Private Link

Best Practices

Product Documentation

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 Practices

Sharing Services to VPCs in Different Regions

Last updated：2023-11-28 16:41:35

This document describes how to share cloud services deployed in your VPC with VPCs in other regions through Private Link and Cloud Connect Network (CCN).

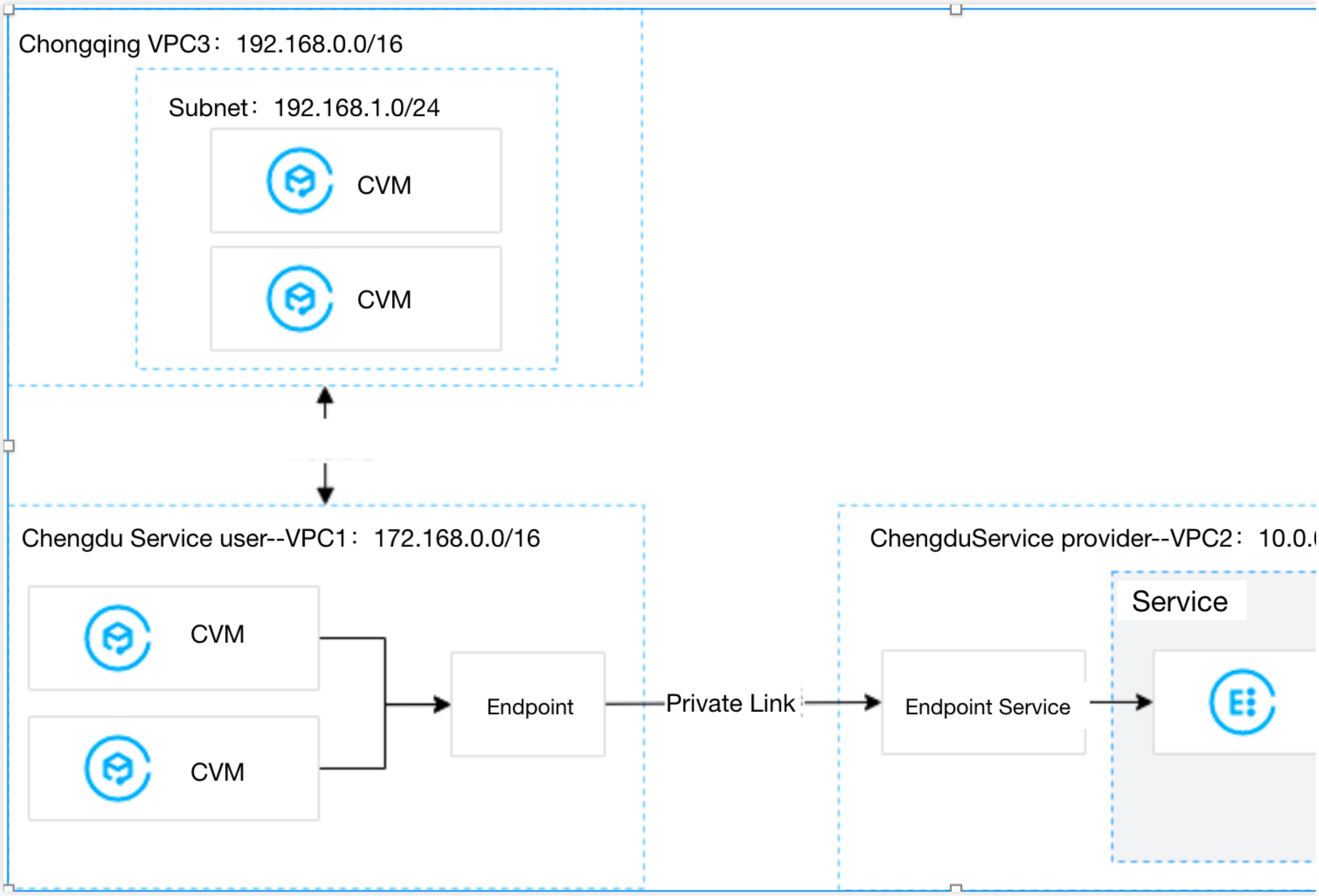
Overview

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. To share cloud services between VPCs across regions, you can use CCN to establish a cross-region connection, and then access the services in the Private Link service provider's VPC through the endpoint in the service user's VPC.

A Private Link connection involves a VPC endpoint and endpoint services. 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

A company has deployed applications in VPC2 in the Chengdu region, and it wants to share the resources in VPC2 with clients in VPC1 in Chengdu region and clients in VPC3 in Chongqing region. To avoid security risks caused by public network access, they decided to connect the VPCs via Tencent Cloud Private Link and CCN.


Chongqing VPC3：192.168.0.0/16
Subnet：192.168.1.0/24
CVM
CVM
Chengdu Service user--VPC1：172.168.0.0/16
CVM
CVM
Endpoint
Private Link
ChengduService provider--VPC2：10.0.
Endpoint Service
Service

Note

In this example, the three VPCs are under the same account.

Prerequisites

Create VPC2 for the service provider, VPC1 for the service consumer in the same region and VPC3 for the service consumer in another region.

(https://www.tencentcloud.com/document/product/214/8975!4a16ae41857804b10fcf0fe39fb0a94b)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.

Directions

Step 1. (Service provider) Create an endpoint service

Note

In this example, there is a private Layer-4 CLB instance created in VPC2. Relevant service resources are deployed in the backend CVM instance of CLB. 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.

Parameter	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 balacningCLB	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, **Yes** 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 acceptance**. 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 owner account of the endpoint service to connect. 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 1we set to automatically accept connection requests from all endpoints. When the endpoint is created, the status is **Available**.

Step 3. Connect VPC3 and VPC1 with CCN

1. Log in to the CCN console.
2. Click **Create** to create a CCN instance to associate VPC1 and VPC3, and click **OK**.

Note

For details, see Getting Started with CCN.

Step 4. (Service consumer) Initiate a connection request

Verify the connection from VPC1 to VPC2:

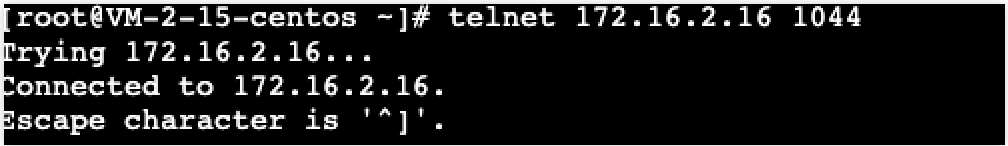
a. Log in to a CVM in VPC1 and access the backend service of the service provider through VIP+VPORT.

b. Run telnet *VIP VPORT*.

Note

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

If the following information is returned, the access is successful:



```
[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 the connection from VPC3 in Chongqing to VPC2 through the endpoint in VPC1 in Chengdu:

a. Log in to a CVM in VPC3 and access the backend service of the service provider through VIP + VPORT. The "VIP" is the VIP acquired by the endpoint in VPC1, which is 172.16.2.16 in this example. The "VPORT" is the listening port of CLB in VPC2, which is 1044 in this example.

b. Run telnet *VIP VPORT* to verify the connection.

Note

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

If the following information is returned, the access is successful:

```
<img src="https://main.qcloudimg.com/raw/2504940fd846c6cb3a37a8fd2b8812ec.png" widt
```

Sharing Services to VPCs Under Different Accounts

Last updated：2023-11-28 16:41:35

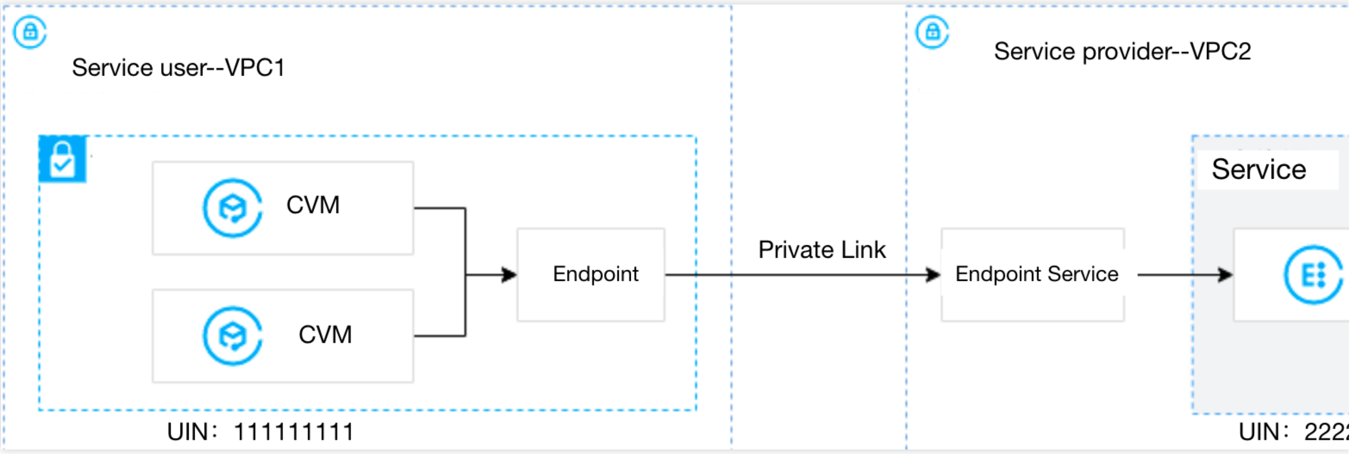
This document describes how to create a private link and share the cloud services deployed in the VPC under your account with a VPC in the same region under another account.

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 for the service provider, and VPC1 for the service consumer.

The service consumer and provider share their UINs with each other. The service provider adds the consumer's UIN to the allowlist.

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.

The service provider provides the CLB VPORT to the service consumer.

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.

Directions

Step 1. (Service provider) Create an endpoint service

Note

In this example, there is a private Layer-4 CLB instance created in VPC2. Relevant service resources are deployed in the backend CVM instance of CLB. 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.

Parameter	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 request	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 provider) Add the service consumer account to the allowlist

1. Click **More** > **Manage allowlist** on the right of the created endpoint service, or click the endpoint service ID to enter the details page, and then select the **Allowlist** tab.
2. On the allowlist management page, click **Add**.
3. In the pop-up dialog box, enter the UIN and description of the service consumer, and click **OK** .

Step 3. (Service consumer) Create an endpoint

1. Click **VPC Endpoint** in the left sidebar.
2. Click **Create** and 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 owner account of the endpoint service to connect. In this example, we select **Other Tencent Cloud 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. After configuring the parameters, click **OK**. The connection status of the current endpoint becomes **Pending acceptance**.

Step 4. (Service provider) Accept connection requests

To implement the connection across accounts, the service provider should accept the connection request initiated by the service consumer.

1. Click **More** > **Manage VPC endpoints** on the right of the created endpoint service, or click the endpoint service ID to enter the details page, and select **VPC endpoint**.
2. Click **Accept** and click **OK** in the pop-up window. After that, the status of the endpoint changes to **Available**.

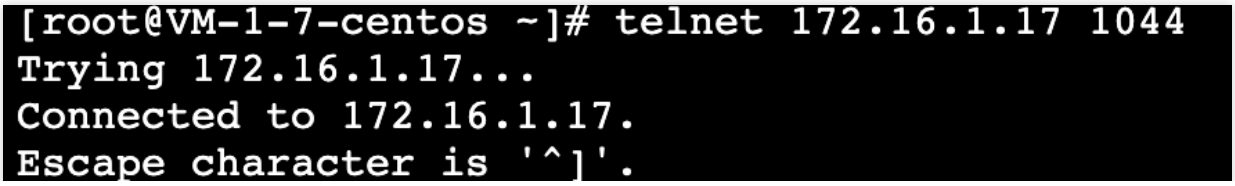
Step 5. (Service consumer) Verify the connection

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*.

Note

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

If the following message appears, it indicates that the connection is established:



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