Cloud Connect

Best Practices

Issue	01
Date	2022-01-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

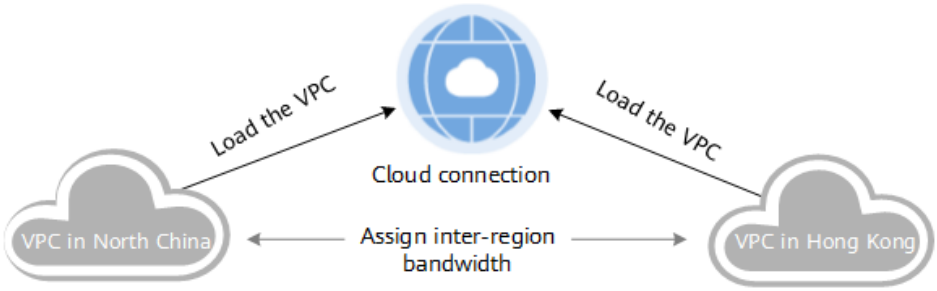
Contents

1 Connecting Two VPCs in Different Regions

Scenarios

Your company has two branches, one in Beijing and the other in Hong Kong, and you have created a VPC for each branch. If the two branches require private network communications and a way to transmit data between the two VPCs, what you need is a cloud connection that links the VPC in the CN North-Beijing4 region to the VPC in the CN-Hong Kong region, so that the two branches can communicate with each other over a private network.

Figure 1-1 Communications between VPCs in different regions



Solution Design

Configuration Procedure

1. Apply for a cross-border permit.
2. Create a cloud connection.
3. Load the two VPCs.
4. Buy a bandwidth package.
5. Assign inter-region bandwidth.
6. Check the routes and related configuration.

Table 1-1 Resource information

Region	VPC	Subnet	Other CIDR Block
CN North-Beijing4	VPC-01	subnet-1 (192.168.1.0/24)	192.168.44.0/24
CN-Hong Kong	VPC-e725	subnet-e730 (192.168.0.0/24)	192.168.11.0/24

Prerequisites

Applying for a Cross-Border Permit

Step 1 Prepare all required materials.

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Cross-Border Permit**.
4. Click **Download Materials**.
5. Print and sign the *Cloud Connect Cross-Border Circuit Service Agreement*, *Letter of Authorization for Representative*, and *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*, and stamp your company's official seal.
6. Prepare a scanned copy of your company's business license, of the representative's ID card, of the *Cloud Connect Cross-Border Circuit Service Agreement*, of the *Letter of Authorization for Representative*, and of the *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*. Ensure that all materials are stamped with your company's official seal.

Step 2 Submit an application.

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Cross-Border Permit**.
4. Click **Submit Application**.
5. Fill in the enterprise and representative information, and upload the prepared materials.
6. Click **Submit**.

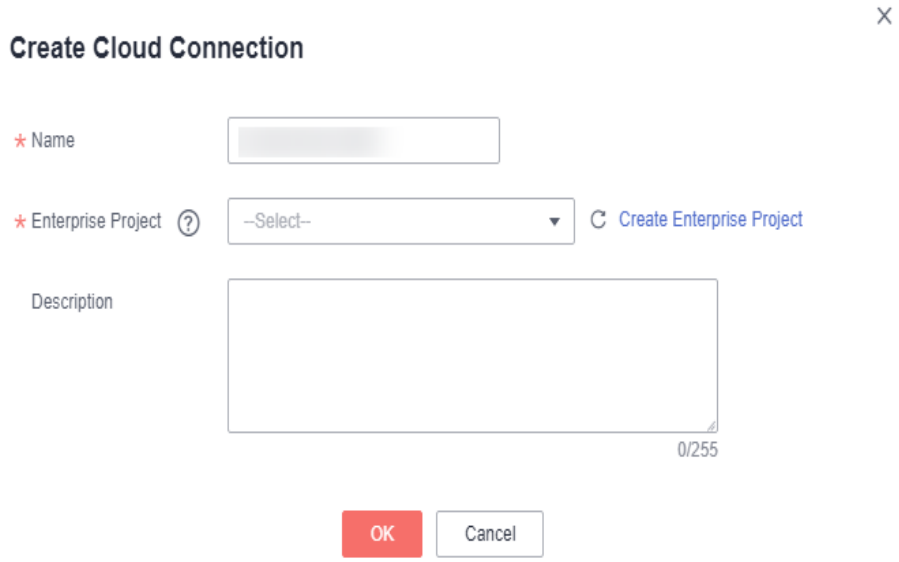
   After you submit the application, the status will change to **Pending approval**. The review takes about one working day. When the status changes to **Approved**, you can buy bandwidth packages.

----End

Procedure

1. Create a cloud connection.
   a. Log in to the management console.
   b. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
   c. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.
   d. Click **Create Connection**.
   e. Click **Create Cloud Connection**. On the displayed page, configure the parameters and click **OK**.

      Figure 1-2 Creating a cloud connection



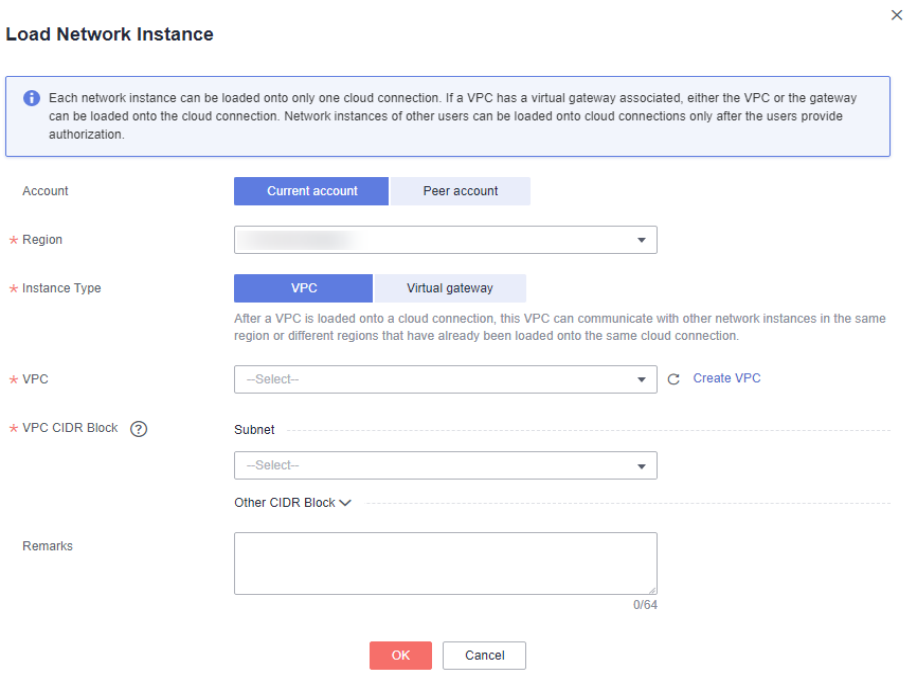
2. Load network instances.
   a. Locate the cloud connection, in this case, **cloudconnect-001**, and click its name.
   b. Click **Load Network Instance**.
   c. Configure other parameters based on **Table 1-2** and then click **OK**.

      Table 1-2 Parameter description

Parameter	Description	Example Value
Account	Specifies whether network instances are from the current account or another account.	Current account

Parameter	Description	Example Value
Region	Specifies the region where the VPC you want to connect is located.	CN North-Beijing4 CN-Hong Kong
Instance Type	Specifies the type of the network instance you want to load to the cloud connection. Two options are available, **VPC** and **Virtual gateway**.	VPC
VPC	Specifies the VPC you want to load to the cloud connection. This parameter is mandatory if you have set **Instance Type** to **VPC**.	CN North Beijing4: VPC-01 CN-Hong Kong: VPC-e725
VPC CIDR Block	Specifies the subnets of the VPC you want to load and the custom CIDR blocks. If you have set **Instance Type** to **VPC**, configure the following two parameters: • **Subnet**: Select one or all subnets of the VPC. • **Other CIDR Block**: Add one or more custom CIDR blocks as needed.	Subnet: CN North-Beijing4: subnet-1 (192.168.1.0/24) CN-Hong Kong: subnet-e730 (192.168.0.0/24) Other CIDR Block CN North-Beijing4: 192.168.44.0/24 CN-Hong Kong: 192.168.11.0/24

Figure 1-3 Loading network instances



d. In the dialog box indicating that the loading is successful, click **Load Another Instance**, configure the parameters based on **Table 1-2**, and then click **OK**.

3. Buy a bandwidth package.

   By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions. To ensure normal network communications between regions in the same geographic region or across geographic regions, you need to purchase a bandwidth package and bind it to a cloud connection.

   a. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.

   b. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.

   c. Click **Buy Bandwidth Package**.

   d. Configure the parameters based on **Table 1-3** and click **Buy Now**.

Table 1-3 Parameter description

Parameter	Description	Example Value
Billing Mode	Specifies how you want the bandwidth package to be billed. You can purchase it by year or month as desired.	Yearly/Monthly

Parameter	Description	Example Value
Name	Specifies the bandwidth package name. The name can contain 1 to 64 characters, including digits, letters, hyphens (-), underscores (_), and periods (.).	bandwidthPackge-8047
Billed By	Specifies by what you want the bandwidth package to be billed.	Bandwidth
Applicability	Specifies whether you want to use the bandwidth package for network communications within a geographic region or between geographic regions. Two options are available: **Single Geographic Region**: The regions you assign inter-region bandwidths to are in the same geographic region. **Across Geographic Regions**: The regions you assign inter-region bandwidths to are in different geographic regions.	Single Geographic Region
Geographic Region	Specifies the geographic region where regions requiring inter-region bandwidths are located.	Chinese mainland Asia-Pacific
Bandwidth	Specifies the bandwidth you require for network communications across regions, in Mbit/s. The sum of all inter-region bandwidths you assign cannot exceed the bandwidth of the bandwidth package. Assign the bandwidth based on your network plan.	5
Required Duration	Specifies how long you require the bandwidth package for. Auto renewal is supported.	1 month

Parameter	Description	Example Value
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default
Cloud Connection	Specifies the cloud connection you want to bind the bandwidth package to. Two options are available, **Bind now** and **Bind later**.	Bind now

e. Confirm the information and click **Pay Now**.

f. Click **Pay**.

Go back to the bandwidth package list and locate the bandwidth package. If its status changes to **Normal**, you can bind the bandwidth package to a cloud connection.

4. Assign inter-region bandwidth.

a. Log in to the management console.

b. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.

c. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.

d. In the cloud connection list, locate the cloud connection and click its name.

e. Click **Inter-Region Bandwidths**.

f. Click **Assign Inter-Region Bandwidth** and configure the parameters based on **Table 1-4**.

Table 1-4 Parameter description

Parameter	Description	Example Value
Regions	Specifies the two regions between which network communications are required.	CN North-Beijing4 CN-Hong Kong
Bandwidth Package	Specifies the bandwidth package you want to bind to the cloud connection.	bandwidthPackge-8047 (Chinese mainland – Asia Pacific)

Parameter	Description	Example Value
Bandwidth	Specifies the bandwidth you require for communications between regions, in Mbit/s. The sum of all inter-region bandwidths you assign based on the bandwidth package cannot exceed the bandwidth of the bandwidth package. Plan the bandwidth in advance.	5 Mbit/s

g. Click **OK**.

Now the VPCs in two regions can communicate with each other.

5. View the routes and verify the configuration.

2 Connecting Multiple VPCs Across Regions

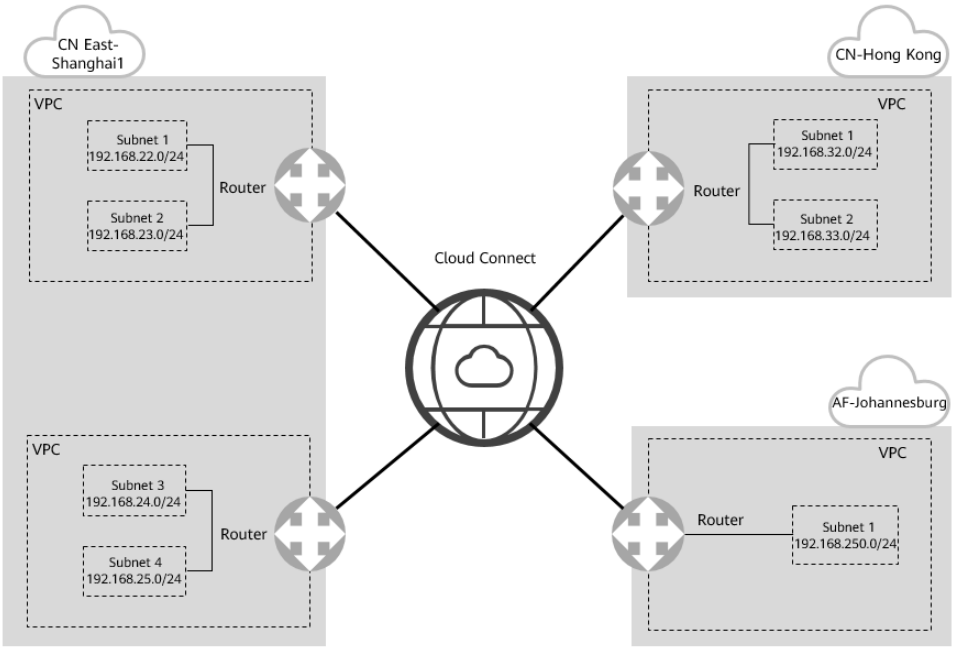
Background

Resources in the VPCs in different regions can use EIPs or VPN connections to communicate with each other. However, EIPs and VPN connections rely on the Internet, which can be unstable, and if you use EIPs, data cannot be encrypted. To ensure stable network quality and prevent data breach, you can use Cloud Connect to connect the VPCs.

Scenarios

You have four VPCs, two in the CN East-Shanghai1 region, one in the CN-Hong Kong region, and one in the AF-Johannesburg region. The two VPCs in the CN East-Shanghai1 region each have two subnets. You can use Cloud Connect to connect the VPCs in the three regions to build a network that features high performance, high availability, and low latency. The following figure shows a typical scenario where Cloud Connect is used to enable communications among VPCs in different regions.

Figure 2-1 Cross-region multi-VPC communications



When you configure Cloud Connect, note that:

- Subnet CIDR blocks of the VPCs cannot overlap or conflict with each other.
- Existing routes, including those you add for VPC Peering, Direct Connect, or VPN, cannot conflict with the routes of subnets that you load to the cloud connection.

Prerequisites

- You have created the VPCs and subnets that need to communicate with each other across regions.
- Your account balance is sufficient to purchase bandwidth packages.
- You have applied for a cross-border permit from China Unicom. In this practice, there are two VPCs outside the Chinese mainland. In accordance with the regulations of the Ministry of Industry and Information Technology (MIIT), before you purchase bandwidth packages, you need to apply for a cross-border permit from China Unicom.

  NOTE

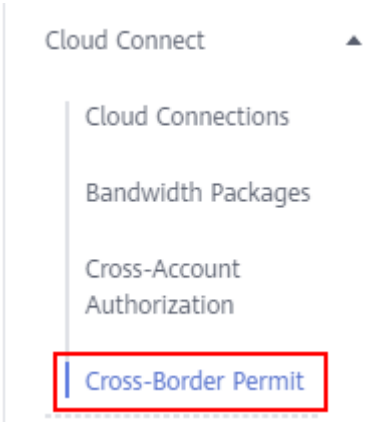
  If you do not need cross-border network communications, you can ignore the last item.

Procedure

Step 1 Apply for a cross-border permit.

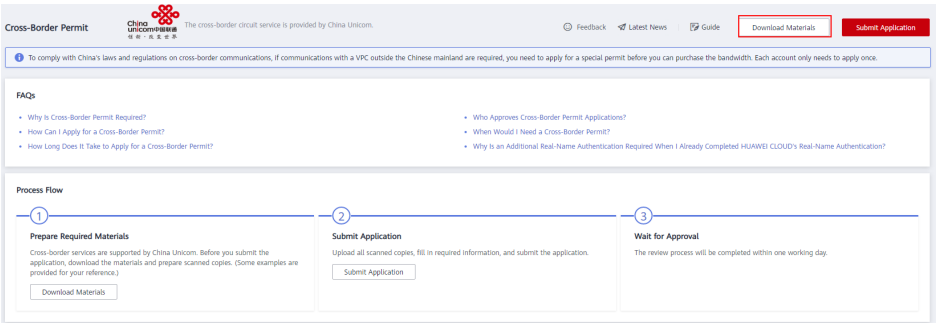
1. In the navigation pane on the left, choose **Cross-Border Permit**.

Figure 2-2 Cross-border permit



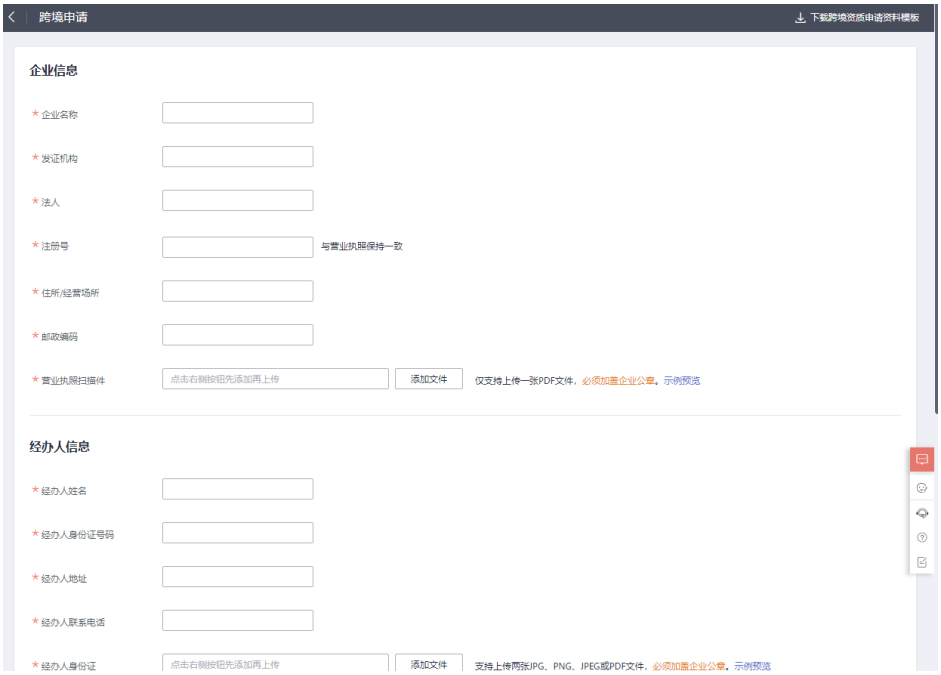
2. Click **Download Materials** to download the materials and examples.

Figure 2-3 Download Materials



3. Click **Submit Application**. Enter all required information and upload the prepared materials.

Figure 2-4 Applying for a cross-border permit

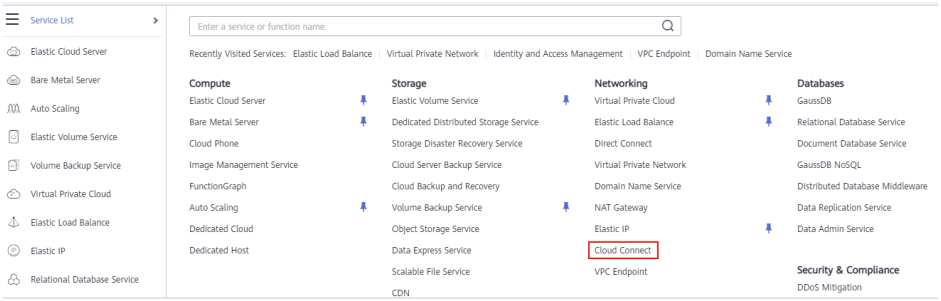


4. Click **Submit** and wait for approval, which requires one working day.

Step 2 Create a cloud connection.

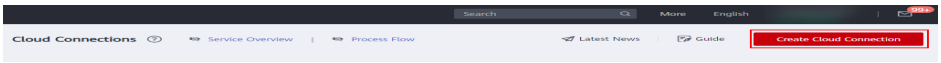
1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.

Figure 2-5 Accessing the Cloud Connect console



3. On the **Cloud Connections** page, click **Create Cloud Connection**.

Figure 2-6 Create Cloud Connection



4. Configure the parameters and click **OK**.

Figure 2-7 Configuring the parameters

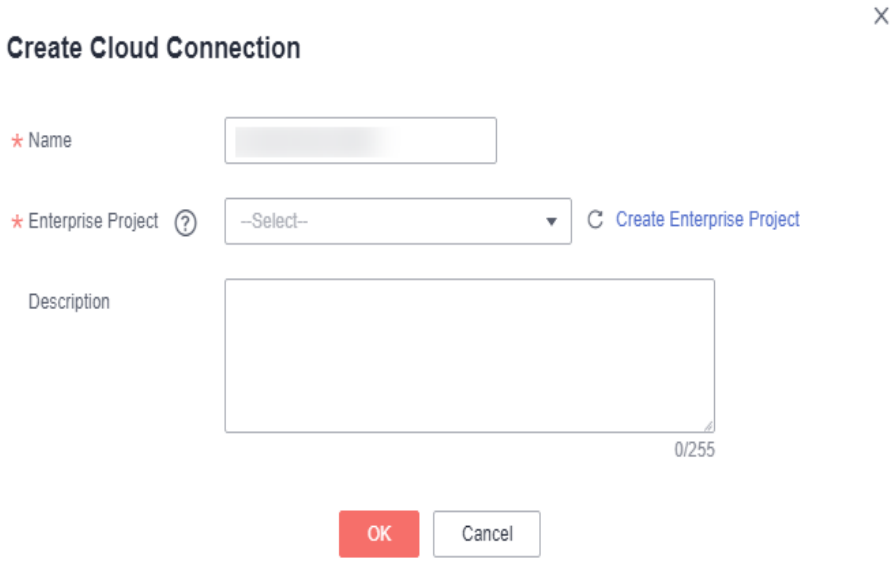


Table 2-1 describes the parameters.

Table 2-1 Parameter description

Parameter	Description	Example Value
Name	Specifies the cloud connection name. The name can contain only letters, digits, underscores (_), hyphens (-), and periods (.).	CloudConnect
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default
Description	Provides supplementary information about the cloud connection. The description can contain a maximum of 255 characters.	A Cloud Connect instance for Demo

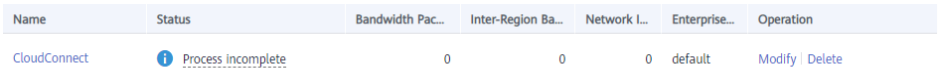
5. Click **OK**.

Step 3 Load network instances.

Load the VPCs to the created cloud connection.

1. In the cloud connection list, locate the cloud connection you just created and click its name, for example, **CloudConnect** in the following figure.

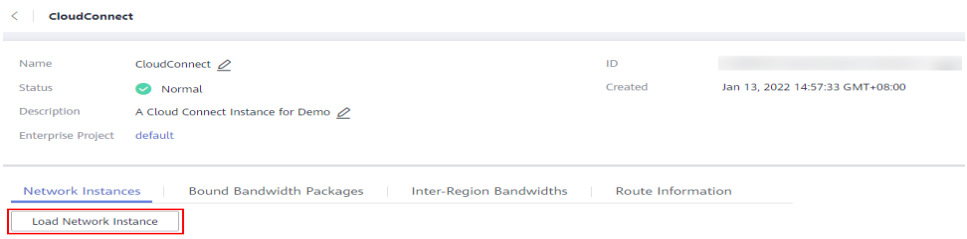
Figure 2-8 Cloud connection



NOTE

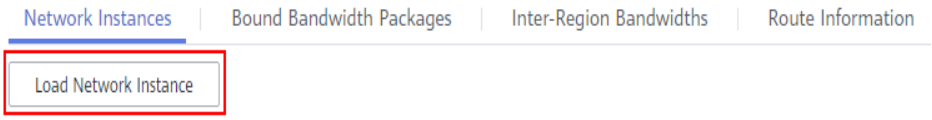
On the displayed page, you can view details about the cloud connection, such as its name, ID, status, time when the cloud connection was created, and description. There are also four tabs: **Network Instances**, **Bound Bandwidth Packages**, **Inter-Region Bandwidths**, and **Route Information**.

Figure 2-9 Cloud connection details



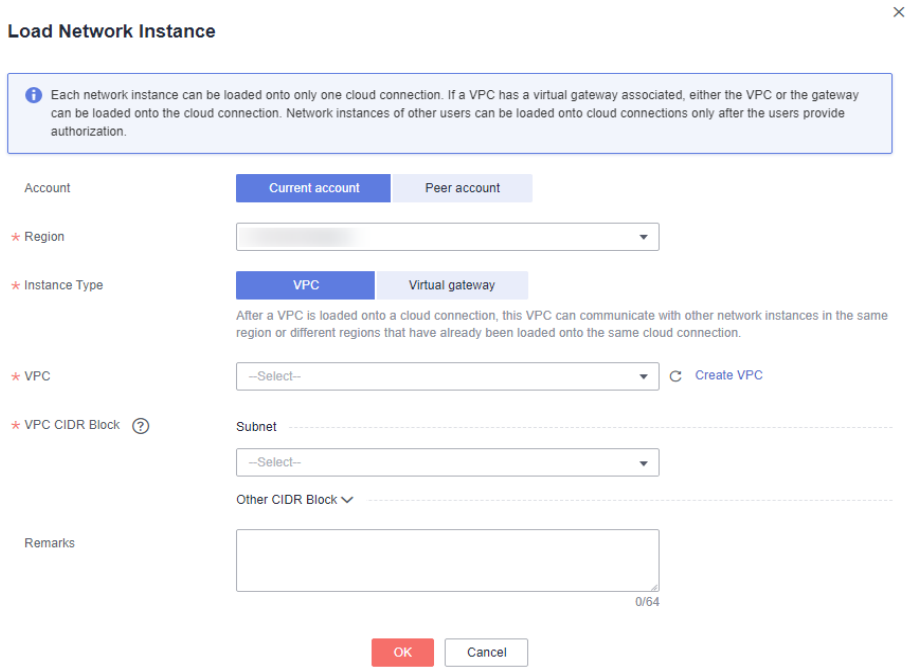
2. Under **Network Instances**, click **Load Network Instance**.

Figure 2-10 Load Network Instance



3. Select **CN East-Shanghai1** for **Region** and **VPC** for **Instance Type**, select the VPC and its subnets, and click **OK**.

Figure 2-11 Loading a network instance



4. Repeat the preceding steps to load the other VPC in the CN East-Shanghai1 region, the VPC in the CN-Hong Kong region, and the VPC in the AF-Johannesburg region to the cloud connection.

NOTE

The four VPCs in the three regions are now on the same network. You can view the routes of each region on the **Route Information** tab page.

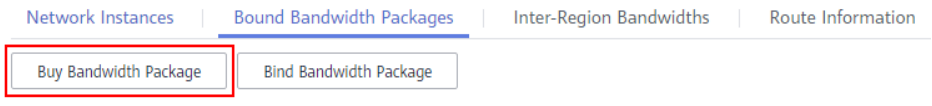
Step 4 Buy a bandwidth package.

By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions.

To ensure normal network communications, you need to purchase a bandwidth package and bind the package to the cloud connection.

1. Locate the created cloud connection and click its name to go to the details page. Under **Bound Bandwidth Packages**, click **Buy Bandwidth Package**.

Figure 2-12 Buy Bandwidth Package



2. On the **Buy Bandwidth Package** page, configure the name, billing mode, bandwidth package applicability, geographic region, bandwidth size, and required duration, and determine whether to enable auto renewal and directly bind the bandwidth package to the cloud connection. Select **Across Geographic Region** for **Applicability** because the four VPCs are in three geographic regions.

   a. To enable network communications between the CN East-Shanghai1 and the CN-Hong Kong regions, select Chinese mainland and Asia Pacific as geographic regions and set the bandwidth to 30 Mbit/s.

   b. To enable network communications between the CN East-Shanghai1 and AF-Johannesburg regions, select Chinese mainland and Southern Africa as geographic regions and set the bandwidth to 2 Mbit/s.

   Click **Bind now**, select the cloud connection you just created, and click **Buy Now**.

3. Confirm the information and click **Pay Now**.
4. Click **Pay**.

   Go back to the bandwidth package list, locate the bandwidth package, and verify that its status is **Normal**.

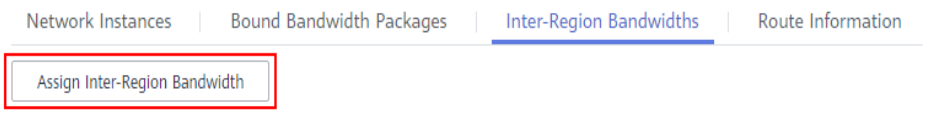
   On the **Bandwidth Packages** page, you can view the purchased bandwidth package and its details, including the billing mode, order information, the cloud connection it is bound to, used bandwidth, and remaining bandwidth. You can also modify, unbind, renew, and unsubscribe from the bandwidth package.

Step 5 Assign inter-region bandwidths.

On the cloud connection details page, assign bandwidths for network communications between regions.

1. Locate the created cloud connection and click its name to go to the details page. Under **Inter-Region Bandwidths**, click **Assign Inter-Region Bandwidth**.

   Figure 2-13 Assign Inter-Region Bandwidth

2. Select **CN East-Shanghai1** and **CN-Hong Kong** for **Regions**. The bandwidth package that you have purchased is displayed. Set the bandwidth to 30 Mbit/s.

   Repeat the preceding steps to assign 2 Mbit/s of bandwidth for network communications between CN East-Shanghai1 and AF-Johannesburg.

3. View the assigned bandwidths on the **Inter-Region Bandwidths** tab page.

   Now, the four VPCs can communicate with each other.

NOTE

The default security group rule denies all the inbound traffic. Ensure that security group rules in both directions are correctly configured for resources in the regions to ensure normal communications.

----End

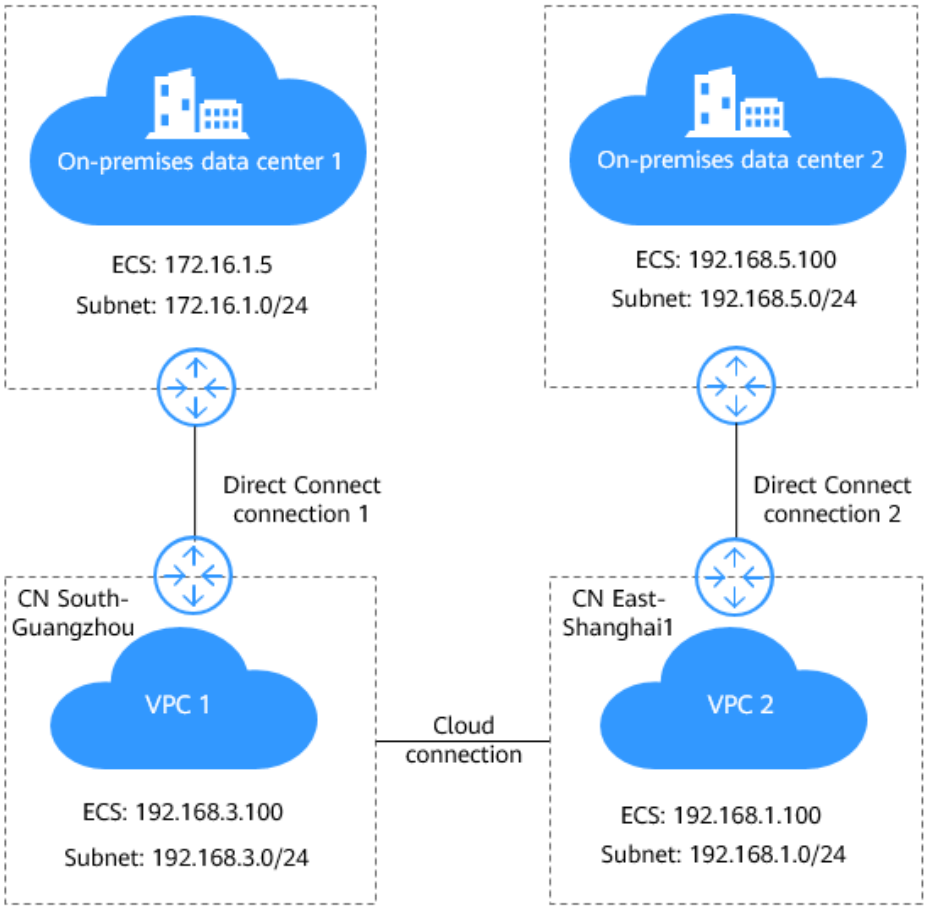
3 Connecting Multiple On-premises Data Center to Multiple VPCs in Different Regions

Scenarios

If you have more than one on-premises data center and more than one VPC, you can use Direct Connect and Cloud Connect to connect all your on-premises data centers to the VPCs in different regions.

Figure 3-1 shows the networking topology

Figure 3-1 Networking topology



NOTE

When you configure Cloud Connect, note that:

- Subnet CIDR blocks of the VPCs cannot overlap or conflict with each other.
- Existing routes, including those you add for VPC Peering, Direct Connect, or VPN, cannot conflict with the routes of subnets that you load to the cloud connection.

Prerequisites

- You have registered a HUAWEI CLOUD account and completed real-name authentication.
- Your account balance is sufficient to purchase the required resources, including Direct Connect connections, bandwidth packages, and ECSs.
- You have selected appropriate Direct Connect locations and completed the site survey of your on-premises data centers with the carrier. For details, see **Preparations**.
- You have created the VPCs and subnets that need to communicate with each other across regions.
- You have configured all VPC subnets for your on-premises data center.

Procedure

Step 1 Configure Direct Connect.

1. Create a Direct Connect connection.
   a. Log in to the Direct Connect console.
   b. On the console homepage, click  in the upper left corner and select the desired region and project.
   c. Hover on  to display **Service List** and choose **Networking** > **Direct Connect**.
   d. In the navigation pane on the left, choose **Direct Connect** > **Connections**.
   e. Click **Create Connection**.
   f. On the **Create Connection** page, configure the parameters based on **Table 3-1**.

Table 3-1 Parameter description

Parameter	Description	Example Value
Region	Specifies the region where the connection is deployed. You can change the region here, or use the region selector in the upper left corner of the console.	CN South-Guangzhou
Connection Name	Specifies the connection name. Enter a desired name.	dc-cc
Location	Specifies the location that your leased line can access.	Guangzhou-Huangpu-Huaxinyuan
Carrier	Specifies the carrier that provides the leased line.	China Telecom
Port Type	Specifies the type of the port used by the connection. There are four types of ports: 1GE, 10GE, 40GE, and 100GE.	1GE single-mode optical port
Leased Line Bandwidth	Specifies the bandwidth of the connection, in Mbit/s. Select a value from the drop-down list. This is the bandwidth of the leased line you have purchased from the carrier.	1,000

Parameter	Description	Example Value
Your Equipment Room Address	Specifies the address of your equipment room. The address must be specific to the floor on which your equipment room is located, for example, Equipment Room XX, Building XX, No. XX, Huajing Road, Fengdong District, Shanghai.	N/A
Description	Provides supplementary information about the connection.	N/A
Billing Mode	Specifies the billing model of the connection. Currently, only **Yearly/ Monthly** is supported.	Yearly/Monthly
Required Duration	Specifies the duration for which you require the connection.	5 months
Auto-renew	Specifies whether to automatically renew the connection to ensure service continuity. It is recommended that you set the auto-renewal period to be the same as the required duration. If the required duration is three months, the system automatically renews the subscription for three months.	5 months
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default
Contact Person/ Phone Number/ Contact Email	Specifies information about the person who is responsible for your connection. If you do not provide the contact information, your account information will be used. This will increase the review period.	Tom +086 13912345678 (Chinese mainland) Tom@mail.com

g. Click **Next**

h. Confirm the order and click **Pay**.

i. Click **Pay**.

2. Connect your data center to the location.

   a. After the payment is complete, switch back to the connection list. Locate the newly created connection, click **Apply for LOA** in the **Operation** column, and then enter information about the construction plan and equipment room LOA.

b. Click **Confirm** to submit the LOA application, and wait for the approval. During this period, you can view the LOA.

c. After the LOA is approved, request the carrier to complete the construction. Click **Download LOA**, save and print the LOA, and contact your carrier. The carrier and construction personnel must carry the LOA when entering the construction site.

d. After the cabling is complete, obtain the line code and in-building cable label from your carrier and click **Report Completion of Construction**.

e. Wait for HUAWEI CLOUD to complete the construction. HUAWEI CLOUD engineers will connect the leased line to the HUAWEI CLOUD gateway port.

f. After the construction is completed, click **Confirm Completion** in the **Operation** column.

g. Click **Confirm**. The connection status will change to **Normal**.

NOTE

LOA application, cabling by the carrier, and construction by HUAWEI CLOUD involve coordination with the equipment room operator, and the time for these activities depends on special situations such as holidays and national policies.

3. Create a virtual gateway.

After creating a connection, create a virtual gateway to associate it with the VPC in South China.

a. Log in to the management console.

b. On the console homepage, click  in the upper left corner and select the desired region and project.

c. Hover on  to display **Service List** and choose **Networking** > **Direct Connect**.

d. In the navigation pane on the left, choose **Direct Connect** > **Virtual Gateways**.

e. Click **Create Virtual Gateway**.

f. Configure the parameters based on **Table 3-2**.

Figure 3-2 Create Virtual Gateway

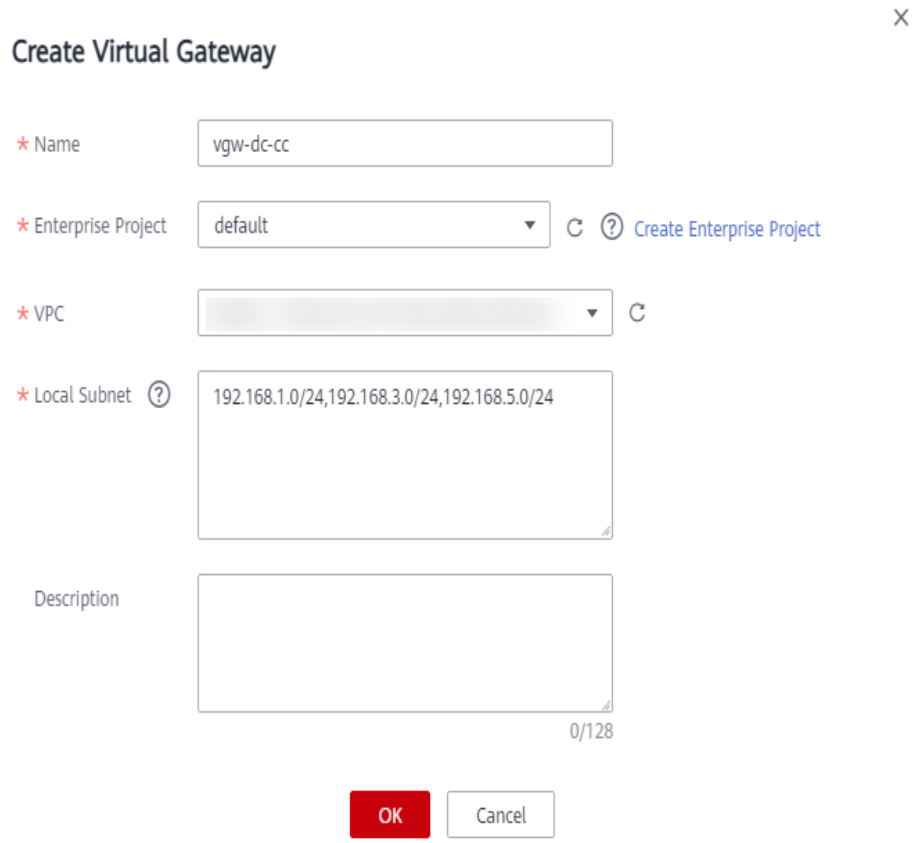


Table 3-2 Parameter description

Parameter	Description	Example Value
Name	Specifies the virtual gateway name. The name can contain 1 to 64 characters.	vgw-dc-cc
VPC	Specifies the VPC associated with the virtual gateway.	VPC-GuangZhou
Local Subnet	Specifies the CIDR blocks of subnets in the VPC to connect to the on-premises network.	192.168.1.0/24 192.168.3.0/24 192.168.5.0/24
Description	Provides supplementary information about the virtual gateway. The description can contain a maximum of 128 characters.	-

> **NOTE**
>
> Add CIDR blocks of all VPC subnets that will communicate with the data center to ensure normal communications.

g. Click **OK**.

When the virtual gateway status changes **Normal**, the virtual gateway has been created.

4. Create a virtual interface.

After the connection and the virtual gateway are ready, you need to create a virtual interface so that your network can access the VPC in CN South-Guangzhou.

a. Log in to the management console.

b. On the console homepage, click  in the upper left corner and select the desired region and project.

c. Hover on  to display **Service List** and choose **Networking** > **Direct Connect**.

d. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.

e. Click **Create Virtual Interface**.

f. Configure the parameters based on **Table 3-3**.

Figure 3-3 Create Virtual Interface

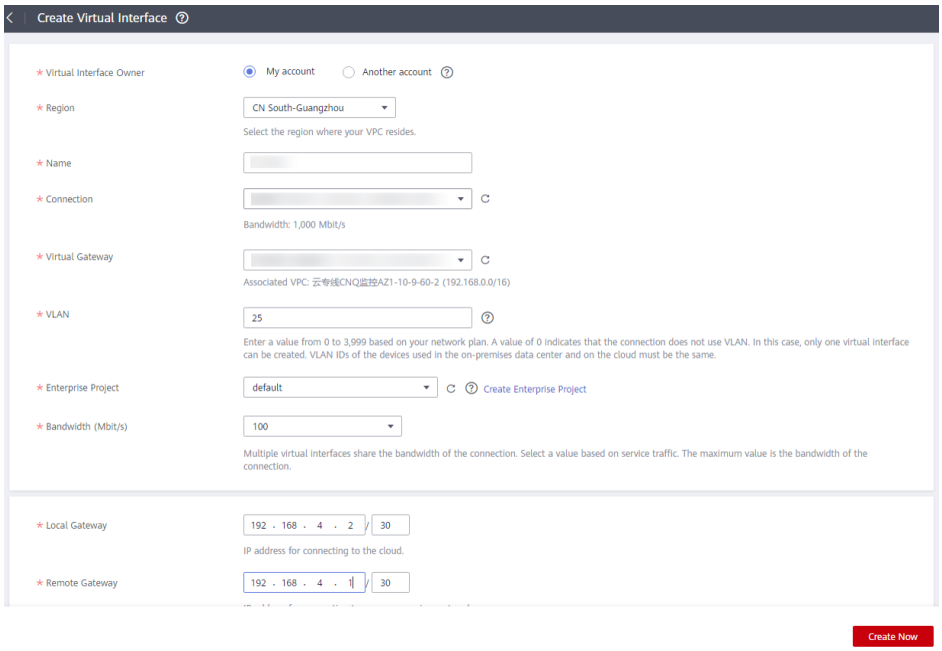


Table 3-3 Parameter description

Parameter	Description	Example Value
Region	Specifies the region where the connection is deployed. You can change the region here, or use the region selector in the upper left corner of the console.	CN South-Guangzhou
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters.	vif-dc-cc
Connection	Specifies the connection you use to connect your data center to the cloud.	dc-cc
Virtual Gateway	Specifies the virtual gateway to which the virtual interface will connect.	vgw-dc-cc
VLAN	Specifies the VLAN of the virtual interface. You need to configure the VLAN if you buy a self-service connection. The VLAN for a hosted connection will be allocated by the carrier or partner. In this scenario, you do not need to configure the VLAN.	25
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default
Bandwidth	Specifies the bandwidth that can be used by the virtual interface, in Mbit/s. The bandwidth cannot exceed that of the connection.	500
Local Gateway	Specifies the IP address of the network interface on the HUAWEI CLOUD side.	192.168.4.2/30

Parameter	Description	Example Value
Remote Gateway	Specifies the network IP address for connecting to your data center. The IP address of the remote gateway must be in the same network segment as that of the local gateway, and it is recommended that both IP addresses use a 30-bit mask.	192.168.4.1/30
Remote Subnet	Specifies the subnets and masks of your network. If there are multiple subnets, use commas (,) to separate them.	172.16.1.0/24
Routing Mode	Specifies the routing mode. Two options are available, static routing and BGP routing. If there are two or more connections, select BGP routing.	BGP
BGP ASN	Specifies the ASN of the BGP peer. Enter a value from 1 to 65535, excluding 64512, which is reserved by HUAWEI CLOUD. This parameter is required if you select BGP routing.	12345
BGP MD5 Authentication Key	Specifies the password used to authenticate the BGP peer using MD5. This parameter is mandatory if you select BGP routing, and you must ensure that the parameter values on both gateways are the same. The value contains 8 to 255 characters and must contain at least two types of the following characters: ■ Uppercase letters ■ Lowercase letters ■ Digits ■ Special characters ~!, .:;-_"(){}[]/@#$ %^&*+|=	12345678

Parameter	Description	Example Value
Description	Provides supplementary information about the virtual interface. The description can contain a maximum of 128 characters.	N/A

g. Click **Submit**. When the status of the virtual interface changes **Normal**, the virtual interface has been created.

h. Ping a server in on-premises data center 1 from an ECS in the VPC in CN South-Guangzhou (VPC 1) to test network connectivity.

5. Repeat **Step 1.1** to **Step 1.4** to establish network connectivity between on-premises data center 2 and the VPC in CN East-Shanghai1 (VPC 2).

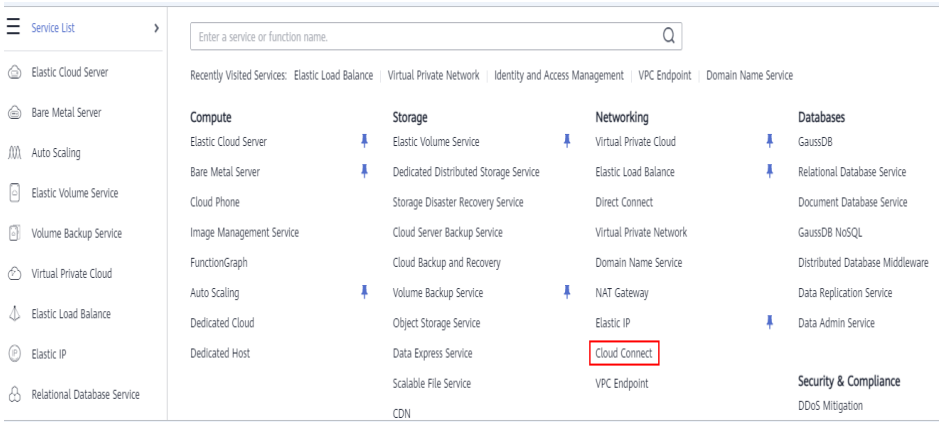
Step 2 Configure Cloud Connect.

1. Create a cloud connection.

a. Log in to the management console.

b. Hover on ☰ to display **Service List** and choose **Networking** > **Direct Connect**.

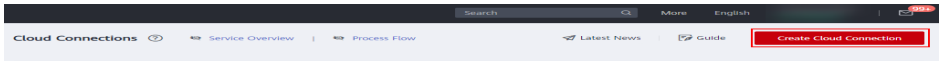
Figure 3-4 Cloud Connect



c. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.

d. On the displayed page, click **Create Cloud Connection**.

Figure 3-5 Create Cloud Connection



e. Configure the parameters based on **Table 3-4**.

Table 3-4 Parameter description

Parameter	Description	Example Value
Name	Specifies the cloud connection name. The name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).	CloudConnect
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default
Description	Provides supplementary information about the cloud connection. The description can contain a maximum of 255 characters.	A cloud connection for demo

f. Click **OK**.

2. Load network instances.

   Load the network instances to the created cloud connection.

   a. In the cloud connection list, click the cloud connection named **CloudConnect**.

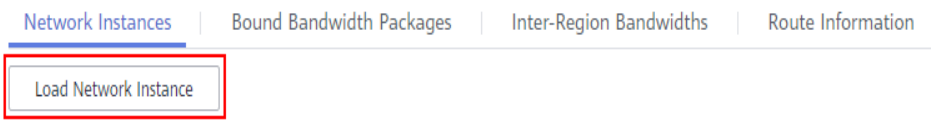
   NOTE

   On the displayed page, you can view details about the cloud connection, such as its name, ID, status, time when the cloud connection was created, and description. There are also four tabs: **Network Instances**, **Bound Bandwidth Packages**, **Inter-Region Bandwidths**, and **Route Information**.

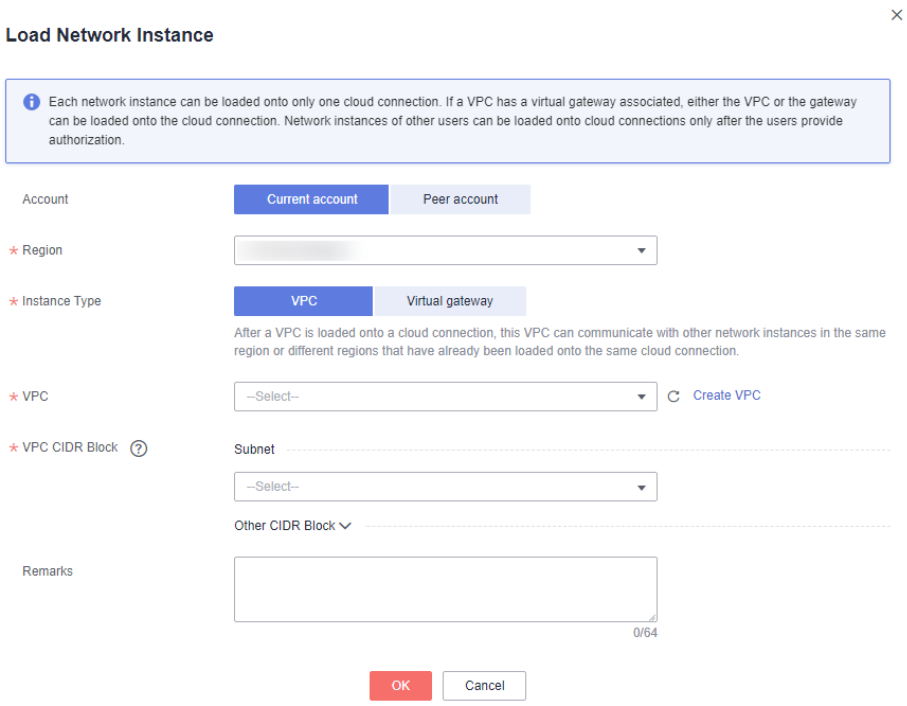
   Figure 3-6 Cloud connection details

   b. Under **Network Instances**, click **Load Network Instance**.

   Figure 3-7 Load Network Instance



   c. Configure the parameters.



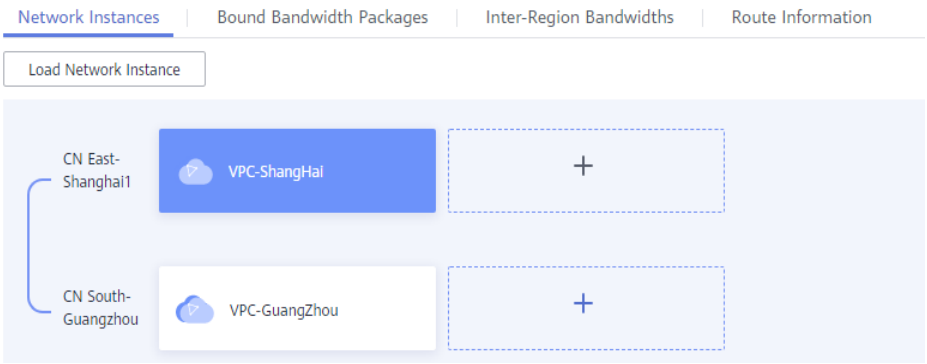
NOTE

To establish network communications with your on-premises data center, you need to add the subnet used in your on-premises data center as a custom CIDR block.

d. Click **OK**. The VPC in the CN South-Guangzhou region is loaded to the cloud connection.

e. Repeat the preceding steps to load the VPC in the CN East-Shanghai region to the cloud connection.

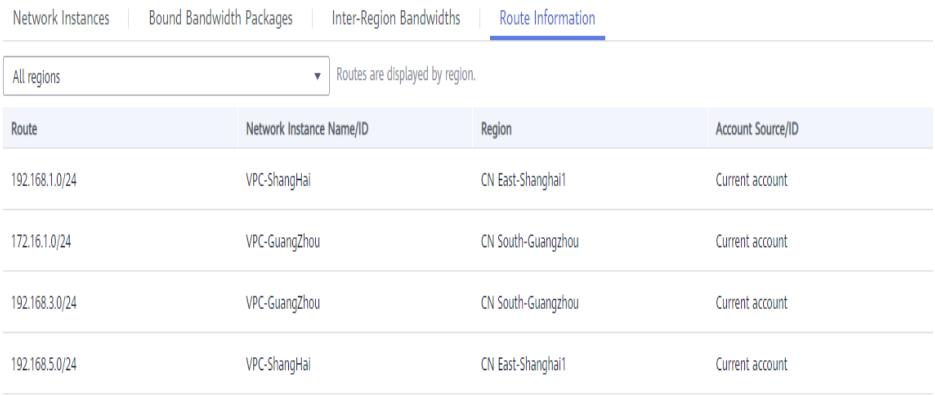
Figure 3-8 Loading the other VPC



NOTE

After you load the VPCs, the VPCs in the two regions are on the same network. You can view the routes of each VPC on the **Route Information** tab page.

Figure 3-9 Route Information



3. Buy a bandwidth package.

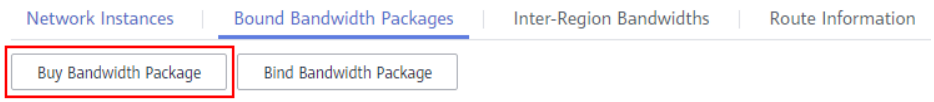
   By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions.

   To ensure normal network communications, you need to purchase a bandwidth package and bind the package to the cloud connection.

   a. In the cloud connection list, click the cloud connection named **CloudConnect**.

   b. On the details page of the cloud connection, click **Bound Bandwidth Packages** and then **Buy Bandwidth Package**.

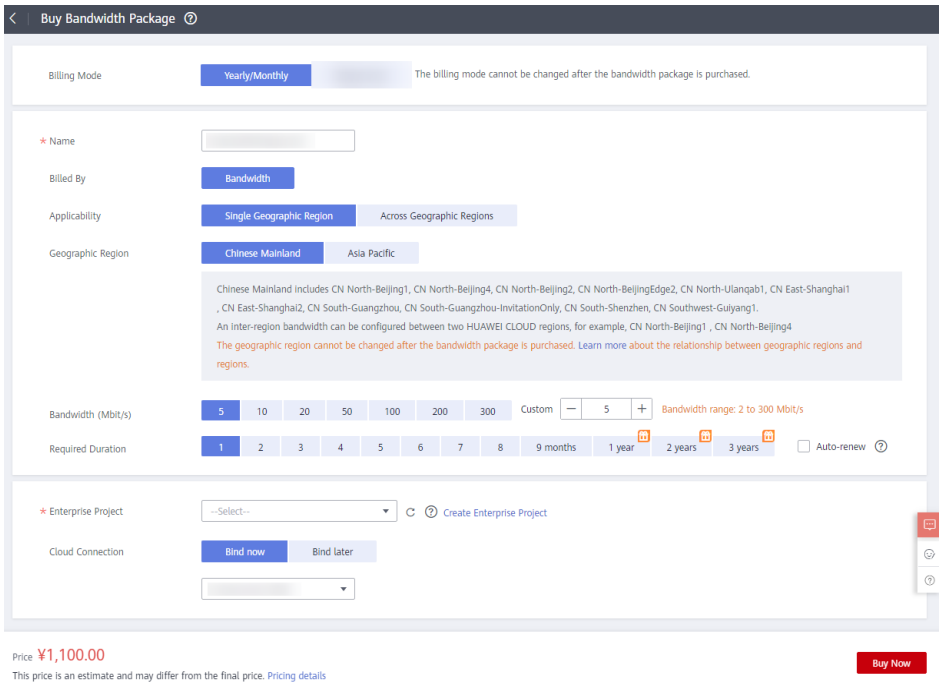
   Figure 3-10 Buy Bandwidth Package

   c. Configure the parameters.

   Because the two VPCs are in the Chinese mainland, select **Single Geographic Region** for **Applicability** and **Chinese mainland** for **Geographic Region**.

Figure 3-11 Buying a bandwidth package



d. Click **Buy Now**.

e. Confirm the information and click **Pay Now**.

f. Click **Pay**.

Go back to the bandwidth package list, locate the bandwidth package, and verify that its status is **Normal**.

NOTE

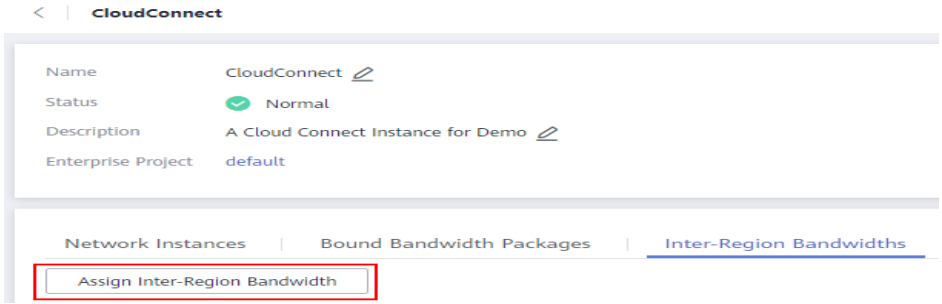
In the navigation pane on the left, choose **Bandwidth Packages**. On the displayed page, locate the bandwidth package you just purchased. You can view its details, including the billing mode, order information, cloud connection to which it is bound, used bandwidth, and remaining bandwidth. You can also modify, unbind, renew, and unsubscribe from the bandwidth package.

4. Assign an inter-region bandwidth.

a. In the cloud connection list, click the cloud connection named **CloudConnect**.

b. On the details page of the cloud connection, click **Inter-Region Bandwidths** and then **Assign Inter-Region Bandwidth**.

Figure 3-12 Assign Inter-Region Bandwidth



c. Configure the parameters.

Select **CN South-Guangzhou** and **CN East-Shanghai1** for **Regions**. The system automatically displays the bandwidth package bound to the cloud connection. Set the bandwidth based on your requirements, for example, 1 Mbit/s.

d. View the assigned bandwidth on the **Inter-Region Bandwidths** tab page.

NOTE

The default security group rule denies all the inbound traffic. Ensure that security group rules in both directions are correctly configured for resources in the regions to ensure normal communications.

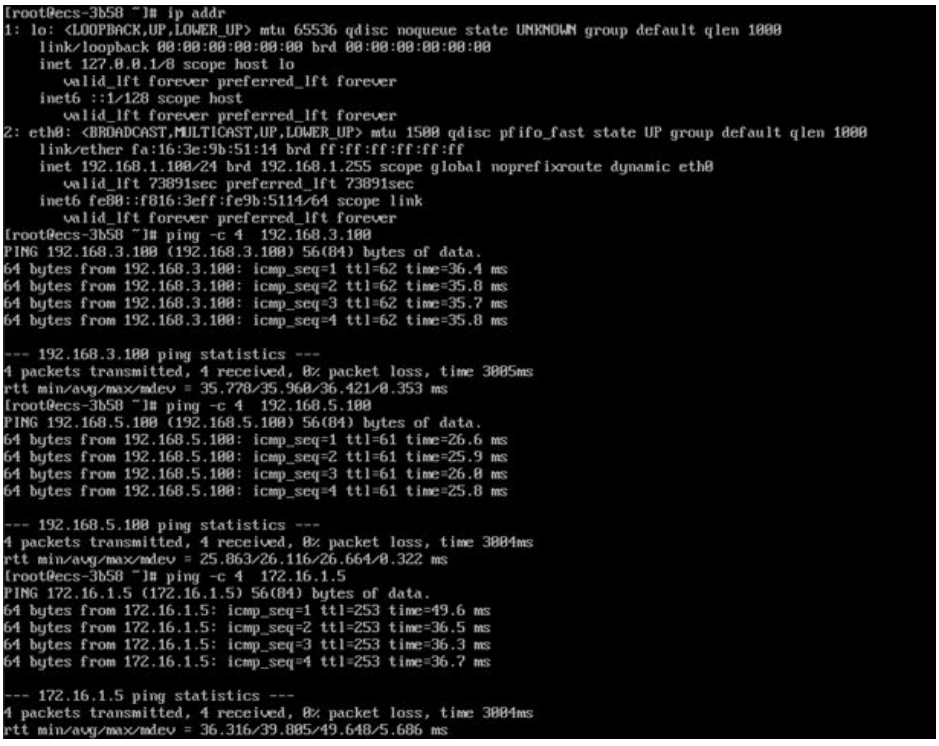
Step 3 Configure local routes.

- In on-premises data center 1, add routes to the VPC in CN East-Shanghai1 (192.168.1.0/24), the VPC in CN South-Guangzhou (192.168.3.0/24), and on-premises data center 2 (192.168.5.0/24).
- In on-premises data center 2, add routes to the VPC in CN East-Shanghai1 (192.168.1.0/24), the VPC in CN South-Guangzhou (192.168.3.0/24), and on-premises data center 1 (172.16.1.0/24).

----End

Verification

1. Ping an ECS in the CN East-Shanghai1 region and an ECS in each data center from an ECS in the CN South-Guangzhou region.



2. Ping an ECS in the CN South-Guangzhou region and an ECS in each data center from an ECS in the CN East-Shanghai1 region.


```
[root@ecs-hn ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 10
    link/ether fa:16:3e:4e:b8:c6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.3.100/24 brd 192.168.3.255 scope global noprefixroute dynamic eth0
       valid_lft 31353124sec preferred_lft 31353124sec
    inet6 fe80::f816:3eff:fe4e:b8c6/64 scope link
       valid_lft forever preferred_lft forever
[root@ecs-hn ~]# ping -c 4 192.168.1.100
PING 192.168.1.100 (192.168.1.100) 56(84) bytes of data.
64 bytes from 192.168.1.100: icmp_seq=1 ttl=62 time=36.4 ms
64 bytes from 192.168.1.100: icmp_seq=2 ttl=62 time=35.7 ms
64 bytes from 192.168.1.100: icmp_seq=3 ttl=62 time=35.9 ms
64 bytes from 192.168.1.100: icmp_seq=4 ttl=62 time=35.6 ms

--- 192.168.1.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 35.672/35.949/36.489/0.397 ms
[root@ecs-hn ~]# ping -c 4 192.168.5.100
PING 192.168.5.100 (192.168.5.100) 56(84) bytes of data.
64 bytes from 192.168.5.100: icmp_seq=1 ttl=61 time=40.6 ms
64 bytes from 192.168.5.100: icmp_seq=2 ttl=61 time=40.2 ms
64 bytes from 192.168.5.100: icmp_seq=3 ttl=61 time=40.1 ms
64 bytes from 192.168.5.100: icmp_seq=4 ttl=61 time=40.2 ms

--- 192.168.5.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 40.128/40.326/40.690/0.257 ms
[root@ecs-hn ~]# ping -c 4 172.16.1.5
PING 172.16.1.5 (172.16.1.5) 56(84) bytes of data.
64 bytes from 172.16.1.5: icmp_seq=1 ttl=255 time=17.8 ms
64 bytes from 172.16.1.5: icmp_seq=2 ttl=255 time=4.12 ms
64 bytes from 172.16.1.5: icmp_seq=3 ttl=255 time=7.09 ms
64 bytes from 172.16.1.5: icmp_seq=4 ttl=255 time=5.28 ms

--- 172.16.1.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 4.124/8.579/17.807/5.432 ms
```

3. View the routes.

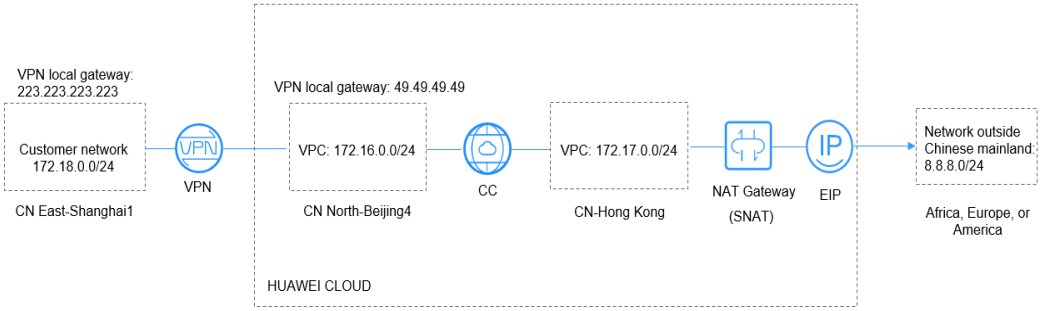
4 Working with SNAT to Access the Internet Outside China from a Private Network

Scenarios

This practice provides detailed operations for accessing the Internet outside China by using Cloud Connect, VPN, and NAT Gateway.

Figure 4-1 shows the networking topology.

Figure 4-1 Networking



NOTE

- In this practice, consider the VPC in CN East-Shanghai1 as the on-premises network.
- The network outside China is 8.8.8.0/24, and 8.8.8.8 is the only IP address for test.
- Your account must have the permission for cross-border network communication. If you do not have the permission, you can authorize the other user to load the VPCs.

Procedure

Step 1 Create the following VPCs and ensure that the VPC CIDR blocks do not conflict with each other.

- VPC in CN East-Shanghai1: 172.18.0.0/24
- VPC in CN North-Beijing4: 172.16.0.0/24

- VPC in CN-Hong Kong: 172.17.0.0/24

For details, see **Creating a VPC**.

Step 2 Configure the VPN service.

Buy a VPN gateway and a VPN connection to connect networks in CN North-Beijing4 and CN East-Shanghai1.

For details, see **Buying a VPN Gateway** and **Buying a VPN Connection**.

- Gateway and subnet configurations for CN North-Beijing4:
  - Local subnets: 172.16.0.0/24, 172.17.0.0/24, and 8.8.8.0/24
  - Remote gateway: 223.223.223.223
  - Remote subnet: 172.18.0.0/24
- Gateway and subnet configurations for CN East-Shanghai1:
  - Local subnet: 172.18.0.0/24
  - Remote gateway: 49.49.49.49
  - Remote subnets: 172.16.0.0/24, 172.17.0.0/24, and 8.8.8.0/24

NOTE

When you configure the VPN connection between CN North-Beijing4 and CN East-Shanghai1, ensure that local subnets in CN North-Beijing4 and remote subnets in CN East-Shanghai1 contain the network outside China (8.8.8.0/24) so that this network can be pinged.

Step 3 Configure Cloud Connect.

1. Create a cloud connection.

   For details, see **Creating a Cloud Connection**.
2. Load the VPCs.

   For details, see **Loading a Network Instance**.
3. Add custom CIDR blocks.

   For details, see **Adding a Custom CIDR block**.
   - Custom CIDR blocks for CN North-Beijing4: 172.18.0.0/24 and 172.16.0.0/24
   - Custom CIDR blocks for CN-Hong Kong: 172.17.0.0/24 and 8.8.8.0/24

   NOTE

   To enable communications among all nodes, you need to add all local subnets.
4. Buy a bandwidth package.

   By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions. You need to buy a bandwidth package to ensure normal network communications across regions.

   For details, see **Buying a Bandwidth Package**.
5. Assign inter-region bandwidths.

   For details, see **Assigning Inter-Region Bandwidth**.

Step 4 Buy an ECS in CN North-Beijing4, CN East-Shanghai1, and CN-Hong Kong.

For details, see **Purchasing an ECS**.

- Private IP address of the ECS in CN North-Beijing4: 172.16.0.3
- Private IP address of the ECS in CN East-Shanghai1: 172.18.0.3
- Private IP address of the ECS in CN-Hong Kong: 172.17.0.3

Step 5 Buy an EIP and configure a NAT gateway.

Buy an EIP in the CN-Hong Kong region, buy a NAT gateway, and add SNAT rules that include the following CIDR blocks:

For details, see **Assigning an EIP and Binding It to an ECS** and **Adding an SNAT Rule**.

- VPC CIDR block: 172.17.0.0/24
- Direct Connect/Cloud Connect CIDR block: 172.18.0.0/24
- Direct Connect/Cloud Connect CIDR block: 172.16.0.0/24

NOTE

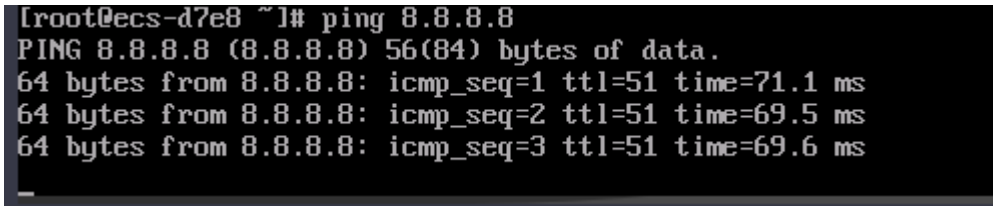
Add SNAT rules to allow access to the Internet and ping the network outside China (8.8.8.0/24).

----End

Verification

After the configuration is complete, test the network connectivity.

Ping the gateway (8.8.8.8) from the ECS in CN East-Shanghai1.



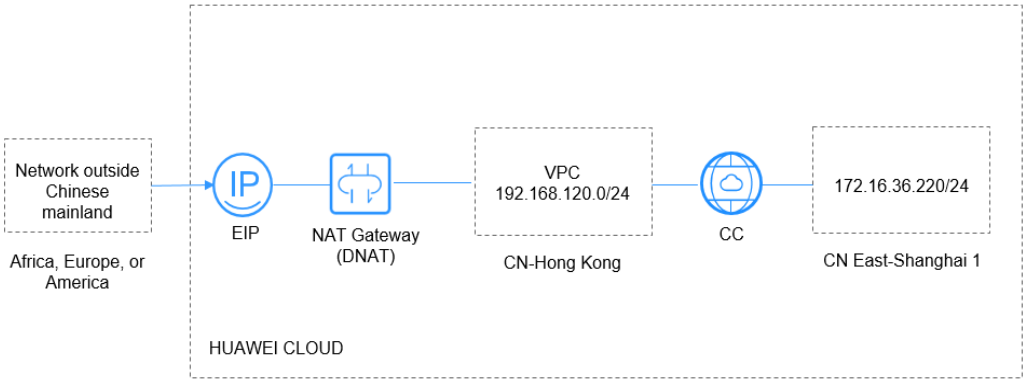
5 Working with DNAT to Access a Private Network from the Internet Outside China

Scenarios

- This practice provides detailed operations for allowing access to a private network from the Internet outside China.
- A DNAT rule is required so that ECSs in the VPCs in China can provide services accessible from the Internet.

Figure 5-1 shows the networking topology.

Figure 5-1 Networking



NOTE

In this practice, consider the VPC in CN East-Shanghai1 as the on-premises network.

The network outside China is 0.0.0.0/0.

Your account must have the permission for cross-border network communication. If you do not have the permission, you can authorize the other user to load the VPCs.

Procedure

Step 1 Create the following VPCs and ensure that the VPC CIDR blocks do not conflict with each other:

- VPC in CN East-Shanghai1: 172.16.36.0/24
- VPC in CN-Hong Kong: 192.168.120.0/24

For details, see **Creating a VPC**.

Step 2 Configure Cloud Connect.

1. Create a cloud connection.
   For details, see **Creating a Cloud Connection**.
2. Load the VPCs.
   For details, see **Loading a Network Instance**.
3. Add a custom CIDR block.
   For details, see **Adding a Custom CIDR block**.
   Custom CIDR block for CN-Hong Kong: 0.0.0.0/0

   NOTE

   You need to add the default route 0.0.0.0/0 from the cloud connection to the NAT gateway.
4. Buy a bandwidth package.
   By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions. You need to buy a bandwidth package to ensure normal network communications across regions.
   For details, see **Buying a Bandwidth Package**.
5. Assign an inter-region bandwidth.
   For details, see **Assigning Inter-Region Bandwidth**.

Step 3 Buy an ECS in CN East-Shanghai1.

For details, see **Purchasing an ECS**.

Private IP address of the ECS in CN East-Shanghai1: 172.16.36.220

Step 4 Buy an EIP and configure a NAT gateway.

Purchase an EIP in CN-Hong Kong, purchase a NAT gateway, and add a DNAT rule. (Select **Direct Connect/Cloud Connect** when you add the DNAT rule.)

For details, see **Assigning an EIP and Binding It to an ECS** and **Adding a DNAT Rule**.

Set the private IP address to 172.16.36.220 when you add the DNAT rule.

NOTE

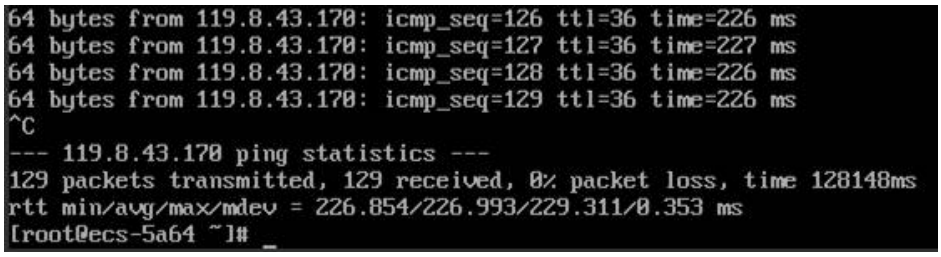
Configuring the DNAT rule enables the ECS to provide services accessible from the Internet.

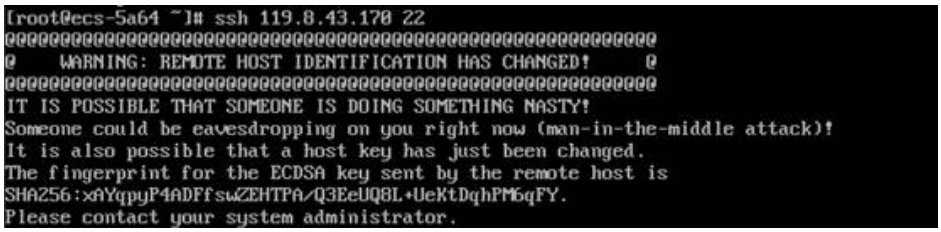
----End

Verification

After the configuration is complete, test the network connectivity and access the corresponding port.

Ping the EIP bound to the DNAT rule and the port used by the EIP from any client on the Internet.





6 Accelerating Access to a Website Across Regions

Scenarios

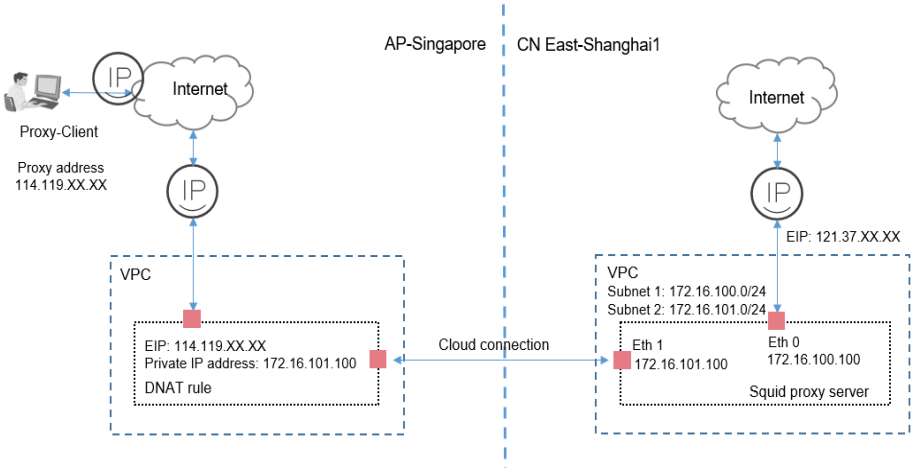
This practice provides detailed operations for accelerating access to a website across regions.

NOTE

Components required in this scenario include a NAT gateway, a cloud connection, and a web proxy server.

Figure 6-1 shows the networking topology.

Figure 6-1 Networking



NOTE

In this practice, an HTTP proxy server is used, such as a Squid proxy server, and it is only used for browser-based web access.

Proxy-Client: Use a Windows server with the web proxy installed as the client and set the proxy address to the EIP (114.119.xx.xx) in AP-Singapore.

NAT Gateway: Configure a DNAT rule to map the EIP (114.119.xx.xx) in AP-Singapore to the IP address (172.16.101.100) bound to the NIC (Eth 1) of the Squid proxy server in CN East-Shanghai1.

Prerequisites

- Your cross-border permit has been approved.
- You have deployed a proxy server based on your network conditions.

  NOTE

  In this practice, you need to configure the proxy server by yourself.

Procedure

Step 1 Create two VPCs and ensure that the VPC CIDR blocks do not conflict with each other.

For details, see **Creating a VPC**.

Add two subnets to the VPC in CN East-Shanghai1.

- Subnet 1: 172.16.100.0/24
- Subnet 2: 172.16.101.0/24

Step 2 Configure Cloud Connect.

Create a cloud connection, load the VPCs, and add a custom CIDR block.

1. Create a cloud connection.

   For details, see **Creating a Cloud Connection**.
2. Load the VPCs.

   When you load the VPC in CN East-Shanghai1, select only subnet 2.

   For details, see **Loading a Network Instance**.
3. Add a custom CIDR block.

   Add a custom CIDR block 0.0.0.0/0 for the VPC in AP-Singapore.

   For details, see **Adding a Custom CIDR block**.

   NOTE

   You need to add the default route 0.0.0.0/0 from the cloud connection to the NAT gateway.
4. Buy a bandwidth package.

   By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions. You need to buy a bandwidth package to ensure normal network communications across regions.

   For details, see **Buying a Bandwidth Package**.

5. Assign an inter-region bandwidth.

   For details, see **Assigning Inter-Region Bandwidth**.

Step 3 Buy an ECS with two NICs in CN East-Shanghai1.

- Eth 0: 172.16.100.100
- Eth 1: 172.16.101.100

For details, see **Purchasing an ECS**.

NOTE

Bind an EIP to Eth 0 so that the ECS can access the Internet.

Step 4 Configure Squid on the ECS.

1. To ensure normal routing, add a policy-based route for the ECS in CN East-Shanghai1.

```
ip rule add from 172.16.101.100 table 100
ip route add default via 172.16.101.1 table 100
```

2. Install and configure Squid on the ECS in a secure and reliable manner based on your network requirements.

Step 5 Buy two EIPs and configure a NAT gateway.

1. Buy an EIP in CN East-Shanghai1 and bind the EIP to Eth 0 (172.16.100.100).

   For details, see **Assigning an EIP and Binding It to an ECS**.

2. Buy an EIP in AP-Singapore, purchase a NAT gateway, and add a DNAT rule. (Select **Direct Connect/Cloud Connect** when you add the DNAT rule.)

   For details, see **Assigning an EIP and Binding It to an ECS** and **Adding a DNAT Rule**.

NOTE

Private IP address: IP address (172.16.101.100) of the Eth 1

EIP: EIP (114.119.XX.XX) used by Proxy-Client

Squid proxy server: Eth 0 is used for Internet access, and Eth 1 is used for DNAT mapping.

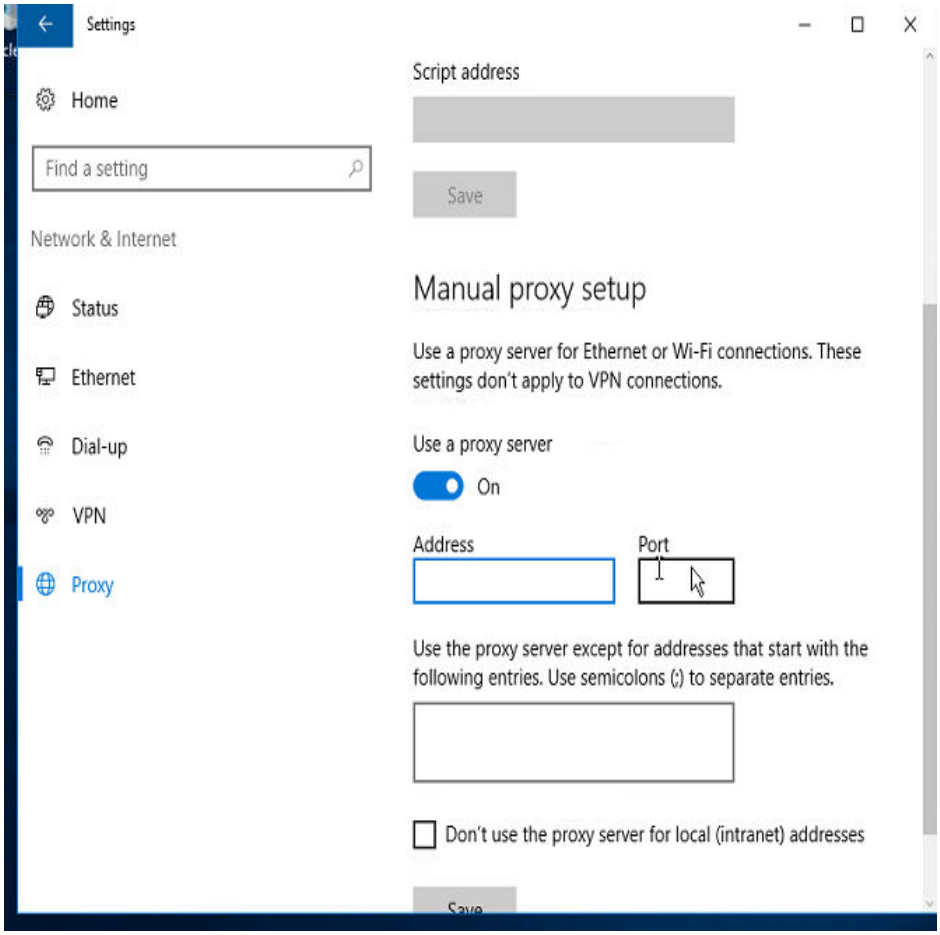
Configuring the DNAT rule enables the squid proxy server in the VPC to provide services accessible from the Internet. The proxy client allows access to the services provided by the Squid proxy server.

Step 6 Configure Proxy-Client.

Prepare a Windows server and configure it as the client.

1. Select **Settings**.
2. Choose **Network and Internet** > **Proxy** > **Manual proxy setup**.
3. Enable **Use a proxy server**.
4. Set **Address** and **Port**.

Figure 6-2 Proxy configuration



NOTE

Address: Enter the EIP (114.119.XX.XX) bound to the DNAT rule.

5. Click **Save**.

----End

Verification

After the configuration is complete, access the website from Proxy-Client to check whether access is normal.

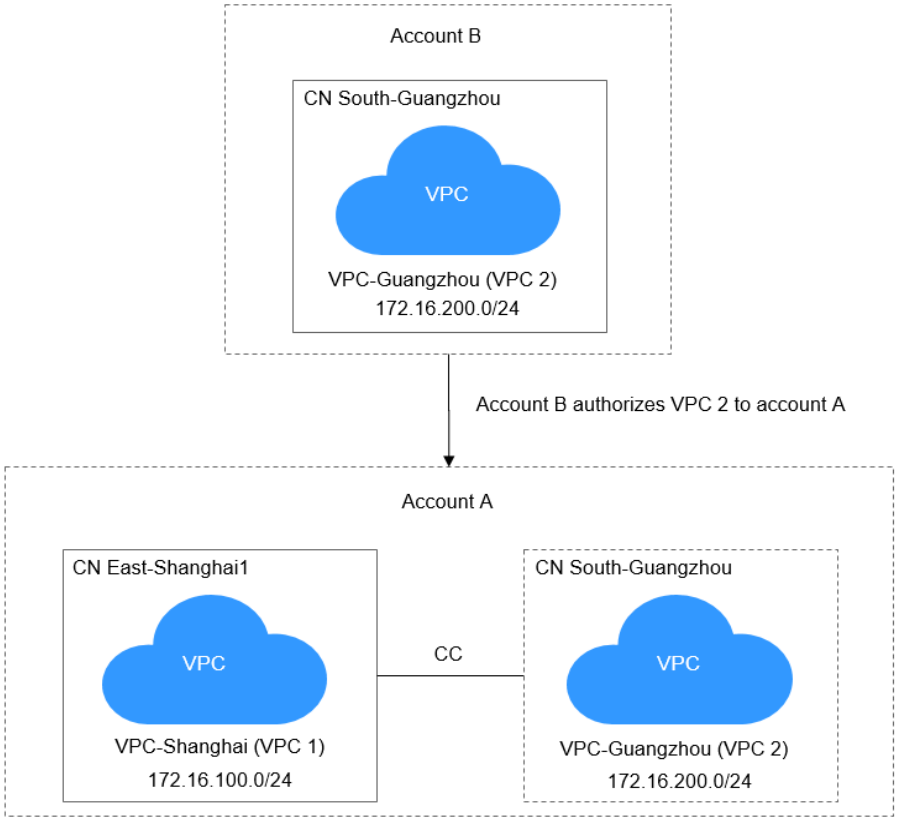
7 Authorizing Network Instances Across Accounts

Scenarios

Cloud Connect enables you to load the VPCs of other users to your own cloud connections so that your VPCs can communicate with those of other users.

Figure 7-1 shows the networking topology.

Figure 7-1 Networking



NOTE

- Account A: This is your account. You need to create a cloud connection, ask account B to authorize VPC 2 to you, and load VPC 2 to your cloud connection.
- Account B: authorizes VPC 2 to you.

  If multiple VPCs in different regions under account B need to communicate with each other, you can ask account B to authorize all these VPCs to you.
- After account B authorizes VPC 2, you can load VPC 1 and VPC 2 to your cloud connection so that the two VPCs can communicate with each other. Account B does not need to create a cloud connection, purchase a bandwidth package, or configure an inter-region bandwidth.

Prerequisites

You have the permissions of **Tenant Guest**, **VPC Administrator**, and **Cross Connect Administrator** in the region where the authorized VPC resides.

In this scenario, account A must have the permissions of the preceding roles in the CN South-Guangzhou region where VPC 2 of account B resides.

For details, see **Permission Management**.

Procedure

Step 1 Create a VPC using account A, create another VPC using account B, and ensure that CIDR blocks of the two VPCs do not conflict with each other.

Account A VPC: 172.16.100.0/24

Account B VPC: 172.16.200.0/24

For details, see **Creating a VPC**.

Step 2 Create a cloud connection using your account.

For details, see **Creating a Cloud Connection**.

Step 3 Ask account B to authorize VPC 2 to your account.

For details, see **Authorizing a Network Instance**.

Step 4 Load the two VPCs to your cloud connection.

Load VPC 2 of account B. For details, see **Loading Network Instances of Others**.

Load VPC 1. For details, see **Loading a Network Instance**.

Step 5 Buy a bandwidth package using your account and bind it to your cloud connection.

For details, see **Purchasing a Bandwidth Package**.

Step 6 Assign inter-region bandwidths using your account.

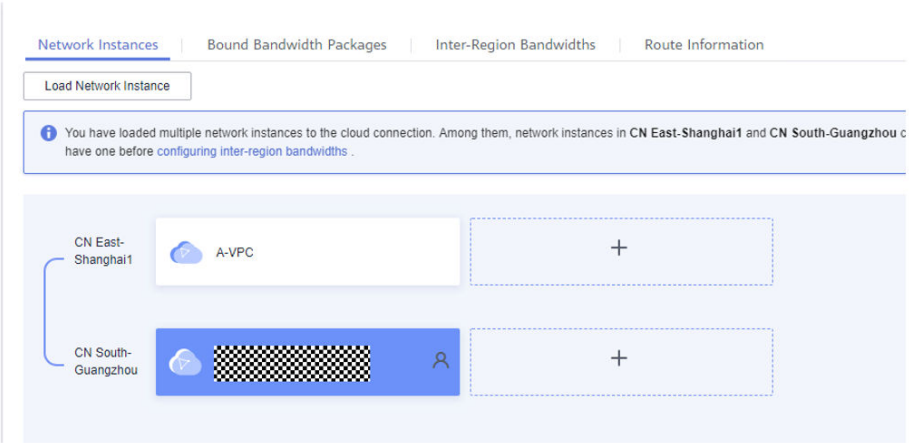
For details, see **Assigning Inter-Region Bandwidth**.

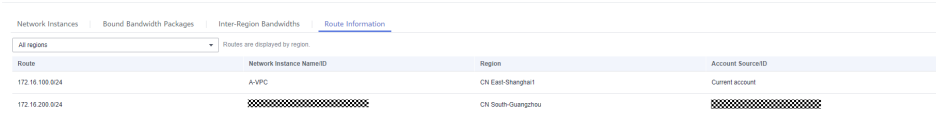
----End

Verification

View the routes of the cloud connection and verify that network communications between the VPCs are normal.

For details, see **Viewing Route Information**.





8 Connecting VPCs of the Same Type in Different Regions by Using Cloud Connect and VPC Peering

Scenarios

This practice provides detailed operations for combining VPC Peering and Cloud Connect to enable communications between VPCs of the same service in different regions.

As shown in the following figure, there are three VPCs in CN East-Shanghai1 and CN South-Guangzhou, respectively. The three VPCs in each region are a production VPC, an office VPC, and a transit VPC, and they need to be connected as follows:

- The production VPC in CN East-Shanghai1 communicates with the production VPC in CN South-Guangzhou.
- The office VPC in CN East-Shanghai1 communicates with the office VPC in CN South-Guangzhou.
- The production VPCs and the office VPC cannot communicate with each other.

Figure 8-1 Networking diagram

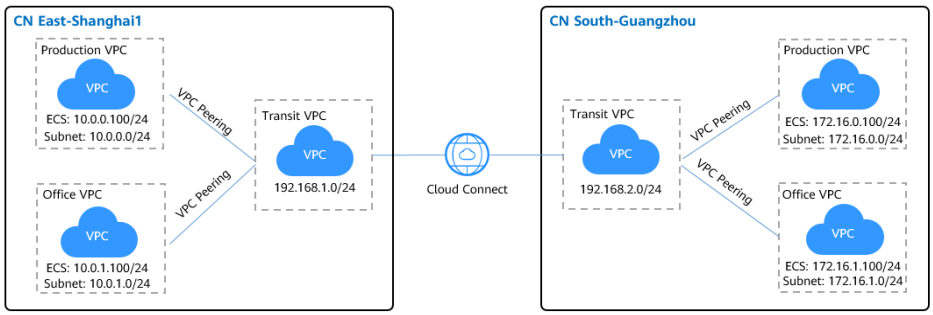


Table 8-1 Service configuration

Cloud Service	Scenario	Description	Related Operations
VPC Peering	Two VPCs are in the same region.	Create a VPC peering connection to connect two VPCs in the same region. The two VPCs can be in your account or in different accounts.	**Creating a VPC Peering Connection to Connect Another VPC in Your Account** **Creating a VPC Peering Connection to Connect a VPC in Another Account**
Cloud Connect	VPCs are in different regions.	Connect a cloud connection to connect the VPCs across regions. The VPCs can be in the same account or in different accounts.	**Communications Between VPCs Across Regions**

CAUTION

To connect the VPCs using Cloud Connect and VPC Peering, ensure that the subnets in the VPCs do not overlap or conflict.

Prerequisites

- You have registered a HUAWEI CLOUD account and completed real-name authentication.
- Your account balance is sufficient to purchase the required resources, including bandwidth packages and ECSs.
- You have created the VPCs and subnets that need to communicate with each other.

Procedure

Step 1 Configure VPC Peering.

1. **Create a VPC peering connection.**
   a. Log in to the management console.
   b. Click  in the upper left corner to select a region and a project.
   c. Hover on  to display **Service List** and choose **Networking** > **Virtual Private Cloud**.
   d. In the navigation pane on the left, choose **VPC Peering**.
   e. In the upper right corner, click **Create VPC Peering Connection**.
   f. Configure the parameters based on **Table 8-2**. Select **My account** for **Account**.

Figure 8-2 Creating a VPC peering connection

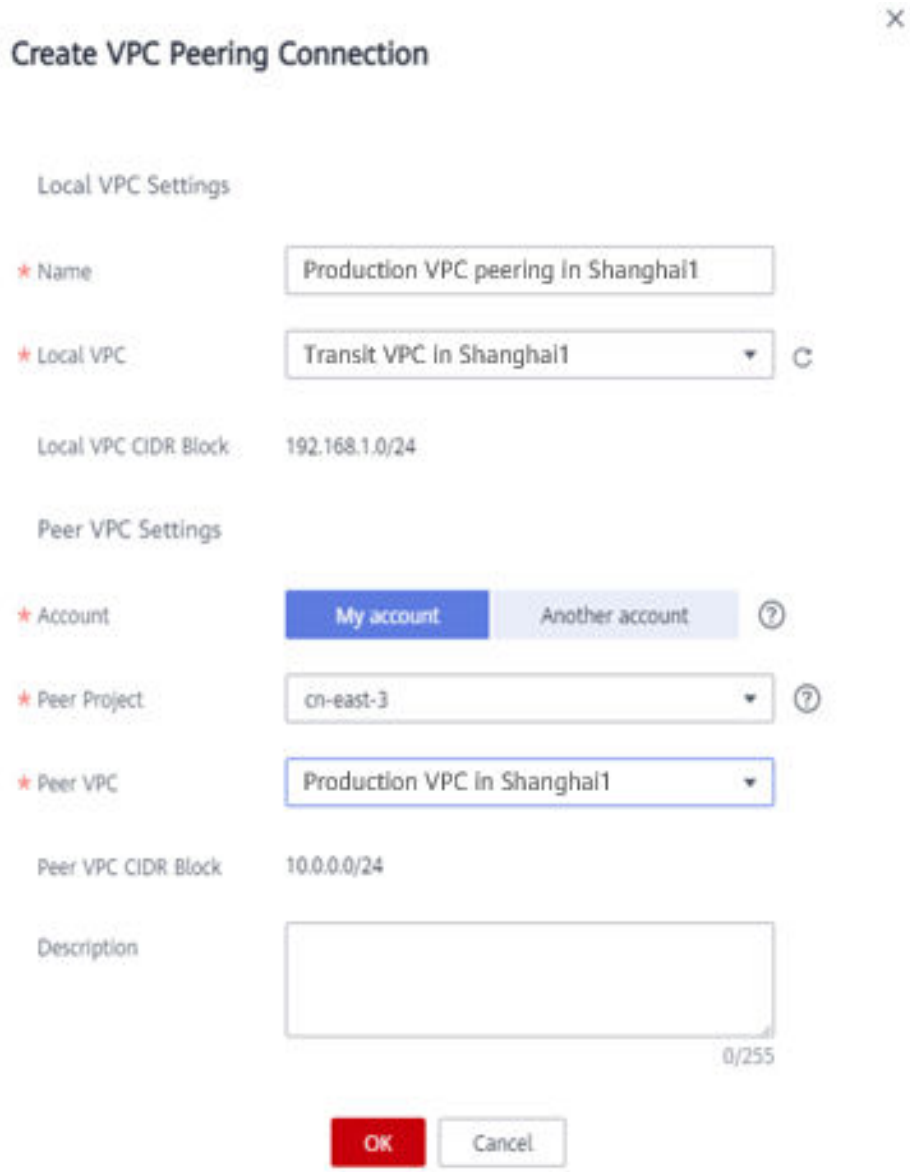


Table 8-2 Parameter description

Parameter	Description	Example Value
Name	Specifies the name of the VPC peering connection. The name contains a maximum of 64 characters, which consist of letters, digits, hyphens (-), and underscores (_).	Production VPC peering in Shanghai1

Parameter	Description	Example Value
Local VPC	Specifies one VPC you want to connect over the VPC peering connection. You can select one from the drop-down list.	Transit VPC in Shanghai1
Local VPC CIDR Block	Specifies the CIDR block for the local VPC.	192.168.1.0/24
Account	Specifies the account that owns the peer VPC. – **My account**: The VPC peering connection will be created between two VPCs, in the same region, in your account. – **Another account**: The VPC peering connection will be created between your VPC and a VPC in another account, in the same region.	My account
Peer Project	Specifies the peer project name. The project name of the current project is used by default.	cn-east-3
Peer VPC	Specifies another VPC you want to connect over the VPC peering connection. You can select one from the drop-down list if the VPC peering connection is created between two VPCs in your own account.	Production VPC in Shanghai1
Peer VPC CIDR Block	Specifies the CIDR block for the peer VPC. The local and peer VPCs cannot have matching or overlapping CIDR blocks. Otherwise, the routes added for the VPC peering connection may not take effect.	10.0.0.0/24
Description	(Optional) Provides supplementary information about the VPC peering connection. The description can contain a maximum of 255 characters and cannot contain angle brackets (<>).	-

g. Click **OK**.

2. **Add routes for the VPC peering connection.**

   If you request a VPC peering connection with another VPC in your own account, the system automatically accepts the request. However, to enable

communications between the two VPCs, you need to add local and peer routes on the **Route Tables** page for the VPC peering connection.

a. Log in to the management console.

b. Click  in the upper left corner to select a region and a project.

c. Hover on  to display **Service List** and choose **Networking** > **Virtual Private Cloud**.

d. In the navigation pane on the left, choose **Route Tables**.

e. Search for or create a route table for the local VPC and add the local route. **Table 8-3** describes the parameters.

Figure 8-3 Adding local route

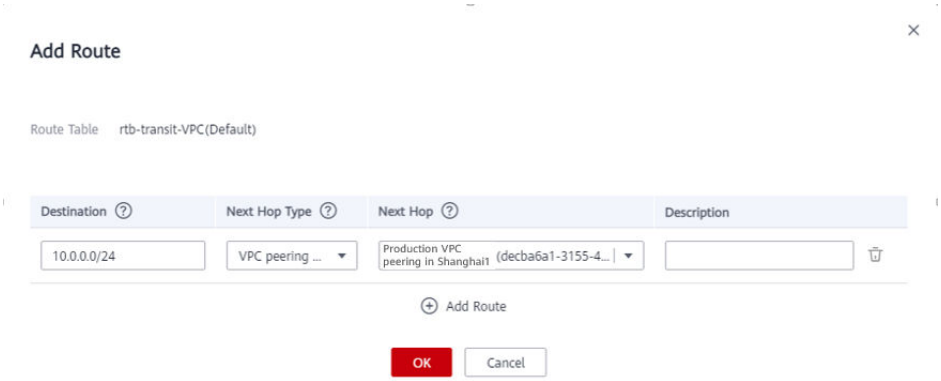


Table 8-3 Parameter description

Parameter	Description	Example Value
Destination	Specifies the CIDR block for the peer VPC.	10.0.0.0/24
Next Hop Type	Specifies the next hop type. Select **VPC peering connection**.	VPC peering connection
Next Hop	Specifies the next hop address. Select the name of the current VPC peering connection.	Production VPC peering in Shanghai1
Description	(Optional) Provides supplementary information about the route. The description can contain a maximum of 255 characters and cannot contain angle brackets (<>).	-

f. Search for or create a route table for the peer VPC and add the peer route.

Figure 8-4 Adding peer route

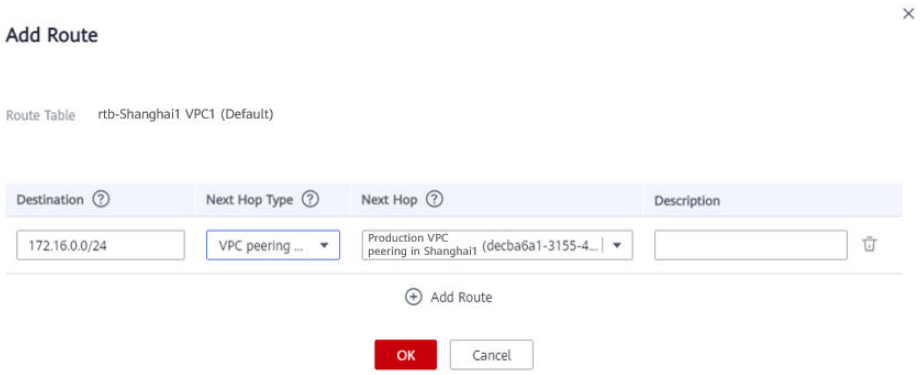


Table 8-4 Parameter description

Parameter	Description	Example Value
Destination	Specifies the CIDR block for the peer VPC.	172.16.0.0/24
Next Hop Type	Specifies the next hop type. Select **VPC peering connection**.	VPC peering connection
Next Hop	Specifies the next hop address. Select the current VPC peering connection.	Production VPC peering in Shanghai1
Description	(Optional) Provides supplementary information about the route. The description can contain a maximum of 255 characters and cannot contain angle brackets (<>).	-

g. Repeat the above steps to create a VPC peering connection between the office VPC and the transit VPC in CN East-Shanghai1 and add local and peer routes.

NOTE

Repeat the above operations to create two VPC peering connections in CN South-Guangzhou, with one connecting the production VPC to the transit VPC and the other connecting the office VPC to the transit VPC.

In the above steps, you can visit the route table module directly from the navigation pane on the left.

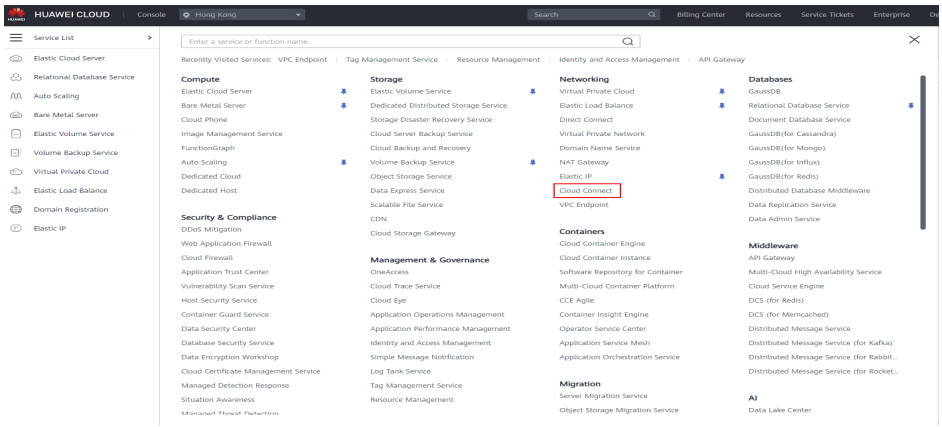
Step 2 Configure Cloud Connect.

1. **Create a cloud connection.**

   a. Log in to the management console.

   b. Hover on ☰ to display **Service List** and choose **Networking** > **Cloud Connect**.

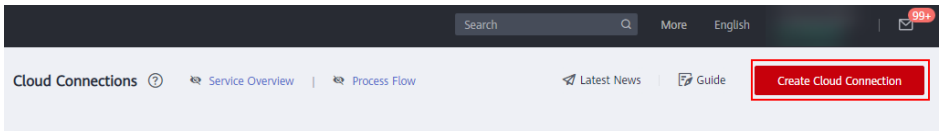
Figure 8-5 Cloud Connect



c. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.

d. On the displayed page, click **Create Cloud Connection**.

Figure 8-6 Create Cloud Connection



e. Configure the parameters based on **Table 8-5**.

Table 8-5 Parameter description

Parameter	Description	Example Value
Name	Specifies the cloud connection name. The name can contain 1 to 64 characters, including letters, digits, underscores (_), hyphens (-), and periods (.).	CloudConnect
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default
Description	Provides supplementary information about the cloud connection. The description can contain a maximum of 255 characters.	A Cloud Connect instance for demo

f. Click **OK**.

2. **Load network instances.**

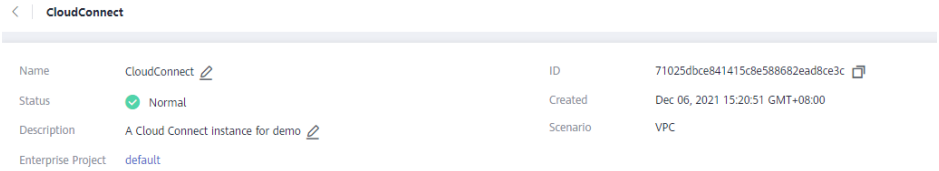
   Load the transit VPC in CN East-Shanghai1 to the created cloud connection.

a. In the cloud connection list, click the cloud connection named **CloudConnect**.

NOTE

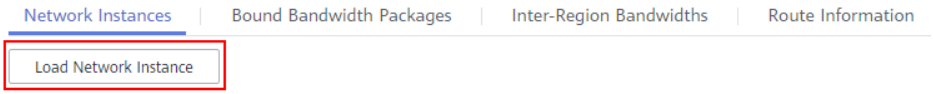
On the displayed page, you can view details about the cloud connection, such as its name, ID, status, time when the cloud connection was created, and description. There are also four tabs: **Network Instances**, **Bound Bandwidth Packages**, **Inter-Region Bandwidths**, and **Route Information**.

Figure 8-7 Cloud connection details



b. Under **Network Instances**, click **Load Network Instance**.

Figure 8-8 Load Network Instance



c. Configure the parameters.

Figure 8-9 Loading a network instance

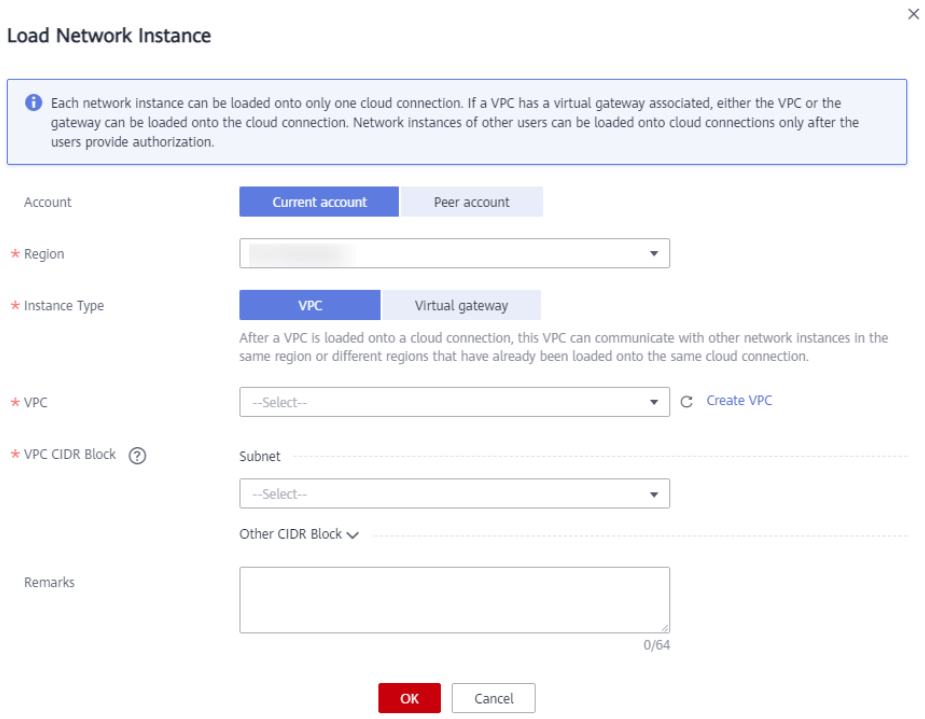
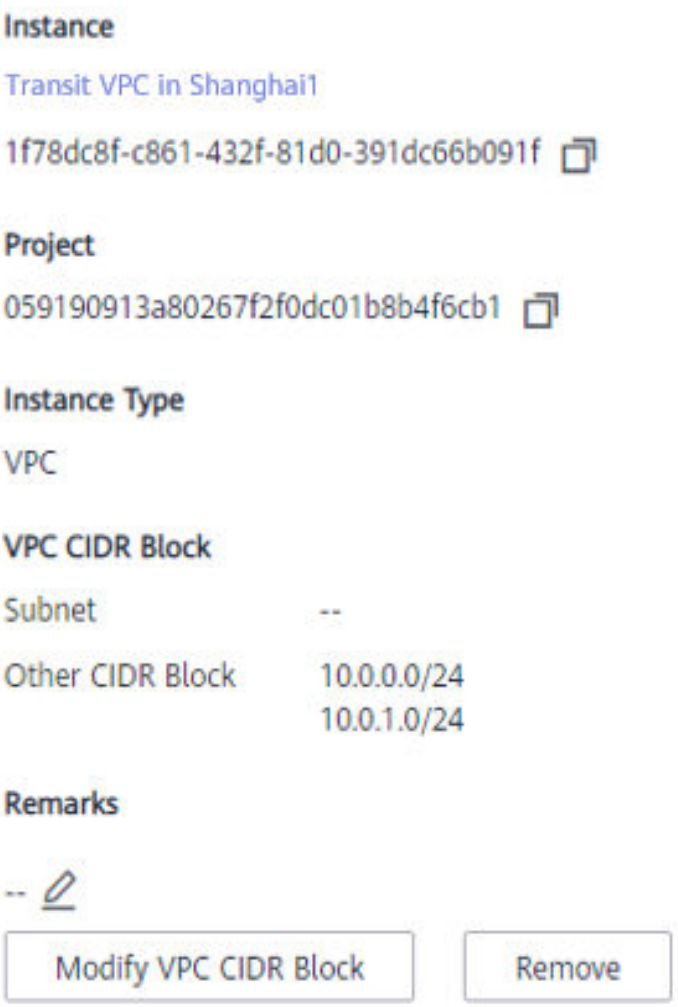


Figure 8-10 Network instance details



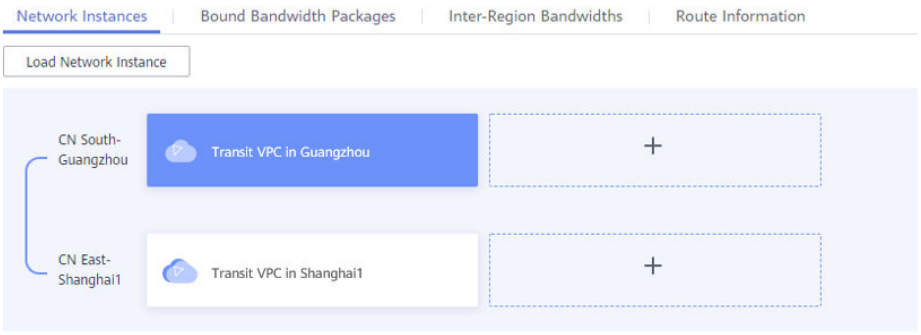
NOTE

To communicate with the production VPC and the office VPC in CN East-Shanghai1, you need to set the CIDR blocks of the two VPCs as custom CIDR blocks.

d. Click **OK**.

e. Repeat the above steps to load the transit VPC in CN South-Guangzhou to the cloud connection and set the CIDR block of the production VPC and the CIDR block of the office VPC in CN South-Guangzhou as custom CIDR blocks.

Figure 8-11 Loading another VPC



NOTE

After the VPCs are loaded, they are on the same network, and you can view the routes of each VPC on the **Route Information** tab page.

3. **Buy a bandwidth package.**

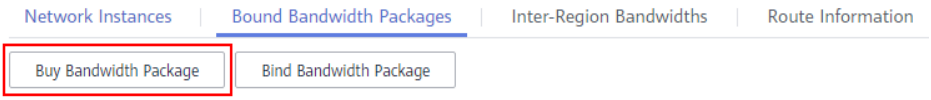
   By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions.

   To ensure normal network communications, you need to purchase a bandwidth package and bind the package to the cloud connection.

   a. In the cloud connection list, click the cloud connection named **CloudConnect**.

   b. On the details page of the cloud connection, click **Bound Bandwidth Packages** and then **Buy Bandwidth Package**.

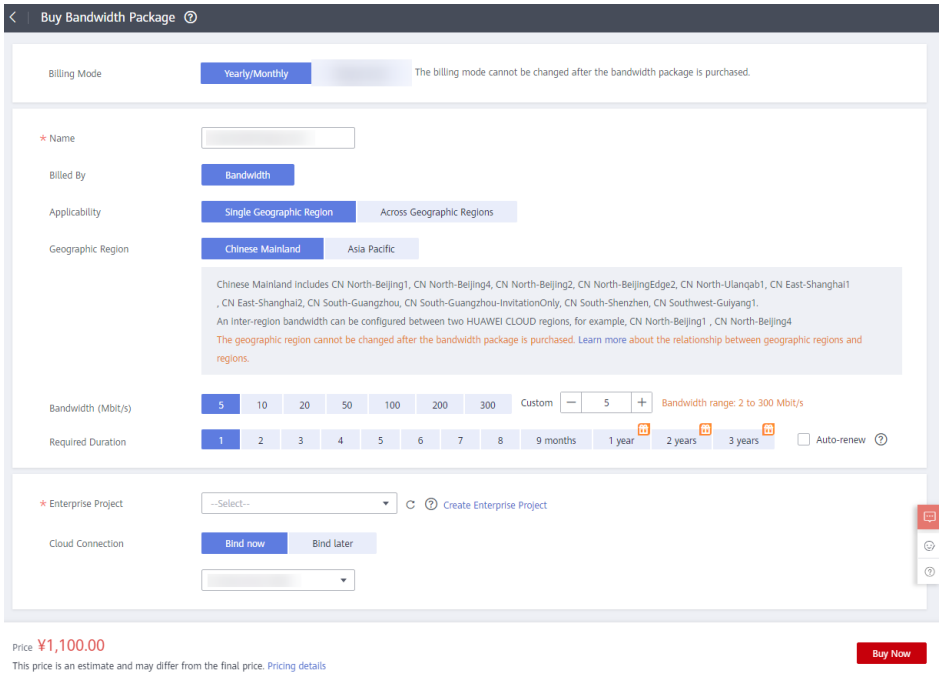
   Figure 8-12 Buy Bandwidth Package

   c. Configure the parameters.

   Because the two VPCs are in the Chinese mainland, select **Single Geographic Region** for **Applicability** and **Chinese mainland** for **Geographic Region**.

Figure 8-13 Buying a bandwidth package



d. Click **Buy Now**.

e. Confirm the information and click **Pay Now**.

f. Click **Pay**.

Go back to the bandwidth package list and locate the bandwidth package. If its status changes to **Normal**, you can bind the bandwidth package to a cloud connection.

NOTE

On the **Bandwidth Packages** page, you can view the purchased bandwidth package and its details, including the billing mode, order information, the cloud connection it is bound to, used bandwidth, and remaining bandwidth. You can also modify, unbind, renew, and unsubscribe from the bandwidth package.

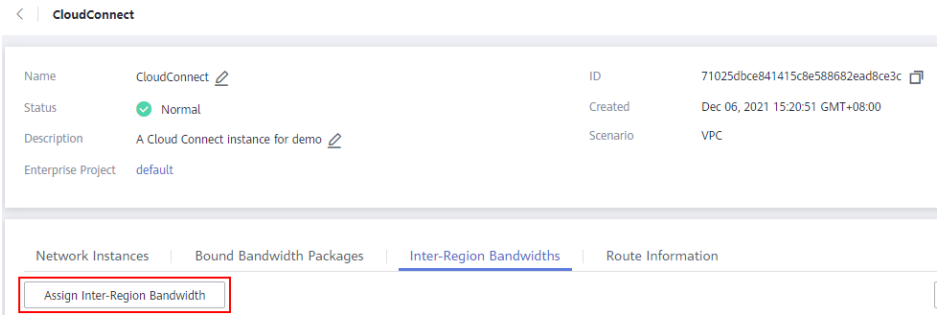
4. **Assign inter-region bandwidth.**

Assign bandwidth from the purchased bandwidth package for network communications between the VPCs.

a. In the cloud connection list, click the cloud connection named **CloudConnect**.

b. On the details page of the cloud connection, click **Inter-Region Bandwidths** and then **Assign Inter-Region Bandwidth**.

Figure 8-14 Assigning inter-region bandwidth



c. Configure the parameters.

Select **CN South-Guangzhou** and **CN East-Shanghai1** for **Regions**. The system automatically displays the bandwidth package bound to the cloud connection. Set the bandwidth based on your requirements, for example, 1 Mbit/s.

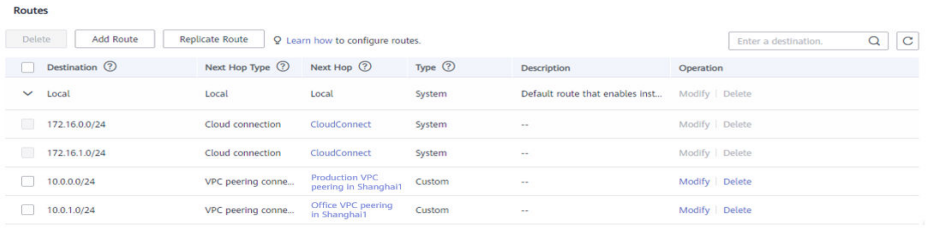
d. View the assigned bandwidth on the **Inter-Region Bandwidths** tab page.

----End

Verification

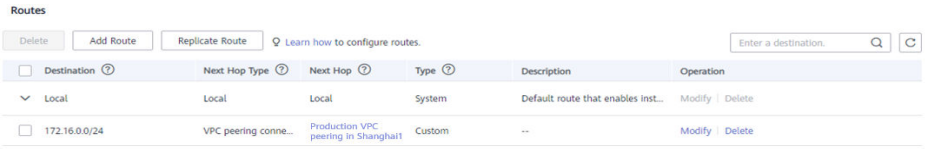
- Check the route table of the transit VPC in CN East-Shanghai1.

Figure 8-15 Route table of the transit VPC in CN East-Shanghai1



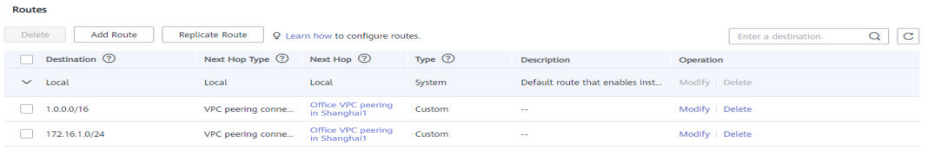
- Check the route table of the production VPC in CN East-Shanghai1.

Figure 8-16 Route table of the production VPC in CN East-Shanghai1



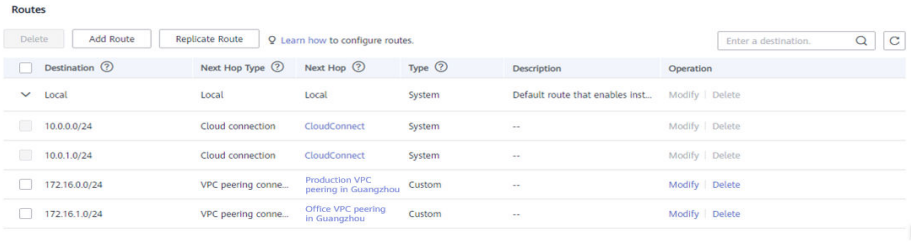
- Check the route table of the office VPC in CN East-Shanghai1.

Figure 8-17 Route table of the office VPC in CN East-Shanghai1



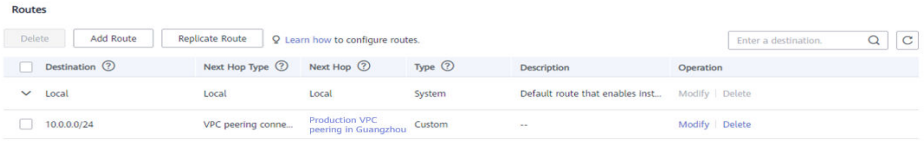
- Check the route table of the transit VPC in CN South-Guangzhou.

Figure 8-18 Route table of the transit VPC in CN South-Guangzhou



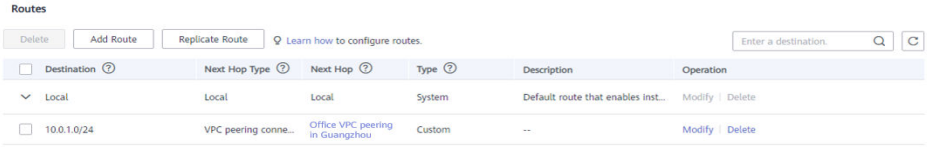
- Check the route table of the production VPC in CN South-Guangzhou.

  Figure 8-19 Route table of the production VPC in CN South-Guangzhou



- Check the route table of the office VPC in CN South-Guangzhou.

  Figure 8-20 Route table of the office VPC in CN South-Guangzhou



- Ping an ECS in the production VPC in CN South-Guangzhou from an ECS in the production VPC in CN East-Shanghai1.

  Figure 8-21 Pinging two ECSs

```
[root@vpc1-ecs ~]# ping 172.16.0.100
PING 172.16.0.100 (172.16.0.100) 56(84) bytes of data.
64 bytes from 172.16.0.100: icmp_seq=2 ttl=61 time=36.7 ms
64 bytes from 172.16.0.100: icmp_seq=3 ttl=61 time=33.3 ms
64 bytes from 172.16.0.100: icmp_seq=4 ttl=61 time=33.2 ms
64 bytes from 172.16.0.100: icmp_seq=5 ttl=61 time=33.2 ms
64 bytes from 172.16.0.100: icmp_seq=6 ttl=61 time=33.1 ms
^C
--- 172.16.0.100 ping statistics ---
6 packets transmitted, 5 received, 16.6667% packet loss, time 13ms
rtt min/avg/max/mdev = 33.130/33.894/36.679/1.402 ms
[root@vpc1-ecs ~]# _
```

- Ping an ECS in the office VPC in CN South-Guangzhou from an ECS in the office VPC in CN East-Shanghai1.

Figure 8-22 Pinging two ECSs

```
[root@ecs ~]# ping 10.0.1.100
PING 10.0.1.100 (10.0.1.100) 56(84) bytes of data.
64 bytes from 10.0.1.100: icmp_seq=1 ttl=62 time=32.1 ms
64 bytes from 10.0.1.100: icmp_seq=2 ttl=62 time=31.10 ms
64 bytes from 10.0.1.100: icmp_seq=3 ttl=62 time=31.10 ms
64 bytes from 10.0.1.100: icmp_seq=4 ttl=62 time=31.10 ms
64 bytes from 10.0.1.100: icmp_seq=5 ttl=62 time=31.9 ms
64 bytes from 10.0.1.100: icmp_seq=6 ttl=62 time=31.9 ms
```

