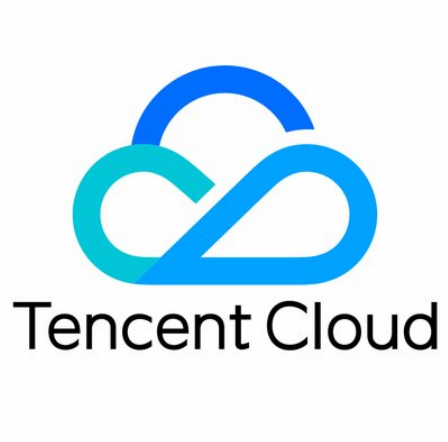
Virtual Private Cloud

Interconnection on Tencent Cloud

Product Documentation



Contents

Interconnection on Tencent Cloud
Peering Connection

Last updated：2019-02-19 12:24:06

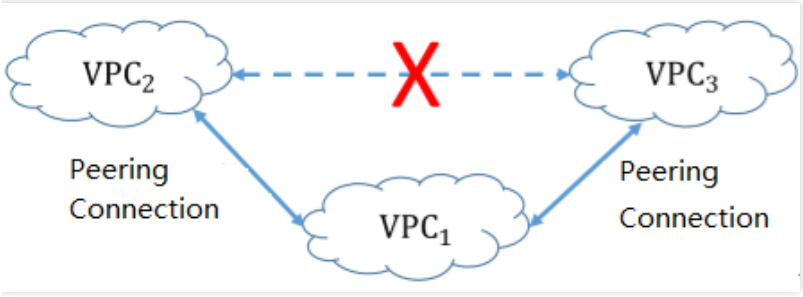
Overview

VPC peering connection is a cross-VPC network interconnection service for office data synchronization that allows VPC IPs to route traffic between peer VPCs as if they belong to the same network. The interconnection between VPCs of the same or different users in the same or different regions can be achieved. You can also achieve traffic interconnection between different VPCs by configuring routing policies on both ends. Peering connections do not depend on a single piece of hardware, so no single point of failure or bandwidth bottleneck exists.
Cross-region interconnections include: VPC cross-region interconnections (the cross-region peering connections) and basic network cross-region interconnections (you need to submit a Ticket to apply for it).

Note: Click to view Cross-region Connection Service Agreement. If any infringement of this agreement is identified, Tencent Cloud may at any time restrict, suspend or terminate services to you under the agreement as appropriate, and retain the right to pursue related liability.

Interconnectivity of Peering Connection is Not Transitive

Peering connection allows interconnections between VPCs, but this interconnection is not transitive. As shown below, peering connection is established between VPC 1 and VPC 2, as is done between VPC 1 and VPC 3. However, due to the non-transitivity of peering connection, the traffic interconnection between VPC 2 and VPC 3 cannot be achieved.



Note: Even if a peering connection is established, communication cannot be achieved if routes for sending and returning packets are not configured on both ends.

Intra-region Peering Connections and VPC Cross-region Peering Connections (the VPC Cross-region Interconnections)

VPC supports both intra-region and cross-region peering connections (the cross-region interconnection). As both types of connections are different in physical distance and underlying architecture, they are also different in function and billing method, as shown below:

Intra-region Peering Connections and VPC Cross-region Peering Connections (the VPC Cross-region Interconnections)

VPC supports both intra-region and cross-region peering connections (the cross-region interconnection). As both types of connections are different in physical distance and underlying architecture, they are also different in function and billing method, as shown below:

Comparison Item	Intra-region Peering Connection	Cross-region Peering Connection
Underlying architecture	Local private network within a single region based on Tencent Cloud	Cross-region internal MPLS network based on Tencent Cloud
Bandwidth	Interconnection with public cloud supports up to 5 Gbps Interconnection with BM supports up to 1 Gbps	For a maximum of 1 Gbps, the upper limit of bandwidth supports the following configurations (in Mbps): 10, 20, 50, 100, 200, 500 and 1,000
Billing Rule	Free of charge	Daily billing based on the regions where both ends of the peering connection are located and the actually network bandwidth used. For more information, please see Price Overview
Availability	Above 99.95%, with no single point of failure	Above 99.95%, with no single point of failure
Cross-account connection	Support	Support
Access Permission	CVMs on both ends of a peering connection can access all resources of each other including CVMs, databases, load balancers	CVMs on both ends of a peering connection can access all resources of each other including CVMs, databases, load balancers
Function Limits	VPC IP address ranges to which both ends of a peering connection belong must not overlap; multiple peering connections will not affect one another	VPC IP address ranges to which both ends of a peering connection belong must not overlap; if multiple peer VPCs are connected to the same VPC, the IP address ranges that these peer VPCs belong to must not overlap

Intra-region peering connection is used primarily to connect applications located in different VPCs within the same region.
The typical application for cross-region peering connection (cross-region interconnection) is **Cross-region disaster recovery**. VPCs within different regions are connected by means of cross-region connection to rapidly deploy a 2-region-3-DC solution for disaster recovery, thus meeting the needs of financial-level network disaster recovery with high bandwidth and reliability.

Gateway Traffic Control for Peering Connections

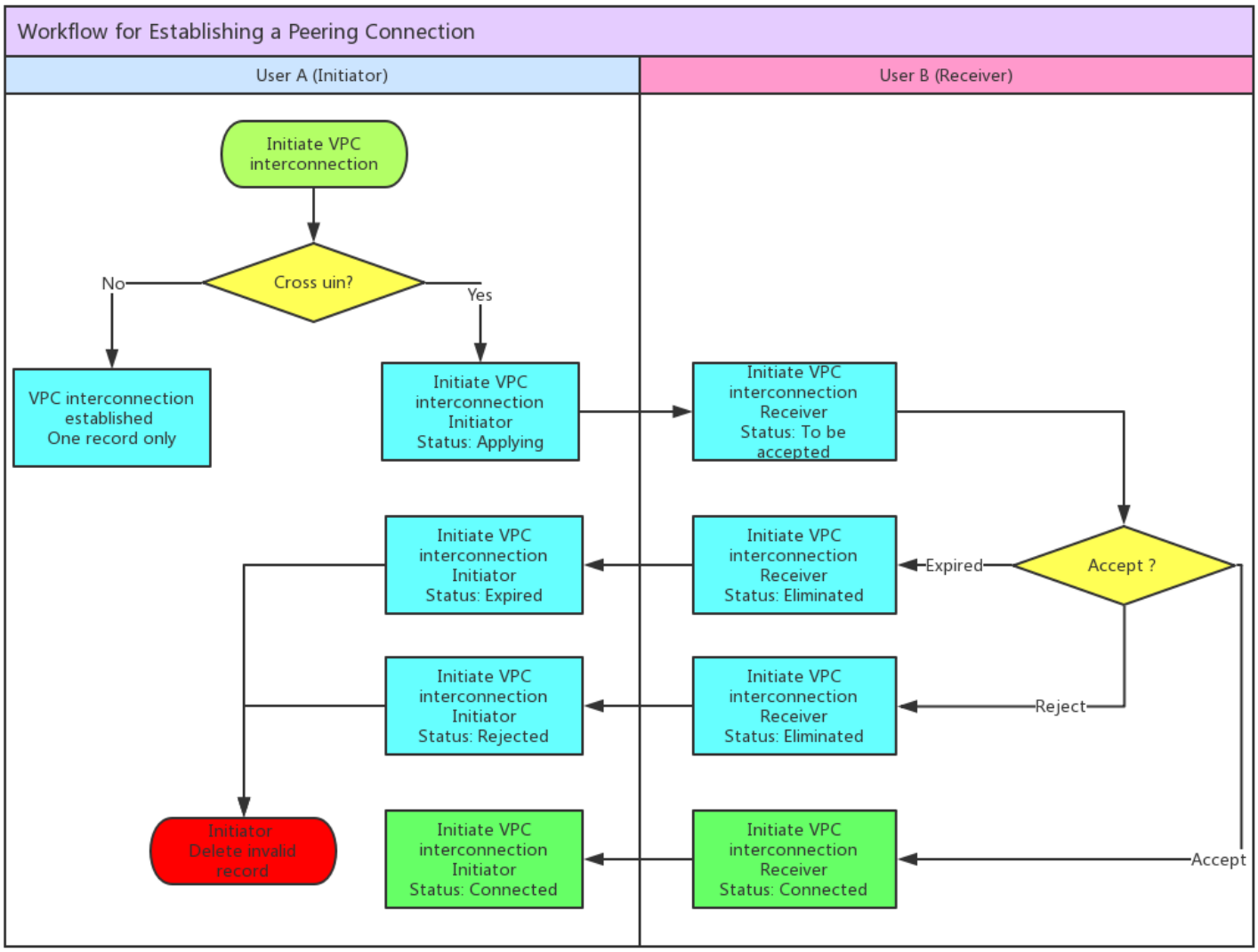
Gateway traffic control for peering connections provides the "monitoring" and "controlling" capabilities at **IP-gateway** granularity. Refined gateway traffic visualization enables network OPS personnel to get a clear picture of the traffic in the gateway. The speed restricting capability at IP-gateway granularity helps block exceptional traffic.
For example, in the early morning of one day, the gateway traffic of a company surges. With intelligent gateway traffic control, the OPS personnel can trace data to find which IPs cause this traffic surge according to the time when the traffic surge occurs, so as to rapidly locate its source. In addition, the gateway traffic control provides bandwidth control based on IP-gateway granularity, which can restrict the bandwidth from an IP to the gateway and block exceptional traffic to guarantee key businesses.

The advantages of gateway traffic control are as follows:

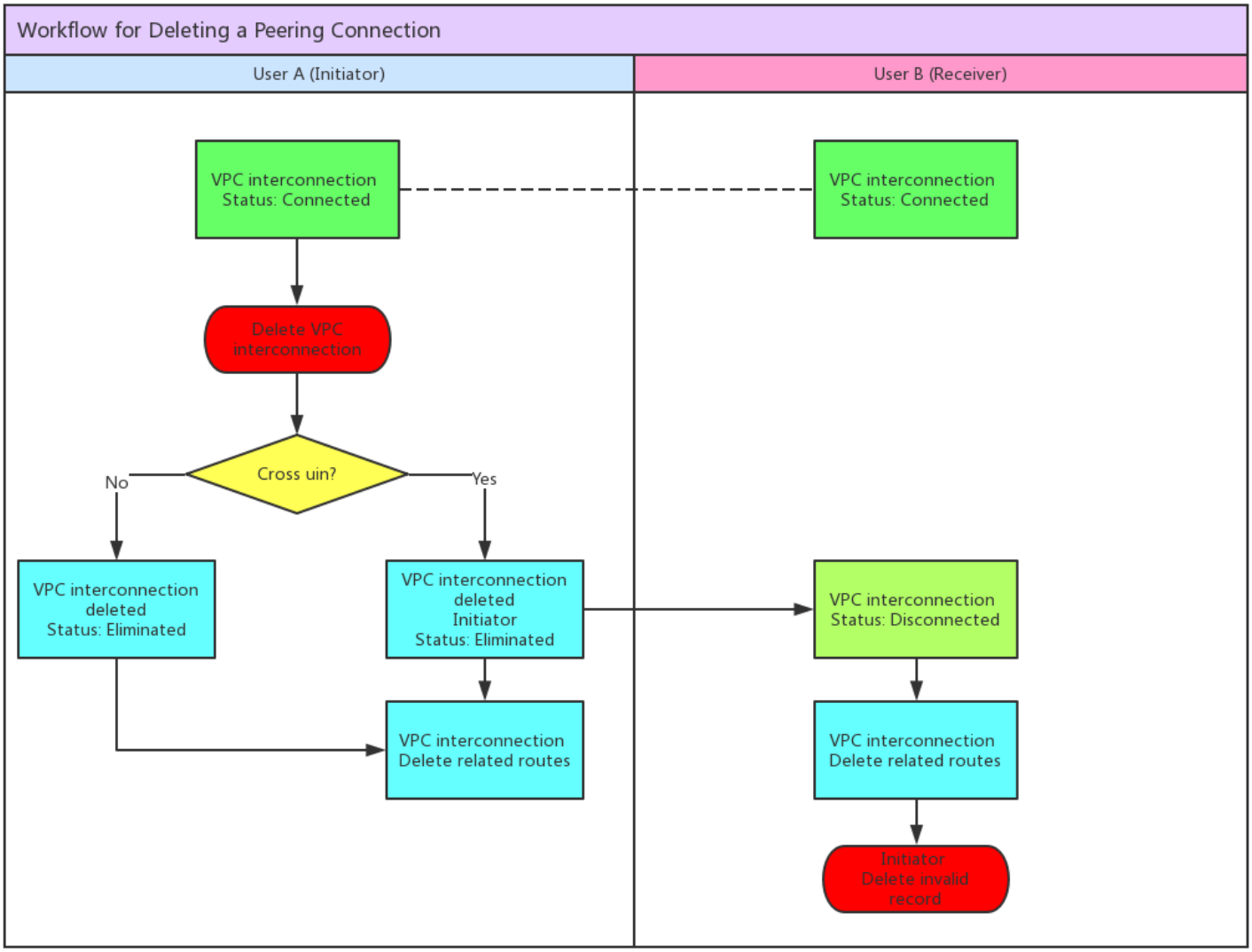
- Featured with the capability for accurate gateway troubleshooting, it can minimize the network failure time. It can also analyze the source IP and its key metrics by combining real-time traffic query and TOP N ranking features, to rapidly locate the exceptional traffic.
- With "monitoring" and "controlling" capabilities based on IP-gateway granularity and by using the minute-level network traffic query, it can find the exceptional traffic that maliciously occupies the bandwidth in real time, and set bandwidth limits at IP-gateway granularity, so as to guarantee the stable operation of core businesses.
- It has full-time and full-traffic gateway traffic analysis capability, to help reduce cloud network cost. It controls the cost through qos, thus restricting the bandwidth of non-key businesses to reduce cost in case of limited network budget.

Workflows

Workflow for Establishing a Peering Connection



Workflow for Deleting a Peering Connection



Service Limits

Please note the following when you use peering connection:

- To enable real communication between both ends of a peering connection, you must configure routing rules in routing tables of both the sending and receiving ends.
- Costs for cross-region peering connection are paid by the requester of such connection.
- If the other party does not accept a peering connection request, the request will automatically expire after 7 days.
- Please do not accept peering connection requests from unknown accounts because they may pose risks to your network.
- The VPC CIDR on both ends of a peering connection cannot overlap, otherwise an error will occur at the time of creation.
- For a cross-region peering connection, the CIDRs of multiple peer networks of one VPC cannot overlap, otherwise an error will occur.

- The peering connection can be interrupted on either end at any time. The communication between two VPCs is terminated immediately upon the interruption.
- There is no bandwidth limit for intra-region peering connection, and a bandwidth limit must be set for across-region peering connections.

Resource	Limit	Description
Bandwidth limit for cross-region peering connection	1 Gbps	If you need a larger bandwidth, submit a ticket. No limit on bandwidth is set for an intra-region peering connection.

| Number of peering connections supported by each VPC |10 | | |

Note: To request for the peering connection in other regions, submit a ticket.

For additional service limits of VPC, please see Service Limits.

Billing Method

Billing Method Description

1) Intra-region peering connection is available for free.
2) Cross-region peering connections (the VPC cross-region interconnections) & basic network cross-region interconnections:

- Postpaid on a daily basis. Payment is borne on the peering connection initiator.
- Calculated as the peak bandwidth of the day multiplied by the applicable tiered price.
- Peak bandwidth of the current day is calculated as this: bandwidth is captured once every 5 minutes, and the maximum one out of both inbound and outbound bandwidth of that day is taken as the peak bandwidth.
  For more information, please see the following table:

Feature	Billing Model	Configuration	Price	
			Beijing Shanghai Guangzhou	Singapore,Toronto,Korea,Frankfurt,Silicon Valley,Japan,Russia,Hong Kong
Intra-region Peering Connection	Free			
Cross-	Peak bandwidth	(0 , 20] Mbps	3.19	15

region Peering Connection	of the day Bill by days (USD/Mbps/day) Peak bandwidth is calculated as the average bandwidth every 5 minutes	(20 ,100] Mbps	1.98	12
		(100 , 500] Mbps	1.48	9
		(500 , 2000] Mbps	1.19	6
		> 2,000 Mbps	0.82	5

Contact business department to inquire more about the prices.

For more information about the prices of VPC services, please see VPC Price Overview.

Note:

1. In order for you to view the cost, the billing system describes peering connections as: bill for cross-region interconnection (mainland) and bill for peering connection of which both ends are in Mainland China
2. Basic network cross-region interconnection is **not supported in the following regions**: Shanghai Finance, Shenzhen Finance and Silicon Valley.

Free cross-region interconnection bandwidth campaign (Key customers are entitled to its benefits by default, but it is no longer available to common customers)

Benefits for VIP customers and common customers during the campaign are as follows:

VIP customers (The benefits are entitled to all VIP customers)

- Extra free bandwidth of 100Mbps is offered for each peering connection in Mainland China (automatically assigned by the system).

Common customers (The campaign is closed)

- An extra bandwidth of 10 Mbps is offered free of charge for each peering connection in Mainland China.

Note:

- It takes effect on the day the bandwidth remission is approved upon review. The bandwidth beyond the free quota is billed based on tiered prices. This is valid until December 31, 2017. You can view the remission details in the pop-up window for the creation of peering connection or in the details page.

- **This benefit is not applicable for basic network cross-region interconnection.**

Operation Instructions

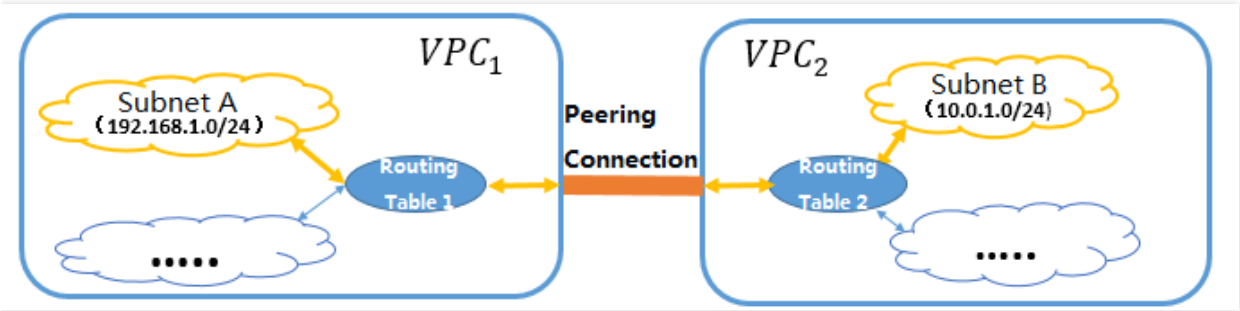
Quick Start

Cross-region connection and cross-account communication of VPC are both advanced features of peering connection, so you can take the following steps to implement cross-account and cross-region interconnections over peering connection.

- There are two steps to implement communication over peering connection:
  Step 1: Create a peering connection.
  Step 2: Set routing tables on both ends.

- There are three steps to implement cross-account communication over peering connection:
  Step 1: Create a peering connection.
  Step 2: Accept request for peering connection.
  Step 3: Set routing tables on both ends.

Example:
IP address range 1: The subnet A `192.168.1.0/24` of VPC1 in **Guangzhou**.
IP address range 2: The subnet B `10.0.1.0/24` of VPC2 in **Beijing**.
The following steps are required to achieve interconnection between IP address range 1 and IP address range 2 via peering connection:



Step 1: Create Peering Connection

1) Log in to Tencent Cloud Console, and click "Virtual Private Cloud" in the navigation bar.
2) Select the "Peering Connection" tab in the VPC console, and select the region "**Guangzhou**" and the VPC `VPC1` above the list, and then click "New" to create a peering connection.
3) Enter a name (such as `PeerConn`), select **Beijing** in "Peer Region", the "Peer account type" and `VPC2` in "Peer network".

- If the type of the peer account is "My Account", select it directly from the drop-down list.
- If the type of the peer account is "Other Accounts", enter the account ID and VPC ID of the peer account.

4) Select the maximum bandwidth

- For a intra-region peering connection, there is no restriction on bandwidth. **No modification** to this.
- A maximum bandwidth can be selected for a cross-region peering connection. Submit a ticket to request for a larger cross-region bandwidth.

5) A peering connection between the VPCs under the same account takes effect immediately upon its creation.
4) When you create a peering connection to a VPC under another account, the connection takes effect only after the peer accepts the connection request.

> Note: Any fees charged for a cross-region peering connection are paid by the initiator of the connection.

(Optional) Step 2: Accept Request for Peering Connection

If VPC2 belongs to other user, you need to notify the user to accept your request for peering connection.
1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar to select the "Peering Connection" in the VPC console.
2) Select the region **Beijing** above the list, find the peering connection to be accepted in the peering connection list: `PeerConn` , and click "Accept".
3) The creation of peering connection is completed.

> Note: When the peering connection is created, the interconnection between VPCs of both ends is not allowed until the route that is directed to the peering connection is added in "both" VPCs.

Step 3: Configure Routing tables on Both Ends for Peering Connection

1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar and select the "Subnet" tab in VPC console.
2) Click the ID of the routing table (routing table A) associated to the specified subnet (subnet A) on the local end of the peering connection, to go to the details page of the routing table.
3) Click to edit the routing policy. Enter the peer CIDR (`10.0.1.0/24`) for "Destination", select "Peering connections" for "Next hop type", and select the created peering connection (PeerConn) for "Next hop".
4) Save the routing table.
Use the same configuration for the peer routing table.

> Note:
> 1) You must configure routes on both ends before you can communicate via the peering connection.
> 2) For communication between multiple IP address ranges of two VPCs on both ends, you only need to **increase the corresponding routing tables** instead of creating multiple peering connections.

After the routing table is configured, the communication can be achieved between different IP address ranges of two VPCs.

Viewing Routing Policy Related to Peering Connection

1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar to select the "Peering Connection" in the VPC console.
2) Select the region and VPC above the list.
3) Click the ID of the specified peering connection to go to its details page. You can see in the related routing policy that the next hop is the destination IP address range, the associated subnet, and the related routing table of the peering connection.

> Note: If you have established a peering connection but cannot communicate via it, check whether the configurations of the routing tables on **both ends** are correct by taking this step.

Viewing Monitoring Data of Network Traffic over Cross-region Peering Connection (Cross-region Interconnection)

No upper limit is set on the network traffic for intra-region peering connection.
Monitoring of network traffic is only supported for cross-region peering connections.
1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar to select the "Peering Connection" in the VPC console.
2) Select the region and VPC above the list.
3) Click the Monitoring icon of the specified peering connection to view the **inbound/outbound bandwidth, number of inbound/outbound packets and packet loss**.

Configuring Traffic Control for Cross-region Peering Connection (Cross-region Interconnection)

Network traffic over intra-region peering connection is free of charge. No traffic control is applicable. Maximum bandwidth is 5 Gbps.
Traffic control is supported for cross-region peering connection.
1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar to select the "Peering Connection" in the VPC console.
2) Click the ID of corresponding peering connection in the list page to go to its details page.
3) In the basic information section, click "Change Bandwidth". Select the corresponding bandwidth, and save it to take effect.

Enabling Traffic Control Details for Peering Connection

After it is enabled, you can view the metrics of IP traffic flowing through a peering connection over the past 7 days, and also set the outbound bandwidth for an IP to flow to a specific peering connection.

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Peering Connection".
   2) In the peering connection list, click an ID to go to the peering connection details page.
   3) Click the "Monitor" tab, and enable the switch of "Traffic Control Details for Peering Connection" on the upper right corner.

After the Traffic Control Details for Peering Connection is enabled, it takes 5 to 6 days to collect and publish data. During this period, you can view the monitoring details table at the lower part of the monitoring chart.

Note: This feature is under internal trial. Submit a ticket to apply for it.

Setting Traffic Control Details for Peering Connection

After the Traffic Control Details for Peering Connection is enabled, you can set the outbound bandwidth for an IP to flow to a specific peering connection.

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Peering Connection".
   2) In the peering connection list, click an ID to go to the peering connection details page.
   3) Click the "Monitor" tab, find the IP for which monitoring details need to be set, and set a limit on its outbound bandwidth.

Viewing Traffic Control Details for Peering Connection

1. Log in to Tencent Cloud Console, click "Virtual Private Cloud" in the navigation bar to go to the VPC Console, and then select "Peering Connection".
   2) In the peering connection list, click an ID to go to the peering connection details page.
2. Click the "Monitor" tab, and then click "View Restricted IP" in the upper right of the table of traffic control details for peer connection.

Rejecting Peering Connection

You can reject the request for the peering connection with a status of "To be Accepted". Except for the accounts you trust, you can reject any unnecessary requests.

1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar and select the "Peering Connection" tab in VPC console.
2) View the peering connection to be accepted in the peering connection list, and click "Reject" button in the Operation column.
3) The peering connection is rejected and disappears.

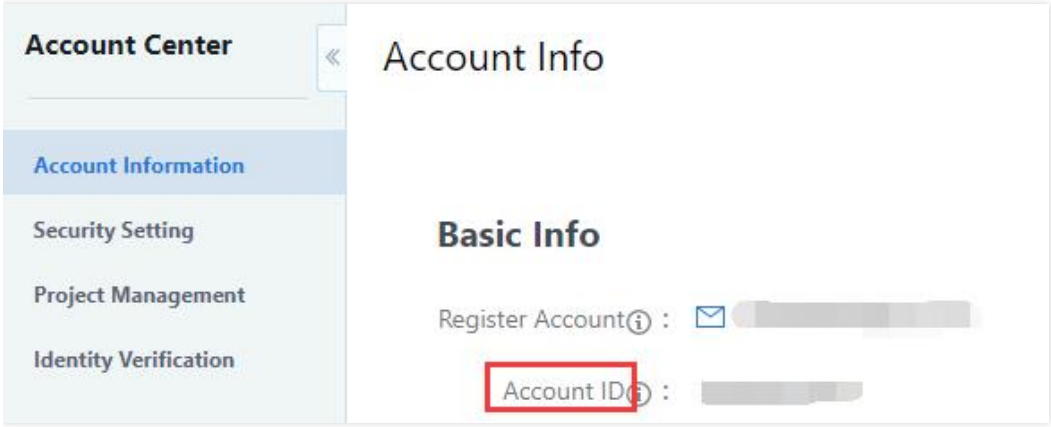
Deleting Peering Connection

The peering connection can be deleted on either end at any time, and becomes invalid immediately upon deletion. When the peering connection is deleted, the routing entry containing this peering connection in the routing table is also deleted.

1) Log in to [Tencent Cloud Console], and click "Virtual Private Cloud" in the navigation bar.
2) Select the "Peering Connection" tab in the VPC console to view the established peering connections in the peering connection list, and click "Delete" in the Operation column.
3) After you confirm the deletion action, the peering connection is deleted.

Viewing Peer Account ID

When you create a cross-account peering connection/shared Direct Connect, you need to enter the account ID for the peer **developer**, which you can check as follows:
1) Log in to Tencent Cloud Console, and click the account name on the upper right corner.
2) View the Account ID in Basic Info.



Deleting Peering Connection

The peering connection can be deleted on either end at any time, and becomes invalid immediately upon deletion. When the peering connection is deleted, the routing entry containing this peering connection in the routing table is also deleted.

1) Log in to [Tencent Cloud Console], and click "Virtual Private Cloud" in the navigation bar.
2) Select the "Peering Connection" tab in the VPC console to view the established peering connections in the peering connection list, and click "Delete" in the Operation column.
3) After you confirm the deletion action, the peering connection is deleted.

Enabling Basic Network Cross-region Interconnection

Submit a Ticket to apply for the basic network cross-region interconnection.

Setting Alarms for Cross-Region Interconnection

1) Log in to Tencent Cloud Console, click "Cloud Products" -> "Monitor & Management" -> "Cloud Monitor" in the top navigation bar, and select "My Alarms" -> "Alarm Policy" in the left navigation bar, and then click "Add Alarm Policy".
2) Enter the alarm "Policy Name", select "Peering Connection" or "Basic Network Cross-Region Interconnection" in Policy Type, and then add alarm triggering condition.
3) Associate alarm objects: select the alarm receiver group, and when it is saved, you can view the set alarm polices in Policy List.
4) View the alarm information: when any alarm conditions are triggered, you will receive SMS/email/internal message or other notices, and you can also find the information in the left navigation "My Alarms" -> "Alarm List".

API Overview

You can use API operations to set and manage your peering connection. For more information on additional resources in VPC, please see Overview of All VPC APIs.

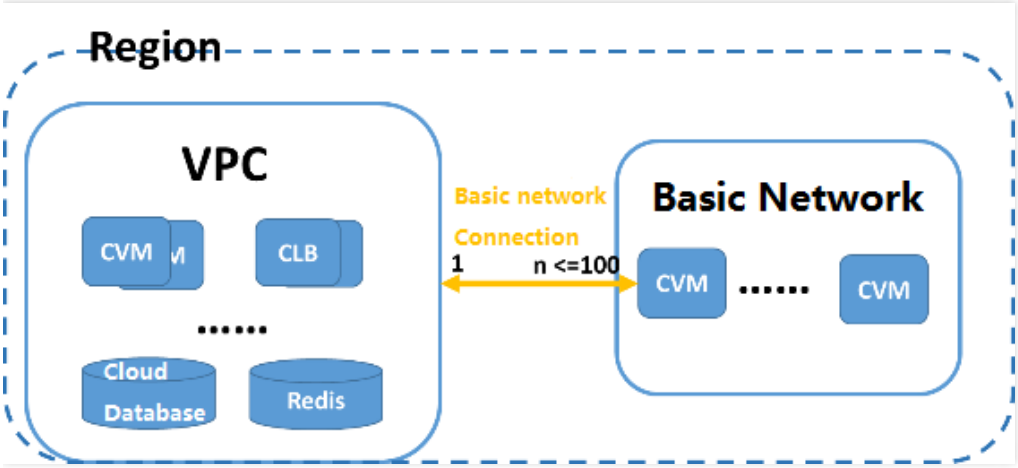
Feature	Action ID	Description
Create Intra-region peering connection	CreateVpcPeeringConnection	Create an intra-region peering connection.
Delete Intra-region peering connection	DeleteVpcPeeringConnection	Delete an intra-region peering connection.
Modify Intra-region peering connection	ModifyVpcPeeringConnection	Modify an intra-region peering connection.
Accept Intra-region peering connection	AcceptVpcPeeringConnection	Accept an intra-region peering connection.
Reject Intra-region peering connection	RejectVpcPeeringConnection	Reject an intra-region peering connection.
Enable expired Intra-region peering connection	EnableVpcPeeringConnection	Enable an expired intra-region peering connection.
Create cross-region peering connection	CreateVpcPeeringConnectionEx	Create a cross-region peering connection.
Delete cross-region peering connection	DeleteVpcPeeringConnectionEx	Delete a cross-region peering connection.
Modify cross-region peering connection	ModifyVpcPeeringConnectionEx	Modify a cross-region peering connection.
Accept cross-region peering connection	AcceptVpcPeeringConnectionEx	Accept a cross-region peering connection.
Reject cross-region peering connection	RejectVpcPeeringConnectionEx	Reject a cross-region peering connection.
Enable expired cross-region peering connection	EnableVpcPeeringConnectionEx	Enable an expired cross-region peering connection.
Query peering connection	DescribeVpcPeeringConnections	Query a peering connection.

Classiclink

Last updated：2018-10-18 15:51:03

Introduction

Classiclink means to associate CVMs in the basic network with specified VPCs, thus allowing CVMs in the basic network to communicate with cloud services in VPCs (such as CVMs and databases). By default, VPC network is completely isolated. Neither other VPCs nor the basic network is able to communicate with it. Peering Connection made it possible for different VPCs to communicate with each other. While communication between the basic network and a certain VPC is made possible by Classiclink. As shown in the figure below, the basic network CVM can access cloud resources within the VPC such as CVM, cloud database, private network cloud load balancer, cloud cache and so on. However, the CVM in the VPC can only access the basic network CVM which is interconnected with it, but not the other computing resources within the basic network. This feature only supports interconnection within the same region, as shown below.



Influence on Basic Network Interconnected CVMs Caused by Router, Security Group and Network ACL

- The private IP of the associated basic network CVM will be automatically added to the Local policy of the VPC's routing table, in which case the CVM in the VPC and services in this basic network will be able to communicate with each other. You do not need to manually modify the routing table rules in the current VPC.
- After the basic network CVM is associated with VPC, their security firewall and network ACL will remain effective. That is to say, you can restrict the access from associated basic network CVM by configuring network ACL for the VPC subnet. You can also configure security group rules for CVMs in the basic network and VPC to restrict network access for both directions.

Service Limits

- This feature only supports the interconnection between basic network and VPC. You cannot change the network environment for the CVM. Once the network environment (VPC or basic network) has been determined for the CVM, you will no longer be able to change it.
- A basic network CVM can be associated with only one VPC at a time.
- Currently, interconnection feature is only supported for VPC and basic network under the same region.
- Classiclink feature is only supported for VPCs within the network segment `10.[0~47].0.0/16`. The IP range for VPCs of other network segments may conflict with the basic network IP segment.
- CVM traffic during the Classiclink can only be routed to private IP address within the VPC, but not the other destinations other than the VPC. That is, the basic network CVM cannot access public network or VPC resources outside the current VPC through network equipment such as its VPN gateway, direct connect gateway, public network gateway, peering connection, NAT gateway and so on. Likewise, the peer of VPN, direct connection and peering connection cannot access the current basic network CVM either.
- The cloud load balancer instance within the VPC cannot be bound with the basic network CVM which is interconnected with the current VPC.
- Changing the private IP of the basic network CVM will cancel the association with the VPC, which means the original record will lose its functional effect. Please add the record again in the VPC Console if you wish to associate them.
- The interconnection relationship with VPC will not be unbound by actions against the CVM such as isolation due to arrears, security isolation, cold migration, failover, configuration modification, operating system switching and so on.
- The interconnection relationship with VPC will be automatically unbound if the CVM is returned.

Resource	Restriction	Description
Number of basic network CVMs that can be associated with each VPC	100	
Supported network segment	Only VPCs of the network segment `10.[0~47].0.0/16 (including subsets)` are supported	To prevent conflict between the IPs of basic network CVM and VPC
Supported cloud resources	Cloud virtual machine (CVM)	Cannot access basic network resources such as CDB, CMEM, LB, etc.

Billing Method

The Classiclink feature is free to use. Refer to Tencent Cloud VPC Pricing Overview for prices of other VPC services.

Instructions

Associating Basic Network CVM with VPC

Example:
If you wish to allow CVM "TomCVM" to communicate with VPC "TomVPC" via Classiclink, you will need to follow the following steps:
1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar to enter the VPC Console.
2) Select **Region: Beijing**, click the VPC to be interconnected with basic network (`TomVPC`) and enter its detail page.
3) Click "Classlink" tab, and click "Bind CVM" button.
4) In the pop-up window, select the CVM in the basic network to be associated with the VPC: `TomCVM` .
5) Click "OK" to complete the operation. The association relationship will take effect immediately.

Viewing CVMs Interconnected with the Basic Network

1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar to enter the VPC Console.
2) Select region, click the ID of the VPC to be interconnected with basic network and enter its detail page.
3) Click "Classlink" tab to view the list of basic network CVMs associated with the VPC.

Disassociating VPC and Basic Network CVM

1) Log in to Tencent Cloud Console. Click "Virtual Private Cloud" in the navigation bar to enter the VPC Console.
2) Click the ID of the VPC to be interconnected with basic network and enter its detail page.
3) Click "Classlink". In the list of basic network CVMs, select the CVM to be disassociated and click "Disassociate" button.
4) Click "OK" to complete the disassociation process.

Related APIs

You can use APIs to configure and manage the interconnection between your VPC and basic network. Refer to Overview of All VPC APIs for more information about VPC API services.