Private Link
Best Practice

Contents

Best Practice
Cross-Region VPC Service Sharing

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

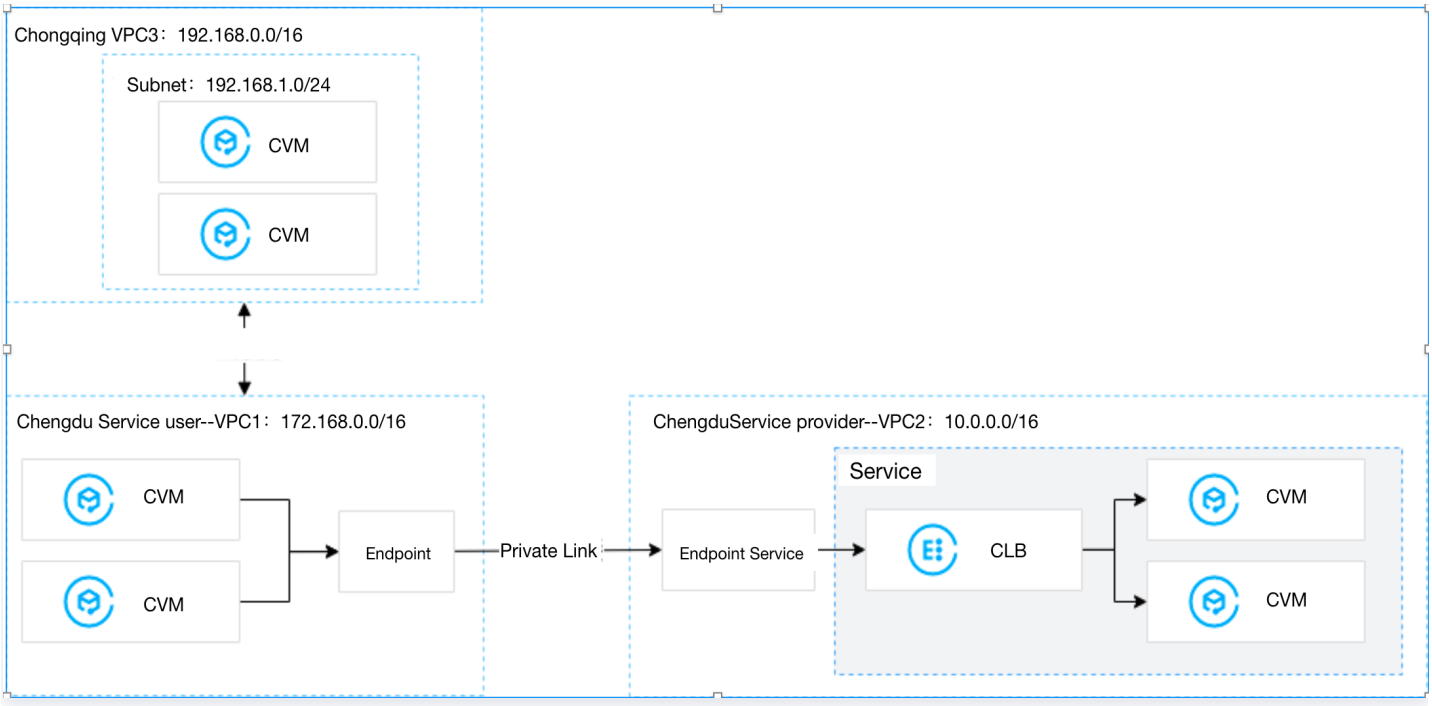
If your cloud services deployed in a VPC need to be shared with VPCs in other regions, you can use Private Connection and Cloud Connect Network services.

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.

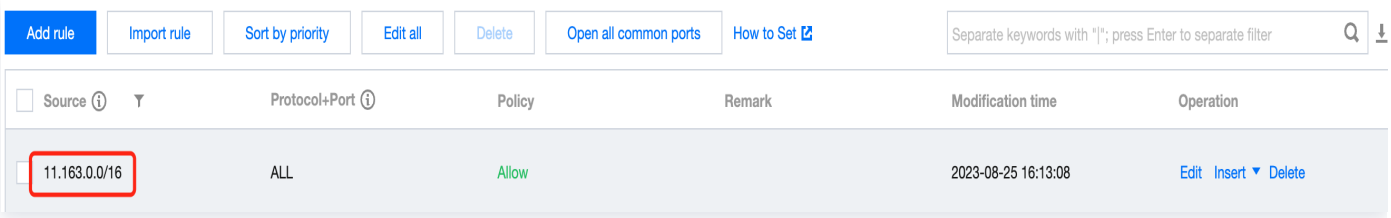


Note

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.

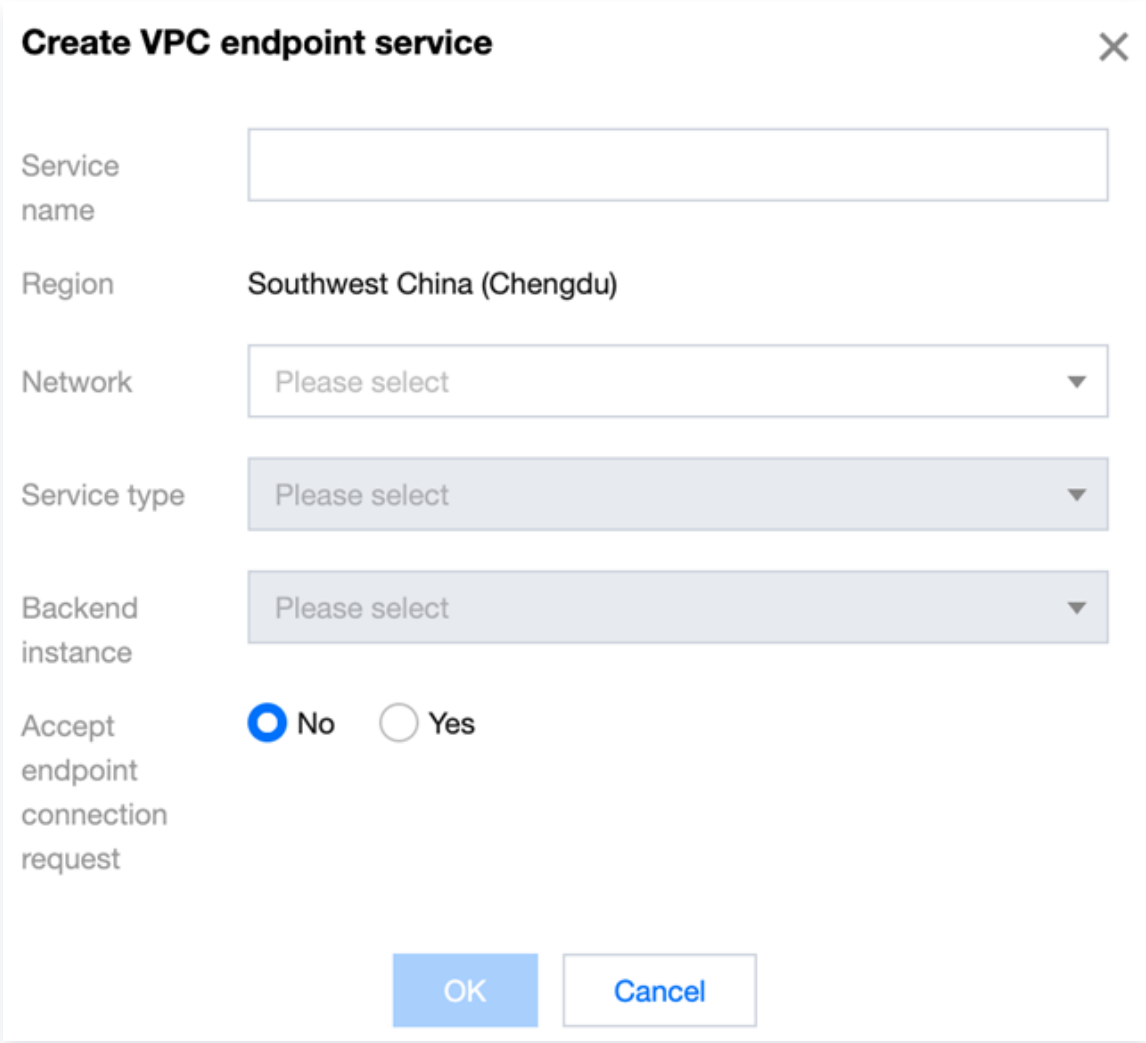


Instructions

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.



Parameter name	Description

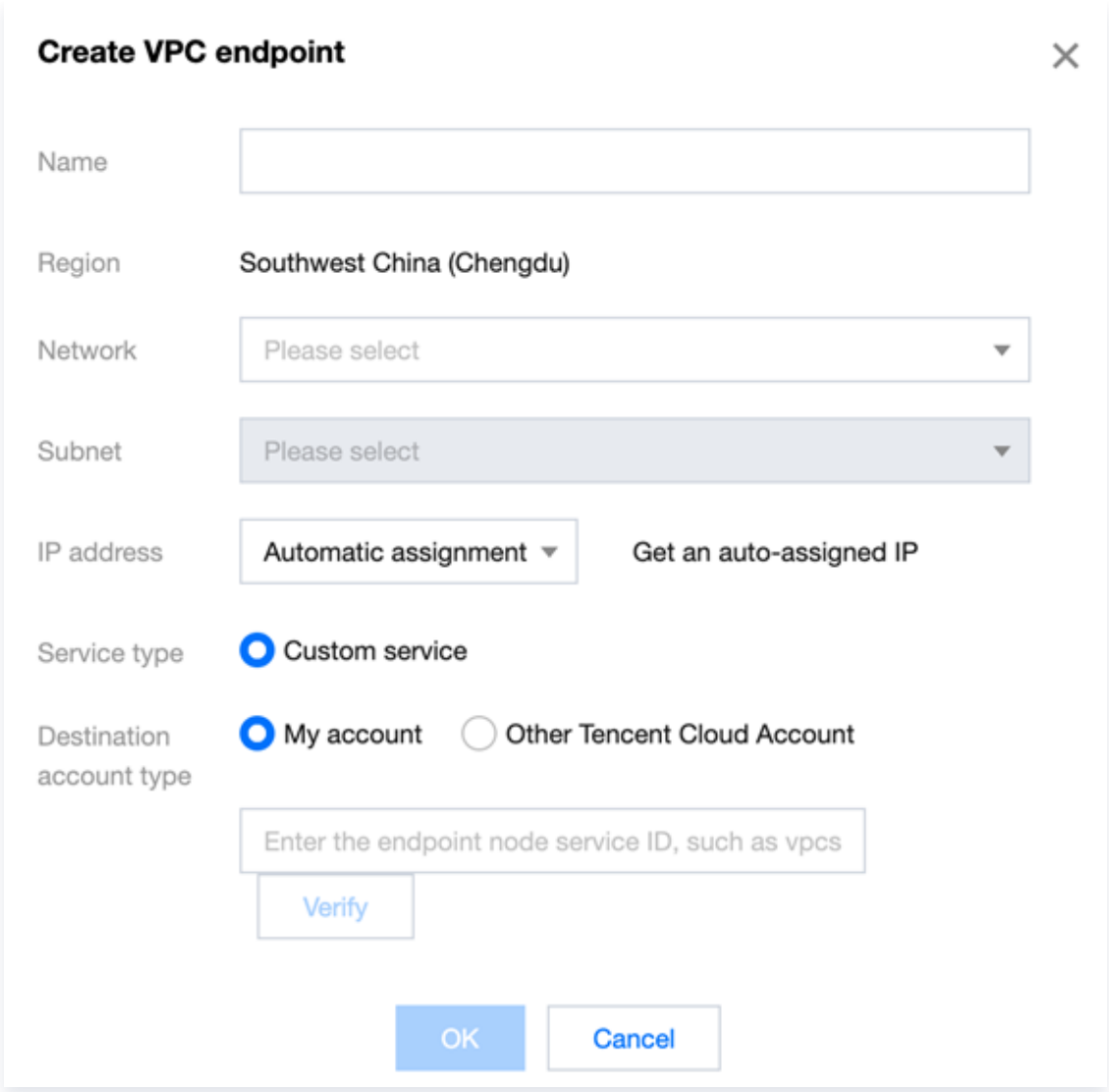
Service name	Customize the Endpoint Service name.
Region	Endpoint service region.
Network	Select the associated VPC; in this example, choose VPC2.
Cloud Load Balancer	Select the Cloud Load Balancer instance that has been created in the VPC. In this example, choose the CLB instance already created in VPC2.
Accept endpoint connection request	Specify whether the Endpoint Service **will** or **will not** automatically accept connection requests initiated by the Endpoint. In this example, we choose **yes**: • 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.

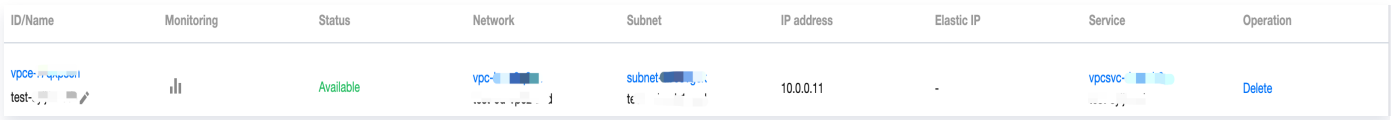
1. In the left sidebar, click **Endpoint**.
2. Click **Create** and, in the pop-up window for creating a new Endpoint, configure the relevant parameters.



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**: • For access between VPCs under the same account, select **My**

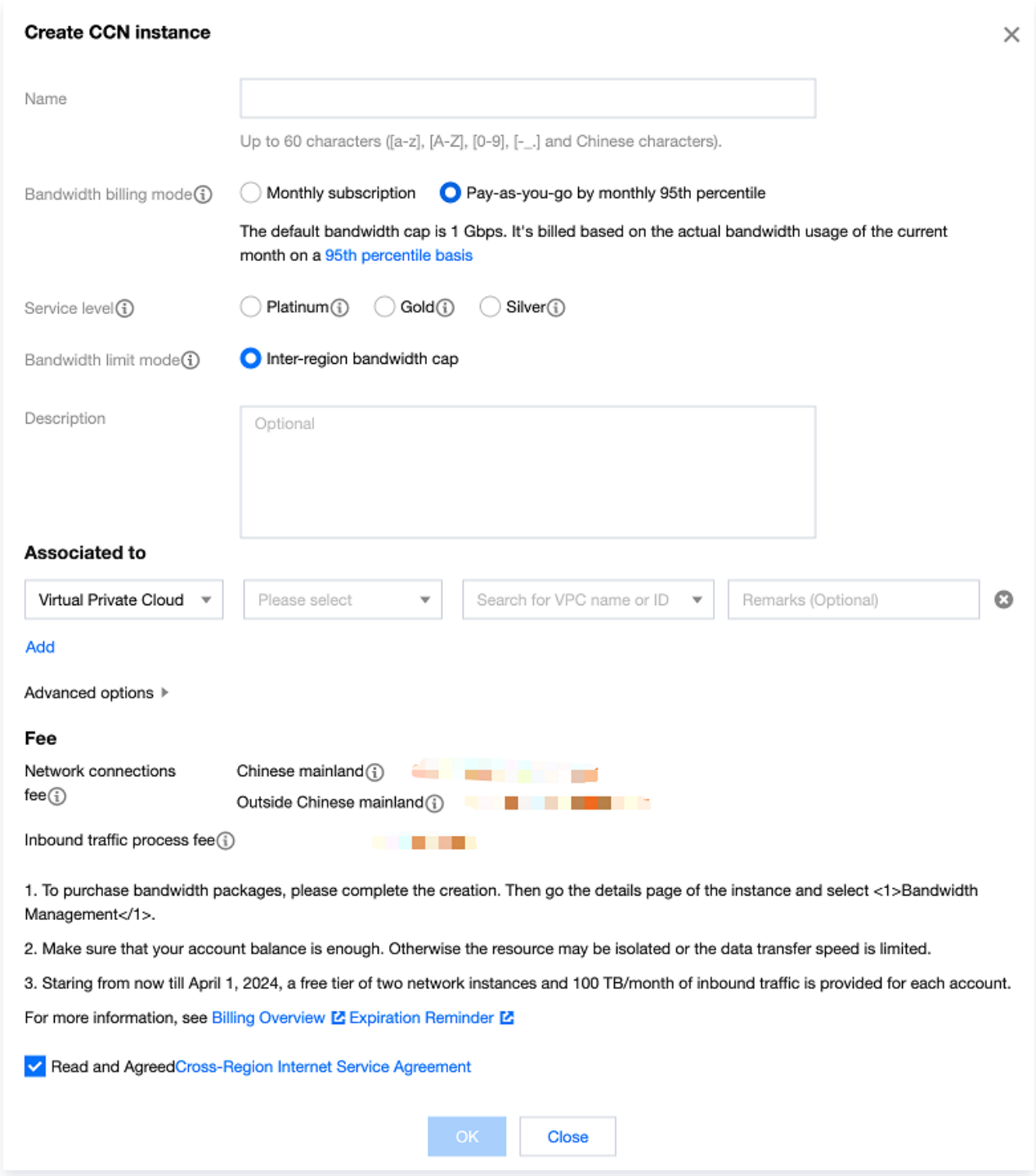
account type	**Account**. • For cross-account VPC access, select **Other Account**.
Select a service	Enter the endpoint node service ID and click **Verify**; only verified services can establish a connection.

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**.



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

1. Log in to the CCN console.
2. 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.



Note

For more detailed information, please see Getting Started with Cloud Connect Network.

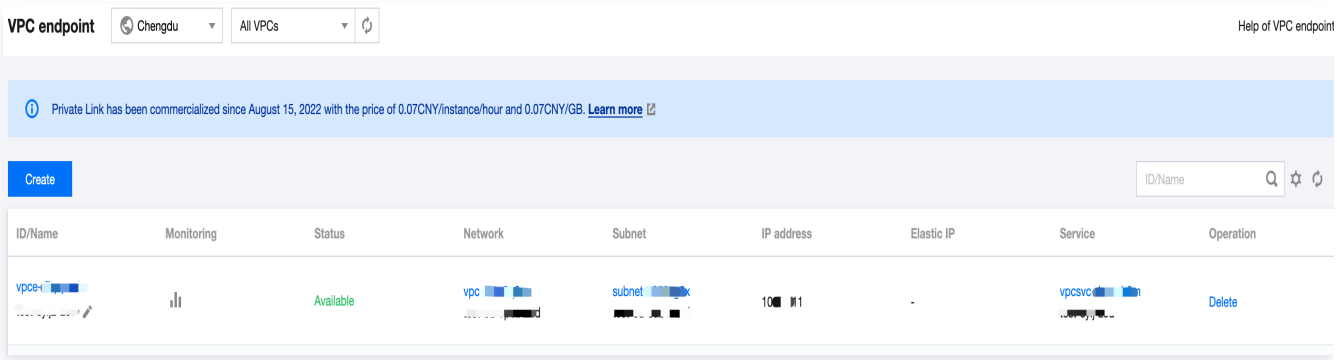
Step 4: Service consumer initiates access request to verify the connection

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

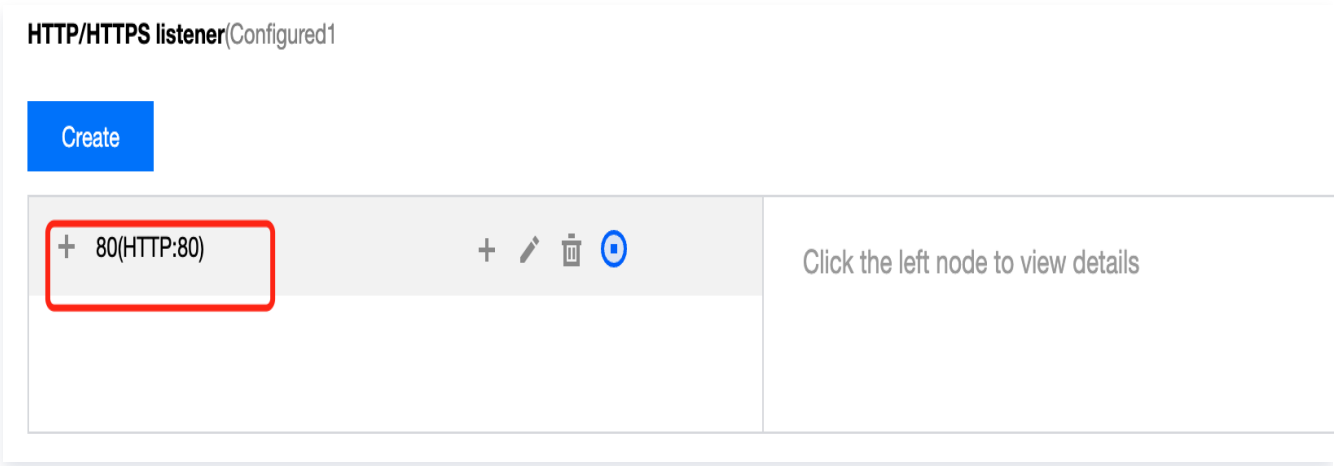
a. Log in to a CVM in the service consumer's VPC1 and access the service provider's backend services using VIP + VPORT.
b. In this example, use telnet to verify connectivity by running *telnet VIP VPORT*.

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

Obtain the Endpoint VIP:



Obtain the CLB VPort:



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:

```
<img src="https://main.qcloudimg.com/raw/2504940fd846c6cb3a37a8fd2b8812e
```

Cross-Account VPC Service Sharing

Last updated: 2023-09-02 01:31:04

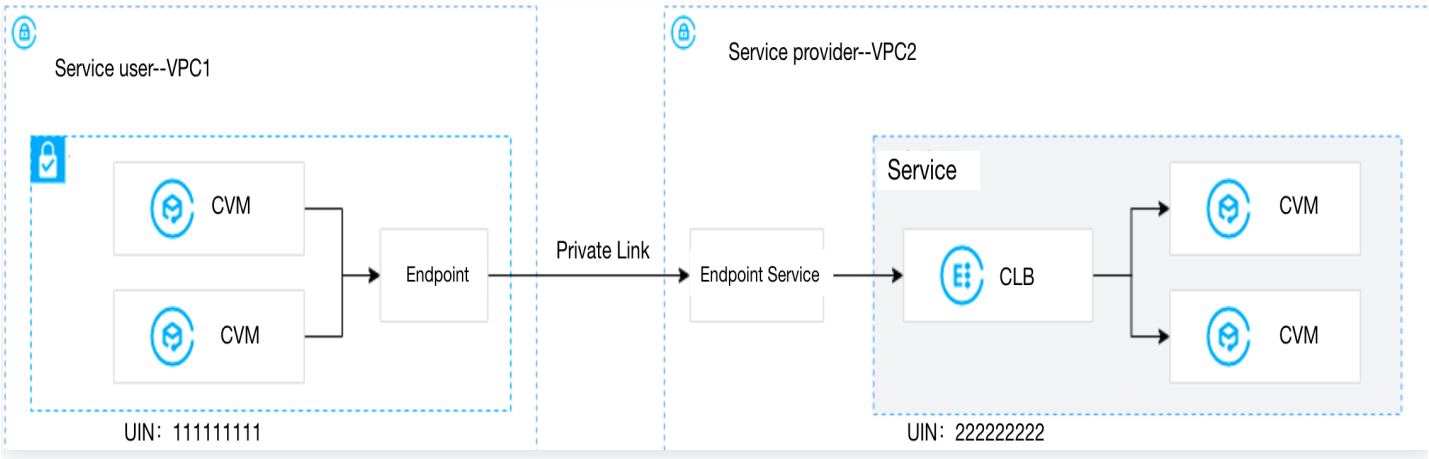
This guide will help you quickly create a Private Connection Service, allowing you to share cloud services deployed in your account's VPC with other accounts' VPCs for access.

Background Information

A Virtual Private Cloud (VPC) is your exclusive cloud-based Virtual Private Cloud, with complete isolation between different VPCs by default. By using Private Link Service, you can establish secure and stable access connections between Tencent Cloud VPCs and other VPCs, simplifying network architecture and avoiding potential security risks associated with public network access.
To establish a connection using Private Link, you need to create an Endpoint Service and an Endpoint. Before creating an Endpoint Service, you need to create an internal Layer 4 Cloud Load Balancer (CLB) instance and a listener associated with the deployed Cloud Virtual Machine (CVM) instance. Then, associate the CLB instance when creating the Endpoint Service. At this point, the Endpoint Service will serve as the access entry point for the service provider's business, allowing the service consumer's created Endpoint to request a connection. Once the connection is successfully established, the service consumer can access the service provider's deployed business services.

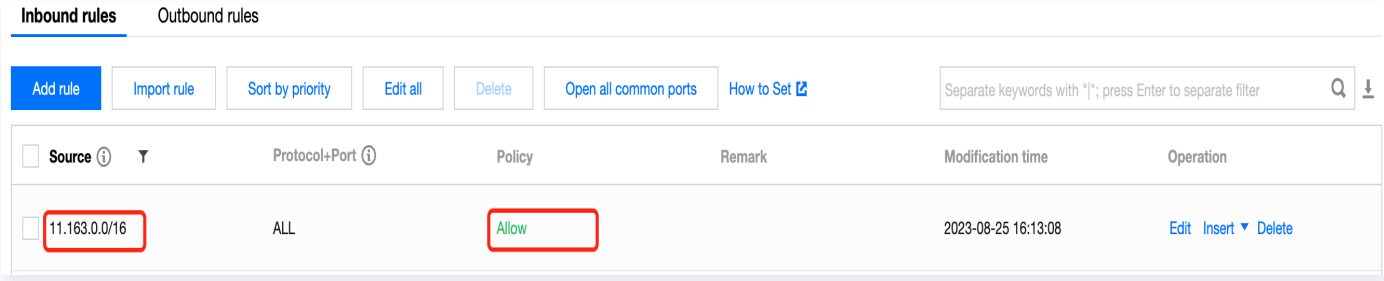
Scenario Example

In this guide, we will use the following business scenario as an example. A company has its business deployed in VPC2 and needs to share access to this business with other departments' VPC1 under different accounts within the company. To avoid potential security risks associated with public network access, Tencent Cloud's Private Link is used to implement a secure private network access solution from VPC1 to VPC2.



Preparations

- Service provider's VPC2 and service consumer's VPC1 have been created.
- The service consumer should provide their UIN account to the service provider, who will then add it to the allowlist to enable connectivity. Additionally, the service consumer should obtain the service provider's UIN account.
- 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.
- The service provider must inform the service consumer of the Cloud Load Balancer's VPORT in advance.
- **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.

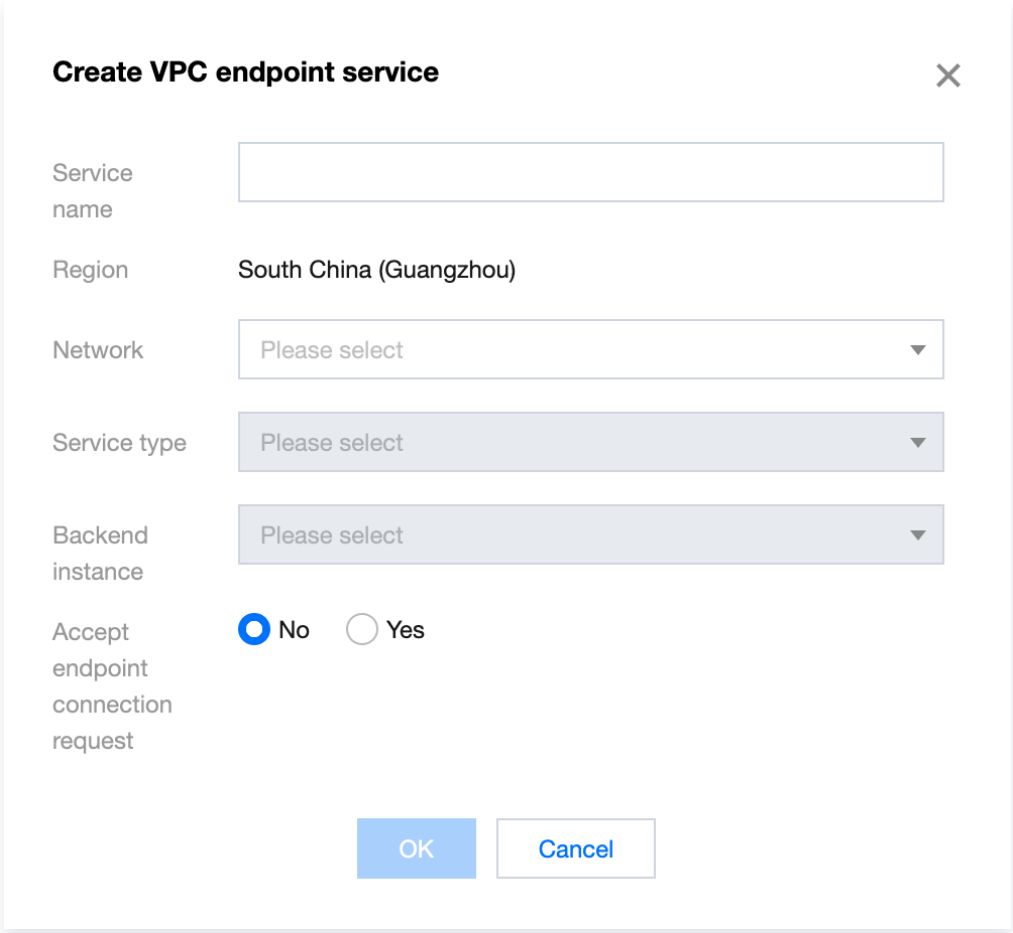


Instructions

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.



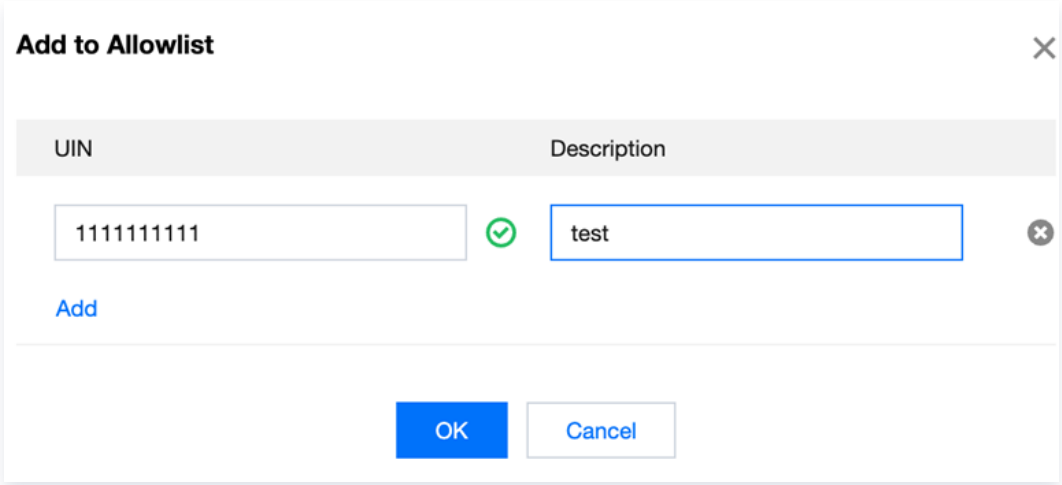
Parameter name	Description
Service name	Customize the Endpoint Service name.
Region	Endpoint Service Region.
Network	Select the associated VPC; in this example, choose VPC2.
Cloud Load Balancer	Select the Cloud Load Balancer instance that has been created in the VPC. In this example, choose the CLB instance already created in VPC2.
Accept endpoint connection request	Specify whether the Endpoint Service **does** or **does not** automatically accept connection requests initiated by the Endpoint. In this example, we choose **not to** automatically accept requests. • When **Yes** 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 **Available**.

- 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.

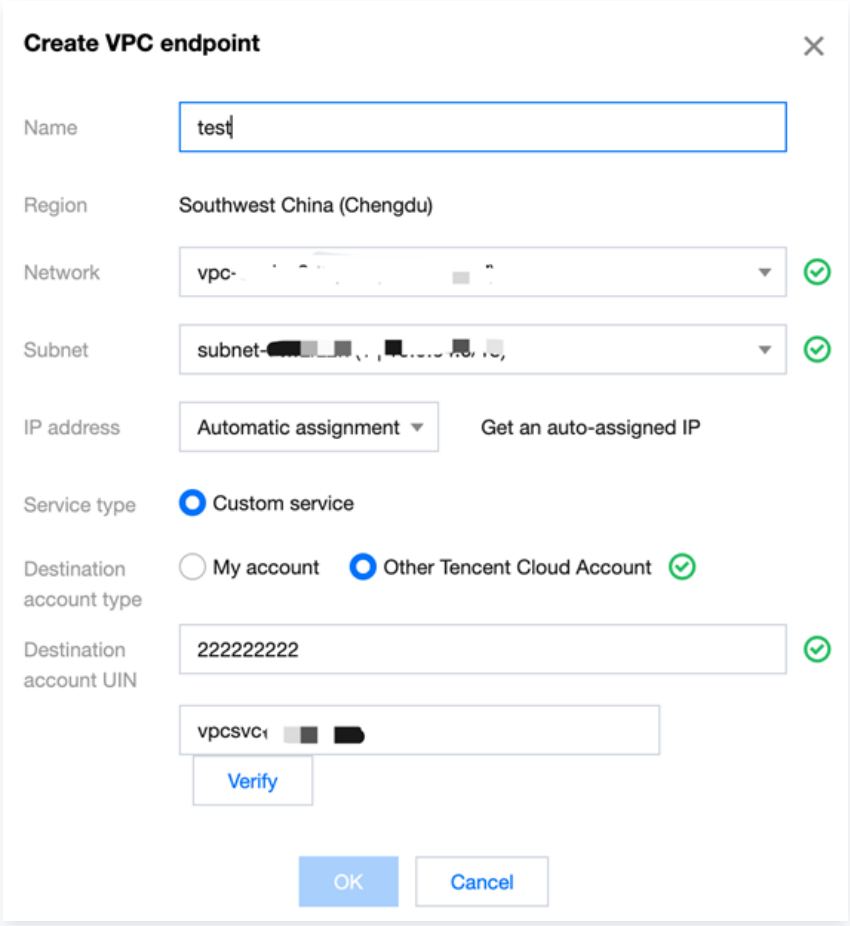
Step 2: Add Service Consumer Account to the Allowlist

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**.



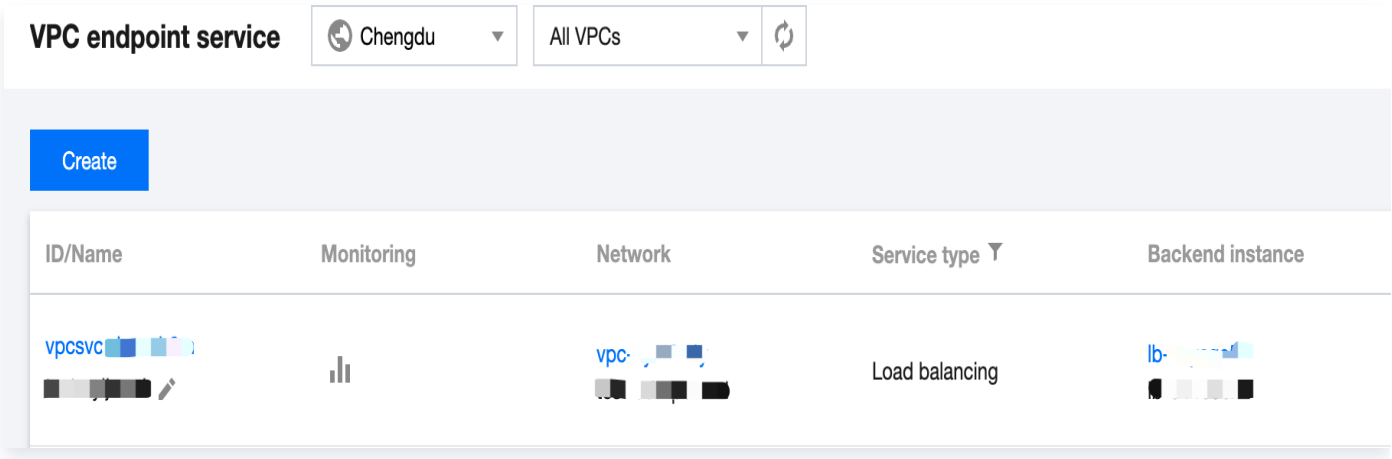
Step 3: Service Consumer Creates an Endpoint

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.

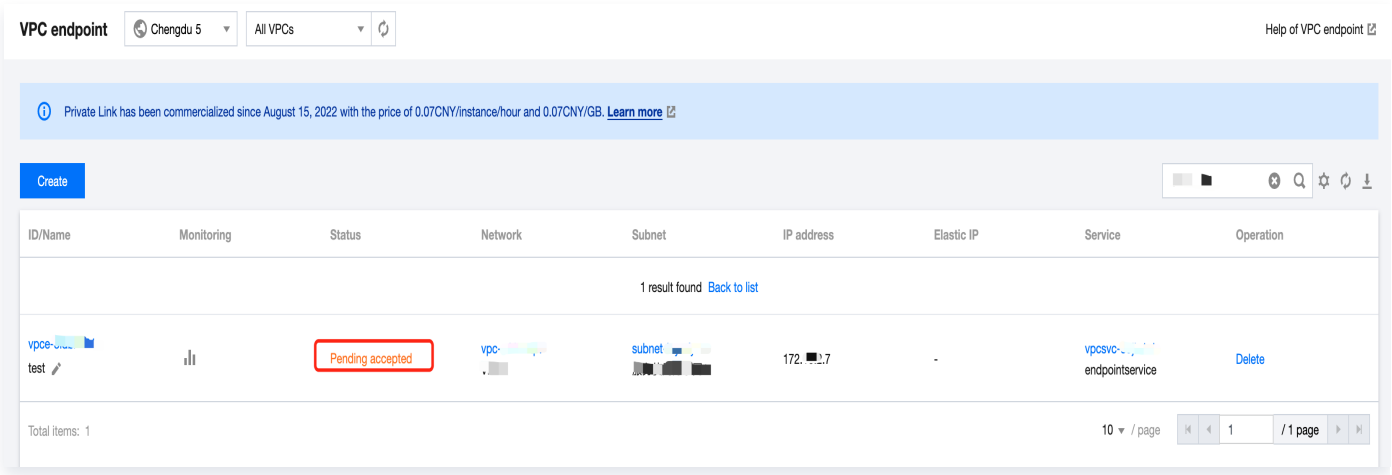


Parameter name	Description
Name	Specify a custom name for the endpoint.
Region	Endpoint Region
Network	Select the VPC where the Endpoint is located; in this example, choose VPC1.
Subnet	Select the subnet where the Endpoint is located.
IP Addresses	Endpoint IP address: You can specify an IP address, which 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 **Another Account**: • For access between VPCs within the same account, select **My Account**. • For cross-account VPC access, select **Other Account**.

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



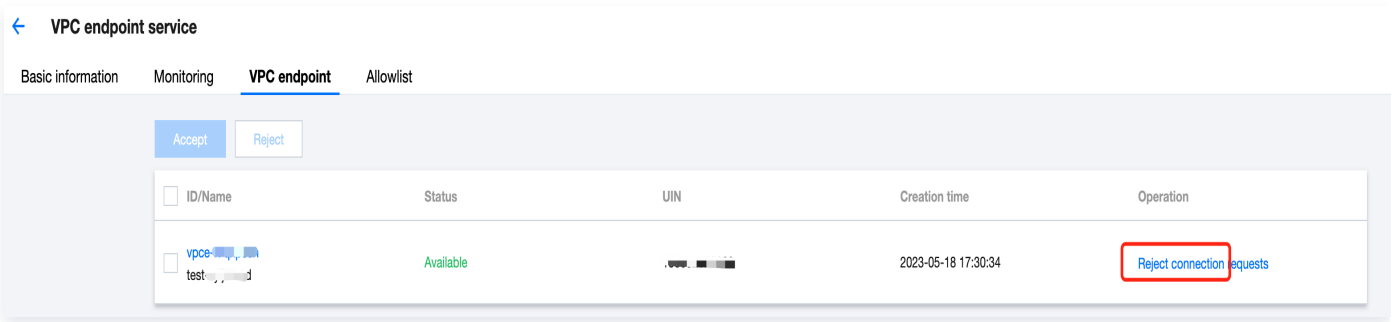
3. After completing the parameter configuration, click **OK**. The current connection status of the Endpoint is **Pending Acceptance**.



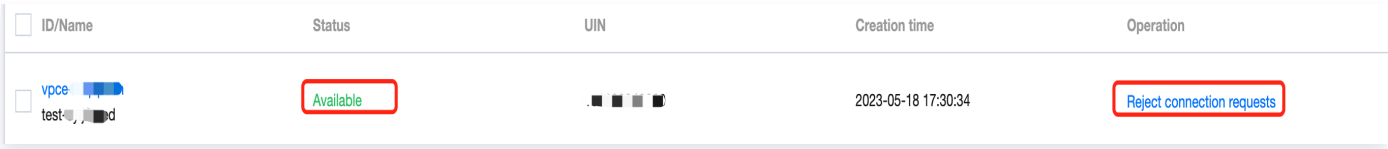
Step 4: Manage Endpoint Connection Requests

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**.



After accepting, the Endpoint's status changes to **Available**:

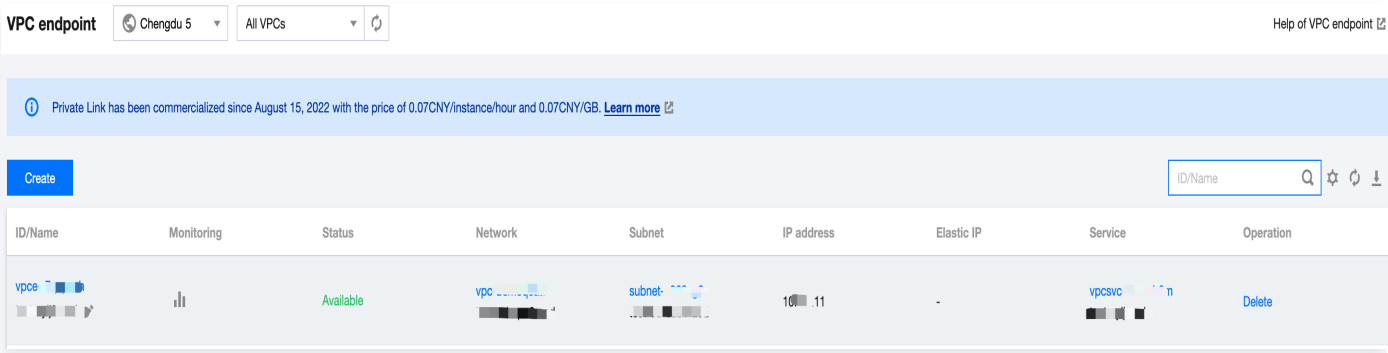


Step 5: Service consumer initiates access request to verify the connection

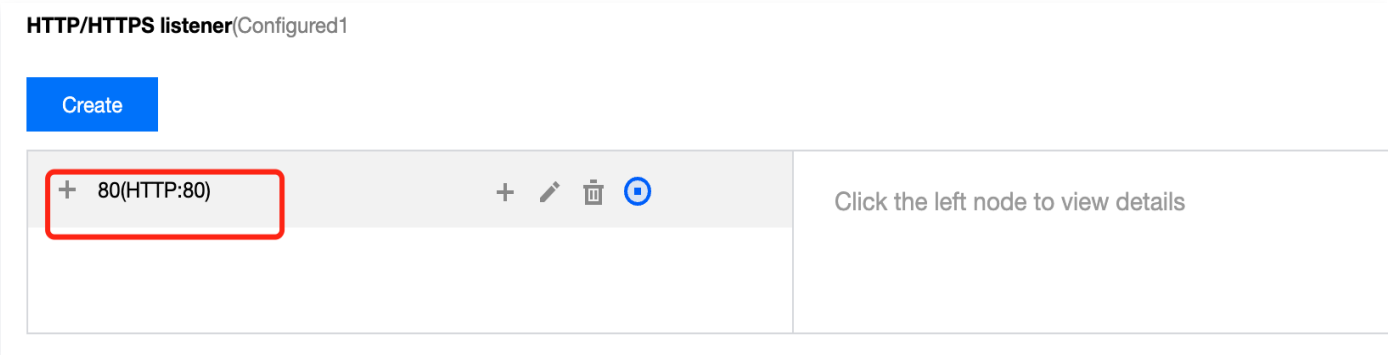
1. Log in to a CVM instance under the service consumer's VPC1 and access the service provider's backend services via VIP+VPORT.
2. In this example, telnet is used to verify connectivity by executing *telnet VIP VPORT*.

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

Obtain the Endpoint VIP:



Obtaining the CLB VPort:



If the following information appears, it indicates a successful connection:

```
[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 '^]'.
```