Direct Connect

User Guide

Issue 01

Date 2026-01-09

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

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 Using IAM to Grant Access to Direct Connect

1.1 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.

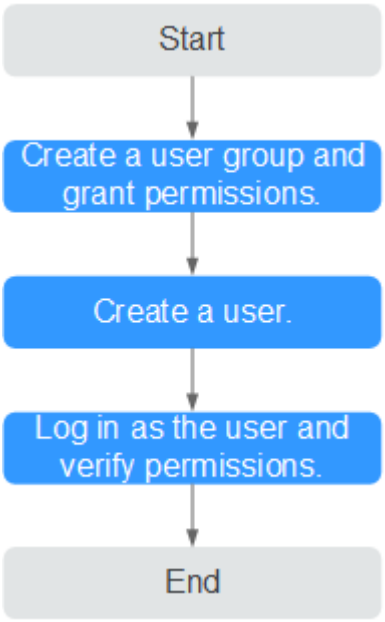
Figure 1-1 shows the process for granting permissions.

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 1-1 Process for granting Direct Connect permissions



1. **Create a user group and assign it 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 it to a user group**

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

3. **Log in as the IAM user** and verify permissions.

   Log in to the **Direct Connect console** as the created user, switch to the authorized region, and verify the permissions.

   - Go to the connection list page and 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.

1.2 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 grammar.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see **Creating a Custom Policy**. The following are example 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"
         ]
      }
   ]
}
```


2 Connections

2.1 Connection Overview

Connections are dedicated channels for on-premises data centers to access the cloud. Connections are more stable, reliable, and secure than Internet-based connections, and provide up to 100 Gbit/s of bandwidth. Direct Connect provides ports only. After you request a connection, you need to work with the carrier and Huawei Cloud to establish network connectivity between your on-premises data center and the cloud.

Direct Connect provides standard connections and hosted connections.

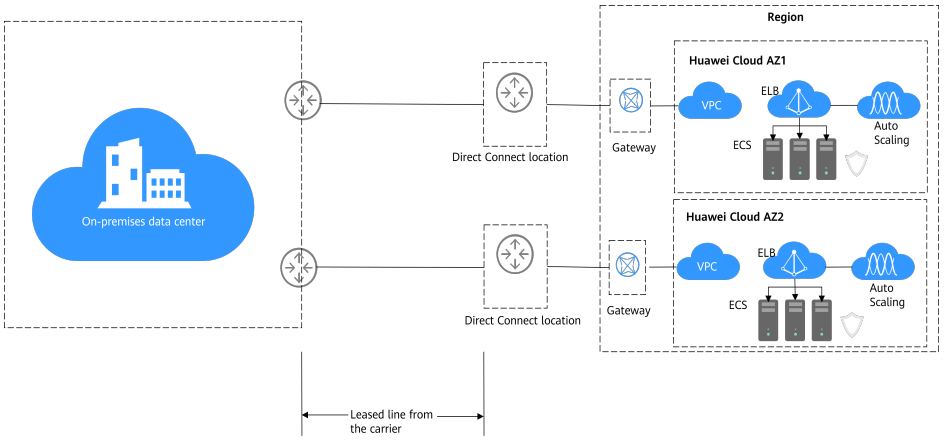
- Standard connection: A standard connection provides an exclusive port. You can create standard connections on the management console. To improve reliability, you can create multiple connections terminated at different locations and allow them to serve as backups for each other.

  You can choose self-service connections or full-service connections.

  - Self-service connection: Huawei Cloud only provides the port. You need to create a connection on the console, and lease a line from a carrier.
  - Full-service connection: You only need to create a connection on the console, and Huawei Cloud will complete all operations required for network connectivity.

  Figure 2-1 shows an example of how standard connections work.

Figure 2-1 Accessing the cloud using standard connections

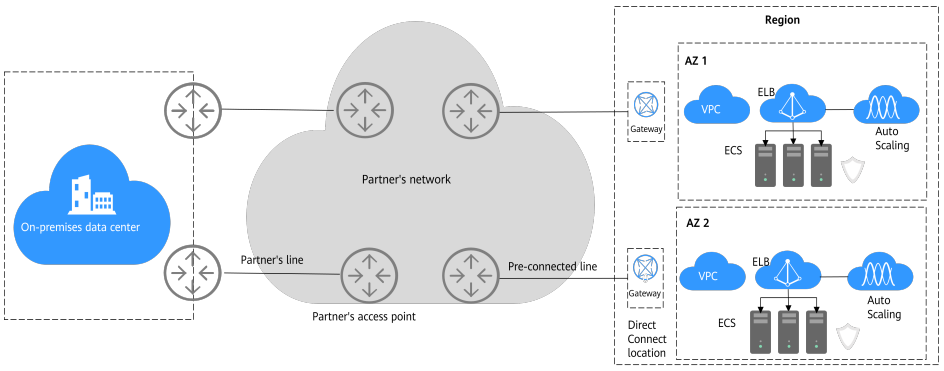


- Hosted connection: If you use a hosted connection to access the cloud, the port you use is shared with other users. The connection is created by a carrier (a partner of Huawei Cloud), who allocates the required VLAN and bandwidth for your connection. Only one virtual interface can be associated with each hosted connection.

  If you are a partner, you can request operations connections. If you are a common user, you can purchase a host connection from your partner. Hosted connections must be hosted on operations connections, and your partner will allocate VLAN and bandwidth resources to the connection.

  Figure 2-2 shows an example of how hosted connections work.

Figure 2-2 Accessing the cloud using hosted connections



Connections support redundant configuration. If there are two connections terminated at different locations in the same region, they can work in an active/standby pair to back each other up. If one connection becomes faulty, the other will take over, ensuring stable services.

2.2 Creating a Connection

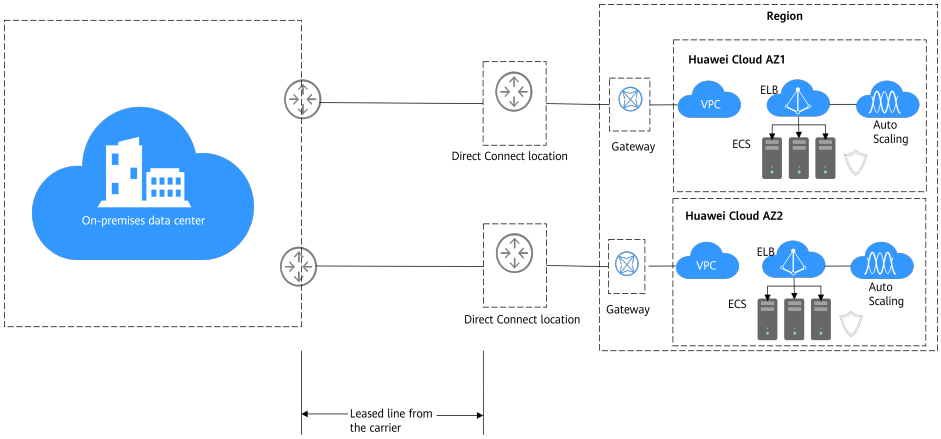
Standard Connection

Standard connections provide self-service connections and full-service connections for you to choose as required.

- Self-service connection: Huawei Cloud only provides the port. You need to create a connection on the console, and lease a line from a carrier.
- Full-service connection: You only need to create a connection on the console, and Huawei Cloud will complete all operations required for network connectivity.

Figure 2-3 shows an example of how standard connections work.

Figure 2-3 Accessing the cloud using standard connections



Creating a Self-Service Connection

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 Connection**.
4. On the **Create Connection** page, enter the equipment room details and select the Huawei Cloud location and port based on **Table 2-1**.

Figure 2-4 Creating a connection

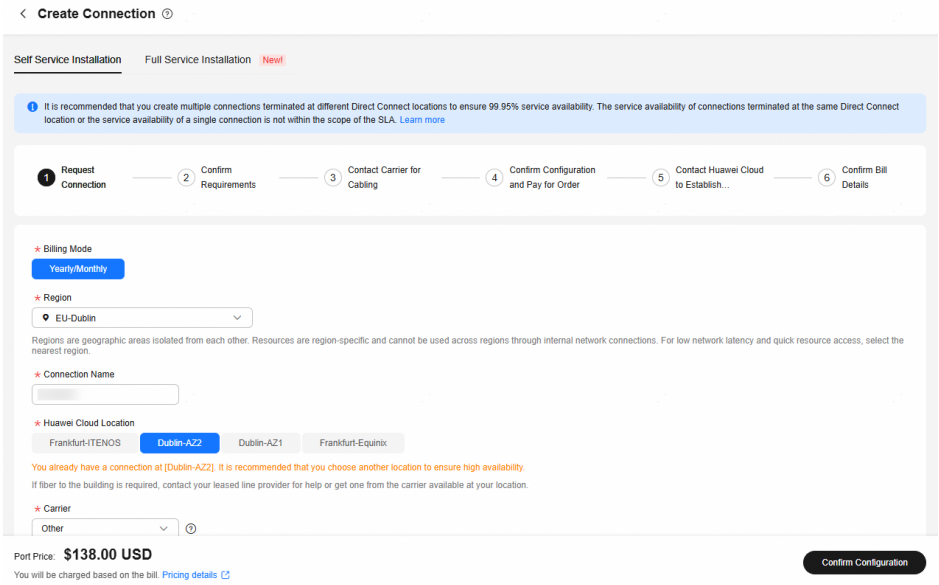


Table 2-1 Parameters for creating a connection

Parameter	Description	Example Value
Billing Mode	Specifies how you will be billed for the connection. Currently, only **Yearly/ Monthly** is supported.	Yearly/Monthly
Region	Specifies the region where the connection will be deployed. You can also change the region in the upper left corner of the console.	EU-Dublin
Connection Name	Specifies the name of the connection.	dc-123
Huawei Cloud Location	Specifies the Direct Connect location where your leased line can be connected to.	Dublin-AZ2
Carrier	Specifies the carrier that provides the leased line.	Other
Port Type	Specifies the type of the port. You can select **1GE single-mode optical port**, **10GE single-mode optical port**, **40GE single-mode optical port**, or **100GE single-mode optical port**.	1GE single-mode optical port
Leased Line Bandwidth (Mbit/s)	Specifies the bandwidth of the leased line. This is the bandwidth of the leased line you have will purchase from the carrier.	100
Equipment Room Address	Specifies the address of your equipment room. The address must be specific to the floor your equipment room is on.	Room xx, xx building, xx road, xx district, xx city
Tag	Adds tags to help you identify your connection. You can change them after the connection is created.	example_key1 example_value1
Description	Provides supplementary information about the connection.	-

Parameter	Description	Example Value
Required Duration	Specifies how long the connection will be used for.	3 months
Auto-renew	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.	3 months
Enterprise Project	Specifies the enterprise project by which connections are centrally managed. Select an existing enterprise project.	default

5. Click **Confirm Configuration**.
6. Confirm the configuration and click **Submit**.

   Then confirm the requirements with the Direct Connect manager.

   If your request is not approved, repeat **3** to **6** based on the review comments and submit the request again.
7. Contact the carrier for cabling after your request is approved.

   After the cabling is complete, locate the connection in the connection list and click **Confirm Cabling** in the **Operation** column.
8. In the displayed dialog box, click **OK**.
9. In the connection list, locate the connection and click **Confirm Configuration** in the **Operation** column.
10. Confirm the configuration and click **Pay Now**.
11. Confirm the order, select a payment method, and click **Confirm**.
12. 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.
13. 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.

Then you need to 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.

Creating a Full-Service Connection

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 Connection**.
4. Click **Full Service Installation**.
5. Provide information about your equipment room and select a Huawei Cloud location. For details about the parameters, see **Table 2-2**.

Figure 2-5 Full-Service Installation

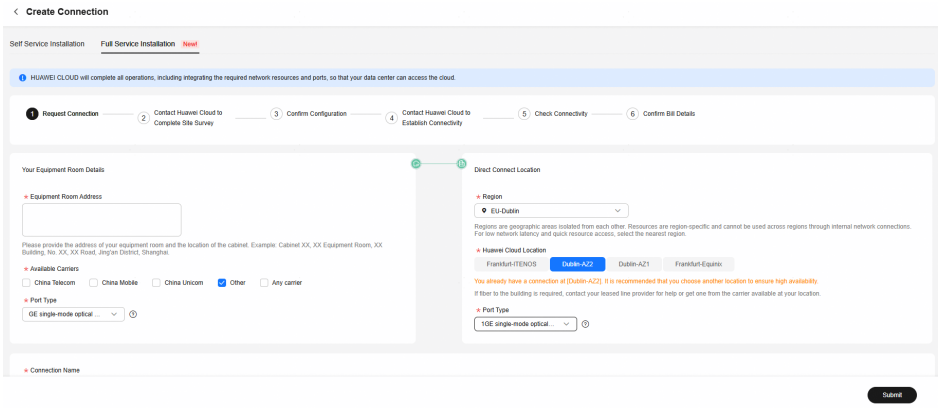


Table 2-2 Parameters for creating a connection

Parameter	Description	Example Value
Equipment Room Address	Specifies the address of your equipment room. The address must be specific to the floor your equipment room is on.	Room xx, xx building, xx road, xx district, xx city
Available Carriers	Specifies the carriers that are allowed to enter your equipment room.	Other
Port Type	Specifies the type of port on the device in your equipment room for connecting to the leased line.	GE single-mode optical port
Region	Specifies the region where the connection will be deployed. You can also change the region in the upper left corner of the console.	EU-Dublin

Parameter	Description	Example Value
Huawei Cloud Location	Specifies the Direct Connect location where your leased line can be connected to.	Dublin-AZ2
Port Type	Specifies the type of the port. You can select **1GE single-mode optical port**, **10GE single-mode optical port**, **40GE single-mode optical port**, or **100GE single-mode optical port**.	GE single-mode optical port
Connection Name	Specifies the name of your connection.	dc-123
Billing Mode	Specifies how you will be billed for the connection. Currently, only **Yearly/ Monthly** is supported.	Yearly/Monthly
Leased Line Bandwidth (Mbit/s)	Specifies the bandwidth of the leased line.	1,000
Required Duration	Specifies how long the connection will be used for.	1 year
Tag	Adds tags to help you identify your connection. You can change them after the connection is created.	example_key1 example_value1
Enterprise Project	Specifies the enterprise project by which connections are centrally managed. Select an existing enterprise project.	default
Contact Person/ Phone Number/ Email	Specifies the contact information about the person 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.	Tom +86 139xxxxxxxx Tom@mail.com

6. Click **Submit**.
7. Wait for Huawei Cloud to complete the 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.

8. Confirm and pay for the order.
   a. In the connection list, locate the connection and click **Confirm Configuration** in the **Operation** column.
   b. 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.

   c. 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.
9. Wait for Huawei Cloud to complete the following work:
   a. Contacts the carrier to deploy the leased line.
   b. Connects your on-premises data center to the cloud using the leased line.
   c. 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.

   d. Enables the port.
10. Confirm that you want to enable Direct Connect.
    a. In the connection list, locate the connection and click **Confirm Completion** in the **Operation** column.
    b. Click **OK**. Confirm that your connection is available for use, and the billing starts.

Partner Connections

Only certified Huawei Cloud partners can create partner connections, including operations connections and hosted connections.

Creating an Operations Connection

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. Specify the required parameters and click **Confirm Configuration**.
5. Confirm the configuration and click **Submit**.

   Then confirm the requirements with the Direct Connect manager.

6. Contact the carrier for cabling after your request is approved.

   After the cabling is complete, locate the connection in the connection list and click **Confirm Cabling** in the **Operation** column.
7. In the displayed dialog box, click **OK**.
8. In the connection list, locate the connection and click **Confirm Configuration** in the **Operation** column.
9. Confirm the configuration and click **Pay Now**.
10. Confirm the order, select a payment method, and click **Confirm**.
11. 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.
12. Verify that the connection is in the **Normal** state, which means that the connection is ready, and the billing starts.

Creating a Hosted Connection

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**.

2.3 Manage Connections

Scenario

This section describes how to view, modify, delete, renew, and unsubscribe from a connection.

Managing Self-Service Connections

Viewing a Self-Service Connection

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

Modifying a Self-Service Connection

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

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**.

Renewing a Self-Service Connection

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

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.

Unsubscribing from a Self-Service Connection

You can only unsubscribe from connections that are in the **Normal** state.

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 displayed 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**.

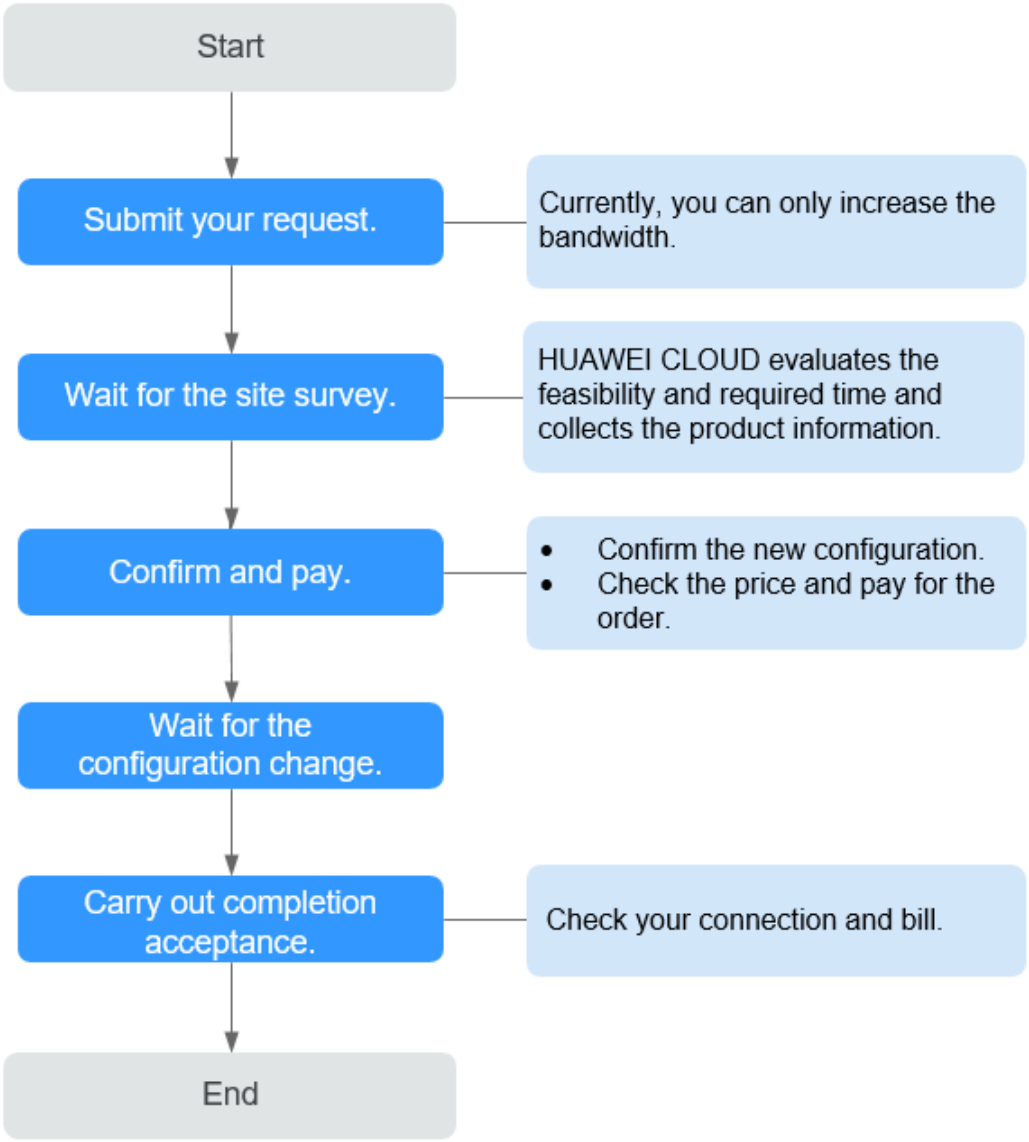
Managing Full-Service Connections

Viewing a Full-Service Connection

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

Modifying a Full-Service Connection

After a full-service connection is created, you can only increase the bandwidth.



1. Submit your request.
   a. Log in to the management console. Under **Networking**, click **Direct Connect**.
   b. Locate the connection you want to modify and click **Change Configuration** in the **Operation** column.
   c. Change the bandwidth as required.

      NOTE

      Currently, only bandwidth increase is supported.

   d. Click **Submit**.
2. Wait for the site survey.

   Huawei Cloud evaluates the feasibility and required time, confirms with you about the product information, and then places you an order.
3. Confirm and pay for the order.

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

b. Confirm the new connection configuration and click **Next**.

NOTE

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

4. Wait for the configuration change.

   It is estimated that 20 working days are required, during which your network connection may be interrupted. You need to confirm the time for the change to take effect.

5. Confirm the new configuration.

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

Renewing a Full-Service Connection

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

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.

Unsubscribing from a Full-Service Connection

Currently, self-service connections cannot be unsubscribed from on the console. Contact your customer manager to unsubscribe from your connection.

Managing Partner Connections

Managing Operations Connections

- **Viewing an Operations Connection**
  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 operations connection list, locate the operations connection and click its name.
  d. On the displayed page, view the detailed information about the operations connection.
- **Modifying an Operations Connection**
  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 operations connection list, locate the operations connection you want to modify and click **More** > **Modify** in the **Operation** column.

d. Modify the connection and then click **OK**.

- **Renewing an Operations Connection**

  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 operations connection list, locate the operations connection you want to renew and choose **More** > **Renew** in the **Operation** column.

  d. Set the duration that you want to renew the connection and click **Pay**. Then pay the order as prompted.

- **Unsubscribing from an Operations Connection**

  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 operations connection list, locate the operations connection that you want to unsubscribe from and choose **More** > **Unsubscribe** in the **Operation** column.

  d. In the operations connection list, locate the target operations connection and click **Unsubscribe from Resource** in the **Operation** column.

  e. On the displayed page, confirm the amount to be refunded.

  f. Click **Confirm**.

Managing Hosted Connections

- **Viewing a Hosted Connection**

  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 operations connection list, locate the operations connection that the hosted connection is hosted on and click **Manage Hosted Connection** in the **Operation** column.

  d. 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**

  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 operations connection list, locate the operations connection that the hosted connection is hosted on and click **Manage Hosted Connection** in the **Operation** column.

  d. In the hosted connection list, locate the hosted connection you want to modify and click **Modify** in the **Operation** column.

e. Modify the hosted connection and click **OK**.

- **Deleting a Hosted Connection**
  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 operations connection list, locate the operations connection that the hosted connection is hosted on and click **Manage Hosted Connection** in the **Operation** column.
  d. In the hosted connection list, locate the hosted connection you want to delete and click **Delete** in the **Operation** column.
  e. Click **OK**.

2.4 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**.

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 go to its details page.
4. On the **Tags** tab, click **Edit Tag**.
5. On the **Edit Tag** page, click **Add** and enter the tag key and value.
   Table 2-3 describes the tag key and value requirements.

Table 2-3 Tag key and value requirements

Parameter	Requirements
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or start with _**sys**_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and the following special characters: _.:/=+-@

6. 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 go to its details page.
4. On the **Tags** tab, click **Edit Tag**.
5. On the **Edit Tag** page, locate the tag to be modified and enter the new tag key and value.
6. 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 go to its details page.
4. On the **Tags** tab, click **Edit Tag**.
5. In the tag list, locate the tag you want to delete and click **Delete**.
6. Click **OK**.

3 Direct Connect Gateways

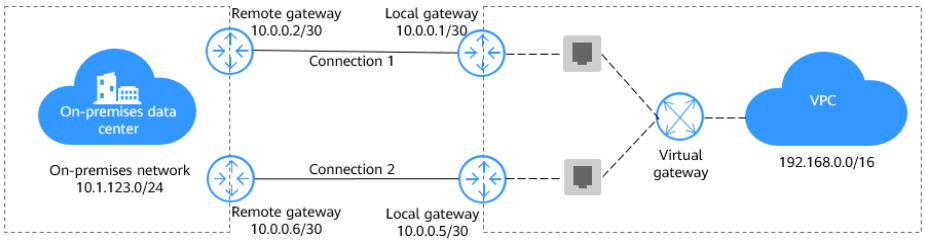
3.1 Direct Connect Gateway Overview

Direct Connect provides two types of gateways: virtual gateway and global DC gateway.

Virtual Gateway

A virtual gateway is a logical gateway that enables an on-premises data center to access a VPC over a connection. To enable an on-premises data center to access a VPC over a connection, you can associate the VPC with a virtual gateway. To access other VPCs, you can use VPC Peering or Cloud Connect to connect the VPC your on-premises data center is accessing to these VPCs.

A virtual gateway can only have one VPC associated. An on-premises data center can access the same VPC over two connections through one virtual gateway.



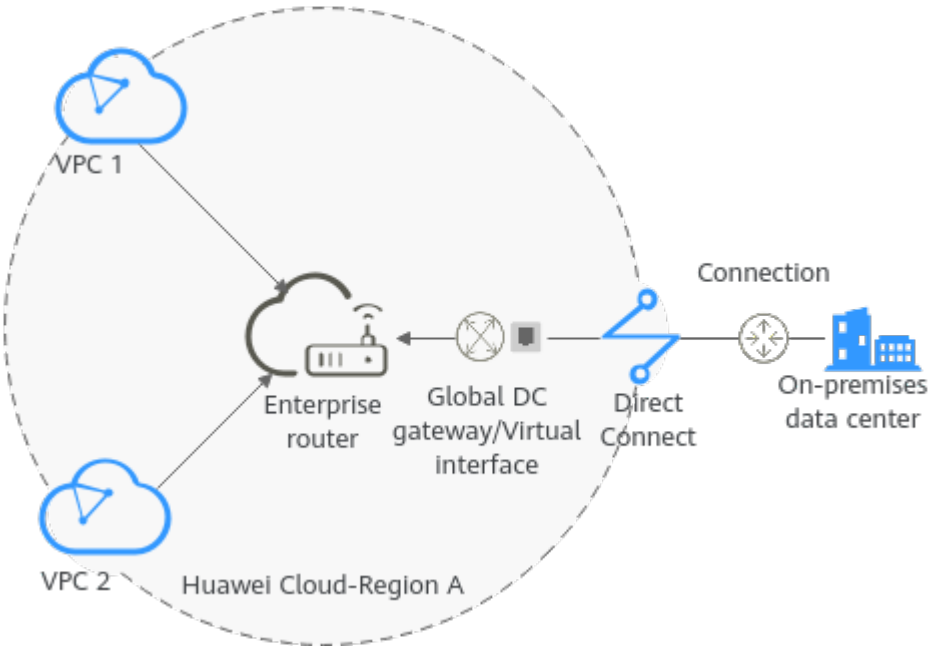
Global DC Gateway

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 be attached to different enterprise routers to build a central network so that an on-premises data center can access the VPCs in different regions over the Huawei backbone network. This reduces network latency, simplifies network topology, and improves O&M efficiency.

A global DC gateway can only be associated with connections terminated at the same Direct Connect location. If there are multiple connections terminated at

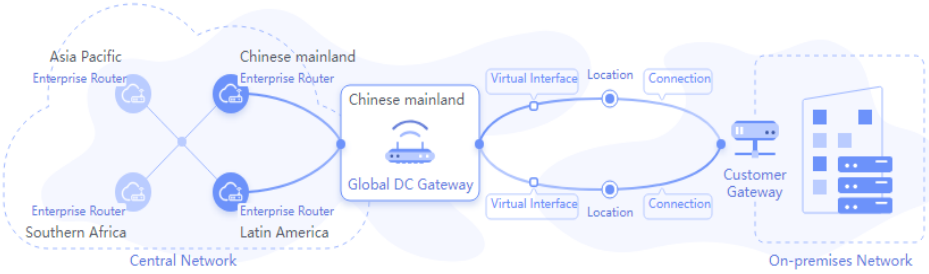
different Direct Connect locations, you need to create multiple global DC gateways.



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



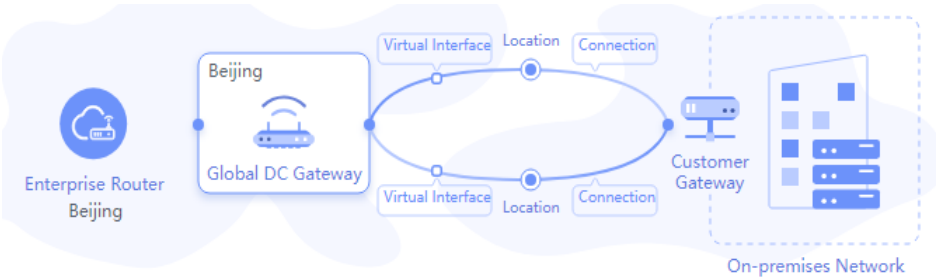
NOTE

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 communications. 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 Virtual Gateway

3.2.1 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. In the **Create Virtual Gateway** dialog box, set the parameters based on **Table 3-1**.

Figure 3-3 Creating a virtual gateway

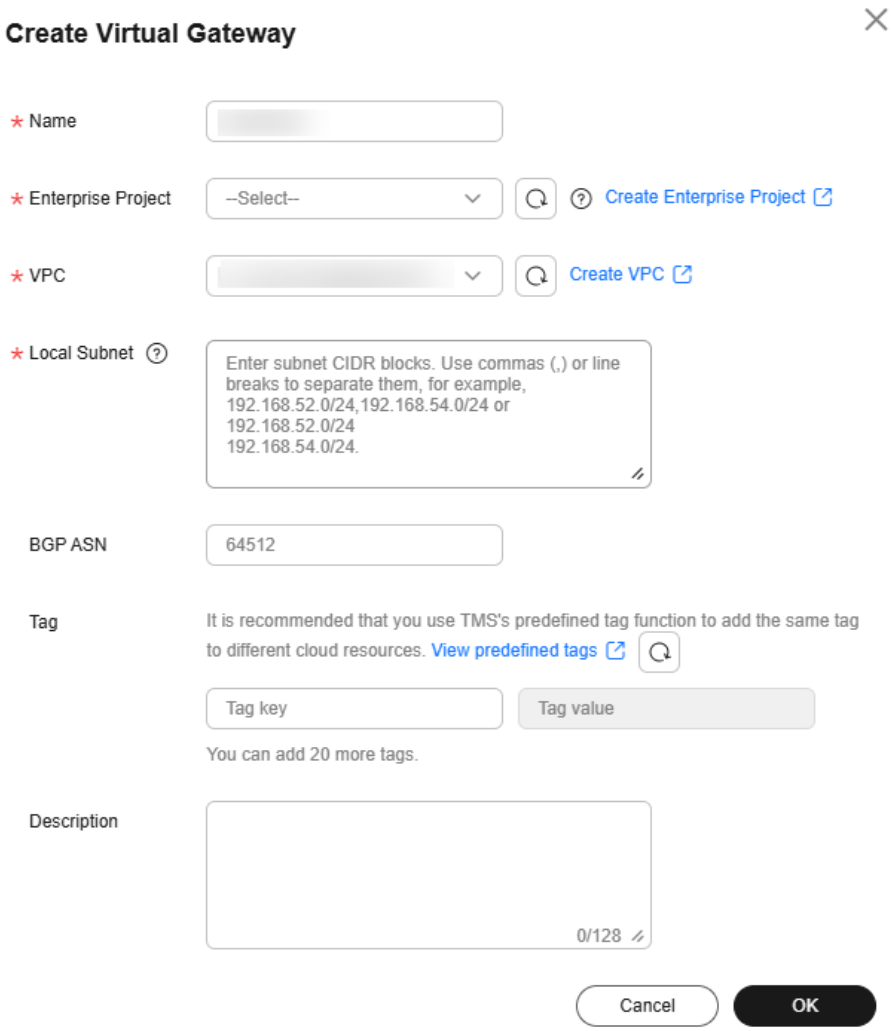


Table 3-1 Parameters required for creating a virtual gateway

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

Parameter	Description	Example Value
Local Subnet	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 them with a comma (,).	192.168.0.0/16
BGP ASN	Specifies the BGP ASN of the virtual gateway.	64512
Tag	Adds tags to help you identify your virtual gateway. You can change them after the virtual gateway is created.	example_key1 example_value1
Description	Provides supplementary information about the virtual gateway.	-

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

3.2.2 Managing Virtual Gateways

Scenario

You can view, modify, and delete a virtual gateway.

Viewing a Virtual Gateway

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.

Modifying a Virtual Gateway

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 parameters as needed and click **OK**.

Deleting a Virtual Gateway

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**.

3.2.3 Managing Virtual Gateway Tags

Scenario

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

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

Adding a Tag

Add a tag to an existing virtual gateway.

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 virtual gateway list, locate the virtual gateway and click its name to go to the details page of the virtual gateway.
4. In the lower part of the page, click **Edit Tag**.
5. On the **Edit Tag** page, click **Add**.

   Enter the tag key and value as prompted.

   Table 3-2 describes the tag key and value requirements.

Table 3-2 Tag naming requirements

Parameter	Requirements
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or start with _**sys**_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@

Parameter	Requirements
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and the following special characters: _.:/=+-@

6. Click **OK**.

Editing a Tag

Modify the value of a tag added to a virtual gateway.

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 virtual gateway list, locate the virtual gateway and click its name to go to the details page of the virtual gateway.
4. In the lower part of the page, click **Edit Tag**.
5. On the **Edit Tag** page, reset the tag key and value.
6. Click **OK**.

Deleting a Tag

Delete a tag from a virtual gateway.

CAUTION

Deleted tags cannot be recovered.

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 virtual gateway list, locate the virtual gateway and click its name to go to the details page of the virtual gateway.
4. In the lower part of the page, click **Edit Tag**.
5. In the tag list, locate the tag you want to delete and click **Delete**.

3.3 Global DC Gateways

3.3.1 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 locations, you need to create multiple global DC gateways.

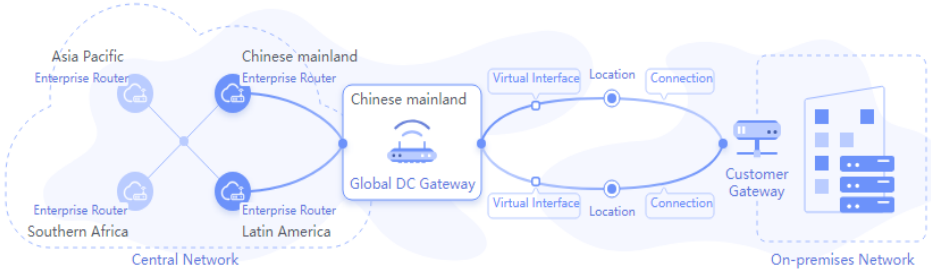
NOTE

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 3-4 Communication with VPCs in different regions using global DC gateways



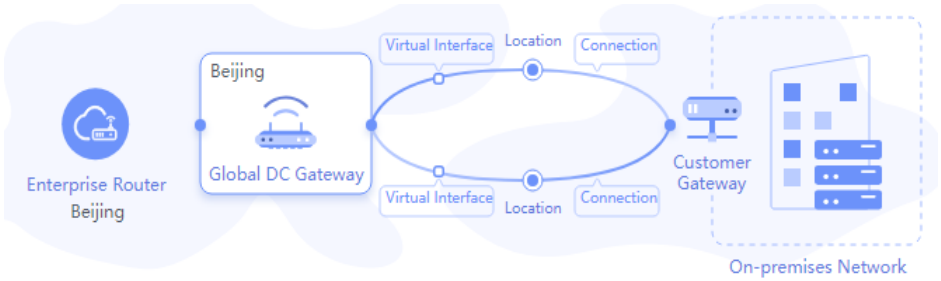
NOTE

If you need to use a central network for cross-region VPC communications, **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 communications. This can reduce the network latency, simplify network topology, and improve network O&M efficiency.

Figure 3-5 Communication with VPCs in the same region using global DC gateways



3.3.2 Creating a Global DC Gateway

Scenario

A global DC gateway can be attached to enterprise routers in the same region for network communications. 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 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 and **Completing Real-Name Authentication**.

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

- **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 a carrier that can lease a line to you based on your requirements.

  - 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.

> **CAUTION**
>
> During the site survey, the construction party only needs to apply to the equipment room supplier for entering the carrier's meet-me room for the site survey.

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 3-3**.

Table 3-3 Parameters for creating a global DC gateway

Parameter	Description	Example Value
Name	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.	dgw-123
Enterprise Project	Specifies the enterprise project by which global DC gateways are centrally managed. Select an existing enterprise project.	default

Parameter	Description	Example Value
BGP ASN	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.	64512
Tag	Adds tags to help you identify your global DC gateway. You can change them after the global DC gateway is created.	example_key1 example_value1
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** after you complete **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 3-4**.

Table 3-4 Parameters for creating a virtual interface

Parameter	Description	Example Value
Region	Specifies the region where the connection resides. You can also change the region in the upper left corner of the console.	EU-Dublin
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters.	vif-123

Parameter	Description	Example Value
Virtual Interface Priority	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.	Preferred
Connection	Specifies the connection you can use to connect your on-premises network to Huawei Cloud.	-
Gateway	Specifies the type of the gateway that the virtual interface connects to. The default option is **Global DC Gateway**.	Global DC Gateway
Global DC Gateway	Specifies the global DC gateway that will be used.	dgw-123
VLAN	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.	30
Bandwidth (Mbit/s)	Specifies the bandwidth that can be used by the virtual interface. The bandwidth cannot exceed that of the connection or LAG.	50 Mbit/s
Enterprise Project	Specifies the enterprise project by which virtual interfaces are centrally managed. Select an existing enterprise project.	default

Parameter	Description	Example Value
Tag	Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created.	example_key2 example_value2
IP Address Family	Specifies the address type of the virtual interface. The default option is **IPv4**.	IPv4
Local Gateway	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.	10.0.0.1/30
Remote Gateway	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.	10.0.0.2/30
Routing Mode	Specifies whether static routing or BGP 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
Remote Subnet	Specifies the subnets and masks of your on-premises network. If there are multiple subnets, use commas (,) to separate them. This parameter is required when static routing is selected.	192.168.51.0/24, 10.1.123.0/24

Parameter	Description	Example Value
BGP ASN	Specifies the ASN of the BGP peer. This parameter is required when BGP routing is selected.	12345
BGP MD5 Authentication Key	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 ~!,.:;-_"(){}[]/@#$%^&*+|=	Qaz12345678
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** after you complete **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 3-5**.

Table 3-5 Parameters for associating an instance

Parameter	Description	Example Value
Resource Type	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 communications, **submit a service ticket**.	Peer link
Peer Link Name	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.	connection-123
Global DC Gateway	Specifies the global DC gateway used for setting up the peer link. By default, the created global DC gateway is selected.	dgw-123
Peer Link Type	The default option is **Enterprise Router**.	Enterprise router
Link To	Specifies the enterprise router at the other end of the peer link.	-

3. Click **OK**.

3.3.3 Managing Global DC Gateways

Scenario

You can view, modify, and delete a global DC gateway.

Viewing a Global DC Gateway

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

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.

Modifying a Global DC Gateway

You can modify the name, IP address family, and description of 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. 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 type 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.

Associating an Instance with a Global DC Gateway

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 communications, **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 a Global DC Gateway 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.

Deleting a Global DC Gateway

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 3-6**.

Table 3-6 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 interface by referring to **Deleting a Virtual Interface**.
The global DC gateway has been added to a central network as an attachment.	Delete the attachment by referring to **Deleting an Attachment**.
The global DC gateway has peer links.	Delete the peer links. For details about how to view the peer links, see **Viewing Peer Links**.

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**.

3.3.4 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**.

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. On the **Tags** tab, click **Edit Tag**.
5. On the **Edit Tag** page, click **Add** and enter the tag key and value.
   Table 3-7 describes the tag key and value requirements.

   Table 3-7 Tag naming requirements

Parameter	Requirements
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or start with **_sys_**. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and the following special characters: _.:/=+-@

6. 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 edit.
4. On the **Tags** tab, click **Edit Tag**.
5. On the **Edit Tag** page, locate the tag to be modified and enter the new tag key and value.
6. Click **OK**.

Deleting a Tag

Delete a tag from a global DC gateway.

CAUTION

Deleted tags cannot be recovered.

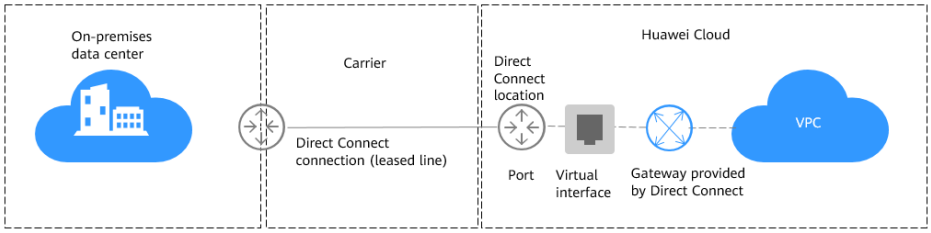
1. Go to the **Global DC Gateways** page.
2. In the upper left corner of the page, click  and select a region and project.
3. Click the name of the global DC gateway that you want to delete a tag from.
4. On the **Tags** tab, click **Edit Tag**.
5. In the tag list, locate the tag you want to delete and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

4 Virtual Interfaces

4.1 Virtual Interface Overview

A virtual interface is a point of entry for an on-premises data center to access a VPC over a connection. A virtual interface associates a connection with a virtual gateway and connects the virtual gateway to a remote gateway, enabling communications between the on-premises data center and the VPC.

Virtual interfaces support static routing and BGP routing. You can use BGP to connect your on-premises data center to the virtual gateway over a connection. BGP helps you build a hybrid cloud more efficiently, flexibly, and reliably.



4.2 Creating a Virtual Interface

Scenario

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

You can create virtual interfaces for the current account or other accounts.

Creating a Virtual Interface for the Current Account

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

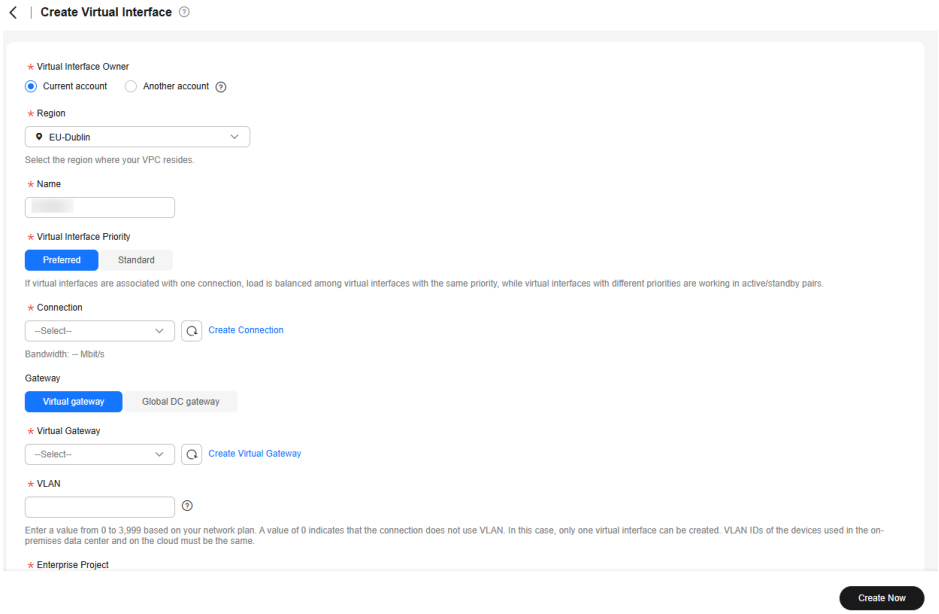


Table 4-1 Parameters for creating a virtual interface

Parameter	Description	Example Value
Virtual Interface Owner	Specifies the account that this virtual interface will be created for. There are two options: • **Current account**: You will create a virtual interface for the current account. • **Another account**: You will create a virtual interface for another account so that this account can use your connection to access the VPC from the on-premises data center. Select **Current account** in this example.	Current account
Region	Specifies the region where the connection is deployed. You can also change the region here or in the upper left corner of the console.	EU-Dublin

Parameter	Description	Example Value
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters.	vif-123
Virtual Interface Priority	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.	Preferred
Connection	Specifies the connection you will use to connect your on-premises network to Huawei Cloud.	dc-123
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
Virtual Gateway	This parameter is mandatory when **Virtual Interface Owner** is set to **Current account** and **Gateway** is set to **Virtual gateway**. Select a virtual gateway that the virtual interface connects to.	vgw-123
Global DC Gateway	This parameter is mandatory when **Virtual Interface Owner** is set to **Current account** and **Gateway** is set to **Global DC gateway**. Select a global DC gateway that the virtual interface connects to.	dgw-123

Parameter	Description	Example Value
VLAN	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.	30
Enterprise Project	Specifies the enterprise project by which virtual interfaces are centrally managed. Select an existing enterprise project.	default
Bandwidth (Mbit/s)	Specifies the bandwidth that can be used by the virtual interface. The bandwidth cannot exceed that of the connection.	50 Mbit/s

Parameter	Description	Example Value
Enable Rate Limiting	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.	Not enabled
Tag	Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created.	example_key1 example_value1
IP Address Family	Specifies the address type of the virtual interface. The default option is **IPv4**.	IPv4

Parameter	Description	Example Value
Local Gateway	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.	10.0.0.1/30
Remote Gateway	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 communications between your on-premises data center and the cloud.	10.0.0.2/30
Routing Mode	Specifies whether static routing or BGP 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

Parameter	Description	Example Value
Remote Subnet	Specifies the subnets and masks of your on-premises network. If there are multiple subnets, use commas (,) to separate them. This parameter is required when static routing is selected.	192.168.51.0/24, 10.1.123.0/24
BGP ASN	Specifies the autonomous system (AS) number of the BGP peer. This parameter is required when BGP routing is selected.	12345
BGP MD5 Authentication Key	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 ~!,.:;-_"(){}[]/@#$%^&*+|=	Qaz12345678
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 of the virtual interface changes to **Normal**, the virtual interface has been created.

   Ping the IP address of a server in the VPC from your on-premises data center to test network connectivity. If the test is successful, your on-premises data center can connect to Huawei Cloud and access the desired VPC.

Creating a Virtual Interface for Another Account

You can create a virtual interface for another account so that this account can use your connection to access the VPC.

Virtual interfaces that you create for other users take effect only after the users accept them.

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

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

Parameter	Description	Example Value
Virtual Interface Owner	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.	Another account
Region	Specifies the region where the connection is deployed. You can also change the region in the upper left corner of the console.	EU-Dublin
Name	Specifies the virtual interface name. The name can contain 1 to 64 characters.	vif-123

Parameter	Description	Example Value
Virtual Interface Priority	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.	Preferred
Connection	Specifies the connection you can use to connect your on-premises network to Huawei Cloud.	dc-123
Gateway	Specifies the type of the gateway that the virtual interface connects to. You can select a virtual gateway or global DC gateway. In this example, select a virtual gateway.	Virtual gateway
Project ID	Specifies the ID of the project that the virtual gateway belongs to. This parameter is mandatory when **Gateway** is set to **Virtual gateway**. On the management console, hover the cursor on the account name in the upper right corner and select **My Credentials**. On the **My Credentials** page, view the project ID.	-

Parameter	Description	Example Value
ID	Specifies the ID of the virtual gateway. This parameter is mandatory when **Gateway** is set to **Virtual gateway**. In the virtual gateway list, hover the cursor on the virtual gateway name and view the name and ID of the virtual gateway.	-
Project ID	Specifies the ID of the project that the global DC gateway belongs to. This parameter is mandatory when **Gateway** is set to **Global DC gateway**. On the management console, hover the cursor on the account name in the upper right corner and select **My Credentials**. On the **My Credentials** page, view the project ID.	-
Global DC Gateway ID	Specifies the ID of the global DC gateway. This parameter is mandatory when **Gateway** is set to **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	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.	30

Parameter	Description	Example Value
Bandwidth (Mbit/s)	Specifies the bandwidth that can be used by the virtual interface. The bandwidth cannot exceed that of the connection.	50 Mbit/s
Enable Rate Limiting	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.	Not enabled
Tag	Adds tags to help you identify your virtual interface. You can change them after the virtual interface is created.	example_key1 example_value1
IP Address Family	Specifies the address type of the virtual interface. **IPv4** is selected by default.	IPv4

Parameter	Description	Example Value
Local Gateway	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.	10.0.0.1/30
Remote Gateway	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 communications between your on-premises data center and the cloud.	10.0.0.2/30
Routing Mode	Specifies whether static routing or BGP 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.	192.168.51.0/24, 10.1.123.0/24

Parameter	Description	Example Value
Remote Subnet	Specifies the subnets and masks of your on-premises network. If there are multiple subnets, use commas (,) to separate them. This parameter is required when static routing is selected.	BGP
BGP ASN	Specifies the ASN of the BGP peer. This parameter is required when BGP routing is selected.	12345
BGP MD5 Authentication Key	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 ~!,.:;-_"(){}[]/@#$%^&*+|=	Qaz12345678
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.

5. Click **Create Now**. When the status of the virtual interface changes to **Normal**, the virtual interface has been created.

   Ping the IP address of a server in the VPC from your on-premises data center to test network connectivity. If the test is successful, your on-premises data center can connect to Huawei Cloud and access the desired VPC.

4.3 Managing Virtual Interfaces

Scenario

You can view, modify, and delete a virtual interface.

Viewing a Virtual Interface

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.

Modifying a Virtual Interface

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.
4. Modify the name, remote subnet, and description, and then click **OK**.

Deleting a Virtual Interface

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**.

4.4 Testing Dual-Connection Automatic Switchovers

Scenario

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

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.

- 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.

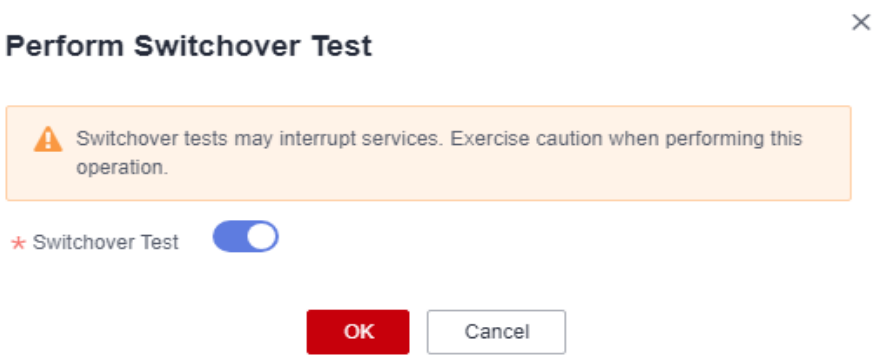
Prerequisites

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

Procedure

1. Go to the **Virtual Interfaces** page.
2. 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 4-2 Enabling switchover test



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

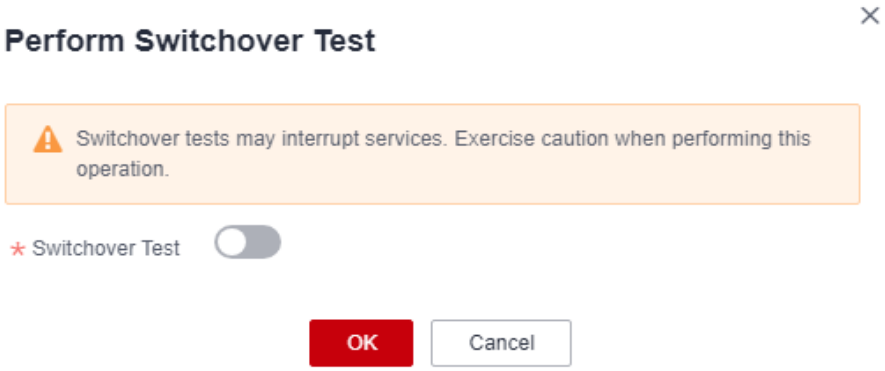
e. Run the **ping** command on an ECS to verify the connectivity between the ECS and the on-premises data center. If a response packet is received, the switchover test is successful.

3. 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 4-3 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.

4. Repeat steps 2 and 3 to perform a switchover test on the virtual interface associated with connection 2.

4.5 Managing Virtual Interface Tags

Scenario

After a virtual interface is created, you can add tags to it, or edit, view or delete its tags.

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

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**.

Adding a Tag

Add a tag to an existing virtual interface.

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 details page of the virtual interface.
4. On the **Tags** tab, click **Edit Tag**.
5. On the **Edit Tag** page, click **Add** and enter the tag key and value.

   Table 4-3 describes the tag key and value requirements.

   Table 4-3 Tag naming requirements

Parameter	Requirements
Key	• Cannot be left blank. • Must be unique for each resource. • Can contain a maximum of 128 characters. • Cannot start or end with a space, or start with _**sys**_. Only letters, digits, spaces, and the following special characters are allowed: _.:=+-@
Value	• Can be left blank. • Can contain a maximum of 255 characters. • Can contain letters, digits, spaces, and the following special characters: _.:/=+-@

6. Click **OK**.

Editing a Tag

Modify the value of a tag added to a virtual interface.

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 details page of the virtual interface.
4. On the **Tags** tab, click **Edit Tag**.
5. On the **Edit Tag** page, locate the tag to be modified and enter the new tag key and value.
6. Click **OK**.

Deleting a Tag

Delete a tag from a virtual interface.

CAUTION

Deleted tags cannot be recovered.

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 details page of the virtual interface.
4. On the **Tags** tab, click **Edit Tag**.
5. In the tag list, locate the tag you want to delete and click **Delete**.
6. Click **OK**.

5 Network Topology

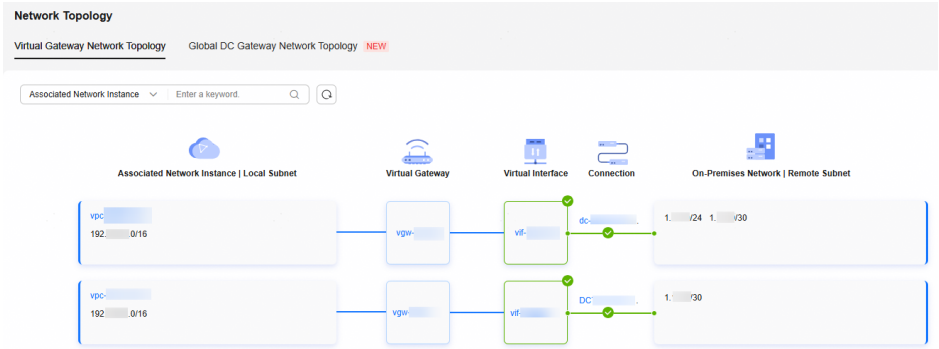
Scenario

After creating a connection, you can view the connection status and resource information in the Direct Connect network topology. Currently, you can view the virtual gateway network topology and the global DC gateway network topology.

This section describes how you can view the virtual gateway topology.

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.

6 Monitoring and O&M

6.1 Cloud Eye Monitoring

6.1.1 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:

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

6.1.2 Monitoring Metrics

Function

This section 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

Connection Monitoring Metrics

Table 6-1 Monitoring metrics supported by Direct Connect connections

ID	Metric	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval
network_incoming_bits_rate	Network Incoming Bandwidth	Bit rate for inbound data to the Direct Connect side of a connection	≥ 0	bit/s	1000 (SI)	direct_connect_id	1 minute
network_outgoing_bits_rate	Network Outgoing Bandwidth	Bit rate for outbound data from the Direct Connect side of a connection	≥ 0	bit/s	1000 (SI)	direct_connect_id	1 minute
network_incoming_bytes	Network Incoming Traffic	The number of bytes for inbound data to the Direct Connect side of a connection	≥ 0	byte	1000 (SI)	direct_connect_id	1 minute
network_outgoing_bytes	Network Outgoing Traffic	The number of bytes for outbound data from the Direct Connect side of a connection	≥ 0	byte	1000 (SI)	direct_connect_id	1 minute
network_incoming_packets_rate	Network Incoming Packet Rate	Packet rate for inbound data to the Direct Connect side of a connection	≥ 0	Packet/s	N/A	direct_connect_id	1 minute

ID	Metric	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval
network_outgoing_packets_rate	Network Outgoing Packet Rate	Packet rate for outbound data from the Direct Connect side of a connection	≥ 0	Packet/s	N/A	direct_connect_id	1 minute
network_incoming_packets	Network Incoming Packets	The number of packets for inbound data to the Direct Connect side of a connection	≥ 0	Packet	N/A	direct_connect_id	1 minute
network_outgoing_packets	Network Outgoing Packets	The number of packets for outbound data from the Direct Connect side of a connection	≥ 0	Packet	N/A	direct_connect_id	1 minute
network_status	Port Status	The status of the port used by a connection	**0** indicates **DOWN**. 1-UP	N/A	N/A	direct_connect_id	1 minute
in_errors	Inbound Error Packets	The number of inbound packets that could not be transmitted to the Direct Connect gateway over the connection because of errors	≥ 0	Packet	N/A	direct_connect_id	1 minute

Virtual Interface Monitoring Metrics

Table 6-2 Monitoring metrics supported by virtual interfaces

ID	Metric	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval
network_incoming_bits_rate	Network Incoming Bandwidth	Bit rate for inbound data to the Direct Connect side of a connection	≥ 0	bit/s	1000 (SI)	virtual_interface_id	1 minute
network_outgoing_bits_rate	Network Outgoing Bandwidth	Bit rate for outbound data from the Direct Connect side of a connection	≥ 0	bit/s	1000 (SI)	virtual_interface_id	1 minute
network_incoming_bytes	Network Incoming Traffic	The number of bytes for inbound data to the Direct Connect side of a connection	≥ 0	byte	1000 (SI)	virtual_interface_id	1 minute
network_outgoing_bytes	Network Outgoing Traffic	The number of bytes for outbound data from the Direct Connect side of a connection	≥ 0	byte	1000 (SI)	virtual_interface_id	1 minute
network_incoming_packets_rate	Network Incoming Packet Rate	Packet rate for inbound data to the Direct Connect side of a connection	≥ 0	Packet/s	N/A	virtual_interface_id	1 minute

ID	Metric	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval
network_outgoing_packets_rate	Network Outgoing Packet Rate	Packet rate for outbound data from the Direct Connect side of a connection	≥ 0	Packet/s	N/A	virtual_interface_id	1 minute
network_incoming_packets	Network Incoming Packets	The number of packets for inbound data to the Direct Connect side of a connection	≥ 0	Packet	N/A	virtual_interface_id	1 minute
network_outgoing_packets	Network Outgoing Packets	The number of packets for outbound data from the Direct Connect side of a connection	≥ 0	Packet	N/A	virtual_interface_id	1 minute

Dimensions

Key	Value
direct_connect_id	Connection ID. You can query the connection ID on the **connection list** page.
virtual_interface_id	Virtual interface ID. You can query the virtual interface ID on the **virtual interface list** page.

6.1.3 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.

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

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 as an example.)

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

   NOTE

   This command 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.

Namespace

SYS.DCAAS

Metrics

Table 6-3 Monitoring metrics

ID	Metric	Description	Value Range	Unit	Conversion Rule	Dimension	Monitoring Interval
latency	Latency	Network latency of a connection	≥ 0	ms	N/A	virtual_interface_id	1 minute
packet_loss_rate	Packet Loss Rate	Packet loss rate of a connection	0~100	%	N/A	virtual_interface_id	1 minute

Dimensions

Key	Value
virtual_interface_id	Virtual interface ID (associated with an automated connection) You can query the virtual interface ID on the **virtual interface list** page.

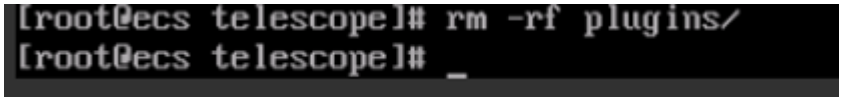
Helpful Links

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.

6.1.4 Installing Metric Collection Plug-ins

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

There are two plug-ins:

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

  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

The plug-ins can only be installed on Linux ECSs that are in the same VPC as the connection.

Prerequisites

Cloud Eye is available in the region.

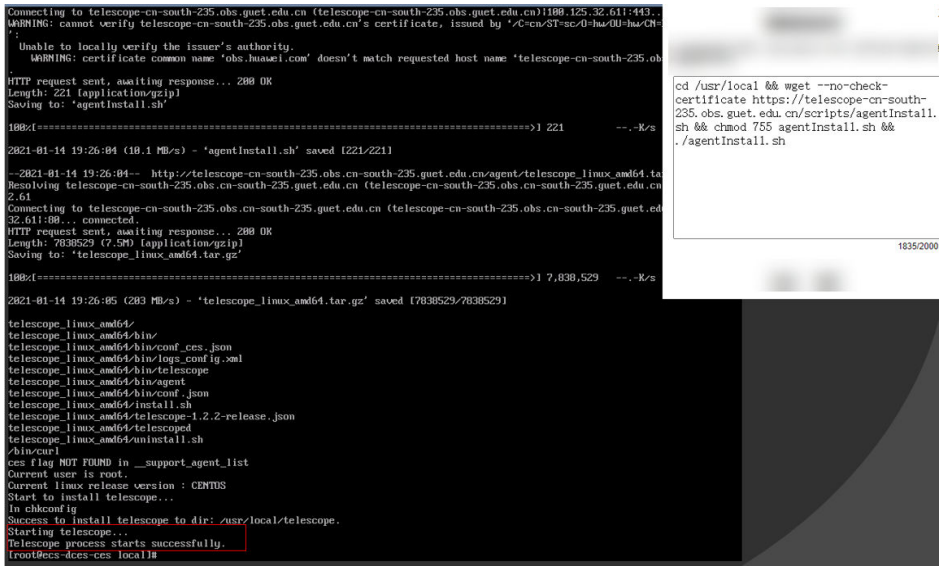
Procedure

Step 1 Install the Agent provided by Cloud Eye for server monitoring.

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring** > **Elastic Cloud Server**.
4. Click **Install and configure the Agent**.
5. Select the Agent based on the server type.

   (x86 servers with image version of 7.0 or later are recommended.)
6. Copy the installation command and run it on the server.

If "Telescope process starts successfully" is displayed, the Agent has been installed.



Step 2 Upload the plug-ins to an OBS bucket.

1. Log in to the management console.
2. Choose **Service List** > **Storage** > **Object Storage Service**.
3. Click **Create Bucket**.
4. Configure the parameters.

   Enter a bucket name and set **Bucket Policy** to **Public Read**.

CAUTION

The public read permission allows any user to read objects in the bucket without identity authentication. To ensure data security, change the bucket policy to **Private** after configuring the plug-ins.

5. Click **Create Now**.
6. Click the name of the created bucket in the bucket list.
7. On the **Overview** page of the bucket, copy the access domain name.
8. In the navigation pane on the left, click **Objects**.
9. On the **Objects** page, click **Upload Object**.
10. Decompress the **dc_plugins_x86.rar** and upload the decompressed file to the OBS bucket.

Step 3 Use the one-click installation script dc-installer.sh to configure the plug-ins.

1. Log in to the ECS as user **root**.
2. Create the **user.txt** file in the **/usr/local/** directory and add user information to the file.

```
cd /usr/local/
vi user.txt
```

The **user.txt** file contains the path of the plug-ins in the OBS bucket, resource ID, and remote IP address.

- Path of the plug-ins in the OBS bucket: Select dc-nqa-collector for automated connections. Select history-dc-nqa-collector for historical connections. The path is in the following format:

  https://cesplugin.obs.*xxx*.edu.cn/dc-nqa-collector

- Information about monitored resources: Each resource occupies a line, and consists of a resource ID and a remote IP address separated from the resource ID by a comma (,). To add multiple resources, add lines in the same format, as shown below:

  75e09ecf-*xxxx-xxxx-xxx*-e1295e03e5dc,*x.x.x.x*

  - Resource ID: If dc-nqa-collector is used, resource ID is the virtual interface ID, which can be queried on the **Virtual Interfaces** page of the Direct Connect console. If history-dc-nqa-collector is used, resource ID is the historical connection ID, which can be queried on the Historical Connections page of the Direct Connect console.
  - Remote IP address: the IP address of the remote gateway or an IP address in the remote subnet, which will be used to ping an IP address in the VPC. If dc-nqa-collector is used, you can query the IP address of the remote gateway on the **Virtual Interfaces** page. If history-dc-nqa-collector is used, you can query the IP address in the remote subnet on the **Historical Connections** page.

    NOTE

    Ensure that each resource ID matches one remote IP address. You cannot enter multiple IP addresses or CIDR blocks.

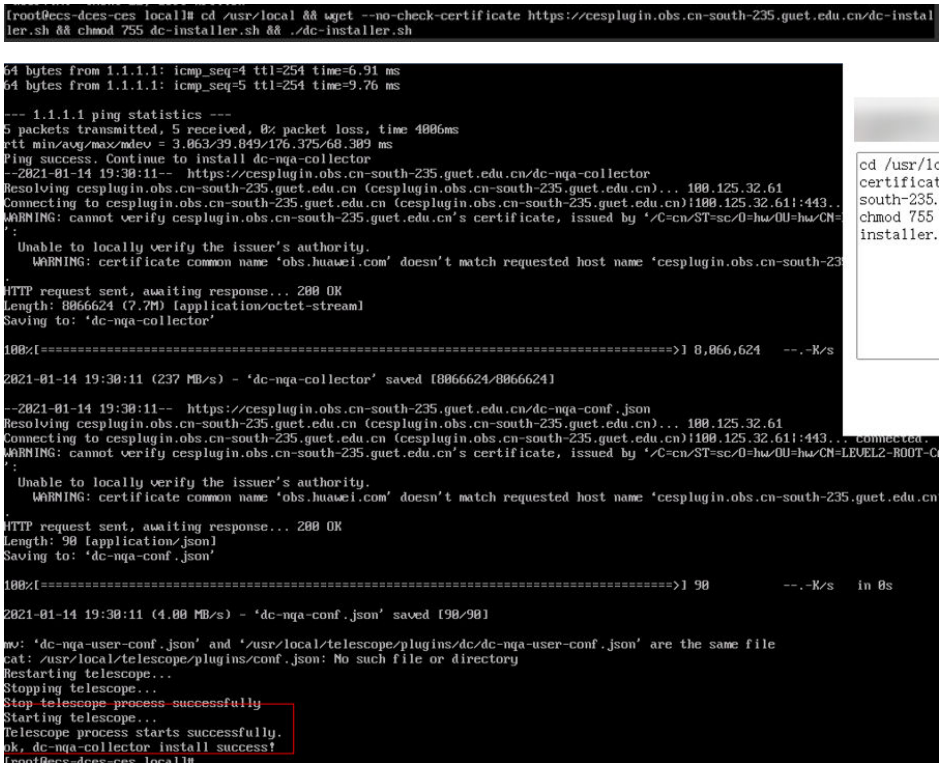
    After the plug-ins are installed, if you want to add more resources for monitoring, edit the **user.txt** file by adding new IDs and IP addresses in sequence, and then perform **Step 3.3**.

3. Execute the one-click installation script.

   The path in the command is where the script is stored in the OBS bucket.

   The following is an example command.

   ```
   cd /usr/local && wget --no-check-certificate https://xxxx.cn/dc-installer.sh && chmod 755 dc-installer.sh && ./dc-installer.sh
   ```



Step 4 View monitoring information.

1. Log in to the management console.
2. Under **Management & Deployment**, select **Cloud Eye**.
3. In the navigation pane on the left, choose **Server Monitoring** > **Elastic Cloud Server**.

   Ensure that the Agent is in the **Running** state.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Direct Connect**.
5. Click the name of the monitored object to view the network latency and packet loss rate.

----End

6.1.5 Creating 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 **Cloud Eye console**.
2. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
3. On the **Alarm Rules** page, click **Create Alarm Rule**.
4. Configure the parameters and 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**.

6.1.6 Viewing Metrics

1. Log in to the **Cloud Eye console**.
2. In the navigation pane on the left, choose **Cloud Service Monitoring**. In the displayed list, click **Direct Connect DCAAS**.

   The **Details** page is displayed.
3. Select the resource type from the drop-down list.

   Example:

   - Cloud service: **Direct Connect**
   - Resource name: **Connections**
4. Click the **Resources** tab.
5. 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.

6.2 Using CTS to Collect Direct Connect Key Operations

6.2.1 Key Operations Recorded by CTS

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

Table 6-4 lists the operations that can be recorded by CTS.

Table 6-4 Direct Connect operations that can be recorded by CTS

Operation	Resource Type	Trace Name
Creating a connection	dcaasConnection	createConnection
Modifying a connection	dcaasConnection	modifyConnection

Operation	Resource Type	Trace Name
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
Deleting a virtual interface	dcaasVirtualInterface	deleteVirtualInterface

6.2.2 Viewing Traces

Scenarios

Cloud Trace Service (CTS) records operations performed on cloud service resources. A record contains information such as the user who performed the operation, IP address, operation content, and returned response message. These records facilitate security auditing, issue tracking, and resource locating. They also help you plan and use resources, and identify high-risk or non-compliant operations.

What Is a Trace?

A trace is an operation log for a cloud service resource, tracked and stored by CTS. Traces record operations such as adding, modifying, or deleting cloud service resources. You can view them to identify who performed operations and when for detailed tracking.

What Is a Management Tracker and Data Tracker?

A management tracker identifies and associates with all your cloud services, recording all user operations. It records management traces, which are operations performed by users on cloud service resources, such as their creation, modification, and deletion.

A data tracker records details of user operations on data in OBS buckets. It records data traces reported by OBS, detailing user operations on data in OBS buckets, including uploads and downloads.

Constraints

- Before the organization function is enabled, you can query the traces of a single account on the CTS console. After the organization function is enabled, you can only view multi-account traces on the **Trace List** page of each account, or in the OBS bucket or the **CTS/system** log stream configured for the management tracker with the organization function enabled.
- You can only query operation records of the last seven days on the CTS console. They are automatically deleted upon expiration and cannot be manually deleted. To store them for longer than seven days, configure transfer to Object Storage Service (OBS) or Log Tank Service (LTS) so that you can view them in the OBS buckets or LTS log streams.
- After creating, modifying, or deleting a cloud service resource, you can query management traces on the CTS console 1 minute later and query data traces 5 minutes later.
- Data traces are not displayed in the trace list of the new version. To view them, you need to go to the old version.

Prerequisites

1. **Register with Huawei Cloud and complete real-name authentication.**

   If you already have a Huawei Cloud account, skip this step. If you do not have one, do as follows:

   a. Log in to the **Huawei Cloud official website**, and click **Sign Up**.

   b. Sign up for a HUAWEI ID as prompted. For details, see **Signing Up for a HUAWEI ID and Enabling Huawei Cloud Services**.

      Your personal information page is displayed after the registration completes.

   c. Complete individual or enterprise real-name authentication by referring to **Real-Name Authentication**.

2. **Grant permissions for users.**

   If you log in to the console using a Huawei Cloud account, skip this step.

   If you log in to the console as an IAM user, first contact your CTS administrator (account owner or a user in the **admin** user group) to obtain the **CTS FullAccess** permissions. For details, see **Assigning Permissions to an IAM User**.

Viewing Real-Time Traces in the Trace List of the New Edition

Step 1 Log in to the **CTS console**.

Step 2 In the navigation pane, choose **Trace List**.

Step 3 In the time range drop-down list above the trace list, select a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also select **Custom** to specify a custom time range within the last seven days.

Step 4 The search box above the trace list supports advanced queries. Combine one or more filters to refine your search.

Table 6-5 Trace filtering parameters

Parameter	Description
Read-Only	After selecting the **Read-Only** filter, you can select either **Yes** or **No** from the drop-down list. • **Yes**: filters read-only operation traces, for example, resource query operations. This option is available after **Read-Only Trace Reporting** has been enabled in the **Configuration Center** and at least one read-only trace has been triggered. • **No**: filters non-read-only operation traces, such as creating, modifying, and deleting resources.
Trace Name	Name of a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. For details about the operations that can be audited for each cloud service, see **Supported Services and Operations**. Example: **updateAlarm**
Trace Source	Cloud service name abbreviation. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. Example: **IAM**
Resource Name	Name of a cloud resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. If the cloud resource involved in the trace does not have a resource name or the corresponding API operation does not involve the resource name parameter, leave this field empty. Example: **ecs-name**
Resource ID	ID of a cloud resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. Leave this field empty if the resource has no resource ID or if resource creation failed. Example: *{VM ID}*
Trace ID	Value of the **trace_id** parameter for a trace reported to CTS. The entered value requires an exact match. Fuzzy matching is not supported. Example: **01d18a1b-56ee-11f0-ac81-******1e229**

Parameter	Description
Resource Type	Type of a resource involved in a trace. The entered value is case-sensitive and requires an exact match. Fuzzy matching is not supported. For details about the resource types of each cloud service, see **Supported Services and Operations**. Example: **user**
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of **trace_type** in a trace is **SystemAction**, the operation is triggered by the service and the trace's operator may be empty.
Trace Status	Select one of the following options from the drop-down list: • **normal**: The operation succeeded. • **warning**: The operation failed. • **incident**: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.
Enterprise Project ID	ID of the enterprise project to which a resource belongs. To check enterprise project IDs, go to the Enterprise Project Management Service (EPS) console and choose **Project Management** in the navigation pane. Example: **b305ea24-c930-4922-b4b9-******1eb2**
Access Key	Temporary or permanent access key ID. To check access key IDs, hover over your username in the upper right corner of the console and select **My Credentials** from the pop-up list. On the displayed page, choose **Access Keys** in the navigation pane. Example: **HSTAB47V9V*******TLN9**

Step 5 On the **Trace List** page, you can also export and refresh the trace list, and customize columns to display.

- Enter any keyword in the search box and press **Enter** to filter desired traces.
- Click **Export** to export all traces in the query result as an .xlsx file. The file can contain up to 5,000 records.
- Click to view the latest information about traces.
- Click to customize the information to be displayed in the trace list. If **Auto wrapping** is enabled ( ), excess text will move down to the next line; otherwise, the text will be truncated. By default, this function is disabled.

Step 6 (Optional) On the **Trace List** page of the new edition, click **Old Edition** in the upper right corner to switch to the **Trace List** page of the old edition.

----End

Viewing Traces in the Trace List of the Old Edition

Step 1 Log in to the **CTS console**.

Step 2 In the navigation pane, choose **Trace List**.

Step 3 Each time you log in to the CTS console, the new edition is displayed by default. Click **Old Edition** in the upper right corner to switch to the trace list of the old edition.

Step 4 In the upper right corner of the page, set a desired query time range: **Last 1 hour**, **Last 1 day**, or **Last 1 week**. You can also click **Customize** to specify a custom time range within the last seven days.

Step 5 Set filters to search for your desired traces.

Table 6-6 Trace filtering parameters

Parameter	Description
Trace Type	Select **Management** or **Data**. • Management traces record operations performed by users on cloud service resources, including creation, modification, and deletion. • Data traces are reported by OBS and record operations performed on data in OBS buckets, including uploads and downloads.
Trace Source	Select the name of the cloud service that triggers a trace from the drop-down list.
Resource type	Select the type of the resource involved in a trace from the drop-down list. For details about the resource types of each cloud service, see **Supported Services and Operations**.
Operator	User who triggers a trace. Select one or more operators from the drop-down list. If the value of **trace_type** in a trace is **SystemAction**, the operation is triggered by the service and the trace's operator may be empty.
Trace Status	Select one of the following options: • **Normal**: The operation succeeded. • **Warning**: The operation failed. • **Incident**: The operation caused a fault that is more serious than a normal failure, for example, causing other faults.

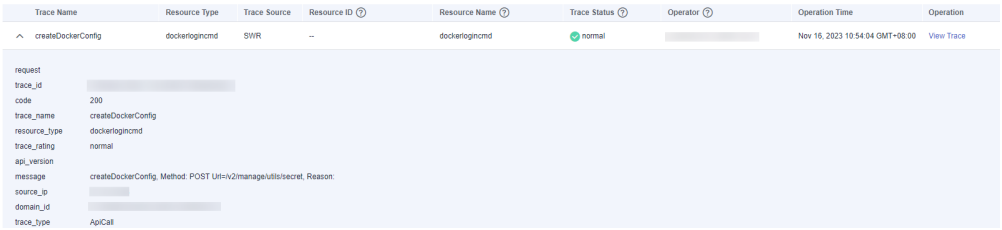
Step 6 Click **Query**.

Step 7 On the **Trace List** page, you can also export and refresh the trace list.

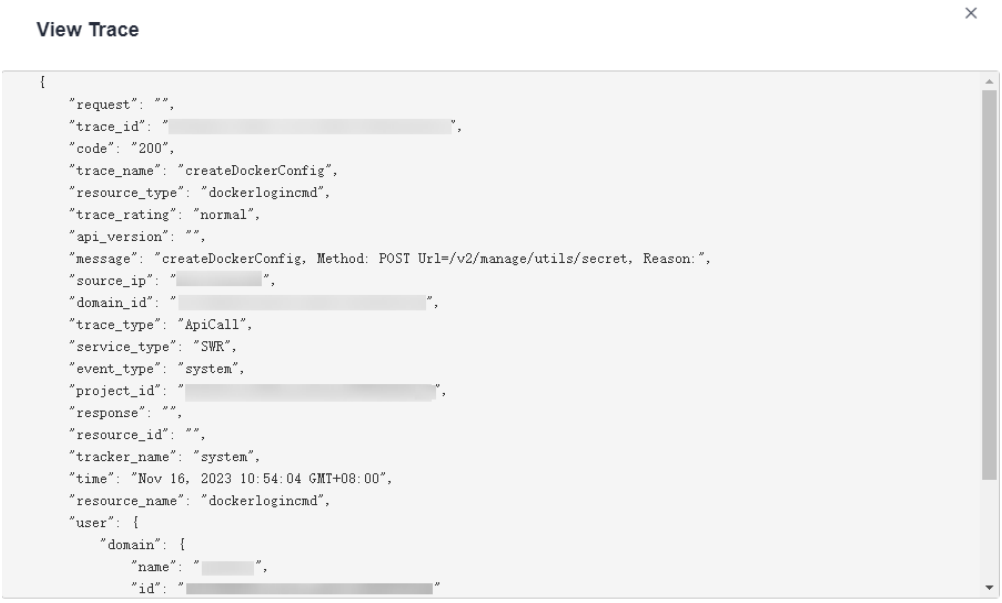
- Click **Export** to export all traces in the query result as a CSV file. The file can contain up to 5,000 records.

- Click to view the latest information about traces.

Step 8 Click on the left of a trace to expand its details.



Step 9 Click **View Trace** in the **Operation** column. The trace details are displayed.



Step 10 (Optional) On the **Trace List** page of the old edition, click **New Edition** in the upper right corner to switch to the **Trace List** page of the new edition.

----End

Helpful Links

- For details about the key fields in the trace structure, see **Trace Structure** and **Example Traces**.

7 Quota Adjustment

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

