Peering Connection

Product Documentation

Contents

Peering Connection 3
• Product Introduction 3
• Peering Connection Overview 3
• Product Features 4
• Use Limits 6
• Related Products 7
• Purchase Guide 8
• Billing Overview 8
• Quick Start 9
• Creating Intra-Account Peering Connection 9
• Creating Cross-Account Peering Connection 13
• Operation Guide 17
• Configuring the Route to Peering Connection 17
• Creating and Deleting Peering Connection 18
• Viewing Related Routing Policies 20
• Viewing Monitoring Data of Network Traffic Over a Cross-region Peering Connection 21
• Rejecting a Peering Connection 22
• Deleting a Peering Connection 23
• Viewing the Peer Account ID 24
• FAQs 25
• Concepts 25

Product Introduction
Peering Connection Overview

Introduction

Peering Connection is a high-bandwidth and high-quality cloud resource interconnection service that helps you establish communication links among cloud resources. Peering connections can be used across multiple regions, multiple accounts, and multiple types of heterogeneous networks, which can easily implement complex network scenarios, such as 2-region-3-center and one server shared by game players. It enables interconnection between VPCs, allowing you to deploy different businesses.

VPC peering connection is a cross-VPC network interconnection service used for synchronizing office data. It enables interconnection between two VPCs as if they were on the same network. After routing policies are configured at both ends, interconnection is enabled between VPCs of the same user or different users in the same region or across regions. Peering connection does not depend on any separate hardware. Therefore, no single points of failure and bandwidth bottlenecks will occur in a peering connection.

Strengths

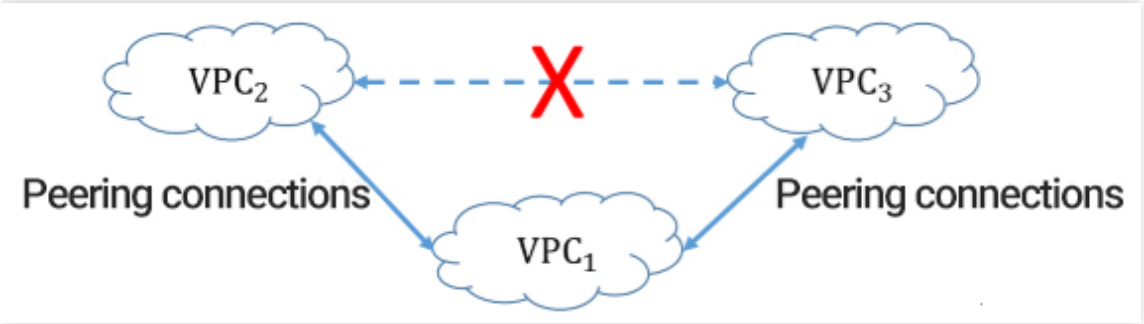
Peering connection service has the following strengths over Internet transmission transmission.

- Higher Quality
    - Using the same self-built private network with group businesses, the peering connection is not affected by the quality of public network providing significantly better availability, latency, and packet loss rate.
- Enhanced Security
    - Protected by DDoS Security of the Anti-DDoS basic system, the peering connection offers high defense capabilities.
    - Avoiding wide-area Internet and ISP links, the peering connection minimizes the risk of data theft during public network transmission.

Product Features

1. Non-transitive Connectivity of Peering Connection

A peering connection enables connectivity between two VPCs, but the connectivity cannot be transited.For example, as shown in the following figure, peering connections are created between VPC 1 and VPC 2, and between VPC 1 and VPC 3. However, due to the non-transitivity of peering connections, traffic cannot flow between VPC 2 and VPC 3.



> Note:
>
> Even if a peering connection is created, both ends of the connection cannot communicate with each other if routes for sending and returning packets are not configured at both ends.

2. Intra-Region and Cross-Region Peering Connection

VPC supports both intra-region and cross-region peering connections. Due to the differences in physical distance and underlying implementation architecture, there are some differences between the two types of connections, as shown in the table below.

Comparison Items	Intra-Region Peering Connection	Cross-Region Peering Connection
Underlying architecture	Local private network within a single region	Cross-region internal MPLS network
Cross-account connection	Supported	Supported

Comparison Items	Intra-Region Peering Connection	Cross-Region Peering Connection
Access permission	The CVMs at either end of a peering connection can access all the resources at the peer end, including CVMs, databases, and CLBs.	The CVMs at either end of a peering connection can access all the resources at the peer end, including CVMs, databases, and CLBs.
Feature Limits	The VPC IP ranges at both ends of the peering connection cannot overlap. Peering connections are independent of each other.	The VPC IP ranges at both ends of the peering connection cannot overlap. If multiple peer VPCs are connected to the same VPC, the IP ranges to which these peer VPCs belong cannot overlap.
Use Cases	Mainly used to connect applications located in different Virtual Private Clouds within the same region.	Typical use cases: cross-region disaster recovery. By utilizing cross-region peering connections, VPCs in different regions can communicate with each other, which helps rapidly deploy a 2-region-3-center solution for disaster recovery and meets the requirement for financial-level network disaster recovery with high bandwidth and reliability.

Use Limits

Use Limits

Note the following when you use a peering connection:

- To enable real communication between both ends of a peering connection, you must configure routing rules in the route tables of both the sending and receiving ends.
- If the peer does not accept a peering connection request, the request will automatically expire after 7 days.
- Do not accept peering connection requests from unknown accounts because they may pose risks to your network.
- The VPC CIDR blocks on both ends of a peering connection cannot overlap. Otherwise, an error will occur.
- For a cross-region peering connection, the CIDR blocks of multiple peer networks of one VPC cannot overlap. Otherwise, an error will occur.
- Either end of a peering connection can interrupt the connection. Then, traffic between the two VPCs is disconnected immediately.

Resource Limitations

Resource	Limitation	Description
The number of peering connections supported by each VPC	10	-

Related Products

For related product information, see the following table:

Product Name	Relationship with Peering Connection
Cloud Virtual Machine (CVM)	The CVMs at either end of a peering connection can access all the resources at the peer end, including CVMs, databases, and CLBs.
Cloud Load Balancer (CLB)	The CVMs at either end of a peering connection can access all the resources at the peer end, including CVMs, databases, and CLBs.
Virtual Private Cloud (VPC)	A peering connection enables route interconnection between two VPCs.
Routing Table	A peer connection enables communication only after route tables are correctly configured at both ends.
Cloud Monitor	You can log in to the Cloud Monitor Console to set alarm policies.

Purchase Guide
Billing Overview

Billing overview

Peering connections are billed by the bandwidth of interconnection. The intra-region peering connection is free of charge while the cross-region peering connection is billed by the bandwidth daily peak.Billing by Daily Peak: The daily peak inbound/outbound bandwidth is taken for settlement.

Purchase Method

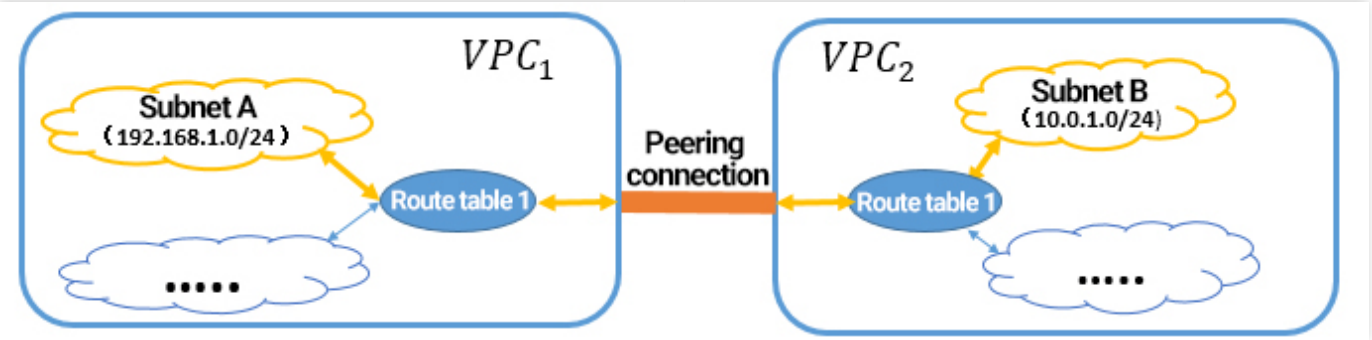
The purchase method is the peering connection creation process. For detailed directions, see Quick Start > Creating Intra-Account Peering Connection or Quick Start > Creating Cross-Account Peering Connection.

Quick Start
Creating Intra-Account Peering Connection

Both cross-region and cross-account communication of VPCs are advanced features of peering connections. This document describes how to implement cross-region communication through an example.

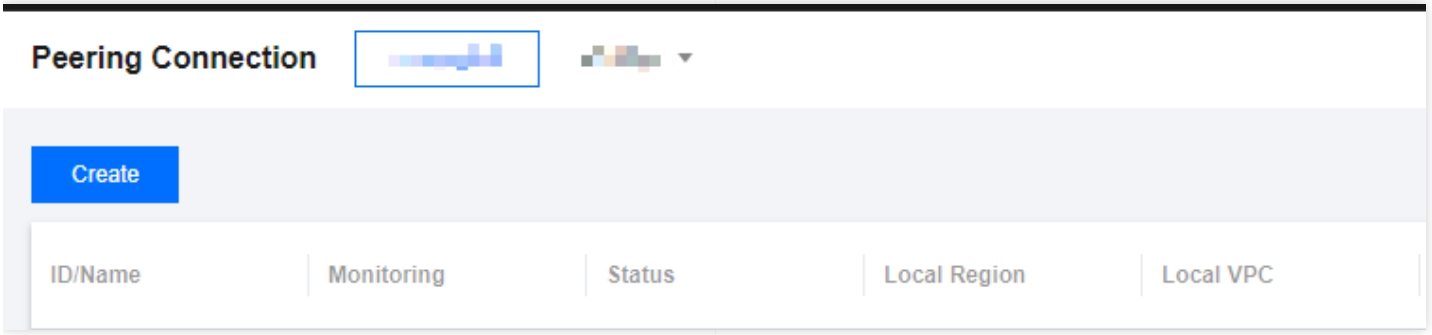
Example

- IP range 1: subnet A 192.168.1.0/24 in VPC1 of City 1.
- IP range 2: subnet B 10.0.1.0/24 in VPC2 of City 2.
  To implement communication between IP ranges 1 and 2 over a peering connection under the same account, two steps are required. The specific directions are as follows.

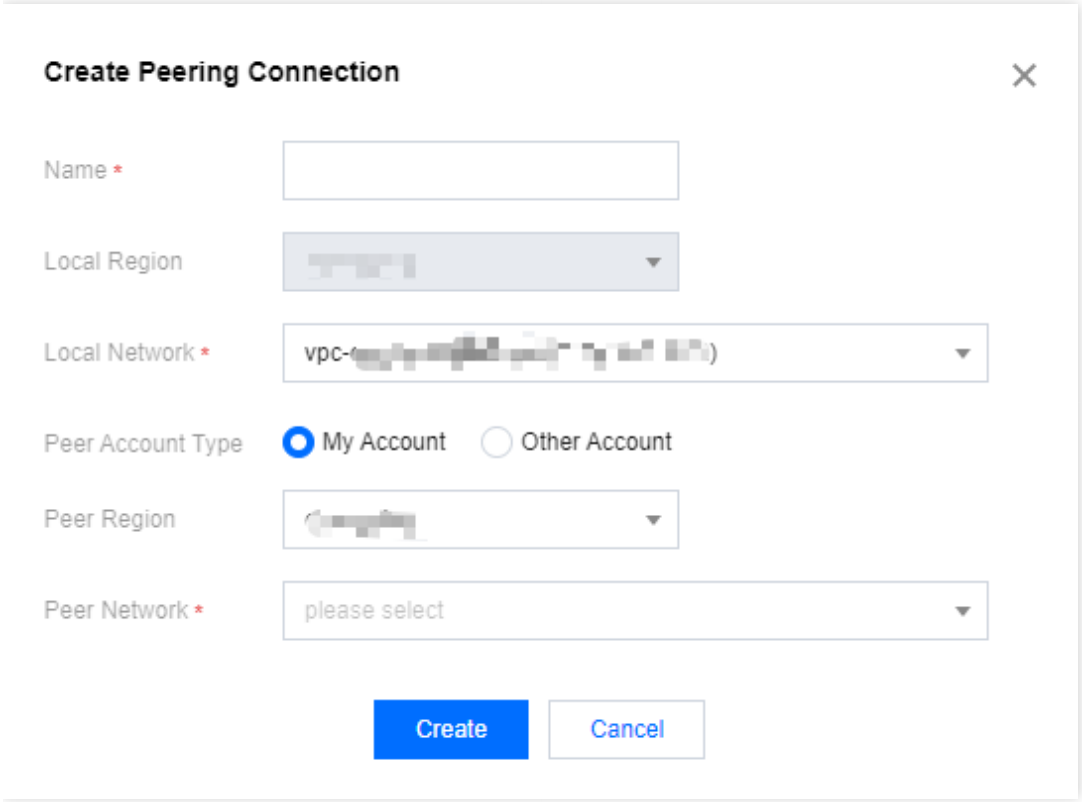


Step 1: Create a peering connection

1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Peering Connection in the left sidebar to enter the Management page.
3. Select a region and a VPC above the list and then click Create to create a peering connection.



4. Enter a name, select the local region and network, and select the peer region, account type, VPC, and bandwidth cap.After selecting My Account as the peer account type, you need to select the corresponding instance from the pull-down menu.



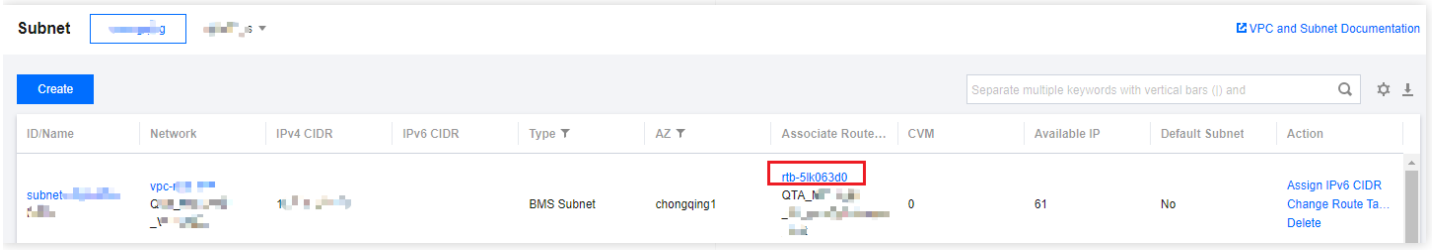
5. Click Create. A peering connection between two VPCs under the same account takes effect immediately after its creation.

Step 2: Set up routing tables at both ends

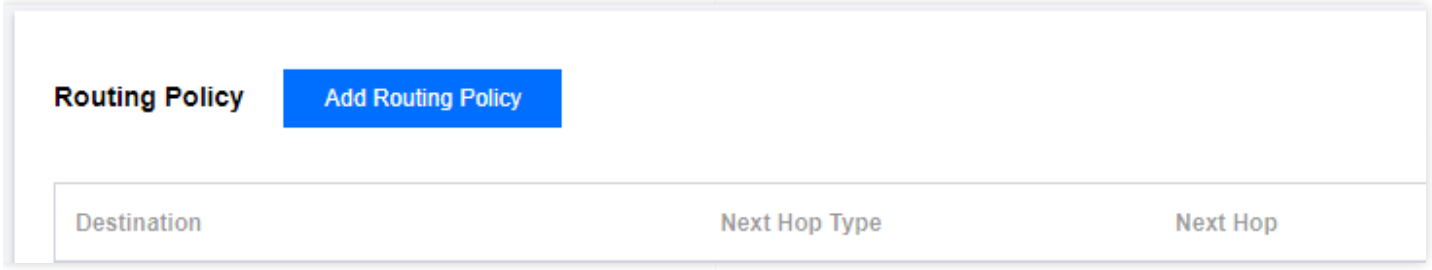
> Note:
>
> - You must configure routes on both sides to implement communication over a peering connection.

- To communicate between multiple IP ranges of the two VPCs, you just need to add corresponding routing table entries, without the need for creating multiple peering connections.

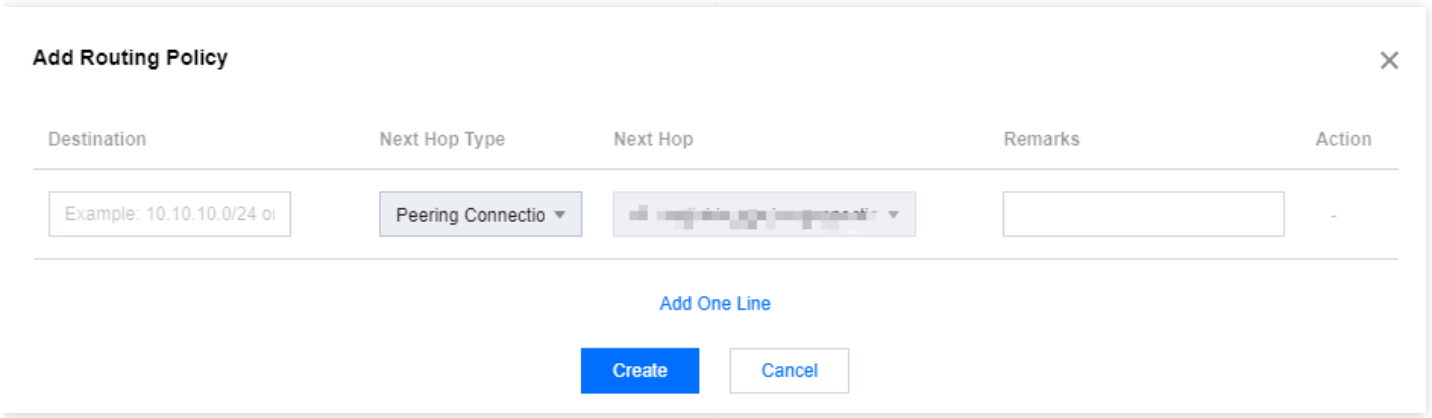
1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Click the ID of the route table (route table A) associated with the local subnet (subnet A) of the peering connection to access the route table details page.



4. Click Add Routing Policy.



5. Enter the peer CIDR (10.0.1.0/24) for the destination, select Peering Connections for the Next Hop Type, and select the created peering connection for the Next Hop Type.

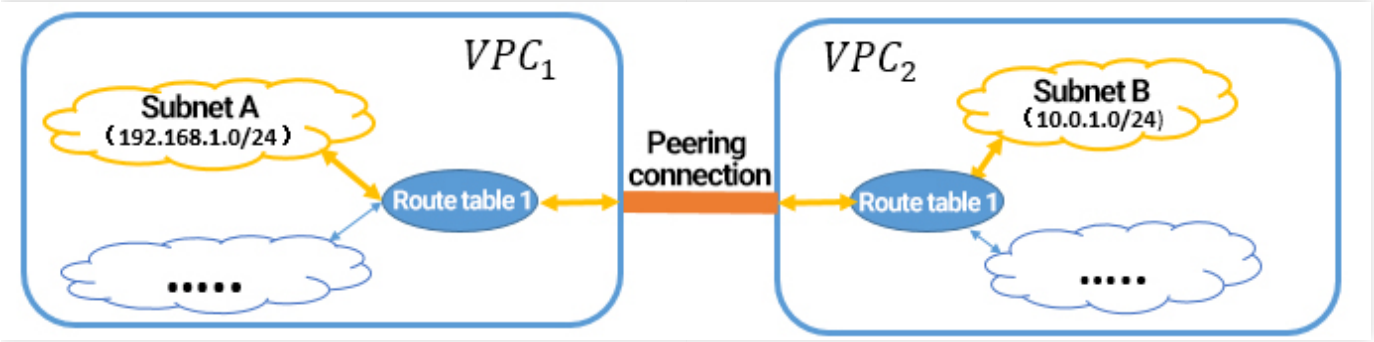


6. Click Create. After the routing table is configured, communication is enabled between the IP ranges of the two VPCs. The peer routing table is configured in the same way as that at the local end.

Creating Cross-Account Peering Connection

Example

- IP range 1: subnet A 192.168.1.0/24 in VPC1 of City 1.
- IP range 2: subnet B 10.0.1.0/24 in VPC2 of City 2.
  To enable communication between IP ranges 1 and 2 over a peering connection across different accounts, two steps are required. For specific operations, see below.



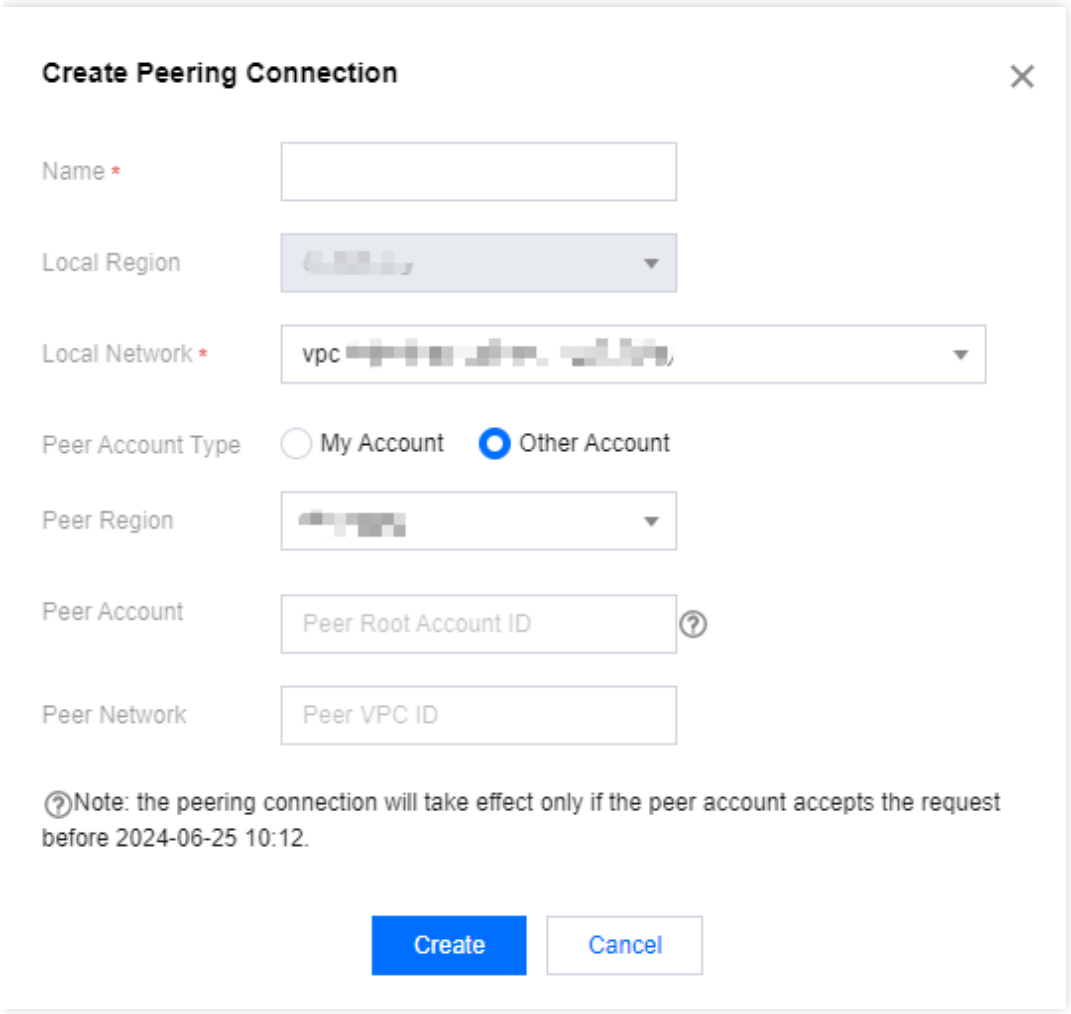
Step 1: create a peering connection

1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.

2. Click Peering Connection in the left sidebar to enter the Management page.

3. Select a region and a VPC above the list and then click Create to create a peering connection.

4. Enter a name, select the local region and network, and select the peer region, account type, VPC, and bandwidth cap.When the peer account type is Other Accounts, enter the account ID and VPC ID of the peer account.



5. Click Create to establish the cross-account VPC peering connection. The peering connection takes effect immediately after creation.

Step 2: Accept the peering connection

If VPC2 belongs to another user, you need to notify the user of accepting your peering connection request.

1. Log in to the VPC console, and click Peering Connection in the left sidebar to enter the Management page.
2. Select the target region above the list, locate the peering connection (PeerConn) you want to accept, and click Accept.

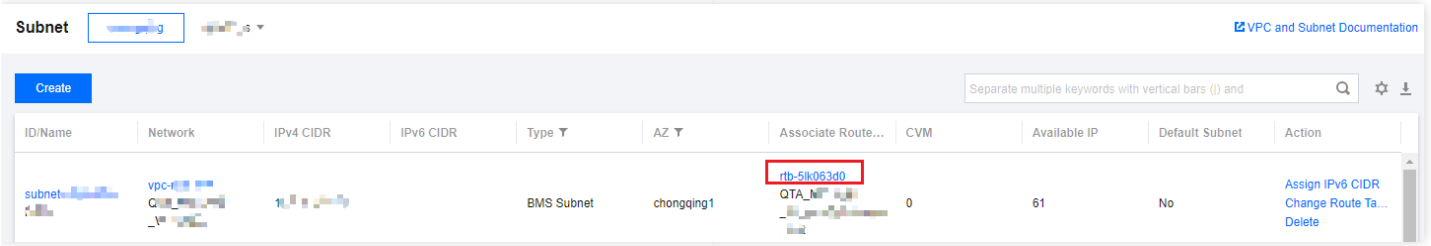
Step 3: Set up routing tables at both ends

> Note:
>
> - You must configure routes on both sides to implement communication over a peering

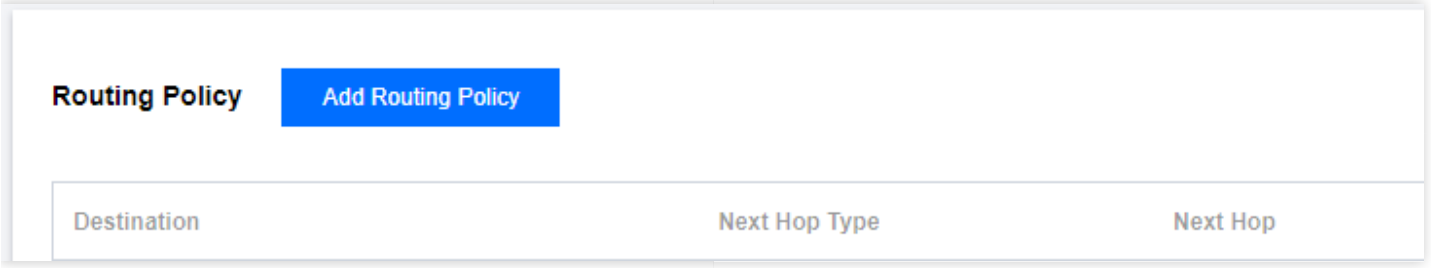
connection.

- To communicate between multiple IP ranges of the two VPCs, you just need to add corresponding routing table entries, without the need for creating multiple peering connections.

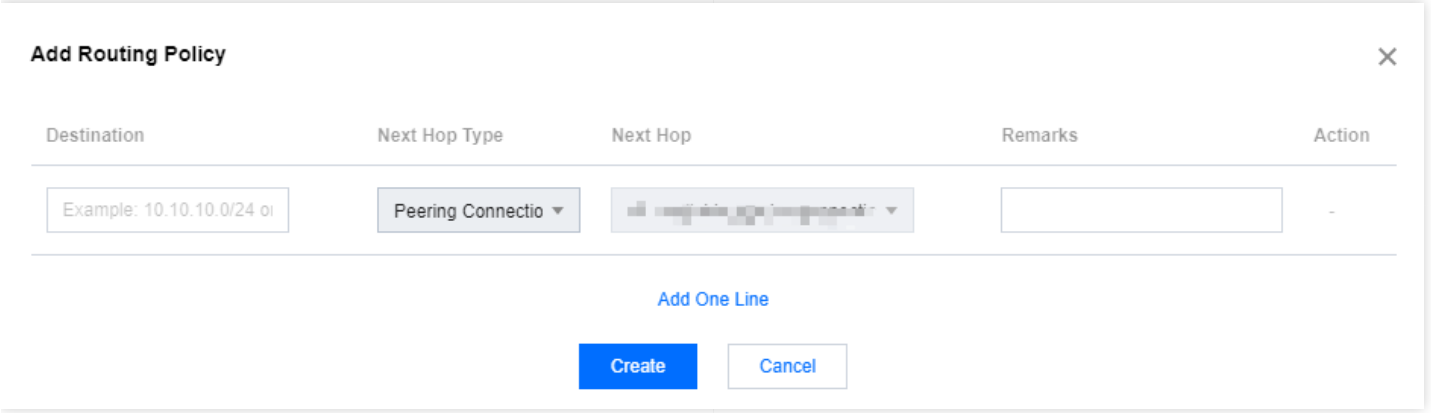
1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Click the ID of the route table (route table A) associated with the local subnet (subnet A) of the peering connection to access the route table details page.



4. Click Add Routing Policy.



5. Enter the peer CIDR (10.0.1.0/24) for the destination, select Peering Connections for the Next Hop Type, and select the created peering connection (PeerConn) for the Next Hop.

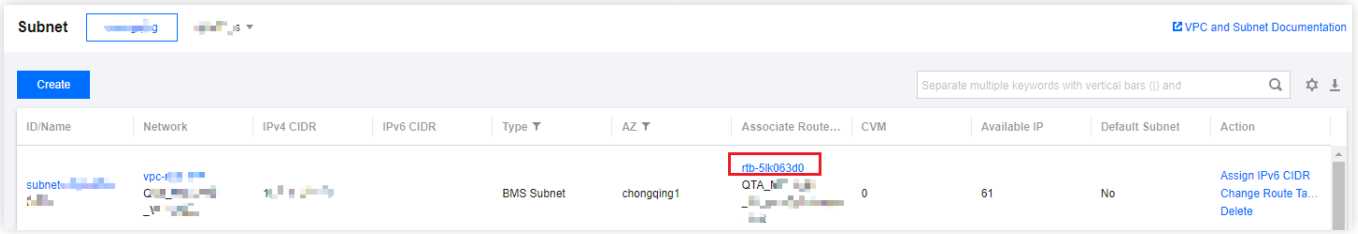


6. Click OK. After the routing table is configured, communication is enabled between the IP ranges of the

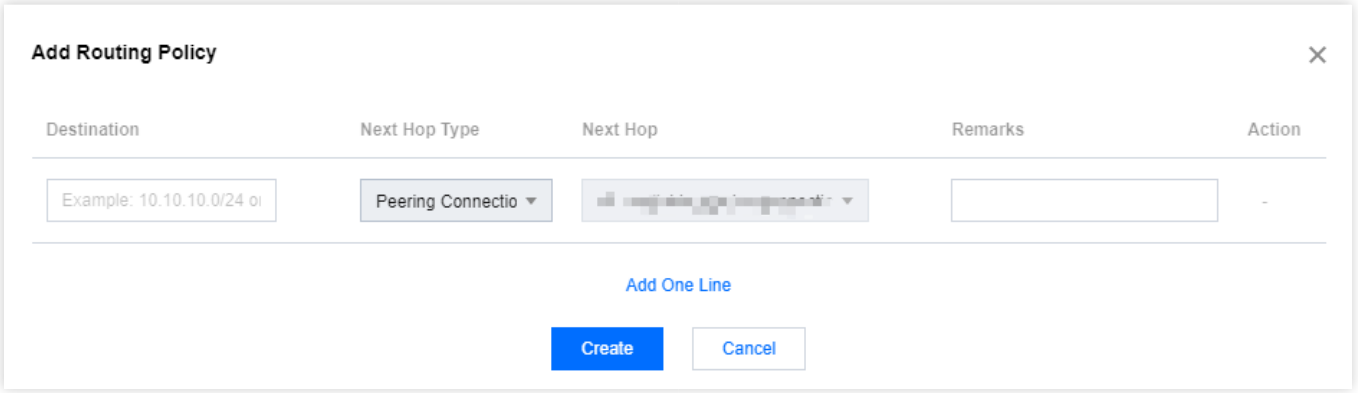
two VPCs. The peer routing table is configured in the same way as that at the local end.

Operation Guide
Configuring the Route to Peering Connection

1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Subnet in the left sidebar to enter the Management page.
3. Click the ID of the route table (route table A) associated with the local subnet (subnet A) of the peering connection to access the route table details page.



4. Click Add Routing Policy.
5. Enter the peer CIDR (10.0.1.0/24) for the destination, select Peering Connections for the Next Hop Type, and select the created peering connection (PeerConn) for the Next Hop.



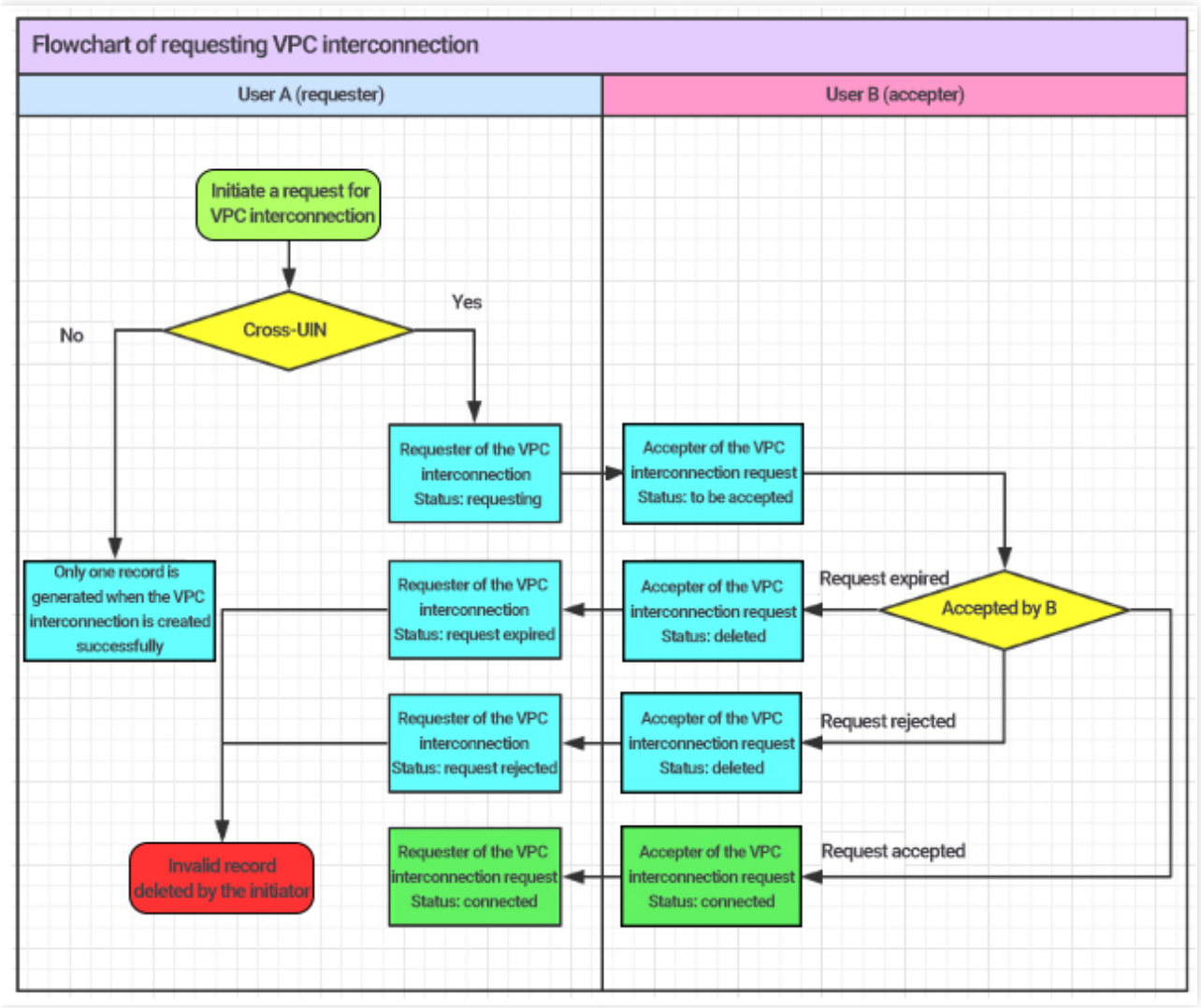
6. Click Create. After the routing table is configured, communication is enabled between the IP ranges of the two VPCs. The peer routing table is configured in the same way as that at the local end.

> Note:
>
> - You must configure routes on both sides to implement communication over a peering connection.
> - Between two VPCs, communication between multiple local IP ranges and multiple peer IP ranges only requires adding corresponding route table entries and does not require establishing multiple peering connections.

Creating and Deleting Peering Connection

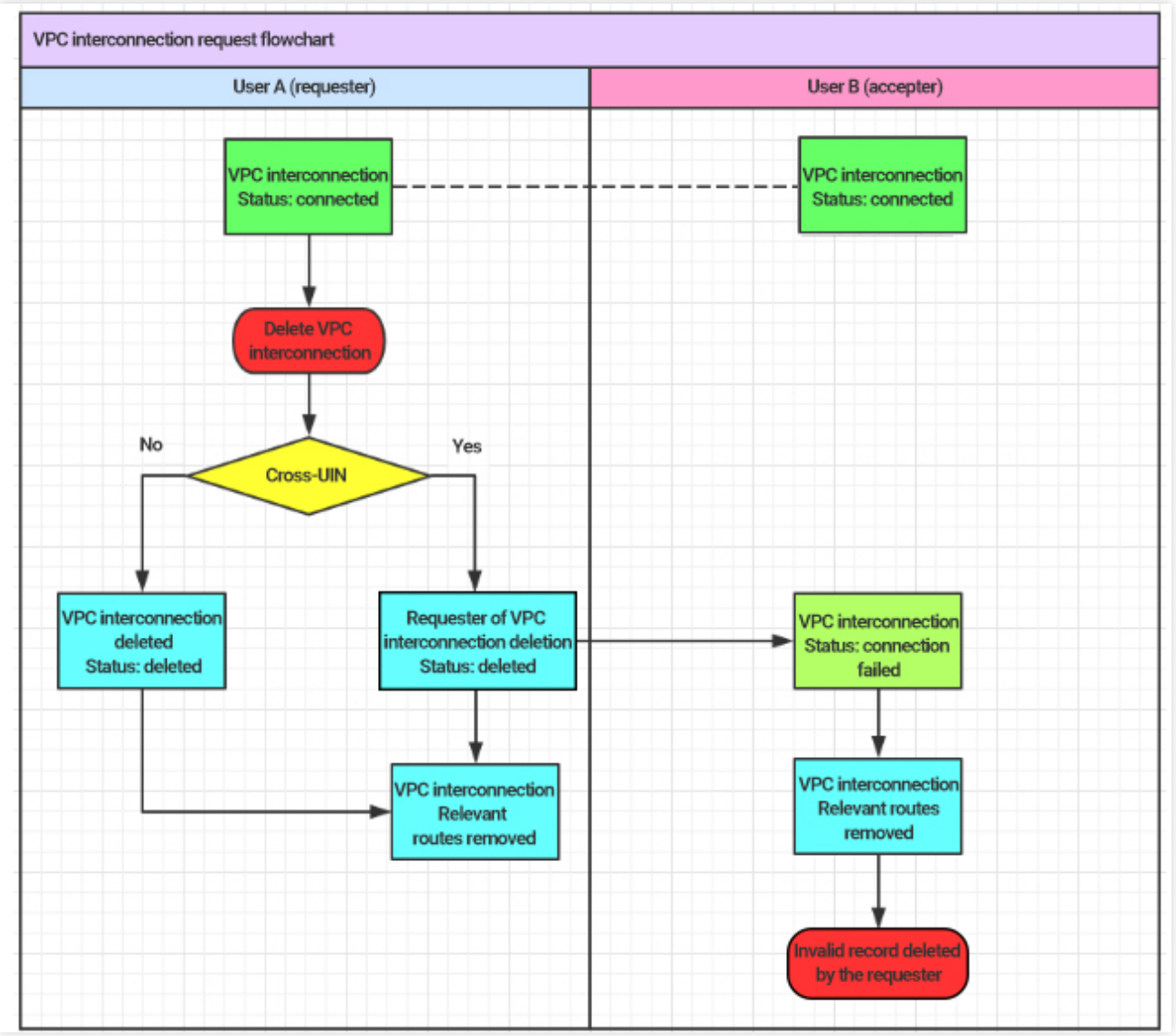
1. Process for Creating Peering Connection

The process for creating a peering connection is shown below. For detailed directions, see Quick Start > Creating Intra-Account Peering Connection or Quick Start > Creating Cross-Account Peering Connection.



2. Process for Deleting Peering Connection

The process for deleting a peering connection is shown below. For detailed steps, see Deleting a Peering Connection.


VPC interconnection request flowchart
User A (requester)
User B (accepter)
VPC interconnection Status: connected
VPC interconnection Status: connected
Delete VPC interconnection
No
Cross-UIN
Yes
VPC interconnection deleted Status: deleted
Requester of VPC interconnection deletion Status: deleted
VPC interconnection Status: connection failed
VPC interconnection Relevant routes removed
VPC interconnection Relevant routes removed
Invalid record deleted by the requester

Viewing Related Routing Policies

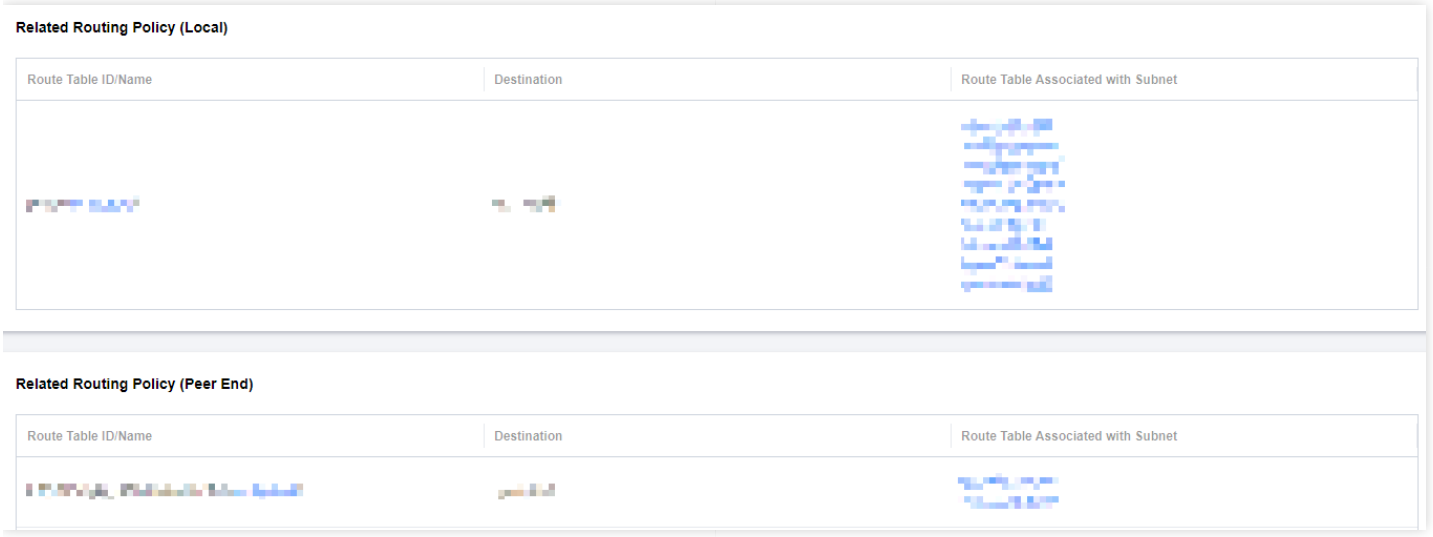
1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.

2. Click Peering Connection in the left sidebar to enter the Management page.

3. Select a region and a VPC above the list.

4. Click the ID of the target peering connection to go to the details page.

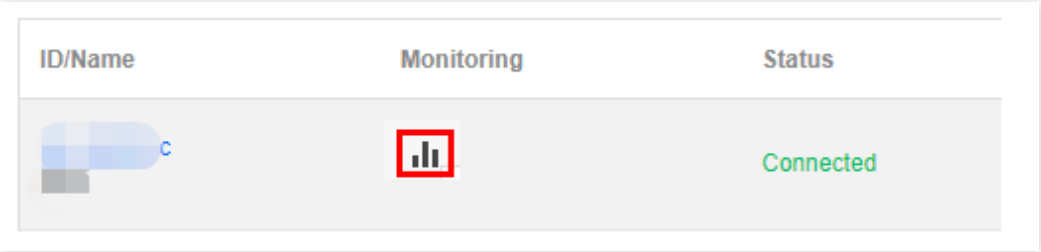
5. Check the following items in the related routing policy: The next hop is the destination IP range, the associated subnet, and the related routing table of the peering connection.



Viewing Monitoring Data of Network Traffic Over a Cross-region Peering Connection

> Note:
>
> - No upper limit is set on network traffic for intra-region peering connections.
> - Cross-region peering connections support network traffic monitoring.

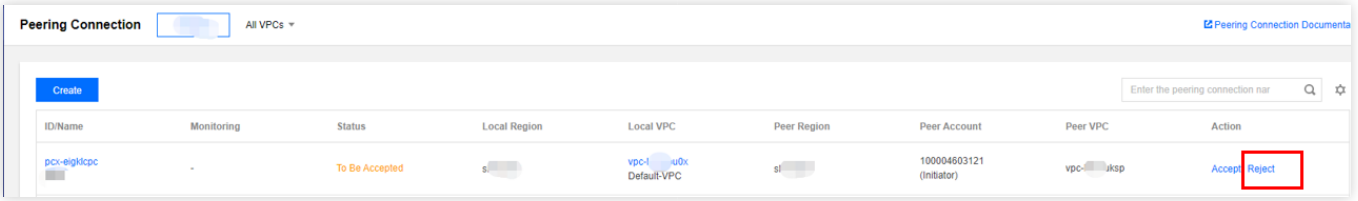
1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Peering Connection in the left sidebar to enter the Management page.
3. Click the monitoring icon for the target peering connection to view the inbound and outbound bandwidth, number of inbound and outbound packets, and packet loss rate.



Rejecting a Peering Connection

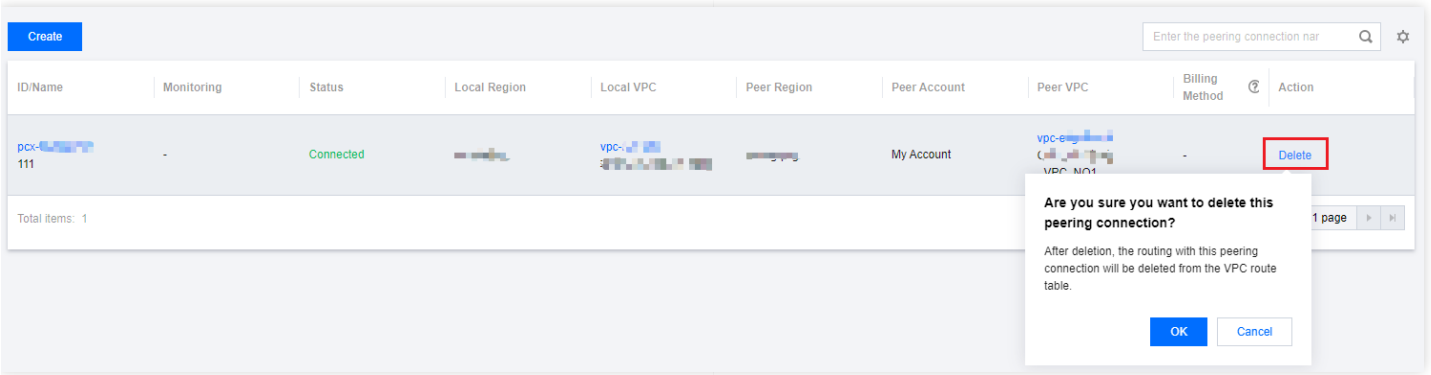
A peering connection request in the To Be Accepted status can be rejected. You can reject a connection request from an untrusted account.

1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Peering Connection in the left sidebar to enter the Management page.
3. Locate the request in the "To Be Accepted" status in the list, and click Reject in the Operation column. Confirm the operation when prompted.



Deleting a Peering Connection

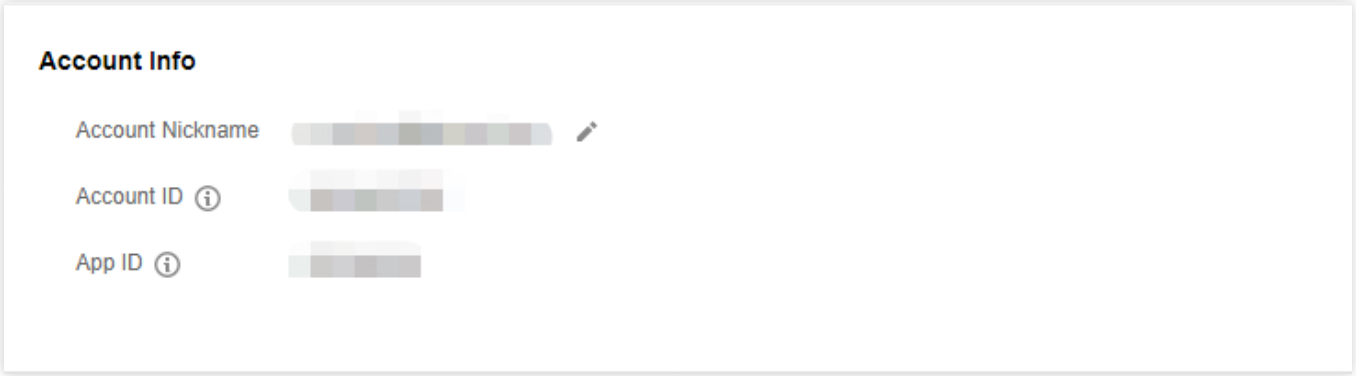
1. Log in to Cloud Console, select Cloud Products > Cloud Computing & Networking > Virtual Private Cloud to enter the VPC console.
2. Click Peering Connection in the left sidebar to enter the Management page.
3. Locate the target peering connection in the list, click Delete in the Operation column, and confirm it.



Viewing the Peer Account ID

When you create a cross-account peering connection, you need to enter the account ID of the peer developer, which you can check as follows:

1. Log in to Cloud Console, and click the account name in the upper-right corner.
2. Click Account Information to view the account ID on the details page.



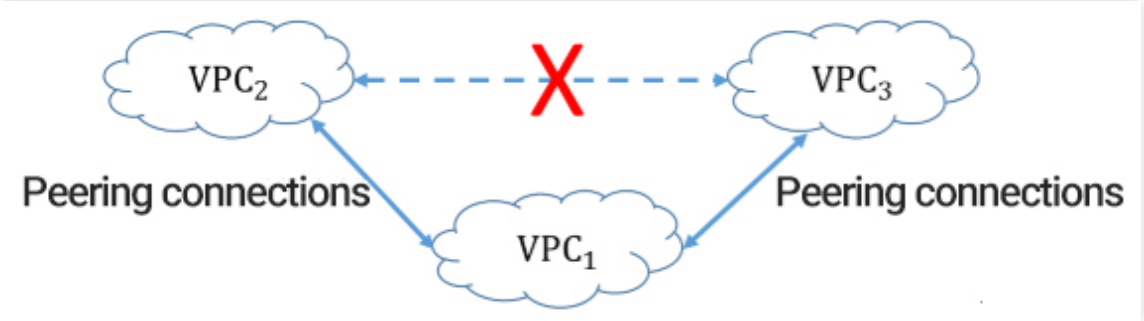
FAQs
Concepts

What is peering connection?

VPC peering connection is a cross-VPC network interconnection service used for synchronizing office data. For details, see Product Overview.

Is the connectivity of a peering connection transitive?

A peering connection enables connectivity between two VPCs, but the connectivity cannot be transited.For example, as shown in the following figure, peering connections are created between VPC 1 and VPC 2, and between VPC 1 and VPC 3. However, due to the non-transitivity of peering connections, traffic cannot flow between VPC 2 and VPC 3.



> Note:
>
> Even if a peering connection is created, both ends of the connection cannot communicate with each other if routes for sending and returning packets are not configured at both ends.

What is the difference between intra-region and cross-region peering connections?

- Intra-region peering connections are mainly used to connect applications located in different VPCs within the same region.
- Cross-regional peering connections are mainly used to implement connectivity between VPCs in different regions.

What are the restrictions on using peering connection?

When using the peering connection, you need to be aware of the restrictions on resources and connections. For details, see Usage Limitations.

If a peering connection is deleted at one end, is the VPC at the other end still accessible from the peer end?

No. The peering connection can be disconnected at either end at any time. The connection is ineffective immediately upon disconnection. The VPC at either end is accessible only after the connection is created again.

Can I connect VPC peering connection to the VPC of other cloud accounts?

Yes. This is possible as long as the owner of the other VPC accepts your peering connection request.

Can I create a peering connection between two VPCs with overlapped IP ranges?

No. The IP ranges of VPCs at the two ends of a peering connection cannot overlap.

Is traffic encrypted?

No. After a peering connection is created, access between two VPCs is similar to that between two CVMs in the same VPC, without additional encryption. Network traffic within a VPC is always isolated from other networks.

Is a single point of failure possible?

Single points of failure or bandwidth bottlenecks cannot occur because a peering connection between VPCs is not a gateway or a VPN connection and it does not depend on separate hardware.