLB instance already created in VPC2.                                                                                                                                                                                                                                                                                                                                                      |
| Accept endpoint connection request | <p>Specify whether the Endpoint Service <b>does</b> or <b>does not</b> automatically accept connection requests initiated by the Endpoint. In this example, we choose <b>not to</b> automatically accept requests.</p> <ul style="list-style-type: none"><li>When <b>Yes</b> is selected for automatic acceptance, the Endpoint Service will accept all connection requests from Endpoints by default. Once the Endpoint is successfully created, its status will be <b>Available</b>.</li></ul> |

- When selecting **No**, to not accept automatic connections, the Endpoint connection status will be **Pending Acceptance**. The Endpoint Service must manually perform **Accept Connection** to change the status from **Pending Acceptance** to **Available**.

4. After completing the parameter settings, click **OK** to finish creating the Endpoint Service.

## Step 2: Add Service Consumer Account to the Allowlist

1. Click **More > Manage User Allowlist** on the right side of the created Endpoint Service, or click the Endpoint Service ID to enter the **Allowlist** tab in the details page.
2. In the whitelist management interface, click on "Add".
3. In the pop-up dialog box, please enter the service consumer's UIN account and description information based on the actual situation, and click **OK**.

## Step 3: Service Consumer Creates an Endpoint

1. In the left sidebar, click **Endpoint**.
2. Click **Create** and, in the pop-up window for creating a new Endpoint, configure the relevant parameters.



### Create VPC endpoint

Name

test

Region

Southwest China (Chengdu)

Network

vpc-

✓

Subnet

subnet-

✓

IP address

Automatic assignment

Get an auto-assigned IP

Service type

☒ Custom service

Destination account type

☐ My account ☒ Other Tencent Cloud Account ✓

Destination account UIN

222222222 ✓

vpcsvc1

Verify

OK

Cancel

| Parameter name           | Description                                                                                                                                                                                                                                                                                                              |
|--------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Name                     | Specify a custom name for the endpoint.                                                                                                                                                                                                                                                                                  |
| Region                   | Endpoint Region                                                                                                                                                                                                                                                                                                          |
| Network                  | Select the VPC where the Endpoint is located; in this example, choose VPC1.                                                                                                                                                                                                                                              |
| Subnet                   | Select the subnet where the Endpoint is located.                                                                                                                                                                                                                                                                         |
| IP Addresses             | Endpoint IP address: You can specify an IP address, which should be a private IP within VPC1, or you can choose to have the IP address automatically assigned.                                                                                                                                                           |
| Destination account type | Select the account to which the Endpoint Service to be connected belongs. In this example, choose <b>Another Account</b> : <ul style="list-style-type: none"><li>For access between VPCs within the same account, select <b>My Account</b>.</li><li>For cross-account VPC access, select <b>Other Account</b>.</li></ul> |
|                          |                                                                                                                                                                                                                                                                                                                          |

Select a service

After entering the Endpoint Service ID, click Validate. Only validated services can establish a connection.

VPC endpoint service

Chengdu

All VPCs



Create

ID/Name

Monitoring

Network

Service type

Backend instance

vpcsvc



vpc-

Load balancing

lb-

3. After completing the parameter configuration, click **OK**. The current connection status of the Endpoint is **Pending Acceptance**.

VPC endpoint

Chengdu 5

All VPCs



Help of VPC endpoint

Private Link has been commercialized since August 15, 2022 with the price of 0.07CNY/instance/hour and 0.07CNY/GB. [Learn more](#)

Create



ID/Name

Monitoring

Status

Network

Subnet

IP address

Elastic IP

Service

Operation

1 result found [Back to list](#)

vpc-

test



Pending accepted

vpc-

subnet

172.17.0.7

-

vpcsvc-

endpointservice

Delete

Total items: 1

10 / page

1 / 1 page

## Step 4: Manage Endpoint Connection Requests

For cross-account connections, the service provider must accept the connection request initiated by the service consumer in order to establish communication.

1. Click **More > Manage Endpoint Connections** on the right side of the created Endpoint Service, or click the Endpoint Service ID to enter the **Endpoints** tab on the details page.
2. Click **Accept Connection**, and in the pop-up confirmation dialog, click **Confirm**.

VPC endpoint service

Basic information

Monitoring

VPC endpoint

Allowlist

Accept

Reject



ID/Name

Status

UIN

Creation time

Operation

vpc-




test

Available

-

2023-05-18 17:30:34

Reject connection requests

| ID/Name                                                                                                                                                                            | Status    | UIN                                                                               | Creation time       | Operation                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|-----------------------------------------------------------------------------------|---------------------|--------------------------------------------|
| vpce- <br>test-  | Available |  | 2023-05-18 17:30:34 | <a href="#">Reject connection requests</a> |

1. Log in to a CVM instance under the service consumer's VPC1 and access the service provider's backend services via VIP+VPORT.
2. In this example, telnet is used to verify connectivity by executing *telnet VIP VPORT*.

If the server does not have telnet installed, please run `yum install telnet` to install telnet first.

VPC endpoint

Chengdu 5

All VPCs

Help of VPC endpoint

Private Link has been commercialized since August 15, 2022 with the price of 0.07CNY/instance/hour and 0.07CNY/GB. [Learn more](#)

Create

ID/Name

| ID/Name                    | Monitoring | Status    | Network                    | Subnet                        | IP address | Elastic IP | Service                       | Operation |
|----------------------------|------------|-----------|----------------------------|-------------------------------|------------|------------|-------------------------------|-----------|
| <div>vpc</div> <div></div> |            | Available | <div>vpc</div> <div></div> | <div>subnet</div> <div></div> | 10.1.1.1   | -          | <div>vpcsvc</div> <div></div> | Delete    |

**HTTP/HTTPS listener**(Configured1)

Create

80(HTTP:80)

Click the left node to view details

Page 19 of 20

```
[root@VM-1-7-centos ~]# telnet 172.16.1.17 1044
Trying 172.16.1.17...
Connected to 172.16.1.17.
Escape character is '^]'.
```