Cloud Connect Network

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

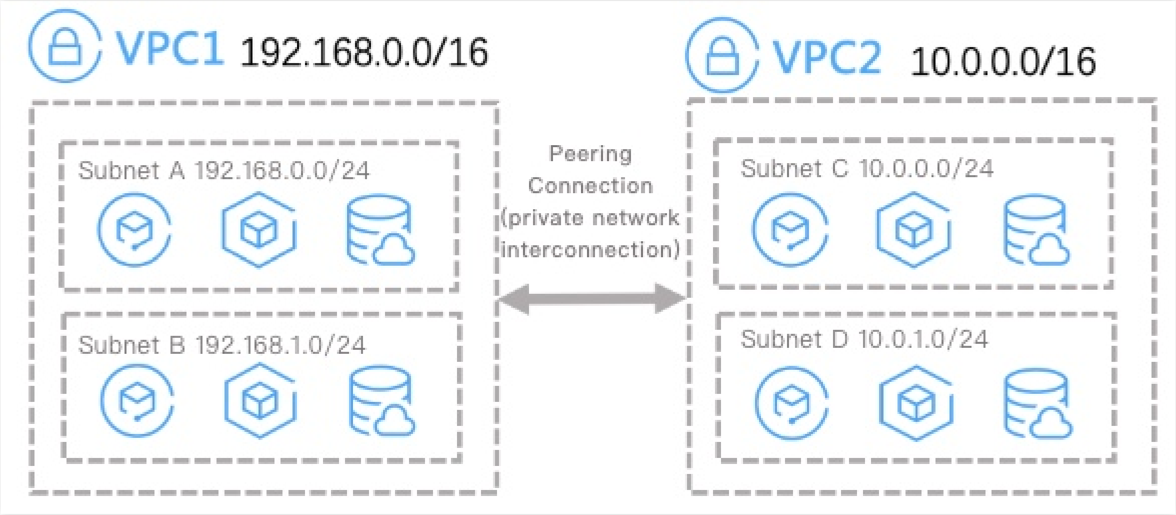
Migrating VPCs with Peering Connection to CCN

Last updated：2024-01-10 14:41:59

When the peering connection no longer meets your business requirements, you can smoothly migrate your network architecture to CCN, so as to get a quick and flexible access to the secure and reliable global network and achieve interconnection over the public and private network.

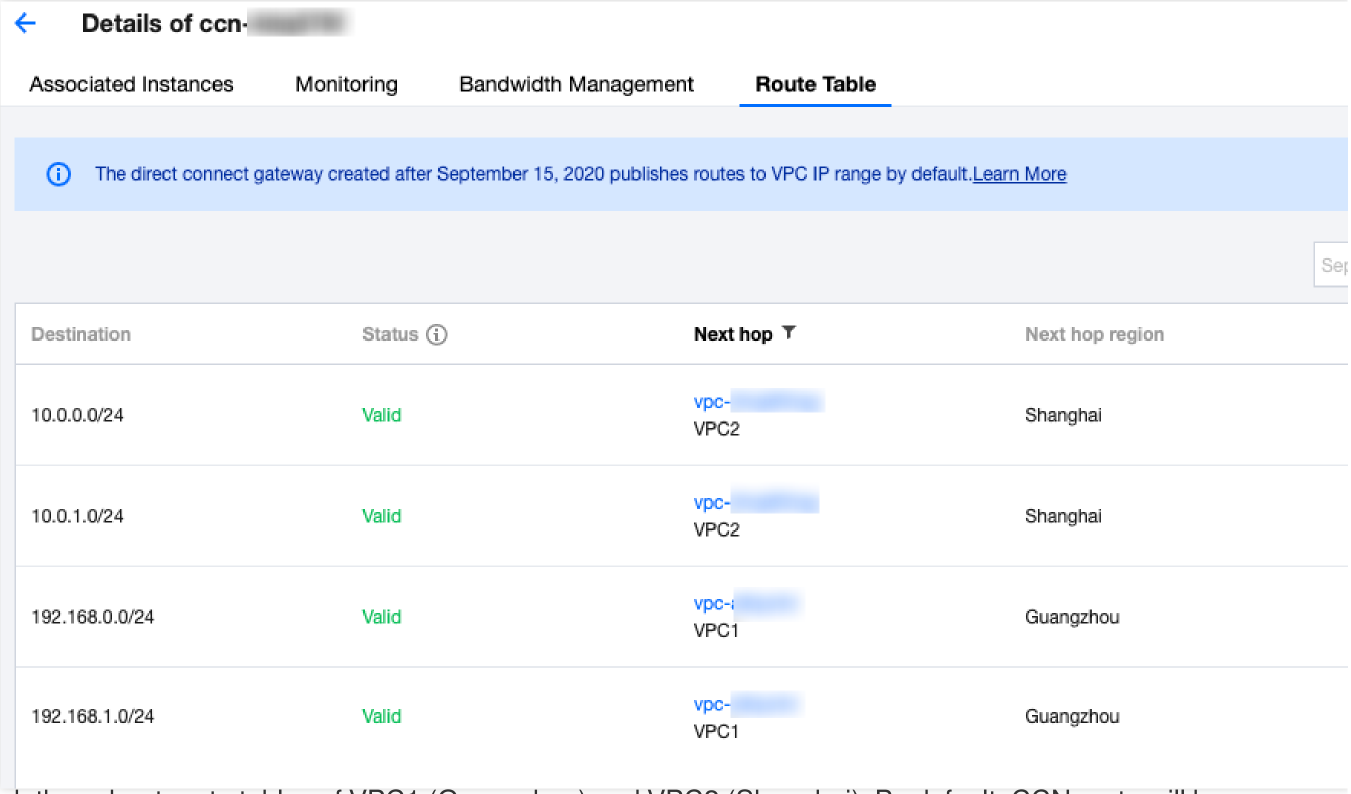
Scenario

VPC1 and VPC2 are peer connected and you want to migrate them to CCN, to allow them connect with other VPCs over the public and private network.
VPC1 (Guangzhou): 192.168.0.0/16, Subnet A: 192.168.0.0/24, Subnet B: 192.168.1.0/24.
VPC2 (Shanghai): 10.0.0.0/16, Subnet C: 10.0.0.0/24, Subnet D: 10.0.1.0/24.



Directions

1. Create a CCN instance by referring to Creating a CCN Instance. Skip this step if you already have one.
2. Associate VPC1 (Guangzhou) and VPC2 (Shanghai) with the corresponding CCN instance. For more information, see Associating Network Instances.
And then, in the CCN instance route table, you should see routing policies with VPC1 (Guangzhou) and VPC2 (Shanghai) subnets as destination. There are four routing policies in this example, pointing to subnets A, B, C, and D.



Details of ccn-[redacted]

The direct connect gateway created after September 15, 2020 publishes routes to VPC IP range by default.Learn More

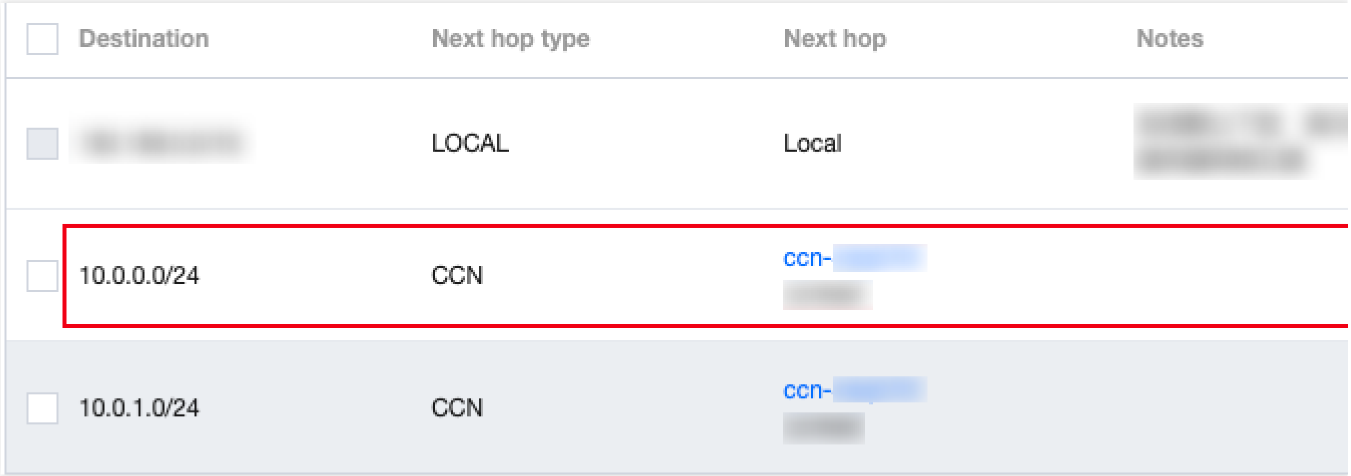
Destination	Status	Next hop	Next hop region
10.0.0.0/24	Valid	vpc-[redacted] VPC2	Shanghai
10.0.1.0/24	Valid	vpc-[redacted] VPC2	Shanghai
192.168.0.0/24	Valid	vpc-[redacted] VPC1	Guangzhou
192.168.1.0/24	Valid	vpc-[redacted] VPC1	Guangzhou

3. Check the subnet route tables of VPC1 (Guangzhou) and VPC2 (Shanghai). By default, CCN route will be distributed to subnet routes. If the distribution fails, you need to enable or disable necessary route manually complete the migration. There're three possible scenarios as follows.

Note:

Access the subnet route tables of VPC1 (Guangzhou) and VPC2 (Shanghai) as needed, and operate depending on the scenarios.

Scenario 1: the CCN route does not conflict with existing peering connections, the CCN route will take effect.



□	Destination	Next hop type	Next hop	Notes
□	[redacted]	LOCAL	Local	[redacted]
□	10.0.0.0/24	CCN	ccn-[redacted] [redacted]	
□	10.0.1.0/24	CCN	ccn-[redacted] [redacted]	

Complete the migration as follows:

1. **Disable** the route that using this peering connection as the next hop.

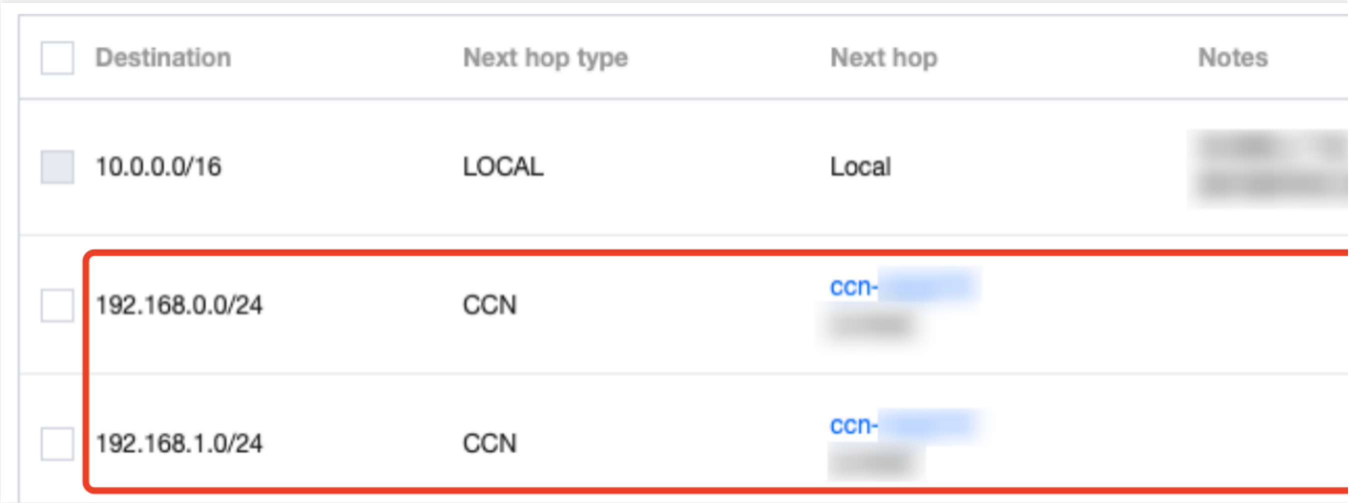
2. Check the monitoring data of network traffic over the peering connection. For more information, see Viewing Monitoring Data of Network Traffic.

Note：

You can delete the peering connection if there is no traffic go through it.

Scenario 2: the CCN route is included in the route of peering connection, the CCN route will be ignored by default.

The route with the longest mask will be matched and used for forwarding. You can manually enable the CCN route to make it effective.



□	Destination	Next hop type	Next hop	Notes
□	10.0.0.0/16	LOCAL	Local	[redacted]
□	192.168.0.0/24	CCN	ccn-[redacted]	
□	192.168.1.0/24	CCN	ccn-[redacted]	

Complete the migration as follows:

3.1.1 **Enable** the routing policies using CCN as the next hop.

3.1.2 View the monitoring data of network traffic over the peering connection. For more information, see Viewing Monitoring Data of Network Traffic.

Note:

You can delete the peering connection if there is no traffic go through it.

Scenario 3: if the CCN route includes or is the same as the peering connection route, the CCN route will be ignored by default.

The route with the longest mask will be matched and used for forwarding. You need to adjust the destination block of the peering connection route, and then manually enable the CCN route to make them effective. Complete the migration as follows:

3.1.1 Modify the route of the peering connection. Change the destination that includes the original destination block and with a subnet mask shorter than that of the CCN route. For example, change “10.0.0.0/24” to “10.0.0.0/16”.

3.1.2 **Enable** the route with CCN as the next hop.

After the change, traffic will be first forwarded via the route with CCN as the next hop, and the original route with peering connection as the next hop becomes invalid.

3.1.3 View the monitoring data of network traffic over the peering connection. For more information, see Viewing Monitoring Data of Network Traffic.

Note:

You can delete the peering connection if there is no traffic go through it.

Separate Deployment of Test Environment and Production Environment

Last updated：2024-01-10 14:41:59

You have activated the CCN service, and all VPCs in your organization have been interconnected through CCN. By default, network instances added to CCN are interconnected.

In certain scenarios, you can divide different network zones in your organization network, and network instances in different zones are isolated from each other. This can be implemented through the custom route table feature of CCN. Specifically, you can plan different custom route tables for CCN and associate different network instances with them in order to isolate network instances.

Note:

The custom route table feature is currently in beta test. To try it out, please submit a ticket.

Overview

The network instances associated with CCN are divided into a test zone and a production zone. Network instances are interconnected within the same zone but isolated across zones.

As shown below, create two custom route tables for the CCN instance: the test route table and the production route table.

Here:

The test route table only receives and learns routes from and is bound to the test VPC.

The production route table only receives and learns routes from and is bound to the production VPC.

Prerequisites

1. You have activated the CCN service and created a CCN instance. For detailed directions, please see Creating a CCN Instance.
2. The CCN instance has been associated with 4 network instances (for verification and subject to your actual business needs). For detailed directions, please see Associating Network Instances.

Directions

Step 1. Plan a custom route table

According to the isolation of network zones, two custom route tables need to be planned: the test route table and the production route table.

The routing plan of the custom route table is as follows:

Item	Test Route Table	Production Route Table
Route reception policy	Receive the routes of the network instances in the network zone of the test environment, i.e., routes of the test frontend VPC and the test backend VPC.	Receive the routes of the network instances in the network zone of the production environment, i.e., routes of the production frontend VPC and the production backend VPC.
Bound network instance	Bind the network instances in the network zone of the test environment, i.e., the test frontend VPC and test backend VPC.	Bind the network instances in the network zone of the production environment, i.e., the production frontend VPC and production backend VPC.

Step 2. Create a custom route table

1. Log in to the CCN console.
2. In the CCN list, click the CCN ID to enter the details page and access the **Route Table** tab.
3. Click **Create Route Table**.
4. In the pop-up window, enter the name and other information.
5. Click **OK**.
6. Repeat steps 3–5 to create the production route table.

Step 3. Set the route reception policy

1. Click the test route table ID to enter the details page and access the **Route Reception Policy** tab.
2. Click **Add Network Instance**.
3. On the **Select a network instance** tab, select the network instances in the test zone, i.e., the test frontend VPC and test backend VPC.
4. Click **OK** to complete the route reception policy configuration of the test route table.
5. Select the production route table and repeat steps 1–4 to configure its route reception policy.

Step 4. Bind a network instance

1. Click the test route table ID to enter the details page and access the **Bind an Instance** tab.
2. Click **Bind Network Instance**.
3. On the **Select a network instance** tab, select the network instances in the test zone, i.e., the test frontend VPC and test backend VPC.
4. Click **OK** to complete binding the test route table to network instances.

5. Select the production route table and repeat steps 1–4 to bind it to network instances.

Control of Interconnection Between Internal Network and Partner Network

Last updated：2024-01-10 14:41:59

You have activated the CCN service, and all VPCs in your organization have been interconnected through CCN. By default, network instances added to CCN are interconnected.

In certain scenarios, you may want to restrict your partner's network instances from directly accessing your organization's internal network zone without affecting the interconnection between internal VPC network instances. This can be implemented through the custom route table feature of CCN. Specifically, you can plan different custom route tables for CCN and create an interconnection VPC, through which your partner's VPC can access your internal network zone.

Note:

The custom route table feature is currently in beta test. To try it out, please submit a ticket.

Overview

The network instances associated with CCN are divided into an internal zone, a peering zone, and an external partner zone. Network instances in the internal zone are interconnected, while the partner VPC access the internal zone through the interconnection VPC.

As shown below, create three custom route tables for the CCN instance: the internal route table, the interconnection route table, and the external route table.

Here:

Internal VPCs are interconnected after they are bound to the internal route table.

The interconnection VPC is bound to the interconnection route table, which contains the routing information of the internal VPCs and the partner VPC.

The partner VPC is bound to the external route table, which contains only the routing information of the interconnection VPC.

Prerequisites

1. You have activated the CCN service and created a CCN instance. For detailed directions, please see Creating a CCN Instance.
2. The CCN instance has been associated with 4 network instances (for verification and subject to your actual business needs). For detailed directions, please see Associating Network Instances.

Directions

Step 1. Plan a custom route table

According to the conditions of network zones, three custom route tables need to be planned: the internal route table, the interconnection route table, and the external route table.

The routing plan of the custom route table is as follows:

Item	Internal Route Table	Connection Route Table	External Route Table
Route reception policy	Receive the routes of the network instances in the internal network zone, i.e., routes of the internal VPCs.	Receive the routes of the network instances in the internal network zone and partner network zone, i.e., routes of the internal VPCs and partner VPC.	Receive the routes of the network instances in the interconnection network zone, i.e., routes of the interconnection VPC.
Bound network instance	Bind network instances in the internal network zone, i.e., internal VPCs.	Bind network instances in the interconnection network zone, i.e., the interconnection VPC.	Bind network instances in the partner network zone, i.e., the partner VPC.

Step 2. Create a custom route table

1. Log in to the CCN console.
2. In the CCN list, click the CCN ID to enter the details page and access the **Route Table** tab.
3. Click **Create Route Table**.
4. In the pop-up window, enter the name and other information.
5. Click **OK**.
6. Repeat steps 3–5 to create the interconnection route table and external route table.

Step 3. Set the route reception policy

1. Click the internal route table ID to enter the details page and access the **Route Reception Policy** tab.
2. Click **Add Network Instance**.
3. On the **Select a network instance** tab, select the network instances in the internal network zone, i.e., the internal VPC 1 and internal VPC 2.
4. Click **OK** to complete the route reception policy configuration of the internal route table.
5. Repeat steps 1–4 to configure the route reception policies of the interconnection route table and external route table.

Note:

Please set according to the route table reception policy in the route plan.

Step 4. Bind a network instance

1. Click the internal route table ID to enter the details page and access the **Bind an Instance** tab.
2. Click **Bind Network Instance**.
3. On the **Select a network instance** tab, select the network instances in the internal zone, i.e., the internal VPC 1 and internal VPC 2.
4. Click **OK** to complete binding the internal route table to the network instance.
5. Repeat steps 1–4 to bind the interconnection route table and external route table to network instances.

Network Firewall Deployment

Last updated：2024-01-10 14:41:59

You have activated the CCN service, and all VPCs in your organization have been interconnected through CCN. By default, network instances added to CCN are interconnected.

In certain scenarios, you may want to control the interconnection between network instances. This can be implemented through the custom route table feature of CCN. Specifically, you can plan different custom route tables for CCN to manage business VPC interconnection with the firewall VPC.

Note:

The custom route table feature is currently in beta test. To try it out, please submit a ticket.

Overview

The network instances associated with CCN are divided into a business zone and a firewall zone, and the interconnection between network instances in the business zone is managed by the firewall VPC.

As shown below, create two custom route tables for the CCN instance: the business route table and the firewall route table.

Here:

The business route table only receives and learns routes from the firewall VPC and is bound to the business VPC.

The firewall route table only receives and learns routes from the business VPC and is bound to the firewall VPC.

Prerequisites

1. You have activated the CCN service and created a CCN instance. For detailed directions, please see Creating a CCN Instance.

2. The CCN instance has been associated with 3 network instances (for verification and subject to your actual business needs). For detailed directions, please see Associating Network Instances.

Directions

Step 1. Plan a custom route table

According to the conditions of network zones, two custom route tables need to be planned: the business route table and the firewall route table.

The routing plan of the custom route table is as follows:

Item	Business route table	Firewall route table
Route reception policy	Receive the routes of the network instances in the network zone of the firewall, i.e., routes of the firewall VPC.	Receive the routes of the network instances in the network zone of the business, i.e., routes of the business VPC 1 and business VPC 2.
Bound network instance	Bind the network instances in the network zone of the business, i.e., the business VPC 1 and business VPC 2.	Bind the network instances in the network zone of the firewall, i.e., the firewall VPC.

Step 2. Create a custom route table

1. Log in to the CCN console.
2. In the CCN list, click the CCN ID to enter the details page and access the **Route Table** tab.
3. Click **Create Route Table**.
4. In the pop-up window, enter the name and other information.
5. Click **OK**.
6. Repeat steps 3–5 to create the firewall route table.

Step 3. Set the route reception policy

1. Click the business route table ID to enter the details page and access the **Route Reception Policy** tab.
2. Click **Add Network Instance**.
3. On the **Select a network instance** tab, select the firewall VPC.
4. Click **OK** to complete the route reception policy configuration of the business route table.
5. Select the firewall route table and repeat steps 1–4 to configure its route reception policy.

Note:

Please set according to the route table reception policy in the route plan.

Step 4. Bind a network instance

1. Click the business route table ID to enter the details page and access the **Bind an Instance** tab.
2. Click **Bind Network Instance**.
3. On the **Select a network instance** tab, select the network instances in the business zone, i.e., the business VPC 1 and business VPC 2.
4. Click **OK** to complete binding the business route table to network instances.
5. Select the firewall route table and repeat steps 1–4 to bind it to network instances.

Managing Subnet Routes by Configuring Route Table Selection Policy

Last updated：2024-01-10 14:41:59

You can assign different addressing routes for subnets in the same VPC by configuring and managing route table selection policy and using the custom route tables. Thus, you can manage the paths requested by the networks in CCN in a more fine-grained manner.

Note:

The custom route table and route table selection policy features are currently in beta test. To try it out, please submit a ticket.

Overview

You can assign different addressing route tables for subnets in different business VPCs by configuring route table selection policy.

For example, we create three **custom route tables** for the CCN instance, i.e. business route table 1, business route table 2 and office route table. We configure the next hop route table of subnet 2 in the business VPC as business route table 2 by adding the route table selection policy.

The information is as follows:

The business route table 1 only receives and learns routes from the office VPC 1 and is bound to the business VPC.

The business route table 2 only receives and learns routes from the office VPC 2 and is not bound to any network instance.

The office route table receives and learns routes from the business VPC and is bound to the office VPC 1 and office VPC 2.

Prerequisite

1. You have activated CCN service and created a CCN instance. For more information, see Creating a CCN Instance.
2. You have associated three network instances in the CCN instance (it is for verification, you can configure this based on your actual needs). For more information on how to associate network instances, see Associating Network Instances.

Directions

Step 1: planning for the custom route table and route table selection policy

Plan of the custom route table

The routing plan of the custom route table is as follows:

Item	Business route table 1	Business route table 2	Office route table
Route reception policy	Office VPC 1	Office VPC 2	Business VPC
Bound network instance	Business VPC	Not bound to any network instance	Office VPC 1 and office VPC 2

Plan of route table selection policy

Source network instance	Source IP range	Next hop route table
Business VPC	10.0.100.0/24	Business route table 2

Step 2: creating a custom route table

1. Log in to the CCN Console.
2. In the CCN list, click the **ID**/**Name** of the desired CCN instance to open the **Route Table** tab.
3. Click **Create Route Table**.
4. Enter the name and other relevant information in the pop-up window.
5. Click **OK** to complete the creation for business route table 1.
6. Repeat steps 3-5 to create business route table 2 and office route table.

Step 3: setting the route reception policy

1. Click the ID of business route table 1 to enter the details page and access the **Route Reception Policy** tab.
2. Click **Add Network Instance**.
3. Select "Office VPC 1" in **Select a Network Instance** tab.
4. Click **OK** to complete the route reception policy configuration for the business route table 1.
5. Repeat steps 1-4 to configure route reception policy for business route table 2 and office route table.

Note:

Please set according to the route table reception policy in the route plan.

Step 4: binding a network instance

1. Click the ID of business route table 1 to enter the details page and access the **Bind an Instance** tab.
2. Click **Bind Network Instance**.
3. Select "Business VPC" in the **Select a Network Instance** tab.
4. Click **OK** to complete binding the business route table 1 to the network instance.
5. Select the office route table and repeat steps 1-4 to bind it to the network instance.

Note:

Business route table 2 is not bound to any network instance.

Step 5: configuring route table selection policy

1. Click **Add Policy** in the **Route Table Selection Policy** tab.
2. Enter relevant parameters in **Add route table selection policy** pop-up window. Source network instance: business VPC; source IP range: 10.0.100.0/24; next hop route table: business route table 2.
3. Click **OK** to complete adding the route table selection policy.