Direct Connect

User Guide

Issue 01

Date 2025-02-10

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.

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/

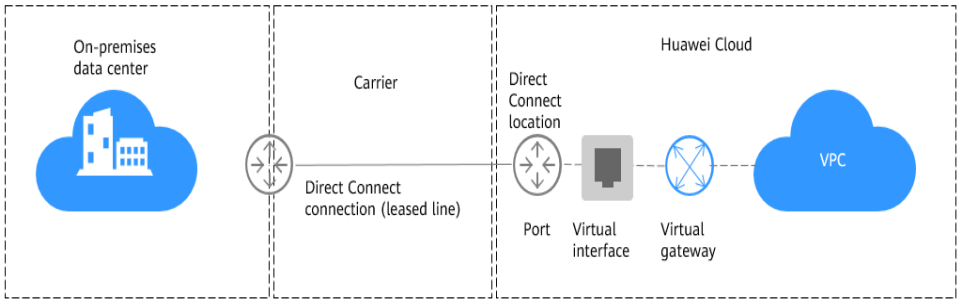
Contents

1 Connections

1.1 Creating a Connection

Figure 1-1 shows how Direct Connect connects your on-premises data center to a VPC.

Figure 1-1 Connecting your on-premises data center to a VPC



Self-Service Installation

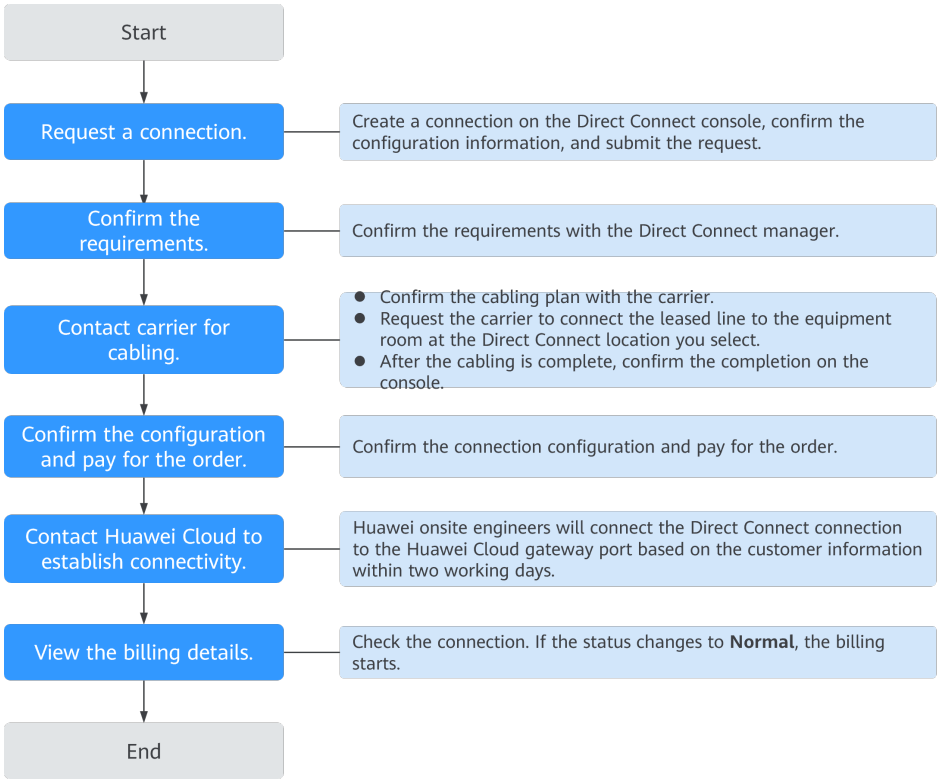
- **Scenario**

  You need to create a connection to connect your on-premises data center to the Direct Connect location you have selected to build a hybrid cloud.

  After you create a connection on the console, Huawei Cloud will provide a dedicated port for exclusive use. To establish connectivity, you need to contact the carrier to connect the leased line to the Direct Connect location you have selected.

  Figure 1-2 shows the process of connecting your on-premises data center to Huawei Cloud using Direct Connect.

Figure 1-2 Self-service installation process



- **Procedure**

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

  b. In the upper left corner of the page, click  and select a region and project.

  c. In the upper right corner, click **Create Connection**.

  d. On the **Create Connection** page, enter the equipment room details and select the Direct Connect location and port based on **Table 1-1**.

Figure 1-3 Creating a self-service connection

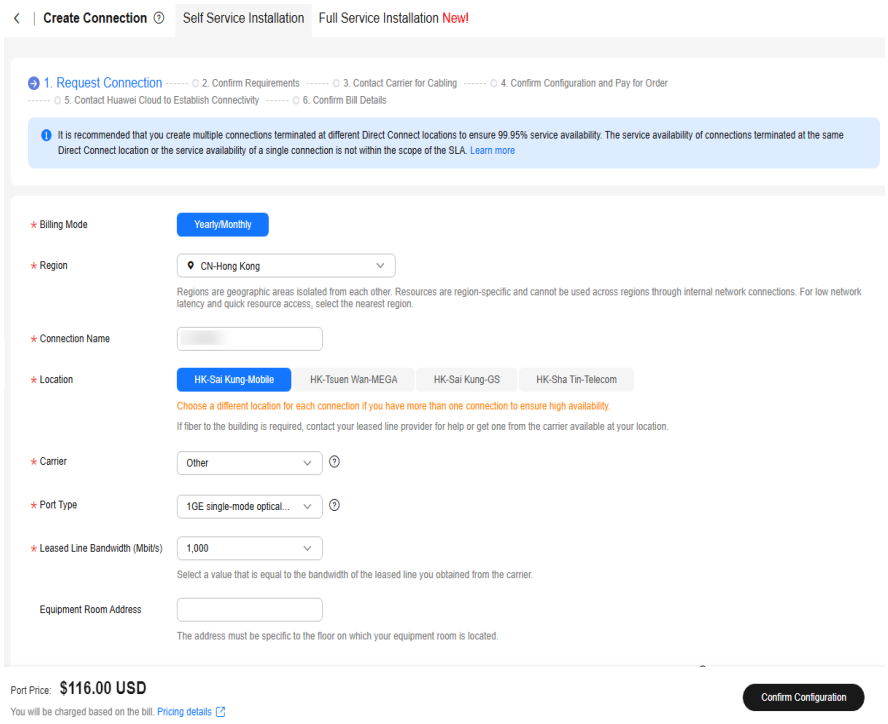


Table 1-1 Parameters for creating a connection

Parameter	Example Value	Description
Billing Mode	Yearly/Monthly	Specifies how you will be billed for the connection. Currently, only **Yearly/Monthly** is supported.
Region	CN-Hong Kong	Specifies the region where the connection resides. You can also change the region in the upper left corner of the console.
Connection Name	dc-123	Specifies the name of the connection.
Location	HK-Sai Kung-Mobile	Specifies the Direct Connect location where your leased line can be connected to.
Carrier	Other	Specifies the carrier that provides the leased line.
Port Type	1GE single-mode optical port	Specifies the type of the port: 1GE single-mode optical port, 10GE single-mode optical port, 40GE single-mode optical port, or 100GE single-mode optical port.

Parameter	Example Value	Description
Leased Line Bandwidth (Mbit/s)	100	Specifies the bandwidth of the line you need to lease from the carrier.
Equipment Room Address	Room xx, xx building, xx road, xx district, xx city	Specifies the address of your equipment room. The address must be specific to the floor your equipment room is on.
Tag	example_key1 example_value1	Adds tags to help you identify your connection. You can change them after the connection is created.
Description	-	Provides supplementary information about the connection.
Required Duration	3 months	Specifies how long the connection will be used for.
Auto-renew	3 months	Specifies whether to automatically renew the subscription to ensure service continuity. For example, if you select this option and the required duration is three months, the system automatically renews the subscription for another three months.
Enterprise Project	default	Specifies the enterprise project by which connections are centrally managed. Select an existing enterprise project.

e. Click **Confirm Configuration**.

f. Confirm the configuration and click **Request Connection**.

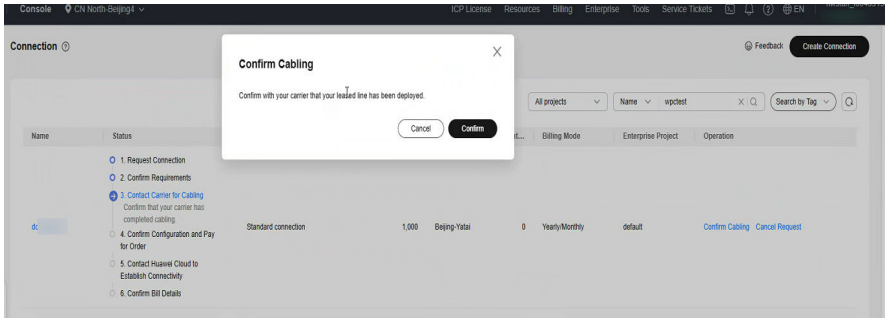
Then confirm the requirements with the Direct Connect manager.

If the request is not approved, repeat **c** to **f** based on the review comments and submit the request again.

g. After the request is approved, contact the carrier for cabling.

After the cabling is complete, locate the connection in the connection list and click **Confirm Cabling** in the **Operation** column.

Figure 1-4 Confirm Cabling



h. In the displayed dialog box, click **OK**.

i. In the connection list, locate the connection and click **Confirm Configuration** in the **Operation** column.

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

k. Confirm the order, select a payment method, and click **Confirm**.

l. Wait for Huawei Cloud to complete the construction.

   Huawei onsite engineers will connect the leased line to the port on the Huawei Cloud gateway based on the customer's information within two working days.

m. Verify that the connection is in the **Normal** state, which means that the connection is ready, and the billing starts.

NOTE

After the connection is ready, you need to create a virtual gateway and associate it with the VPC you want to access on the **Virtual Gateways** page.

Create a virtual interface to associate the connection with the created virtual gateway, so that you can connect your on-premises data center to the VPC through the connection.

Full-Service Installation

- **Scenario**

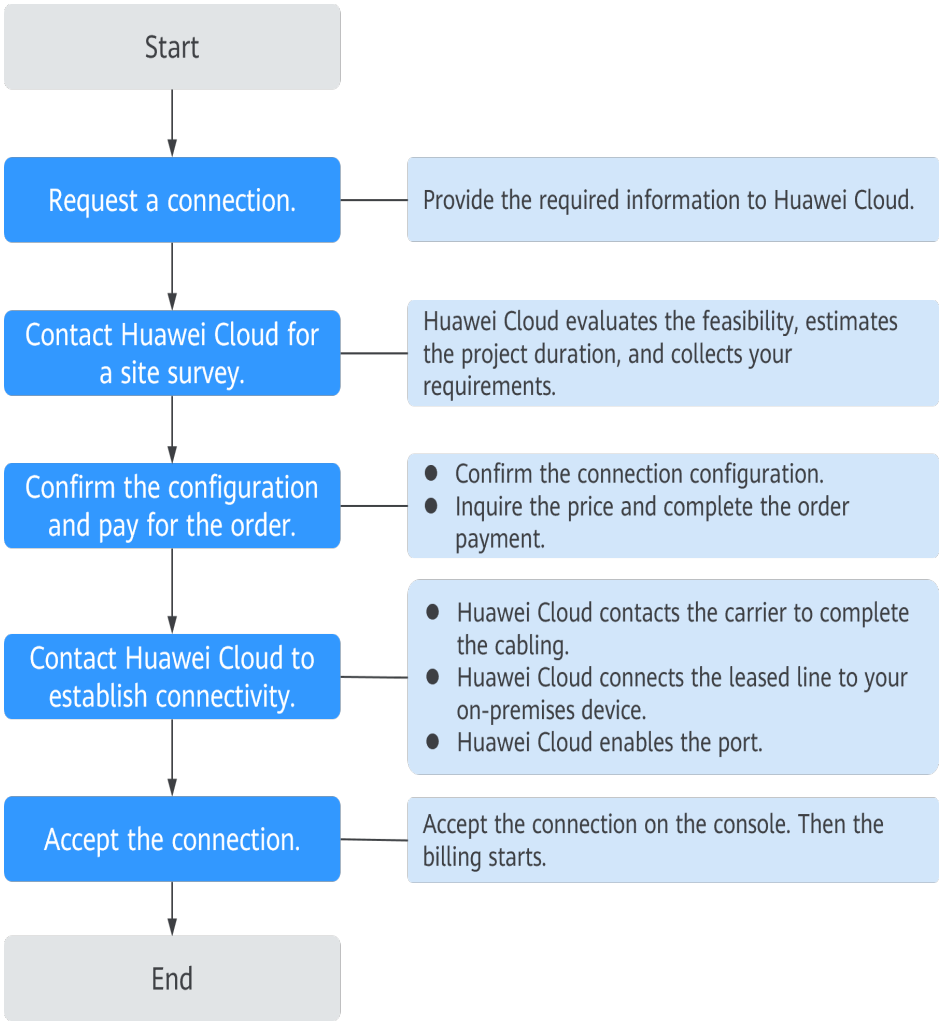
  Huawei Cloud completes all operations required for connecting your on-premises data center to the cloud, including integrating the network resources and ports.

  Figure 1-5 shows the entire process.

  NOTE

  Full-service connections are now available in the following regions: CN-Hong Kong and CN South-Guangzhou.

Figure 1-5 Full-service installation process



- **Procedure**

  a. Submit your request.

     i. Go to the **Connections** page.

     ii. In the upper left corner of the page, click  and select a region and project.

     iii. In the upper right corner, click **Create Connection**.

     iv. Click **Full Service Installation**.

     v. Provide information about your equipment room and select a Huawei Cloud location. For details about the parameters, see **Table 1-2**.

Figure 1-6 Creating a full-service connection

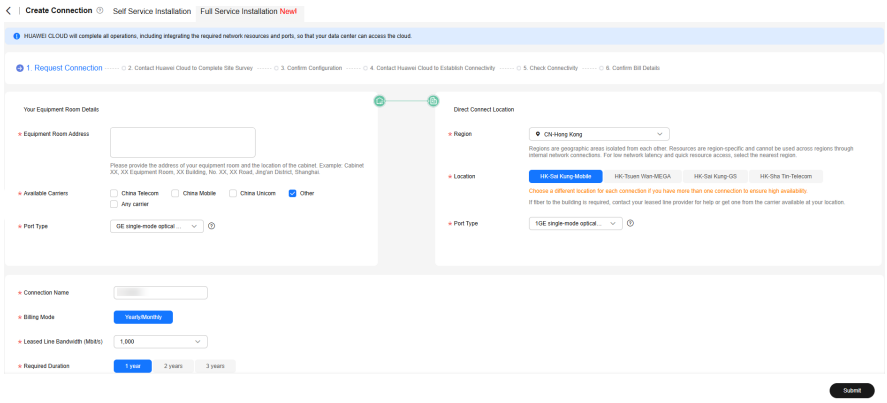


Table 1-2 Parameters for creating a connection

Parameter	Example Value	Description
Equipment Room Address	Room xx, xx building, xx road, xx district, xx city	Specifies the address of your equipment room. The address must be specific to the floor your equipment room is on.
Available Carriers	Other	Specifies the carriers that are allowed to enter your equipment room.
Port Type	GE single-mode optical port	Specifies the type of port on the device in your equipment room for connecting to the leased line.
Region	CN-Hong Kong	Specifies the region where the connection resides. You can also change the region in the upper left corner of the console.
Location	HK-Sai Kung-Mobile	Specifies the Direct Connect location where your leased line can be connected to.
Port Type	GE single-mode optical port	Specifies the type of the port: GE single-mode optical port, GE electrical port, 10GE single-mode optical port, 10GE electrical port, 40GE single-mode optical port, or 100GE single-mode optical port.
Connection Name	dc-123	Specifies the name of your connection.
Leased Line Bandwidth (Mbit/s)	1,000	Specifies the bandwidth of the leased line.

Parameter	Example Value	Description
Billing Mode	Yearly/Monthly	Specifies how you will be billed for the connection. Currently, only **Yearly/Monthly** is supported.
Required Duration	1 year	Specifies how long the connection will be used for.
Enterprise Project	default	Specifies the enterprise project by which connections are centrally managed. Select an existing enterprise project.
Contact Person/Phone Number/Email	Tom +86 139xxxxxxxx Tom@mail.com	Specifies who is responsible for your connection. **CAUTION** If no contact information is provided, we will contact the person in your account information. This will prolong the review period.

vi. Click **Submit**.

b. Wait for Huawei Cloud's site survey.

Huawei Cloud evaluates your requirements and the carrier's resources and confirms whether your requirements can be met. If your requirements can be met, Huawei Cloud will place an order for you.

NOTE

Generally, the site survey takes three working days.

c. Confirm and pay for the order.

i. In the connection list, locate the connection and click **Confirm Configuration** in the **Operation** column.

ii. Confirm the connection configuration and expenses, and then click **Next**.

NOTE

You need to read and agree to the **Full-Service Installation Statement** before paying for the order.

iii. On the purchase page, select a payment mode and click **Pay**.

NOTE

If you select **Download Contract**, download a contract on the contract page and complete the payment. Discounts, if any, will automatically apply.

d. Wait for Huawei Cloud to complete the following work:

i. Contacts the carrier to deploy the leased line.

ii. Connects your on-premises data center to the cloud using the leased line.

iii. Contacts the carrier to complete in-building cabling.

NOTE

This step is required when you choose a full-service connection with a dedicated port and need cabling for your site.

iv. Enables the port.

e. Confirm that you want to enable Direct Connect.

i. In the connection list, locate the connection and click **Confirm Completion** in the **Operation** column.

ii. Click **OK**. Confirm that your connection is available for use, and the billing starts.

1.2 Viewing a Connection

Scenario

After a connection is created, you can view its details.

Procedure

1. Go to the **Connections** page.
2. Locate the connection you want to view and click its name to view the details.

1.3 Modifying a Connection

Scenario

After creating a connection, you can modify its name, bandwidth, equipment room address, and description.

1. In the upper left corner of the page, click  and select a region and project.
2. Locate the connection you want to modify and click **Modify** in the **Operation** column.
3. Modify the connection and click **OK**.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection you want to modify and click **Modify** in the **Operation** column.
4. Modify the connection and click **OK**.

1.4 Unsubscribing from a Connection

Scenario

If you do not need to use a self-service connection any longer, you can unsubscribe from it.

NOTE

You can only unsubscribe from connections that are in the **Normal** state. If a connection is being created, you can unsubscribe from it after the connection is created.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click and select a region and project.
3. Locate the connection that you want to unsubscribe from and click **Unsubscribe** in the **Operation** column.
4. Locate the target connection and click **Unsubscribe from Resource** in the **Operation** column.
5. On the **Unsubscribe** page, select the reason for unsubscription, confirm the refund amount, and select **I understand a handling fee will be charged for this unsubscription**.
6. Click **Confirm**.

1.5 Renewing a Connection

Scenario

You can renew the subscription when a connection is about to expire.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click and select a region and project.
3. Locate the connection you want to renew and choose **More** > **Renew** in the **Operation** column.
4. Set the duration that you want to renew the connection and click **Pay**. Then pay the order as prompted.

1.6 Managing Connection Tags

Scenario

After a connection is created, you can view its tags or add, edit or delete a tag.

A tag is the identifier of a connection and consists of a key and a value. You can add 20 tags to a connection.

NOTE

If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value.

For details about predefined tags, see **Predefined Tag Overview**.

If you have configured tag policies for Direct Connect, you need to add tags to your connections based on the tag policies. If you add a tag that does not comply with the tag policies, connections may fail to be created. Contact your administrator to learn more about tag policies.

Adding a Tag

Add a tag to an existing connection.

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection and click its name to switch to the **Summary** page.
4. Click the **Tags** tab.
5. Click **Add Tag**.
6. In the displayed dialog box, enter a key and a value.

   If you have configured tag policies for Direct Connect, you need to add tags to your connections based on the tag policies. If you add a tag that does not comply with the tag policies, connections may fail to be created. Contact your administrator to learn more about tag policies.

   Table 1-3 describes the tag key and value requirements.

   Table 1-3 Tag key and value requirements

Parameter	Requirements
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 characters. • Can contain only letters, digits, hyphens, and underscores.
Value	• Can be left blank. • Can contain a maximum of 43 characters. • Can contain only letters, digits, periods, hyphens, and underscores.

7. Click **OK**.

Editing a Tag

Modify the value of a tag added to a connection.

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection and click its name to switch to the **Summary** page.
4. Click the **Tags** tab.
5. In the tag list, locate the tag you want to modify and click **Edit** in the **Operation** column.
6. Enter a new value.
7. Click **OK**.

Deleting a Tag

Delete a tag from a connection.

CAUTION

Deleted tags cannot be recovered.

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection and click its name to switch to the **Summary** page.
4. Click the **Tags** tab.
5. In the tag list, locate the tag you want to delete and click **Delete** in the **Operation** column.
6. Click **Yes**.

2 Virtual Gateways

2.1 Creating a Virtual Gateway

Scenario

You can create a virtual gateway and associate it with the VPC that you need to access.

Procedure

1. Go to the **Virtual Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the upper right corner, click **Create Virtual Gateway**.
4. Configure the parameters based on **Table 2-1**.

Figure 2-1 Creating a virtual gateway

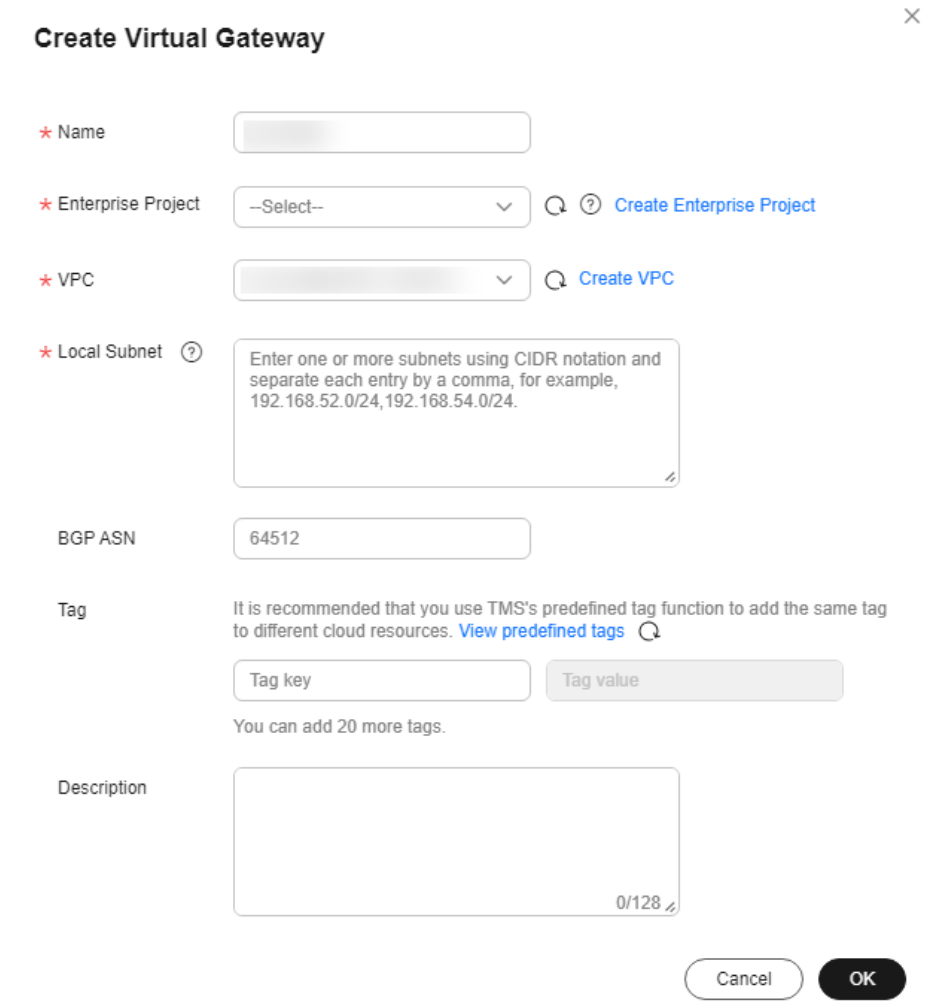


Table 2-1 Parameters required for creating a virtual gateway

Parameter	Example Value	Description
Name	vgw-123	Specifies the virtual gateway name. The name can contain 1 to 64 characters.
Enterprise Project	default	Specifies the enterprise project by which virtual gateways are centrally managed. Select an existing enterprise project.
VPC	VPC-001	Specifies the VPC to be associated with the virtual gateway.

Parameter	Example Value	Description
Local Subnet	192.168.0.0/16	Specifies the CIDR blocks of the subnets in the VPC to be accessed using Direct Connect. You can add one or more CIDR blocks. If there are multiple CIDR blocks, separate every entry with a comma (,).
BGP ASN	64512	Specifies the BGP ASN of the virtual gateway. **NOTE** Generally, Huawei Cloud's BGP ASN is 64512. There are two special cases: • In the CN North-Beijing1 region, the default BGP ASN of Huawei Cloud is 65533. • In the AP-Bangkok region, the BGP ASN of some Direct Connect locations is 65535 by default. For details, contact the Direct Connect manager.
Tag	example_key1 example_value1	Adds tags to help you identify your virtual gateway. You can change them after the virtual gateway is created.
Description	-	Provides supplementary information about the virtual gateway.

5. Click **OK**.
   When the status changes to **Normal**, the virtual gateway has been created.

2.2 Viewing a Virtual Gateway

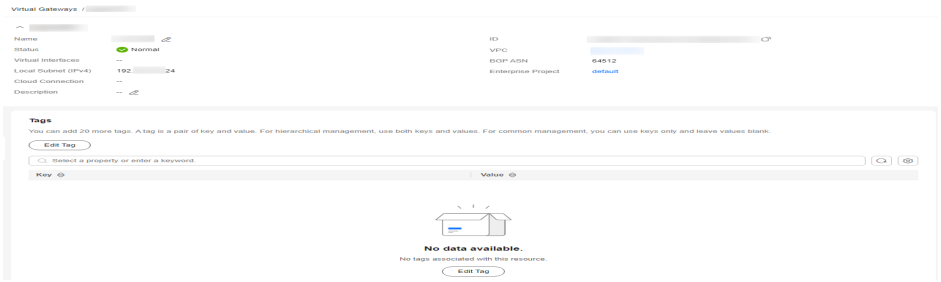
Scenario

You can view details about a virtual gateway.

Procedure

1. Go to the **Virtual Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the virtual gateway and click its name to view the details.

Figure 2-2 Viewing a virtual gateway



2.3 Modifying a Virtual Gateway

Scenario

After creating a virtual gateway, you can modify its settings.

Procedure

1. Go to the **Virtual Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the virtual gateway you want to modify and click **Modify** in the **Operation** column.
4. Modify the name, local subnet, and description, and then click **OK**.

Figure 2-3 Modifying a virtual gateway

2.4 Deleting a Virtual Gateway

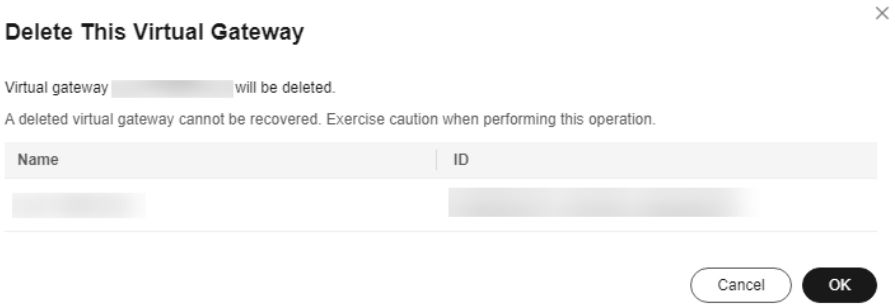
Scenario

You can delete a virtual gateway if you do not need it any longer and there are no virtual interfaces associated with it.

Procedure

1. Go to the **Virtual Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the virtual gateway you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **OK**.

Figure 2-4 Deleting a virtual gateway



3 Global DC Gateways

3.1 Global DC Gateway Overview

What Is a Global DC Gateway?

A global DC gateway enables your on-premises data center to access VPCs in multiple regions so you can use a single connection to provide high-speed access to cloud compute and storage resources in any region.

A global DC gateway can only be associated with connections terminated at the same Direct Connect location. If there are multiple connections terminated at different Direct Connect location, you need to create multiple global DC gateways.

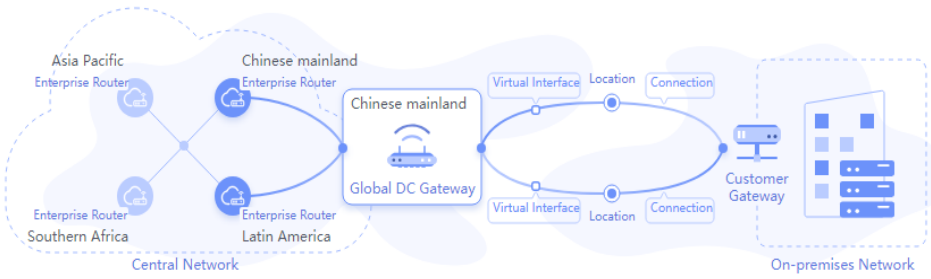
NOTE

Global DC gateways have been launched in some regions. You can view the regions where this feature is available on the console.

Connecting an On-Premises Data Center to VPCs in Different Regions

A global DC gateway can be attached to enterprise routers in different regions. This can reduce the network latency, simplify network topology, and improve network O&M efficiency.

Figure 3-1 Communication with VPCs in different regions using global DC gateways



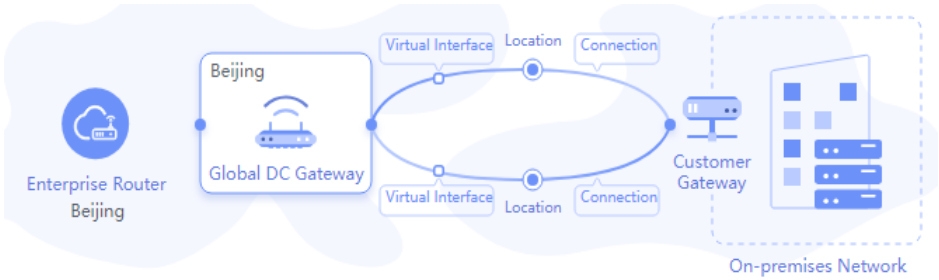
NOTE

If you need to use a central network for cross-region VPC communication, **submit a service ticket**.

Connecting an On-Premises Data Center to VPCs in the Same Region

A global DC gateway can be attached to enterprise routers in the same region for network communication. This can reduce the network latency, simplify network topology, and improve network O&M efficiency.

Figure 3-2 Communication with VPCs in the same region using global DC gateways



3.2 Creating a Global DC Gateway

Scenario

A global DC gateway can be attached to enterprise routers in the same region for network communication. This can reduce the network latency, simplify network topology, and improve network O&M efficiency.

This section describes how to create a global DC gateway and associate an enterprise router with it.

Procedure

Step	Description
Preparations	Before creating Direct Connect connections, sign up for a HUAWEI ID, enable cloud services, complete real-name authentication, top up your account, confirm the Direct Connect locations, confirm the port availability, contact the carrier to complete the site survey, and confirm the prices.

Step	Description
Step 1: Create a Connection	Create a connection to order a dedicated port and work with the carrier to connect the leased line to the cloud. This process involves operations of the customer, carrier, and Huawei Cloud. The operation instructions and the progress of each phase will be displayed on the console.
Step 2: Create a Global DC Gateway	When creating a global DC gateway, you can choose not to associate it with virtual interfaces and connections.
Step 3: Create a Virtual Interface	After a connection and a global DC gateway are created, you need to create a virtual interface to access the desired VPC.
Step 4: Associate an Instance	Associate the global DC gateway with an enterprise router. (A global DC gateway can also be associated with a central network.)

Preparations

Before creating resources such as connections, sign up for a HUAWEI ID, enable cloud services, complete real-name authentication, top up your account, confirm the Direct Connect locations, and complete the site survey.

- **Signing Up and Completing Real-Name Authentication**

  To access the Direct Connect console, you need an account. If you do not have an account, sign up for one.

  For details, see **Signing up for a HUAWEI ID and Enabling Huawei Cloud Services** and **Completing Real-Name Authentication**.

  If you have enabled Huawei Cloud services and completed real-name authentication, skip this step.

- **Topping up Your Account**

  Top up your account to ensure that your account has sufficient balance.

  - For details about Direct Connect pricing, see **Product Pricing Details**.
  - For details about how to top up an account, see **Topping up an Account**.

- **Selecting a Direct Connect Location**

  When selecting a location, you need to consider the distance to your on-premises data center, which carrier you want to choose, and which type of port will be used.

  - Distance to your on-premises data center

    Select a location nearest to your on-premises data center to reduce network latency. The telecom carriers and bandwidth capabilities vary at different locations.

  - Carrier

Select whichever carrier that can best meet your service requirements. Generally, you can choose one from carriers such as China Unicom, China Telecom, and China Mobile.

- Port type

  Decide what type of port you want to use, an optical port or electrical port.

  - Optical port: The carrier directly provides a fiber optic transmission path for the end user. The port speed is effectively infinite, only limited by the auto-negotiation rate of the optical modules at both ends, for example, 1GE, 10GE, 40GE, and 100GE.
  - Electrical port: Generally, RJ45 ports are used. The carrier uses an optical transceiver to convert electrical signals to optical signals required on the transmission network. The industry standard is to use this type of port when the bandwidth is less than 100 Mbit/s.

    NOTE

    - Currently, 1GE and 10GE single-mode optical ports can transmit data up to 10 km. If you need an optical port to transmit data for more than 10 km, or you need a 40GE or 100GE port, you need to purchase the optical modules by yourself.
    - Ensure that the leased line provider can provide the optical fibers to connect to Direct Connect devices.
    - No O/E conversion device is allowed on Huawei Cloud. Ensure that the leased line provider uses the correct line type to connect to Direct Connect devices.

To obtain detailed address of a **Direct Connect location**, contact the Direct Connect manager or **submit a service ticket**.

- **Requesting a Site Survey**: After you select a location, contact the carrier for a site survey.

  a. Consult the carrier about how to access the cloud.

     You can contact the Direct Connect manager or **submit a service ticket** to obtain the detailed address of the equipment room.

  b. Submit an application to Huawei Cloud for conducting a site survey in the equipment room.

     The application must include the name, ID card number, and contact information of the personnel who will go to the equipment room for the site survey.

     NOTE

     Pay attention to the following when you request a site survey:

     If the site survey can be completed at the meet-me room of the carrier, you do not need to submit an application.

  c. After the application is approved, Huawei Cloud will assist the carrier in entering the equipment room for completing the site survey within two working days.

  d. Ask the carrier to carry out the site survey and confirm the expenses, including those for:

- The port (paid to Huawei Cloud) and one-time setup (free for now)
- The leased line (paid to the carrier)
- In-building cabling

Step 1: Create a Connection

For details, see **Step 1: Create a Connection**.

Step 2: Create a Global DC Gateway

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the upper right corner, click **Create Global DC Gateway**.
4. Configure the parameters based on **Table 3-1**.

Table 3-1 Parameters for creating a global DC gateway

Parameter	Example Value	Description
Name	**dgw-123**	Specifies the name of the global DC gateway. • Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. • The name can contain 1 to 64 characters.
Enterprise Project	default	Specifies the enterprise project by which global DC gateways are centrally managed. Select an existing enterprise project.
BGP ASN	64512	Specifies the autonomous system number used on the cloud for a BGP session. You can use the default ASN, or specify an ASN in the range of 64512–65534 or 1–4294967295.
Tag	example_key1 example_value1	Adds tags to help you identify your global DC gateway. You can change them after the global DC gateway is created.
Description	-	Provides supplementary information about the global DC gateway. It can contain 0 to 128 characters.

5. Click **OK**.

   The page for creating a virtual interface is displayed.

   You can continue to **create a virtual interface** or click **Later** in the lower part of the page to suspend subsequent operations.

Step 3: Create a Virtual Interface

1. If you select **Later** for **Step 2: Create a Global DC Gateway**, locate the global DC gateway and click **Create Virtual Interface** in the **Operation** column.

   You can also click **Create one** in the **Virtual Interfaces** column.

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

Table 3-2 Parameters for creating a virtual interface

Parameter	Example Value	Description
Region	CN-Hong Kong	Specifies the region where the connection resides. You can also change the region in the upper left corner of the console.
Name	vif-123	Specifies the virtual interface name. The name can contain 1 to 64 characters.
Virtual Interface Priority	Preferred	Specifies whether the virtual interface will be preferentially used over other virtual interfaces. There are two options: **Preferred** and **Standard**. If multiple virtual interfaces are associated with one Direct Connect device, the load is balanced among virtual interfaces with the same priority, while virtual interfaces with different priorities are working in active/standby pairs.
Connection	-	Specifies the connection you can use to connect your on-premises network to Huawei Cloud.
Gateway	Global DC Gateway	Specifies the type of the gateway that the virtual interface connects to. The default option is **Global DC Gateway**.
Global DC Gateway	**dgw-123**	Specifies the global DC gateway that will be used.

Parameter	Example Value	Description
VLAN	30	Specifies the ID of the VLAN for the virtual interface. You need to configure the VLAN if you create a standard connection. The VLAN for a hosted connection will be allocated by the partner. You do not need to configure the VLAN.
Bandwidth (Mbit/s)	50	Specifies the bandwidth that can be used by the virtual interface. The bandwidth cannot exceed that of the connection or LAG.
Enterprise Project	default	Specifies the enterprise project by which virtual interfaces are centrally managed. Select an existing enterprise project.
Tag	example_key2 example_value2	Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created.
IP Address Family	**IPv4**	Specifies the address type of the virtual interface. The default option is **IPv4**.
Local Gateway	10.0.0.1/30	Specifies the IP address used by Huawei Cloud to connect to your on-premises network. After you configure **Local Gateway** on the console, the configuration will be automatically delivered to the gateway used by Huawei Cloud.
Remote Gateway	10.0.0.2/30	Specifies the gateway on your on-premises network. The remote gateway must be in the same IP address range as the local gateway. Generally, a subnet with a 30-bit mask is recommended.
Remote Subnet	192.168.51.0/24, 10.1.123.0/24	Specifies the subnets and masks of your on-premises network. If there are multiple subnets, use commas (,) to separate them.

Parameter	Example Value	Description
Routing Mode	BGP	Specifies whether static routing or dynamic routing is used to route traffic between your on-premises network and the cloud network. If there are or will be two or more connections, select BGP routing for higher availability.
BGP ASN	12345	Specifies the ASN of the BGP peer. This parameter is required when BGP routing is selected.
BGP MD5 Authentication Key	**Qaz12345678**	Specifies the password used to authenticate the BGP peer using MD5. This parameter can be set when BGP routing is selected, and the parameter values on both gateways must be the same. The key contains 8 to 255 characters and must contain at least two types of the following characters: • Uppercase letters • Lowercase letters • Digits • Special characters ~!,.:;-_"(){}[]/@#$%^&*+|=
Description	-	Provides supplementary information about the virtual interface.

3. Click **OK**.

   After the virtual interface is created, you can associate an instance with the global DC gateway.

   You can **associate an instance** with the global DC gateway now, or click **Later** in the lower part of the page to suspend subsequent operations.

Step 4: Associate an Instance

The following are steps for you to associate an enterprise router with the global DC gateway to set up a peer link.

1. If you select **Later** for **Step 3: Create a Virtual Interface**, locate the global DC gateway in the global DC gateway list and click **Add one** in the **Peer Link** column.
2. Configure the parameters based on **Table 3-3**.

Table 3-3 Parameters for associating an instance

Parameter	Example Value	Description
Resource Type	CN-Hong Kong	Specifies the type of the resource that the global DC gateway connects to. There are two options: **Central network** and **Peer link**. Select **Peer link** here. **NOTE** If you need to use a central network for cross-region VPC communication, **submit a service ticket**.
Name	connection-123	Specifies the name of the peer link you want to set up. • Only letters, digits, underscores (_), hyphens (-), and periods (.) are allowed. • The name can contain 1 to 64 characters.
Global DC Gateway	**dgw-123**	Specifies the global DC gateway used for setting up the peer link. By default, the created global DC gateway is selected.
Peer Link Type	Enterprise router	The default option is **Enterprise Router**.
Link To	-	Specifies the enterprise router at the other end of the peer link.

3. Click **OK**.

3.3 Associating an Instance with a Global DC Gateway

Scenario

After a global DC gateway is created, you can use it to set up peer links or attach it to a central network.

NOTE

If you need to use a central network for cross-region VPC communication, **submit a service ticket**.

Setting Up a Peer Link

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click and select a region and project.

3. In the global DC gateway list, locate the global DC gateway and click **More** > **Associate Instance** in the **Operation** column.
4. On the **Associate Instance** page, select the type of the instance to be associated.

   Select **Peer link** here.
5. Configure the parameters and click **OK**.

   After the peer link is created, you can click the name of the global DC gateway to go to the Peer Links tab and view the created peer link.

Attaching to a Central Network

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the global DC gateway list, locate the global DC gateway and click **More** > **Associate Instance** in the **Operation** column.
4. On the **Associate Instance** page, select the type of the instance to be associated.

   Select **Central network** here.
5. Click the redirection link to go to the **Central Networks** page.

   Add the global DC gateway as an attachment on a central network. For details, see **Adding Attachments**.

3.4 Viewing a Global DC Gateway

Scenario

After a global DC gateway is created, you can view its details, such as, its name, ID, status, location, BGP ASN, virtual interfaces, enterprise project, IP address family, peer links, tags, and routes.

Procedure

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the global DC gateway list, view the name, ID, status, location, BGP ASN, enterprise project, virtual interfaces, and peer links.

   Click the name of the global DC gateway to view more information.
   - On the **Basic Information** tab, view the name, ID, status, enterprise project, description, location, BGP ASN, the number of peer links, virtual interfaces, IP address family, the time when the gateway was created, and routes.
   - On the **Peer Links** tab, view the name, ID, status, bandwidth, resource type, resource linked to the global DC gateway, region, and location of each peer link.
   - On the **Tags** tab, view the tags added to the global DC gateway.

3.5 Modifying a Global DC Gateway

Scenario

You can modify the name, IP address family, and description of an existing global DC gateway.

Procedure

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the global DC gateway list, click the name of the global DC gateway you want to modify to go to the **Basic Information** page.

   You can also click  on the right of the global DC gateway name to change its name.
4. On the **Basic Information** tab, modify its name, description, IP address family, and routes.
   - Modifying the name or description: Click  next to the name or description, enter a new name or description as prompted, and click  .
   - Modifying the IP address family: Click **Modify** on the right of **IP Address Family**, change the address family of the global DC gateway, and click **OK**.
   - Modifying the routes: In the lower part of the page, add or delete the routes for the global DC gateway.

3.6 Deleting a Global DC Gateway

Scenario

You can delete a global DC gateway you no longer need.

Constraints

If a global DC gateway is in use, it cannot be deleted. You need to delete the resources associated with the global DC gateway, as described in **Table 3-4**.

Table 3-4 Reasons that a global DC gateway cannot be deleted and solutions

Reason	Solution
The global DC gateway has a virtual interface associated.	Delete the virtual interfaces. For details, see **Deleting a Virtual Interface**.

Reason	Solution
The global DC gateway has peer links.	Delete the peer links. For details about how to view the peer links, see **Viewing Peer Links**.

Procedure

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the global DC gateway list, locate the global DC gateway you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, click **OK**.

3.7 Managing Global DC Gateway Tags

Scenario

After a global DC gateway is created, you can add tags to it, or edit, view or delete its tags.

A tag is an identifier of a global DC gateway and consists of a key and a value. You can add 20 tags to a global DC gateway.

NOTE

If a predefined tag has been created on TMS, you can directly select the corresponding tag key and value.

For details about predefined tags, see **Predefined Tag Overview**.

If you have configured tag policies for Direct Connect, you need to add tags to your global DC gateways based on the tag policies. If you add a tag that does not comply with the tag policies, global DC gateways may fail to be created. Contact your administrator to learn more about tag policies.

Adding a Tag

Add a tag to an existing global DC gateway.

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Click the name of the global DC gateway that you want to add a tag to.
4. Click the **Tags** tab.
5. Click **Add Tag**.
6. In the displayed dialog box, enter a key and a value.

   Table 3-5 describes the tag key and value requirements.

Table 3-5 Tag naming requirements

Parameter	Requirements
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 36 characters. • Can contain only letters, digits, hyphens, and underscores.
Value	• Can be left blank. • Can contain a maximum of 43 characters. • Can contain only letters, digits, periods, hyphens, and underscores.

7. Click **OK**.

Editing a Tag

Modify the value of a tag added to a global DC gateway.

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Click the name of the global DC gateway whose tag you want to modify.
4. Click the **Tags** tab.
5. In the tag list, locate the tag you want to modify and click **Edit** in the **Operation** column.
6. Enter a new value.
7. Click **OK**.

Deleting a Tag

Delete a tag from a global DC gateway.

CAUTION

Deleted tags cannot be recovered.

1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Click the name of the global DC gateway that you want to delete a tag from.
4. Click the **Tags** tab.
5. In the tag list, locate the tag you want to delete and click **Delete** in the **Operation** column.
6. Click **Yes**.

4 Virtual Interfaces

4.1 Creating a Virtual Interface

Scenario

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

Procedure

1. Go to the **Virtual Interfaces** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the upper right corner, click **Create Virtual Interface**.
   Configure the parameters based on **Table 4-1**.

Figure 4-1 Creating a virtual interface

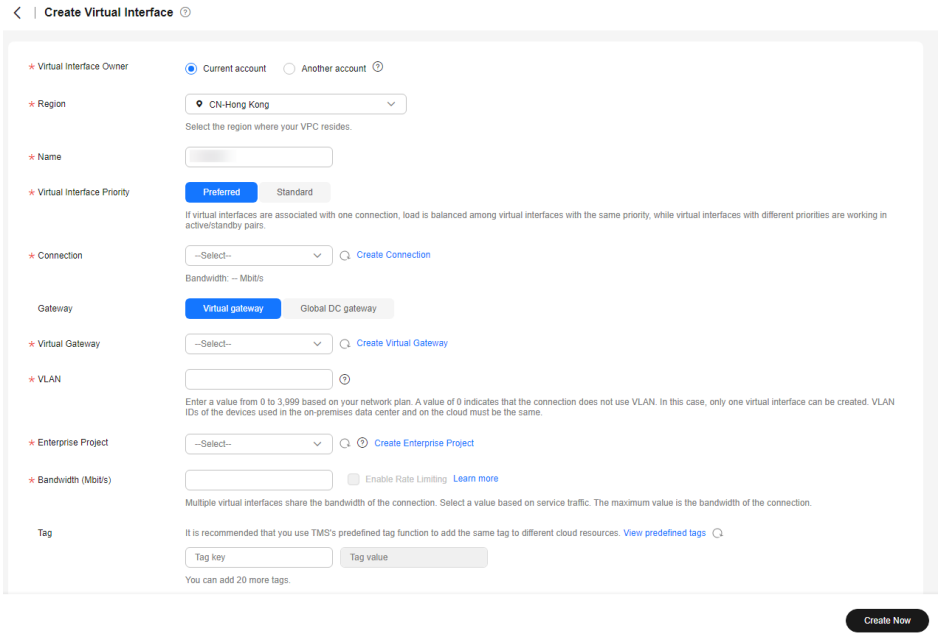


Table 4-1 Parameters for creating a virtual interface for your own account

Parameter	Example Value	Description
Virtual Interface Owner	Current account	Specifies the account that this virtual interface will be created for.
Region	CN-Hong Kong	Specifies the region where the connection resides. You can also change the region in the upper left corner of the console.
Name	vif-123	Specifies the virtual interface name. The name can contain 1 to 64 characters.
Virtual Interface Priority	Preferred	Specifies whether the virtual interface will be preferentially used over other virtual interfaces. There are two options: **Preferred** and **Standard**. If multiple virtual interfaces are associated with one Direct Connect device, the load is balanced among virtual interfaces with the same priority, while virtual interfaces with different priorities are working in active/standby pairs.
Connection	dc-123	Specifies the connection you can use to connect your on-premises network to Huawei Cloud.
Gateway	Virtual gateway	Specifies the type of the gateway that the virtual interface connects to. You can select a virtual gateway or global DC gateway.
Virtual Gateway	vgw-123	Specifies the virtual gateway that the virtual interface connects to. This parameter is mandatory when **Gateway** is set to **Virtual gateway**.
Global DC Gateway	dgw-123	Specifies the global DC gateway that the virtual interface connects to. This parameter is mandatory when **Gateway** is set to **Global DC gateway**.

Parameter	Example Value	Description
VLAN	30	Specifies the ID of the VLAN for the virtual interface. You need to configure the VLAN if you create a standard connection. The VLAN for a hosted connection will be allocated by the partner. You do not need to configure the VLAN.
Bandwidth (Mbit/s)	50	Specifies the bandwidth that can be used by the virtual interface. The bandwidth cannot exceed that of the connection.
Enable Rate Limiting	Not enabled	Limits the highest bandwidth that can be used by the virtual interface. If this option is enabled, the rate limit gradients are as follows: ● If the bandwidth is less than or equal to 100 Mbit/s, the rate limit gradient is 10 Mbit/s. ● If the bandwidth is greater than 100 Mbit/s but is less than or equal to 1,000 Mbit/s, the rate limit gradient is 100 Mbit/s. ● If the bandwidth is greater than 1,000 Mbit/s but is less than or equal to 100 Gbit/s, the rate limit gradient is 1 Gbit/s. ● If the bandwidth is greater than 100 Gbit/s, the rate limit gradient is 10 Gbit/s. For example, if the bandwidth is 52 Mbit/s, the actual rate limit is 60 Mbit/s. If the bandwidth is 115 Mbit/s, the actual rate limit is 200 Mbit/s. **NOTE** Bandwidth rate limiting of virtual interfaces is being and will be launched in each region. You can view the regions where bandwidth rate limiting is rolled out on the management console.
Enterprise Project	default	Specifies the enterprise project by which virtual interfaces are centrally managed. Select an existing enterprise project.
Tag	example_key1 example_value1	Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created.

Parameter	Example Value	Description
IP Address Family	**IPv4**	Specifies the address type of the virtual interface. **IPv4** is selected by default.
Local Gateway	10.0.0.1/30	Specifies the IP address used by Huawei Cloud to connect to your on-premises network. After you configure **Local Gateway** on the console, the configuration will be automatically delivered to the gateway used by Huawei Cloud.
Remote Gateway	10.0.0.2/30	Specifies the IP address used by the on-premises data center to connect to Huawei Cloud. After you configure **Remote Gateway** on the console, you need to configure the IP address on the interface of the on-premises device. **CAUTION** The IP addresses of the local gateway and remote gateway must be in the same IP address range. Generally, an IP address range with a 30-bit mask is used. The IP addresses you plan cannot conflict with IP addresses used on your on-premises network. Plan an IP address range that will be used at both ends of the connection for network communication between your on-premises data center and the cloud.
Remote Subnet	192.168.51.0/24, 10.1.123.0/24	Specifies the subnets and masks of your on-premises network. If there are multiple subnets, use commas (,) to separate them.
Routing Mode	BGP	Specifies whether static routing or dynamic routing is used to route traffic between your on-premises network and the cloud network. If there are or will be two or more connections, select BGP routing for higher availability.
BGP ASN	12345	Specifies the autonomous system number (ASN) of the BGP peer. This parameter is required when BGP routing is selected.

Parameter	Example Value	Description
BGP MD5 Authentication Key	**Qaz12345678**	Specifies the password used to authenticate the BGP peer using MD5. This parameter can be set when BGP routing is selected, and the parameter values on both gateways must be the same. The key contains 8 to 255 characters and must contain at least two types of the following characters: • Uppercase letters • Lowercase letters • Digits • Special characters ~!,.:;-_"(){}[]/@#$ %^&*+|=
Description	-	Provides supplementary information about the virtual interface.

If you want to create a virtual interface for another account, configure the parameters based on **Table 4-2**.

Figure 4-2 Creating a virtual interface for another account

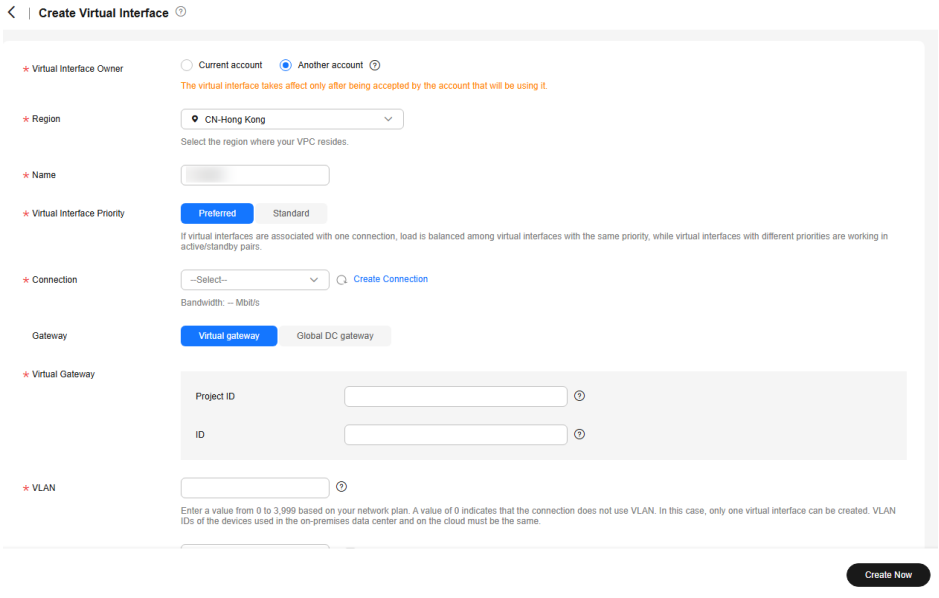


Table 4-2 Parameters for creating a virtual interface for another account

Parameter	Example Value	Description
Virtual Interface Owner	Another account	Specifies the account that this virtual interface will be created for. You create a virtual interface for another account so that this account can use your connection to access the VPC. **NOTE** Virtual interfaces that you create for other users take effect only after other users accept them.
Region	CN-Hong Kong	Specifies the region where the connection resides. You can also change the region in the upper left corner of the console.
Name	vif-123	Specifies the virtual interface name. The name can contain 1 to 64 characters.
Virtual Interface Priority	Preferred	Specifies whether the virtual interface will be preferentially used over other virtual interfaces. There are two options: **Preferred** and **Standard**. If multiple virtual interfaces are associated with one Direct Connect device, the load is balanced among virtual interfaces with the same priority, while virtual interfaces with different priorities are working in active/standby pairs.
Connection	dc-123	Specifies the connection you can use to connect your on-premises network to Huawei Cloud.
Gateway	Virtual gateway	Specifies the type of the gateway that the virtual interface connects to. You can select a virtual gateway or global DC gateway. A virtual gateway is used as an example.
Project ID	-	Specifies the ID of the project that the virtual gateway belongs to. On the management console, hover the cursor over the account name in the upper right corner and select **My Credentials**. On the **My Credentials** page, view the project ID. This parameter is mandatory when **Gateway** is set to **Virtual gateway**.

Parameter	Example Value	Description
ID	-	Specifies the ID of the virtual gateway. In the virtual gateway list, hover the cursor over the virtual gateway name and view the name and ID of the virtual gateway. This parameter is mandatory when **Gateway** is set to **Virtual gateway**.
Project ID	-	Specifies the ID of the project that the global DC gateway belongs to. On the management console, hover the cursor over the account name in the upper right corner and select **My Credentials**. On the **My Credentials** page, view the project ID. This parameter is mandatory when **Gateway** is set to **Global DC gateway**.
Global DC Gateway ID	-	This parameter is mandatory when **Gateway** is set to **Global DC gateway**. Specifies the ID of the global DC gateway. In the global DC gateway list, hover the cursor over the global DC gateway name and view the name and ID of the global DC gateway.
VLAN	30	Specifies the ID of the VLAN for the virtual interface. You need to configure the VLAN if you create a standard connection. The VLAN for a hosted connection will be allocated by the partner. You do not need to configure the VLAN.
Bandwidth (Mbit/s)	50	Specifies the bandwidth that can be used by the virtual interface. The bandwidth cannot exceed that of the connection.

Parameter	Example Value	Description
Enable Rate Limiting	Not enabled	Limits the highest bandwidth that can be used by the virtual interface. If this option is enabled, the rate limit gradients are as follows: • If the bandwidth is less than or equal to 100 Mbit/s, the rate limit gradient is 10 Mbit/s. • If the bandwidth is greater than 100 Mbit/s but is less than or equal to 1,000 Mbit/s, the rate limit gradient is 100 Mbit/s. • If the bandwidth is greater than 1,000 Mbit/s but is less than or equal to 100 Gbit/s, the rate limit gradient is 1 Gbit/s. • If the bandwidth is greater than 100 Gbit/s, the rate limit gradient is 10 Gbit/s. For example, if the bandwidth is 52 Mbit/s, the actual rate limit is 60 Mbit/s. If the bandwidth is 115 Mbit/s, the actual rate limit is 200 Mbit/s. **NOTE** Bandwidth rate limiting of virtual interfaces is being and will be launched in each region. You can view the regions where bandwidth rate limiting is rolled out on the management console.
Tag	example_key1 example_value1	Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created.
IP Address Family	**IPv4**	Specifies the address type of the virtual interface. **IPv4** is selected by default.
Local Gateway	10.0.0.1/30	Specifies the IP address used by Huawei Cloud to connect to your on-premises network. After you configure **Local Gateway** on the console, the configuration will be automatically delivered to the gateway used by Huawei Cloud.

Parameter	Example Value	Description
Remote Gateway	10.0.0.2/30	Specifies the IP address used by the on-premises data center to connect to Huawei Cloud. After you configure **Remote Gateway** on the console, you need to configure the IP address on the interface of the on-premises device. **CAUTION** The IP addresses of the local gateway and remote gateway must be in the same IP address range. Generally, an IP address range with a 30-bit mask is used. The IP addresses you plan cannot conflict with IP addresses used on your on-premises network. Plan an IP address range that will be used at both ends of the connection for network communication between your on-premises data center and the cloud.
Remote Subnet	192.168.51.0/24,10.1.123.0/24	Specifies the subnets and masks of your on-premises network. If there are multiple subnets, use commas (,) to separate them.
Routing Mode	BGP	Specifies whether static routing or dynamic routing is used to route traffic between your on-premises network and the cloud network. If there are or will be two or more connections, select BGP routing for higher availability.
BGP ASN	12345	Specifies the ASN of the BGP peer. This parameter is required when BGP routing is selected.
BGP MD5 Authentication Key	**Qaz12345678**	Specifies the password used to authenticate the BGP peer using MD5. This parameter can be set when BGP routing is selected, and the parameter values on both gateways must be the same. The key contains 8 to 255 characters and must contain at least two types of the following characters: • Uppercase letters • Lowercase letters • Digits • Special characters ~!,.:;-_"(){}[]/@#$ %^&*+|=

Parameter	Example Value	Description
Description	-	Provides supplementary information about the virtual interface.

NOTE

When you configure the local and remote gateways, note the following:

- The local gateway is used by Huawei Cloud for connecting to your equipment room. After you configure **Local Gateway** on the console, the configuration will be automatically delivered to the gateway used by Huawei Cloud.
- The remote gateway is used by your equipment room for connecting to Huawei Cloud. After you configure **Remote Gateway** on the console, you also need to configure the gateway deployed in your equipment room.
- The local and remote gateways must use the same CIDR block and cannot conflict with service IP addresses on the network.

4. Click **Create Now**.

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

5. Ping the IP address of a server in the VPC from your on-premises data center to test network connectivity.

4.2 Viewing a Virtual Interface

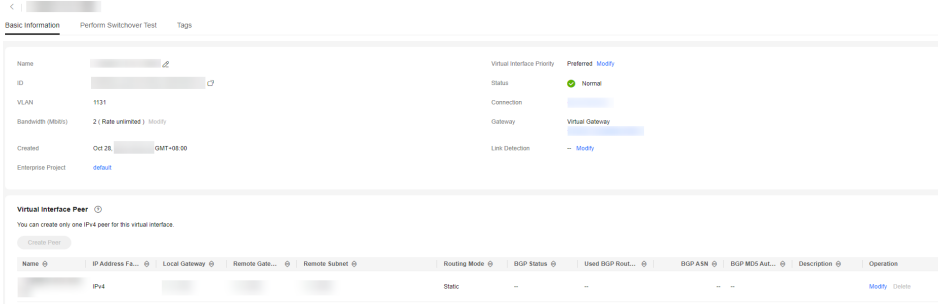
Scenario

You can view details about a virtual interface.

Procedure

1. Go to the **Virtual Interfaces** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the virtual interface list, locate the virtual interface and click its name to go to the **Basic Information** page of the virtual interface.

Figure 4-3 Viewing a virtual interface



4.3 Modifying a Virtual Interface

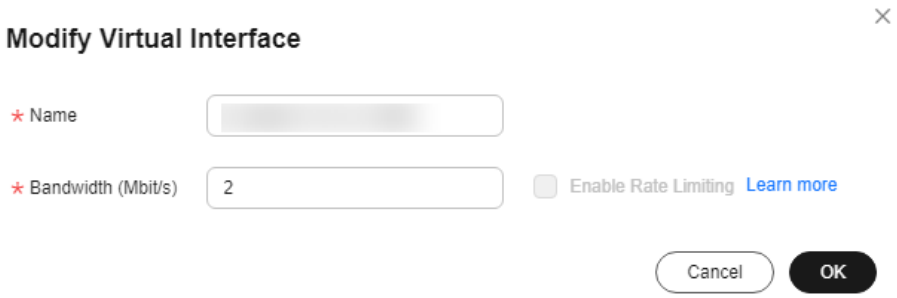
Scenario

After a virtual interface is created, you can modify its name, bandwidth, rate limiting, and priority as well as the name, remote subnet, and description of a virtual interface.

Procedure

1. Go to the **Virtual Interfaces** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the virtual interface list, locate the virtual interface you want to modify and click **Modify** in the **Operation** column.

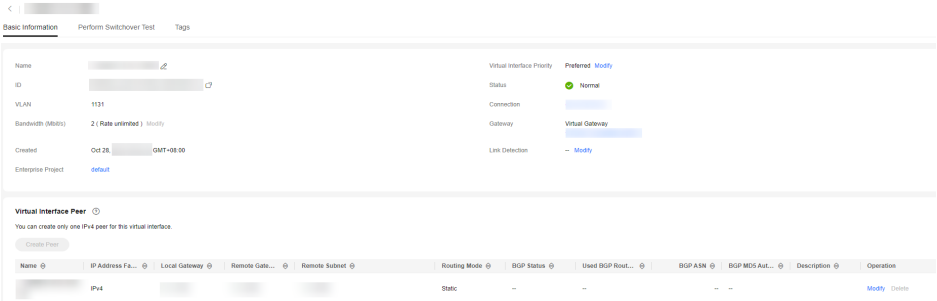
Figure 4-4 Modifying virtual interface 1



You can also click the name of the virtual interface to go to the **Basic Information** page of the virtual interface, where you can modify the name, bandwidth, rate limiting, priority, and peer of the virtual interface.

For details virtual interface peers, see **Managing Virtual Interface Peers**.

Figure 4-5 Modifying virtual interface 2



NOTE

If multiple virtual interfaces are associated with one Direct Connect device, the load is balanced among virtual interfaces with the same priority, while virtual interfaces with different priorities are working in active/standby pairs.

4.4 Deleting a Virtual Interface

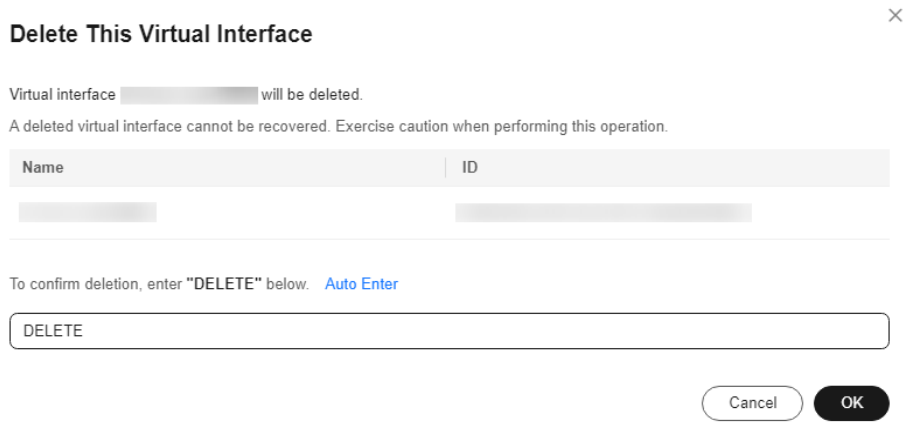
Scenario

You can delete a virtual interface if you do not need it any longer.

Procedure

1. Go to the **Virtual Interfaces** page.
2. In the upper left corner of the page, click and select a region and project.
3. In the virtual interface list, locate the virtual interface you want to delete and click **Delete** in the **Operation** column.
4. In the displayed dialog box, enter **DELETE** and click **OK**.

Figure 4-6 Deleting a virtual interface



4.5 Managing Virtual Interface Peers

Overview

A virtual interface peer is a configuration of a virtual interface to support the IPv4/IPv6 dual stack and is used to connect the customer gateway to the virtual gateway. A virtual interface peer is automatically created when you create a virtual interface.

Constraints

A virtual interface has at least one virtual interface peer, and the last virtual interface peer cannot be deleted.

Viewing a Virtual Interface Peer

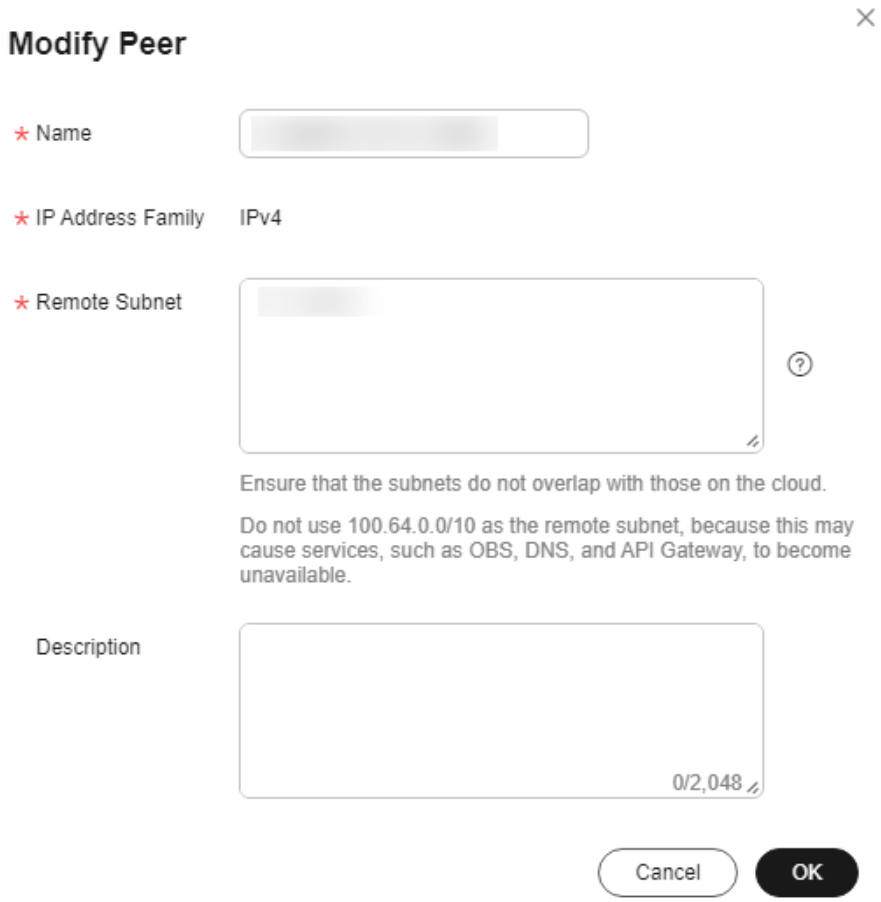
1. Go to the **Virtual Interfaces** page.

2. In the upper left corner of the page, click and select a region and project.
3. Locate the virtual interface and click its name.
4. In the lower part of the page, locate the virtual interface peer you want to view and view its details.

Modifying a Virtual Interface Peer

1. Go to the **Virtual Interfaces** page.
2. In the upper left corner of the page, click and select a region and project.
3. Locate the virtual interface and click its name.
4. In the lower part of the page, locate the virtual interface peer you want to modify and click **Modify** in the **Operation** column.
5. Modify the virtual interface peer. An IPv4 virtual interface peer is used as an example here.

   Figure 4-7 Modifying a virtual interface peer



6. Click **OK**.

5 Historical Connections

5.1 Viewing a Historical Connection

Scenario

You can view details about a connection that was originally requested through email or on the phone rather than using the console.

Procedure

1. Go to the **Historical Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection you want to view and click ˅ before its name to view the details.

5.2 Modifying a Historical Connection

Scenario

You can modify the name and remote subnets of a historical connection.

Procedure

1. Go to the **Historical Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the connection you want to modify and click **Modify** in the **Operation** column.
4. Modify the connection and then click **OK**.

6 Partner Connections

6.1 Operations Connections

Creating an Operations Connection

Scenario

If you are a partner, you can create an operations connection.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the upper right corner, click **Create Operations Connection**.
4. Configure the parameters and click **Create Now**.
5. Confirm the order and click **Pay**.
6. Click **Pay**.

Viewing an Operations Connection

Scenario

You can view details about an operations connection that you have created.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Locate the operations connection you want to view and click its name.
4. View details about the operations connection.

Modifying an Operations Connection

Scenario

You can modify the name, bandwidth, equipment room address, and description of an operations connection.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the operations connection list, locate the operations connection you want to modify and click **More** > **Modify** in the **Operation** column.
4. Modify the connection and then click **OK**.

Unsubscribing from an Operations Connection

Scenario

You can unsubscribe from an operations connection if you no longer need it.

Prerequisites

Delete the virtual gateway and virtual interface associated with your connection, delete the connection, and unsubscribe from the operations connection.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the operations connection list, locate the operations connection that you want to unsubscribe from and choose **More** > **Unsubscribe** in the **Operation** column.
4. In the operations connection list, locate the target operations connection and click **Unsubscribe from Resource** in the **Operation** column.
5. On the displayed **Unsubscribe** page, confirm the amount to be refunded.
6. Click **Confirm**.

Renewing an Operations Connection

Scenario

You can renew the subscription if an operations connection is about to expire.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the operations connection list, locate the operations connection you want to renew and choose **More** > **Renew** in the **Operation** column.
4. Set the duration that you want to renew the connection and click **Pay**. Then pay the order as prompted.

6.2 Hosted Connections

Creating a Hosted Connection

Scenario

If you are a partner, you can create a hosted connection for your user.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the upper right corner, click **Create Hosted Connection**.
4. Configure the parameters and click **OK**.

Viewing a Hosted Connection

Scenario

You can view details about a hosted connection you have created as a partner.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the operations connection list, locate the operations connection that the hosted connection depends on and click **Manage Hosted Connection** in the **Operation** column.
4. In the hosted connection list, locate the hosted connection you want to view and click on the left of its name to view the details.

Modifying a Hosted Connection

Scenario

You can modify the name, bandwidth, equipment room address, and description of a hosted connection.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the operations connection list, locate the operations connection that the hosted connection depends on and click **Manage Hosted Connection** in the **Operation** column.
4. In the hosted connection list, locate the hosted connection you want to modify and click **Modify** in the **Operation** column.
5. Modify the hosted connection and click **OK**.

Deleting a Hosted Connection

Scenario

You can delete a hosted operation if you do not need it any longer.

Procedure

1. Go to the **Connections** page.
2. In the upper left corner of the page, click  and select a region and project.
3. In the operations connection list, locate the operations connection that the hosted connection depends on and click **Manage Hosted Connection** in the **Operation** column.
4. In the hosted connection list, locate the hosted connection you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

7 Network Topology

Scenario

After creating a connection, you can view the connection status and resource information in the Direct Connect network topology.

NOTE

The network topology function has been available in the following regions: CN North-Beijing4, CN East-Shanghai1, CN South-Guangzhou, CN Southwest-Guiyang1, CN-Hong Kong, AP-Bangkok, AP-Singapore, AF-Johannesburg, and LA-Mexico City2.

Procedure

1. Go to the **Network Topology** page.
2. In the upper left corner of the page, click  and select a region and project.
3. View your connections, their virtual gateways and virtual interfaces, and VPCs that can be accessed over these connections.

   NOTE

   If a site survey is being performed, cabling is not complete, or the specification is being changed, the connection is displayed as abnormal in the network topology. You can check its status on the connection list page.

8 Cloud Eye Monitoring

8.1 Overview

Monitoring is critical to ensuring the performance, reliability, and availability of a service. Monitoring data lets you keep track of the status of your resources. Cloud Eye collects and displays monitoring data for you in a convenient, visualized manner. You can use Cloud Eye to automatically monitor connections in real time and manage alarms and notifications, so that you can keep track of the performance of each connection.

To learn more information, see the following topics:

- **Metrics**
- **Network Quality Metrics (Plug-ins Required)**
- **Setting Alarm Rules**
- **Viewing Monitoring Metrics**

8.2 Metrics

Function

Table 8-1 describes the metrics reported by Direct Connect to Cloud Eye as well as their namespace and dimensions. You can use the management console to query the metrics of the monitored objects and alarms generated for Direct Connect.

NOTE

You can view metrics of standard connections, full-service connections (dedicated port), and hosted connections.

Namespace

SYS.DCAAS

Metrics

Table 8-1 Direct Connect metrics

ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval
network_incoming_bits_rate	Network Incoming Bandwidth	Bit rate for inbound data to the Direct Connect side of a connection Unit: bit/s	≥ 0 bits/s	Connections and historical connections	1 minute
network_outgoing_bits_rate	Network Outgoing Bandwidth	Bit rate for outbound data from the Direct Connect side of a connection Unit: bit/s	≥ 0 bits/s	Connections and historical connections	1 minute
network_incoming_bytes	Network Incoming Traffic	The number of bytes for inbound data to the Direct Connect side of a connection Unit: byte	≥ 0 bytes	Connections and historical connections	1 minute
network_outgoing_bytes	Network Outgoing Traffic	The number of bytes for outbound data from the Direct Connect side of a connection Unit: byte	≥ 0 bytes	Connections and historical connections	1 minute
network_incoming_packets_rate	Network Incoming Packet Rate	Packet rate for inbound data to the Direct Connect side of a connection Unit: Packet/s	≥ 0 packets/s	Connections and historical connections	1 minute
network_outgoing_packets_rate	Network Outgoing Packet Rate	Packet rate for outbound data from the Direct Connect side of a connection Unit: Packet/s	≥ 0 packets/s	Connections and historical connections	1 minute

ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval
network_incoming_packets	Network Incoming Packets	The number of packets for inbound data to the Direct Connect side of a connection Unit: Packet	≥ 0 packets	Connections and historical connections	1 minute
network_outgoing_packets	Network Outgoing Packets	The number of packets for outbound data from the Direct Connect side of a connection Unit: Packet	≥ 0 packets	Connections and historical connections	1 minute
network_status	Port Status	The status of the port used by a connection	**0** indicates **DOWN**. 1-UP	Connections and historical connections	1 minute
bgp_receive_route_num_v4	IPv4 Routes	The number of IPv4 routes that a virtual interface learned through BGP	≥ 0	Virtual interface	1 minute
bgp_receive_route_num_v6	IPv6 Routes	The number of IPv6 routes that a virtual interface learned through BGP	≥ 0	Virtual interface	1 minute
bgp_peer_status_v4	IPv4 Peer Status	Status of an IPv4 virtual interface peer	**0** indicates **DOWN**. **1** indicates **ACTIVE**.	Virtual interface	1 minute

ID	Metric	Description	Value Range	Monitored Object	Monitoring Interval
bgp_peer_status_v6	IPv6 Peer Status	Status of an IPv6 virtual interface peer	**0** indicates **DOWN**. **1** indicates **ACTIVE**.	Virtual interface	1 minute
in_errors	Inbound Error Packets	The number of inbound packets that cloud not be transmitted to the Direct Connect gateway over the connection because of errors	0-2^{32}	Connection	1 minute

Dimensions

Key	Value
direct_connect_id	Connection
virtual_interface_id	Virtual interface
history_direct_connect_id	Historical connection

8.3 Network Quality Metrics (Plug-ins Required)

The network quality of connections is monitored using two plug-ins, and there are two key metrics: network latency and packet loss rate.

Direct Connect provides two monitoring plug-ins:

- dc-nqa-collector: monitors the connections requested on the Direct Connect console.
- history-dc-nqa-collector: monitors historical connections.

For details, see **Installing the Direct Connect Metric Collection Plug-ins**.

NOTE

- Automated connections are requested using the console and can be self-service or full-service connections. Each connection has at least a virtual gateway and a virtual interface, and their routes are automatically advertised. Connections in most regions are automated connections.
- Historical connections are requested by email or phone. They do not have virtual gateways and virtual interfaces, and their routes must be configured manually. Historical connections exist only in some regions.

Constraints

- For each virtual interface, only one VM can be configured for monitoring, or monitoring data may fail to be reported.
- No images can be configured for the VM where the Direct Connect monitoring plug-ins are installed, or monitoring data may fail to be reported.
- The VM where the Direct Connect monitoring plug-ins are installed must be in the same account and region as the virtual interface.

Procedure

1. Configure the Direct Connect plug-ins.

   For details, see **Installing Direct Connect Metric Collection Plug-ins**.
2. Configure the return route for the detection source IP address in the on-premises data center.

   Example route (A Huawei-developed device is used an example.)

   ```
   ip route-static 192.168.1.100 255.255.255.255 10.0.0.1
   ```

   NOTE

   This is to add a return route whose destination is the detection source IP address used in the on-premises data center and next hop is the local gateway configured on the corresponding virtual interface. This ensures that the return packets from the on-premises data center can reach the detection source in the VPC through the correct path.

Metrics

Table 8-2 Network quality metrics

ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval
latency	Latency	Network latency of a connection Unit: ms	≥ 0 ms	Virtual interfaces and historical connections	1 minute

ID	Metric Name	Description	Value Range	Monitored Object	Monitoring Interval
packet_loss_rate	Packet Loss Rate	Packet loss rate of a connection Unit: Percentage	0–100%	Virtual interfaces and historical connections	1 minute

Dimensions

Key	Value
virtual_interface_id	Virtual interface (associated with an automated connection)
history_direct_connect_id	Historical connection

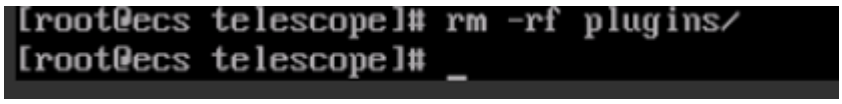
Helpful Links

You can delete the **plugins** directory to delete the installed plug-ins based on your service requirements.

Command:

```
cd /usr/local/uniagent/extension/install/telescope/
rm -rf plugins/
```

Example:



NOTE

The **plugins** directory is automatically created when the plug-ins are installed. Deleting this directory does not affect your services.

8.4 Configuring an Alarm Rule

Scenario

You can configure alarm rules to customize monitored objects and notification policies and to learn connection status at any time.

Procedure

1. Log in to the management console.
2. On the console homepage, click in the upper left corner and select the desired region and project.
3. In the service list, choose **Management & Governance** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule**.
6. Click **Create**.

   After the alarm rule is created, you will be notified when an alarm is triggered.

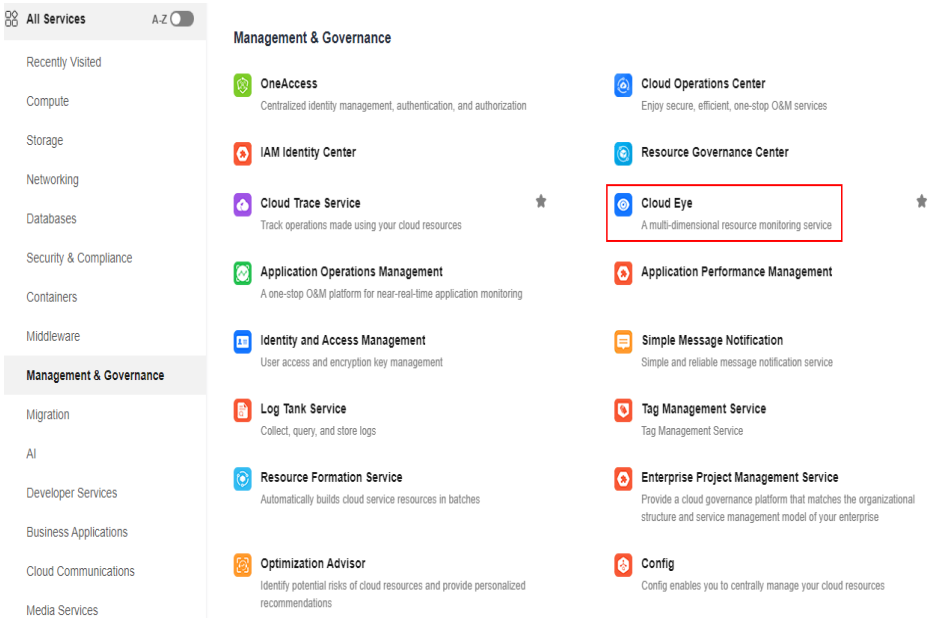
   NOTE

   For more examples of creating alarm rules, see **Cloud Eye User Guide**.

8.5 Viewing Metrics

1. Log in to the management console.
2. On the console homepage, click in the upper left corner and select the desired region and project.
3. Click to display **Service List** and choose **Management & Governance** > **Cloud Eye**.

   Figure 8-1 Cloud Eye



4. In the navigation pane on the left, choose **Cloud Service Monitoring**. In the displayed list, click **Direct Connect DCAAS**.

   The **Details** page is displayed.

5. Select the resource type from the drop-down list.

   Example:

   - Cloud service: **Direct Connect**
   - Resource name: **Connections**

6. Click the **Resources** tab.
7. Locate the target instance and click **View Metric** in the **Operation** column.

   You can view data of the last 1, 3, 12, or 24 hours, or last 7 days. You can also specify a time period.

9 Permissions Management

9.1 Creating a User and Granting Permissions

Use **IAM** to implement fine-grained permissions control for your Direct Connect resources. With IAM, you can:

- Create IAM users for employees based on the organizational structure of your enterprise. Each IAM user has their own security credentials, providing access to cloud resources.
- Grant only the permissions required for users to perform a specific task.
- Entrust another account or cloud service to perform professional and efficient O&M on your cloud resources.

Skip this part if your account does not require individual IAM users.

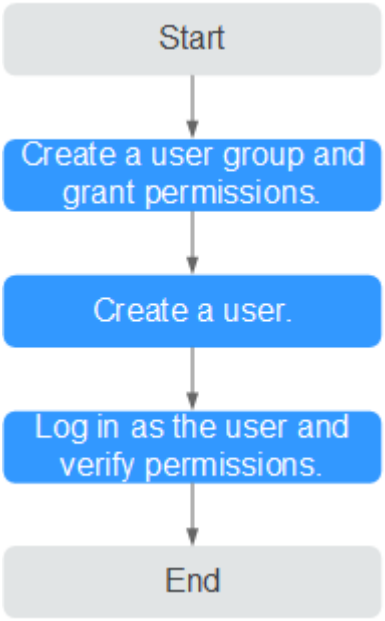
Figure 9-1 shows the process for granting permissions.

Prerequisites

Before you assign permissions to a user group, you need to understand Direct Connect permissions that can be assigned to the user group and select permissions based on actual requirements. For details about the system permissions of Direct Connect, see **Permissions**. For the system policies of other services, see **System Permissions**.

Process Flow

Figure 9-1 Process for granting Direct Connect permissions



1. **Create a user group and assign permissions**.

   Create a user group on the IAM console and assign the **Direct Connect Administrator** policy to the group.

2. **Create a user and add the user to the user group**

   Create a user on the IAM console and add the user to the group created in **1**.

3. **Log in to the management console as the created user**.

   Log in to the Direct Connect console using the created user and verify that the user has read-only permissions for Direct Connect.

   - In the service list, choose **Networking** > **Direct Connect**. Click **Create Connection** in the upper right corner. If the connection is successfully created, the **Direct Connect Administrator** policy has already taken effect.
   - Choose any other service in the Service List. A message will appear indicating that you have no sufficient permissions to access the service.

9.2 Example Custom Policies

Custom policies can be created to supplement the system-defined policies of Direct Connect.

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following are examples custom policies created for Direct Connect.

Example Custom Policies

- Example 1: Allowing users to update a virtual gateway

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "dcaas:vgw:update"
         ]
      }
   ]
}
```

- Example 2: Denying users to delete a connection

  A deny policy must be used together with other policies. If permissions assigned to a user contain both Allow and Deny actions, the Deny action takes precedence over the Allow action.

  The following method can be used if you need to assign permissions of the **DCAAS FullAccess** policy to a user but also forbid the user from deleting connections. Create a custom policy for denying connection deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on Direct Connect except deleting connections.

  The following is an example of a deny policy:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Deny",
         "Action": [
            "dcaas:directConnect:delete"
         ]
      }
   ]
}
```

- Example 3: Defining permissions for multiple services in a policy

  A custom policy can contain the actions of multiple services that are of the global or project-level type.

  The following is an example policy containing actions of multiple services:

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc:vpcs:list",
            "vpc:subnets:get",
            "vpc:routes:list"
         ]
      },
      {
         "Effect": "Allow",
         "Action": [
            "dcaas:vif:list",
            "dcaas:vgw:list",
            "dcaas:directConnect:list"
         ]
      }
   ]
}
```


10 Using CTS to Collect Direct Connect Key Operations

10.1 Key Operations Recorded by CTS

With CTS, you can record operations associated with Direct Connect for later query, audit, and backtrack operations.

Table 10-1 lists the operations that can be recorded by CTS.

Table 10-1 Direct Connect operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a connection	dcaasConnection	createConnection
Modifying a connection	dcaasConnection	modifyConnection
Deleting a connection	dcaasConnection	deleteConnection
Creating a virtual gateway	dcaasVirtualGateway	createVirtualGateway
Modifying a virtual gateway	dcaasVirtualGateway	modifyVirtualGateway
Deleting a virtual gateway	dcaasVirtualGateway	deleteVirtualGateway
Creating a virtual interface	dcaasVirtualInterface	createVirtualInterface
Modifying a virtual interface	dcaasVirtualInterface	modifyVirtualInterface

Operation	Resource Type	Trace Name
Deleting a virtual interface	dcaasVirtualInterface	deleteVirtualInterface

10.2 Viewing Traces

Scenario

After you enable CTS, the system starts recording operations on cloud resources. You can view traces of the last seven days on the CTS console.

This topic describes how to query these records.

Procedure

1. Log in to the management console.
2. On the console homepage, click  in the upper left corner and select the desired region and project.
3. Click  to display **Service List** and choose **Management & Governance** > **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify filtering criteria. The following filters are available:
   - **Trace Type**, **Trace Source**, **Resource Type**, and **Search By**

     Select a filter criterion from the drop-down list.

     - If you select **Trace name** for **Search By**, you need to specify a trace name.
     - If you select **Resource ID** for **Search By**, you need to specify a resource ID.
     - If you select **Resource name** for **Search By**, you need to specify a resource name.
   - **Operator**: Select a user who performs operations.
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Time range: You can specify the time period to query traces.
6. Click on the left of the record to be queried to extend its details.
7. Locate a trace and click **View Trace** in the **Operation** column.

11 Quotas

What Is Quota?

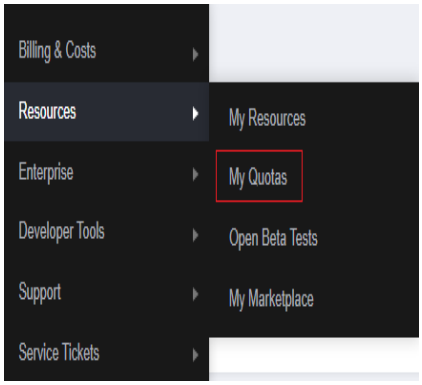
Quotas can limit the number or amount of resources available to users, such as the maximum number of ECS or EVS disks that can be created.

If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

How Do I View My Quotas?

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 11-1 My Quotas

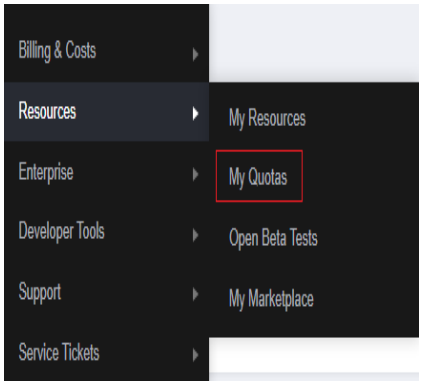
4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.

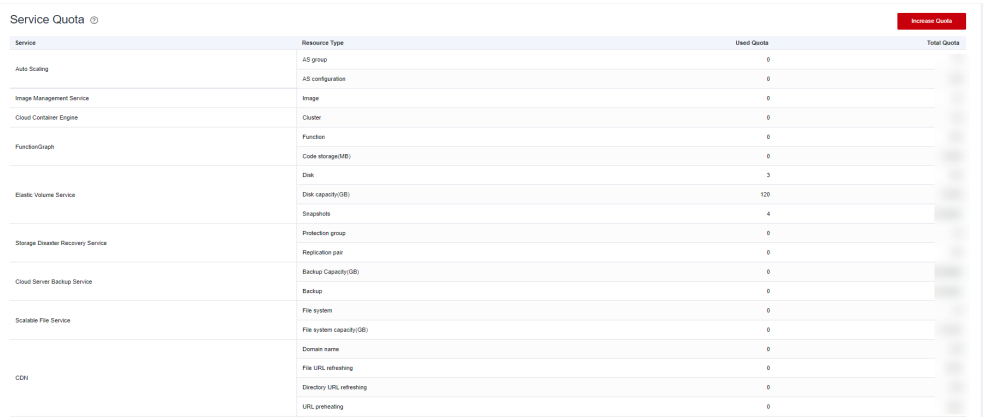
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 11-2 My Quotas



3. Click **Increase Quota** in the upper right corner of the page.

   Figure 11-3 Increasing quota



4. On the **Create Service Ticket** page, configure parameters as required.
   In the **Problem Description** area, fill in the content and reason for adjustment.
5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

12 Appendixes

12.1 Dual-Connection Switchover Test

Function

Dual-connection access ensures high SLA. To achieve this, dual-connection automatic switchover needs to be supported. Before O&M of dual-connection access, you can perform switchover tests on the console to verify connectivity and simplify the delivery process.

Application Scenario

Perform the dual-connection switchover test before the connections are used for network connectivity.

Prerequisites

There are two connections, with each having a virtual interface associated.

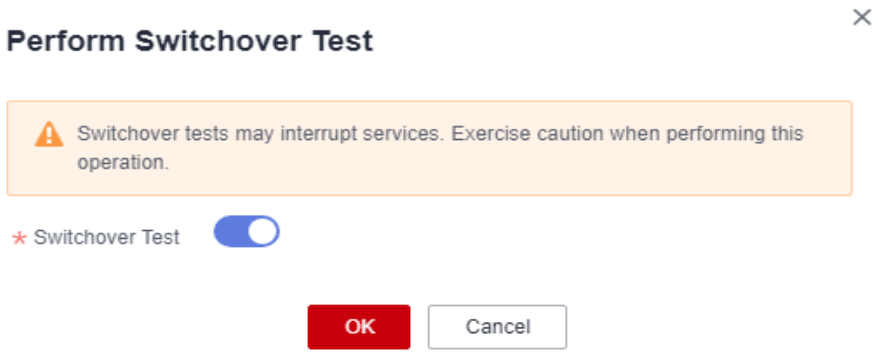
Procedure

1. Log in to the management console.
2. On the console homepage, click  in the upper left corner and select the desired region and project.
3. Click  to display **Service List** and choose **Networking** > **Direct Connect**.
4. In the navigation pane on the left, choose **Direct Connect** > **Virtual Interfaces**.
5. Enable the switchover test for the virtual interface associated with one connection, for example, connection 1 and check the connectivity between an ECS and the on-premises data center.
   a. On the **Virtual Interfaces** page, click the name of the target virtual interface.

b. On the **Switchover Test** page of the virtual interface, click **Switchover Test**.

c. In the **Perform Switchover Test** dialog box, enable the switchover test and click **OK**

Figure 12-1 Enabling switchover test



d. Refresh the page. On the **Basic Information** page of the virtual interface, ensure that its status is **Disabled manually**.

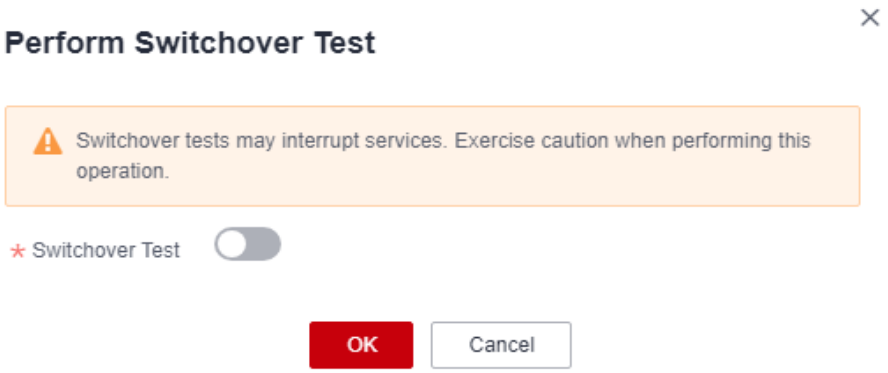
e. Run the **ping** command on an ECS to verify the connectivity between the ECS and the on-premises data center. If a response packet is received, the switchover test is successful.

6. Disable the switchover test for the virtual interface associated with connection 1 to restore access over dual connections.

a. On the **Switchover Test** page of the virtual interface, click **Switchover Test**.

b. In the **Perform Switchover Test** dialog box, disable the switchover test and click **OK**

Figure 12-2 Disabling switchover test



c. Refresh the page. On the **Basic Information** page of the virtual interface, ensure that its status is **Normal**.

d. Run the **ping** command on the ECS to verify the connectivity between the ECS and the on-premises data center. If a response packet is received, the switchover test is successful.

7. Repeat 5 and 6 to perform a switchover test on the virtual interface associated with connection 2.

NOTE

In the switchover test record, if the operation type is displayed as **Enable**, the **shutdown** command is executed, and the virtual interface is disabled. If the operation type is displayed as **Disable**, the **undo shutdown** command is executed, and the virtual interface is enabled.

12.2 Connection Bandwidth Testing Methods

Scenario

After your on-premises data center is connected to the cloud, you need to test the link performance to ensure that the connection can meet your service requirements. This section describes how you can use iPerf3 to test the bandwidth of a connection.

Prerequisites

- Network connectivity between your on-premises data center and the cloud has been established, and the routes have been configured.
- A network access device is available in the on-premises data center as the client or server in the iPerf3 tests.

  The IP address of the network access device is 192.168.0.1.
- Six ECSs that can access the Internet are available as the clients or servers in the iPerf3 tests. The ECSs establish control connections with the on-premises network access device for transmitting test information and test results.

  In this example, the six ECSs use the c7.large.2 flavor and image CentOS 8.2 64bit (40 GB), and their IP addresses are from 172.16.0.2 to 172.16.0.7.

Procedure

Step 1 Install iPerf3 and set up the test environment.

Install iPerf3 on the on-premises network access device and on the six ECSs. The following describes how to install iPerf3 on an ECS.

1. Log in to the ECS.
2. Install iPerf3.
   a. Download iPerf3.
   ```
   yum install iperf3
   ```
   b. Check whether the installation is successful.
   ```
   iperf3 -v
   ```
   The installation is successful when the system displays the following information:

Step 2 Use iPerf3 to test the bandwidth of a connection.

Table 12-1 describes the parameters related to iPerf3.

Table 12-1 iPerf3 parameter description

Parameter	Description
-s	A server-specific parameter. It indicates that iPerf3 runs in server mode.
-c	A client-specific parameter. It indicates that iPerf3 runs in client mode.
-i	The interval between reports, in seconds.
-p	• Server: The listening port on the server. The default value is 5201. Both TCP and UDP are listened on. • Client: The port for the client to connect to the server. The default value is 5201. If the -u parameter also exists, the connection is initiated through UDP. Otherwise, a TCP connection is used by default.
-u	UDP is used to send packets. If this parameter is not specified, TCP is used.
-l	The length of the read/write buffer. The recommended value is 1,400 for testing the bandwidth and 16 for testing the packet forwarding performance.
-b	The bandwidth (in bit/s) used if a UDP connection is established.
-t	The total transmission time, in seconds. It is the duration for iPerf3 to repeatedly send data packets of a specified length within a specified period. The default value is 10 seconds.
-A	CPU affinity. You can bind the iPerf3 process to the logical CPU with the corresponding number to prevent the iPerf3 process from being scheduled among different CPUs.

1. Test the bandwidth of the connection with the on-premises network access device functioning as the server.
   a. Run the following commands on the on-premises network access device to start the iPerf3 process in server mode and specify different ports:

      ```
      iperf3 -s -i 1 -p 16001
      iperf3 -s -i 1 -p 16002
      iperf3 -s -i 1 -p 16003
      iperf3 -s -i 1 -p 16004
      iperf3 -s -i 1 -p 16005
      iperf3 -s -i 1 -p 16006
      ```

   b. Run the **iperf3 -u -l 1400 -b 100m -t 120 -c server_ip -i 1 -p port** command on each ECS to start the iPerf3 process in client mode and specify different ports of the on-premises network access device.

      Example commands are as follows:

      ```
      iperf3 -u -l 1400 -b 100m -t 120 -c 192.168.0.1 -i 1 -p 16001 #First ECS
      iperf3 -u -l 1400 -b 100m -t 120 -c 192.168.0.1 -i 1 -p 16002 #Second ECS
      iperf3 -u -l 1400 -b 100m -t 120 -c 192.168.0.1 -i 1 -p 16003 #Third ECS
      iperf3 -u -l 1400 -b 100m -t 120 -c 192.168.0.1 -i 1 -p 16004 #Fourth ECS
      ```



```
iperf3 -u -l 1400 -b 100m -t 120 -c 192.168.0.1 -i 1 -p 16005 #Fifth ECS
iperf3 -u -l 1400 -b 100m -t 120 -c 192.168.0.1 -i 1 -p 16006 #Sixth ECS
```

2. Test the bandwidth of the connection with the on-premises network access device as a client.

   a. Run the **iperf3 -s -i 1 -p 16001** command on each ECS to start the iPerf3 process in server mode and specify the port.

   b. Run the following commands on the on-premises network access device to start six iPerf3 processes in client mode:

```
iperf3 -u -l 1400 -b 100m -t 120 -c 172.16.0.2 -i 1 -p 16001
iperf3 -u -l 1400 -b 100m -t 120 -c 172.16.0.3 -i 1 -p 16001
iperf3 -u -l 1400 -b 100m -t 120 -c 172.16.0.4 -i 1 -p 16001
iperf3 -u -l 1400 -b 100m -t 120 -c 172.16.0.5 -i 1 -p 16001
iperf3 -u -l 1400 -b 100m -t 120 -c 172.16.0.6 -i 1 -p 16001
iperf3 -u -l 1400 -b 100m -t 120 -c 172.16.0.7 -i 1 -p 16001
```

3. Analyze the test result.

   After the iPerf3 process on the client is executed, the following information is displayed. The packets per second (PPS) of the tested link can be calculated using the formula: PPS = Number of packets received by the peer end/Time.

```
[ ID] Interval       Transfer    Bandwidth      Jitter    Lost/Total Datagrams
[  4] 0.00-10.00 sec  237 MBytes  199 Mbits/sec  0.027 ms  500/30352 (1.6%)
[  4] Sent 30352  datagrams
```

   The following table describes the fields in the command output.

Field	Description
Transfer	Transmitted data volume
Bandwidth	Bandwidth of the connection
Jitter	Jitter
Lost/Total Datagrams	Number of lost packets/Total number of packets (packet loss rate)

----End

