

**Cloud Connect**

# **User Guide**

**Issue**            01  
**Date**             2025-05-30



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2025. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

The purchased products, services and features are stipulated by the contract made between Huawei Cloud 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.

## **Huawei Cloud Computing Technologies Co., Ltd.**

Address: Huawei Cloud Data Center Jiaoxinggong Road  
Qianzhong Avenue  
Gui'an New District  
Gui Zhou 550029  
People's Republic of China

Website: <https://www.huaweicloud.com/intl/en-us/>

---

# Contents

---

|  |           |
|--|-----------|
| <b>1 Using a Cloud Connection to Connect VPCs in the Same Region and Account.....</b>                                  | <b>1</b>  |
| <b>2 Using a Cloud Connection to Connect VPCs in the Same Account But Different Regions.....</b>                       | <b>10</b> |
| <b>3 Using a Central Network and Enterprise Routers to Connect VPCs in the Same Account But Different Regions.....</b> | <b>25</b> |
| <b>4 Common Practices.....</b>   | <b>38</b> |

# 1 Using a Cloud Connection to Connect VPCs in the Same Region and Account

Connect the VPCs in the same account and the same region using a cloud connection.

 **NOTE**

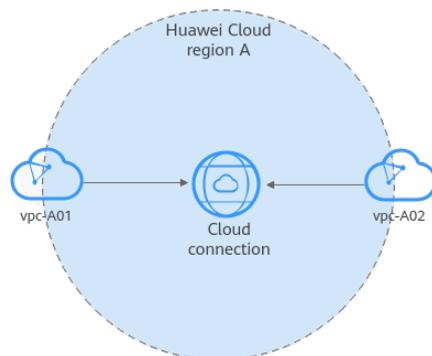
For details about the regions where cloud connections are available, see [Region Availability](#).

## Solution Architecture

Two VPCs in the same region need to communicate with each other.

You need to create a cloud connection and load both VPCs to the cloud connection.

**Figure 1-1** Communication between VPCs in the same account and same region



## Network and Resource Planning

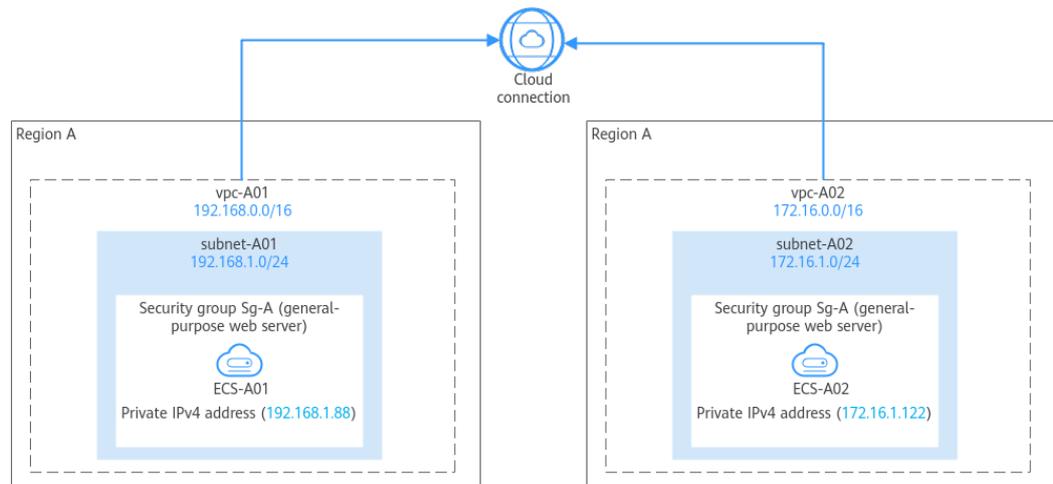
To use a cloud connection to connect VPCs in the same region, you need to:

- Plan CIDR blocks for VPCs and subnets.
- Plan the quantity, names, and main parameters of cloud resources, including VPCs and ECSs.

### Planning the Network

**Figure 1-2** and **Table 1-1** show the network planning and description for communication between VPCs in the same region.

**Figure 1-2** Network planning for communication between VPCs in the same region



**Table 1-1** Network planning for communication between VPCs in the same region

| Resource | Description  |
|----------|--|
| VPCs     | <ul style="list-style-type: none"> <li>The CIDR blocks of the VPCs to be connected cannot overlap with each other. Overlapping VPC CIDR blocks will cause route conflicts. If the VPCs have overlapping CIDR blocks, you need to modify the CIDR blocks.</li> <li>Each VPC comes with a default route table that has the default IPv4 local route, which enables subnets in the VPC to communicate with each other.</li> </ul>   |
| ECSs     | <p>In this example, two ECSs are deployed in the same VPC and region. An ECS can be only associated with a security group in the same region as the ECS. This means the two ECSs in this example can be associated with the same or different security groups in their region.</p> <ul style="list-style-type: none"> <li>Same security group: The two ECSs can communicate with each other by default and no further network configuration is required.</li> <li>Different security groups: You need to add the inbound rules in <b>Table 1-4</b> to allow access to each other. For more information about security groups, see <b>Security Group and Security Group Rule Overview</b>.</li> </ul> |

### Planning Resources

The VPCs and ECSs must be in the same region, but they can be in different AZs.

#### NOTE

The following resource details are only for your reference. You can modify them if needed.

- **Table 1-2** describes the two VPCs in detail. Their CIDR blocks cannot overlap with each other.

**Table 1-2** VPC details

| VPC     | VPC CIDR Block | Subnet Name | Subnet CIDR Block | Route Table         |
|---------|----------------|-------------|-------------------|---------------------|
| vpc-A01 | 192.168.0.0/16 | subnet-A01  | 192.168.1.0/24    | Default route table |
| vpc-A02 | 172.16.0.0/16  | subnet-A02  | 172.16.1.0/24     | Default route table |

- **Table 1-3** describes the two ECSs in detail, with each ECS in a VPC.

**Table 1-3** ECS details

| ECS Name | Image   | VPC     | Subnet     | Security Group                     | Private IP Address |
|----------|---|---------|------------|------------------------------------|--------------------|
| ECS-A01  | Public image: Huawei Cloud EulerOS 2.0 Standard Edition | vpc-A01 | subnet-A01 | Sg-A: (general-purpose web server) | 192.168.1.88       |
| ECS-A02  |   | vpc-A02 | subnet-A02 |                                    | 172.16.1.122       |

- Security group rules: If the two ECSs are in different security groups (Sg-A and Sg-B), you need to add rules to the security groups to allow traffic between the ECSs.

Set **Source** to the security group of the two ECSs to allow mutual access.

**Table 1-4** Security group rules (security group as the source)

| Security Group | Direction | Action | Type | Protocol & Port | Source | Description   |
|----------------|-----------|--------|------|-----------------|--------|---|
| Sg-A           | Inbound   | Allow  | IPv4 | All             | Sg-B   | Allows instances in Sg-B to access those in Sg-A over any IPv4 protocol and port. |
| Sg-B           | Inbound   | Allow  | IPv4 | All             | Sg-A   | Allows instances in Sg-A to access those in Sg-B over any IPv4 protocol and port. |

## Procedure

**Table 1-5** Communication between VPCs in the same account and region

| Step   | What to Do  |
|--|---|
| <b>Preparations</b>                            | Before using cloud services, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account. |
| <b>Step 1: Create a Cloud Connection</b>       | Create a cloud connection for connecting the VPCs.  |
| <b>Step 2: (Optional) Create VPCs and ECSs</b> | Create VPCs and ECSs in the same region using the same account. If you already have VPCs and ECSs, skip this step.                              |
| <b>Step 3: Load Network Instances</b>          | Load the VPCs to the cloud connection based on your network plan.   |
| <b>Step 4: Verify Network Connectivity</b>     | Log in to the ECSs and verify the network connectivity between VPCs.  |

## 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

1. Go to the **Cloud Connections** page.
2. In the upper right corner of the page, click **Create Cloud Connection**.
3. Configure the parameters based on **Table 1-6**.

**Figure 1-3** Creating a cloud connection

**Table 1-6** Parameters for creating a cloud connection

| Parameter          | Example Value | Description   |
|--------------------|---------------|---|
| Name               | cc-test       | Specifies the cloud connection name.<br>The name can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed.   |
| Enterprise Project | default       | Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.   |
| Scenario           | VPC           | <b>VPC:</b> 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.<br><b>NOTE</b><br>If a predefined tag has been created on Tag Management Service (TMS), you can directly select the corresponding tag key and value.<br>For details about predefined tags, see <a href="#">Predefined Tags</a> . |

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

4. Click **OK**.

## Step 2: (Optional) Create VPCs and ECSs

Perform the following operations to create VPCs and ECSs. If you already have VPCs and ECSs, skip this step.

### Constraints

- The CIDR blocks of the VPCs to be connected cannot overlap with each other. Overlapping VPC CIDR blocks will cause route conflicts. If the VPCs have overlapping CIDR blocks, you need to modify the CIDR blocks.
- Two ECSs in this example are in the same security group. If the ECSs are in different security groups, add rules to the security groups to allow access to each other by referring to [Table 1-4](#).

### Procedure

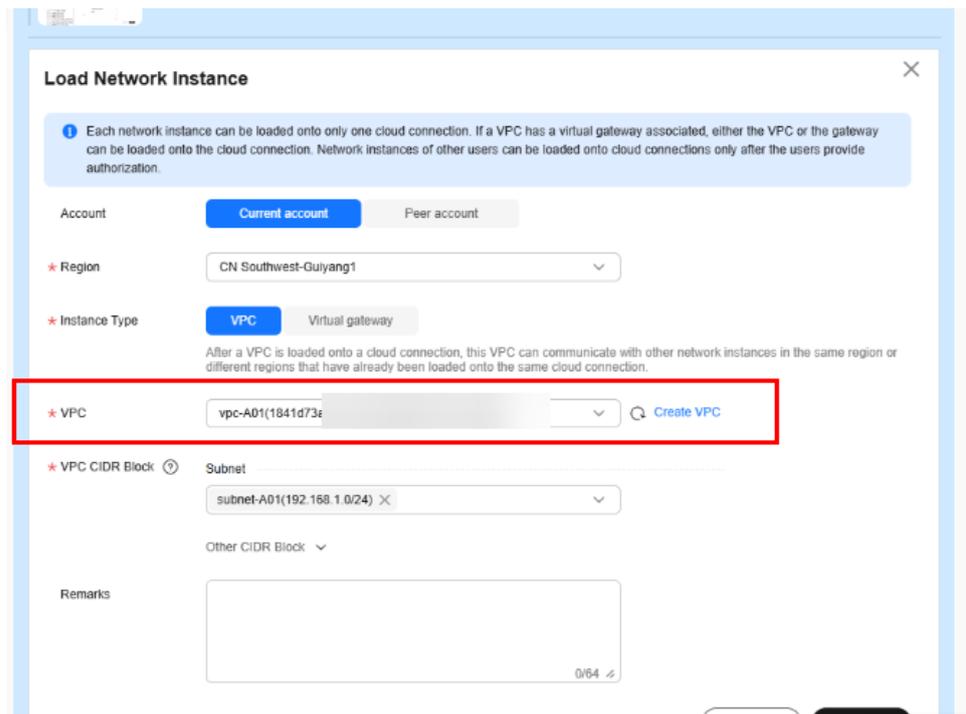
1. Create two VPCs with subnets.  
For details, see [Creating a VPC](#).  
For the details about VPCs and subnets in this example, see [Table 1-2](#).
2. Create two ECSs.  
For details, see [Purchasing a Custom ECS](#).  
For details about the ECSs in this example, see [Table 1-3](#).

## Step 3: Load Network Instances

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

1. Go to the [Cloud Connections](#) page.
2. Click the cloud connection name (for example, **cc-test**) to go to the **Basic Information** tab.
3. Click the **Network Instances** tab.
4. Click **Load Network Instance**.
5. Configure the parameters based on [Table 1-7](#) and click **OK**.

**Figure 1-4** Loading vpc-A01 in the account



**Table 1-7** Parameters for loading network instances in the same account

| Parameter     | Example Value         | Description   |
|---------------|-----------------------|---|
| Account       | Current account       | Specifies the account that provides the network instance.   |
| Region        | CN Southwest-Guiyang1 | Specifies the region where the VPC you want to connect is located.  |
| Instance Type | VPC                   | Specifies the type of the network instance that needs to be loaded to the cloud connection. There are two options: <ul style="list-style-type: none"> <li>• <b>VPC</b></li> <li>• <b>Virtual gateway</b></li> </ul> |
| VPC           | vpc-A01               | Specifies the VPC you want to load to the cloud connection.<br><br>This parameter is mandatory if you have set <b>Instance Type</b> to <b>VPC</b> .   |

| Parameter      | Example Value | Description  |
|----------------|---------------|--|
| VPC CIDR Block | subnet-A01    | Specifies the subnets in the VPC and custom CIDR blocks.<br>If you have set <b>Instance Type</b> to <b>VPC</b> , you need to configure the following two parameters: <ul style="list-style-type: none"> <li>• <b>Subnet:</b> Select one or more subnets in the VPC.</li> <li>• <b>Other CIDR Block:</b> Add one or more custom CIDR blocks as needed.</li> </ul> |
| Remarks        | -             | Provides supplementary information about the network instance.   |

- In the displayed dialog box, click **Continue Loading**. Then, click  to load vpc-A02 in the same region and the account.

**Figure 1-5** Loading vpc-A02 in the same account

**Load Network Instance**
✕

**i** 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** Peer account

\* Region CN Southwest-Guiyang1

\* Instance Type **VPC** Virtual gateway

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.

\* VPC vpc-A02(adb1ce) [Create VPC](#)

\* VPC CIDR Block Subnet

subnet-A02(172.16.1.0/24) ✕

Other CIDR Block ▼

Remarks 0/64 

Cancel OK

## Step 4: Verify Network Connectivity

Log in to each ECS and verify the network connectivity between VPCs.

- Log in to ECS-A01.

Multiple methods are available for logging in to an ECS. For details, see [Logging In to an ECS](#).

In this example, use VNC provided on the management console to log in to the ECSs.

2. Ping the other ECS to verify the network connectivity between VPCs.

**ping** <private-IP-address-of-ECS-A02>

Example command:

**ping 172.16.1.122**

If the following information is displayed, vpc-A01 and vpc-A02 are connected.

```
[root@ecs-a01 ~]# ping 172.16.1.122
PING 172.16.1.122 (172.16.1.122) 56(84) bytes of data.
64 bytes from 172.16.1.122: icmp_seq=1 ttl=62 time=1.12 ms
64 bytes from 172.16.1.122: icmp_seq=2 ttl=62 time=0.778 ms
64 bytes from 172.16.1.122: icmp_seq=3 ttl=62 time=0.691 ms
64 bytes from 172.16.1.122: icmp_seq=4 ttl=62 time=0.673 ms
64 bytes from 172.16.1.122: icmp_seq=5 ttl=62 time=0.604 ms
64 bytes from 172.16.1.122: icmp_seq=6 ttl=62 time=0.507 ms
^C
--- 172.16.1.122 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5117ms
rtt min/avg/max/mdev = 0.507/0.728/1.120/0.193 ms
[root@ecs-a01 ~]# _
```

# 2 Using a Cloud Connection to Connect VPCs in the Same Account But Different Regions

Use a cloud connection to connect VPCs in the same account but different regions.

## NOTE

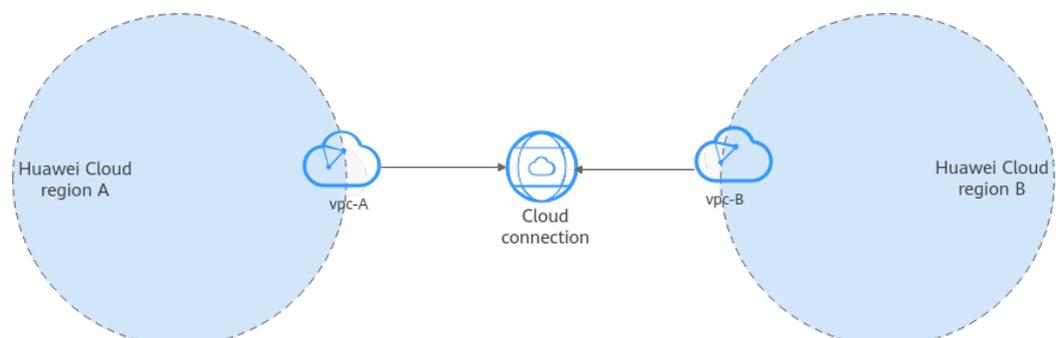
For details about the regions where cloud connections are available, see [Region Availability](#).

## Solution Architecture

You have a VPC (vpc-A) in a region (CN Southwest-Guiyang1) and another VPC (vpc-B) in a different region (CN North-Beijing4). The two VPCs need to communicate with each other.

You need to create a cloud connection and load both VPCs to the cloud connection.

**Figure 2-1** Communication between VPCs in different regions using the same account



## Network and Resource Planning

To use a cloud connection to connect VPCs in different regions, you need to:

- Plan CIDR blocks for VPCs and subnets.

- Plan the quantity, names, and main parameters of cloud resources, including VPCs and ECSs.

### Planning the Network

Figure 2-2 and Table 2-1 show the network planning and description for communication between VPCs in different regions.

Figure 2-2 Cross-region VPC network planning

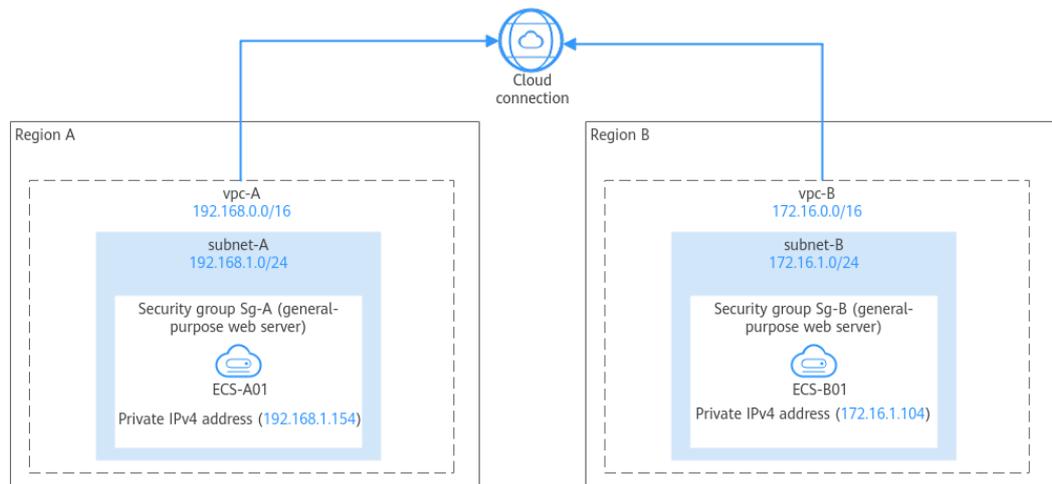


Table 2-1 Description for cross-region VPC communication

| Resource | Description   |
|----------|---|
| VPCs     | <ul style="list-style-type: none"> <li>The CIDR blocks of the VPCs to be connected cannot overlap with each other. Overlapping VPC CIDR blocks will cause route conflicts. If the VPCs have overlapping CIDR blocks, you need to modify the CIDR blocks.</li> <li>Each VPC comes with a default route table that has the default IPv4 local route, which enables subnets in the VPC to communicate with each other.</li> </ul>                                    |
| ECSs     | <p>In this example, two ECSs are deployed in VPCs in different regions. An ECS can be only associated with a security group in the same region as the ECS. Therefore, the two ECSs must be associated with different security groups. To connect the two ECSs, you need to add inbound rules to their security groups by referring to Table 2-4. For more information about security groups, <a href="#">Security Group and Security Group Rule Overview</a>.</p> |

### Planning Resources

The VPCs and ECSs must be in different regions, but they can be in any AZs.

#### NOTE

The following resource details are only for your reference. You can modify them if needed.

- **Table 2-2** describes the two VPCs in detail. Their CIDR blocks cannot overlap with each other.

**Table 2-2** VPC details

| VPC   | VPC CIDR Block | Subnet Name | Subnet CIDR Block | Route Table         |
|-------|----------------|-------------|-------------------|---------------------|
| vpc-A | 192.168.0.0/16 | subnet-A    | 192.168.1.0/24    | Default route table |
| vpc-B | 172.16.0.0/16  | subnet-B    | 172.16.1.0/24     | Default route table |

- **Table 2-3** describes the two ECSs in detail, with each ECS in a VPC.

**Table 2-3** ECS details

| ECS Name | Image   | VPC   | Subnet   | Security Group                     | Private IP Address |
|----------|---|-------|----------|------------------------------------|--------------------|
| ECS-A01  | Public image: Huawei Cloud EulerOS 2.0 Standard Edition | vpc-A | subnet-A | Sg-A: (general-purpose web server) | 192.168.1.154      |
| ECS-B01  |   | vpc-B | subnet-B | Sg-B: (general-purpose web server) | 172.16.1.104       |

- Security group rules: In this example, the two ECSs are in different security groups (Sg-A and Sg-B). You need to add the following rules to the security groups to allow traffic between the ECSs.  
Set **Source** to the CIDR block of the other VPC or subnet.

**Table 2-4** Security group rules (CIDR block as the source)

| Security Group | Direction | Action | Type | Protocol & Port | Source  | Description  |
|----------------|-----------|--------|------|-----------------|---|--|
| Sg-A           | Inbound   | Allow  | IPv4 | All             | IP address: 172.16.0.0/16 (vpc-B's CIDR block)  | Allows IPv4 traffic from 172.16.0.0/16 to the resources in Sg-A over any protocol and port.  |
| Sg-B           | Inbound   | Allow  | IPv4 | All             | IP address: 192.168.0.0/16 (vpc-A's CIDR block) | Allows IPv4 traffic from 192.168.0.0/16 to the resources in Sg-B over any protocol and port. |

## Procedure

**Table 2-5** Communication between VPCs in the same account but different regions

| Step  | What to Do  |
|---|---|
| <b>Preparations</b>                                       | Before using cloud services, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account.   |
| <b>Step 1: (Optional) Apply for a Cross-Border Permit</b> | 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.                    |
| <b>Step 2: Create a Cloud Connection</b>                  | Create a cloud connection.  |
| <b>Step 3: (Optional) Create VPCs and ECSs</b>            | Create VPCs and ECSs in different region using the same account. If you already have VPCs and ECSs, skip this step.   |
| <b>Step 4: Load Network Instances</b>                     | Load the VPCs to the created cloud connection based on your network plan.   |
| <b>Step 5: Buy a Bandwidth Package</b>                    | 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. |
| <b>Step 6: Assign an Inter-Region Bandwidth</b>           |   |

| Step  | What to Do   |
|---|--|
| <a href="#">Step 7: Verify Network Connectivity</a> | Log in to the ECSs and verify the network connectivity between VPCs. |

## 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: (Optional) 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.

In this example, no VPCs (one in CN Southwest-Guiyang1 and the other in CN North-Beijing4) are outside the Chinese mainland, so no cross-border permit is required. You can skip this step.

1. Go to the [Bandwidth Packages](#) page.
  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.
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 2-6** Online cross-border permit application

| Parameter               | Description  |
|-------------------------|--|
| Applicant Name          | The applicant name, which must be the same as the company name in the <i>Letter of Commitment to Information Security</i> .  |
| Huawei Cloud UID        | The account ID to log in to the management console. You can take the following steps to obtain your account ID.<br><ol style="list-style-type: none"><li>1. Log in to the management console.</li><li>2. Click the username in the upper right corner and select <b>My Credentials</b> from the drop-down list.</li><li>3. On the <b>API Credentials</b> page, obtain the <b>Account ID</b>.</li></ol> |
| 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.  |
| 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 2-7** Required materials

| Parameter                                    | Description  | Required Material  | Signature | Seal |
|--|--|--|-----------|------|
| Business License                             | Upload a photo of the business license with the official seal.<br><br>For the position of the seal, see the template provided by Huawei Cloud.   | A scanned copy of your company's business license  | -         | √    |
| Service Agreement                            | Download the <i>Huawei Cloud Cross-Border Circuit Service Agreement</i> , fill in the blank, upload the copy of agreement with the signature and official seal.<br><br><ul style="list-style-type: none"> <li>• Sign the material on the signature block.</li> <li>• Stamp the seal over the signature.</li> </ul>   | A scanned copy of the <i>Huawei Cloud Cross-Border Circuit Service Agreement</i>   | √         | √    |
| Letter of Commitment to Information Security | Download the <i>China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service</i> , fill in the blank, and upload the copy of the letter with the signature and seal.<br><br><ul style="list-style-type: none"> <li>• Sign the material on the signature block.</li> <li>• Stamp the seal over the signature.</li> <li>• Specify the bandwidth you estimated and your company name.</li> </ul> | A scanned copy of the <i>China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service</i> | √         | √    |

4. Click **Submit**.

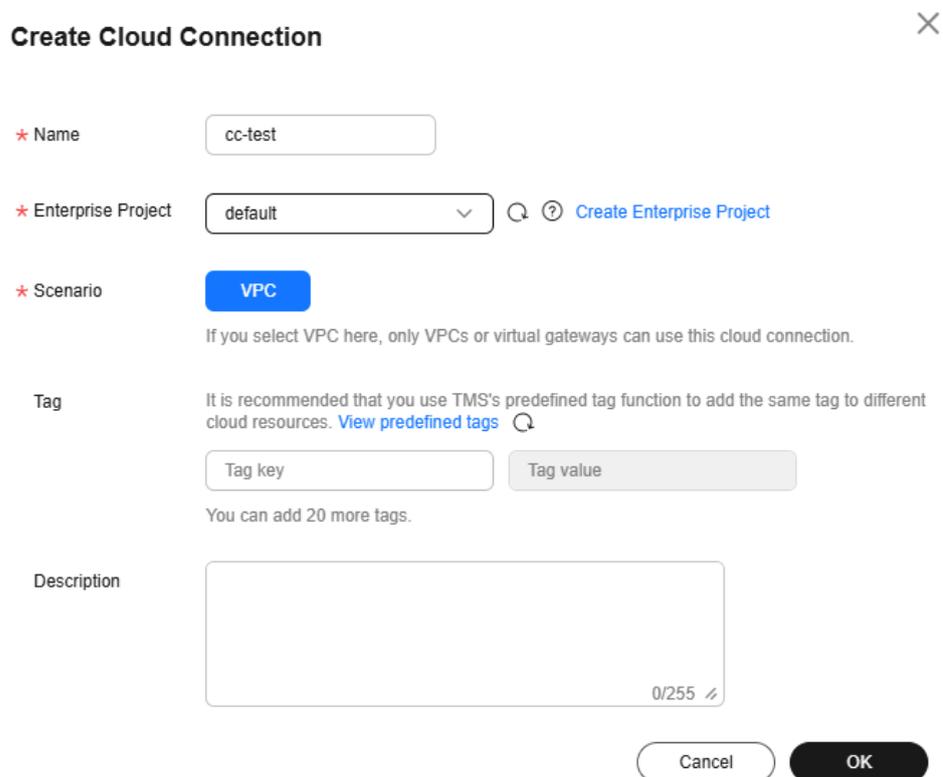
 **NOTE**

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

## Step 2: Create a Cloud Connection

1. Go to the [Cloud Connections](#) page.
2. In the upper right corner of the page, click **Create Cloud Connection**.
3. Configure the parameters based on [Table 2-8](#).

**Figure 2-3** Creating a cloud connection



**Table 2-8** Parameters for creating a cloud connection

| Parameter          | Example Value | Description   |
|--------------------|---------------|---|
| Name               | cc-test       | Specifies the cloud connection name.<br>The name can contain 1 to 64 characters. Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. |
| Enterprise Project | default       | Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.   |

| Parameter   | Example Value | Description  |
|-------------|---------------|--|
| Scenario    | VPC           | <b>VPC:</b> 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.<br><b>NOTE</b><br>If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value.<br>For details about predefined tags, see <a href="#">Predefined Tags</a> . |
| Description | -             | Provides supplementary information about the cloud connection.<br>The description can contain no more than 255 characters.   |

4. Click **OK**.

### Step 3: (Optional) Create VPCs and ECSs

Perform the following operations to create VPCs and ECSs. If you already have VPCs and ECSs, skip this step.

#### Constraints

- The CIDR blocks of the VPCs to be connected cannot overlap with each other. Overlapping VPC CIDR blocks will cause route conflicts. If the VPCs have overlapping CIDR blocks, you need to modify the CIDR blocks.
- In this example, the two ECSs are in different security groups. You need to add rules to the security groups to allow access from each other. For details, see [Table 2-4](#).

#### Procedure

1. Create two VPCs with subnets.  
For details, see [Creating a VPC](#).  
For the details about VPCs and subnets in this example, see [Table 2-2](#).
2. Create two ECSs.  
For details, see [Purchasing a Custom ECS](#).  
For details about the ECSs in this example, see [Table 2-3](#).

### Step 4: Load Network Instances

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

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.

3. Click the **Network Instances** tab.
4. Click **Load Network Instance**.
5. Configure the parameters based on [Table 2-9](#) and click **OK**.

**Figure 2-4** Loading vpc-A in the same account

✕

**i** 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
  Peer account

\* Region

\* Instance Type 
 VPC
  Virtual gateway
 

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.

\* VPC

\* VPC CIDR Block ⓘ Subnet 



Other CIDR Block

Remarks 



0/64 ✎

**Table 2-9** Parameters for loading network instances in the same account

| Parameter     | Example Value         | Description   |
|---------------|-----------------------|---|
| Account       | Current account       | Specifies the account that provides the network instance.<br>Select <b>Current account</b> .  |
| Region        | CN Southwest-Guiyang1 | Specifies the region where the VPC you want to connect is located.  |
| Instance Type | VPC                   | Specifies the type of the network instance that needs to be loaded to the cloud connection. There are two options: <ul style="list-style-type: none"> <li>• <b>VPC</b></li> <li>• <b>Virtual gateway</b></li> </ul> Select <b>VPC</b> . |

| Parameter      | Example Value | Description  |
|----------------|---------------|--|
| VPC            | vpc-A         | Specifies the VPC you want to load to the cloud connection.<br>This parameter is mandatory if you have set <b>Instance Type</b> to <b>VPC</b> .  |
| VPC CIDR Block | subnet-A      | Specifies the subnets in the VPC and custom CIDR blocks.<br>If you have set <b>Instance Type</b> to <b>VPC</b> , you need to configure the following two parameters: <ul style="list-style-type: none"> <li>• <b>Subnet</b></li> <li>• <b>Other CIDR Block</b>: Add one or more custom CIDR blocks as needed.</li> </ul> |
| Remarks        | -             | Provides supplementary information about the network instance.   |

- In the displayed dialog box, click **Continue Loading**. Then, click  to load vpc-B in the same account but in a different region (CN North-Beijing4).

**Figure 2-5** Loading vpc-B in the same account

**Load Network Instance**
✕

**i** 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
 Peer account

\* Region

\* Instance Type 
 VPC
 Virtual gateway

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.

\* VPC  [Create VPC](#)

\* VPC CIDR Block ? Subnet  ✕

Other CIDR Block

Remarks

0/64 

## 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.

1. Go to the [Buy Bandwidth Package](#) page.
2. Configure the parameters based on [Table 2-10](#) and click **Next**.

**Table 2-10** Parameters for buying a bandwidth package

| Parameter                | Example Value             | Description  |
|--------------------------|---------------------------|--|
| <b>Basic Information</b> |                           |  |
| Billing Mode             | Yearly/<br>Monthly        | The only option is <b>Yearly/Monthly</b> .<br>You can purchase it by year or month as needed.  |
| Name                     | bandwidth<br>Package-test | Specifies the bandwidth package name.<br>The name can contain 1 to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.   |
| Enterprise Project       | default                   | Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.  |
| Tag                      | -                         | Specifies the tag to identify the bandwidth package. A tag consists of a key and a value. You can add 20 tags to a bandwidth package.<br><b>NOTE</b><br>If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value.<br>For details about predefined tags, see <a href="#">Predefined Tags</a> .  |
| <b>Bandwidth Details</b> |                           |  |
| Billed By                | Bandwidth                 | Specifies by what you want the bandwidth package to be billed.   |
| Applicability            | Single geographic region  | Specifies whether you want to use the bandwidth package for communication within a geographic region or between geographic regions. There are two options: <ul style="list-style-type: none"> <li>• <b>Single geographic region:</b> Use the bandwidth package for communication between regions in the same geographic region.</li> <li>• <b>Across geographic regions:</b> Use the bandwidth package for communication between regions in different geographic regions.</li> </ul> |

| Parameter          | Example Value    | Description  |
|--------------------|------------------|--|
| Geographic Region  | Chinese mainland | Specifies the geographic regions.  |
| Bandwidth (Mbit/s) | 10               | Specifies the bandwidth you require for communication between regions. 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. Unit: Mbit/s |
| Required Duration  | 1 month          | Specifies how long you require the bandwidth package for. Auto renewal is supported.   |
| Cloud Connection   | Bind later       | Specifies the cloud connection you want to bind the bandwidth package to. There are two options: <ul style="list-style-type: none"><li>• <b>Bind now</b></li><li>• <b>Bind later</b></li></ul>   |

3. Confirm the configuration and submit your order.

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

### Binding a Bandwidth Package to a Cloud Connection

Bind the purchased bandwidth package to the created cloud connection.

1. Go to the [Cloud Connections](#) page.
2. Click the cloud connection name (**cc-test**) to go to the **Basic Information** tab.
3. Click the **Bandwidth Packages** tab.
4. Click **Bind Bandwidth Package**. In the displayed dialog box, select the purchased bandwidth package (**bandwidthPackage-test**) that will be bound to the cloud connection (**cc-test**) and click **OK**.

## Step 6: Assign an Inter-Region Bandwidth

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

1. Go to the [Cloud Connections](#) page.
2. Click the cloud connection name (**cc-test**) to go to the **Basic Information** tab.
3. Click the **Inter-Region Bandwidths** tab.
4. Click **Assign Inter-Region Bandwidth** and configure the parameters based on [Table 2-11](#).

### Assign Inter-Region Bandwidth

Regions

\* Bandwidth Package   
Bandwidth package: 10 Mbit/s; Available bandwidth: 10 Mbit/s

\* Bandwidth  Mbit/s

**Table 2-11** Parameters required for assigning inter-region bandwidth

| Parameter         | Example Value                              | Description  |
|-------------------|--|--|
| Regions           | CN Southwest-Guiyang1<br>CN North-Beijing4 | Specifies the regions of the network instances that need to communicate with each other. Select two regions.   |
| Bandwidth Package | bandwidthPackage-test                      | Specifies the purchased bandwidth package that will be bound to the cloud connection.  |
| Bandwidth         | 10   | 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. |

5. Click **OK**.

Now the network instances 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.

## Step 7: Verify Network Connectivity

Log in to each ECS and verify the network connectivity between VPCs.

1. Log in to ECS-A01.

Multiple methods are available for logging in to an ECS. For details, see [Logging In to an ECS](#).

In this example, use VNC provided on the management console to log in to the ECSs.

2. Ping the other ECS to verify the network connectivity between VPCs.

**ping** <private-IP-address-of-ECS-B01>

Example command:

**ping 172.16.1.104**

If the following information is displayed, vpc-A and vpc-B are connected.

```
[root@ecs-a01 ~]# ping 172.16.1.104
PING 172.16.1.104 (172.16.1.104) 56(84) bytes of data:
64 bytes from 172.16.1.104: icmp_seq=1 ttl=61 time=35.5 ms
64 bytes from 172.16.1.104: icmp_seq=2 ttl=61 time=35.4 ms
64 bytes from 172.16.1.104: icmp_seq=3 ttl=61 time=35.2 ms
64 bytes from 172.16.1.104: icmp_seq=4 ttl=61 time=35.2 ms
64 bytes from 172.16.1.104: icmp_seq=5 ttl=61 time=35.2 ms
64 bytes from 172.16.1.104: icmp_seq=6 ttl=61 time=35.2 ms
64 bytes from 172.16.1.104: icmp_seq=7 ttl=61 time=35.2 ms
^C
--- 172.16.1.104 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6007ms
rtt min/avg/max/mdev = 35.198/35.277/35.531/0.115 ms
[root@ecs-a01 ~]# _
```

# 3 Using a Central Network and Enterprise Routers to Connect VPCs in the Same Account But Different Regions

---

Relying on the Huawei backbone network, you can set up a central network to manage global network resources on premises and on the cloud easily and securely. After attaching the VPCs to enterprise routers in each region, you can add the enterprise routers to a central network, so that all the VPCs attached to the enterprise routers can communicate with each other across regions.

In this topic, a central network and enterprise routers are used to connect the VPCs in the same account but different regions.

## NOTE

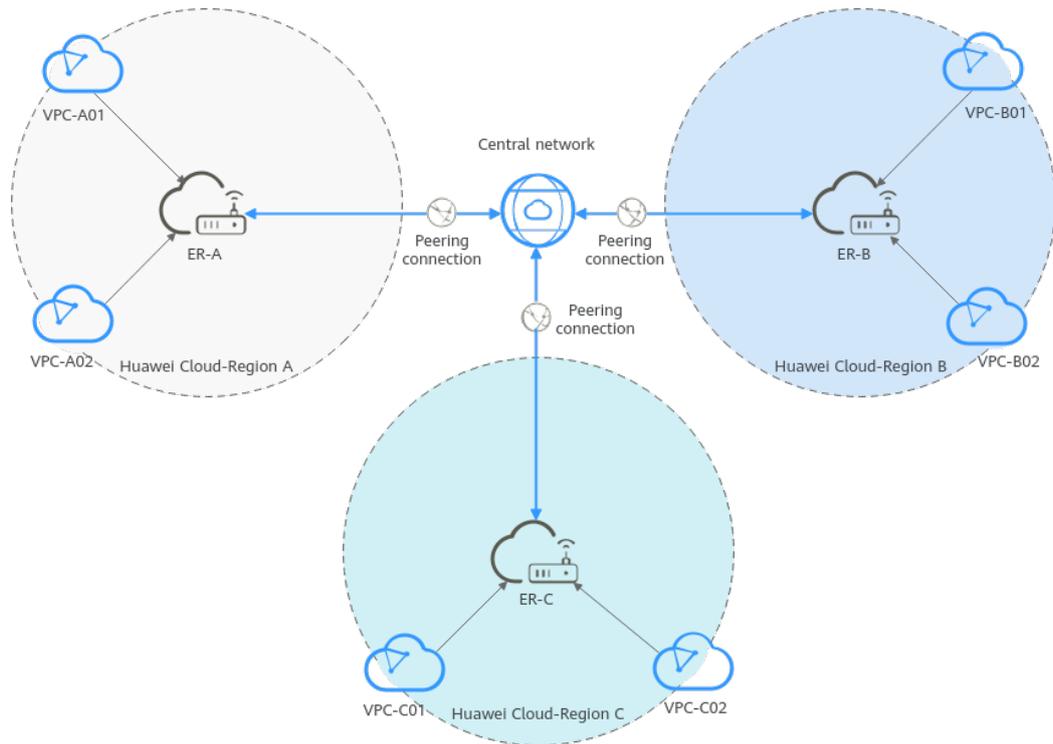
- For details about the regions where central networks are available, see [Region Availability](#).
- The CIDR blocks of the VPCs must be unique. If there are overlapping CIDR blocks, the communication may fail.

## Architecture

For nearby access, an enterprise runs workloads in regions A, B, and C. The VPCs in each region need to communicate with each other. To achieve this, you can:

1. Create an enterprise router in each region: ER-A in region A, ER-B in region B, and ER-C in region C.
2. Create a central network and add ER-A, ER-B, and ER-C to the central network as attachments so that the three enterprise routers can communicate with each other.
3. In region A, attach VPC-A01 and VPC-A02 to ER-A so that the two VPCs can communicate with each other. Perform the same operations in regions B and C. In this way, the VPCs in the three regions can communicate with each other over the central network.

**Figure 3-1** Cross-region VPC network



**NOTE**

You can **share an enterprise router** with different accounts to attach VPCs of these accounts to the same enterprise router for communications.

## Network and Resource Planning

To use a central network and enterprise routers to connect VPCs across regions, you need to:

- Plan the central network, VPCs and their subnets, VPC route tables, and enterprise router route tables.
- Plan the quantities, names, and main parameters of cloud resources, including central network, enterprise router, VPC, and ECS.

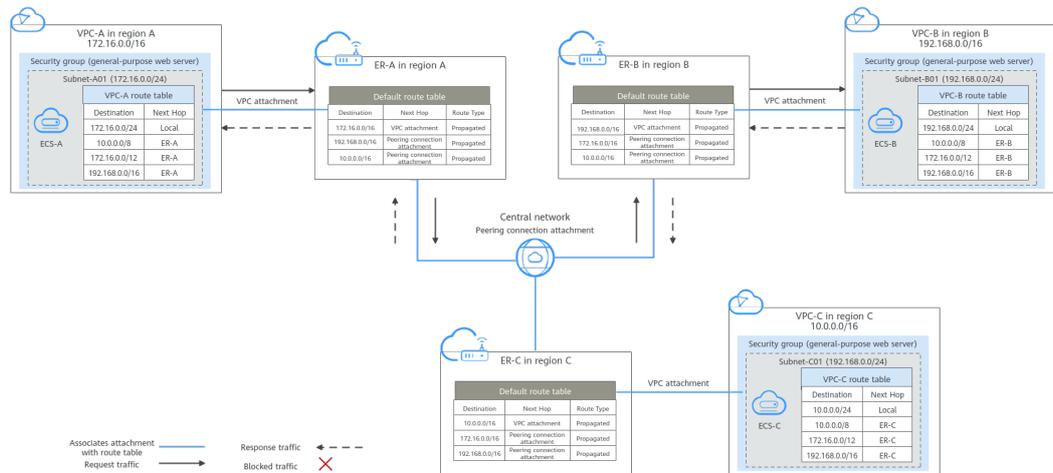
### Network Planning

**Figure 3-2** shows the network planning for communication between VPCs across regions. For details about the network planning, see **Table 3-2**.

**NOTE**

In this example, one VPC is created and attached to an enterprise router in each region. Make the plan based on your service requirements.

**Figure 3-2** Cross-region VPC network planning



**Table 3-1** Network traffic flows

| Traffic Flow                          | What to Do   |
|---------------------------------------|--|
| Request traffic: from VPC-A to VPC-B  | <ol style="list-style-type: none"> <li>In the route table of VPC-A, there are routes with the next hop set to enterprise router ER-A to forward traffic from VPC-A to ER-A.</li> <li>In the route table of enterprise router ER-A, there is a route with the next hop set to the peering connection attachment and destination to 192.168.0.0/16 to forward traffic from ER-A to enterprise router ER-B.</li> <li>In the route table of enterprise router ER-B, there is a route with the next hop set to the VPC-B attachment to forward traffic from ER-B to VPC-B.</li> </ol> |
| Response traffic: from VPC-B to VPC-A | <ol style="list-style-type: none"> <li>In the route table of VPC-B, there are routes with the next hop set to enterprise router ER-B to forward traffic from VPC-B to ER-B.</li> <li>In the route table of enterprise router ER-B, there is a route with the next hop set to the peering connection attachment and destination to 172.16.0.0/16 to forward traffic from ER-B to enterprise router ER-A.</li> <li>In the route table of enterprise router ER-A, there is a route with the next hop set to the VPC-A attachment to forward traffic from ER-A to VPC-A.</li> </ol>  |

**Table 3-2** Description for cross-region VPC communication

| Resource          | Description   |
|-------------------|---|
| VPC               | <ul style="list-style-type: none"> <li>The CIDR blocks of the VPCs to be connected cannot overlap with each other.<br/>In this example, the CIDR blocks of the VPCs are propagated to the enterprise router route table as the destination in routes. The CIDR blocks cannot be modified and overlapping CIDR blocks may cause route conflicts.</li> <li>If your existing VPCs have overlapping CIDR blocks, do not use propagated routes. Instead, you need to manually add static routes to the route table of the enterprise router. The destination can be a subnet CIDR block or a smaller CIDR block.</li> <li>Each VPC has a default route table.</li> <li>Routes in the default route table can be: <ul style="list-style-type: none"> <li>Local: a system route for communications between subnets in a VPC.</li> <li>Enterprise router: automatically added routes with 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations for routing traffic from a VPC subnet to the enterprise router. See <a href="#">Table 3-3</a> for details.</li> </ul> </li> </ul> |
| Central network   | <ul style="list-style-type: none"> <li>Enterprise routers in different regions are added to the central network as attachments.</li> <li>Global connection bandwidths are required for assigning cross-site connection bandwidths to for communication across regions.</li> </ul>   |
| Enterprise router | <p>The network configuration for the enterprise router in the three regions is the same. <a href="#">Table 3-4</a> lists all routes required by the enterprise router.</p> <p>When a central network is set up to connect the enterprise routers, you must enable <b>Default Route Table Association</b> and <b>Default Route Table Propagation</b> for the enterprise routers. In this way, when an instance is added to an enterprise router, a route pointing to the attachment will be automatically added for the enterprise router.</p>   |
| ECS               | <p>An ECS is created in each VPC. If the ECSs are in different security groups, add rules to the security groups to allow access to each other.</p>   |

**Table 3-3** VPC route tables

| Destination   | Next Hop          | Route Type            |
|---------------|-------------------|-----------------------|
| 10.0.0.0/8    | Enterprise router | Static route (custom) |
| 172.16.0.0/12 | Enterprise router | Static route (custom) |

| Destination    | Next Hop          | Route Type            |
|----------------|-------------------|-----------------------|
| 192.168.0.0/16 | Enterprise router | Static route (custom) |

 NOTE

- If you enable **Auto Add Routes** when creating a VPC attachment, you do not need to manually add static routes to the VPC route table. Instead, the system automatically adds routes (with this enterprise router as the next hop and 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16 as the destinations) to all route tables of the VPC.
- If an existing route in the VPC route tables has a destination to 10.0.0.0/8, 172.16.0.0/12, or 192.168.0.0/16, the routes will fail to be added. In this case, do not enable **Auto Add Routes**. After the attachment is created, manually add routes.
- Do not set the destination of a route (with an enterprise router as the next hop) to 0.0.0.0/0 in the VPC route table. If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than the route with the enterprise router as the next hop. In this case, traffic is forwarded to the EIP and cannot reach the enterprise router.

**Table 3-4** Enterprise router route tables

| Enterprise router | Destination                         | Next Hop  | Route Type       |
|-------------------|-------------------------------------|---|------------------|
| Region A:<br>ER-A | VPC-A CIDR block:<br>172.16.0.0/16  | VPC-A attachment:<br>er-attach-VPC-A                    | Propagated route |
|                   | VPC-B CIDR block:<br>192.168.0.0/16 | Peering connection<br>attachment: region-<br>A-region-B | Propagated route |
|                   | VPC-C CIDR block:<br>10.0.0.0/16    | Peering connection<br>attachment: region-<br>A-region-C | Propagated route |
| Region B:<br>ER-B | VPC-B CIDR block:<br>192.168.0.0/16 | VPC-B attachment:<br>er-attach-VPC-B                    | Propagated route |
|                   | VPC-A CIDR block:<br>172.16.0.0/16  | Peering connection<br>attachment: region-<br>B-region-A | Propagated route |
|                   | VPC-C CIDR block:<br>10.0.0.0/16    | Peering connection<br>attachment: region-<br>B-region-C | Propagated route |
| Region C:<br>ER-C | VPC-C CIDR block:<br>10.0.0.0/16    | VPC-C attachment:<br>er-attach-VPC-C                    | Propagated route |
|                   | VPC-A CIDR block:<br>172.16.0.0/16  | Peering connection<br>attachment: region-<br>C-region-A | Propagated route |

| Enterprise router | Destination                         | Next Hop  | Route Type       |
|-------------------|-------------------------------------|---|------------------|
|                   | VPC-B CIDR block:<br>192.168.0.0/16 | Peering connection<br>attachment: region-<br>C-region-B | Propagated route |

### Resource Planning

The enterprise router, VPCs, and ECSs must be in the same region, but they can be in different AZs.

#### NOTE

The following resource planning is only for your reference.

**Table 3-5** Resource planning for cross-region VPC communications

| Resource | Quantity | Description   |
|----------|----------|---|
| VPC      | 3        | <p>A service VPC is required in each region for running workloads. Each VPC needs to be attached to an enterprise router in the same region.</p> <ul style="list-style-type: none"> <li>• <b>Name:</b> Set it based on site requirements. In this example, the names are as follows: <ul style="list-style-type: none"> <li>- Region A: VPC-A</li> <li>- Region B: VPC-B</li> <li>- Region C: VPC-C</li> </ul> </li> <li>• <b>IPv4 CIDR Block:</b> The CIDR blocks of VPCs must be unique. Plan the CIDR blocks based on site requirements. In this example, the CIDR blocks are as follows: <ul style="list-style-type: none"> <li>- VPC-A: 172.16.0.0/16</li> <li>- VPC-B: 192.168.0.0/16</li> <li>- VPC-C: 10.0.0.0/16</li> </ul> </li> <li>• <b>Subnet name and IPv4 CIDR block:</b> The subnet CIDR blocks that need to communicate with each other must be unique. Plan the subnets based on site requirements. In this example, the subnets are as follows: <ul style="list-style-type: none"> <li>- Subnet-A01: 172.16.0.0/24</li> <li>- Subnet-B01: 192.168.0.0/24</li> <li>- Subnet-C01: 10.0.0.0/24</li> </ul> </li> </ul> |

| Resource          | Quantity | Description   |
|-------------------|----------|---|
| Enterprise router | 3        | <p>An enterprise router is required in each region. The VPC in each region is attached to the corresponding enterprise router, and a peering connection attachment is created between every two enterprise routers.</p> <ul style="list-style-type: none"> <li>• <b>Name:</b> Set it based on site requirements. In this example, the names are as follows: <ul style="list-style-type: none"> <li>- Region A: ER-A</li> <li>- Region B: ER-B</li> <li>- Region C: ER-C</li> </ul> </li> <li>• <b>ASN:</b> Set different ASNs for enterprise routers. In this example, the ASNs are as follows: <ul style="list-style-type: none"> <li>- ER-A: 64512</li> <li>- ER-B: 64513</li> <li>- ER-C: 64514</li> </ul> </li> <li>• <b>Default Route Table Association:</b> Enable this option.</li> <li>• <b>Default Route Table Propagation:</b> Enable this option.</li> <li>• <b>Auto Accept Shared Attachments:</b> Set it based on site requirements. In this example, this option is enabled.</li> <li>• <b>Attachment:</b> Three attachments are required for each enterprise router. In this example, the attachments are as follows: <p>ER-A</p> <ul style="list-style-type: none"> <li>- VPC attachment er-attach-VPC-A: connects the network between VPC-A and ER-A.</li> <li>- Peering connection attachment region-A-region-B: connects the network between ER-A and ER-B.</li> <li>- Peering connection attachment region-A-region-C: connects the network between ER-A and ER-C.</li> </ul> <p>ER-B</p> <ul style="list-style-type: none"> <li>- VPC attachment er-attach-VPC-B: connects the network between VPC-B and ER-B.</li> <li>- Peering connection attachment region-B-region-A: connects the network between ER-B and ER-A.</li> <li>- Peering connection attachment region-B-region-C: connects the network between ER-B and ER-C.</li> </ul> <p>ER-C</p> <ul style="list-style-type: none"> <li>- VPC attachment er-attach-VPC-C: connects the network between VPC-C and ER-C.</li> <li>- Peering connection attachment region-C-region-A: connects the network between ER-C and ER-A.</li> <li>- Peering connection attachment region-C-region-B: connects the network between ER-C and ER-B.</li> </ul> </li> </ul> |

| Resource                    | Quantity | Description  |
|-----------------------------|----------|--|
|                             |          | <p><b>NOTICE</b><br/>When a central network is set up to connect the enterprise routers, you must enable <b>Default Route Table Association</b> and <b>Default Route Table Propagation</b> for the enterprise routers.</p>   |
| Central network             | 1        | <p>A central network is required, and all enterprise routers are added to it as attachments.</p> <ul style="list-style-type: none"> <li>● <b>Name:</b> Set it based on site requirements. In this example, the name is gcn-A-B-C.</li> <li>● <b>Policy</b> <ul style="list-style-type: none"> <li>- Region A: enterprise router ER-A</li> <li>- Region B: enterprise router ER-B</li> <li>- Region C: enterprise router ER-C</li> </ul> </li> <li>● <b>Cross-site connection bandwidths:</b> <ul style="list-style-type: none"> <li>- Region A-Region B: 10 Mbit/s</li> <li>- Region A-Region C: 5 Mbit/s</li> <li>- Region B-Region C: 20 Mbit/s</li> </ul> </li> </ul>   |
| Global connection bandwidth | 3        | <p>Three global connection bandwidths are required to connect the cloud backbone networks in different regions.</p> <ul style="list-style-type: none"> <li>● <b>Name:</b> Set it based on site requirements. In this example, the names are as follows: <ul style="list-style-type: none"> <li>- Global connection bandwidth for communication between region A and region B: bandwidth-A-B</li> <li>- Global connection bandwidth for communication between region A and region C: bandwidth-A-C</li> <li>- Global connection bandwidth for communication between region B and region C: bandwidth-B-C</li> </ul> </li> <li>● <b>Bandwidth Type:</b> Set it based on site requirements. In this example, select <b>Geographic-region</b> because the three regions are in the same geographic region.</li> <li>● <b>Geographic Region:</b> Set it based on site requirements. In this example, select <b>Chinese Mainland</b>.</li> <li>● <b>Connect Regions:</b> Select the regions based on site requirements.</li> </ul> |

| Resource | Quantity | Description  |
|----------|----------|--|
| ECS      | 3        | <p>Create an ECS in each VPC to verify network connectivity.</p> <ul style="list-style-type: none"> <li>• <b>ECS Name:</b> Set it based on site requirements. In this example, the names are as follows: <ul style="list-style-type: none"> <li>- Region A: ECS-A</li> <li>- Region B: ECS-B</li> <li>- Region C: ECS-C</li> </ul> </li> <li>• <b>Image:</b> Set it as needed. In this example, public image <b>Huawei Cloud EulerOS 2.0 Standard</b> is used.</li> <li>• <b>Network:</b> Select the VPC and subnet based on site requirements. In this example, the VPCs and subnets are as follows: <ul style="list-style-type: none"> <li>- ECS-A: VPC-A, Subnet-A01</li> <li>- ECS-B: VPC-B, Subnet-B01</li> <li>- ECS-C: VPC-C, Subnet-C01</li> </ul> </li> <li>• <b>Security Group:</b> Select a security group based on site requirements. In this example, the security group <b>sg-demo</b> uses a general-purpose web server template.</li> <li>• Private IP addresses: <ul style="list-style-type: none"> <li>- ECS-A: 172.16.0.91</li> <li>- ECS-B: 192.168.0.5</li> <li>- ECS-C: 10.0.0.29</li> </ul> </li> </ul> |

## Process

**Table 3-6** Steps for connecting VPCs across regions

| Step                | What to Do  |
|---------------------|---|
| <b>Preparations</b> | Before using cloud services, sign up for a HUAWEI ID, enable Huawei Cloud services, complete real-name authentication, and top up your account. |

| Step   | What to Do  |
|--|---|
| <b>Step 1: Create Cloud Resources</b>  | <ol style="list-style-type: none"><li>1. Create three enterprise routers with one in each region.</li><li>2. Create a service VPC and its subnet in each region.</li><li>3. Create three ECSs with one in the subnet of each service VPC.</li><li>4. Create a central network. When creating the central network, create a policy and add the enterprise routers in different regions to the policy.</li><li>5. Purchase three global connection bandwidths to connect networks in different regions.</li></ol> |
| <b>Step 2: Create a VPC Attachment for Each Enterprise Router</b>              | Create a VPC attachment to each enterprise router.  |
| <b>Step 3: Assign Cross-Site Connection Bandwidths for the Central Network</b> | Assign cross-site connection bandwidths on the central network based on service requirements.   |
| <b>Step 4: Verify Network Connectivity</b>                                     | Log in to an ECS and run the <b>ping</b> command to verify the network connectivity.  |

## 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 Cloud Resources

In this example, you need to create a central network, three enterprise routers, three VPCs, and three ECSs based on **Table 3-5.**

1. Create an enterprise router in each of the three regions.

For details, see **Creating an Enterprise Router.**

 **NOTE**

Specify a unique ASN for each enterprise router.

2. Create a VPC in each of the three regions.  
For details, see [Creating a VPC](#).
3. Create an ECS in each of the three regions.  
For details, see [Purchasing a Custom ECS](#).
4. Create a central network and add the enterprise routers to the central network as attachments.
  - a. Create a central network and add the enterprise routers to the central network as attachments.  
For details, see [Creating a Central Network](#).
  - b. On the Enterprise Router console, view the peering connection attachments.  
For details, see [Viewing Details About an Attachment](#).  
If the status of the peering connection attachments is **Normal**, the attachments are available.  
**Default Route Table Association** and **Default Route Table Propagation** are enabled when you create enterprise routers. After peering connection attachments are created for the enterprise routers, Enterprise Router will automatically:
    - Associate the peering connection attachment with the default route table of each enterprise router.
    - Propagate the peering connection attachment to the default route table of each enterprise router. The route tables automatically learn routes from each other.
5. Purchase three global connection bandwidths to connect networks in different regions.  
For details, see [Purchasing a Global Connection Bandwidth](#).

## Step 2: Create a VPC Attachment for Each Enterprise Router

Create a VPC attachment for each enterprise router. For details about resource planning, see [Table 3-5](#).

1. In region A, attach VPC-A to enterprise router ER-A.
  - a. Attach the VPC to the enterprise router.  
In this example, enable **Auto Add Routes** to save you from manually configuring routes in the VPC route table.  
For details, see [Creating VPC Attachments for an Enterprise Router](#).  
**Default Route Table Association** and **Default Route Table Propagation** are enabled when you create the enterprise router. After VPCs are attached to the enterprise routers, Enterprise Router will automatically:
    - Associate the VPC attachments with the default route table of the enterprise router.

- Propagate the VPC attachments to the default route table of the enterprise router. The route table automatically learns the VPC CIDR blocks as the destination of routes.
  - b. (Optional) Add routes to the VPC route table for traffic to route through the enterprise router.  
Skip this step if you have enabled **Auto Add Routes** in the previous step. For details about routes, see [Table 3-3](#).  
For details, see [Adding Routes to VPC Route Tables](#).
2. In region B, attach VPC-B to enterprise router ER-B by referring to [1](#).
  3. In region C, attach VPC-C to enterprise router ER-C by referring to [1](#).

### Step 3: Assign Cross-Site Connection Bandwidths for the Central Network

To allow cross-region VPC communications, you need to assign cross-region connection bandwidths on the central network based on service requirements by referring to [Table 3-5](#).

#### NOTE

By default, Cloud Connect allocates 10 kbit/s of bandwidth for testing connectivity between regions. After the peering connection attachments are created, you can verify the network connectivity between VPCs. For details, see [Step 4: Verify Network Connectivity](#).

To ensure your workloads run normally, you need to purchase global connection bandwidths and assign cross-site connection bandwidths.

1. Assign a cross-site connection bandwidth from the purchased global connection bandwidth for the communication between region A and region B.  
For details, see [Assigning a Cross-Site Connection Bandwidth](#).
2. Assign a cross-site connection bandwidth from the purchased global connection bandwidth for the communication between region A and region C.
3. Assign a cross-site connection bandwidth from the purchased global connection bandwidth for the communication between region B and region C.

### Step 4: Verify Network Connectivity

1. Log in to an ECS.  
Multiple methods are available for logging in to an ECS. For details, see [Logging In to an ECS](#).  
In this example, use VNC provided on the management console to log in to an ECS.
2. In the remote login window of the ECSs, use ping to verify the network connectivity:
  - a. Verify the network connectivity between two VPCs.  
**ping <private-IP-address-of-the-ECS>**  
Log in to ECS-A to verify the network connectivity between VPC-A and VPC-B:  
**ping 192.168.0.5**  
If information similar to the following is displayed, VPC-A and VPC-B can communicate with each other normally:

```
[root@ECS-A ~]# ping 192.168.0.5
PING 192.168.0.5 (192.168.0.5) 56(84) bytes of data.
64 bytes from 192.168.0.5: icmp_seq=1 ttl=62 time=30.6 ms
64 bytes from 192.168.0.5: icmp_seq=2 ttl=62 time=30.2 ms
64 bytes from 192.168.0.5: icmp_seq=3 ttl=62 time=30.1 ms
64 bytes from 192.168.0.5: icmp_seq=4 ttl=62 time=30.1 ms
...
--- 192.168.0.5 ping statistics ---
```

- b. Verify the network connectivity between another two VPCs.

**ping** <private-IP-address-of-the-ECS>

Log in to ECS-A to verify the network connectivity between VPC-A and VPC-C:

**ping 10.0.0.29**

If information similar to the following is displayed, VPC-A and VPC-C can communicate with each other normally:

```
[root@ECS-A ~]# ping 10.0.0.29
PING 10.0.0.29 (10.0.0.29) 56(84) bytes of data.
64 bytes from 10.0.0.29: icmp_seq=1 ttl=62 time=27.4 ms
64 bytes from 10.0.0.29: icmp_seq=2 ttl=62 time=27.0 ms
64 bytes from 10.0.0.29: icmp_seq=3 ttl=62 time=26.10 ms
64 bytes from 10.0.0.29: icmp_seq=4 ttl=62 time=26.9 ms
...
--- 10.0.0.29 ping statistics ---
```

3. Repeat [1](#) and [2](#) to verify the network connectivity between VPC-B and VPC-C.

# 4 Common Practices

If you need a global enterprise-grade cloud network, Cloud Connect is recommended. You can refer to the common practices provided here. Each practice details the application scenario and operations.

## Cross-VPC Communication

| Best Practices   | Description   |
|--|---|
| <a href="#">Connecting Two VPCs Across Regions</a>   | Use a cloud connection to connect two VPCs in different regions, so that the two VPCs can access each other.  |
| <a href="#">Connecting Multiple VPCs Across Regions</a>  | Use a cloud connection to connect multiple VPCs across regions to set up a secure, stable, high-performance, and reliable network.  |
| <a href="#">Connecting VPCs Across Regions Using a Cloud Connection and a VPC Peering Connection</a> | Use a VPC peering connection to connect VPCs in the same region and then use a cloud connection to connect VPCs in different regions, so that all the VPCs can communicate with each other. |

## Communication Between On-Premises Data Centers and VPCs

| Best Practices   | Description  |
|--|--|
| <a href="#">Connecting On-Premises Data Centers to VPCs in Different Regions Using a Cloud Connection and Direct Connect</a> | Use Direct Connect connections to connect on-premises data centers to VPCs and then use a cloud connect to connect all the VPCs, so that the on-premises data centers can access all the VPCs. |