Virtual Private Network

Getting Started

Issue	01
Date	2023-10-11

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.

Contents

1 Preparations

Before you use VPN, make the following preparations:

Registering a HUAWEI ID and Enabling Huawei Cloud Services

If you already have a HUAWEI ID and have enabled Huawei Cloud services, skip this step. If you do not have a HUAWEI ID, perform the following steps to create one:

1. Go to the **Huawei Cloud** official website, and click **Register** in the upper right corner.
2. Complete the registration as prompted. For details, see **Registering a HUAWEI ID and Enabling HUAWEI CLOUD Services**.

   If the registration is successful, the system automatically redirects you to your personal information page.
3. Complete real-name authentication by following the instructions in **Individual Real-Name Authentication**.

Topping Up Your Account

Ensure that your account balance is sufficient.

- For VPN pricing details, see **Pricing Details**.

2 Configuring Enterprise Edition VPN to Connect an On-premises Data Center and a VPC

2.1 Overview

Supported Regions

EU-Dublin

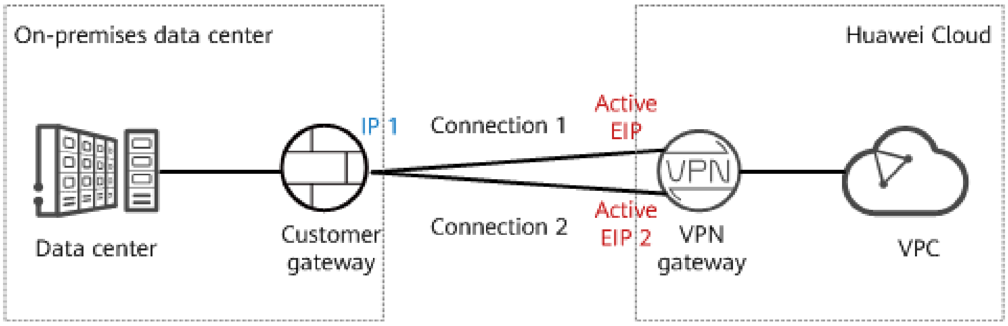
Scenario

To meet business development requirements, enterprise A needs to implement communication between its on-premises data center and its VPC. In this case, enterprise A can use the VPN service to create connections between the on-premises data center and the VPC.

- If the on-premises data center has only one customer gateway and this gateway can be configured with only one IP address, it is recommended that the VPN gateway uses the active-active mode. **Figure 2-1** shows the networking.

  In active-active mode, if connection 1 fails, traffic is automatically switched to connection 2, without affecting enterprise services. After connection 1 recovers, VPN still uses connection 2 for data transmission.

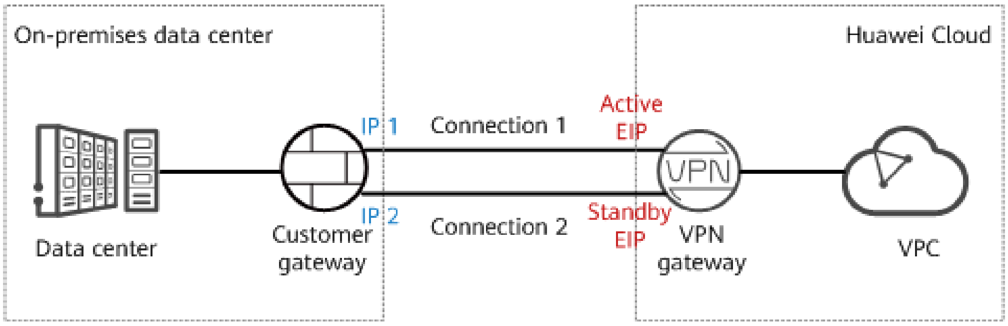
Figure 2-1 Active-active mode



- If the on-premises data center has two customer gateways or has only one customer gateway that can be configured with two IP addresses, it is recommended that the VPN gateway uses the active-standby mode. **Figure 2-2** shows the networking.

  In active-standby mode, connection 1 is the active link and connection 2 is the standby link. By default, traffic is transmitted only through the active link. If the active link fails, traffic is automatically switched to the standby link, without affecting enterprise services. After the active link recovers, traffic is switched back to the active link.

Figure 2-2 Active-standby mode



Limitations and Constraints

- The customer gateway device must support standard IKE and IPsec protocols.
- The customer gateway has a static public IP address.
- The on-premises data center subnets that need to access the VPC do not overlap with the VPC subnets or contain 100.64.0.0/10 or 214.0.0.0/8.

  If the VPC uses Direct Cloud or Cloud Connect connections to communicate with other VPCs, the on-premises data center subnets cannot overlap with those of these VPCs.

Data Plan

In this example, the VPN gateway uses the active-active mode.

Table 2-1 Data plan

Category	Item	Data
VPC	Subnet that needs to access the on-premises data center	192.168.0.0/16
VPN gateway	Interconnection subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses. 192.168.2.0/24

Category	Item	Data
	HA mode	Active-active
	EIP	EIPs are automatically generated when you buy them. By default, a VPN gateway uses two EIPs. In this example, the EIPs are as follows: ● Active EIP: 11.xx.xx.11 ● Active EIP 2: 11.xx.xx.12
VPN connection	Tunnel interface address	This address is used by a VPN gateway to establish an IPsec tunnel with a customer gateway. At the two ends of the IPsec tunnel, the configured local and remote tunnel interface addresses must be reversed. ● VPN connection 1: 169.254.70.1/30 ● VPN connection 2: 169.254.71.1/30
On-premises data center	Subnet that needs to access the VPC	172.16.0.0/16
Customer gateway	Gateway IP address	The gateway IP address is assigned by a carrier. In this example, the gateway IP address is: 22.xx.xx.22
	Tunnel interface address	● VPN connection 1: 169.254.70.2/30 ● VPN connection 2: 169.254.71.2/30

Operation Process

Figure 2-3 shows the process of using the VPN service to enable communication between an on-premises data center and a VPC.

Figure 2-3 Operation process

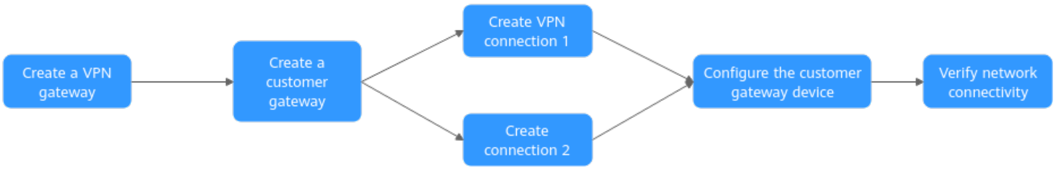

Create a VPN gateway
Create a customer gateway
Create VPN connection 1
Create connection 2
Configure the customer gateway device
Verify network connectivity

Table 2-2 Operation process description

No.	Step	Description
1	**Step 1: Creating a VPN Gateway**	Bind two EIPs to the VPN gateway. If you have purchased EIPs, you can directly bind them to the VPN gateway.
2	**Step 2: Creating a Customer Gateway**	Configure the VPN device in the on-premises data center as the customer gateway.
3	**Step 3: Creating VPN Connection 1**	Create a VPN connection between the active EIP of the VPN gateway and the customer gateway.
4	**Step 4: Creating VPN Connection 2**	Create a VPN connection between active EIP 2 of the VPN gateway and the customer gateway. It is recommended that the routing mode, PSK, IKE policy, and IPsec policy settings of the two VPN connections be the same.
5	**Step 5: Configuring the Customer Gateway Device**	● The local and remote tunnel interface addresses configured on the customer gateway device must be the same as the customer and local tunnel interface addresses of the Huawei Cloud VPN connection, respectively. ● The routing mode, PSK, IKE policy, and IPsec policy settings on the customer gateway device must be same as those of the Huawei Cloud VPN connection.
6	**Step 6: Verifying Network Connectivity**	Log in to an ECS and run the **ping** command to verify the network connectivity.

2.2 Step 1: Creating a VPN Gateway

Prerequisites

- A VPC has been created. For details about how to create a VPC, see **Creating a VPC and Subnet**.
- Security group rules have been configured for ECSs in the VPC, and allow the customer gateway in the on-premises data center to access VPC resources. For details about how to configure security group rules, see **Security Group Rules**.

Procedure

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Choose **Virtual Private Network** > **Enterprise – VPN Gateways**, and click **Buy VPN Gateway**.

Step 4 Set parameters as prompted and click **Next**.

The following describes only key parameters. For details about more parameters, see **Creating a VPN Gateway**.

Table 2-3 Key VPN gateway parameters

Parameter	Description	Example Value
Billing Mode	The options include **Yearly/Monthly** and **Pay-per-use**.	Yearly/Monthly
Region	Select the region nearest to you.	EU-Dublin
Name	Name a VPN gateway.	vpngw-001
Network Type	● **Public network**: A VPN gateway communicates with a customer gateway in an on-premises data center through the Internet. ● **Private network**: A VPN gateway communicates with a customer gateway in an on-premises data center through a private network.	Public network
Associate With	Select **VPC**.	VPC
VPC	Select the VPC that needs to access the on-premises data center.	vpc-001(192.168.0.0/16)
Local Subnet	Specify the VPC subnet that needs to access the on-premises data center. You can manually enter a CIDR block or select a subnet from the drop-down list box.	192.168.0.0/24
Interconnection Subnet	This subnet is used for communication between the VPN gateway and VPC. Ensure that the selected interconnection subnet has four or more assignable IP addresses.	192.168.2.0/24
HA Mode	Select **Active-active**.	Active-active
Active EIP	You can buy a new EIP or use an existing EIP.	11.xx.xx.11
Active EIP 2		11.xx.xx.12

----End

Verification

Check the created VPN gateway on the **VPN Gateways** page. The initial state of the VPN gateway is **Creating**. After about 2 minutes, the state changes to **Normal**, indicating that the VPN gateway is successfully created.

2.3 Step 2: Creating a Customer Gateway

Procedure

Step 1 Choose **Virtual Private Network** > **Enterprise – Customer Gateways**, and click **Create Customer Gateway**.

Step 2 Set parameters as prompted and click **OK**.

The following describes only key parameters. For details about more parameters, see **Creating a Customer Gateway**.

Table 2-4 Customer gateway parameters

Parameter	Description	Example Value
Name	Name a customer gateway.	cgw-001
Routing Mode	Select **Static**.	Static
Gateway IP Address	Enter the IP address of the customer gateway in the on-premises data center.	22.xx.xx.22

----End

Verification

Check the created customer gateway on the **Customer Gateways** page.

2.4 Step 3: Creating VPN Connection 1

Procedure

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Set parameters for VPN connection 1 as prompted and click **Submit**.

   The following describes only key parameters. For details, see **Creating a VPN Connection**.

Table 2-5 Parameter settings for VPN connection 1

Parameter	Description	Example Value
Name	Enter the name of VPN connection 1.	vpn-001
VPN Gateway	Select the VPN gateway created in **Step 1: Creating a VPN Gateway**.	vpngw-001
Gateway IP Address	Select the active EIP of the VPN gateway.	11.xx.xx.11
Customer Gateway	Select the customer gateway created in **Step 2: Creating a Customer Gateway**.	cgw-001
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Enter the subnet of the on-premises data center that needs to access the VPC.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Tunnel Interface IP Address	Specify the tunnel IP address of the VPN gateway. **NOTE** The local and remote interface addresses configured on the customer gateway device must be the same as the values of **Customer Tunnel Interface IP Address** and **Local Tunnel Interface IP Address**, respectively.	169.254.70.2/30
Customer Tunnel Interface IP Address	Specify the tunnel IP address of the customer gateway.	169.254.70.1/30
Link Detection	This function is used for route reliability detection in multi-link scenarios. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	**NQA** enabled

Parameter	Description	Example Value
PSK, Confirm PSK	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default

Verification

Check the created VPN connection on the **VPN Connections** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

2.5 Step 4: Creating VPN Connection 2

Procedure

1. Choose **Virtual Private Network** > **Enterprise – VPN Connections**, and click **Buy VPN Connection**.
2. Set parameters for VPN connection 2 as prompted and click **Submit**.

   For VPN connection 2, you are advised to use the same settings as VPN connection 1, except the connection name, gateway IP address, local tunnel interface IP address, and customer tunnel interface IP address.

Table 2-6 Parameter settings for VPN connection 2

Parameter	Description	Example Value
Name	Enter the name of VPN connection 2.	vpn-002
VPN Gateway	Select the VPN gateway created in **Step 1: Creating a VPN Gateway**.	vpngw-001
Gateway IP Address	Select active EIP 2 of the VPN gateway.	11.xx.xx.12
Customer Gateway	Select the customer gateway created in **Step 2: Creating a Customer Gateway**.	cgw-001

Parameter	Description	Example Value
VPN Type	Select **Static routing**.	Static routing
Customer Subnet	Enter the subnet of the on-premises data center that needs to access the VPC.	172.16.0.0/16
Interface IP Address Assignment	The options include **Manually specify** and **Automatically assign**.	Manually specify
Local Tunnel Interface IP Address	Specify the tunnel IP address of the VPN gateway. **NOTE** The local and remote interface addresses configured on the customer gateway device must be the same as the values of **Customer Tunnel Interface IP Address** and **Local Tunnel Interface IP Address**, respectively.	169.254.71.2/30
Customer Tunnel Interface IP Address	Specify the tunnel IP address of the customer gateway.	169.254.71.1/30
Link Detection	This function is used for route reliability detection in multi-link scenarios. **NOTE** When enabling this function, ensure that the customer gateway supports ICMP and is correctly configured with the customer interface IP address of the VPN connection. Otherwise, VPN traffic will fail to be forwarded.	**NQA** enabled
PSK, Confirm PSK	Specify the negotiation key of the VPN connection. The PSKs configured on the VPN console and the customer gateway device must be the same.	Test@123
Policy Settings	Configure the IKE and IPsec policies, which define the encryption algorithms used by the VPN tunnel. The policy settings on the VPN console and the customer gateway device must be the same.	Default

Verification

Check the created VPN connection on the **VPN Connections** page. The initial state of the VPN connection is **Creating**. As the customer gateway device has not been configured, no VPN connection can be established. After about 2 minutes, the VPN connection state changes to **Not connected**.

2.6 Step 5: Configuring the Customer Gateway Device

Procedure

NOTE

In this example, the customer gateway device is a Huawei AR router. For more examples of configuring customer gateway devices, see **Administrator Guide**.

Step 1 Log in to the AR router.

Step 2 Enter the system view.

```
<AR651>system-view
```

Step 3 Configure an IP address for the WAN interface. In this example, the WAN interface of the AR router is GigabitEthernet 0/0/8.

```
[AR651]interface GigabitEthernet 0/0/8
[AR651-GigabitEthernet0/0/8]ip address 22.xx.xx.22 255.255.255.0
[AR651-GigabitEthernet0/0/8]quit
```

Step 4 Configure a default route.

```
[AR651]ip route-static 0.0.0.0 0.0.0.0 22.xx.xx.1
```

In this command, *22.xx.xx.1* is the gateway address of the AR router's public IP address. Replace it with the actual gateway address.

Step 5 Enable the SHA-2 algorithm to be compatible with the standard RFC algorithms.

```
[AR651]IPsec authentication sha2 compatible enable
```

Step 6 Configure an IPsec proposal.

```
[AR651]IPsec proposal hwproposal1
[AR651-IPsec-proposal-hwproposal1]esp authentication-algorithm sha2-256
[AR651-IPsec-proposal-hwproposal1]esp encryption-algorithm aes-128
[AR651-IPsec-proposal-hwproposal1]quit
```

Step 7 Configure an IKE proposal.

```
[AR651]ike proposal 2
[AR651-ike-proposal-2]encryption-algorithm aes-128
[AR651-ike-proposal-2]dh group15
[AR651-ike-proposal-2]authentication-algorithm sha2-256
```

```
[AR651-ike-proposal-2]authentication-method pre-share
[AR651-ike-proposal-2]integrity-algorithm hmac-sha2-256
[AR651-ike-proposal-2]prf hmac-sha2-256
[AR651-ike-proposal-2]quit
```

Step 8 Configure IKE peers.

```
[AR651]ike peer hwpeer1
[AR651-ike-peer-hwpeer1]undo version 1
[AR651-ike-peer-hwpeer1]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer1]ike-proposal 2
[AR651-ike-peer-hwpeer1]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer1]remote-address 11.xx.xx.11
[AR651-ike-peer-hwpeer1]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer1]rsa signature-padding pss
[AR651-ike-peer-hwpeer1]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer1]quit
#
[AR651]ike peer hwpeer2
[AR651-ike-peer-hwpeer2]undo version 1
[AR651-ike-peer-hwpeer2]pre-shared-key cipher Test@123
[AR651-ike-peer-hwpeer2]ike-proposal 2
[AR651-ike-peer-hwpeer2]local-address 22.xx.xx.22
[AR651-ike-peer-hwpeer2]remote-address 11.xx.xx.12
[AR651-ike-peer-hwpeer2]rsa encryption-padding oaep
[AR651-ike-peer-hwpeer2]rsa signature-padding pss
[AR651-ike-peer-hwpeer2]ikev2 authentication sign-hash sha2-256
[AR651-ike-peer-hwpeer2]quit
```

The commands are described as follows:

- **pre-shared-key cipher**: configures a PSK, which must be the same as that configured on the VPN console.
- **local-address**: specifies the public IP address of the AR router.
- **remote-address**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 9 Configure an IPsec profile.

```
[AR651]IPsec profile hwpro1
[AR651-IPsec-profile-hwpro1]ike-peer hwpeer1
```

```
[AR651-IPsec-profile-hwpro1]proposal hwproposal1
[AR651-IPsec-profile-hwpro1]pfs dh-group15
[AR651-IPsec-profile-hwpro1]quit
#
[AR651]IPsec profile hwpro2
[AR651-IPsec-profile-hwpro2]ike-peer hwpeer2
[AR651-IPsec-profile-hwpro2]proposal hwproposal1
[AR651-IPsec-profile-hwpro2]pfs dh-group15
[AR651-IPsec-profile-hwpro2]quit
```

Step 10 Configure virtual tunnel interfaces.

```
[AR651]interface Tunnel0/0/1
[AR651-Tunnel0/0/1]mtu 1400
[AR651-Tunnel0/0/1]ip address 169.254.70.1 255.255.255.252
[AR651-Tunnel0/0/1]tunnel-protocol IPsec
[AR651-Tunnel0/0/1]source 22.xx.xx.22
[AR651-Tunnel0/0/1]destination 11.xx.xx.11
[AR651-Tunnel0/0/1]IPsec profile hwpro1
[AR651-Tunnel0/0/1]quit
#
[AR651]interface Tunnel0/0/2
[AR651-Tunnel0/0/2]mtu 1400
[AR651-Tunnel0/0/2]ip address 169.254.71.1 255.255.255.252
[AR651-Tunnel0/0/2]tunnel-protocol IPsec
[AR651-Tunnel0/0/2]source 22.xx.xx.22
[AR651-Tunnel0/0/2]destination 11.xx.xx.12
[AR651-Tunnel0/0/2]IPsec profile hwpro2
[AR651-Tunnel0/0/2]quit
```

The commands are described as follows:

- **interface Tunnel0/0/1** and **interface Tunnel0/0/2**: indicate the tunnel interfaces corresponding to the two VPN connections.

  In this example, Tunnel0/0/1 establishes a VPN connection with the active EIP of the VPN gateway, and Tunnel0/0/2 establishes a VPN connection with active EIP 2 of the VPN gateway.
- **ip address**: configures an IP address for a tunnel interface on the AR router.

- **source**: specifies the public IP address of the AR router.
- **destination**: specifies the active EIP or active EIP 2 of the VPN gateway.

Step 11 Configure NQA.

```
[AR651]nqa test-instance IPsec_nqa1 IPsec_nqa1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]test-type icmp
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]destination-address ipv4 169.254.70.2
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]source-address ipv4 169.254.70.1
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]frequency 15
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]ttl 255
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]start now
[AR651-nqa-IPsec_nqa1-IPsec_nqa1]quit
#
[AR651]nqa test-instance IPsec_nqa2 IPsec_nqa2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]test-type icmp
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]destination-address ipv4 169.254.71.2
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]source-address ipv4 169.254.71.1
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]frequency 15
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]ttl 255
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]start now
[AR651-nqa-IPsec_nqa2-IPsec_nqa2]quit
```

The commands are described as follows:

- **nqa test-instance IPsec_nqa1 IPsec_nqa1** and **nqa test-instance IPsec_nqa2 IPsec_nqa2**: configure two NQA test instances named **IPsec_nqa1** and **IPsec_nqa2**.

  In this example, the test instance **IPsec_nqa1** is created for the VPN connection to which the active EIP of the VPN gateway belongs; the test instance **IPsec_nqa2** is created for the VPN connection to which active EIP 2 of the VPN gateway belongs.
- **destination-address**: specifies the tunnel interface address of the VPN gateway.
- **source-address**: specifies the tunnel interface address of the AR router.

Step 12 Configure association between the static route and NQA.

```
[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/1 track nqa IPsec_nqa1 IPsec_nqa1

[AR651]ip route-static 192.168.0.0 255.255.255.0 Tunnel0/0/2 track nqa IPsec_nqa2 IPsec_nqa2
```

The parameters are described as follows:

- **192.168.0.0** indicates the local subnet of the VPC.
- **Tunnel***x* and **IPsec_nqa***x* in the same command correspond to the same VPN connection.

----End

Verification

Step 1 Log in to the management console.

Step 2 Click **Service List** and choose **Networking** > **Virtual Private Network**.

Step 3 Choose **Virtual Private Network** > **Enterprise – VPN Connections**. Verify that the states of the two VPN connections are both **Available**.

----End

2.7 Step 6: Verifying Network Connectivity

Procedure

Step 1 Log in to the management console.

Step 2 Click 📍 in the upper left corner and select the desired region and project.

Step 3 Click **Service List** and choose **Compute** > **Elastic Cloud Server**.

Step 4 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.

Step 5 Run the following command on the ECS:

ping 172.16.0.100

172.16.0.100 is the IP address of a server in the on-premises data center. Replace it with an actual server IP address.

If information similar to the following is displayed, the VPC on the cloud and the on-premises data center can communicate with each other.

```
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=28ms TTL=245
Reply from xx.xx.xx.xx: bytes=32 time=27ms TTL=245
```

----End