Cloud Connect

Getting Started

Issue 01

Date 2026-03-09

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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.

Contents

1 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.

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.

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 1-1 shows the network planning for communication between VPCs across regions. For details about the network planning, see Table 1-2.

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 1-1 Cross-region VPC network planning

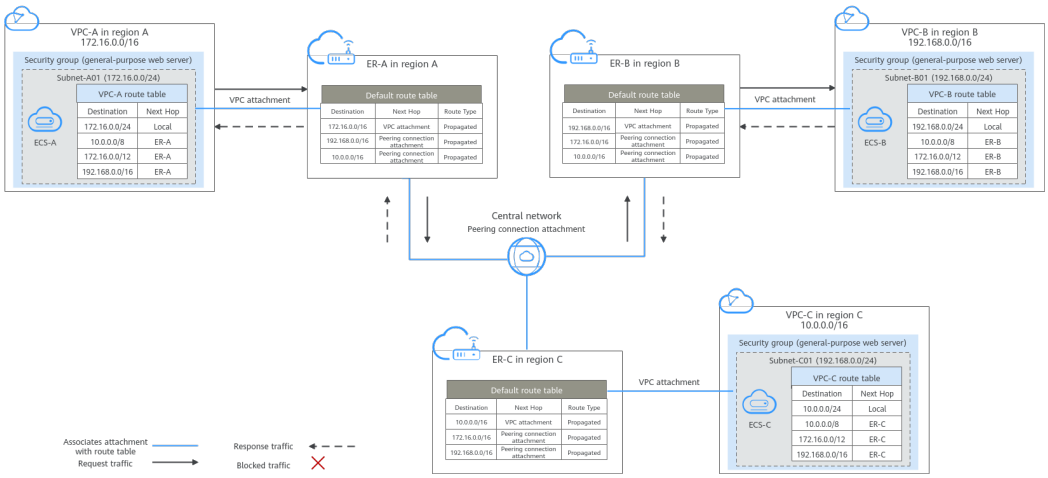

Table 1-1 Network traffic flows

Traffic Flow	What to Do
Request traffic: from VPC-A to VPC-B	1. 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. 2. 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. 3. 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.
Response traffic: from VPC-B to VPC-A	1. 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. 2. 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. 3. 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.

Table 1-2 Description for cross-region VPC communication

Resource	Description
VPC	• The CIDR blocks of the VPCs to be connected cannot overlap with each other. 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. 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. • Each VPC has a default route table. • Routes in the default route table can be: – Local: a system route for communications between subnets in a VPC. – 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 **Table 1-3** for details.
Central network	• Enterprise routers in different regions are added to the central network as attachments. • Global connection bandwidths are required for assigning cross-site connection bandwidths to for communication across regions.
Enterprise router	The network configuration for the enterprise router in the three regions is the same. **Table 1-4** lists all routes required by the enterprise router. When a central network is set up to connect the enterprise routers, you must enable **Default Route Table Association** and **Default Route Table Propagation** 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.
ECS	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.

Table 1-3 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 1-4 Enterprise router route tables

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

Enterprise router	Destination	Next Hop	Route Type
	VPC-B CIDR block: 192.168.0.0/16	Peering connection attachment: region-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 1-5 Resource planning for cross-region VPC communications

Resource	Quantity	Description
VPC	3	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. • **Name**: Set it based on site requirements. In this example, the names are as follows: – Region A: VPC-A – Region B: VPC-B – Region C: VPC-C • **IPv4 CIDR Block**: 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: – VPC-A: 172.16.0.0/16 – VPC-B: 192.168.0.0/16 – VPC-C: 10.0.0.0/16 • Subnet name and IPv4 CIDR block: 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: – Subnet-A01: 172.16.0.0/24 – Subnet-B01: 192.168.0.0/24 – Subnet-C01: 10.0.0.0/24

Resource	Quantity	Description
Enterprise router	3	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. • **Name**: Set it based on site requirements. In this example, the names are as follows: – Region A: ER-A – Region B: ER-B – Region C: ER-C • **ASN**: Set different ASNs for enterprise routers. In this example, the ASNs are as follows: – ER-A: 64512 – ER-B: 64513 – ER-C: 64514 • **Default Route Table Association**: Enable this option. • **Default Route Table Propagation**: Enable this option. • **Auto Accept Shared Attachments**: Set it based on site requirements. In this example, this option is enabled. • **Attachment**: Three attachments are required for each enterprise router. In this example, the attachments are as follows: ER-A – VPC attachment er-attach-VPC-A: connects the network between VPC-A and ER-A. – Peering connection attachment region-A-region-B: connects the network between ER-A and ER-B. – Peering connection attachment region-A-region-C: connects the network between ER-A and ER-C. ER-B – VPC attachment er-attach-VPC-B: connects the network between VPC-B and ER-B. – Peering connection attachment region-B-region-A: connects the network between ER-B and ER-A. – Peering connection attachment region-B-region-C: connects the network between ER-B and ER-C. ER-C – VPC attachment er-attach-VPC-C: connects the network between VPC-C and ER-C. – Peering connection attachment region-C-region-A: connects the network between ER-C and ER-A. – Peering connection attachment region-C-region-B: connects the network between ER-C and ER-B.

Resource	Quantity	Description
		CAUTION When a central network is set up to connect the enterprise routers, you must enable **Default Route Table Association** and **Default Route Table Propagation** for the enterprise routers.
Central network	1	A central network is required, and all enterprise routers are added to it as attachments. • **Name**: Set it based on site requirements. In this example, the name is gcn-A-B-C. • Policy – Region A: enterprise router ER-A – Region B: enterprise router ER-B – Region C: enterprise router ER-C • Cross-site connection bandwidths: – Region A-Region B: 10 Mbit/s – Region A-Region C: 5 Mbit/s – Region B-Region C: 20 Mbit/s
Global connection bandwidth	3	Three global connection bandwidths are required to connect the cloud backbone networks in different regions. • **Name**: Set it based on site requirements. In this example, the names are as follows: – Global connection bandwidth for communication between region A and region B: bandwidth-A-B – Global connection bandwidth for communication between region A and region C: bandwidth-A-C – Global connection bandwidth for communication between region B and region C: bandwidth-B-C • **Bandwidth Type**: Set it based on site requirements. In this example, select **Geographic-region** because the three regions are in the same geographic region. • **Geographic Region**: Set it based on site requirements. In this example, select **Chinese Mainland**. • **Connect Regions**: Select the regions based on site requirements.

Resource	Quantity	Description
ECS	3	Create an ECS in each VPC to verify network connectivity. • **ECS Name**: Set it based on site requirements. In this example, the names are as follows: – Region A: ECS-A – Region B: ECS-B – Region C: ECS-C • **Image**: Set it as needed. In this example, public image **Huawei Cloud EulerOS 2.0 Standard** is used. • **Network**: Select the VPC and subnet based on site requirements. In this example, the VPCs and subnets are as follows: – ECS-A: VPC-A, Subnet-A01 – ECS-B: VPC-B, Subnet-B01 – ECS-C: VPC-C, Subnet-C01 • **Security Group**: Select a security group based on site requirements. In this example, the security group **sg-demo** uses a general-purpose web server template. • Private IP addresses: – ECS-A: 172.16.0.91 – ECS-B: 192.168.0.5 – ECS-C: 10.0.0.29

Process

Table 1-6 Steps for connecting VPCs across regions

Step	What to Do
Preparations	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
Step 1: Create Cloud Resources	1. Create three enterprise routers with one in each region. 2. Create a service VPC and its subnet in each region. 3. Create three ECSs with one in the subnet of each service VPC. 4. Create a central network. When creating the central network, create a policy and add the enterprise routers in different regions to the policy. 5. Purchase three global connection bandwidths to connect networks in different regions.
Step 2: Create a VPC Attachment for Each Enterprise Router	Create a VPC attachment to each enterprise router.
Step 3: Assign Cross-Site Connection Bandwidths for the Central Network	Assign cross-site connection bandwidths on the central network based on service requirements.
Step 4: Verify Network Connectivity	Log in to an ECS and run the **ping** 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**.

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 1-5**.

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 with a Subnet**.

3. Create an ECS in each of the three regions.

   For details, see **Purchasing an ECS in Custom Config Mode**.

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.

   b. On the Enterprise Router console, view the peering connection attachments.

      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.

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 1-5**.

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 1-3**.

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 1-5**.

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.
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.

