Cloud Connect Network

Operation Guide

Product Documentation

Contents

Operation Guide
- Operations Overview
- Documentations of CCN's Multi-Route Table Feature
- Instance Management
  - Creating a CCN Instance
  - Associating Network Instances
  - Checking Associated Network Instances
  - Deleting a CCN Instance
  - Disassociating a Network Instance
  - Publishing IP Ranges through Direct Connect Gateway to CCN
  - Disassociate a Cross-account VPC
  - Associating Cross-Account VPC
- Route Management
  - Route Tables and Route Overview
    - Route Overview
    - Custom Definition Route Tables
  - Viewing Routing Information
  - Viewing the Route Table Associated with VPC
  - Enabling a Route
  - Disabling a Route
- Bandwidth Management
  - Configuring Bandwidth
  - Managing Bandwidth
- Monitoring and Alarms
  - Viewing Monitoring Data
  - CCN Cross-Region Flow Logging

Operation Guide
Operations Overview

Last updated：2024-01-10 14:41:59

This document guides you through an index of instructions on various CCN operations 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 a Network Instance
Checking Associated Network Instances
Deleting a CCN Instance
Disassociating a Network Instance
Publishing an IP Range Through Direct Connect Gateway to CCN
Associating a Cross-Account VPC
Disassociating a Cross-account VPC

Route Management

Route Overview
Viewing Routing Information
Viewing the Route Table with VPC Associated
Enabling a Route
Disabling a Route

Bandwidth Management

Configuring Bandwidth
Managing Bandwidth

Monitoring and Alarms

Viewing Monitoring Information

Documentations of CCN's Multi-Route Table Feature

Last updated：2024-01-10 14:41:59

CCN allows you to customize a route table and a route selection policy to flexibly manage the connections between network instances and manage routes at a finer granularity.

Best Practices

Isolated Deployment of Test and Production Environments
Connecting Internal Network and Partner Network
Network Firewall Deployment
Managing Subnet-Level Route by Using Route Table Selection Policies

Instance Management
Creating a CCN Instance

Last updated：2024-01-10 14:41:59

CCN connects a VPC with another or with IDCs. This document describes how to create a CCN.

Directions

1. Log in to the CCN Console.
2. Click **+Create** at the top of the **CCN** page.
3. Complete the following configurations in the **Create a CCN instance** pop-up window.

Field	Subfield	Description
Name	-	Name of the CCN instance
Billing Mode	Pay-as-you-go by monthly 95 percentile	Bill the actual bandwidth usage of the current month on 95th percentile basis. It's applicable to business with fluctuating bandwidth demands.
Service Level	Platinum	It’s ideal for key businesses that require extremely high communication quality, such as payment.
	Gold	It’s suitable for businesses that require high communication quality, such as game acceleration.
	Silver	It’s suitable for cost-sensitive jitter-insensitive businesses, such as data backup.
Bandwidth Limit Mode	Inter-region Bandwidth Cap	The inbound and outbound bandwidth cap between two regions

4. Click **OK**.

Subsequent Operations

After creating a CCN instance, you need to associate network instances with it, check its route table, and configure the bandwidth to enable interconnection.
For more information on how to associate network instances, see Associating Network Instances.

For more information on how to check whether the routing policies of each subnet in the VPC associated with the CCN take effect, see Viewing Routing Information.
For pay-as-you-go CCN instances billed by monthly 95th percentile, you can configure a cross-region bandwidth cap as needed to control the bandwidth cost. For detailed directions, see Configuring Bandwidth.

Associating Network Instances

Last updated：2024-01-10 14:41:59

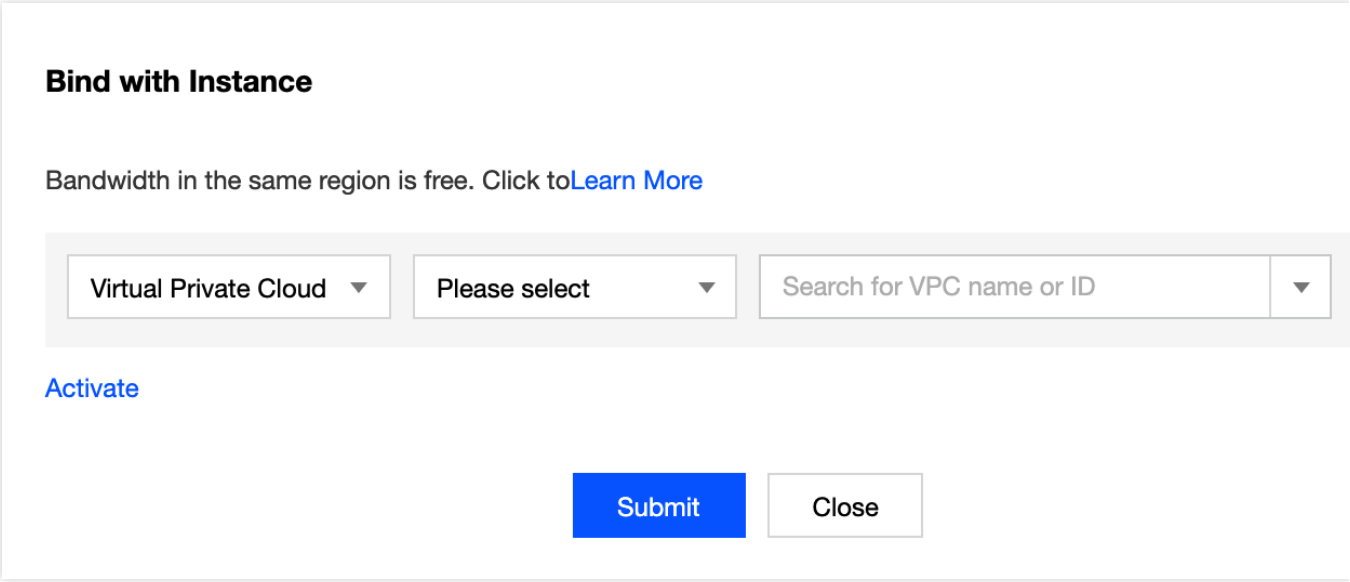
1. Log in to the CCN console and access the CCN management page.
2. Click the **ID/Name** of the desired CCN instance to access the **Associated Instances** page. Click **Add an instance**.
3. In the pop-up window, select a network instance type from **VPC**, **Direct Connect Gateway**, **BM Virtual Private Cloud**, and **VPN Gateway**. Select the region to which the network instance belongs and the specific network instance.

Note

For CCN to automatically add the routes from the VPN gateway, the VPN gateway for CCN has the VPN tunnel created and SPD policy configured. For more information, see Connecting IDC to CCN.

(Optional) To associate more network instances, click **Add** and follow the preceding steps.

Click **OK**.



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

Checking Associated Network Instances

Last updated：2024-01-10 14:41:59

This document introduces how to view network instances associated with a CCN instance.

Directions

1. Log in to the CCN console.
2. Locate the target CCN instance, click the instance ID/name in the **ID/Name** column or click **Manage Instances** in the **Operation** column.
3. On the **Associate with Instance** tab page, you can see all the network instances associated with the current CCN instance.

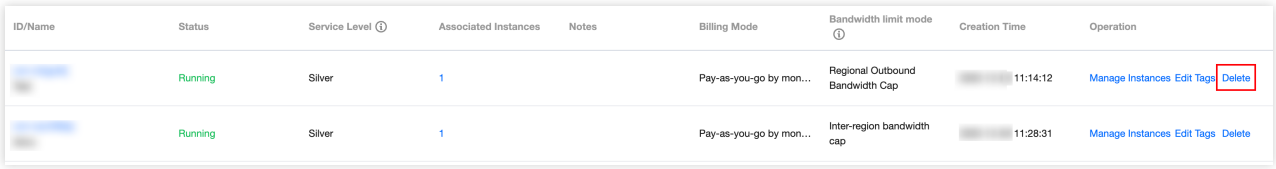
Deleting a CCN Instance

Last updated：2024-01-10 14:41:59

Note:

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

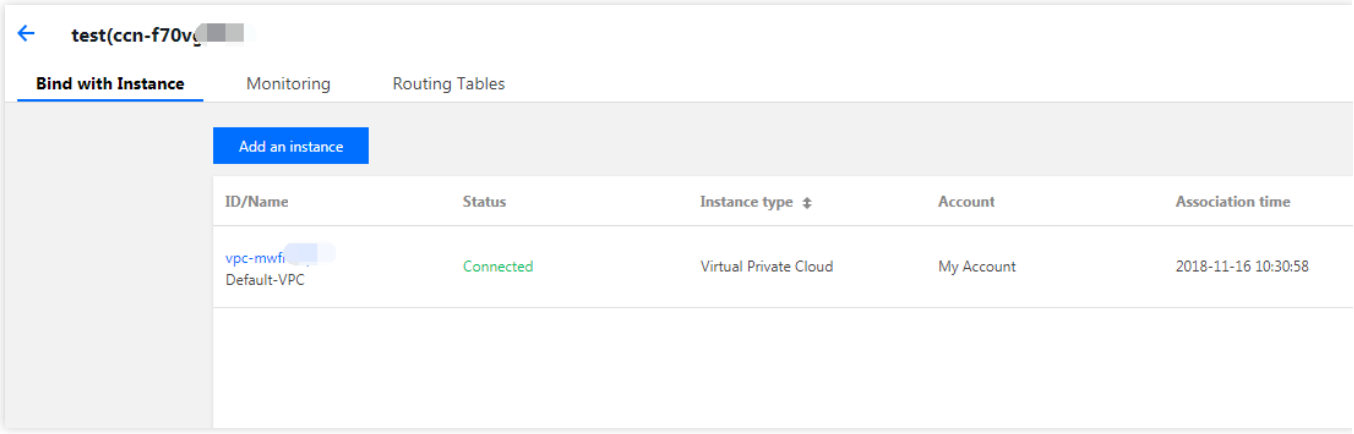
1. Log in to the CCN console and access the CCN management page.
2. In the CCN list, find the row of the CCN instance to be deleted. Then, click **Delete** in the **Operation** column, and click **Confirm**.



Disassociating a Network Instance

Last updated：2024-01-10 14:41:59

1. Log in to the CCN console and access the CCN management page.
2. In the CCN list, click the ID of the CCN to be disassociated to open the details page.
3. 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**.



Publishing IP Ranges through Direct Connect Gateway to CCN

Last updated：2024-01-10 14:41:59

After associating a CCN with the direct connect gateway, you need to configure a routing policy for the CCN, with the direct connect gateway as the next hop and IDC IP range as the destination to implement communication. The routing policy can be either manually entered (Static) or automatically synced (BGP). For more information, see Route Overview. This document describes how to publish IP ranges through the direct connect gateway to CCN.

Note:

Up to 20 routes can be published to CCN through direct connect gateway. To publish more routes, submit a ticket.

Background

As shown in the following direct connect network architecture, your IDC associated with the CCN-based direct connect gateway and CCN can communicate with a Tencent Cloud VPC. The destination IP range of VPC routes to IDC is `192.168.0.0/24` . After configuring the IDC IP range on the direct connect gateway, the CCN route table will add a routing policy with the direct connect gateway as the next hop and `192.168.0.0/24` as the destination to implement the route propagation.

Note:

If you configure multiple IDC IP ranges on the direct connect gateway, CCN will forward the route with the longest mask. For more information, see Route Overview.

Prerequisites

You have created a CCN-based direct connect gateway as instructed in Creating Direct Connect Gateway.

Directions

1. Log in to the Direct Connect console, and click **Direct Connect Gateway** in the left sidebar.
2. Select a region and a VPC at the top. Click the ID/Name of the target instance to enter its details page.
3. Click **Publish IP range** on the details page.

The IP range published is an IDC IP range that specifies the route published through the direct connect gateway to CCN. After the route is received, CCN will automatically add a route with the direct connect gateway as the next hop and IDC IP range as the destination.

4. (Optional) Associate with CCN.

If you did not specify a CCN instance when creating the direct connect gateway, click **Associate with CCN**, select a CCN instance to be associated in the pop-up window, and click **OK**.

Then the CCN instance will be associated and the CCN icon becomes green. The dotted line between direct connect gateway and CCN changes to solid, indicating their interconnection.

5. Create a dedicated tunnel.

A dedicated tunnel is the network segmentation of a connection. It provides a linkage of IDC to Tencent Cloud.

Under the **Dedicated tunnels** icon connected with the direct connect gateway, click **Create dedicated tunnel** to redirect to the **Create dedicated tunnels** page, where you can configure a dedicated tunnel.

For more information on the parameter configurations, see Applying for a Dedicated Tunnel.

Then the dedicated tunnel is created and the **Dedicated tunnels** icon becomes green. The dotted line between direct connect gateway and dedicated tunnel changes to solid, indicating the direct connect gateway is configured with a dedicated tunnel.

6. Publish IDC IP ranges to CCN.

After an IDC IP range is published to CCN, the CCN route is synced to the direct connect gateway, while whether the direct connect gateway route is synced to CCN depends on the publishing method of the IDC IP range.

Custom: the manual configuration mode. CCN obtains the specified direct connect gateway route.

Auto-propagation: the BGP mode. CCN automatically obtains the direct connect gateway route published from the dedicated tunnel. But it depends on the publishing time.

Custom

Auto-propagation

Switching methods

Formerly named **Static** or manual configuration.

1. (Optional) Select a CCN instance in the **Publish rules** section.

Perform this step if you want to associate one CCN instance with the direct connect gateway or change the associated CCN instance.

Note:

The **Publishing method** defaults to **Custom**. To switch to **Auto-propagation**, submit a ticket.

2. Select the **Custom** tab on the **IP range details** page. Click **Create** and enter the information of the IP range that is published to CCN. Click **Save**.

Then the direct connect gateway will publish the IDC IP range you entered to CCN.

Note:

Up to 100 IDC IP ranges can be published. To publish more IDC IP ranges, please submit a ticket.

Formerly named **BGP mode**. To use it, please submit a ticket.

1. (Optional) Select a CCN instance in the **Publish rules** section.

Perform this step if you want to associate one CCN instance with the direct connect gateway or change the associated CCN instance.

Note:

The **Auto-propagation** is selected after this feature is enabled. If needed, you can select **Custom** and complete the relevant configurations.

Either custom or auto-propagation can be selected.

2. Configure IDC IP ranges.

In the **Auto-propagation** mode, the information of IDC IP ranges will be automatically synced to the direct connect gateway.

Note:

Publishing IDC IP ranges may be delayed for one minute. If there are any updates on the IDC IP range, please refresh the current page.

You can switch between the two methods for publishing the IDC IP ranges through the direct connect gateway to CCN.

Switching to auto-propagation

Submit a ticket to enable the auto-propagation feature.

The custom IP ranges published to CCN will be withdrawn after the switching. The information of IDC IP ranges will be automatically synced to the direct connect gateway and published to CCN.

Switching to custom

Configure IP ranges to be published to CCN in the **Custom** tab on the **IP range details** page after the switching.

7. View the published IDC IP ranges.

The published IDC IP ranges will be shown on the **IP range details** page.

Disassociate a Cross-account VPC

Last updated：2024-01-10 14:41:59

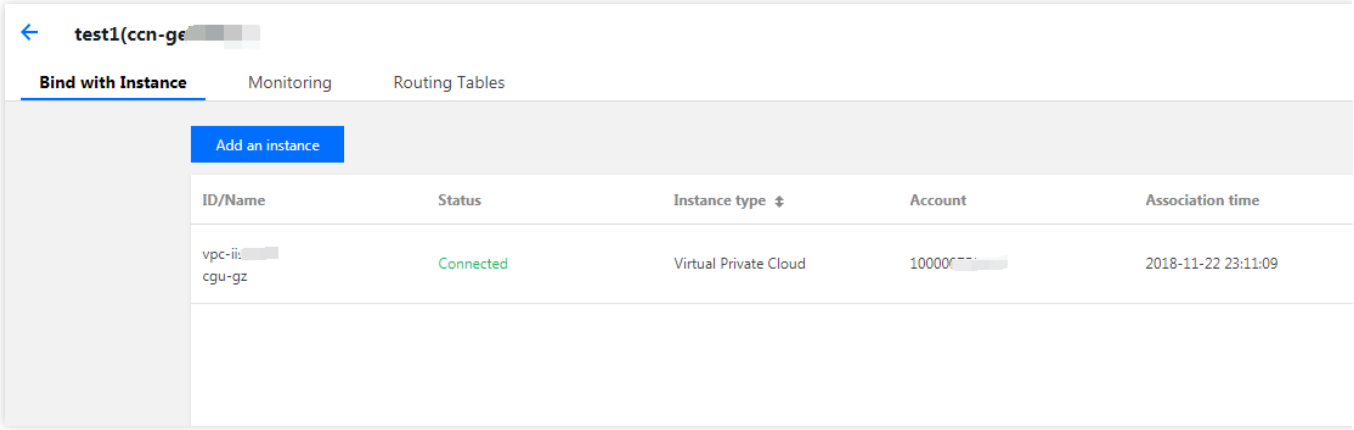
You can associate a VPC under another account to your CCN instance. That association can be removed unilaterally by users from either account.

Note:

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

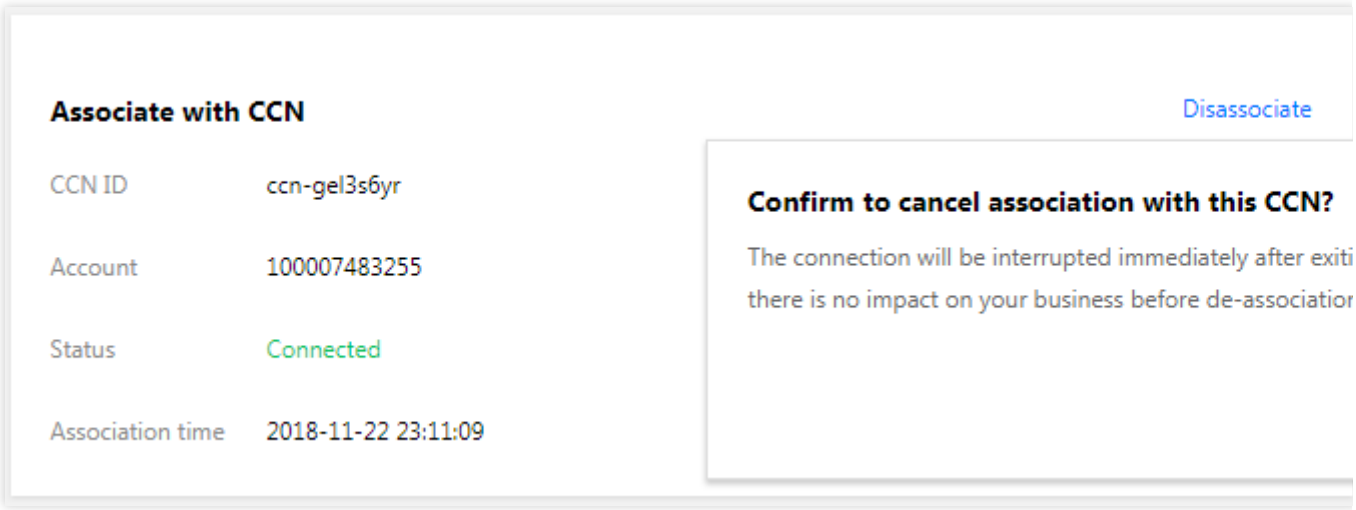
Method 1: Remove the Association Using the CCN Console

1. Log in to the CCN console and access the CCN management page.
2. In the CCN list, click the ID of the desired CCN to open the details page.
3. 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

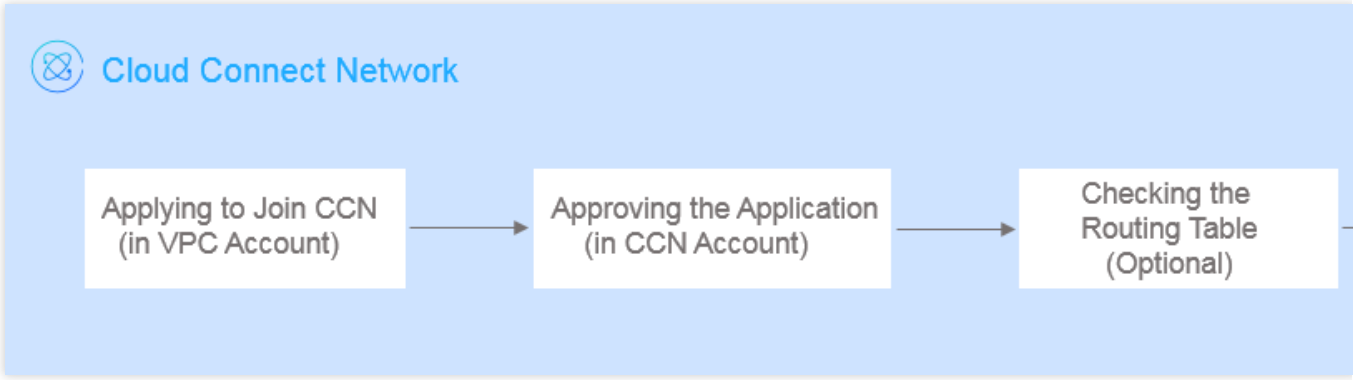
1. Log in to the VPC Console and then click the ID of the desired VPC to open the details page.
2. In the **Associate with CCN** section, click **Disassociate**. The **Are you sure you want to disassociate from this CCN instance?** page appears. Click **Disassociate**.



Associating Cross-Account VPC

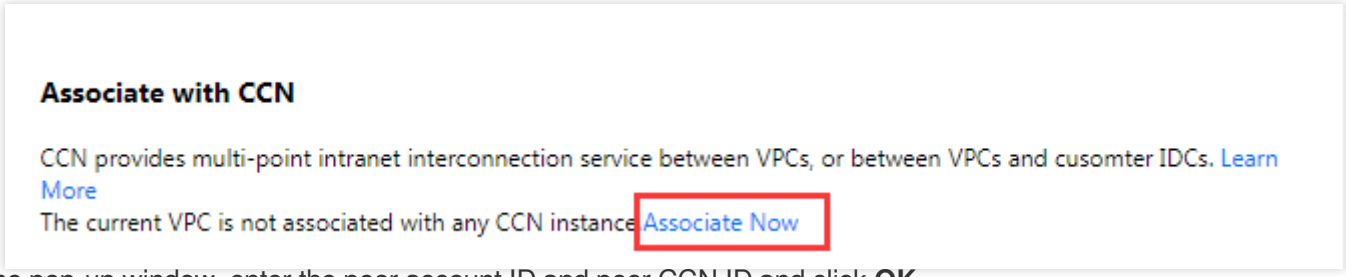
Last updated：2024-01-10 14:41:59

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 workflow is illustrated below:



Submitting Association Request (VPC Side)

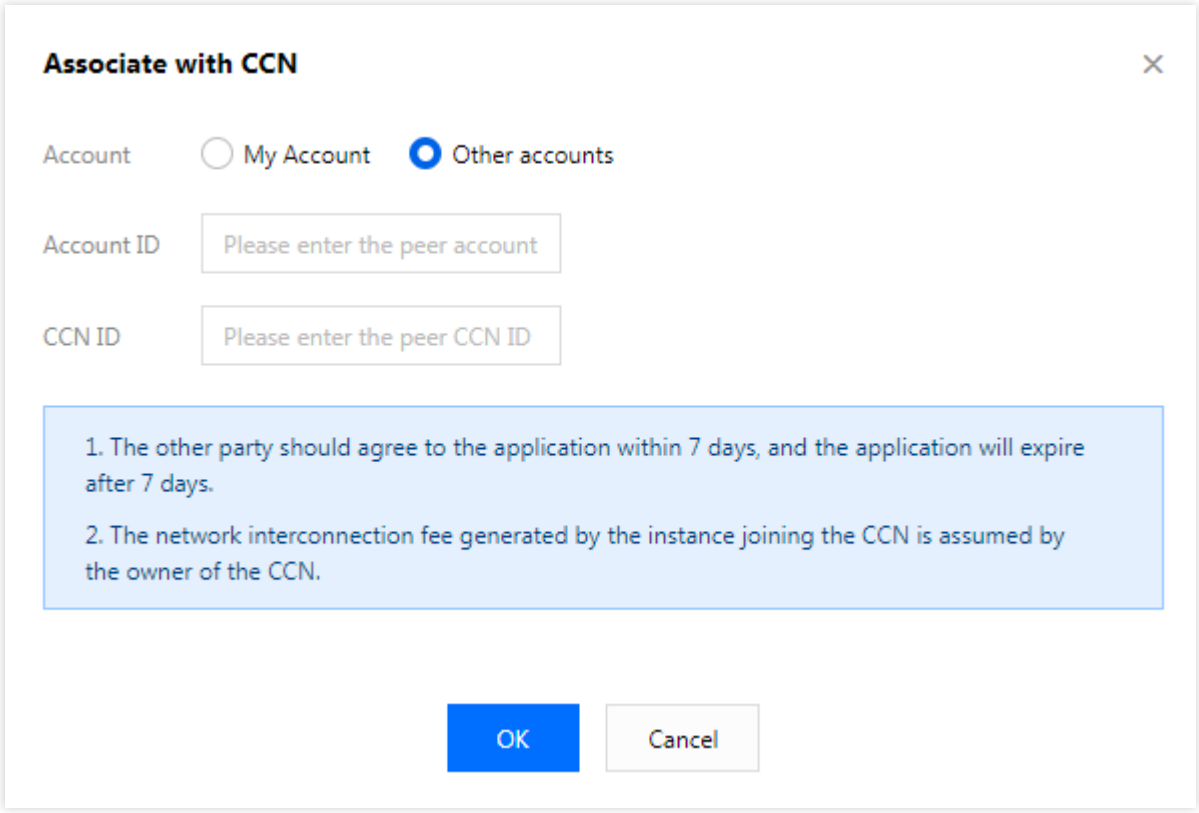
1. Log in to the VPC console.
2. Click the ID of the target VPC to enter the details page and click **Associate Now**.



3. In the pop-up window, enter the peer account ID and peer CCN ID and click **OK**.

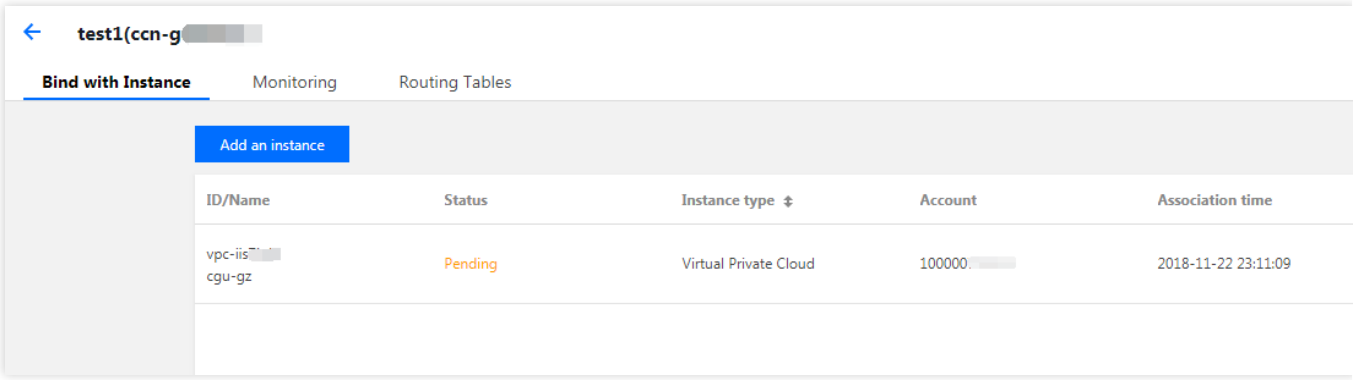
Note:

You need to enter the root account ID for **Account ID**.



Accepting the Application via the CCN Account

1. Log in to the CCN console and click the ID of the CCN instance with a pending association request.
2. On the **Associated Instances** page, locate the VPC to be associated, and click **Agree** to add the VPC to the CCN instance.



(Optional) Checking 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.

Route Management
Route Tables and Route Overview
Route Overview

Last updated：2024-01-10 14:41:59

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 add or delete routes, but you can enable or disable them.

Automatic Route Addition

To automatically add a CCN route, there are three stages:
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 route to take effect by default, i.e., determining 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: 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. The route can be propagated in the following two ways:
1.1 Custom: you need to manually enter the IDC IP range to propagate to CCN, and the next hop is the corresponding direct connect gateway, which facilitates IP range convergence and filtering.
1.2 Auto-propagation: the route is dynamically learned through BGP, and the next hop is the corresponding direct connect gateway, which makes it easy to perceive route changes in IDC. Routes are published to CCN 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:
Auto-propagation is currently in beta. To try it out, please submit a ticket.
AS-PATH description:
The information of AS-PATH can be viewed in the direct connect gateway.
AS-PATH supports a 32-bit string. If the string is exceptional, the route will be deleted, and a string exception event will be reported, for which you can configure event alarms.
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 alarms.

The AS-PATH that passes through direct connect gateway - CCN - direct connect gateway now supports three new AS numbers (45090, 139341, and 45090).

2. During addition

Check policy: if a new route overlaps any existing route, the new one will become invalid by default to avoid affecting existing routes. You can enable it after assessing the impact.
Non-check policy: all routes will be valid except ECMP routes. For more information, please see the routing logic in same IP ranges in the section 3 below.
Note:
The non-check policy is currently in beta. To try it out, please submit a ticket.

3. After addition

Different IP ranges overlapped: the route with the longest mask will be used. A more specific IP range has a higher priority. For example, if the destination of route A is `10.0.1.0/20` and that of route B is `10.0.1.0/24`, route B will be first matched based on the longest mask principle when both routes are enabled.
Sa
me IP ran
ges: any route whose next hop is direct connect gateway supports ECMP. For example, you can enable multiple routes to the same IP range `10.0.1.0/20`. However, other routes do not support ECMP and cannot be enabled simultaneously. For example, if there are two or more routes to the IP range `10.0.1.0/20` whose next hops are VPC or VPC and direct connect gateway, only one route can be enabled.
Note:
See below for the description of inbound routes in the CCN-Direct Connect network architecture. For more information, see Direct Connect Gateway Overview.
The CCN-based 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-based 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	When the Route will be Deleted
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

Custom Definition Route Tables

Last updated：2024-10-21 11:34:27

After a CCN is created, the system will automatically create a default route table and control route entries to manage traffic on CCN. You cannot add or delete routes, but you can enable or disable them. You can also manually create custom route tables and flexibly manage the interconnectivity of network instances in the CCN. This document introduces the concepts related to the custom route table.

Use Limits

The CCN binding with the SD-WAN access service and Edge devices does not support the multi-route table feature.

Comparison of Default Route Table and Custom Route Table

Comparison Item	Default Route Table	Custom Route Table
Creation method	It is created by the system after a CCN instance is created.	It is manually created.
Number of route tables	Only 1	The upper limit is 10. To create more custom route tables, consult online.
Route receiving policy	The initial policy is to receive all routes and it cannot be modified.	The initial policy is not to receive any routes. You need to configure the route receiving policy before use; otherwise the route information cannot be learned. For the details of configuring the route receiving policy in the custom route table, see Configuration of Route Receiving Policy.
Is deletion supported	Deletion is not supported	Deletion is supported; however, it cannot be deleted when bound by network instances.

Relationship Between Route Table and Network Instances

The route table and the network instance have a paired binding relationship. For example, binding route table A to network instance B and binding route table B to network instance A will produce the same result, that is, a network instance is bound to a route table. For the data messages sent by the network instance after binding, the bound route

table will be used for finding and forwarding.
The relationship between the route table and the network instance has the following characteristics:
A network instance added to the CCN can be bound to only one route table. If no specific route table is designated, it will be automatically bound to the default route table.
A network instance will be automatically unbound from the route table when it is removed from the CCN.
After a network instance is bound to a route table under CCN, it can be switched to any other route table under the same CCN instance. Once the new route table is bound successfully, it will be automatically unbound from the original route table.

Creating Custom Route Tables

1. Log in to the CCN console.
2. In the CCN list, click the **CCN ID** for which you need to create a custom route table to enter the **Route Table** tab on the details page.
3. Click **New Routing Table**.
4. In the New Routing Table dialog box, configure the information of the custom route table and then click **OK**.

Note:

The upper limit for the number of custom route tables is 10. For more custom route tables, please consult Online Support. Custom route tables can be deleted, but they cannot be deleted if they are associated with network instances or referenced by the route table selection policy.

Viewing Route Tables

Viewing Custom Route Tables

1. Log in to the CCN console.
2. In the CCN list, click the **CCN ID** you want to view to enter the details page.
3. In the **Route Table** tab, click the **Route Table ID** to view related information:
In the **Route Entries** tab, view the information of route entries for the route table.
In the **Bind Instance** tab, view the network instances bound to the route table.
4. In the **Route Reception Policy** tab, view the routes of the network instances received by the route table.

Note:

There are two statuses for route table entries: If there is no IP range conflict, the status defaults to **Valid**. If it conflicts with other existing routes, the status is **Invalid**. For conflict rules and limitations, see Route Limitation. If you need to use invalid routes, see Disable Route and Enable Route.

Viewing Network Instance Route Tables

1. Log in to the CCN console.
2. In the CCN list, click the **CCN ID** you want to view to enter the **Associated Instances** tab on the details page.
3. Click **Network Instance ID**, and click the **Route Table** on the basic information page of VPC.
4. Click **Route Table ID**. On the route table details page, you can view the entry information of the next CCN route in the related route policy.

Deleting Custom Route Tables

Note:
Before deleting a custom route table, please ensure the following conditions are met:
The current custom route table is not associated with any network instance.
1. Log in to the CCN console.
2. In the CCN list, click the CCN ID for which you need to delete the custom route table to enter the **Route Table** tab on the details page.
3. In the left area of the tab, click **Delete** next to the custom route table ID.
4. In the Delete Route Table dialog box, click **OK**.

Directions

After the custom route table is created:
To enable a route in the route table, see Enabling a Route.
To disable a route in the route table, see Disabling a Route.

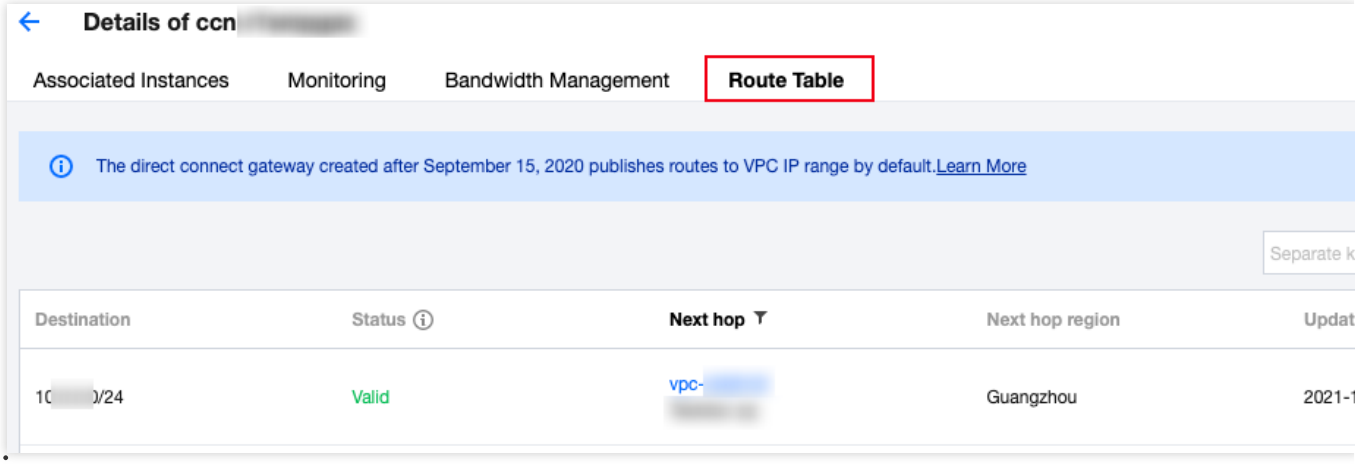
Viewing Routing Information

Last updated：2024-01-10 14:41:59

1.Log in to the CCN console and access the CCN management page.

2. In the CCN list, click the ID of the desired CCN to open the details page.

3. Click the **Route Tables** tab to view the route table of this CCN.



Note：

A route table is in one of the following states:

If no IP range conflict occurs, the route table is **Valid** by default.

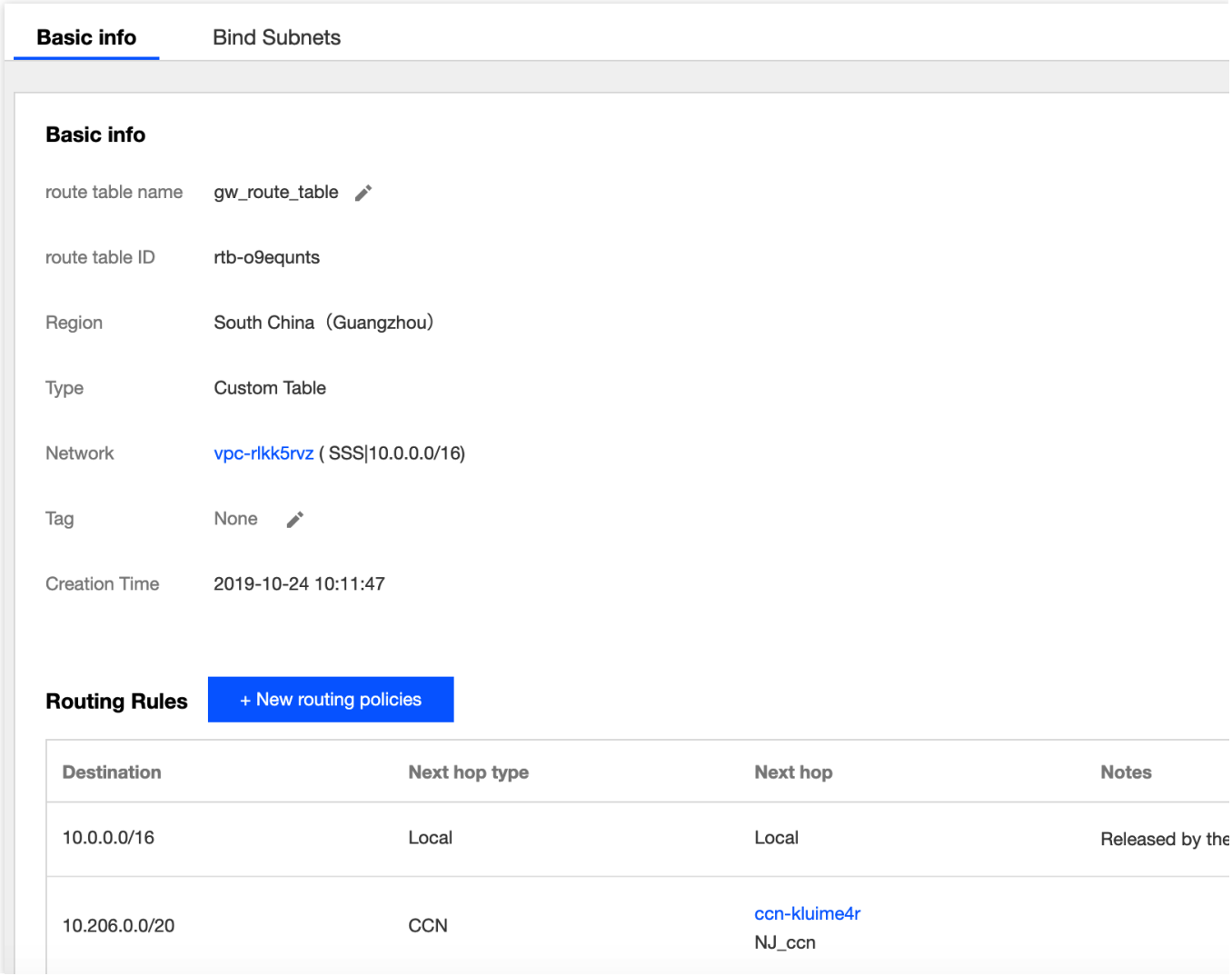
If the route conflicts with an existing route, the route table is **Invalid**. For more information about the conflict rules and restrictions, see Use Limits - Routing Restrictions.

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

Viewing the Route Table Associated with VPC

Last updated：2024-01-10 14:41:59

1. Log in to the Route table console, and filter the region and VPC at the top of the console list.
2. Click the ID of the desired route table to open the details page. In the related routing policy section, you can find the information about the routing policy in which the next hop is a CCN.



Enabling a Route

Last updated：2024-01-10 14:41:59

This document describes how to enable one or multiple CCN routes.

Prerequisites

Disable routes:

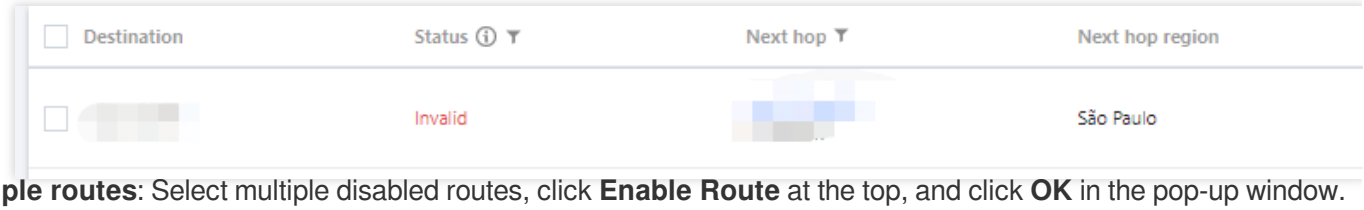
Directions

1. Log in to the CCN console.
2. In the CCN instance list, click the ID of the CCN for which you want to enable routing to access the details page.
3. Enable the route on the **Route Table** tab:

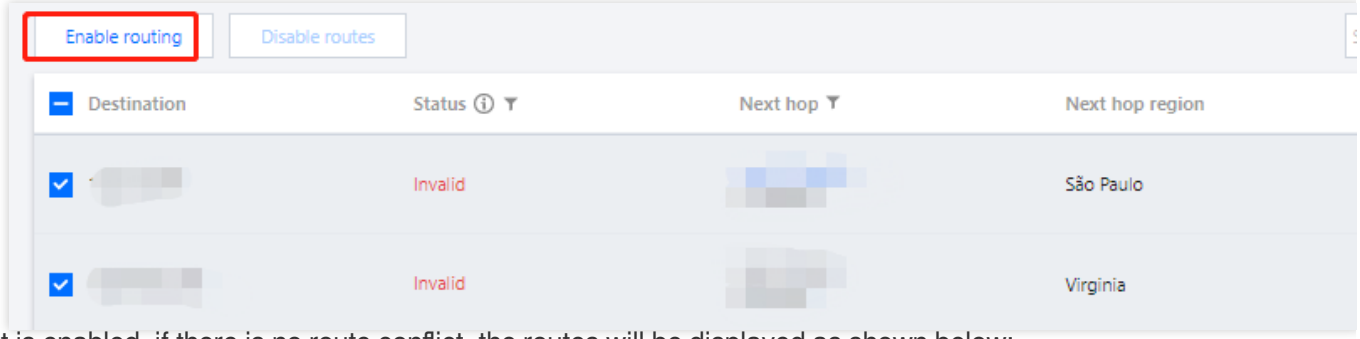
Note:

If the routing rules overlap, match according to the longest mask rule

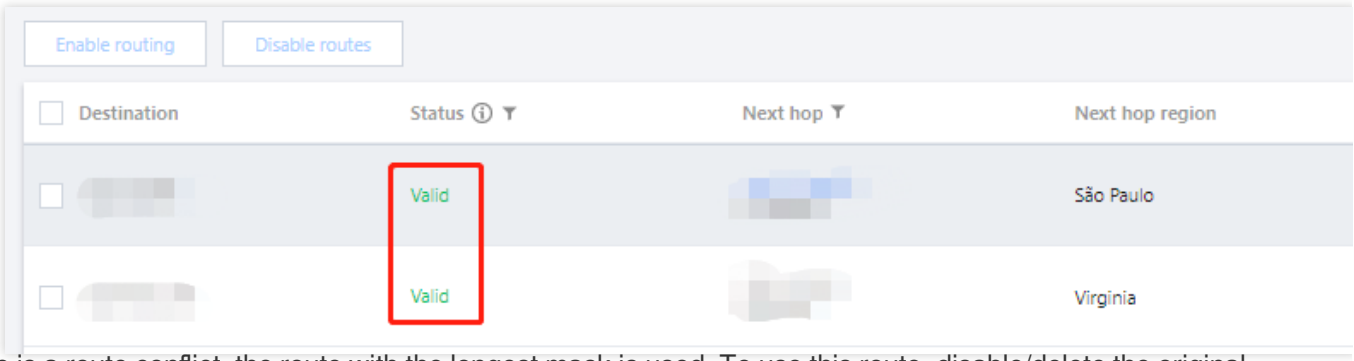
Single route: Click the icon on the right of the disabled route and click **OK** in the **Enable Route** pop-up window.



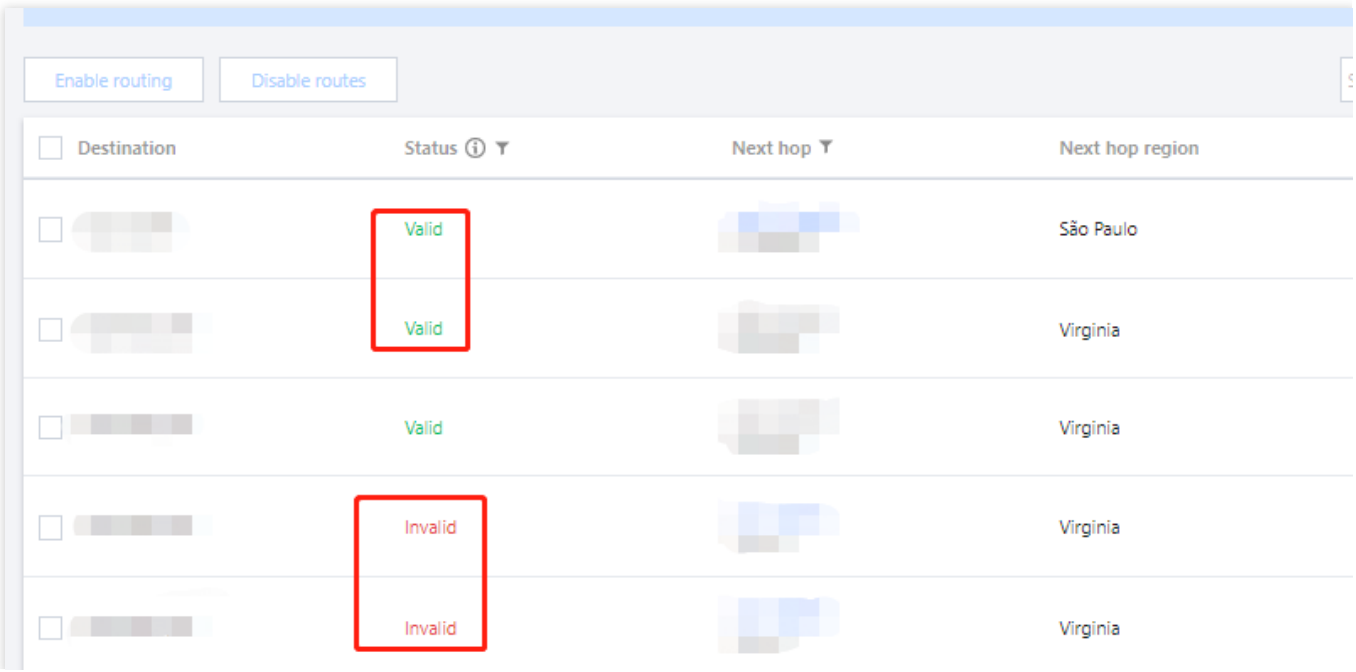
Multiple routes: Select multiple disabled routes, click **Enable Route** at the top, and click **OK** in the pop-up window.



After it is enabled, if there is no route conflict, the routes will be displayed as shown below:



If there is a route conflict, the route with the longest mask is used. To use this route, disable/delete the original conflicting route first.



Disabling a Route

Last updated：2024-01-10 14:41:59

This document describes how to disable one or multiple CCN routes.

Note:

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

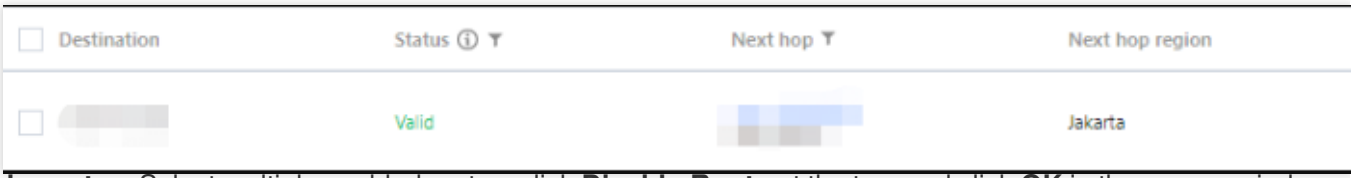
Prerequisites

Enable the route:

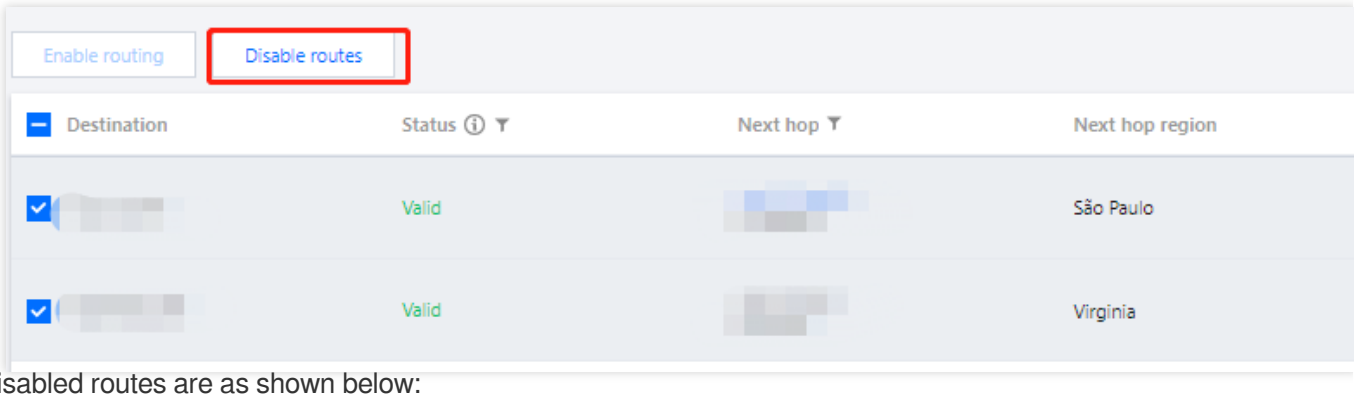
Directions

1. Log in to the CCN console.
2. In the CCN instance list, click the **ID/Name** of the CCN instance for which to disable a route to enter the details page.
3. Disable the route on the **Route Table** tab:

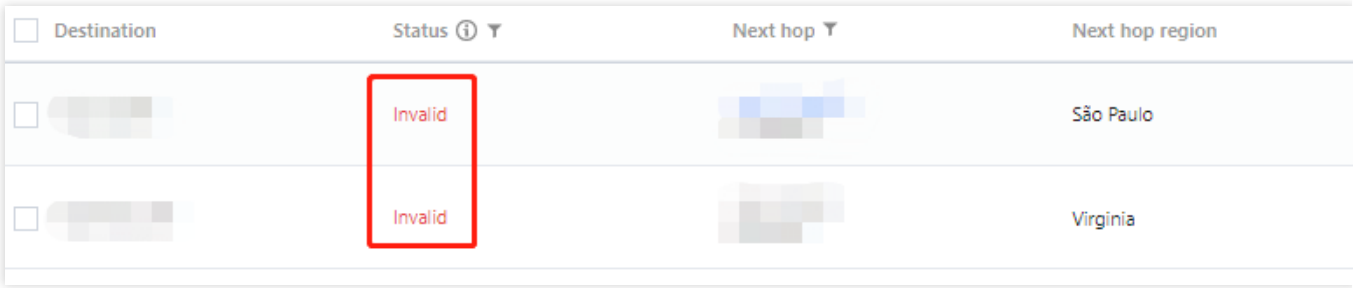
Single route: Click the icon on the right of the enabled route and click **OK** in the **Disable Route** pop-up window.



Multiple routes: Select multiple enabled routes, click **Disable Route** at the top, and click **OK** in the pop-up window.



The disabled routes are as shown below:



Bandwidth Management
Configuring Bandwidth

Last updated：2024-01-10 14:41:59

After creating and associating a CCN instance with network instances, you need to configure bandwidth to enable communications. If the CCN billing mode is pay-as-you-go by monthly 95th percentile, configure a bandwidth cap in both regions the CCN instance connects to.

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.

Setting Cross-region Bandwidth Cap (for Pay-as-you-go CCN Instances Billed by Monthly 95th Percentile)

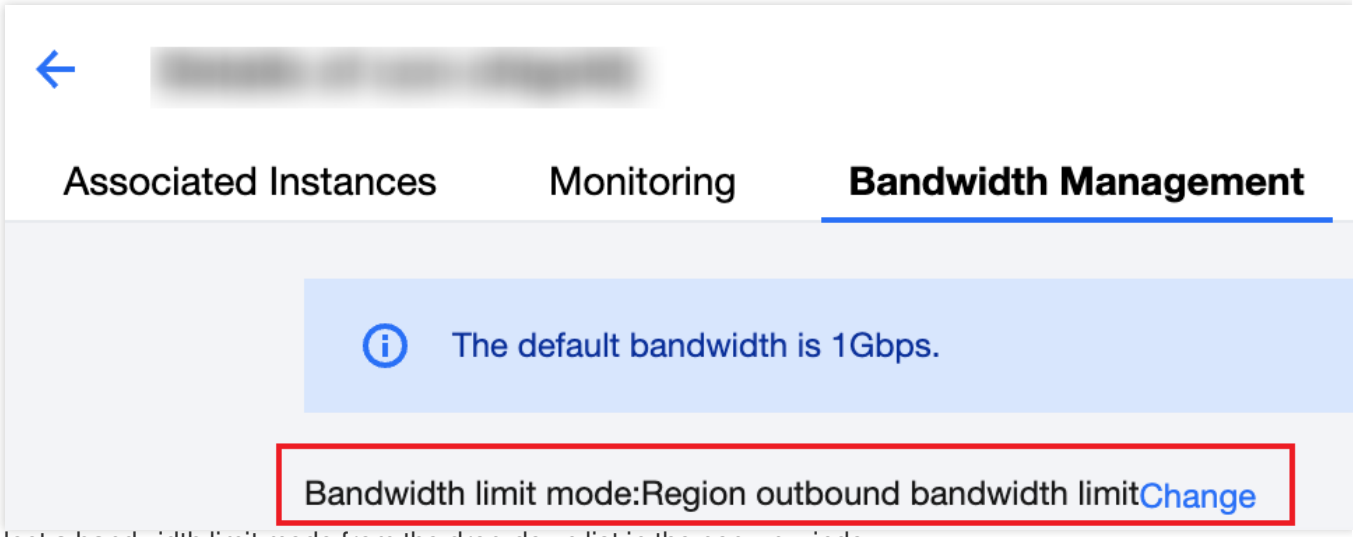
You can configure a cross-region bandwidth cap for pay-as-you-go CCN instances billed by monthly 95th percentile to control the bandwidth costs.

Note:

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

1. Log in to the CCN console and access the CCN management page.
2. On the CCN instance list page, click the **ID/Name** of the target pay-as-you-go CCN instances billed by monthly 95 percentile to enter its details page. Click the **Bandwidth Management** tab.
3. (Optional) Perform the following steps to change the bandwidth limit mode to meet your requirements.

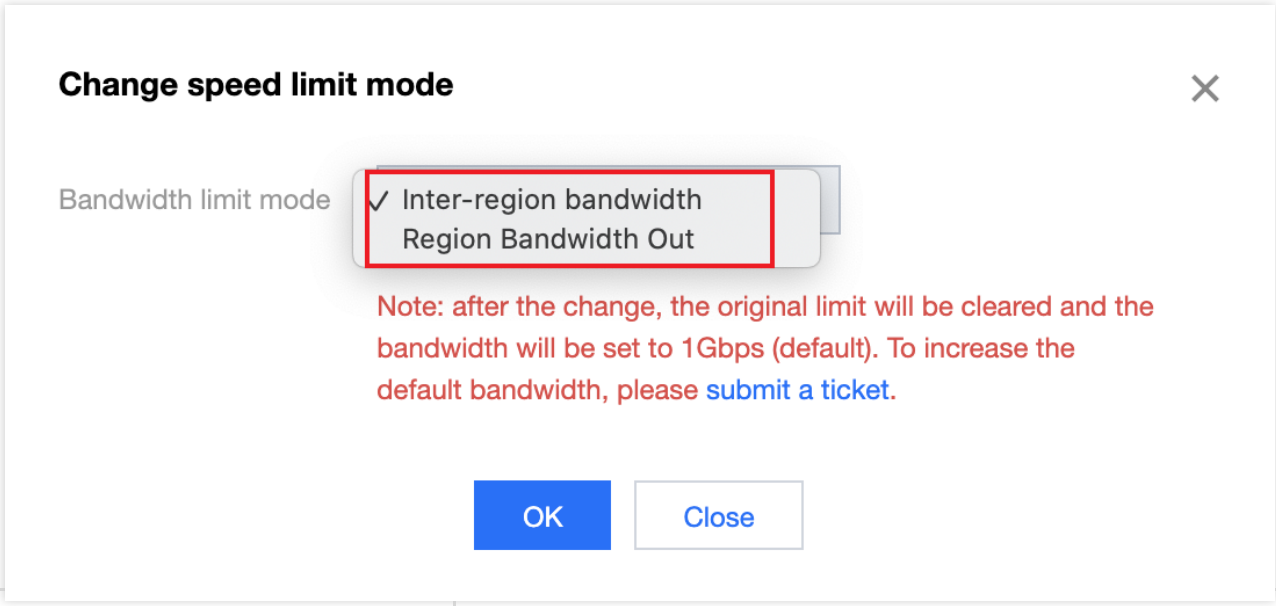
3.1 Click **Change** on the right of the **Bandwidth limit mode**.



3.2 Select a bandwidth limit mode from the drop-down list in the pop-up window.

Note:

Changing the bandwidth limit mode 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.



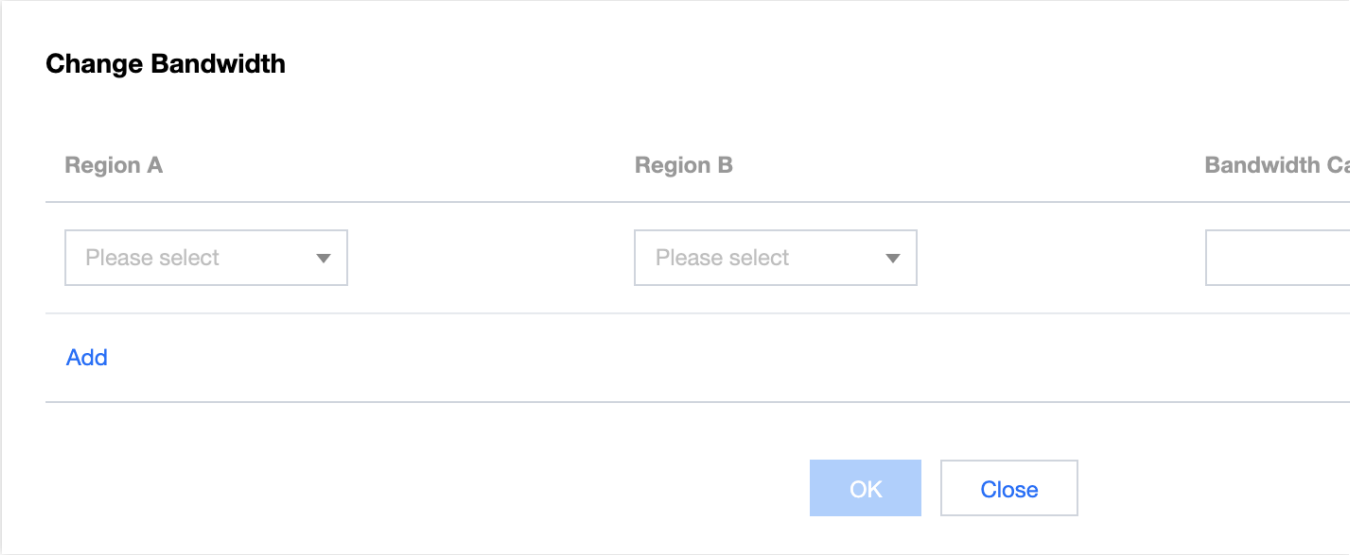
Bandwidth Limit	Notes
Region bandwidth out	The total outbound bandwidth cap from a single region to other regions
Inter-region bandwidth	The inbound and outbound bandwidth cap between two regions

3.3 Click **OK**.

4. Configure the bandwidth cap depending on the bandwidth limit mode of the CCN instance:

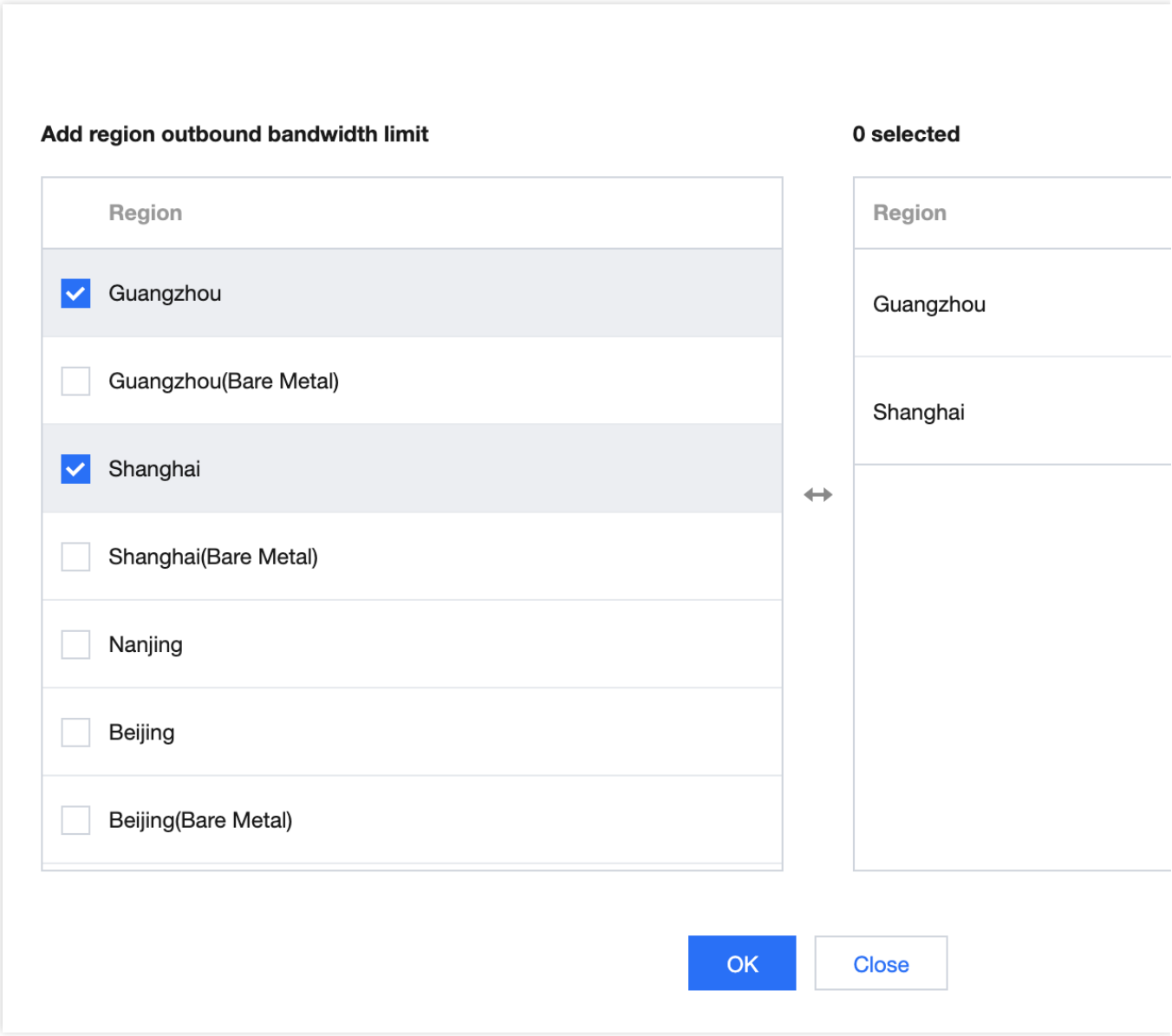
Set inter-region bandwidth limit

Click **Change Bandwidth**. In the pop-up window, select **Region A** and **Region B** from the drop-down list and enter the **Bandwidth Cap**. You can also click **Add** to configure multiple bandwidth limit rules, and then click **OK**.



Set the region outbound bandwidth limit

Click **Adjust bandwidth cap**. In the pop-up window, select regions for which you want to limit the bandwidth on the left and set the bandwidth cap on the right. Click **OK**.



Managing Bandwidth

Last updated：2024-01-10 14:46:59

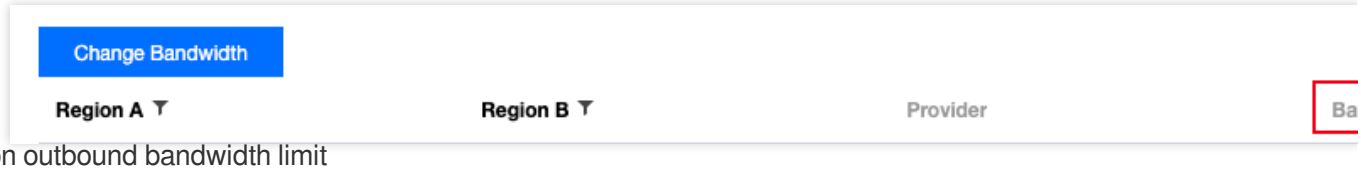
For a pay-as-you-go CCN instance billed by monthly 95th percentile, you can view its bandwidth cap and change the bandwidth limit type in the console.

Prerequisites

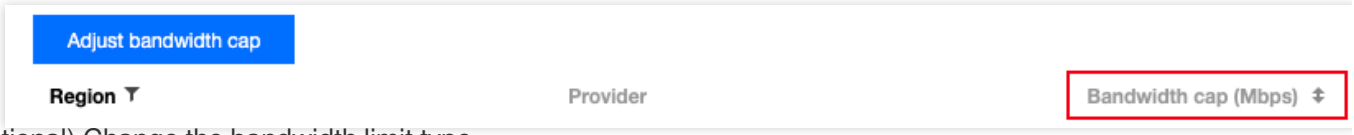
You have created a CCN instance and associated it with network instances as instructed in Creating a CCN Instance and Associating Network Instances.
Check that there is no route conflict in the route table. For more information, see Viewing Routing Information.

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

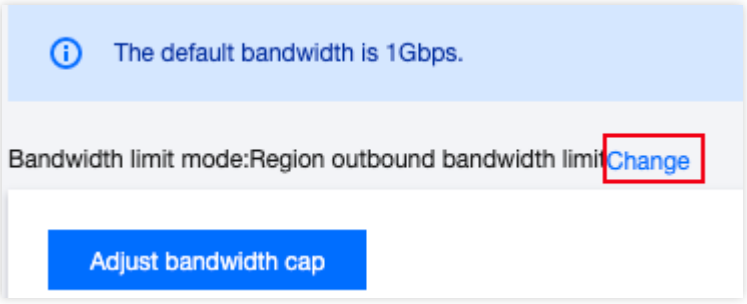
1. Log in to the CCN console and access the CCN management page.
2. On the CCN instance list page, lick the **ID/Name** of the target pay-as-you-go CCN instance to enter its details page. Click the **Bandwidth Management** tab.
This tab displays the bandwidth cap of the current bandwidth limit type.
Inter-region bandwidth limit



Region outbound bandwidth limit



3. (Optional) Change the bandwidth limit type.
3.1 Click **Change** on the right of **Speed limit mode**.



3.2 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

4. Click **OK**.

Monitoring and Alarms
Viewing Monitoring Data

Last updated：2024-01-10 14:41:59

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

Directions

1. Log in to the CCN console and enter the CCN management page.
2. On the CCN instance list page, click the ID/Name of the target CCN instance to enter its details page. Select the **Monitoring** tab.
3. View the following monitoring data of the current bandwidth limit mode:

Single-region monitoring

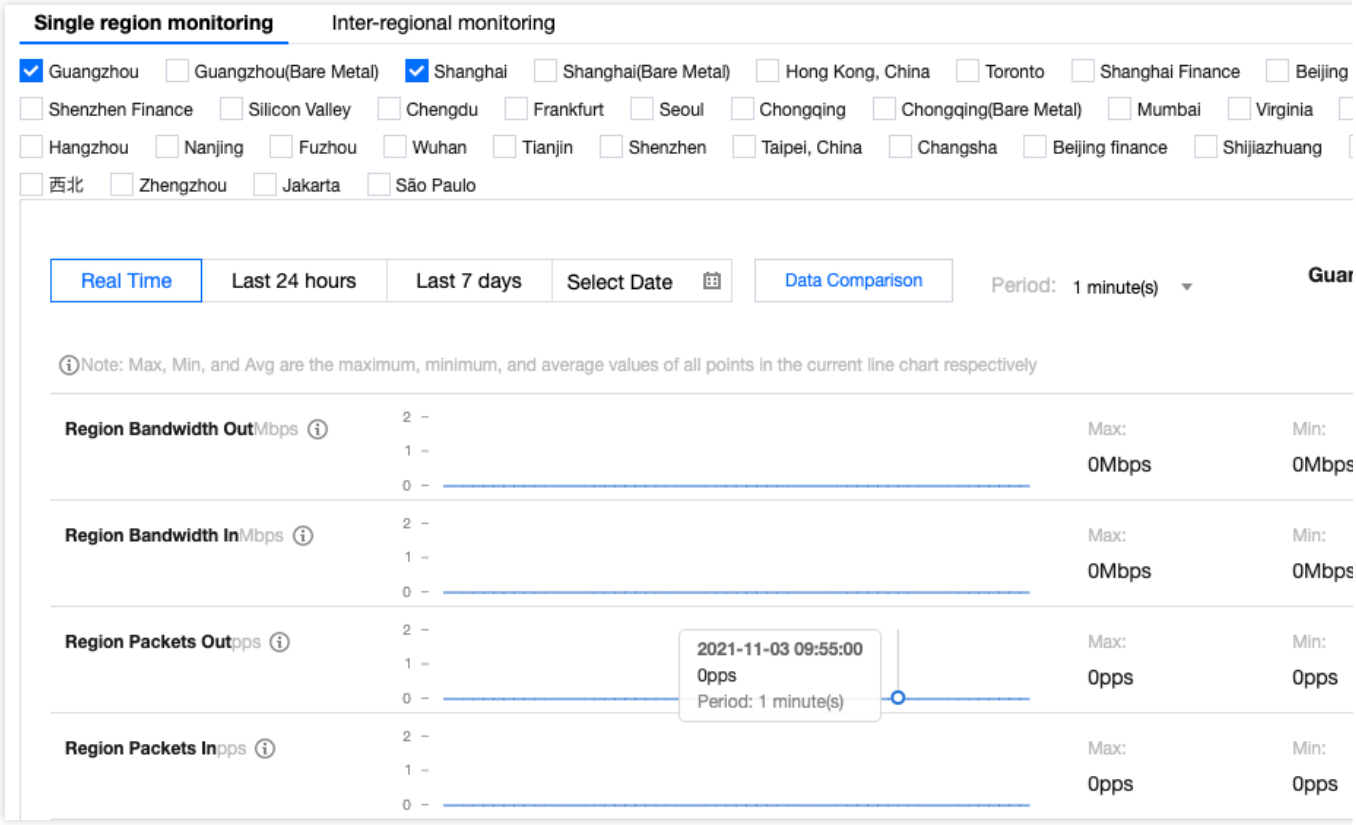
Select a region where network instances are associated with the CCN instance, and view **Region bandwidth out**, **Region bandwidth in**, **Region packets out** and **Region packets in** metrics. You can click **last 24 hours**, **last 7 days** or specify a custom time range to view the monitoring data.

Region bandwidth out: The outbound bandwidth used by the network instances in this region.

Region bandwidth in: The inbound bandwidth used by the network instances in this region.

Region packets out: Number of data packets sent from the network instances in this region.

Region packets in: Number of data packets received by the network instances in this region.



Note:

Click the

icon to show more data of the selected metric. Click the

icon to download it.

Inter-region monitoring

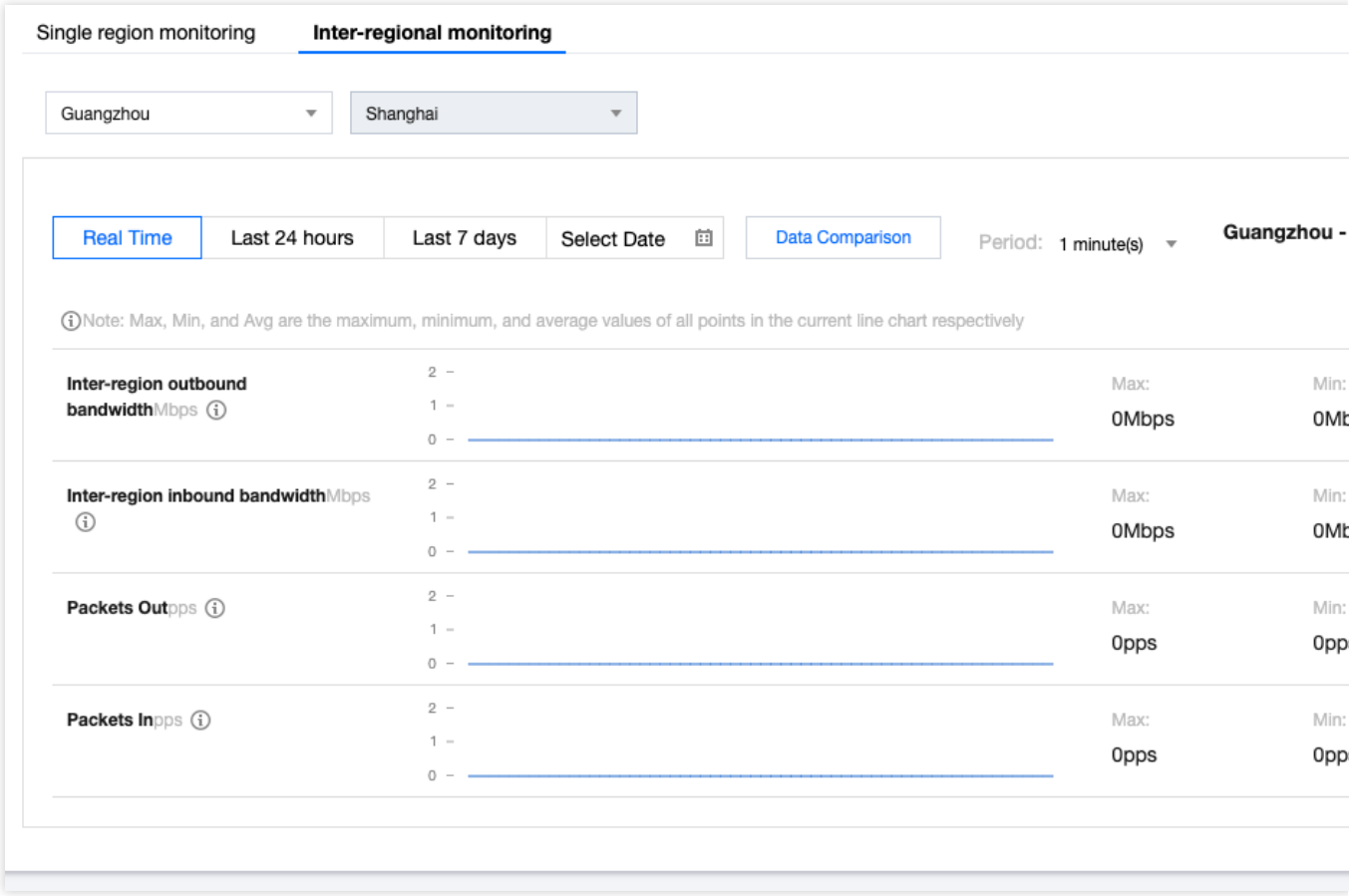
Select two regions where network instances are associated with the CCN instance, and view **Inter-region outbound bandwidth**, **Inter-region inbound bandwidth**, **Packets out** and **Packets in** metrics. You can click **last 24 hours**, **last 7 days** or specify a custom time range to view the monitoring data.

Inter-region outbound bandwidth: The outbound bandwidth used in the source region between the source and destination regions.

Inter-region inbound bandwidth: The inbound bandwidth used in the source region between the source and destination regions.

Packets out: Number of data packets sent from the source region to the destination region.

Packets in: Number of data packets received by the source region from the destination region.



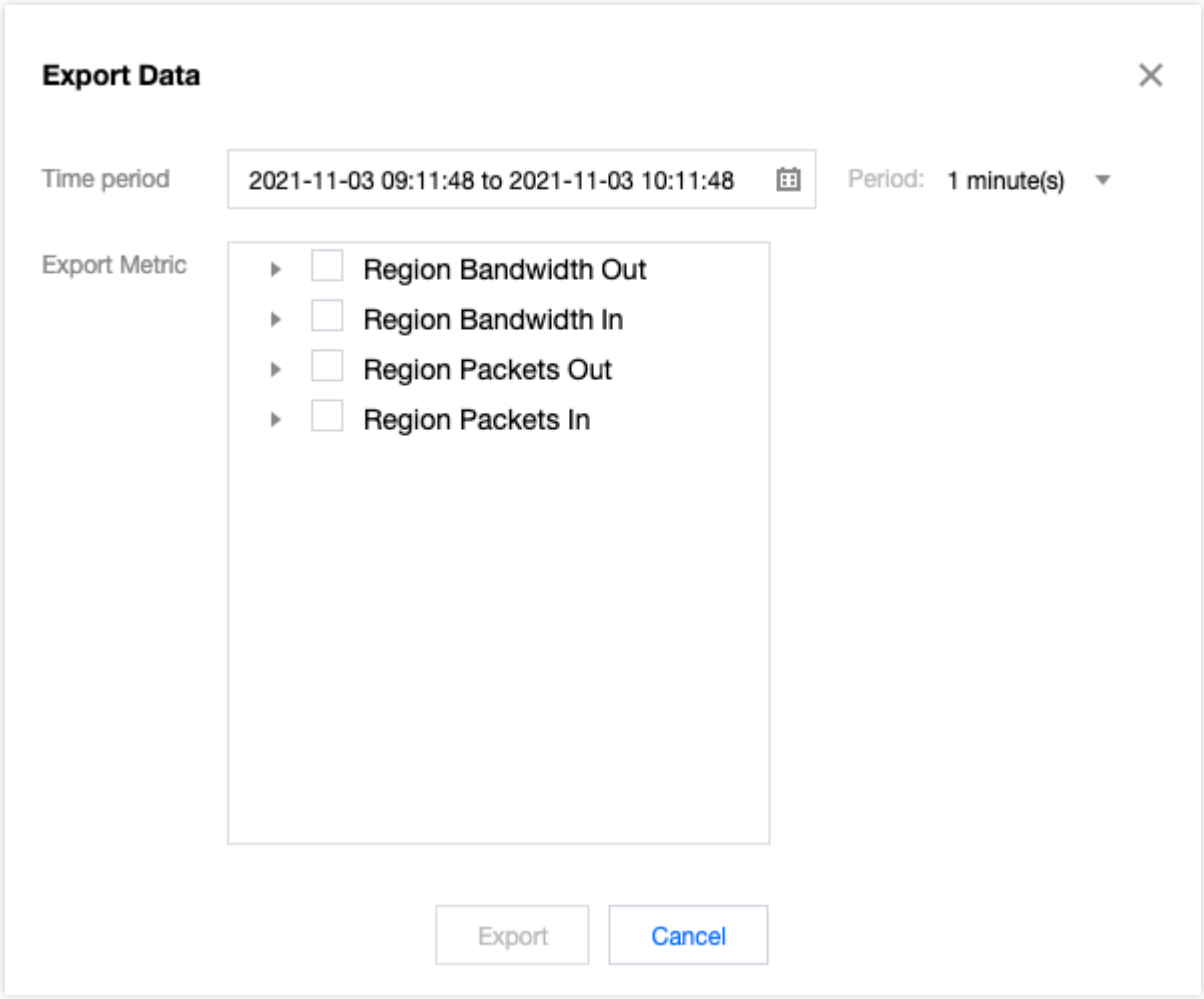
Note:

Click the

icon to show more data of the selected metric. Click the

icon to download it.

4. To export the monitoring data, click the top-right **Export data**. Specify the time range, time granularity and the metrics to export in the pop-up window, and click **Export**.



CCN Cross-Region Flow Logging

Last updated：2024-01-10 14:47:24

CCN provides the flow log collection feature to collect and analyze cross-region traffic and generate logs and analysis charts. This helps you stay informed of cross-region communication and quickly locate and solve problems based on the logs, thus improving the business availability and Ops efficiency.

Note:

The flow log feature is in beta test. To try it out, submit a ticket for application.

The Flow Log service is free of charge, but the data stored in CLS will be charged at the standard prices of CLS.

As flow log data is stored in CLS, make sure that you have granted CLS access to Flow Logs.

Directions

1. Log in to the VPC console and click **Diagnostic Tools** > **Flow Logs** on the left sidebar.
2. Select the region in the top-left corner of the **Flow Logs** page and click **+Create**.
3. Configure the following parameters in the **Create Flow Log** window.

Field	Description
Name	Enter a name for the flow log to be created.
Collection Range	Multiple collection ranges are supported currently. Cross-region CCN traffic is selected here.
CCN	CCN instance ID.
Collection Type	Select the type of traffic to be collected by the flow log: all traffic, or the traffic rejected or accepted by security groups or ACL.
Logset	Specify the storage location in CLS for flow logs. If you already have a logset, select it directly; otherwise, keep Created by System selected, so that the system will create one for you. You can also click Create to create one in the CLS console.
Log Topic	Specify the minimum dimension of log storage, which is used to distinguish between different types of logs, such as `Accept` log. If you already have a log topic, select it directly; otherwise, keep Created by System selected, so that the system will create one for you. You can also go to the CLS console to create one. Note: For more information on how to configure a logset, log topic, and index, see Creating Logsets and Log Topics.

Tag Key	Click Advanced Options to enter or select a tag key for the identification and management of flow logs.
Tag Value	Click Advanced Options to enter or select a tag value. It can also be left empty.

4. Click **OK**.

Note:

You can view the record of a newly created flow log in CLS after six minutes upon the creation (one minute for the capture window and five minutes for data publishing).

5. After about six minutes, click **Storage Location** or **View** to enter the **Search and Analysis** page of the CLS service, select the region and time period for which to view logs, and click **Search and Analyze** to view the logs.

Note:

For field descriptions, see Appendix. For more information on log analysis, see Quick Analysis.

Appendix

Flow log records of cross-region CCN traffic

The flow logs of cross-region CCN traffic record the network flows filtered by the "quintuple + traffic source region + traffic destination region" rule in a specific capture window; that is, only flow logs that meet the rule in the capture window can be recorded as flow logs of cross-region CCN traffic.

Quintuple + traffic source region + traffic destination region

A quintuple refers to a collection of five values: source IP address, source port, destination IP address, destination port, and transport layer protocol.

The traffic source region refers to the region from which cross-region CCN traffic is sent.

The traffic destination region refers to the region to which cross-region CCN traffic arrives.

Capture window

It refers to a time period of one minute, during which FL aggregates data and takes about five minutes to publish the flow log records. Flow log records are strings separated with spaces in the following format:

```
srcaddr dstregionid dstport start dstaddr version packets ccnid protocol
srcregionid bytes action region-id srcport end log-status
```

Field	Data Type	Description
srcaddr	text	Source IP.
dstregionid	text	Traffic destination region.
dstport	long	Traffic destination port. This field will take effect only for UDP/TCP protocols and will be displayed as "-" for other protocols.

start	long	The timestamp when the first packet is received in the current capture window. If there are no packets in the capture window, it will be displayed as the start time of the capture window in Unix seconds.
dstaddr	text	Destination IP.
version	text	Flow log version.
packets	long	Number of packets transferred in the capture window. This field will be displayed as "-" when log-status is NODATA.
ccnid	text	Unique CCN instance ID. To get the information of your CCN instance, contact us.
protocol	long	IANA protocol number of the traffic. For more information, see Assigned Internet Protocol Numbers.
srcregionid	text	Traffic source region.
bytes	long	Number of bytes transferred in the capture window. This field will be displayed as "-" when log-status is NODATA.
action	text	Operation associated with the traffic: ACCEPT: Cross-region traffic normally forwarded over CCN. REJECT: Cross-region traffic prevented from being forwarded due to traffic throttling.
region-id	text	Region where logs are recorded.
srcport	text	Traffic source port. This field will take effect only for UDP/TCP protocols and will be displayed as "-" for other protocols.
end	long	The timestamp when the last packet is received in the current capture window. If there are no packets in the capture window, it will be displayed as the end time of the capture window in Unix seconds.
log-status	text	Logging status of the flow log. Valid values: OK: Data is normally logged to the specified destination. NODATA: There was no inbound or outbound network flow in the capture window, in which case both the packets and bytes fields will be displayed as -1.

FAQs

How do I view flow logs between specified regions?

If the flow log feature is enabled in the Shanghai region, all outbound traffic from Shanghai and inbound traffic to Shanghai will be collected. To collect the flow logs between two regions, you can filter out the expected flow logs by

`srcregion` and `dstregion` in CLS. For more information, see Context Search and Analysis.