Cloud Connect

Best Practices

Issue 01

Date 2025-01-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

1 Connecting VPCs in the Same Region But in Different Accounts

1.1 Using a Cloud Connection to Connect VPCs in the Same Region But Different Accounts

Process Description

If you want to connect the VPCs in your account to those in another account, you can create a cloud connection, request permission from the other account to use their VPCs, and load all the VPCs to your cloud connection.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

Figure 1-1 How a cloud connection enables VPCs in the same region but different accounts to communicate with each other

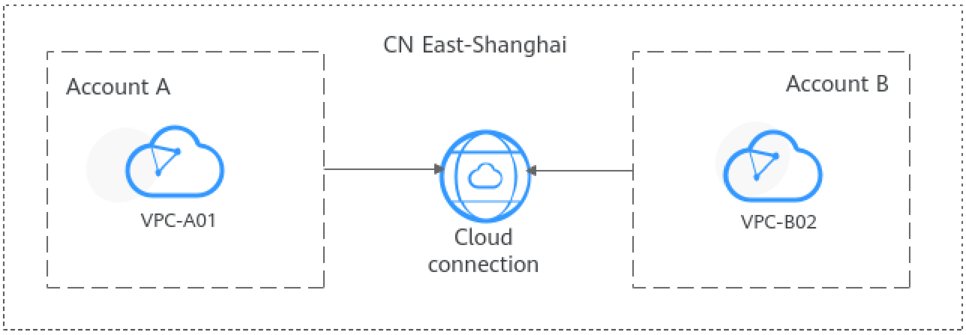
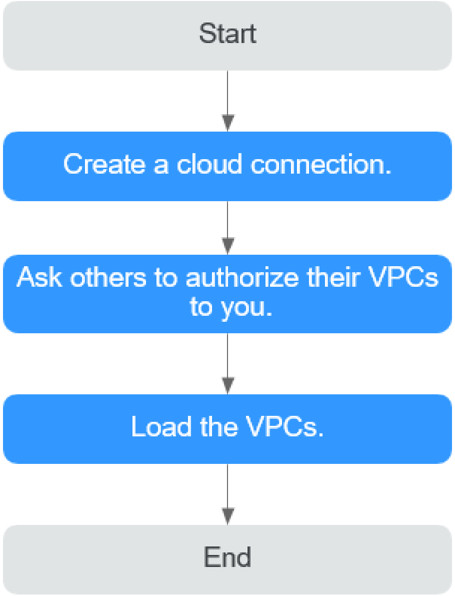


Figure 1-2 illustrates how you can enable VPCs in the same region but in different accounts to communicate with each other using a cloud connection.

Figure 1-2 Process of enabling communication between VPCs


Start
Create a cloud connection.
Ask others to authorize their VPCs to you.
Load the VPCs.
End

Preparations

Before creating a cloud connection, you need to sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account. Ensure that your account has sufficient balance.

1. Sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication.

   If you already have a HUAWEI ID, skip this part. If you do not have a HUAWEI ID, perform the following operations to create one:

   a. **Sign up for a HUAWEI ID and enable Huawei Cloud services**.

   b. Complete **real-name authentication**.

2. Top up your account.

   Ensure that your account has sufficient balance. For details about how to top up an account, see **Topping up an Account**.

Step 1: Create a Cloud Connection

Step 1 Go to the **Cloud Connections** page.

Step 2 In the upper right corner of the page, click **Create Cloud Connection**.

Step 3 Configure the parameters based on **Table 1-1**.

Table 1-1 Parameters for creating a cloud connection

Parameter	Example Value	Description
Name		Specifies the cloud connection name. The name can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Enterprise Project		Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.
Scenario		**VPC**: VPCs or virtual gateways can use this cloud connection.
Tag		Identifies the cloud connection. A tag consists of a key and a value. You can add 20 tags to a cloud connection. **NOTE** If a predefined tag has been created on Tag Management Service (TMS), you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tags**.
Description		Provides supplementary information about the cloud connection. The description can contain no more than 255 characters.

Step 4 Click **OK**.

----End

Step 2: Request Permission to Use the VPC in the Other Account

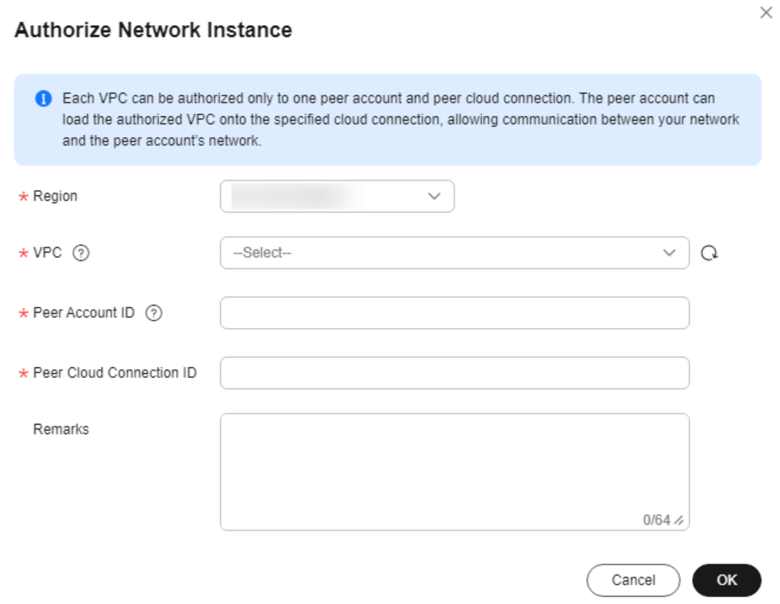
In this example, the two VPCs are in different accounts. If the VPC in your account (account A) needs to communicate with that in the other account (account B), ask this other account to grant you the permission to load their VPC to your cloud connection. This other account can take the following steps to grant you the permission to load their VPC:

Step 1 Go to the **Cross-Account Authorization** page.

Step 2 On the **Network Instances Authorized by Me** tab, click **Authorize Network Instance**.

Step 3 Configure the parameters based on **Table 1-2**.

Figure 1-3 Cross-account authorization



Authorize Network Instance

Each VPC can be authorized only to one peer account and peer cloud connection. The peer account can load the authorized VPC onto the specified cloud connection, allowing communication between your network and the peer account's network.

* Region

* VPC: --Select--

* Peer Account ID

* Peer Cloud Connection ID

Remarks: 0/64

Table 1-2 Parameters for the other account to grant you the permission to load their VPC to your cloud connection

Parameter	Description
Region	Specifies the region where the VPC is located.
VPC	Specifies the VPC to be loaded to your cloud connection.
Peer Account ID	Specifies the ID of your account.
Peer Cloud Connection ID	Specifies the ID of your cloud connection that the VPC is to be loaded to.
Remarks	Provides supplementary information about cross-account authorization.

Step 4 Click **OK**.

----End

Step 3: Load Network Instances

Load the VPCs that need to communicate with each other to the cloud connection you have created. To load the VPC in the other account, take the following steps:

Step 1 Go to the **Cloud Connections** page.

Step 2 Click the name of the cloud connection to go to the **Basic Information** page.

Step 3 Click the **Network Instances** tab.

Step 4 Click **Load Network Instance**. In the displayed dialog, select **Peer account**.

Configure other parameters based on **Table 1-3** and click **OK**.

Table 1-3 Parameters for loading network instances across accounts

Parameter	Description
Account	Specifies the account that provides the network instance. Select **Peer account**.
Peer Account ID	Specifies the ID of the other account.
Region	Specifies the region where the VPC you want to connect is located.
Peer Project ID	Specifies the project ID of the VPC in the other account.
Instance Type	VPC Specifies the type of the network instance that needs to be loaded to the cloud connection.
Peer VPC	Specifies the VPC to be loaded.
VPC CIDR Block	Specifies the subnets in the VPC you want to load and custom CIDR blocks.
Remarks	Provides supplementary information about the network instance.

NOTE

- A network instance can only be loaded to one cloud connection.
- If a VPC is loaded, the associated virtual gateway cannot be loaded.

Step 5 Click **Continue Loading** if you need to load another network instance. If you do not need to load another network instance now, close the dialog box and view the loaded network instance on the **Network Instances** tab.

----End

2 Connecting VPCs in Different Regions and Accounts

2.1 Using a Cloud Connection to Connect VPCs in Different Regions and Accounts

Process Description

If you want to connect VPCs in your account to those in another account, you can create a cloud connection, request this other account to allow you to load their VPCs to your cloud connection. Then, purchase a bandwidth package and assign bandwidth between regions so that VPCs in these regions can communicate with each other.

If a VPC is outside the Chinese mainland and other VPCs are inside the Chinese mainland, you need to apply for a cross-border permit before you purchase bandwidth packages.

Figure 2-1 shows an example.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

Figure 2-1 How a cloud connection enables VPCs in different accounts and regions to communicate with each other

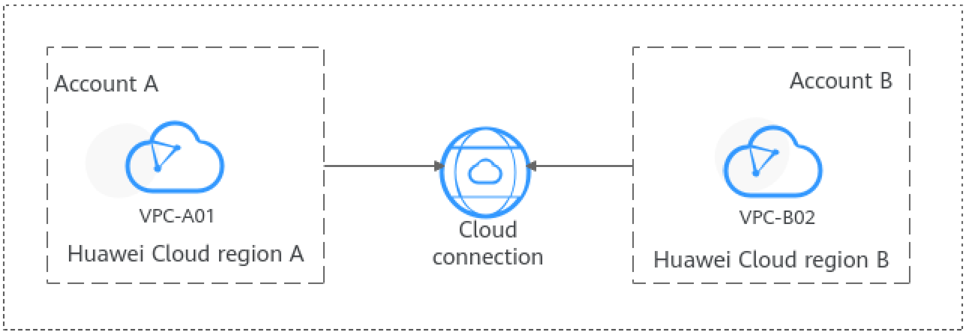
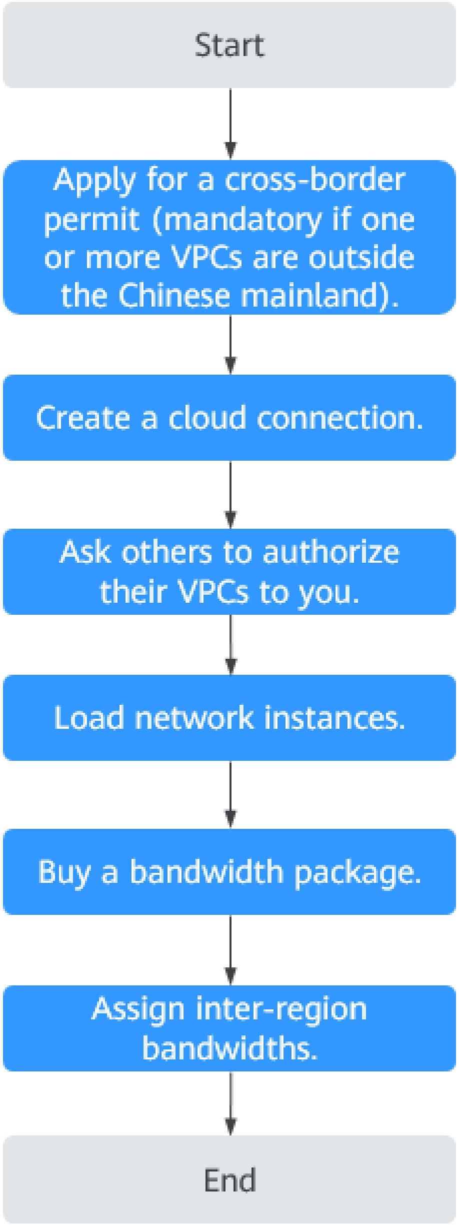


Figure 2-2 illustrates how you can enable communication among VPCs that are in different accounts and regions.

Figure 2-2 Process of enabling communication between VPCs


Start
Apply for a cross-border permit (mandatory if one or more VPCs are outside the Chinese mainland).
Create a cloud connection.
Ask others to authorize their VPCs to you.
Load network instances.
Buy a bandwidth package.
Assign inter-region bandwidths.
End

Preparations

Before creating a cloud connection, you need to sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account. Ensure that your account has sufficient balance.

1. Sign up for a HUAWEI ID, enable Huawei Cloud services, and complete real-name authentication.

   If you already have a HUAWEI ID, skip this part. If you do not have a HUAWEI ID, perform the following operations to create one:

   a. **Sign up for a HUAWEI ID and enable Huawei Cloud services**.

   b. Complete **real-name authentication**.

2. Top up your account.

   Ensure that your account has sufficient balance. For details about how to top up an account, see **Topping up an Account**.

Step 1: Apply for a Cross-Border Permit

If a VPC you want to connect is outside the Chinese mainland, you need to apply for a cross-border permit.

Skip this step if cross-border communication is not required.

Step 1 Go to the **Bandwidth Packages** page.

Step 2 On the displayed page, click **apply now**.

If the registered address of your business entity is in the Chinese mainland, click **here** to go to the **Cross-Border Service Application System** page.

If the registered address of your business entity is outside the Chinese mainland, click **here** to go to the **Cross-Border Service Application System** page.

NOTE

Select the address for applying for the cross-border permit based on the registration address of your business entity.

Step 3 On the displayed page, select an applicant type, configure the parameters as prompted, and upload the required materials.

NOTICE

Prepare and upload the materials required on the application page.

Table 2-1 Online cross-border permit application

Parameter	Description
Applicant Name	This name must be the same as the company name in the *Letter of Commitment to Information Security*.
Huawei Cloud UID	The account ID to log in to the management console. You can take the following steps to obtain your account ID. 1. Log in to the management console. 2. Click the username in the upper right corner and select **My Credentials** from the drop-down list. 3. On the **API Credentials** page, view the **Account ID**.
Bandwidth (Mbit/s)	For reference only

Parameter	Description
Start Date	For reference only
Termination Date	For reference only
Customer Type	Select a type based on the actual situation.
Country of the Customer	Country where the applicant is located.
Contact Name	-
Contact Number	-
Type of ID	-
ID Number	-
Scope of Business	Briefly describe the main business.
Number of Employees	For reference only
Branch Location Country	Country where the applicant branch is located. Set this parameter based on the actual situation.

Table 2-2 Required materials

Parameter	Description	Required Material	Signature	Company Seal
Business License	Upload a photo of the business license with the official seal. For the position of the seal, see the template.	A scanned copy of your company's business license	-	√
Service Agreement	Download the *Huawei Cloud Cross-Border Circuit Service Agreement*, fill in the blank, upload the copy of agreement with the signature and official seal. ● Sign the material on the signature block. ● Stamp the seal over the signature.	A scanned copy of the *Huawei Cloud Cross-Border Circuit Service Agreement*	√	√

Parameter	Description	Required Material	Signature	Company Seal
Letter of Commitment to Information Security	Download the *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*, fill in the blank, and upload the copy of the letter with the signature and seal. ● Sign the material on the signature block. ● Stamp the seal over the signature. ● Specify the bandwidth you estimated and your company name.	A scanned copy of the *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*	√	√

Step 4 Click **Submit**.

----End

Step 2: Create a Cloud Connection

Step 1 Go to the **Cloud Connections** page.

Step 2 In the upper right corner of the page, click **Create Cloud Connection**.

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

Table 2-3 Parameters for creating a cloud connection

Parameter	Example Value	Description
Name		Specifies the cloud connection name. The name can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Enterprise Project		Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.
Scenario		**VPC**: VPCs or virtual gateways can use this cloud connection.

Parameter	Example Value	Description
Tag		Identifies the cloud connection. A tag consists of a key and a value. You can add 20 tags to a cloud connection. **NOTE** If a predefined tag has been created on Tag Management Service (TMS), you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tags**.
Description		Provides supplementary information about the cloud connection. The description can contain no more than 255 characters.

Step 4 Click **OK**.

----End

Step 3: Request Permission to Use the VPC in the Other Account

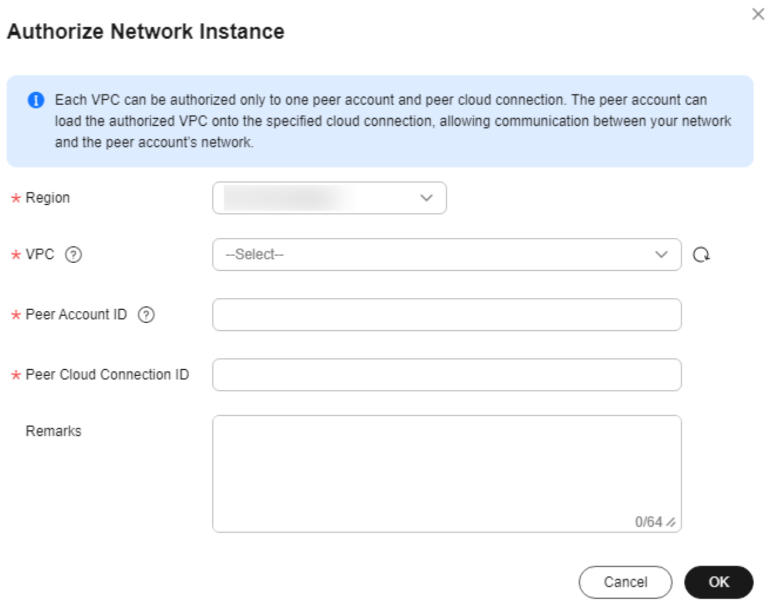
In this example, the two VPCs are in different accounts. If the VPC in your account (account A) needs to communicate with that in the other account (account B), ask this other account to grant you the permission to load their VPC to your cloud connection. This other account can take the following steps to grant you the permission to load their VPC:

Step 1 Go to the **Cross-Account Authorization** page.

Step 2 On the **Network Instances Authorized by Me** tab, click **Authorize Network Instance**.

Step 3 Configure the parameters based on **Table 2-4**.

Figure 2-3 Cross-account authorization



Authorize Network Instance

Each VPC can be authorized only to one peer account and peer cloud connection. The peer account can load the authorized VPC onto the specified cloud connection, allowing communication between your network and the peer account's network.

* Region [redacted]

* VPC --Select--

* Peer Account ID

* Peer Cloud Connection ID

Remarks 0/64

Table 2-4 Parameters for the other account to grant you the permission to load their VPC to your cloud connection

Parameter	Description
Region	Specifies the region where the VPC is located.
VPC	Specifies the VPC to be loaded to your cloud connection.
Peer Account ID	Specifies the ID of your account.
Peer Cloud Connection ID	Specifies the ID of your cloud connection that the VPC is to be loaded to.
Remarks	Provides supplementary information about cross-account authorization.

Step 4 Click **OK**.

----End

Step 4: Load Network Instances

Load the VPCs that need to communicate with each other to the cloud connection you have created. To load the VPC in the other account, take the following steps:

Step 1 Go to the **Cloud Connections** page.

Step 2 Click the name of the cloud connection to go to the **Basic Information** page.

Step 3 Click the **Network Instances** tab.

Step 4 Click **Load Network Instance**. In the displayed dialog, select **Peer account**.

Configure other parameters based on **Table 2-5** and click **OK**.

Table 2-5 Parameters for loading network instances across accounts

Parameter	Description
Account	Specifies the account that provides the network instance. Select **Peer account**.
Peer Account ID	Specifies the ID of the other account.
Region	Specifies the region where the VPC you want to connect is located.
Peer Project ID	Specifies the project ID of the VPC in the other account.
Instance Type	VPC Specifies the type of the network instance that needs to be loaded to the cloud connection.
Peer VPC	Specifies the VPC to be loaded.

Parameter	Description
VPC CIDR Block	Specifies the subnets in the VPC you want to load and custom CIDR blocks.
Remarks	Provides supplementary information about the network instance.

NOTE

- A network instance can only be loaded to one cloud connection.
- If a VPC is loaded, the associated virtual gateway cannot be loaded.

Step 5 Click **Continue Loading** if you need to load another network instance. If you do not need to load another network instance now, close the dialog box and view the loaded network instance on the **Network Instances** tab.

----End

Step 5: Buy a Bandwidth Package

By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity. To enable normal communication between regions in the same geographic region or different geographic regions, you need to purchase a bandwidth package and bind it to the cloud connection.

NOTE

One cloud connection can only have one bandwidth package regardless of if the cloud connection is used for communication within a geographic region or between geographic regions. For example, if network instances are in the Chinese mainland and Asia Pacific, your cloud connection can only have one bandwidth package.

Step 1 Go to the **Buy Bandwidth Package** page.

Step 2 Configure the parameters based on **Table 2-6** and click **Buy Now**.

Table 2-6 Parameters for buying a bandwidth package

Parameter	Description
Billing Mode	The only option is **Yearly/Monthly**. You can purchase it by year or month as needed.
Name	Specifies the bandwidth package name. The name can contain 1 to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.
Billed By	Specifies by what you want the bandwidth package to be billed.

Parameter	Description
Applicability	Specifies whether you want to use the bandwidth package for communication within a geographic region or between geographic regions. There are two options: ● **Single geographic region**: Use the bandwidth package between regions in the same geographic region. ● **Across geographic regions**: Use the bandwidth package between regions in different geographic regions.
Geographic Region	Specifies the geographic region(s).
Bandwidth	Specifies the bandwidth you require for communication between regions, in Mbit/s. The sum of all inter-region bandwidths you assign cannot exceed the total bandwidth of the bandwidth package. Assign the bandwidth based on your network plan.
Tag	Identifies the bandwidth package. A tag consists of a key and a value. You can add 20 tags to a bandwidth package. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tags**.
Required Duration	Specifies how long you require the bandwidth package for. Auto renewal is supported.
Cloud Connection	Specifies the cloud connection you want to bind the bandwidth package to. There are two options: ● Bind now ● Bind later

Step 3 Confirm the configuration and click **Pay Now**.

Step 4 On the payment information page, click **Confirm**.

View the bandwidth package in the bandwidth package list. If the status changes to **Normal**, the purchase is successful.

----End

Bind the purchased bandwidth package to the created cloud connection.

If you choose **Bind later** when buying a bandwidth package, you need to bind it to the created cloud connection now.

Step 1 Go to the **Cloud Connections** page.

Step 2 Click the name of the cloud connection to go to the **Basic Information** page.

Step 3 Click the **Bandwidth Packages** tab.

Step 4 Click **Bind Bandwidth Package**. In the displayed dialog box, select the purchased bandwidth package and click **OK**.

----End

Step 6: Assign Inter-Region Bandwidth

By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity.

Step 1 Go to the **Cloud Connections** page.

Step 2 Click the name of the cloud connection to go to the **Basic Information** page.

Step 3 Click the **Inter-Region Bandwidths** tab.

Step 4 Click **Assign Inter-Region Bandwidth** and configure the parameters based on **Table 2-7**.

Table 2-7 Parameters required for assigning inter-region bandwidth

Parameter	Description
Regions	Specifies the regions of the network instances that need to communicate with each other. Select two regions.
Bandwidth Package	Specifies the purchased bandwidth package that will be bound to the cloud connection.
Bandwidth	Specifies the bandwidth you require for communication between regions, in Mbit/s. The sum of all inter-region bandwidths you assign cannot exceed the total bandwidth of the bandwidth package. Plan the bandwidth in advance.

Step 5 Click **OK**.

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

NOTE

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

----End

3 Connecting On-Premises Data Centers and VPCs

3.1 Using Cloud Connect and Direct Connect to Connect an On-premises Data Center to a VPC

Scenarios

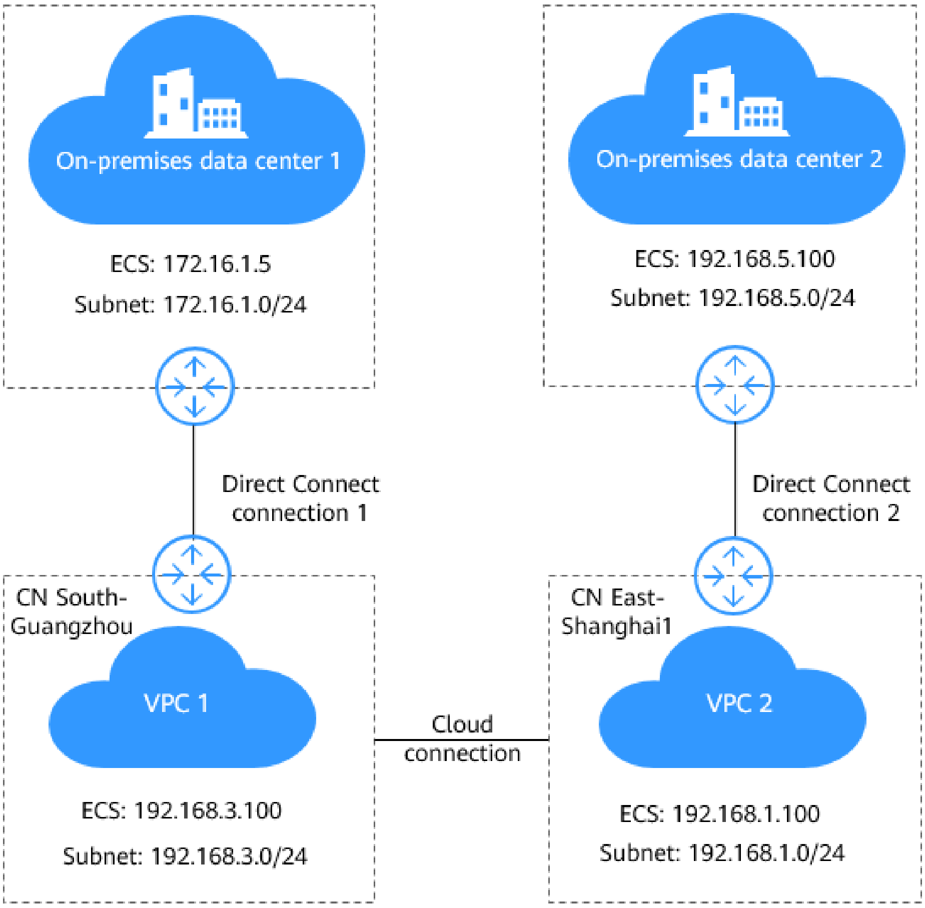
If you have more than one on-premises data center and VPC, you can use Direct Connect and a cloud connection to connect all your on-premises data centers to the VPCs in different regions.

Figure 3-1 shows an example.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

Figure 3-1 Connecting on-premises data centers and VPCs



NOTE

When you configure a cloud connection, note that:

- Subnet CIDR blocks of the VPCs cannot overlap or conflict with each other.
- The routes for the subnets in the VPCs cannot conflict with existing routes, including those added for VPC Peering, Direct Connect, or VPN.

Prerequisites

- You have a Huawei Cloud account, and the Huawei Cloud account has been configured with operation permissions of related services.
- The account balance is sufficient to purchase the required resources, such as Direct Connect connections, bandwidth packages, and ECSs.
- Direct Connect locations have been determined and the site survey of on-premises data centers have been completed together with the carrier. For details, see **Preparations**.
- The VPCs and subnets that need to communicate with each other across regions have been created.
- All VPC subnets have been configured for your on-premises data centers.

Procedure

Step 1 Configure Direct Connect. In this example, two Direct Connect connections are required to connect each on-premises data center to the cloud.

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. Click ☰ 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 Parameters required for creating a connection

Parameter	Description
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.
Connection Name	Specifies the connection name. Enter a desired name.
Location	Specifies the location where your leased line can connect to Huawei Cloud.
Carrier	Specifies the carrier that provides the leased line.
Port Type	Specifies the type of the port used by the connection. There are four types of ports: 1GE, 10GE, 40GE, and 100GE.
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.
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.

Parameter	Description
Tag	Identifies the connection. A tag consists of a key and a value. You can add 20 tags to a connection. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tags**.
Description	Provides supplementary information about the connection.
Billing Mode	Specifies how you are charged. Currently, only **Yearly/Monthly** is supported.
Required Duration	Specifies the duration for which you require the connection.
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 every three months.
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.
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 prolong the review.

   g. Click **Next**.
   h. Confirm the order and click **Pay**.
   i. Click **OK**.
2. Connect your data center to the location you select.
   a. After you have paid for the order, the system automatically allocates a connection ID for you, and the connection information is displayed on the management console. The connection status is **Creating**, when you will be contacted to confirm the construction plan and relevant information (including your company name, constructor, expected construction time, and construction workers).
   b. After having confirmed the construction plan, you can arrange the carrier to deploy the dedicated line and connect it to your equipment room based on your construction plan.
   c. In normal cases, Huawei resident engineers will connect the dedicated line to the Huawei Cloud gateway port within two working days.

d. After the construction is complete, the connection status becomes **Normal**, indicating that the connection is ready.

3. Create a virtual gateway.

   Create a virtual gateway to associate it with 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.

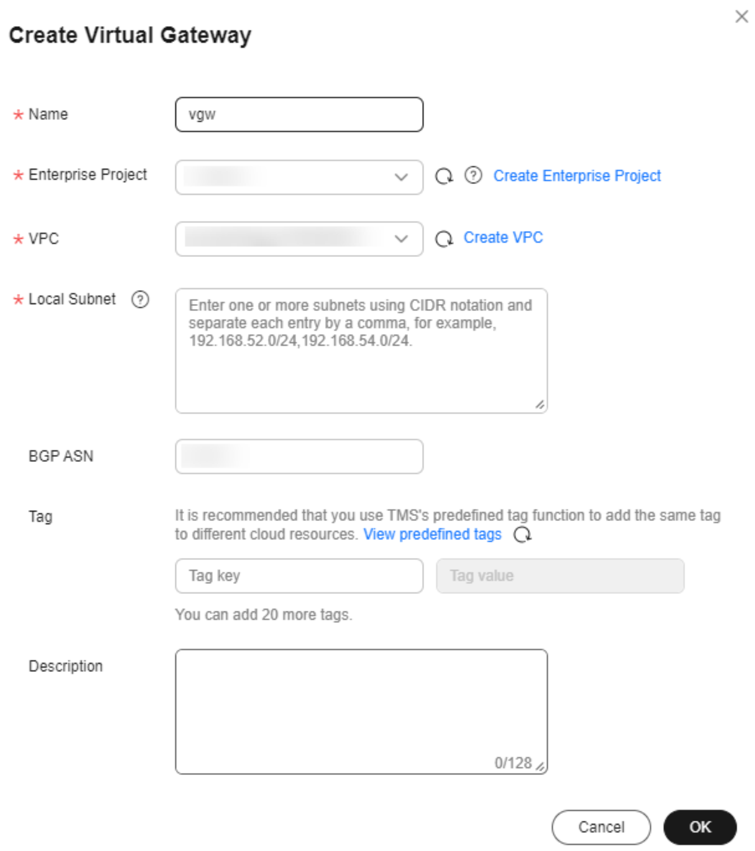
   c. Click ☰ to display **Service List** and choose **Networking** > **Direct Connect**.

   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



Create Virtual Gateway

* Name	vgw
* Enterprise Project	Create Enterprise Project
* VPC	Create VPC
* Local Subnet	Enter one or more subnets using CIDR notation and separate each entry by a comma, for example, 192.168.52.0/24,192.168.54.0/24.
BGP ASN	
Tag	It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags Tag key / Tag value You can add 20 more tags.
Description	0/128

Table 3-2 Parameters required for creating a virtual gateway

Parameter	Description
Name	Specifies the virtual gateway name. The name can contain 1 to 64 characters.
VPC	Specifies the VPC associated with the virtual gateway.
Local Subnet	Specifies the CIDR blocks of subnets in the VPC to connect to the on-premises network.
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 each on-premises data center to ensure normal communication.

g. Click **OK**.

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

4. Create a virtual interface.

Create a virtual interface over which the on-premises data center connects to Huawei Cloud so that the on-premises data center 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.

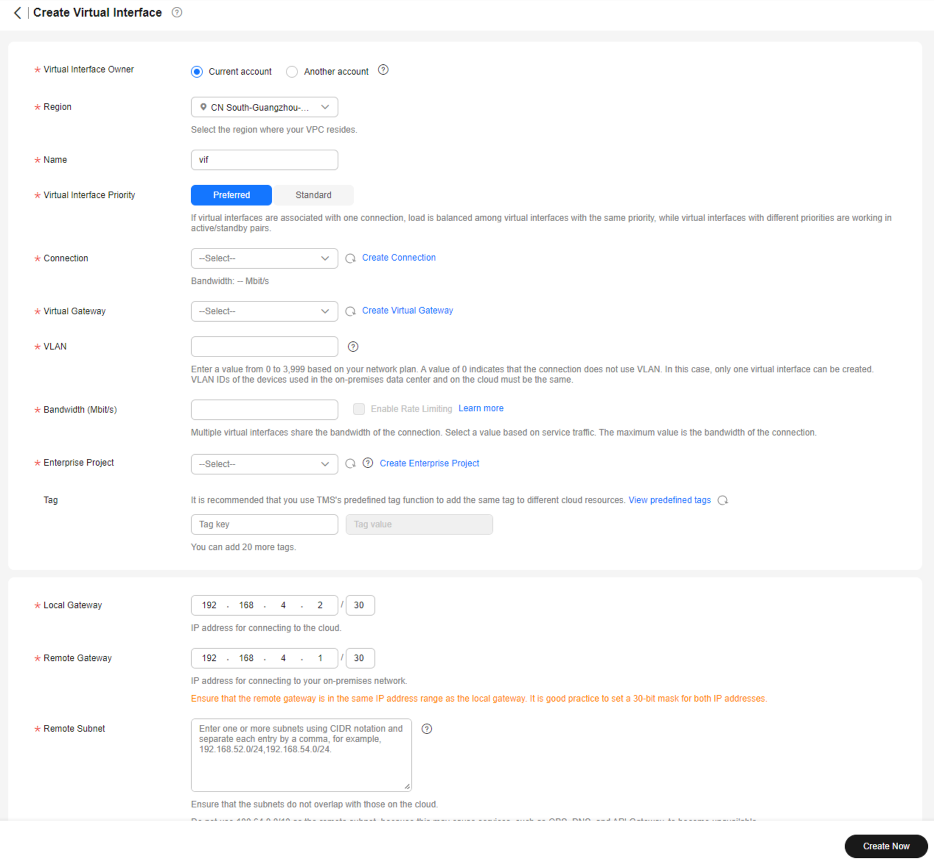
c. Click ≡ to display **Service List** and choose **Networking** > **Direct Connect**.

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



Create Virtual Interface

* Virtual Interface Owner: ● Current account ○ Another account

* Region: CN South-Guangzhou-...
Select the region where your VPC resides.

* Name: vif

* Virtual Interface Priority: Preferred | Standard
If virtual interfaces are associated with one connection, load is balanced among virtual interfaces with the same priority, while virtual interfaces with different priorities are working in active/standby pairs.

* Connection: --Select-- Create Connection
Bandwidth: -- Mbit/s

* Virtual Gateway: --Select-- Create Virtual Gateway

* VLAN:
Enter a value from 0 to 3,999 based on your network plan. A value of 0 indicates that the connection does not use VLAN. In this case, only one virtual interface can be created. VLAN IDs of the devices used in the on-premises data center and on the cloud must be the same.

* Bandwidth (Mbit/s): □ Enable Rate Limiting Learn more
Multiple virtual interfaces share the bandwidth of the connection. Select a value based on service traffic. The maximum value is the bandwidth of the connection.

* Enterprise Project: --Select-- Create Enterprise Project

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags
Tag key | Tag value
You can add 20 more tags.

* Local Gateway: 192 . 168 . 4 . 2 / 30
IP address for connecting to the cloud.

* Remote Gateway: 192 . 168 . 4 . 1 / 30
IP address for connecting to your on-premises network.
Ensure that the remote gateway is in the same IP address range as the local gateway. It is good practice to set a 30-bit mask for both IP addresses.

* Remote Subnet: Enter one or more subnets using CIDR notation and separate each entry by a comma, for example, 192.168.52.0/24,192.168.54.0/24.
Ensure that the subnets do not overlap with those on the cloud.
Do not use 100.64.0.0/10 as the remote subnet, because this may cause services, such as OBS, DNS, and API Gateway, to become unavailable.

Create Now

Table 3-3 Parameters required for creating a virtual interface

Parameter	Description
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.
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters.
Connection	Specifies the connection you use to connect your data center to the cloud.
Virtual Gateway	Specifies the virtual gateway to which the virtual interface will connect.
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.

Parameter	Description
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.
Bandwidth	Specifies the bandwidth that can be used by the virtual interface, in Mbit/s. The bandwidth cannot exceed that of the connection.
Local Gateway	Specifies the IP address for connecting to the cloud.
Remote Gateway	Specifies the IP address for connecting to the on-premises network. 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.
Remote Subnet	Specifies the subnets and masks of the on-premises data center. If there are multiple subnets, use commas (,) to separate them.
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 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.
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 ~!, .:;-_"(){}[]/@#$ %^&*+|=

Parameter	Description
Description	Provides supplementary information about the virtual interface. The description can contain a maximum of 128 characters.

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 Create a cloud connection.

1. Create a cloud connection.

a. Go to the **Cloud Connections** page.

b. In the upper right corner of the page, click **Create Cloud Connection**.

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

Table 3-4 Parameters for creating a cloud connection

Parameter	Description
Name	Specifies the cloud connection name.
Enterprise Project	Specifies the enterprise project for managing the cloud connection. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.
Scenario	Specifies whether the cloud connection is used to connect VPCs or enterprise routers. If you select **VPC** here, only VPCs or virtual gateways can use this cloud connection.
Tag	Identifies the cloud connection. A tag consists of a key and a value. You can add 20 tags to a cloud connection. **NOTE** If you have configured tag policies for Cloud Connect, add tags to cloud connections based on the tag policies. If you add a tag that does not comply with the tag policies, cloud connections may fail to be created. Contact your administrator to learn more about tag policies.

Parameter	Description
Description	(Optional) Provides supplementary information about the cloud connection. The description can contain no more than 255 characters and cannot contain angle brackets (<>).

d. Click **OK**.

2. Load network instances.

   Load the VPCs in CN South-Guangzhou and CN East-Shanghai1 to the created cloud connection.

   a. In the cloud connection list, click the name (**CloudConnect**) of the cloud connection.

   b. On the **Network Instances** tab, click **Load Network Instance**.

   c. Configure the parameters.

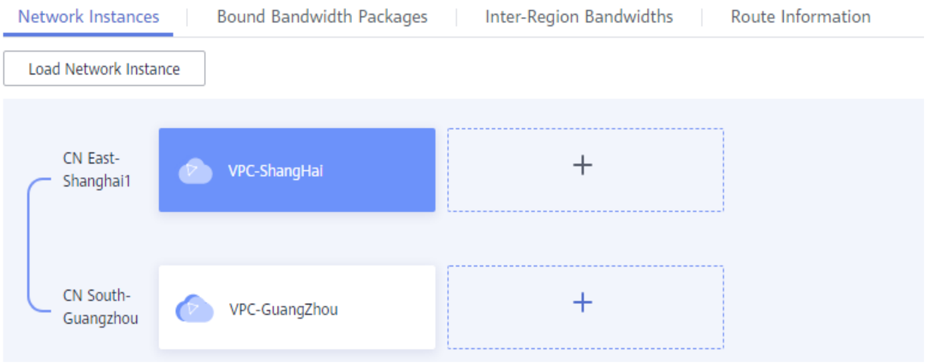
   NOTE

   To enable the on-premises data center to access the VPC, you need to add the subnet used in the on-premises data center as a custom CIDR block.

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

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

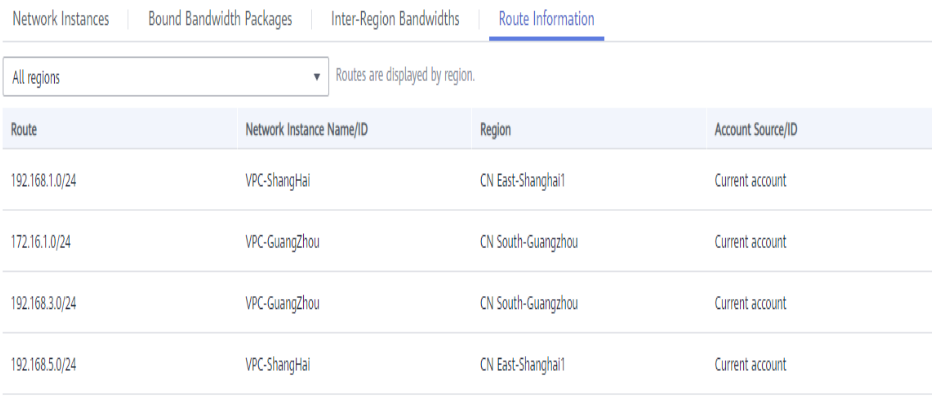
Figure 3-4 Loading the other VPC



NOTE

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

Figure 3-5 Route Information



Route	Network Instance Name/ID	Region	Account Source/ID
192.168.1.0/24	VPC-ShangHai	CN East-Shanghai1	Current account
172.16.1.0/24	VPC-GuangZhou	CN South-Guangzhou	Current account
192.168.3.0/24	VPC-GuangZhou	CN South-Guangzhou	Current account
192.168.5.0/24	VPC-ShangHai	CN East-Shanghai1	Current account

3. Buy a bandwidth package.

   By default, Cloud Connect provides 10 kbit/s of bandwidth for testing cross-region network connectivity.

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

   a. In the cloud connection list, click the name (**CloudConnect**) of the cloud connection.

   b. On the **Bandwidth Packages** tab, click **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**.

   d. Click **Buy Now**.

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

   f. Click **OK**.

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

      NOTE

      In the navigation pane, choose **Bandwidth Packages**. On the displayed page, locate the bandwidth package you just purchased. You can view its details, such as the billing mode, order information, cloud connection bound to, 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 name (**CloudConnect**) of the cloud connection.

   b. On the **Inter-Region Bandwidths** tab, click **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.

NOTE

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

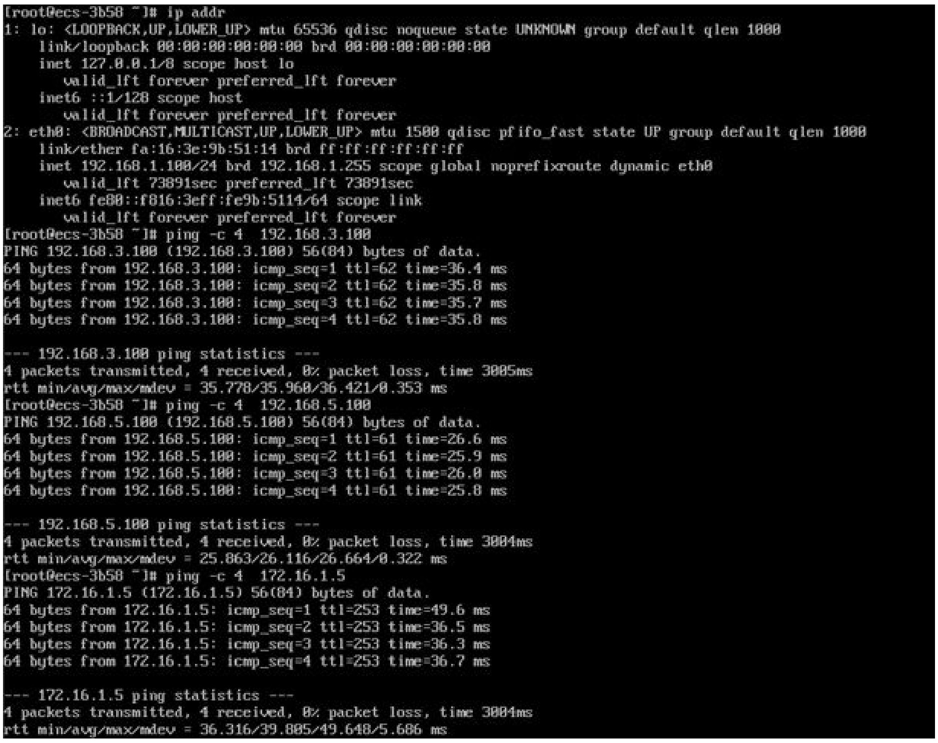
Step 3 Configure local routes on the on-premises data centers.

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

----End

Verification

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



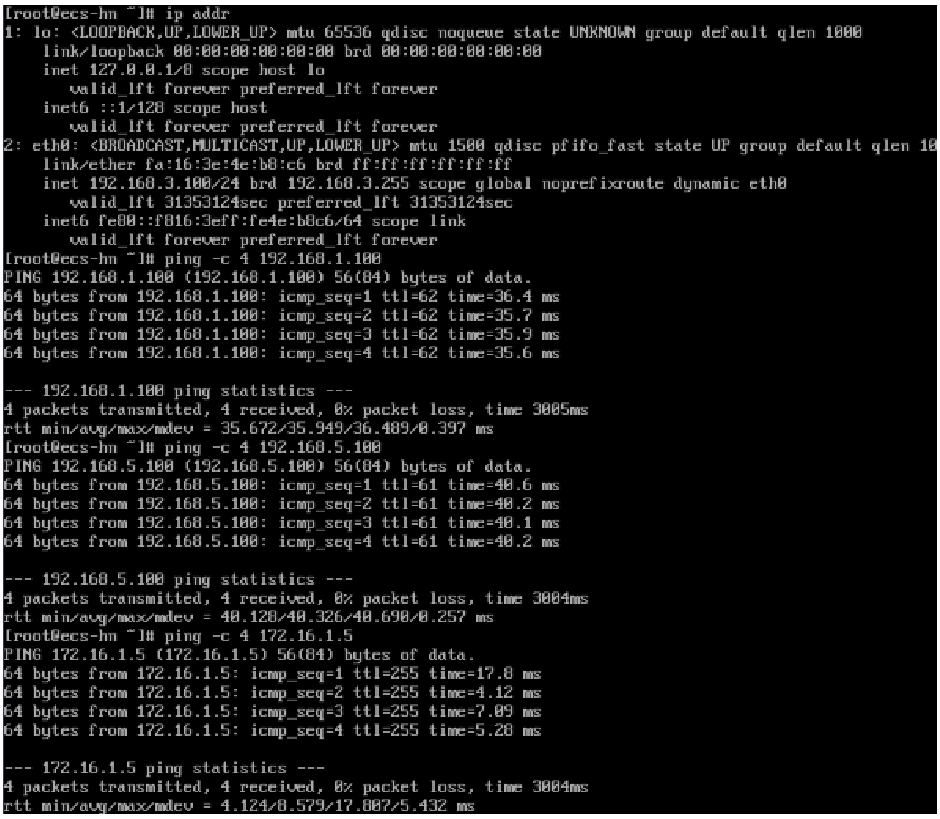
```
[root@ecs-3b58 ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether fa:16:3e:9b:51:14 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.100/24 brd 192.168.1.255 scope global noprefixroute dynamic eth0
       valid_lft 73891sec preferred_lft 73891sec
    inet6 fe80::f816:3eff:fe9b:5114/64 scope link
       valid_lft forever preferred_lft forever
[root@ecs-3b58 ~]# ping -c 4  192.168.3.100
PING 192.168.3.100 (192.168.3.100) 56(84) bytes of data.
64 bytes from 192.168.3.100: icmp_seq=1 ttl=62 time=36.4 ms
64 bytes from 192.168.3.100: icmp_seq=2 ttl=62 time=35.8 ms
64 bytes from 192.168.3.100: icmp_seq=3 ttl=62 time=35.7 ms
64 bytes from 192.168.3.100: icmp_seq=4 ttl=62 time=35.8 ms

--- 192.168.3.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 35.778/35.960/36.421/0.353 ms
[root@ecs-3b58 ~]# 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=26.6 ms
64 bytes from 192.168.5.100: icmp_seq=2 ttl=61 time=25.9 ms
64 bytes from 192.168.5.100: icmp_seq=3 ttl=61 time=26.0 ms
64 bytes from 192.168.5.100: icmp_seq=4 ttl=61 time=25.8 ms

--- 192.168.5.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 25.863/26.116/26.664/0.322 ms
[root@ecs-3b58 ~]# 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=253 time=49.6 ms
64 bytes from 172.16.1.5: icmp_seq=2 ttl=253 time=36.5 ms
64 bytes from 172.16.1.5: icmp_seq=3 ttl=253 time=36.3 ms
64 bytes from 172.16.1.5: icmp_seq=4 ttl=253 time=36.7 ms

--- 172.16.1.5 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3004ms
rtt min/avg/max/mdev = 36.316/39.805/49.648/5.686 ms
```

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



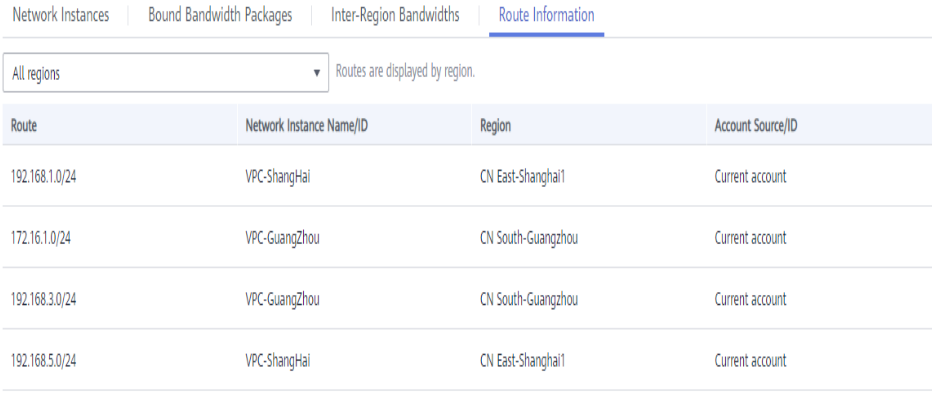
```
[root@ecs-hn ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft 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.



Route	Network Instance Name/ID	Region	Account Source/ID
192.168.1.0/24	VPC-ShangHai	CN East-Shanghai1	Current account
172.16.1.0/24	VPC-GuangZhou	CN South-Guangzhou	Current account
192.168.3.0/24	VPC-GuangZhou	CN South-Guangzhou	Current account
192.168.5.0/24	VPC-ShangHai	CN East-Shanghai1	Current account

4 Connecting VPCs in Different Geographic Regions

4.1 Using a Cloud Connection to Connect VPCs in Two Geographic Regions

Solution Overview

Scenario

A company has two branches, one in Beijing and the other in Hong Kong. There are two VPCs available, one in the CN North-Beijing4 region, and the other in the CN-Hong Kong region. To enable the two branches to communicate with each other over a private network, a cloud connection is used to link the two VPCs in different regions.

NOTE

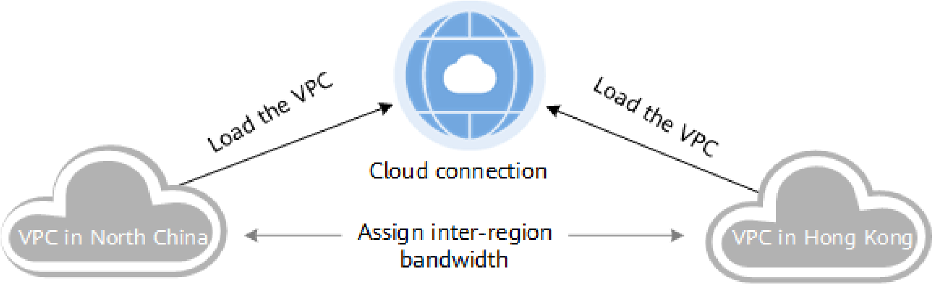
For details about the regions where cloud connections are available, see **Region Availability**.

Solution Architecture

1. Create a cloud connection.
2. Load the two VPCs to the cloud connection.
3. Buy a bandwidth package and assign inter-region bandwidths.
4. Confirm whether the two VPCs can communicate with each other through the cloud connection.

For details, see **Figure 4-1**.

Figure 4-1 Communication between VPCs in different regions



Advantages

- Ease of use: In just four simple steps, you can build cross-region connectivity between VPCs.
- High performance: Cloud Connect leverages the global network infrastructure of the public cloud to provide high-quality, low-latency connectivity with bandwidth that can be flexibly adjusted to meet changing service requirements.

Constraints

- A cloud connection cannot be used to connect VPCs that have overlapping CIDR blocks, or communication will fail.
- If you load a VPC to a cloud connection created using the same account, you cannot enter loopback addresses, multicast addresses, or broadcast addresses for the custom CIDR block.
- If a NAT gateway has been created for any VPC you have loaded to a cloud connection, a custom CIDR block needs to be added and set to 0.0.0.0/0.

Resource Planning

The following table describes the resource planning in the best practice.

Table 4-1 Resources required

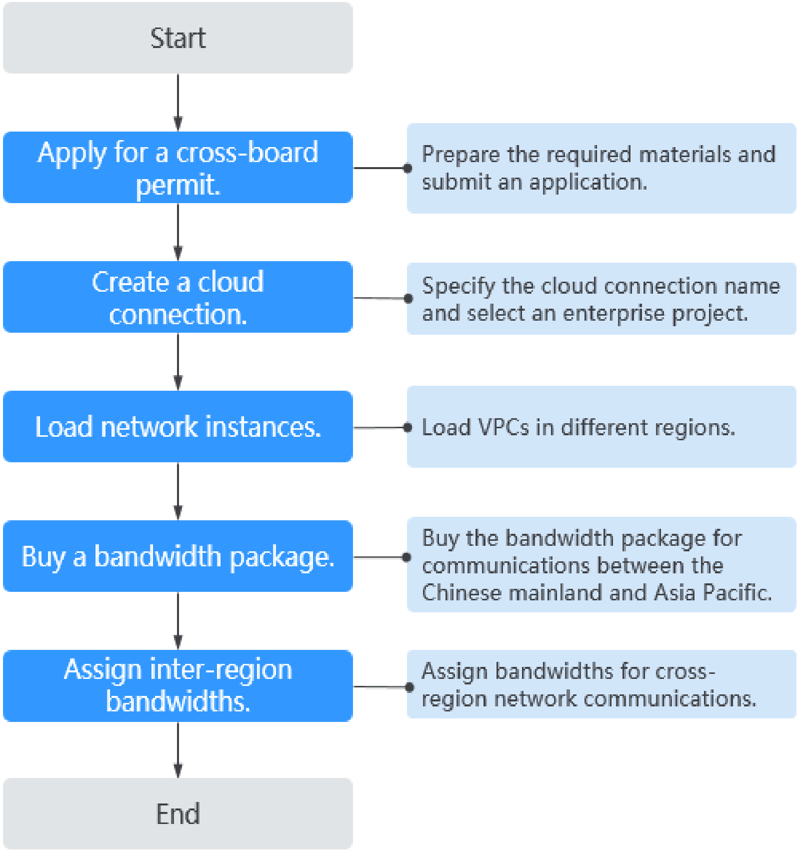
Huawei Cloud Region	Resource	Description	Number of Route Tables	Billing
CN North-Beijing4	VPC	VPC subnet: 192.168.1.0/24 Custom CIDR block: 192.168.44.0/24	1	Free
CN-Hong Kong	VPC	VPC subnet: 192.168.0.0/24 Custom CIDR block: 192.168.11.0/24	1	Free

Huawei Cloud Region	Resource	Description	Number of Route Tables	Billing
Global	Cloud connection	Cross-region (Chinese mainland - Asia Pacific) bandwidth package	1	For details, see **Cloud Connect Pricing Details**.

Procedure for Connecting VPCs in Beijing and Hong Kong

In this example, to connect the VPC in CN North Beijing4 and the VPC in CN-Hong Kong, you need to apply for a cross-border permit to ensure data transmission security. Then, you need to create a cloud connection and load the two VPCs, purchase a bandwidth package, and assign inter-region bandwidth.

Figure 4-2 Process of connecting VPCs in different geographic regions using a cloud connection


Start
Apply for a cross-board permit.
Prepare the required materials and submit an application.
Create a cloud connection.
Specify the cloud connection name and select an enterprise project.
Load network instances.
Load VPCs in different regions.
Buy a bandwidth package.
Buy the bandwidth package for communications between the Chinese mainland and Asia Pacific.
Assign inter-region bandwidths.
Assign bandwidths for cross-region network communications.
End

Step 1: Apply for a Cross-Border Permit

If a VPC you want to connect is outside the Chinese mainland, you need to apply for a cross-border permit.

Skip this step if cross-border communication is not required.

Step 1 Go to the **Bandwidth Packages** page.

Step 2 On the displayed page, click **apply now**.

If the registered address of your business entity is in the Chinese mainland, click **here** to go to the **Cross-Border Service Application System** page.

If the registered address of your business entity is outside the Chinese mainland, click **here** to go to the **Cross-Border Service Application System** page.

NOTE

Select the address for applying for the cross-border permit based on the registration address of your business entity.

Step 3 On the displayed page, select an applicant type, configure the parameters as prompted, and upload the required materials.

NOTICE

Prepare and upload the materials required on the application page.

Table 4-2 Online cross-border permit application

Parameter	Description
Applicant Name	This name must be the same as the company name in the *Letter of Commitment to Information Security*.
Huawei Cloud UID	The account ID to log in to the management console. You can take the following steps to obtain your account ID. 1. Log in to the management console. 2. Click the username in the upper right corner and select **My Credentials** from the drop-down list. 3. On the **API Credentials** page, view the **Account ID**.
Bandwidth (Mbit/s)	For reference only
Start Date	For reference only
Termination Date	For reference only
Customer Type	Select a type based on the actual situation.
Country of the Customer	Country where the applicant is located.

Parameter	Description
Contact Name	-
Contact Number	-
Type of ID	-
ID Number	-
Scope of Business	Briefly describe the main business.
Number of Employees	For reference only
Branch Location Country	Country where the applicant branch is located. Set this parameter based on the actual situation.

Table 4-3 Required materials

Parameter	Description	Required Material	Signature	Company Seal
Business License	Upload a photo of the business license with the official seal. For the position of the seal, see the template.	A scanned copy of your company's business license	-	√
Service Agreement	Download the *Huawei Cloud Cross-Border Circuit Service Agreement*, fill in the blank, upload the copy of agreement with the signature and official seal. ● Sign the material on the signature block. ● Stamp the seal over the signature.	A scanned copy of the *Huawei Cloud Cross-Border Circuit Service Agreement*	√	√

Parameter	Description	Required Material	Signature	Company Seal
Letter of Commitment to Information Security	Download the *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*, fill in the blank, and upload the copy of the letter with the signature and seal. ● Sign the material on the signature block. ● Stamp the seal over the signature. ● Specify the bandwidth you estimated and your company name.	A scanned copy of the *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*	√	√

Step 4 Click **Submit**.

----End

Step 2: Create a Cloud Connection

Step 1 Go to the **Cloud Connections** page.

Step 2 In the upper right corner of the page, click **Create Cloud Connection**.

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

Table 4-4 Parameters for creating a cloud connection

Parameter	Example Value	Description
Name		Specifies the cloud connection name. The name can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Enterprise Project		Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.
Scenario		**VPC**: VPCs or virtual gateways can use this cloud connection.

Parameter	Example Value	Description
Tag		Identifies the cloud connection. A tag consists of a key and a value. You can add 20 tags to a cloud connection. **NOTE** If a predefined tag has been created on Tag Management Service (TMS), you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tags**.
Description		Provides supplementary information about the cloud connection. The description can contain no more than 255 characters.

Step 4 Click **OK**.

----End

Step 3: Load Network Instances

Load the VPCs that need to communicate with each other to the created cloud connection.

Step 1 Go to the **Cloud Connections** page.

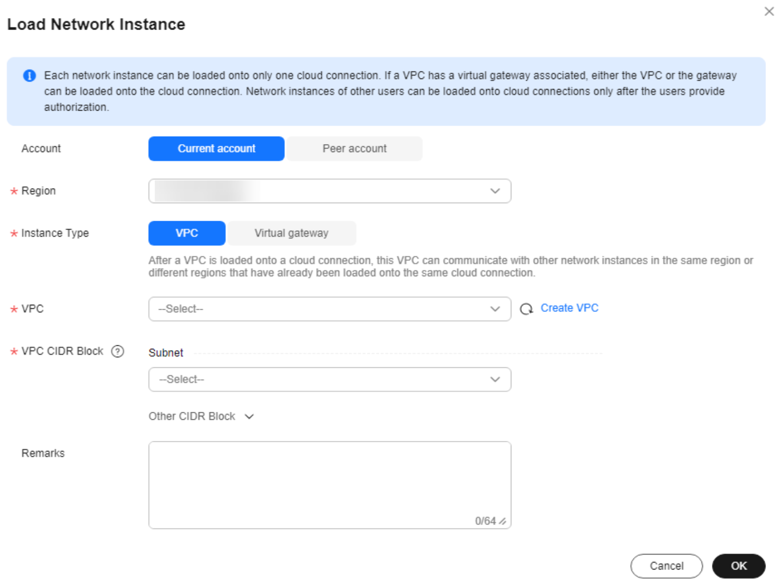
Step 2 Click the name of the cloud connection to go to the **Basic Information** page.

Step 3 Click the **Network Instances** tab.

Step 4 Click **Load Network Instance**.

Step 5 Configure the parameters based on **Table 4-5** and click **OK**.

Figure 4-3 Load Network Instance - Current account



Load Network Instance

Each network instance can be loaded onto only one cloud connection. If a VPC has a virtual gateway associated, either the VPC or the gateway can be loaded onto the cloud connection. Network instances of other users can be loaded onto cloud connections only after the users provide authorization.

Account: Current account

* Instance Type: VPC

After a VPC is loaded onto a cloud connection, this VPC can communicate with other network instances in the same region or different regions that have already been loaded onto the same cloud connection.

Table 4-5 Parameters for loading a network instance to a cloud connection

Parameter	Description
Account	Specifies the account that provides the network instance. Select **Current account**.
Region	Specifies the region where the VPC you want to connect is located.
Instance Type	Specifies the type of the network instance that needs to be loaded to the cloud connection. There are two options: ● VPC ● Virtual gateway Select **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**.
VPC CIDR Block	Specifies the subnets in the VPC and custom CIDR blocks. If you have set **Instance Type** to **VPC**, you need to configure the following two parameters: ● **Subnet**: Select one or more subnets in the VPC. ● **Other CIDR Block**: Add one or more custom CIDR blocks as needed.
Remarks	Provides supplementary information about the network instance.

Step 6 Click **Continue Loading** if you need to load another network instance. If you do not need to load another network instance now, close the dialog box and view the loaded network instance on the **Network Instances** tab.

----End

Step 4: Buy a Bandwidth Package

By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity. To enable normal communication between regions in the same geographic region or different geographic regions, you need to purchase a bandwidth package and bind it to the cloud connection.

NOTE

One cloud connection can only have one bandwidth package regardless of if the cloud connection is used for communication within a geographic region or between geographic regions. For example, if network instances are in the Chinese mainland and Asia Pacific, your cloud connection can only have one bandwidth package.

Step 1 Click the name of the created cloud connection to go to the **Basic Information** page.

Step 2 Click the **Bandwidth Packages** tab.

Step 3 Click **Buy Bandwidth Package**. On the displayed page, configure parameters based on **Table 4-6** and click **Buy Now**.

Table 4-6 Parameters for buying a bandwidth package

Parameter	Description
Billing Mode	The only option is **Yearly/Monthly**. You can purchase it by year or month as needed.
Name	Specifies the bandwidth package name. The name can contain 1 to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.
Billed By	Specifies by what you want the bandwidth package to be billed.
Applicability	Specifies whether you want to use the bandwidth package for communication within a geographic region or between geographic regions. There are two options: ● **Single geographic region**: Use the bandwidth package between regions in the same geographic region. ● **Across geographic regions**: Use the bandwidth package between regions in different geographic regions.
Geographic Region	Specifies the geographic region(s).
Bandwidth	Specifies the bandwidth you require for communication between regions, in Mbit/s. The sum of all inter-region bandwidths you assign cannot exceed the total bandwidth of the bandwidth package. Assign the bandwidth based on your network plan.
Tag	Identifies the bandwidth package. A tag consists of a key and a value. You can add 20 tags to a bandwidth package. **NOTE** If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tags**.
Required Duration	Specifies how long you require the bandwidth package for. Auto renewal is supported.
Cloud Connection	Specifies the cloud connection you want to bind the bandwidth package to. There are two options: ● Bind now ● Bind later

Step 4 Confirm the configuration and click **Pay Now**.

Step 5 On the payment information page, click **Confirm**.

View the bandwidth package in the bandwidth package list. If the status changes to **Normal**, the purchase is successful.

----End

Step 5: Assign Inter-Region Bandwidth

By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity.

Step 1 Click the name of the created cloud connection to go to the **Basic Information** page.

Step 2 Click the **Inter-Region Bandwidths** tab.

Step 3 Click **Assign Inter-Region Bandwidth** and configure the parameters based on **Table 4-7**.

Table 4-7 Parameters required for assigning inter-region bandwidth

Parameter	Description
Regions	Specifies the regions of the network instances that need to communicate with each other. Select two regions.
Bandwidth Package	Specifies the purchased bandwidth package that will be bound to the cloud connection.
Bandwidth	Specifies the bandwidth you require for communication between regions, in Mbit/s. The sum of all inter-region bandwidths you assign cannot exceed the total bandwidth of the bandwidth package. Plan the bandwidth in advance.

Step 4 Click **OK**.

Now the branches in Beijing and Hong Kong can communicate with each other. You can check the routing information to verify the configuration.

----End

4.2 Using a Cloud Connection to Connect VPCs in Three Geographic Regions

Background

Instances in the VPCs in different regions can use EIPs or VPN connections to communicate with each other. However, EIPs and VPN connections are not so reliable because they are over the Internet, and if you use EIPs, data cannot be encrypted. To ensure stable and encrypted transmission, you can use Cloud Connect to connect the VPCs.

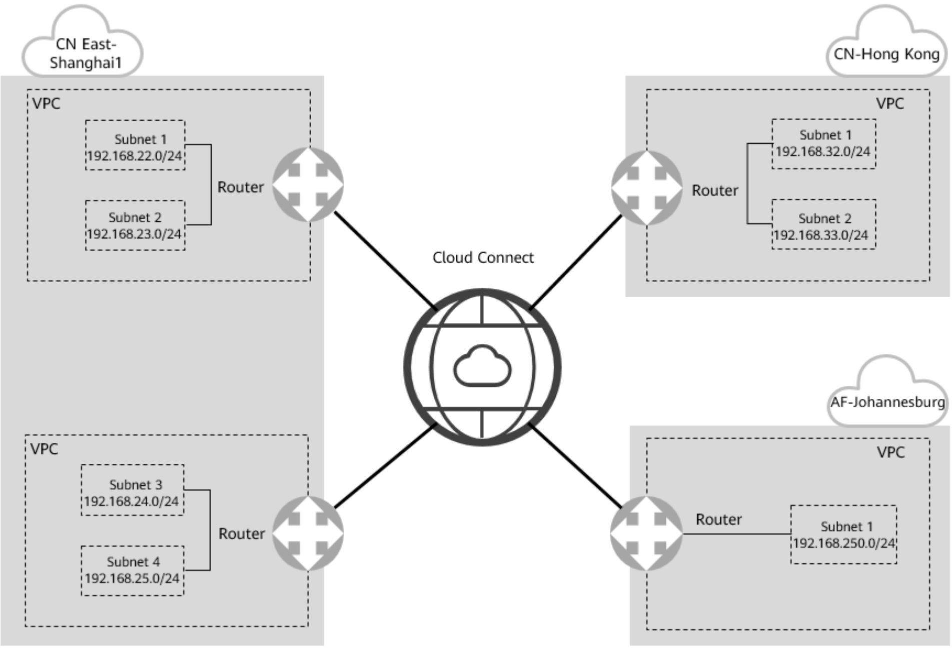
Scenarios

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. You can use a cloud connection 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 a cloud connection is used to enable communication among these VPCs in different regions.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

Figure 4-4 Connecting VPCs in multiple geographic regions



When you configure a cloud connection, note that:

- Subnet CIDR blocks of the VPCs cannot overlap or conflict with each other.
- The routes for the subnets in the VPCs cannot conflict with existing routes, including those added for VPC Peering, Direct Connect, or VPN.

Prerequisites

- The VPCs and subnets that need to communicate with each other across regions have been created.
- The account balance is sufficient to purchase bandwidth packages.
- A cross-border permit has been obtained 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 cross-border communication is not required, you can ignore the last item.

Step 1: Apply for a Cross-Border Permit

If a VPC you want to connect is outside the Chinese mainland, you need to apply for a cross-border permit.

Skip this step if cross-border communication is not required.

Step 1 Go to the **Bandwidth Packages** page.

Step 2 On the displayed page, click **apply now**.

If the registered address of your business entity is in the Chinese mainland, click **here** to go to the **Cross-Border Service Application System** page.

If the registered address of your business entity is outside the Chinese mainland, click **here** to go to the **Cross-Border Service Application System** page.

NOTE

Select the address for applying for the cross-border permit based on the registration address of your business entity.

Step 3 On the displayed page, select an applicant type, configure the parameters as prompted, and upload the required materials.

NOTICE

Prepare and upload the materials required on the application page.

Table 4-8 Online cross-border permit application

Parameter	Description
Applicant Name	This name must be the same as the company name in the *Letter of Commitment to Information Security*.
Huawei Cloud UID	The account ID to log in to the management console. You can take the following steps to obtain your account ID. 1. Log in to the management console. 2. Click the username in the upper right corner and select **My Credentials** from the drop-down list. 3. On the **API Credentials** page, view the **Account ID**.
Bandwidth (Mbit/s)	For reference only
Start Date	For reference only

Parameter	Description
Termination Date	For reference only
Customer Type	Select a type based on the actual situation.
Country of the Customer	Country where the applicant is located.
Contact Name	-
Contact Number	-
Type of ID	-
ID Number	-
Scope of Business	Briefly describe the main business.
Number of Employees	For reference only
Branch Location Country	Country where the applicant branch is located. Set this parameter based on the actual situation.

Table 4-9 Required materials

Parameter	Description	Required Material	Signature	Company Seal
Business License	Upload a photo of the business license with the official seal. For the position of the seal, see the template.	A scanned copy of your company's business license	-	√
Service Agreement	Download the *Huawei Cloud Cross-Border Circuit Service Agreement*, fill in the blank, upload the copy of agreement with the signature and official seal. ● Sign the material on the signature block. ● Stamp the seal over the signature.	A scanned copy of the *Huawei Cloud Cross-Border Circuit Service Agreement*	√	√

Parameter	Description	Required Material	Signature	Company Seal
Letter of Commitment to Information Security	Download the *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*, fill in the blank, and upload the copy of the letter with the signature and seal. ● Sign the material on the signature block. ● Stamp the seal over the signature. ● Specify the bandwidth you estimated and your company name.	A scanned copy of the *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*	√	√

Step 4 Click **Submit**.

----End

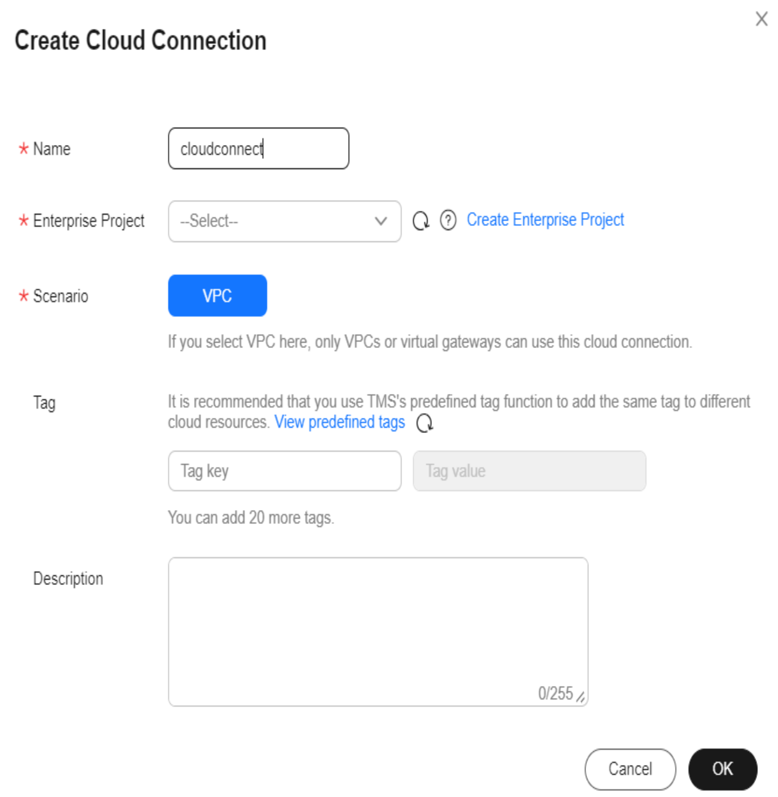
Step 2: Create a Cloud Connection

Step 1 Go to the **Cloud Connections** page.

Step 2 In the upper right corner of the page, click **Create Cloud Connection**.

Step 3 Configure the parameters based on **Table 4-10**.

Figure 4-5 Create Cloud Connection



Create Cloud Connection

* Name: cloudconnect

* Enterprise Project: --Select-- Create Enterprise Project

* Scenario: VPC

If you select VPC here, only VPCs or virtual gateways can use this cloud connection.

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

Tag key | Tag value

You can add 20 more tags.

Description: 0/255

Table 4-10 Parameters for creating a cloud connection

Parameter	Example Value	Description
Name		Specifies the cloud connection name. The name can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.
Enterprise Project		Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.
Scenario		**VPC**: VPCs or virtual gateways can use this cloud connection.
Tag		Identifies the cloud connection. A tag consists of a key and a value. You can add 20 tags to a cloud connection. **NOTE** If a predefined tag has been created on Tag Management Service (TMS), you can directly select the corresponding tag key and value. For details about predefined tags, see **Predefined Tags**.

Parameter	Example Value	Description
Description		Provides supplementary information about the cloud connection. The description can contain no more than 255 characters.

Step 4 Click **OK**.

----End

Step 3: Load Network Instances

Load the VPCs that need to communicate with each other to the created cloud connection.

Step 1 Locate the created cloud connection from the cloud connection list. Click its name to go to the **Basic Information** tab.

Step 2 On the **Network Instances** tab, click **Load Network Instance**.

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

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

NOTE

After the VPCs are connected over the cloud connection, they are on the same network. You can view the routes of each VPC on the **Route Information** tab.

----End

Step 4: Buy Bandwidth Packages

By default, Cloud Connect provides 10 kbit/s of bandwidth for testing cross-region network connectivity.

To ensure normal communication, you need to purchase two bandwidth packages and bind them to the cloud connection.

Step 1 In the cloud connection list, click the name (**CloudConnect**) of the cloud connection.

Step 2 On the **Bandwidth Packages** tab, click **Buy Bandwidth Package**.

Step 3 On the displayed page, configure the name, billing mode, applicability, geographic regions, bandwidth size, and required duration, enable auto renewal (if required), and then bind the bandwidth package to the cloud connection. Select **Across Geographic Region** for **Applicability** because the four VPCs are in three geographic regions.

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

2. To enable communication between CN East-Shanghai1 and AF-Johannesburg, 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**.

Step 4 Confirm the configuration and click **Pay Now**.

Step 5 Click **OK**.

View the bandwidth package in the bandwidth package list. If the status changes to **Normal**, the purchase is successful.

On the **Bandwidth Packages** tab, you can view the purchased bandwidth packages and their details, such as the billing mode, order information, the cloud connection, used bandwidth, and remaining bandwidth. You can also modify, unbind, renew, and unsubscribe from the bandwidth packages.

----End

Step 5: Assign Inter-Region Bandwidths

Assign bandwidth from each purchased bandwidth package for communication between the VPCs.

Step 1 Click the name of the created cloud connection to go to the details page. On the **Inter-Region Bandwidths** tab, click **Assign Inter-Region Bandwidth**.

Step 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 steps to assign 2 Mbit/s of bandwidth for communication between CN East-Shanghai1 and AF-Johannesburg.

Step 3 View the assigned bandwidth on the **Inter-Region Bandwidths** tab.

Now, the VPCs can communicate with each other.

NOTE

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

----End

5 Connecting VPCs in Different Accounts

Scenarios

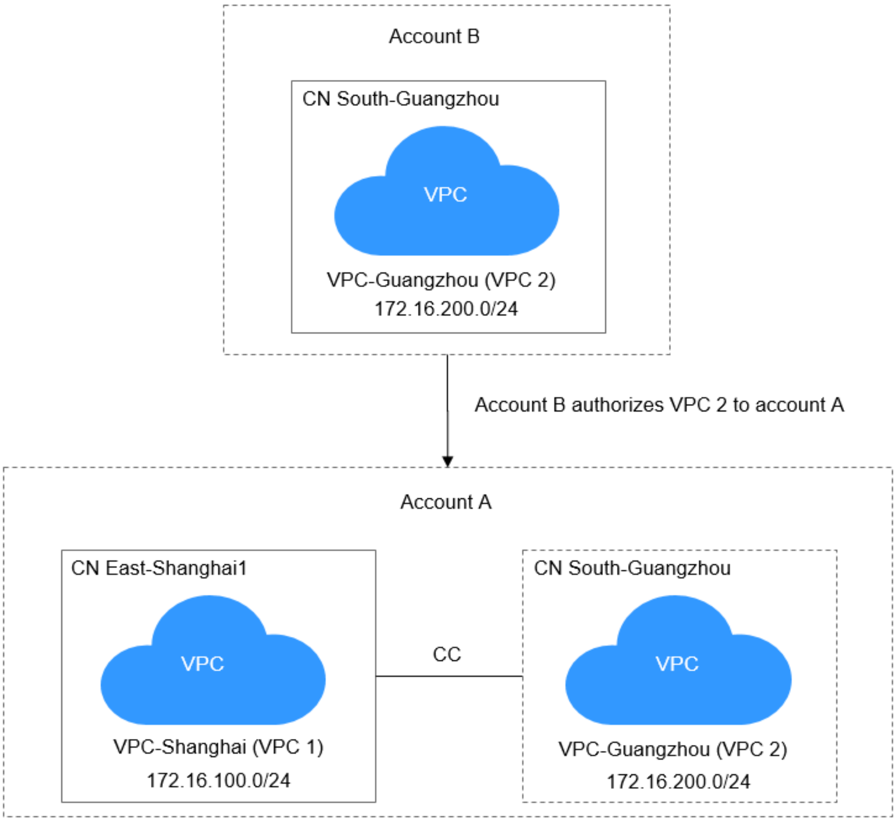
You can load the VPCs in other accounts to your own cloud connection so that these VPCs can communicate with the VPCs in your account.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

Figure 5-1 shows an example.

Figure 5-1 Connecting VPCs in different accounts



NOTE

- Account A: This is your account. You need to ask the other account (account B) to allow you to load VPC 2 to your cloud connection.
- Account B: This is the other account that grants you the permission to load VPC 2 to your cloud connection.

  (If multiple VPCs in account B need to communicate with each other across regions, you can request permission to load all these VPCs to your cloud connection.)
- You load VPC 1 and VPC 2 to your cloud connection to enable the two VPCs to communicate with each other. The other user does not need to create a cloud connection, purchase a bandwidth package, or assign an inter-region bandwidth.

Prerequisites

You have the permissions of **Tenant Guest**, **VPC Administrator**, and **Cross Connect Administrator** for the region where the VPC in the other account 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 in your account, ask this other user to create another VPC in their account, and ensure that CIDR blocks of the two VPCs do not conflict with each other.

VPC in your account: 172.16.100.0/24

VPC in the other account: 172.16.200.0/24

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

Step 2 Create a cloud connection.

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

Step 3 Ask the other user to allow you to load VPC 2 to your cloud connection.

For details, see **Allowing Other Accounts to Load Your VPCs**.

Step 4 Load the two VPCs to your cloud connection.

For details about how to load a VPC of the other user, see **Loading the VPCs of Other Accounts**.

For details about how to load the VPC in your account, see **Loading a Network Instance**.

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

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

Step 6 Assign an inter-region bandwidth.

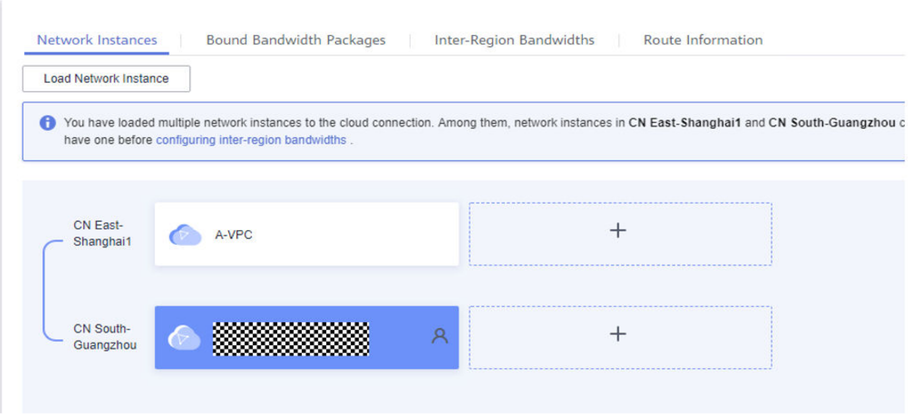
For details, see **Assigning Inter-Region Bandwidth**.

----End

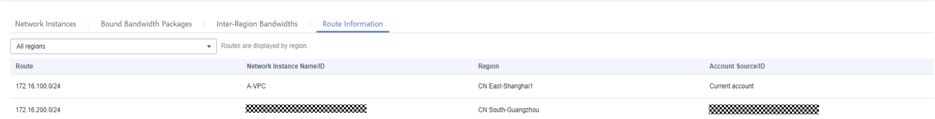
Verification

View the routes of the cloud connection and verify these VPCs can communicate with each other.

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



You have loaded multiple network instances to the cloud connection. Among them, network instances in **CN East-Shanghai1** and **CN South-Guangzhou** c
have one before configuring inter-region bandwidths .



Routes are displayed by region.

Route	Network Instance Name/ID	Region	Account Source/ID
172.16.100.0/24	A-VPC	CN East-Shanghai1	Current account
172.16.200.0/24	[redacted]	CN South-Guangzhou	[redacted]

6 Using a Cloud Connection and SNAT to Enable Private Networks to Access the Internet

Scenario

When customers require high-speed Internet access from their on-premises data centers to locations outside the Chinese mainland, they can use VPN, Cloud Connect, NAT Gateway (SNAT rules), and EIP.

For example, these services can enable fast access to services in Africa, Europe, or America.

NOTE

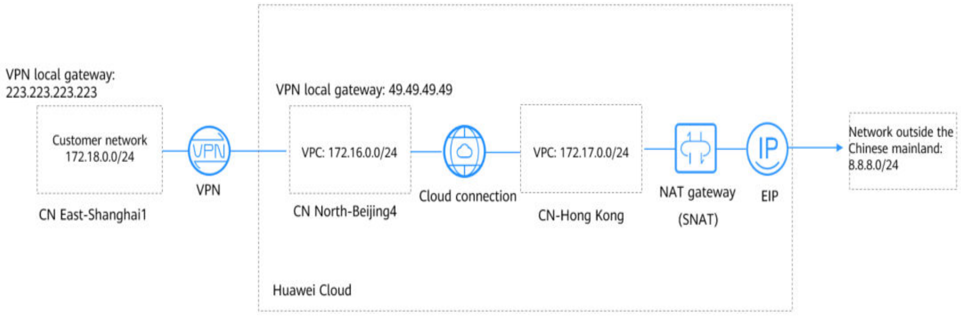
For details about the regions where cloud connections are available, see **Region Availability**.

Use Cases

1. Using VPN to connect a customer's on-premises data center to a VPC in CN North-Beijing4
2. Using a cloud connection to connect the VPC in CN North-Beijing4 to a VPC in CN-Hong Kong for network acceleration
3. Purchasing NAT gateway in CN-Hong Kong, and adding an SNAT rule to enable on-premises servers to share the EIP to access the Internet outside the Chinese mainland

Figure 6-1 shows an example.

Figure 6-1 Enabling access to the Internet



NOTE

- In this solution, the network in CN East-Shanghai1 represents the on-premises data center.
- The CIDR block of the Internet outside the Chinese mainland is 8.8.8.0/24, and 8.8.8.8 is the only IP address used for testing.

Advantages

Cross-border connectivity and accelerated network access provide better user experience.

Constraints

The user account needs cross-border permissions. Otherwise, the user needs to authorize the current VPCs to an account with the cross-border permissions to create a cloud connection.

Resource Planning

Table 6-1 Resources required

Resource	Resource Name	Description	Quantity
VPC	VPC-Test01	Region: CN East-Shanghai1 CIDR block: 172.18.0.0/24 172.18.0.0/24 represents the on-premises network.	1
	VPC-Test02	Region: CN North-Beijing4 CIDR block: 172.16.0.0/24	1
	VPC-Test03	Region: CN-Hong Kong CIDR block: 172.17.0.0/24	1
EIP	EIP-Test	Region: CN-Hong Kong	1
NAT gateway	NAT-Test	You need to purchase it in **VPC-Test03** and use EIP **EIP-Test**.	1

Resource	Resource Name	Description	Quantity
VPN gateway	VPN-GW-Test01	Region: CN North-Beijing4 Local gateway: 49.49.49.49	1
	VPN-GW-Test02	Region: CN East-Shanghai1 Local gateway: 223.223.223.223	1
VPN connection	VPN-Test01	It is created to connect to **VPN-GW-Test01**.	1
	VPN-Test02	It is created to connect to **VPN-GW-Test02**.	1
Cloud connection	CC-Test	It enables cross-region access between CN North-Beijing4 and CN-Hong Kong and accelerates network access.	1
ECS	ECS-Test01	Region: CN East-Shanghai1 Private IP address: 172.18.0.3	1
	ECS-Test02	Region: CN East-Beijing4 Private IP address: 172.16.0.3	1
	ECS-Test03	Region: CN-Hong Kong region Private IP address: 172.17.0.3	1

Process

1. **Create VPCs**.
2. **Create two VPN connections**.
3. **Create a cloud connection.**
4. **Buy three ECSs**.
5. **Buy an EIP and a NAT gateway**.

Procedure

Step 1 Create VPCs.

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

Ensure that the VPC CIDR blocks do not conflict with each other.

- VPC in CN East-Shanghai1 (**VPC-Test01**): 172.18.0.0/24
- VPC in CN North-Beijing4 (**VPC-Test02**): 172.16.0.0/24
- VPC in the CN-Hong Kong (**VPC-Test03**): 172.17.0.0/24

Step 2 Create two VPN connections.

Create **VPN-GW-Test01** in CN North-Beijing4 and buy **VPN-Test01**.

Create **VPN-GW-Test02** in CN East-Shanghai1 and buy **VPN-Test02**.

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

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

- In 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
- In 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 configuring the VPN connection between CN North-Beijing4 and CN East-Shanghai1, you need to ensure that local CIDR blocks in CN North-Beijing4 and remote subnets (8.8.8.0/24) in CN East-Shanghai1 are included so that these subnets can access the Internet outside of the Chinese mainland.

Step 3 Create a cloud connection.

1. Create a cloud connection (**CC-Test**).

   For details, see **Creating a Cloud Connection**.
2. Load the three VPCs to the created cloud connection.

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

   For details, see **Adding Custom CIDR Blocks for a Cloud Connection**.
   - When you load the VPC in CN North-Beijing4, you need to add CIDR blocks 172.18.0.0/24 and 172.16.0.0/24.
   - When you load the VPC in CN-Hong Kong, you need to add CIDR blocks 172.17.0.0/24 and 8.8.8.0/24.

   NOTE

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

   By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity. You need to buy a bandwidth package to ensure normal communication across regions.

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

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

Step 4 Buy three ECSs.

Buy one ECS in each of the following regions: CN East-Shanghai1, CN North-Beijing4, and CN-Hong Kong.

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

- Private IP address of the ECS (**ECS-Test01**) in CN East-Shanghai1: 172.18.0.3
- Private IP address of the ECS (**ECS-Test02**) in CN North-Beijing4: 172.16.0.3
- Private IP address of the ECS (**ECS-Test03**) in CN-Hong Kong: 172.17.0.3

Step 5 Buy an EIP and a NAT gateway.

Buy an EIP (**EIP-Test**) in the CN-Hong Kong region, buy a public NAT gateway (**NAT-Test**), and add an SNAT rule for each of 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 connection/Cloud connection CIDR blocks: 172.18.0.0/24 and 172.16.0.0/24

NOTE

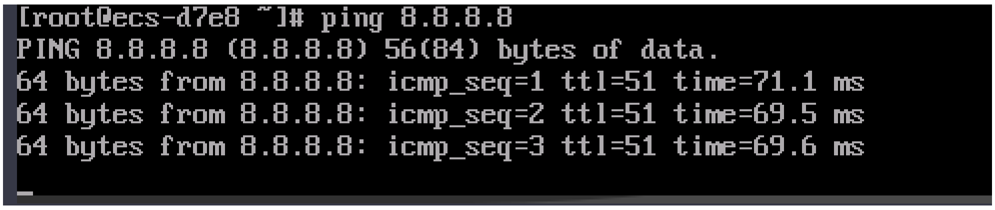
SNAT rules allow servers in private networks to access the Internet (8.8.8.0/24) outside the Chinese mainland.

----End

Verification

Test the network connectivity.

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



```
[root@ecs-d7e8 ~]# ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=51 time=71.1 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=51 time=69.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=51 time=69.6 ms
_
```

7 Using a Cloud Connection and DNAT to Enable the Internet to Access Private Networks

Scenarios

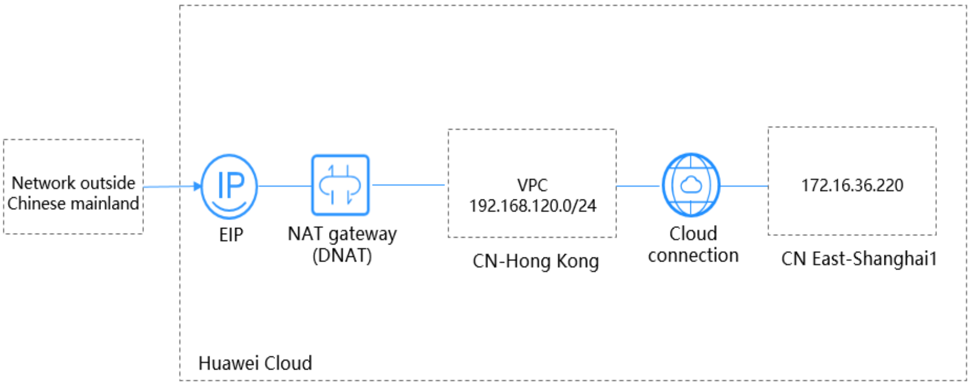
- This practice provides detailed operations for the Internet outside the Chinese mainland to access private networks.
- DNAT rules are required so that ECSs in the VPCs in the Chinese mainland can provide services accessible from the Internet.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

Figure 7-1 shows an example.

Figure 7-1 Enabling access from the Internet



NOTE

In this practice, suppose that the VPC in CN East-Shanghai1 is the on-premises network.

The CIDR block of the Internet outside the Chinese mainland is 0.0.0.0/0.

Your account must have the permission for cross-border communication. If your account does not have the permission, you can ask the other user with the required permission 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 Create a cloud connection.

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 Custom CIDR Blocks for a Cloud Connection**.

   When you load the VPC in CN-Hong Kong, you need to add the custom CIDR block 0.0.0.0/0.

   NOTE

   You need to add the default route 0.0.0.0/0 to allow access from the NAT gateway.

4. Buy a bandwidth package.

   By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity. You need to buy a bandwidth package to ensure normal communication across regions.

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

5. Assign an inter-region bandwidth.

   For details, see **Assigning an 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.

In CN-Hong Kong, buy an EIP and a public 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

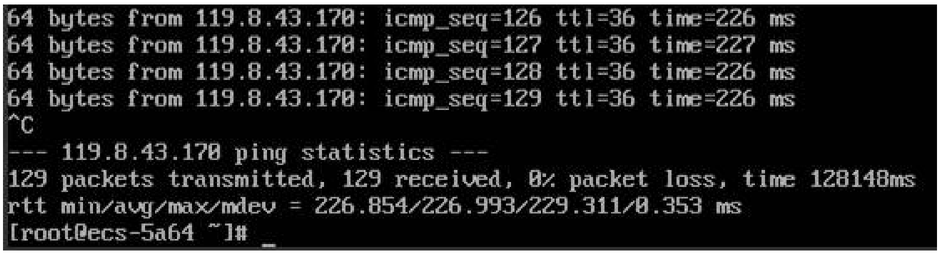
The DNAT rule enables the ECS to provide services accessible from the Internet.

----End

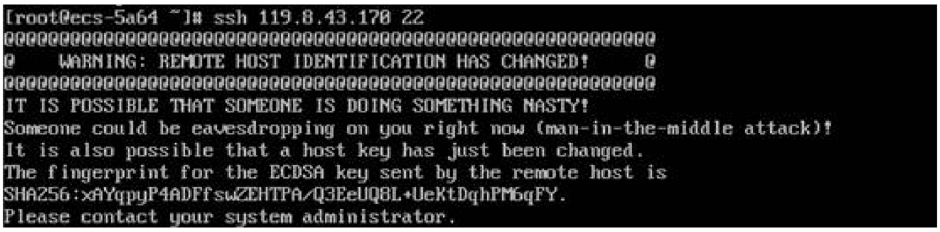
Verification

Test network connectivity.

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



```
64 bytes from 119.8.43.170: icmp_seq=126 ttl=36 time=226 ms
64 bytes from 119.8.43.170: icmp_seq=127 ttl=36 time=227 ms
64 bytes from 119.8.43.170: icmp_seq=128 ttl=36 time=226 ms
64 bytes from 119.8.43.170: icmp_seq=129 ttl=36 time=226 ms
^C
--- 119.8.43.170 ping statistics ---
129 packets transmitted, 129 received, 0% packet loss, time 128148ms
rtt min/avg/max/mdev = 226.854/226.993/229.311/0.353 ms
[root@ecs-5a64 ~]# _
```



```
[root@ecs-5a64 ~]# ssh 119.8.43.170 22
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ECDSA key sent by the remote host is
SHA256:xAYqpyP4ADFfswZEHTPA/Q3EeUQ8L+UeKtDqhPM6qFY.
Please contact your system administrator.
```

8 Using a Cloud Connection and DNAT to Improve the Web Delivery Across Regions

Scenarios

This practice provides detailed operations for improve web delivery across regions.

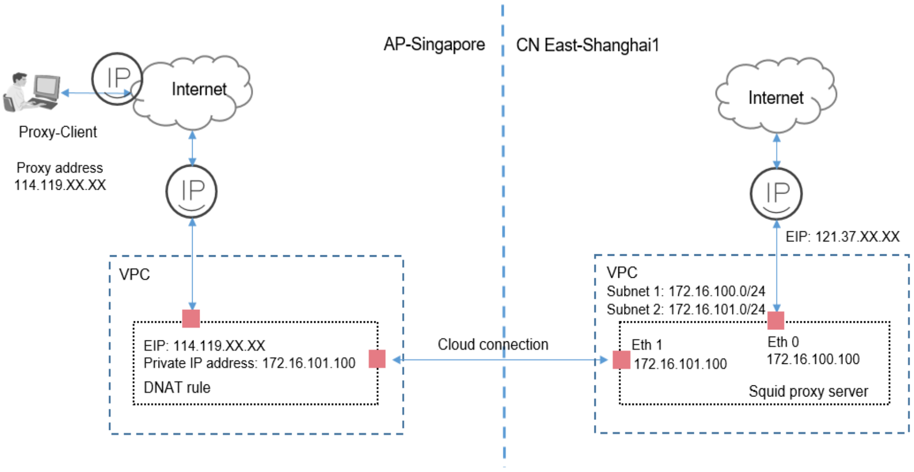
Components required in this practice include a NAT gateway, a cloud connection, and a web proxy server.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

Figure 8-1 shows an example.

Figure 8-1 Improving web delivery across regions



NOTE

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

Proxy-Client: Use a Windows server with a 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 network interface (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 HTTP 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**.

The VPC in CN East-Shanghai1 has two subnets:

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

Step 2 Create a cloud connection.

1. Create a cloud connection.

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

2. Load the two VPCs.

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

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

3. Add custom CIDR blocks.

   When you load the VPC in AP-Singapore, you need to add the custom CIDR block 0.0.0.0/0.

   For details, see **Adding Custom CIDR Blocks for a Cloud Connection**.

   NOTE

   You need to add the default route 0.0.0.0/0 to allow access from the NAT gateway.

4. Buy a bandwidth package.

   By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity. You need to buy a bandwidth package to ensure normal communication across regions.

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

5. Assign an inter-region bandwidth.

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

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

- Eth 0 (for accessing the Internet): 172.16.100.100
- Eth 1 (for communicating with the NAT Gateway): 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 the Squid proxy server.

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 the proxy service.

   Configure the proxy server in a secure and reliable manner based on 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. In AP-Singapore, buy an EIP and a public 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: 172.16.101.100 (IP address of Eth 1)

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 communicating with the NAT gateway.

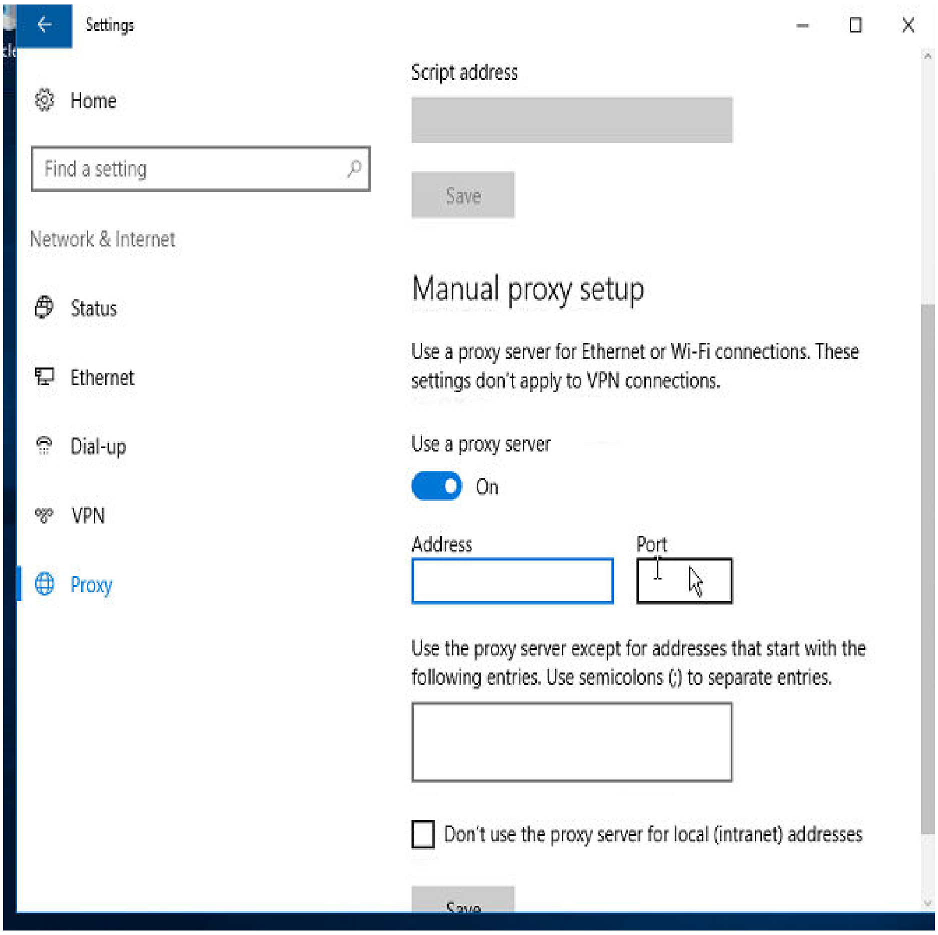
The DNAT rule enables the Squid proxy server to provide services accessible from Proxy-Client on the Internet.

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 8-2 Proxy configuration



Manual proxy setup

Use a proxy server for Ethernet or Wi-Fi connections. These settings don't apply to VPN connections.

Use a proxy server

● On

Address

Port

Use the proxy server except for addresses that start with the following entries. Use semicolons (;) to separate entries.

□ Don't use the proxy server for local (intranet) addresses

NOTE

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

5. Click **Save**.

----End

Verification

Access the website from Proxy-Client to check whether access is normal.

9 Using a Cloud Connection and a VPC Peering Connection to Connect VPCs Across Regions

Scenarios

This practice provides detailed operations for you to enable communication between VPCs in different regions using a VPC Peering connection and a cloud connection.

NOTE

For details about the regions where cloud connections are available, see **Region Availability**.

In the following figure, CN East-Shanghai1 and CN South-Guangzhou each have three VPCs, one production VPC, one office VPC, and one transit VPC:

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

Figure 9-1 Network topology

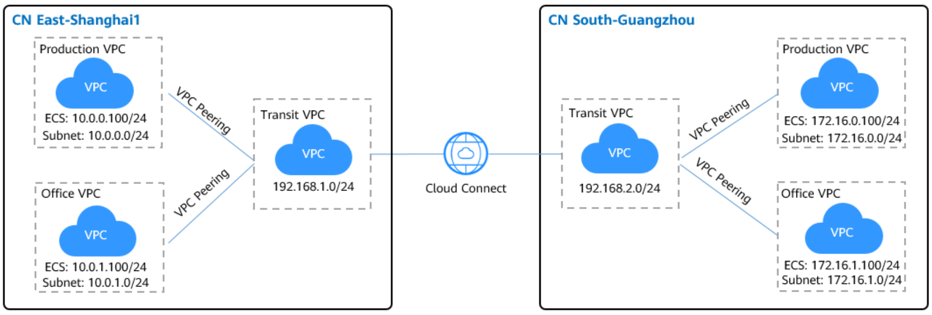


Table 9-1 Service configuration

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 the same account or in different accounts.	**Creating a VPC Peering Connection to Connect Another VPC in the Same Account** **Creating a VPC Peering Connection to Connect a VPC in Another Account**
Cloud connection	VPCs are in different regions.	Create a cloud connection to connect the VPCs across regions. The VPCs can be in the same account or in different accounts.	**Using a Cloud Connection to Connect VPCs in Different Regions**

⚠ CAUTION

To connect the VPCs using a VPC Peering connection and a cloud connection, ensure that the subnets in the VPCs do not overlap or conflict.

Prerequisites

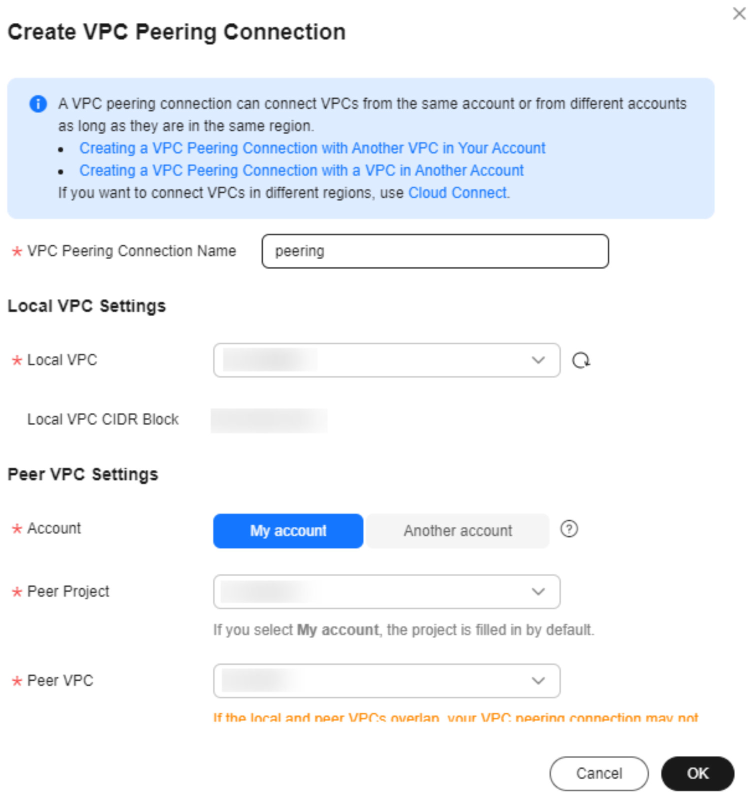
- You have a Huawei Cloud account, and the Huawei Cloud account has been configured with operation permissions of related services.
- The account balance is sufficient to purchase the required resources, such as bandwidth packages and ECSs.
- The VPCs and subnets that need to communicate with each other have been created.

Procedure

Step 1 Configure VPC Peering.

1. Create a VPC peering connection.
   a. Go to the **VPC Peering Connections** page.
   b. In the upper right corner of the page, click **Create VPC Peering Connection**.
      The **Create VPC Peering Connection** page is displayed.
   c. Configure the parameters based on **Table 9-2**. Select **My account**.

Figure 9-2 Creating a VPC peering connection



Create VPC Peering Connection

A VPC peering connection can connect VPCs from the same account or from different accounts as long as they are in the same region.

- Creating a VPC Peering Connection with Another VPC in Your Account
- Creating a VPC Peering Connection with a VPC in Another Account

If you want to connect VPCs in different regions, use Cloud Connect.

* VPC Peering Connection Name: peering

Local VPC Settings

* Local VPC

Local VPC CIDR Block

Peer VPC Settings

* Account: My account | Another account

* Peer Project

If you select **My account**, the project is filled in by default.

* Peer VPC

If the local and peer VPCs overlap, your VPC peering connection may not

Table 9-2 Parameters required for creating a VPC Peering connection

Parameter	Description
Name	Specifies the name of the VPC peering connection. The name contains a maximum of 64 characters and consists of letters, digits, hyphens (-), and underscores (_).
Local VPC	Specifies the VPC you want to connect over the VPC peering connection.
Local VPC CIDR Block	Specifies the CIDR block for the local VPC.
Account	Specifies whether the VPC to be peered with are from your account or from another account. – **My account**: The VPC is from your account. – **Another account**: The VPC is from another account.
Peer Project	Specifies the peer project name. The name of the current project is used by default.

Parameter	Description
Peer VPC	Specifies the other VPC you want to connect. You can select one from the drop-down list if the VPC peering connection is created between two VPCs in your own account.
Peer VPC CIDR Block	Specifies the CIDR block for the peer VPC. The local and peer VPCs cannot have identical or overlapping CIDR blocks. Otherwise, the routes added for the VPC peering connection may not take effect.
Description	(Optional) Provides supplementary information about the VPC peering connection. The description can contain no more than 255 characters and cannot contain angle brackets (<>).

d. Click **OK**.

2. Add routes for the VPC peering connection.

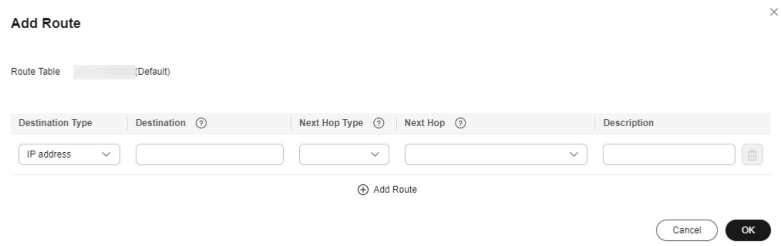
   If you request a VPC peering connection with another VPC in your own account, the system automatically accepts the request. You still need to add local and peer routes on the **Route Tables** page for the VPC peering connection.

   a. Go to the **VPC console**.

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

   c. Search for or create a route table for the local VPC and add routes for the local VPC. **Table 9-3** describes the parameters.

Figure 9-3 Adding local route



Add Route

Route Table (Default)

Destination Type	Destination	Next Hop Type	Next Hop	Description
IP address				

Table 9-3 Parameters required for adding routes for the VPC peering connection

Parameter	Description
Destination	Specifies the CIDR block for the peer VPC.
Next Hop Type	Specifies the next hop type. Select **VPC peering connection**.

Parameter	Description
Next Hop	Specifies the next hop address. Select the created VPC peering connection.
Description	(Optional) Provides supplementary information about the route. The description can contain no more than 255 characters and cannot contain angle brackets (<>).

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

Table 9-4 Parameters required for adding routes for the VPC peering connection

Parameter	Description
Destination	Specifies the CIDR block for the local VPC.
Next Hop Type	Specifies the next hop type. Select **VPC peering connection**.
Next Hop	Specifies the next hop address. Select the created VPC peering connection.
Description	(Optional) Provides supplementary information about the route. The description can contain no more than 255 characters and cannot contain angle brackets (<>).

e. 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 Create a cloud connection.

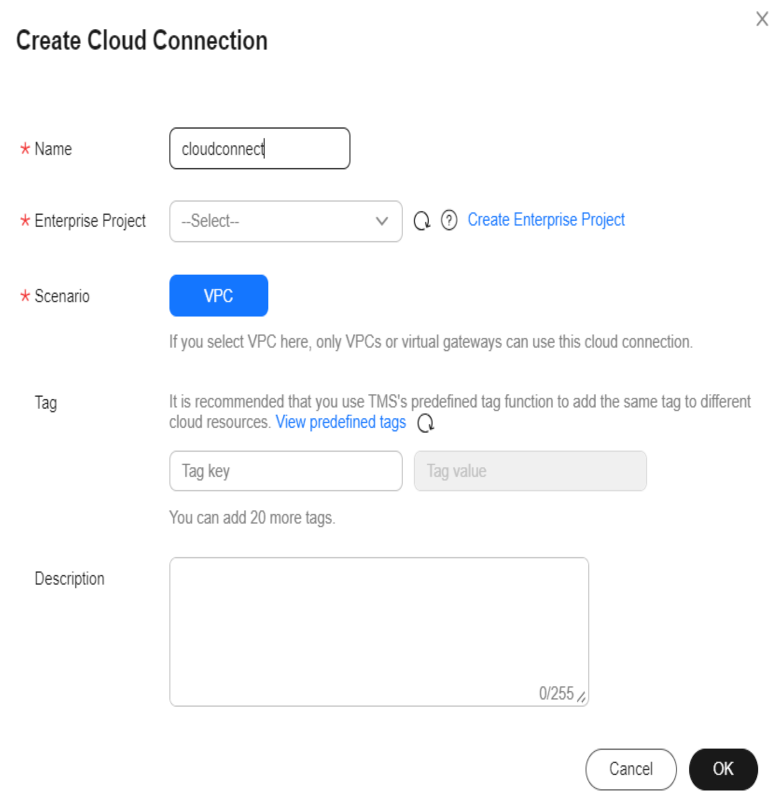
1. Create a cloud connection.

a. Go to the **Cloud Connections** page.

b. In the upper right corner of the page, click **Create Cloud Connection**.

c. Configure the parameters based on **Table 9-5**.

Figure 9-4 Create Cloud Connection



Create Cloud Connection

* Name: cloudconnect

* Enterprise Project: --Select--

* Scenario: VPC

If you select VPC here, only VPCs or virtual gateways can use this cloud connection.

Tag: It is recommended that you use TMS's predefined tag function to add the same tag to different cloud resources. View predefined tags

You can add 20 more tags.

Description: 0/255

Table 9-5 Parameters for creating a cloud connection

Parameter	Description
Name	Specifies the cloud connection name.
Enterprise Project	Specifies the enterprise project for managing the cloud connection. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**. For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**.
Scenario	Specifies whether the cloud connection is used to connect VPCs or enterprise routers. If you select **VPC** here, only VPCs or virtual gateways can use this cloud connection.

Parameter	Description
Tag	Identifies the cloud connection. A tag consists of a key and a value. You can add 20 tags to a cloud connection. **NOTE** If you have configured tag policies for Cloud Connect, add tags to cloud connections based on the tag policies. If you add a tag that does not comply with the tag policies, cloud connections may fail to be created. Contact your administrator to learn more about tag policies.
Description	(Optional) Provides supplementary information about the cloud connection. The description can contain no more than 255 characters and cannot contain angle brackets (<>).

d. Click **OK**.

2. Load network instances.

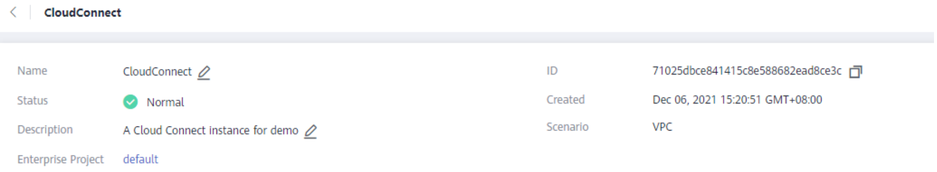
   Load the transit VPC in CN East-Shanghai1 to the created cloud connection.

   a. In the cloud connection list, click the name (**CloudConnect**) of the 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**, **Bandwidth Packages**, **Inter-Region Bandwidths**, and **Route Information**.

      Figure 9-5 Cloud connection details



CloudConnect

Name CloudConnect

Status Normal

Description A Cloud Connect instance for demo

Enterprise Project default

ID 71025dbce841415c8e588682ead8ce3c

Created Dec 06, 2021 15:20:51 GMT+08:00

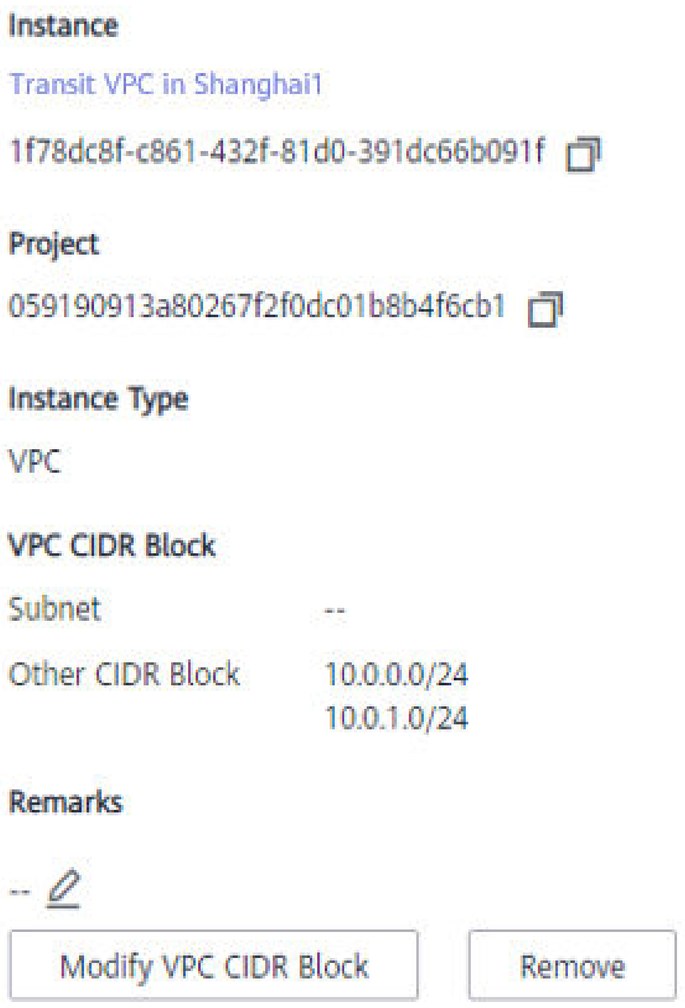
Scenario VPC

   b. Click **Network Instances**.

   c. Click **Load Network Instance**.

   d. Configure the parameters.

Figure 9-6 Network instance details



Instance

Transit VPC in Shanghai1

1f78dc8f-c861-432f-81d0-391dc66b091f

Project

059190913a80267f2f0dc01b8b4f6cb1

Instance Type

VPC

VPC CIDR Block

Subnet	--
Other CIDR Block	10.0.0.0/24 10.0.1.0/24

Remarks

--

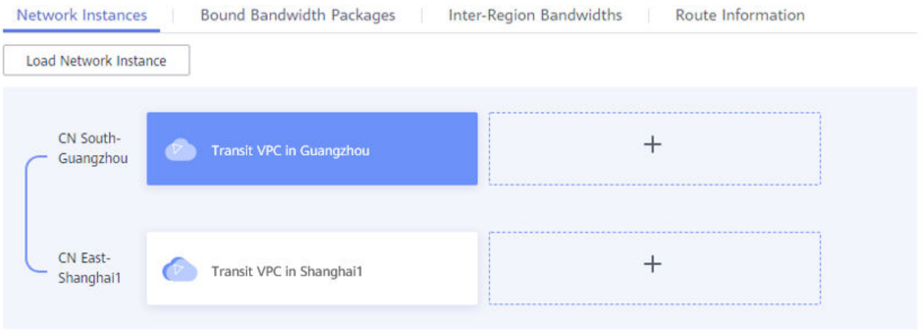
NOTE

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.

e. Click **OK**.

f. 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 9-7 Loading another VPC



NOTE

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

3. Buy a bandwidth package.

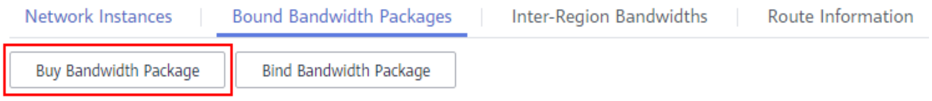
   By default, Cloud Connect provides 10 kbit/s of bandwidth for testing cross-region network connectivity.

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

   a. In the cloud connection list, click the name (**CloudConnect**) of the cloud connection.

   b. On the **Bandwidth Packages** tab, click **Buy Bandwidth Package**.

   Figure 9-8 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**.

   d. Click **Buy Now**.

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

   f. Click **OK**.

   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 the cloud connection.

   NOTE

   In the navigation pane, choose **Bandwidth Packages**. On the **Bandwidth Packages** package, you can view the purchased bandwidth package and its details, such as the billing mode, order information, the cloud connection, used bandwidth, and remaining bandwidth. You can also modify, unbind, renew, and unsubscribe from the bandwidth package.

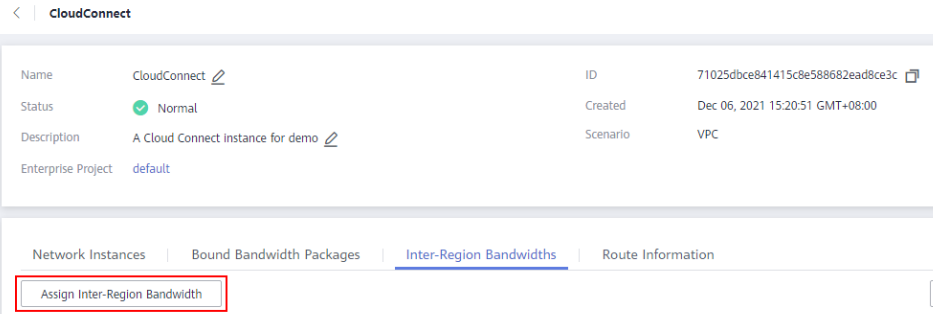
4. Assign an inter-region bandwidth.

Assign bandwidth from the purchased bandwidth package for communication between the VPCs.

a. In the cloud connection list, click the name (**CloudConnect**) of the cloud connection.

b. On the **Inter-Region Bandwidths** tab, click **Assign Inter-Region Bandwidth**.

Figure 9-9 Assigning inter-region bandwidth



Name	CloudConnect	ID	71025dbce841415c8e588682ead8ce3c
Status	Normal	Created	Dec 06, 2021 15:20:51 GMT+08:00
Description	A Cloud Connect instance for demo	Scenario	VPC
Enterprise Project	default		

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.

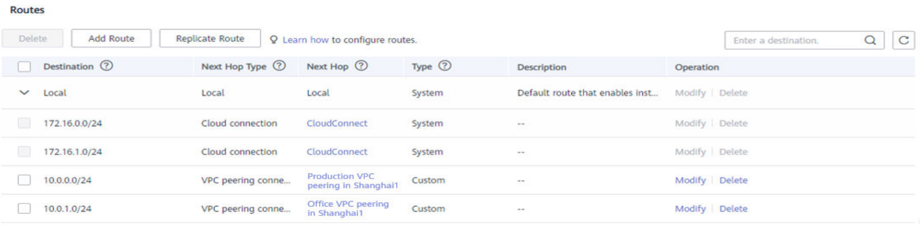
d. View the assigned bandwidth on the **Inter-Region Bandwidths** tab.

----End

Verification

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

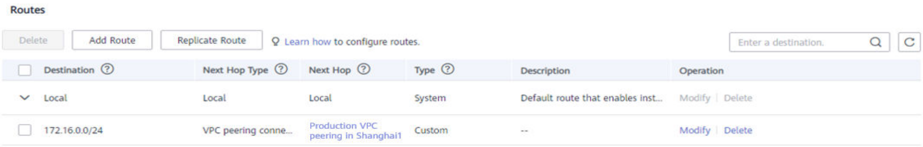
Figure 9-10 Route table of the transit VPC in CN East-Shanghai1



Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables inst...	Modify | Delete
172.16.0.0/24	Cloud connection	CloudConnect	System	--	Modify | Delete
172.16.1.0/24	Cloud connection	CloudConnect	System	--	Modify | Delete
10.0.0.0/24	VPC peering conne...	Production VPC peering in Shanghai1	Custom	--	Modify | Delete
10.0.1.0/24	VPC peering conne...	Office VPC peering in Shanghai1	Custom	--	Modify | Delete

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

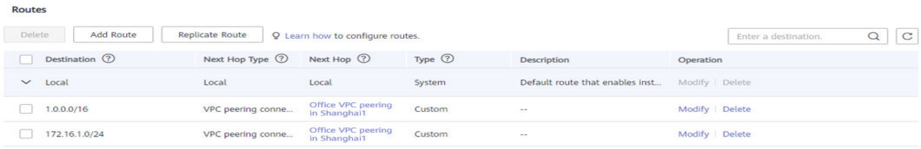
Figure 9-11 Route table of the production VPC in CN East-Shanghai1



Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables inst...	Modify | Delete
172.16.0.0/24	VPC peering conne...	Production VPC peering in Shanghai1	Custom	--	Modify | Delete

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

Figure 9-12 Route table of the office VPC in CN East-Shanghai1



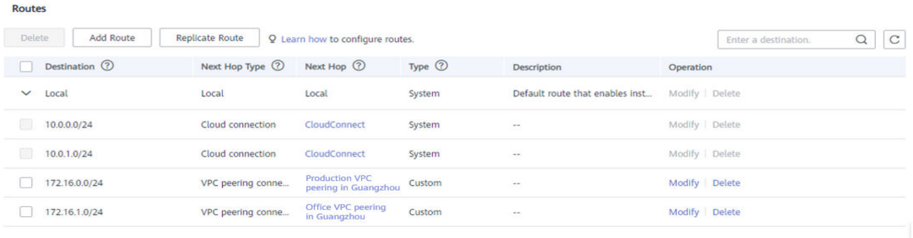
Routes

Delete | Add Route | Replicate Route | Learn how to configure routes. | Enter a destination.

Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables inst...	Modify | Delete
1.0.0.0/16	VPC peering conne...	Office VPC peering in Shanghai1	Custom	--	Modify | Delete
172.16.1.0/24	VPC peering conne...	Office VPC peering in Shanghai1	Custom	--	Modify | Delete

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

Figure 9-13 Route table of the transit VPC in CN South-Guangzhou



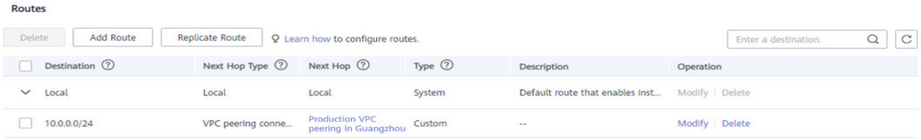
Routes

Delete | Add Route | Replicate Route | Learn how to configure routes. | Enter a destination.

Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables inst...	Modify | Delete
10.0.0.0/24	Cloud connection	CloudConnect	System	--	Modify | Delete
10.0.1.0/24	Cloud connection	CloudConnect	System	--	Modify | Delete
172.16.0.0/24	VPC peering conne...	Production VPC peering in Guangzhou	Custom	--	Modify | Delete
172.16.1.0/24	VPC peering conne...	Office VPC peering in Guangzhou	Custom	--	Modify | Delete

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

Figure 9-14 Route table of the production VPC in CN South-Guangzhou



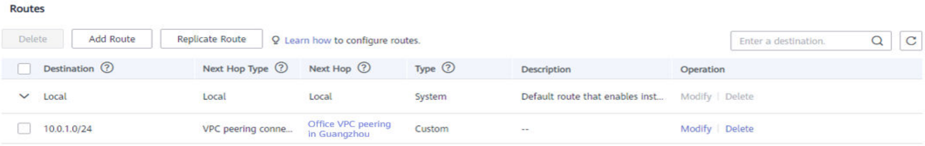
Routes

Delete | Add Route | Replicate Route | Learn how to configure routes. | Enter a destination.

Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables inst...	Modify | Delete
10.0.0.0/24	VPC peering conne...	Production VPC peering in Guangzhou	Custom	--	Modify | Delete

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

Figure 9-15 Route table of the office VPC in CN South-Guangzhou



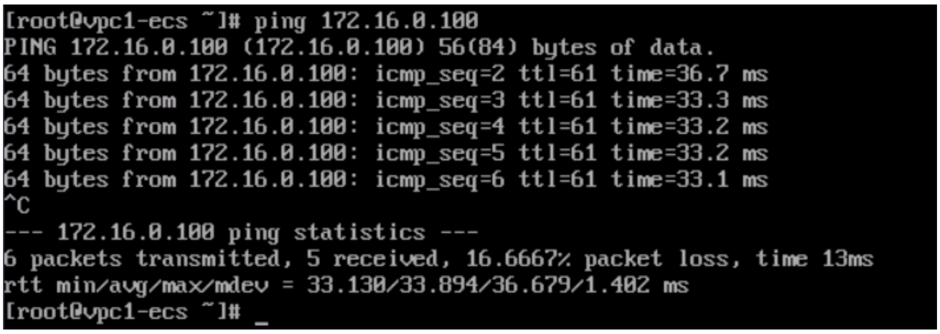
Routes

Delete | Add Route | Replicate Route | Learn how to configure routes. | Enter a destination.

Destination	Next Hop Type	Next Hop	Type	Description	Operation
Local	Local	Local	System	Default route that enables inst...	Modify | Delete
10.0.1.0/24	VPC peering conne...	Office VPC peering in Guangzhou	Custom	--	Modify | Delete

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

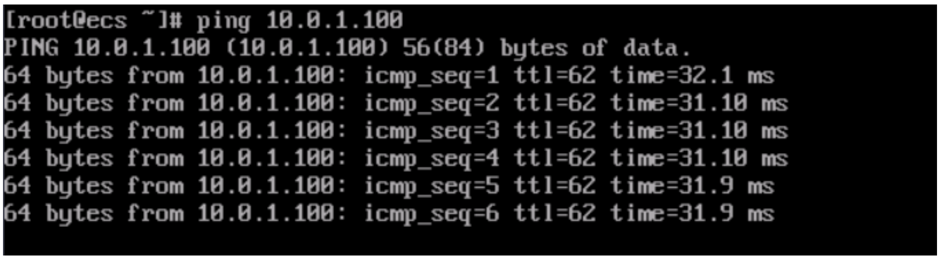
Figure 9-16 Pinging two ECSs



```
[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 9-17 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
```