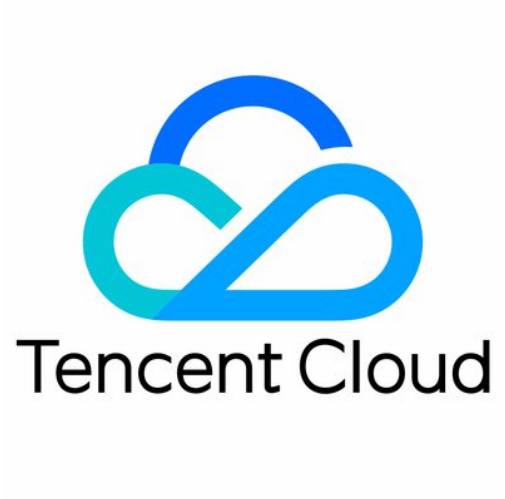
Cloud Connect Network

Operations Guide

Product Documentation



Contents

Operations Guide
Overview

Last updated : 2020-12-29 18:56:50

This documents describes common operations of using Cloud Connect Network and related products, such as creating and deleting CCN instances, associating a network instance, enabling an invalid route, and adjusting the outbound bandwidth cap.

Instance management

- Creating a CCN Instance
- Associating Network Instances
- Deleting a CCN Instance
- Disassociating a Network Instance
- Adding an IDC IP Range
- Disassociating a Cross-account VPC
- Associating a Cross-Account VPC

Route management

- Viewing Routing Information
- Viewing the Route Table of an Associated VPC
- Enabling a Route
- Disabling a Route

Bandwidth management

- Configuring Bandwidth
- Managing Bandwidth

Monitoring and alarms

- Viewing Monitoring Information

Instance Management
Creating a CCN Instance

Last updated : 2020-05-14 16:43:29

1. Log in to the Virtual Private Cloud Console.
2. Click **Cloud Connect Network** in the left sidebar pane to open the Cloud Connect Network (CCN) management page.
3. Click **+New**. The **New CCN instance** page appears.
4. Enter the following information: name, Billing Mode, Service Quality, Speed limit mode, and Description.
5. Associate a network instance. You can also associate one after creating the CCN instance.
   For example, to connect the CCN instance to subnet A (192.168.1.0/24) of VPC 1 in Guangzhou, select **Virtual Private Cloud**, **South China (Guangzhou)**, and the desired VPC.
6. Click **OK**.

Deleting a CCN Instance

Last updated : 2020-02-24 12:07:17

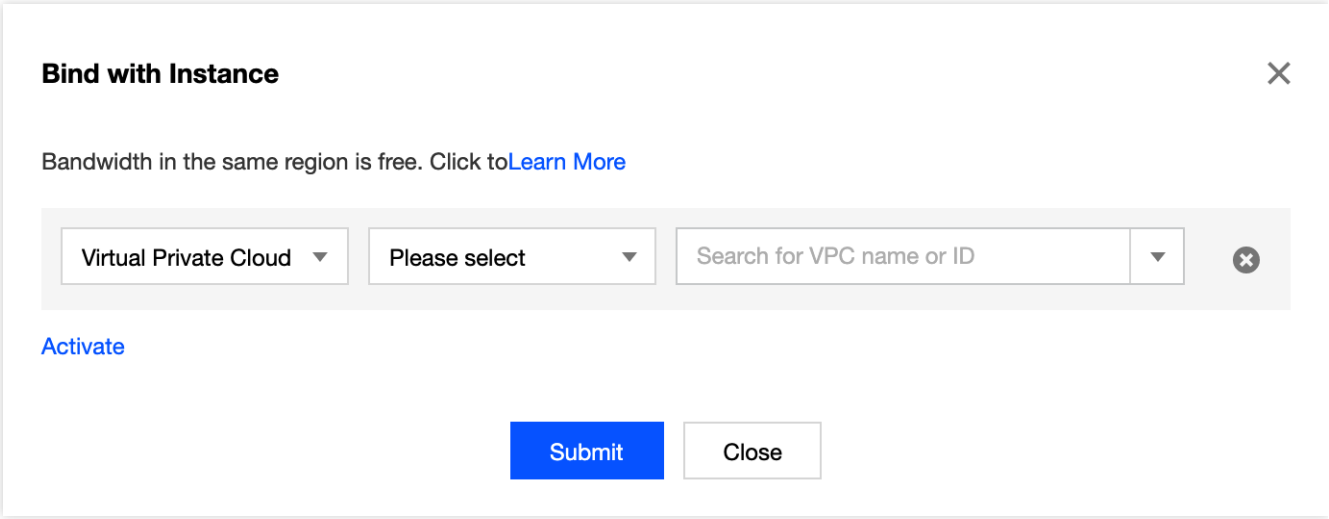
1. Log in to the Virtual Private Cloud Console.
2. Click **Cloud Connect Network** in the left sidebar to open the Cloud Connect Network (CCN) management page.
3. In the CCN list, find the row of the CCN instance to be deleted. Then, click **Delete** in the **Operation** column, and click **Confirm**.

> Note that all connections to the CCN instance are lost when the CCN instance is deleted. Please double check before the operation.

Associating Network Instances

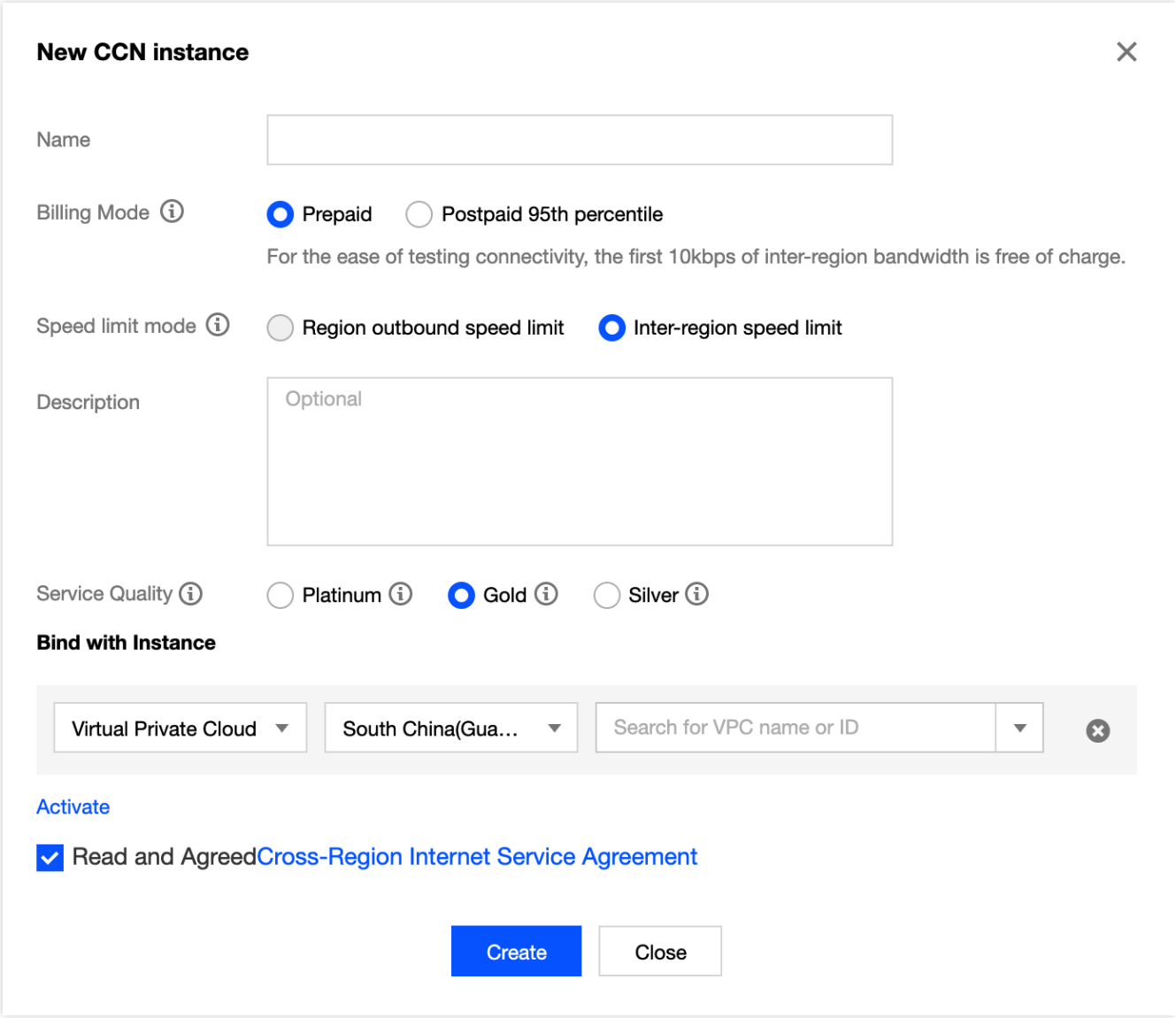
Last updated : 2020-05-12 16:20:15

1. Log in to the Virtual Private Cloud Console.
2. In the left sidebar, click **Cloud Connect Network** to open the Cloud Connect Network (CCN) management page.
3. Associate a network instance by using either of the following methods:
   Method 1: associate the network instance on the details page.
   i. Click the ID of the desired CCN instance to go to the instance details page. Click **Add an instance**. The **Associate with Instance** page appears.
   b. Set the type of the target network instance to **Virtual Private Cloud** or **Direct Connect Gateway** and select the region to which the network instance belongs and the network instance.
   c. (Optional) To associate more network instances, click **Add** and repeat the preceding step.
   d. Click **Submit**.



   Method 2: associate the network instance upon creation.
   When creating a CCN instance, add the network instance to be associated with the CCN

instance.

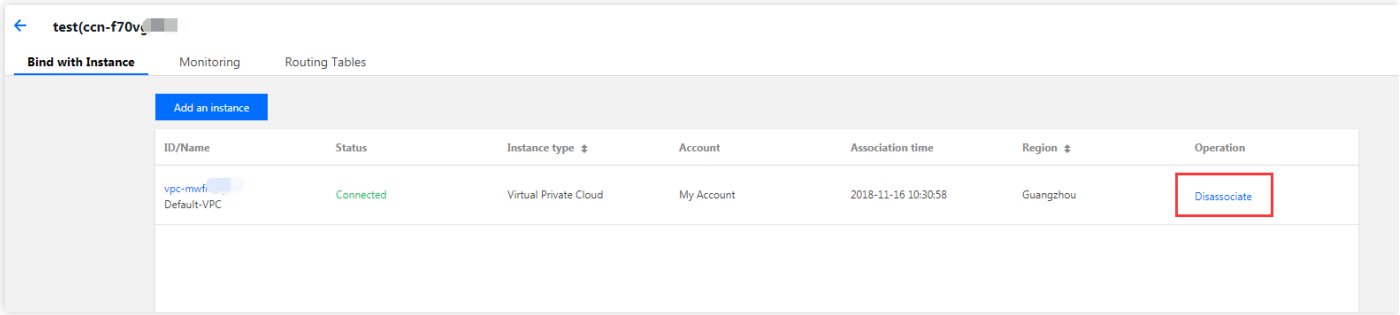


For more information on creating a network instance, refer to Creating VPC and Creating Direct Connect Gateway.

Disassociating a Network Instance

Last updated : 2020-02-24 12:02:59

1. Log in to the Virtual Private Cloud Console.
2. Click **Cloud Connect Network** in the left sidebar pane to open the Cloud Connect Network (CCN) management page.
3. In the CCN list, click the ID of the CCN to be disassociated to open the details page.
4. On the **Bind with Instance** tab, find the row of the network instance to be disassociated. Then, click **Disassociate** in the **Operations** column and click **Confirm**.



Adding an IDC IP Range

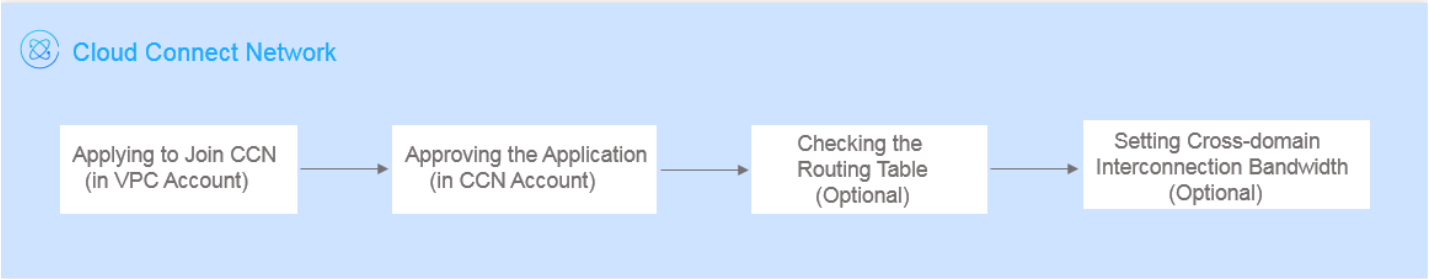
Last updated : 2020-02-24 12:08:21

1. Log in to the Virtual Private Cloud Console.
2. Click **Direct Connect Gateway** in the left sidebar.
3. In the list, click the new direct connect gateway associated with a Cloud Connect Network (CCN) to open the details page.
4. Click the **IDC Block** tab. Then, enter the IDC block to be connected, and click **Save**.

Associating a Cross-Account VPC

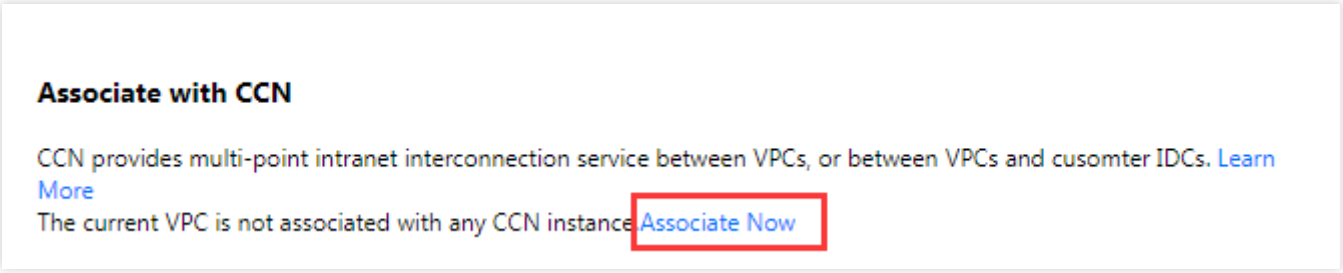
Last updated : 2019-11-25 14:41:19

To associate VPC and CCN under different accounts, the VPC account should initiate an association request. The association is established when the CCN account accepts the request.
The following figure illustrates the detailed steps:

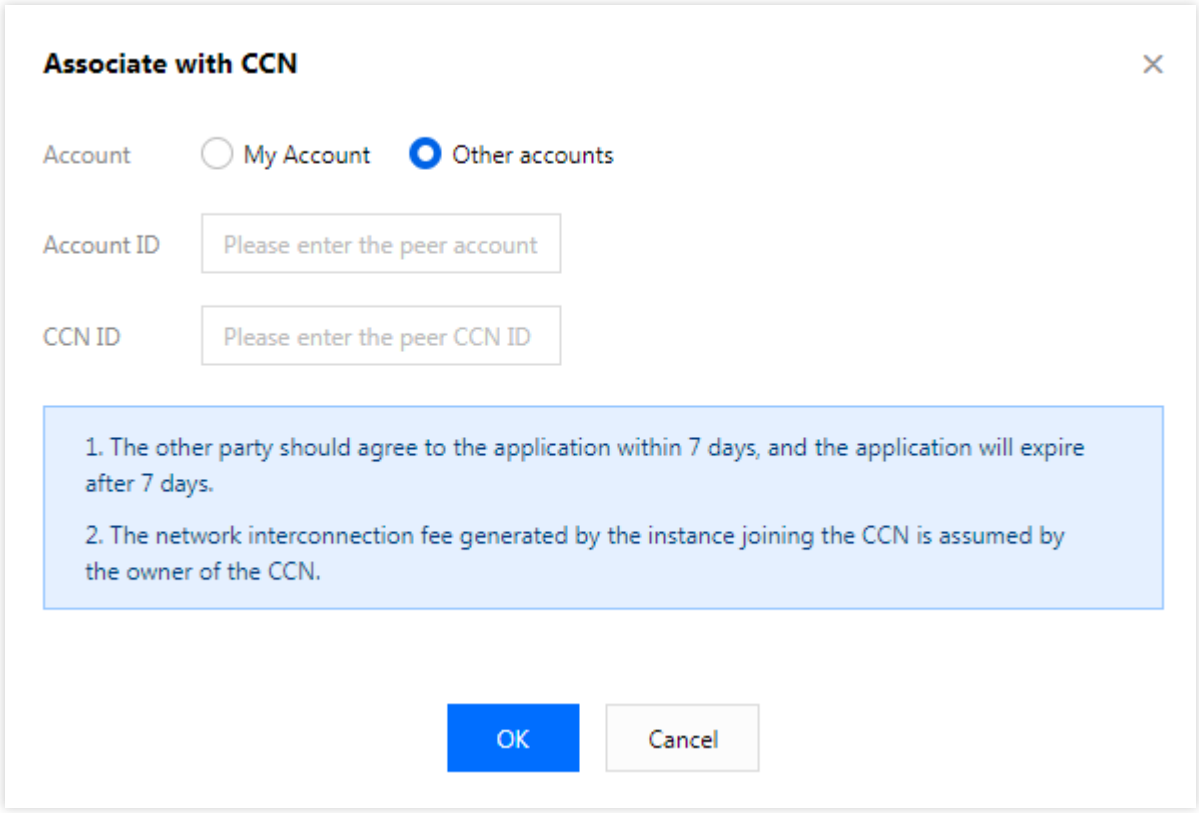


Submitting Association Request via a VPC Account

1. Log in to Tencent Cloud Console and choose **Products** > **Networking** > **Virtual Private Cloud** to open the VPC console.
2. Click **Virtual Private Cloud** in the left sidebar. Then, click the ID of the VPC to be added to a CCN to open the details page.
3. Click **Associate Now**.

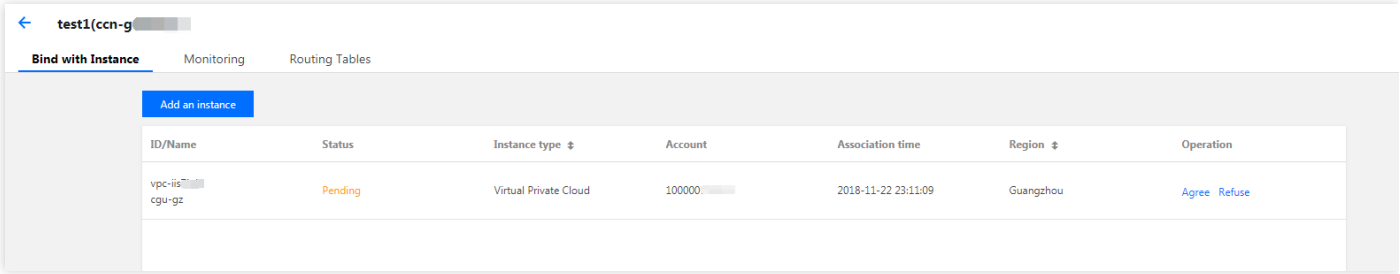


4. In the window that appears, enter the peer account ID and the peer CCN ID, and then click **OK** to submit the application.



Accepting the Application via the CCN Account

1. Log in to Tencent Cloud Console and choose **Products** > **Networking** > **Virtual Private Cloud** to open the VPC console.
2. Click **Cloud Connect Network** in the left sidebar. Then, click the ID of the CCN instance with a pending association request.
3. On the **Bind with Instance** tab page, find the information about the VPC to be approved, and click **Accept** to add the VPC to the CCN.



(Optional) Checking the Route Table

After the association request is accepted and the association succeeds, you need to view the route table to check whether the IP range of this instance conflicts with that of an existing CCN instance, to prevent a routing failure.
For more information about related operations, see Checking Route Table.

(Optional) Setting a Bandwidth for Cross-Region Interconnection

For more information about related operations, see Setting a Bandwidth for Cross-Region Interconnection.

Disassociate a Cross-account VPC

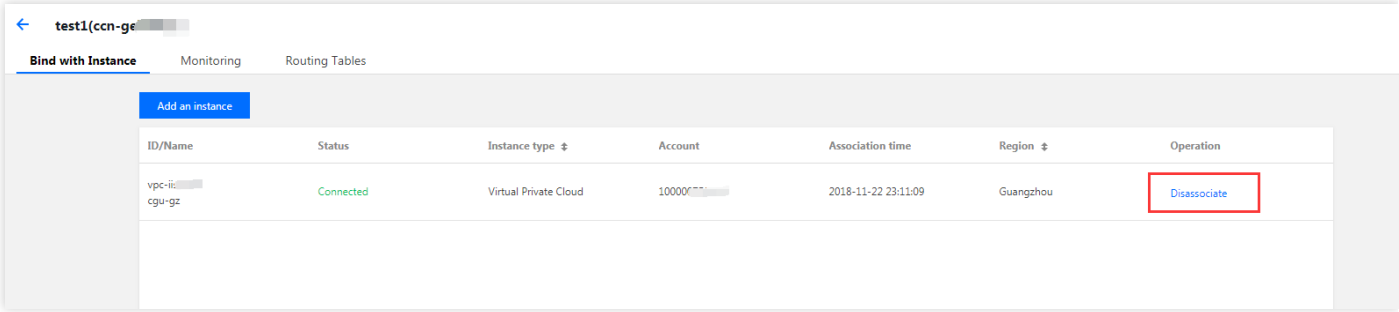
Last updated : 2020-05-14 16:43:29

You can associate a VPC under another account to your CCN instance. That association can be removed unilaterally by users from either account.

> Once the association is removed by either side, the connection it establishes is severed. Proceed with caution.

Method 1: Remove the Association Using the CCN Console

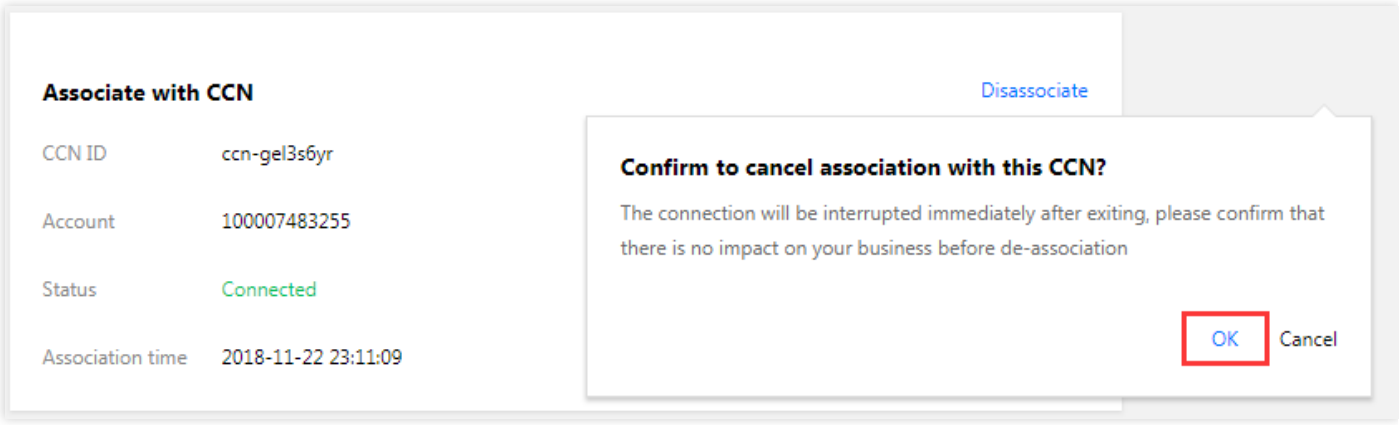
1. Log in to the Tencent Cloud Console and select **Cloud Products** > **Networking** > **VPC** to go to the VPC Console.
2. Click **Cloud Connect Network** in the left sidebar to open the CCN management page.
3. In the CCN list, click the ID of the desired CCN to open the details page.
4. On the **Associate with Instance** tab, find the desired network instance and click **disassociate** in the **Operations** column. The **Confirm to unbind this instance from the CCN** page appears. Click **Confirm**.



Method 2: Remove the Association Using the VPC Console

1. Log in to the Tencent Cloud Console and select **Cloud Products** > **Networking** > **VPC** to go to the VPC Console.
2. Click **Virtual Private Cloud** in the left sidebar, and then click the ID of the desired VPC to open the details page.

3. In the **Associate with CCN** section, click **Disassociate**. The **Are you sure you want to disassociate from this CCN instance?** page appears. Click **Disassociate**.



Route Management
Route Overview

Last updated : 2020-11-27 15:46:29

After a CCN instance is created, the system will automatically create a route table and control route entries to manage traffic on CCN. You cannot manually add or delete routes, but you can enable or disable them.

Automatic Route Addition

The logic of automatic route addition in CCN involves three stages as shown below:

1. Before addition: logic for receiving routes, i.e., determining which routes can be added to the CCN route table.
2. During addition: logic for default route application. This determines which routes added to CCN can take effect.
3. After addition: logic for setting route priority, i.e., determining which effective routes will forward traffic.

1. Before addition

- The associated instance is a VPC in the public cloud: for a new subnet, the destination is a subnet IP range, and the next hop is VPC route to CCN.
- The associated instance is a Direct Connect gateway: the destination is an IDC IP range, and the next hop is Direct Connect gateway route to CCN. There are two ways to pass the route:
  i. Manual entry (static): you need to manually enter the IDC IP range to be passed to CCN, and the next hop is the corresponding Direct Connect gateway, which facilitates IP range convergence and filtering.
  ii. Dynamic learning (BGP): this refers to dynamically learning about routes through BGP, and the next hop is the corresponding Direct Connect gateway, which makes it easy to perceive routing changes in IDC. Currently, routes published to CCN can be controlled based on AS-PATH:
    - If the AS-PATH lengths are the same, CCN will accept all routes.
    - If the AS-PATH lengths are different, CCN will accept routes with a shorter AS-PATH.

Note :

- Dynamic learning (BGP) is in beta testing. If you want to use it, please submit a ticket for application.
- AS-PATH description:
  i. The information of AS-PATH can be viewed in the Direct Connect gateway.
  ii. 32-bit string is supported. If the string is exceptional, the route will be deleted, and a string exception event will be reported, for which you can configure event alarming.
  iii. The maximum AS-PATH length is 30; if the maximum length is exceeded, the AS-PATH will be truncated, and a truncation event will be reported, for which you can configure event alarming.
  iv. Three AS numbers (45090, 139341, and 45090) will be added to the AS-PATH that passes through Direct Connect gateway - CCN - Direct Connect gateway.

2. During addition

- Check policy: if it overlaps any existing route, routes newly added will become invalid by default to avoid affecting existing routes. You can adjust their validity after assessing the impact.
- No-check policy: all routes will be valid except ECMP routes. For more information, please see the routing logic in same IP ranges in section 3 below.

> **Note :**
>
> The no-check policy feature is in beta testing. If you want to use it, please submit a ticket to apply.

3. After addition

- Different IP ranges overlapped: the longest mask matching principle is applied, which gives higher priority to more specific IP ranges. For example, if the destination IP range of route A is `10.0.1.0/20` and the destination IP range of route B is `10.0.1.0/24`, route B will be first matched based on the longest mask matching principle when both routes A and B are enabled.
- Same IP ranges: routes whose next hops are direct connect gateways support ECMP. For example, you can enable multiple routes whose destination IP ranges are `10.0.1.0/20`. Other routes do not support ECMP. This means that these routes cannot be enabled simultaneously. For example, if there are two or more routes whose destination IP ranges are `10.0.1.0/20` and whose next hops are VPC or VPC and direct connect gateway, only one route can be enabled.

> **Note :**
>
> See the following notes for the inbound route of the connection network architecture in CCN. More information can be viewed in Direct Connect Gateway Overview.

- The CCN direct connect gateway created before September 15, 2020, 00:00:00 publishes the route of subnet CIDR block to the dedicated tunnel. For a BGP dedicated tunnel, the VPC subnet CIDR block is synced to IDC based on the BGP protocol.
- The CCN direct connect gateway created after September 15, 2020, 00:00:00 publishes the route of VPC CIDR block to the dedicated tunnel. For a BGP dedicated tunnel, the VPC CIDR block is synced to IDC based on the BGP protocol..

Automatic Route Deletion

Next Hop Type	Trigger of Route Deletion
VPC in public cloud	VPC instance is unbound or subnet is deleted
Direct Connect gateway	1. Direct Connect gateway is unbound 2. Route is modified in Direct Connect gateway i. Manual entry (static): deletion ii. Dynamic learning (BGP): opposite route update

Viewing Routing Information

Last updated : 2020-02-24 11:53:04

1. Log in to the Virtual Private Cloud Console.
2. Click **Cloud Connect Network** in the left sidebar to open the Cloud Connect Network (CCN) management page.
3. In the CCN list, click the ID of the desired CCN to open the details page.
4. Click the **Route Tables** tab to view the route table of this CCN.

A route table is in one of the following states:

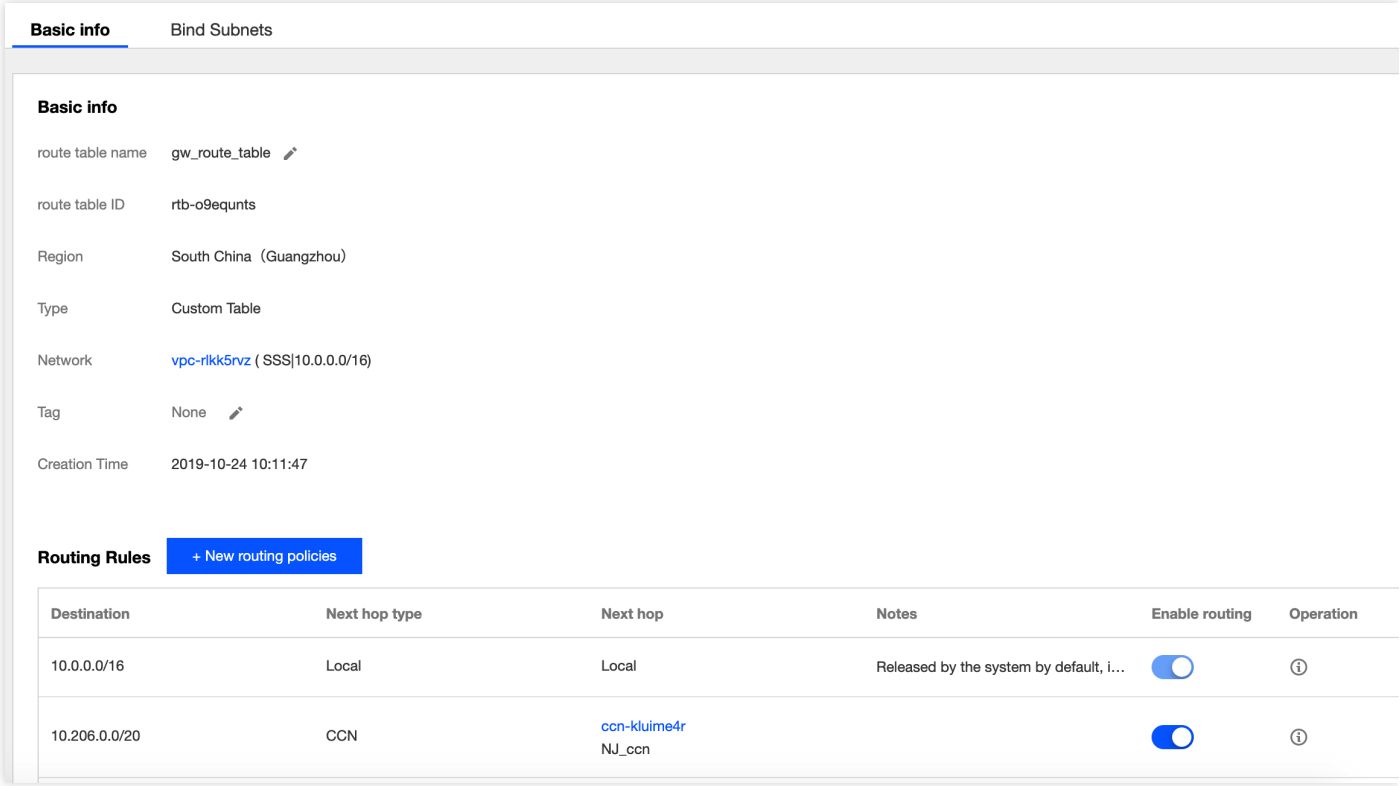
- If no IP range conflict occurs, the route table is **Valid** by default.
- If the route conflicts with an existing route, the route table is **Invalid**. For more information about the conflict rules and restrictions, see Use Limits - Routing Restrictions.

If you need to use an "invalid" route, see Disabling a Route and Enabling a Route.

Viewing the Route Table of an Associated VPC

Last updated : 2019-11-25 15:29:56

1. Log in to Tencent Cloud Console and choose **Products** > **Networking** > **Virtual Private Cloud** to open the Virtual Private Cloud (VPC) console.
2. Click **Route Tables** in the left sidebar.
3. Select a region and VPC above the table.
4. Click the ID of the target route table to open the details page. In the related routing policy, you can find the routing policy information of the associated Cloud Connect Network instance in the **Next Hop** column.

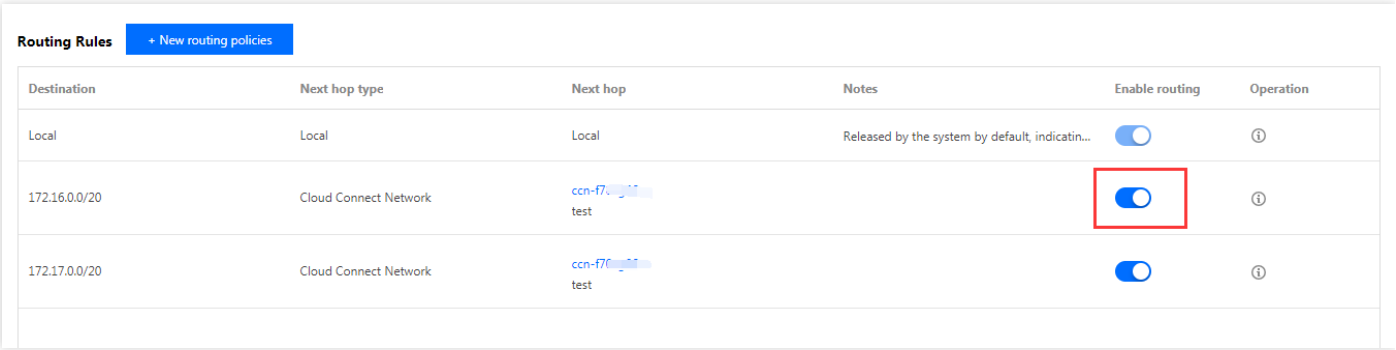


Disabling a Route

Last updated : 2019-11-25 15:51:18

> Disabling a route may affect running services. Therefore, ensure that no data is being forwarded through this route before performing this operation.

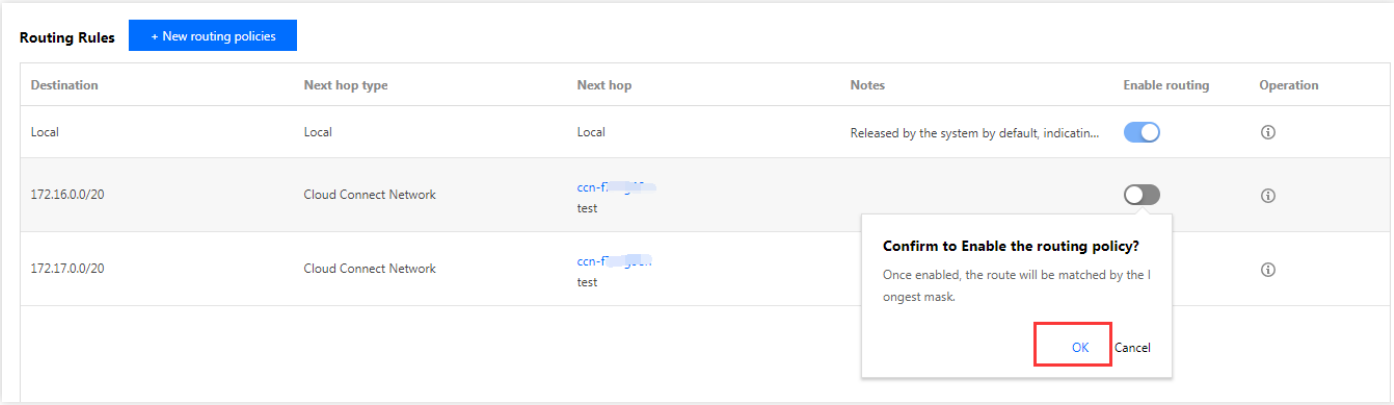
1. Log in to Tencent Cloud Console and choose **Products** > **Networking** > **Virtual Private Cloud** to open the Virtual Private Cloud (VPC) console.
2. Click **Route Tables** in the left sidebar.
3. In the list, click the ID of the route table to be modified to open the details page.
4. Find the routing policy to be disabled. Then, click the button in the **Enable Routing** column to disable the route, and click **OK** to confirm this operation.



Enabling a Route

Last updated : 2019-11-25 15:43:33

1. Log in to Tencent Cloud Console and choose **Products** > **Networking** > **Virtual Private Cloud** to open the Virtual Private Cloud (VPC) console.
2. Click **Route Tables** in the left sidebar.
3. In the list, click the ID of the route table to be modified to open its details page.
4. Find the routing policy to be enabled, and then click the button in the **Enable Routing** column to enable the route. If the enabled route conflicts with another route, disable or delete the latter.



Monitoring and Alarms
View Monitoring Information

Last updated : 2020-12-15 10:24:58

You can view network monitoring data of CCN instances in the console to facilitate your troubleshooting.

Directions

1. Log in to the VPC console and click **Cloud Connect Network** on the left sidebar.
2. On the CCN instance list page, click the **ID/Name** of the target monthly-subscribed CCN instance to enter its details page. Click the **Monitoring** tab.
3. View the following monitoring data of the current bandwidth limit type:
   - Region outbound bandwidth limit
     Select regions where network instances are associated with the CCN instance, and view **Region Bandwidth Out**, **Region Bandwidth In**, **Region Packets Out** and **Region Packets In**. You can filter to display the monitoring data for the last 24 hours, last 7 days or a custom time range.
     - Region Bandwidth Out: the average outbound traffic per second for network instances in the region
     - Region Bandwidth In: the average inbound traffic per second for network instances in the region
     - Region Packet Out: the total outbound traffic per second for network instances in the region
     - Region Packet In: the total inbound traffic per second for network instances in the region

     Note :

     Click the  icon to show more information of the monitoring data. Click the  icon to download it.

   - Inter-region bandwidth limit
     Select regions where network instances are associated with the CCN instance, and view **Inter-region outbound bandwidth**, **Inter-region inbound bandwidth**, **Packets out** and

Packets In. You can filter to display the monitoring data for the last 24 hours, last 7 days or a custom time range.

- Inter-region outbound bandwidth: the average outbound traffic per second for the two regions
- Inter-region inbound bandwidth: the average inbound traffic per second for the two regions
- Packets out: the total outbound traffic for the two regions
- Packets in: the total inbound traffic for the two regions

Note :

Click the  icon to show more information of the monitoring data. Click the  icon to download it.

4. To export monitoring data, click the top-right **Export Data**. You can also specify the time range, time granularity and export metric in the pop-up window and click **Export**.

Bandwidth Management
Configuring Bandwidth

Last updated : 2020-12-15 10:52:00

After a CCN instance is created and associated with network instances, you need to configure a bandwidth limit in both associated regions to enable communications. For a monthly-subscribed CCN instance, you also need to purchase bandwidth for the regions. Please note that the monthly-subscribed CCN instance is currently in beta. To try it out, please contact sales.

Prerequisites

- You have created a CCN instance and associated it with network instances as instructed in Creating a CCN Instance and Associating Network Instances.
- Check that there is no route conflict in the route table. For more information, see Viewing Routing Information.

Purchasing Bandwidth (for Monthly-subscribed CCN Instances)

If you create a monthly-subscribed CCN instance with default bandwidth, you can use a bandwidth of 10 Kbps free of charge in all regions. If you require a higher bandwidth, please purchase bandwidth in the regions to enable communications.

1. Log in to the VPC console and click **Cloud Connect Network** in the left sidebar.

2. On the CCN instance list page, click the **ID/Name** of the target monthly-subscribed CCN instance to enter its details page. Click the **Bandwidth Management** tab.

3. On the **Bandwidth Management** page, click **Purchase Bandwidth**. Perform the following operations in the pop-up window.

   i. Select the two regions associated with the CCN instance, and configure the bandwidth limit and usage period.

> **Note :**
>
> A bandwidth up to 10,000 Mbps can be configured.

ii. Click **Confirm**.

Configuring Inter-region Bandwidth Limit (for Pay-as-you-go CCN Instances Billed by Monthly 95th Percentile)

You can configure the inter-region bandwidth limit for pay-as-you-go CCN instances to control the bandwidth costs.

> **Note :**
>
> The default bandwidth cap is 1 Gbps. If you require a higher bandwidth, please submit a ticket.

1. Log in to the VPC console and click **Cloud Connect Network** in the left sidebar.
2. On the CCN instance list page, click the **ID/Name** of the target pay-as-you-go CCN instances to enter its details page. Click the **Bandwidth Management** tab.
3. Configure the bandwidth limit depending on the speed limit mode of the CCN instance:
   - Set inter-region bandwidth limit
     Click **Change Bandwidth**. Select **Region A** and **Region B** from the drop-down list, and set the bandwidth cap. You can also click **Add** to configure multiple bandwidth limit rules. After the configuration is complete, click **OK**.
   - Set the region outbound bandwidth limit
     Click **Adjust bandwidth speed limit**. In the pop-up window, select desired regions in the **Add region outbound speed limit** list on the left and set the bandwidth cap on the right. Click **OK**.
4. (Optional) Perform the following steps to change the bandwidth limit type to meet your requirements.
   i. Click **Change** on the right of **Speed limit mode**.
   ii. Select a bandwidth limit type from the drop-down list in the pop-up window.

> **Note :**
>
> Changing the bandwidth limit type will delete existing configurations. The bandwidth cap will be set to 1 Gbps by default. If you require a higher bandwidth, please submit a ticket.

Bandwidth Limit	Description
Region bandwidth out	The outbound bandwidth cap of a single region to other regions
Inter-region bandwidth	The inbound and outbound bandwidth cap between regions. Monthly-subscribed CCN instances only support inter-region bandwidth limit.

iii. Click **OK**.

Managing Bandwidth

Last updated : 2020-12-15 10:46:57

For a monthly-subscribed CCN instance, you can view, upgrade and renew its bandwidth in the console. For a pay-as-you-go CCN instance billed by monthly 95th percentile, you can view its bandwidth cap and change the bandwidth limit type in the console. Please note that the monthly-subscribed CCN instance is currently in beta. To try it out, please contact sales.

Prerequisites

- You have created a CCN instance and associated it with network instances as instructed in Creating a CCN Instance and Associating Network Instances.
- Check that there is no route conflict in the route table. For more information, see Viewing Routing Information.

Viewing the Bandwidth of Monthly-subscribed CCN Instances

1. Log in to the VPC console and click **Cloud Connect Network** in the left sidebar.
2. On the CCN instance list page, click the **ID/Name** of the target monthly-subscribed CCN instance to enter its details page. Click the **Bandwidth Management** tab.
   This tab displays the regions where the cross-region bandwidth applies, bandwidth cap, expiration time, and other information.
3. On the **Bandwidth Management** page, perform the following operations as needed.
   - Upgrade bandwidth
     a. Locate the bandwidth package to be upgraded, and click **Upgrade Bandwidth** in the **Operation** column.
     b. Set the bandwidth cap, check the auto-renewal box as needed and click **OK** in the pop-up window.
   - Renew bandwidth
     a. Locate the bandwidth package to be renewed and click **Renew** in the **Operation** column.
     b. Select the renewal duration, check the auto-renewal box as needed and click **OK** in the pop-up window.
   - Auto-renewal
     In the **Auto-renewal** column of the target bandwidth package, toggle the switch on.

Viewing the Bandwidth of Pay-as-you-go CCN Instances Billed by Monthly 95th Percentile

1. Log in to the VPC console and click **Cloud Connect Network** in the left sidebar.
2. On the CCN instance list page, lick the **ID/Name** of the target pay-as-you-go CCN instance to enter its details page. Click the **Bandwidth Management** tab.
   This tab displays the bandwidth cap of the current bandwidth limit type.
   - Inter-region bandwidth limit
   - Region outbound bandwidth limit
3. (Optional) Change the bandwidth limit type.
   i. Click **Change** on the right of **Speed limit mode**.
   ii. Select a bandwidth limit type from the drop-down list in the pop-up window.

> ⚠ **Note :**
>
> Changing the bandwidth limit type will delete existing configurations. The bandwidth cap will be set to 1 Gbps by default. If you require a higher bandwidth, please submit a ticket.

Bandwidth Limit	Description
Region bandwidth out	The outbound bandwidth cap of a single region to other regions
Inter-region bandwidth	The inbound and outbound bandwidth cap between regions. Monthly-subscribed CCN instances only support inter-region bandwidth limit.

   iii. Click **OK**.