Cloud Connect

User Guide

Issue 01

Date 2026-03-09

HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions

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

Notice

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

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

Contents

1 Permissions Management........ 1

1.1 Creating a User and Granting Central Network Permissions........ 1

1.2 Central Network Custom Policies........ 2

2 Central Networks........ 4

2.1 Overview........ 4

2.2 Creating a Central Network........ 6

2.3 Managing Policies........ 8

2.4 Managing Central Network Attachments........ 11

2.5 Managing Cross-Site Connection Bandwidths........ 13

3 Global Connection Bandwidths........ 15

3.1 Overview........ 15

3.2 Buying a Global Connection Bandwidth........ 20

3.3 Adding Instances to a Global Connection Bandwidth........ 21

3.4 Removing Instances from a Global Connection Bandwidth........ 23

3.5 Managing a Global Connection Bandwidth........ 24

4 Monitoring and Auditing........ 25

4.1 Using Cloud Eye to Monitor Central Network Metrics........ 25

4.1.1 Central Network Metrics........ 25

4.1.2 Viewing Central Network Metrics........ 27

4.1.3 Creating an Alarm Rule........ 28

4.2 Using CTS to Record Key Operations on Central Networks........ 28

4.2.1 Key Central Network Operations........ 28

4.2.2 Viewing Central Network Audit Logs........ 30

5 Quotas........ 32

1 Permissions Management

1.1 Creating a User and Granting Central Network Permissions

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

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing Cloud Connect resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust an account or cloud service to perform efficient O&M on your Cloud Connect resources.

Skip this part if you do not require individual IAM users for refined permissions management.

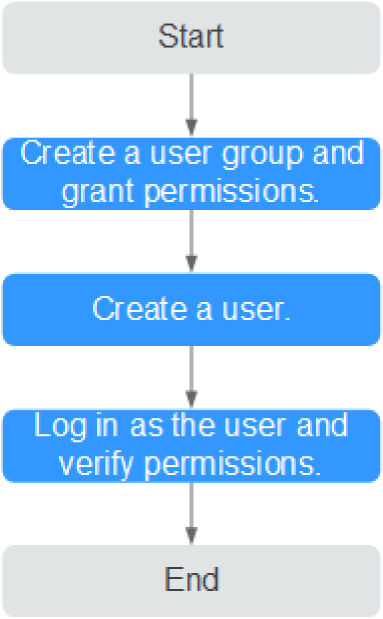
Figure 1-1 shows the process of granting permissions.

Prerequisites

Before you assign permissions to a user group, you need to know the permissions that you can assign to the user group and select permissions based on service requirements. For details about the system permissions, see **Permissions**. For the system policies of other services, see **System Permissions**.

Process Flow

Figure 1-1 Process of granting permissions



Start
Create a user group and grant permissions.
Create a user.
Log in as the user and verify permissions.
End

1. **Create a user group and assign permissions** (the **Cross Connect Administrator** policy used as an example).
2. **Create an IAM user and add it to a group**.

   On the IAM console, create a user and add it to the user group created in **1**.
3. **Log in** and verify permissions.

   After logging in to the Cloud Connect console using the user's credentials, verify that the user has all permissions for Cloud Connect resources.

   – In the service list, choose **Networking** > **Cloud Connect**. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**. Click **Create Central Network** in the upper right corner. If the creation is successful, the **Cross Connect Administrator** policy has taken effect.

   – Choose any other service in the service list. A message will appear indicating that you have sufficient permissions to access the service.

1.2 Central Network Custom Policies

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

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

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Create a JSON policy or edit an existing one.

For details, see **Creating a Custom Policy**. The following section contains examples of common custom policies.

Example Custom Policies

- Example 1: Allowing users to delete central networks

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cc:centralNetwork:delete"
            ]
        }
    ]
}
```

- Example 2: Denying the deletion of central network policies

  A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  The following method can be used if you need to assign permissions of the **CC FullAccess** policy to a user but also forbid the user from deleting central network policies. Create a custom policy and assign both policies to the group that the user belongs to. Then the user can perform all operations on Cloud Connect resources except deleting central network policies. The following is an example of a deny policy:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Deny",
            "Action": [
                "cc:centralNetwork:deletePolicy"
            ]
        }
    ]
}
```

- Example 3: Create a custom policy containing multiple actions.

  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": [
                "cc:centralNetwork:create",
                "cc:centralNetwork:update",
                "cc:centralNetwork:delete",
                "cc:centralNetwork:get"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "er:instances:create",
                "er:instances:update",
                "er:instances:delete",
                "er:instances:get"
            ]
        }
    ]
}
```

2 Central Networks

2.1 Overview

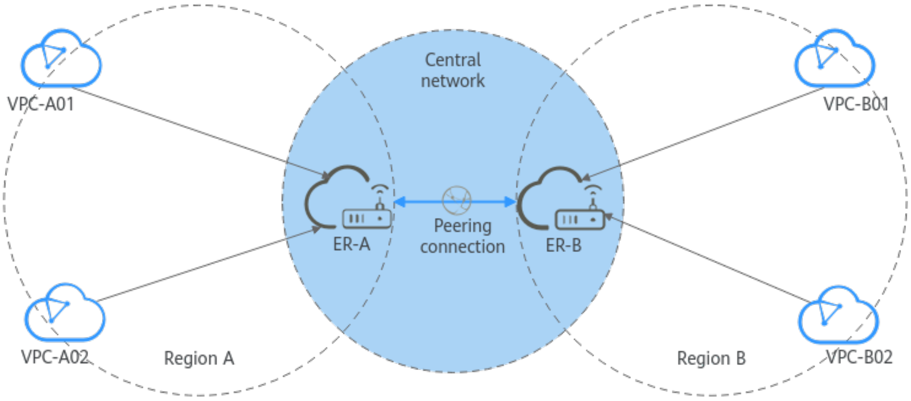
Central Network

Relying on the cloud backbone network, a central network allows you to easily set up a reliable, intelligent enterprise-grade network and manage global network resources on premises and on the cloud. By setting up a central network, you can enable communication between enterprise routers, as well as between enterprise routers and your on-premises data center, in the same region or different regions.

Application Scenarios

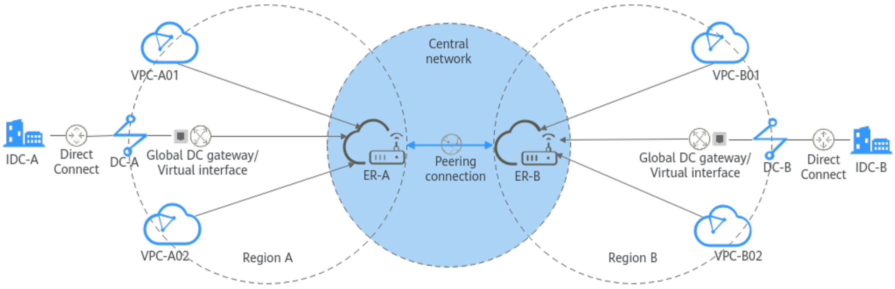
- Cross-region communication on the cloud: Enterprise routers in different regions are added to a central network as attachments so that resources in these regions can communicate with each other over one network.

Figure 2-1 Cross-region communication between enterprise routers



- Communication between on-premises data centers and the cloud: Enterprise routers and global DC gateways are added to a central network as attachments. In this way, multiple VPCs on the cloud can communicate with on-premises data centers across regions.

Figure 2-2 Communication between enterprise routers and on-premises data centers



- Global network: By flexibly changing the central network policies, you can build a global network more conveniently.

Central Network Quotas

Table 2-1 Central network quotas

Quota Type	Default Quota	Adjustable
Central networks in an account	6	Yes .
Policies for a central network	500	Yes .
Policy document size (KB)	10	No
Enterprise routers on a central network as attachments in a region	1	No
Global DC gateways on a central network as attachments in a region	3	Yes .

Constraints on Central Networks

- To use a central network, the following resources must have been created:
  - Enterprise router: used to build a central network
- Policy management
  - A central network can only have one policy. If you apply another policy for this central network, the policy that was previously applied will be automatically cancelled.
  - In each policy, only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default.
  - A policy that is being applied or cancelled cannot be deleted.
- Cross-site connection bandwidth management

- A cross-site connection bandwidth cannot be changed or deleted when it is being created, updated, deleted, frozen, unfrozen, or is recovering.
- The total of cross-site connection bandwidths cannot exceed the global connection bandwidth.
- If a cross-site connection bandwidth is deleted, you will still be billed for the global connection bandwidth.

2.2 Creating a Central Network

Scenarios

After an enterprise router is created, you can create a central network and add the enterprise router to a policy of the central network. In this way, resources can communicate with each other across regions, and network resources in each region can be managed centrally.

If both global DC gateways and enterprise routers are added to a central network, the on-premises data centers can access the cloud.

Constraints

- Before building a central network, you need to create enterprise routers and enable **Default Route Table Association** and **Default Route Table Propagation** for them.

Creating a Central Network

1. Go to the **central network list page**.
2. In the upper right corner of the page, click **Create Central Network**.
3. Configure the central network by referring to **Table 2-2**.

Table 2-2 Parameters for creating a central network

Parameter	Setting
Basic Information	
Name	Enter a name for the central network.

Parameter	Setting
Add Enterprise Router	Add an enterprise router to enable VPCs in the same region to communicate with each other. By working with global DC gateways provided by Direct Connect, enterprise routers enable the VPCs and on-premises data centers to communicate with each other. Enterprise routers in different regions can be connected over a central network to allow for cross-region communication between VPCs and between on-premises data centers and VPCs. Click **Add Enterprise Router** and select the region and route table. Before using the central network, you need to add enterprise routers. Only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default. 10 kbit/s of free bandwidth is provided for testing the connectivity between enterprise routers. If no enterprise router is available for your services, click **Create Enterprise Router** to create one.
Connection Settings (Optional)	
Full-Mesh Peering	This function is enabled by default. Expand the advanced settings to see the full-mesh peering connection list.
Full-Mesh Peering Connections	If this option is enabled, a peering connection will be automatically created between every two enterprise routers you select. The number of enterprise routers you select determines the number of peering connections in the full-mesh peering connection list. You can remove unnecessary peering connections as needed. ● Removing a peering connection: Click **Remove** in the **Operation** column of the target peering connection. ● Connecting a peering connection: Click **Connect** in the **Operation** column of the target peering connection. ● A numerical value that is used to identify a peering connection between two enterprise routers. For full-mesh peering connections, the value can only be 0.
Advanced Settings (Optional)	
Description	Describe the central network for easy identification.

4. Click **Buy Now**. Check the central network configuration, read and select the *Cloud Connect Service Disclaimer*, and click **Submit**.

Follow-up Operations

- Add attachments.

  For details, see **Managing Central Network Attachments**.
- Assign cross-site connection bandwidths.

  For details, see **Managing Cross-Site Connection Bandwidths**.

2.3 Managing Policies

Scenarios

A policy is a single document that defines the configuration of a central network and records how VPCs and global DC gateways access your central network. To better manage your central networks, you can use policies to record the configuration history. You can also apply policies of any version as needed.

You can perform the following operations to manage your central network policies:

- **Creating a Policy**
- **Applying a Policy**
- **Deleting a Policy**

Constraints

- Only one policy can be applied to a central network. If you need to change the policy, apply a new policy. The previously applied policy will be automatically canceled.
- In each policy, only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default.
- A policy that is being applied or cancelled cannot be deleted.

Creating a Policy

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Click the **Policies** tab. You can view the policy applied to the central network. The default version is version 1. You can also check the enterprise routers that have been connected and the full-mesh peering connections.
4. Click **Add Policy** and configure a new policy based on **Table 2-3**.

Table 2-3 Parameters for adding a policy

Parameter	Description	Example Value
Basic Information		

Parameter	Description	Example Value
Add Enterprise Router	Add an enterprise router to enable VPCs in the same region to communicate with each other. By working with global DC gateways provided by Direct Connect, enterprise routers enable the VPCs and on-premises data centers to communicate with each other. Enterprise routers in different regions can be connected over a central network to allow for cross-region communication between VPCs and between on-premises data centers and VPCs. Click **Add Enterprise Router** and select the region and route table. Only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default. 10 kbit/s of free bandwidth is provided for testing the connectivity between enterprise routers. If no enterprise router is available for your services, click **Create Enterprise Router** to create one.	● ER-01 ● ER-02
Connection Settings (Optional)		
Full-Mesh Peering	This function is enabled by default. Expand **Advanced Settings** to check the full-mesh peering connections.	-
Full-Mesh Peering Connections	If this option is enabled, a peering connection will be automatically created between every two enterprise routers you select. The number of selected enterprise routers determines the number of peering connections that will be displayed in the list. You can remove unnecessary peering connections as needed. ● Removing a peering connection: Click **To be removed** in the **Operation** column of the target peering connection. ● Connecting a peering connection: Click **Peering Connection** in the **Operation** column of the target peering connection. ● A numerical value that is used to identify a peering connection between two enterprise routers. For full-mesh peering connections, the value can only be 0.	-

5. Click **Submit**. The **Policies** page is displayed. You can see the policy of version 2 you have added.

Applying a Policy

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Choose the **Policies** tab and click **Apply** on the right of the target policy version. On the **Apply Policy** page, confirm the information shown in **Table 2-4** and click **Submit**.

Table 2-4 Parameters for applying a policy

Parameter	Description
Existing Policy Details	
Existing Policy Name	● **Version 1**: the name of the existing policy. ● **Enterprise Routers**: the enterprise routers on the central network that the existing policy is applied to. ● **Peering Connections**: the peering connections that connect the enterprise routers in the existing policy.
New Policy Details	
New Policy Name	● Version 2: name of the new policy to be applied. ● **Enterprise Routers**: the enterprise routers on the central network that the new policy will be applied to. ● **Peering Connections**: the peering connections that connect the enterprise routers in the new policy.
Policy Change Details	
Enterprise Routers	The enterprise routers on the central network that the new policy will be applied to.
Peering Connections	The peering connections that connect the enterprise routers in the new policy.
Confirm	
Current Configuration	**Existing Policy Name**: **Version 1**
New Configuration	**New Policy Name**: **Version 2**
Enterprise router attachment change	Price for changing the policy of a central network.

4. Confirm the settings and click **Submit**. The **Policies** tab is displayed. If **Version 2** is in the **Applied** state, the new policy is applied.

Deleting a Policy

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. On the **Policies** tab, locate the policy you want to delete and click **Delete** on the right.
4. In the displayed dialog box, click **OK**.

2.4 Managing Central Network Attachments

Scenarios

Attachments are any resources that you want to add to a central network, such as global DC gateways and enterprise routers. In this way, these resources can be connected across regions.

You can perform the following operations to manage your central network attachments:

- **Adding Attachments**
- **Deleting an Attachment**

Constraints

- Only existing global DC gateways or enterprise router route tables can be added to a central network as attachments. If there are no global DC gateways, create one by following the instructions in **Creating a Global DC Gateway**.

  NOTE

  You can check the regions where global DC gateways are available on the Direct Connect console.
- By default, you can add up to three attachments to a central network. To increase the default quota, submit a service ticket.
- Up to five attachments can be added on the console at a time.

Adding Attachments

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. On the **Attachments** tab, click **Add Attachment**.
4. Add network instances such as global DC gateways or enterprise router route tables to the central network. **Table 2-5** describes the parameters.

Table 2-5 Parameters for adding a network instance to a central network as an attachment

Parameter	Setting
Name	Enter a name for the attachment.

Parameter	Setting
Region where the enterprise router on the central network is located	
Region	Select the region of the enterprise router that the network instance is attached to.
Enterprise Router	Select an enterprise router in the selected region. The network instance will be attached to the selected enterprise router. If there are no enterprise routers for you to choose from, click **Create Enterprise Router** to create one first.
Network instance that will be added to a central network	
Attachment Type	Specify the type of the network instance that will be added to the central network as attachment. Only global DC gateways are supported. A global DC gateway can work with enterprise routers in the same region or different regions to build a central network so that your on-premises data center can access the VPCs over the Huawei backbone network. This can reduce network latency, simplify network topology, and improve O&M efficiency.
Region	Select the region where the global DC gateway is located. This region may be different from that of the enterprise router.
Global DC Gateway	Select the global DC gateway that will be attached to the selected enterprise router, so that they can communicate with each other and the on-premises data center can communicate with the cloud network. If there are no global DC gateways for you to choose from, click **Create Global DC Gateway** to create one first.
Configuration Fee	The connections to enterprise routers are not free. The price of connections on a central network is determined by the number of pay-per-use enterprise routers.

If you want to add more attachments, click **Add Attachments** below and configure the parameters.

5. Click **OK**.

   You can view the attachment in the attachment list. If **Status** is **Available**, the attachment is added successfully.

Deleting an Attachment

Deleting an attachment will interrupt network communications on the current network.

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. On the **Attachments** tab, locate the attachment you want to delete and click **Delete** in the **Operation** column.
4. Click **OK**.

2.5 Managing Cross-Site Connection Bandwidths

Scenarios

Add enterprise routers or global DC gateways in different regions to the same policy to set up cross-site connections. Purchase a global connection bandwidth and assign bandwidths for cross-site connections, so that network instances at different sites can communicate with each other over these connections.

You can perform the following operations to manage your cross-site connection bandwidths:

- **Assigning a Cross-Site Connection Bandwidth**
- **Viewing Monitoring Metrics of Cross-Site Connection Bandwidths**
- **Changing Cross-Site Connection Bandwidth**
- **Deleting a Cross-Site Connection Bandwidth**

Constraints

- A cross-site connection bandwidth cannot be modified or deleted when it is being created, updated, deleted, frozen, unfrozen, or is recovering.
- The total of cross-site connection bandwidths cannot exceed the global connection bandwidth.
- After **Deleting a Cross-Site Connection Bandwidth**, you will still be billed if the global connection bandwidth is not deleted.

Assigning a Cross-Site Connection Bandwidth

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Click the **Cross-Site Connection Bandwidths** tab.
4. Locate the cross-site connection and click **Assign** in the **Global Connection Bandwidth** column.
5. On the **Assign Cross-Site Connection Bandwidth** page, select the global connection bandwidth.

   You can also click **Buy Now** to purchase one if there are no available global connection bandwidths.
6. Enter the bandwidth.
7. Click **OK**.

Viewing Monitoring Metrics of Cross-Site Connection Bandwidths

You can view the status of each cross-site connection bandwidth assigned for communication between network resources.

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Switch to the **Cross-Site Connection Bandwidths** tab and click the icon in the **Monitoring** column to view the monitoring data.

NOTE

- By setting up a central network, you can enable communications between enterprise routers, as well as between enterprise routers and your on-premises data center, in the same region or across regions. When a central network is used, attachments on the enterprise routers used in the central network policy will be monitored.
- If a global DC gateway is attached to an enterprise router, only metrics of the enterprise router can be viewed.

Changing Cross-Site Connection Bandwidth

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Click the **Cross-Site Connection Bandwidths** tab.
4. Locate the cross-site connection and click **Change Bandwidth** in the **Operation** column.
5. In the displayed dialog box, change the global connection bandwidth of the cross-site connection.

   You can also change the bandwidth size of the cross-site connection.

   NOTE

   Select a proper bandwidth size. Excessive bandwidth wastes resources, while insufficient bandwidth limits cross-site data transfer speeds. This can cause higher delays, frozen frames, lost packets, and connection timeouts if the traffic exceeds the bandwidth capacity.

   After the change is done, delete the original bandwidth that is no longer needed to avoid unnecessary billing.
6. Click **OK**.

Deleting a Cross-Site Connection Bandwidth

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Click the **Cross-Site Connection Bandwidths** tab.
4. Locate the cross-site connection and click **Delete Bandwidth** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

3 Global Connection Bandwidths

3.1 Overview

What Is a Global Connection Bandwidth?

A global connection bandwidth is used by instances to allow communication over the backbone network.

NOTE

- In Cloud Connect, global connection bandwidths are mainly used by central networks.

There are different types of global connection bandwidths that are designed for different application scenarios, including multi-city, HomeZones, geographic-region, and cross-geographic-region bandwidths. Geographic-region and cross-geographic-region bandwidths are often bound to cloud connections for communication on the cloud.

Table 3-1 Global connection bandwidth types

Bandwidth Type	Instance Type	Description	Scenario
Multi-city	Global EIPs	Select this type of bandwidth if you need communication between cloud regions in the same region, for example, CN East-Shanghai1 and CN East-Shanghai2 in East China.	A global EIP and its associated resource, such as an ECS or load balancer, have to be in the same region. **Multi-city Bandwidth Application Scenario (Global EIP)**

Bandwidth Type	Instance Type	Description	Scenario
Geographic-region	- Global EIPs - Central network	Select this type of bandwidth if you need communication within a geographic region. Geographic regions include the Chinese mainland, Asia Pacific, and Southern Africa. For example, CN East-Shanghai1 and CN South-Guangzhou are regions in the Chinese mainland. For details about the relationship between geographic regions and Huawei Cloud regions, see **Geographic Regions and Huawei Cloud Regions**.	- A global EIP and its associated resource, such as an ECS or load balancer, have to be in the same geographic region. **Geographic-Region Bandwidth Application Scenario (Global EIP)** - Enterprise routers on a central network are from the same geographic region. **Geographic-Region or Cross-Geographic-Region Bandwidth Application Scenario (Central Network)**
Cross-geographic-region	- Global EIPs - Central network	Select this type of bandwidth if you need communication across geographic regions. Geographic regions include the Chinese mainland, Asia Pacific, and Southern Africa. For example, CN East-Shanghai1 and CN-Hong Kong are regions in the Chinese mainland. For details about the relationship between geographic regions and Huawei Cloud regions, see **Geographic Regions and Huawei Cloud Regions**.	- A global EIP and its associated resource, such as an ECS or load balancer, are from different geographic regions. **Cross-Geographic-Region Bandwidth Application Scenario (Global EIP)** - Enterprise routers on a central network are from different geographic regions. **Geographic-Region or Cross-Geographic-Region Bandwidth Application Scenario (Central Network)**

Constraints on Global Connection Bandwidths

- Instances that can be added to a global connection bandwidth must be from the same region as the bandwidth.
- A global connection bandwidth can only be used by instances of the same type. If you want another type of instances to use a global connection bandwidth, you need to unbind the current type of instances first.
  - You can add or remove global EIPs in batches.

  - You can bind one global connection bandwidth to or unbind it from a central network at a time.
- To use a global connection bandwidth on a central network, you need to configure cross-site connections by referring to the following:
  - **Creating a Central Network**
  - **Managing Policies**
- Global connection bandwidths of different types can be used with different instances. For details, see **Table 3-2**.

Table 3-2 Instances that can use a global connection bandwidth

Bandwidth Type	Global EIP	Central Network	Edge Instance
Multi-city	√	×	×
Geographic-region	√	√	×
Cross-geographic-region	√	√	×

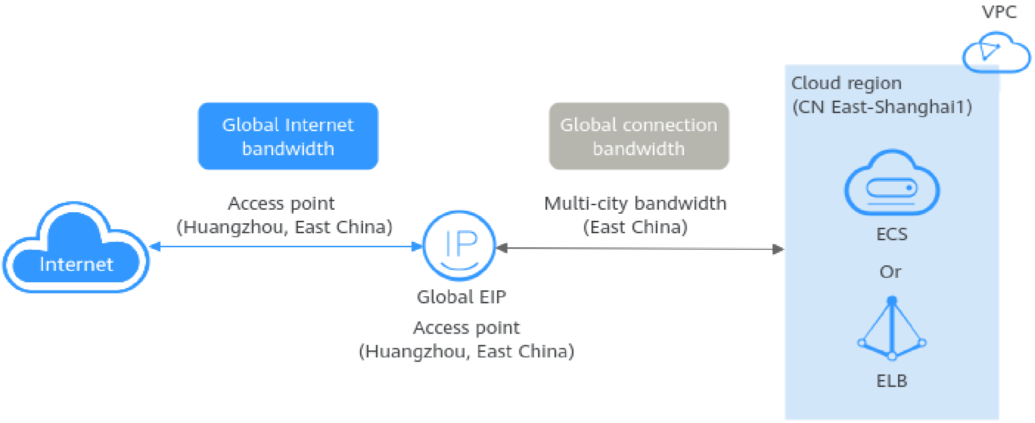
- Before an instance is removed from a global connection bandwidth, ensure the instance is not used to run workloads or establish network connectivity, or the workloads will be unavailable or the network will be interrupted.
- If a global connection bandwidth has been used to assign cross-site connection bandwidths for a central network, the global connection bandwidth cannot be unbound from the central network. You need to delete the cross-site connection bandwidths first.
- If a global connection bandwidth is in use by instances, it cannot be deleted. To delete such a bandwidth, unbind its instance first. For details, see **Removing Instances from a Global Connection Bandwidth**.

Multi-city Bandwidth Application Scenario (Global EIP)

In this example, a global EIP is bound to an ECS.

The ECS is in the CN East-Shanghai1 region, and the access point of the global EIP is in Hangzhou, a city in East China.

Figure 3-1 Multi-city bandwidth application scenario (global EIP)

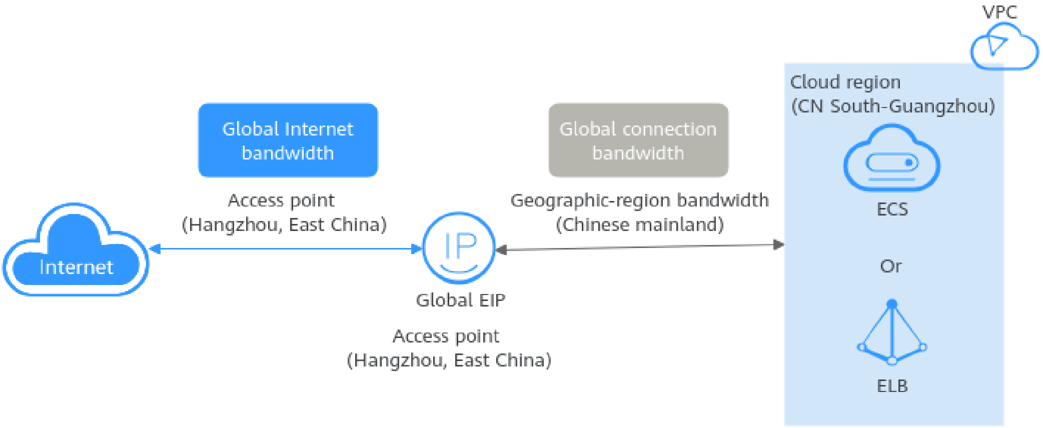


Geographic-Region Bandwidth Application Scenario (Global EIP)

In this example, a global EIP is bound to an ECS.

The ECS is in the CN South-Guangzhou region, and the access point of the global EIP is in Hangzhou. Both Guangzhou and Hangzhou are cities on the Chinese mainland.

Figure 3-2 Geographic-region bandwidth application scenario (global EIP)



Cross-Geographic-Region Bandwidth Application Scenario (Global EIP)

In this example, a global EIP is bound to an ECS.

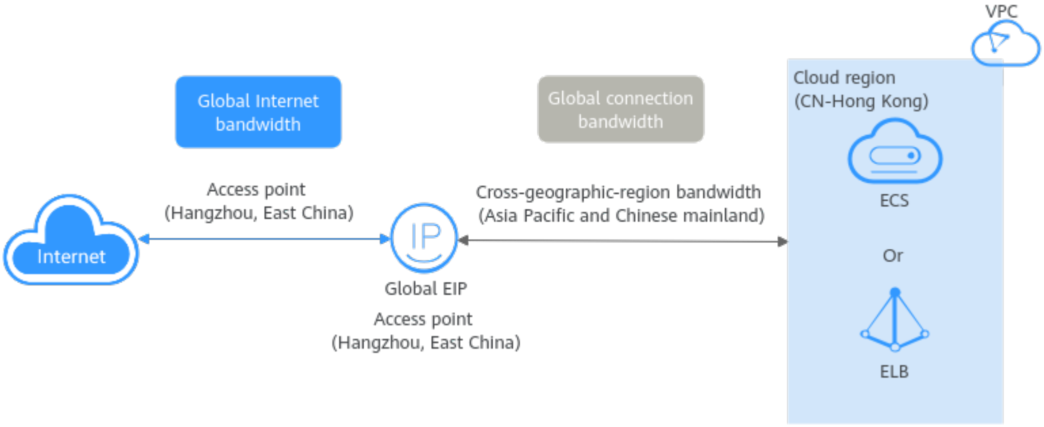
The ECS is in the CN-Hong Kong region, and the access point of the global EIP is in Hangzhou. CN-Hong Kong is a cloud region in Asia Pacific, but Hangzhou is a city on the Chinese mainland.

- Geographic region 1: Asia Pacific, the geographic region where the ECS is located
- Geographic region 2: Chinese mainland, the geographic region where the global EIP is accessed

NOTE

Ensure that the geographic regions 1 and 2 are configured as above.

Figure 3-3 Cross-geographic-region bandwidth application scenario (global EIP)


VPC
Global Internet bandwidth
Global connection bandwidth
Cloud region (CN-Hong Kong)
ECS
Access point (Hangzhou, East China)
Cross-geographic-region bandwidth (Asia Pacific and Chinese mainland)
Internet
IP
Global EIP
Access point (Hangzhou, East China)
Or
ELB

Geographic-Region or Cross-Geographic-Region Bandwidth Application Scenario (Central Network)

In this example, enterprise routers are connected over a cloud connection.

- Enterprise router 1 in CN East-Shanghai1 and enterprise router 2 in CN South-Guangzhou are from the same geographic region. A geographic-region bandwidth can be used for communication between the two enterprise routers.
- Enterprise router 1 in CN East-Shanghai1 and enterprise router 3 in CN-Hong Kong are in different geographic regions. A cross-geographic-region bandwidth can be used for communication between the two enterprise routers.
  - Geographic region 1: Chinese mainland, geographic region where enterprise router 1 is located
  - Geographic region 2: Asia Pacific, geographic region where enterprise router 3 is located

  NOTE

  Ensure that both the geographic regions of enterprise router 1 and enterprise router 3 have been configured.
- Enterprise router 2 in CN South-Guangzhou and enterprise router 3 in CN-Hong Kong are in different geographic regions. A cross-geographic-region bandwidth can be used for communication between the two enterprise routers.
  - Geographic region 1: Chinese mainland, geographic region where enterprise router 2 is located
  - Geographic region 2: Asia Pacific, geographic region where enterprise router 3 is located

3.2 Buying a Global Connection Bandwidth

Scenarios

This section describes how to buy a global connection bandwidth for communication over the backbone network.

Procedure

1. Go to the **Create Global Connection Bandwidth** page.
2. Configure the parameters based on **Table 3-3**.

Table 3-3 Parameters required for buying a global connection bandwidth

Parameter	Setting	Example Value
Billing Mode	Mandatory **Pay-per-use**: a postpaid subscription. You are charged based on the usage duration of the global connection bandwidth. The usage of a global connection bandwidth is calculated by the second but billed by hour. If the usage is less than an hour, you are billed based on the actual duration.	Pay-per-use
Bandwidth Name	Mandatory Enter the name of the bandwidth. The name: ● Must contain 1 to 64 characters. ● Can contain letters, digits, underscores (_), hyphens (-), and periods (.).	bandwidth-test
Enterprise Project	Mandatory Selects an enterprise project by which cloud resources and members are centrally managed.	default

Parameter	Setting	Example Value
Bandwidth Type	Mandatory Select a bandwidth type. There are different types of global connection bandwidths that are designed for different application scenarios, including multi-city, geographic-region, and cross-geographic-region bandwidths. The type of a bandwidth cannot be changed once it is created. For details, see **Global Connection Bandwidth Overview**. You can decide whether to use a geographic-region bandwidth or cross-geographic-region bandwidth based on service scenarios. If you select a geographic-region, cross-geographic-region, or HomeZones bandwidth, you also need to select geographic regions and specify the regions that need to communicate with each other.	Geographic-region
Billed By	Mandatory The price of a global connection bandwidth varies by its size. ● After a bandwidth is purchased, the billing starts immediately regardless of whether the bandwidth is used. ● If a bandwidth is no longer required, delete it in a timely manner to avoid unnecessary fees.	Bandwidth
Bandwidth	Mandatory Select the bandwidth, in Mbit/s.	100

3. Click **Next**.
4. Confirm the configurations and click **Submit**.

   The global connection bandwidth list page is displayed.
5. In the global connection bandwidth list, view the status of the bandwidth.

   If the bandwidth status becomes **Normal**, the purchase is successful.

3.3 Adding Instances to a Global Connection Bandwidth

Scenarios

A global connection bandwidth must be bound to a network instance to control the data transfer speed on the cloud backbone network. This section shows how to add a cloud service instance (global EIP or central network) to a global connection bandwidth.

- **Using a Global Connection Bandwidth on a Central Network (Assigning Bandwidths to a Cross-Site Connection on a Central Network)**
- **Adding Global EIPs to a Global Connection Bandwidth**

Constraints

- Instances that can be added to a global connection bandwidth must be from the same region as the bandwidth.
- A global connection bandwidth can only be used by instances of the same type. If you want another type of instances to use a global connection bandwidth that already has instances, you need to remove the instances first.
  - You can add or remove global EIPs in batches.
  - You can bind one global connection bandwidth to or unbind it from a central network at a time.
- To use a global connection bandwidth on a central network, you need to configure cross-site connections by referring to the following:
  - **Creating a Central Network**
  - **Managing Policies**
  - **Managing Central Network Attachments**
- Global connection bandwidths of different types can be used with different instances. For details, see **Table 3-4**.

Table 3-4 Instances that can use a global connection bandwidth

Bandwidth Type	Global EIP	Central Network
Multi-city	√	×
Geographic-region	√	√
Cross-geographic-region	√	√

Using a Global Connection Bandwidth on a Central Network (Assigning Bandwidths to a Cross-Site Connection on a Central Network)

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Click the **Cross-Site Connection Bandwidths** tab.
4. Locate the cross-site connection and click **Assign** in the **Global Connection Bandwidth** column.
5. On the **Assign Cross-Site Connection Bandwidth** page, select the global connection bandwidth.
6. Specify the bandwidth and click **OK**.

Adding Global EIPs to a Global Connection Bandwidth

1. Go to the **global connection bandwidth list page**.
2. Locate the global connection bandwidth and click **Bind** in the **Operation** column.
3. In the displayed dialog box, select **Global EIP** for **Instance Type**.

   For a multi-city global connection bandwidth, select the two regions where the bandwidth will be used.
4. Search for global EIPs using keyword.
5. Select one or more global EIPs and click **OK**.

3.4 Removing Instances from a Global Connection Bandwidth

Scenarios

You can remove global EIPs from a global connection bandwidth or unbind a global connection bandwidth from a central network.

Constraints

- Before an instance is removed from a global connection bandwidth, the instance is not used to run workloads or establish network connectivity, or the workloads will be unavailable or the network will be interrupted.
- A global connection bandwidth can only be used by one type of instances. If you want to change the instance type, remove all the instances from the global connection bandwidth and then add instances of another type by referring to **Binding a Global Connection Bandwidth**.
- If a global connection bandwidth has been used to assign cross-site connection bandwidths for a central network, the global connection bandwidth cannot be unbound from the central network. You need to delete the cross-site connection bandwidths first.

Deleting a Cross-site Connection Bandwidth from a Central Network

1. Go to the **central network list page**.
2. Locate the central network and click its name.
3. Click the **Cross-Site Connection Bandwidths** tab.
4. Locate the cross-site connection and click **Delete Bandwidth** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

Removing Instances from a Global Connection Bandwidth

1. Go to the **global connection bandwidth list page**.
2. Locate the global connection bandwidth and click **Unbind** in the **Operation** column.

- If the bandwidth is only bound to one instance, click **Remove** in the **Operation** column and then click **OK** in the displayed dialog box.
- If the bandwidth is bound to more than one instance:
  1. On the details page of the bandwidth, click **Associated Instances**.
  2. Select the instances.
  3. Click **Remove** above the instance list.
  4. In the displayed dialog box, click **OK**.

3.5 Managing a Global Connection Bandwidth

Scenarios

You can only modify the bandwidth name and capacity. If you modify the capacity, the new bandwidth takes effect immediately.

You can perform the following operations to manage your global connection bandwidths:

- **Modifying a Global Connection Bandwidth**
- **Deleting a Global Connection Bandwidth**

Constraints

If a global connection bandwidth is in use by instances, it cannot be deleted. To delete such a bandwidth, unbind its instance first. For details, see **Removing Instances from a Global Connection Bandwidth**.

Modifying a Global Connection Bandwidth

1. Go to the **global connection bandwidth list page**.
2. Locate the global connection bandwidth you want to modify and choose **More** > **Modify Bandwidth** in the **Operation** column.
3. On the **Modify Global Connection Bandwidth** page, modify the bandwidth name and capacity and click **Next**.
4. Confirm the information and click **Submit**.

   Once you modify the global connection bandwidth, modify the cross-site connection bandwidths on the central network to apply these changes to the cross-region network communications. For details, see **Assigning a Cross-Site Connection Bandwidth**.

Deleting a Global Connection Bandwidth

1. Go to the **global connection bandwidth list page**.
2. Locate the global connection bandwidth you want to delete and choose **More** > **Delete** in the **Operation** column.
3. In the displayed dialog box, click **OK**.

4 Monitoring and Auditing

4.1 Using Cloud Eye to Monitor Central Network Metrics

4.1.1 Central Network Metrics

Overview

By setting up a central network, you can enable communications between enterprise routers, as well as between enterprise routers and your on-premises data center, in the same region or across regions. When a central network is used, attachments on the enterprise routers used in the central network policy will be monitored.

This section describes metrics reported by enterprise routers in the central network policy to Cloud Eye as well as their namespaces and dimensions. You can view the metrics on the Cloud Eye console.

Namespace

SYS.ER

Metrics

Table 4-1 Monitoring metrics of an enterprise router attachment

ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
attachment_bytes_in	Inbound Traffic	Network traffic going into the attachment	≥ 0	Byte	1024 (IEC)	Enterprise router attachment	1 minute
attachment_bytes_out	Outbound Traffic	Network traffic going out of the attachment	≥ 0	Byte	1024 (IEC)	Enterprise router attachment	1 minute
attachment_bits_rate_in	Inbound Bandwidth	Network traffic per second going into the attachment	≥ 0	bit/s	1000 (SI)	Enterprise router attachment	1 minute
attachment_bits_rate_out	Outbound Bandwidth	Network traffic per second going out of the attachment	≥ 0	bit/s	1000 (SI)	Enterprise router attachment	1 minute
attachment_packets_in	Inbound PPS	Packets going into the attachment per second	≥ 0	pps	1000 (SI)	Enterprise router attachment	1 minute
attachment_packets_out	Outbound PPS	Packets going out of the attachment per second	≥ 0	pps	1000 (SI)	Enterprise router attachment	1 minute

ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
attachment_packets_drop_blackhole	Packets Dropped by Black Hole Route	Packets dropped by black hole route of the attachment	≥ 0	Count	N/A	Enterprise router attachment	1 minute
attachment_packets_drop_noroute	Packets Dropped Due to No Route Matched	Packets dropped because the attachment has no matching routes	≥ 0	Count	N/A	Enterprise router attachment	1 minute

Dimensions

Key	Value
er_attachment_id	Enterprise router attachment

4.1.2 Viewing Central Network Metrics

Scenarios

You can view the metrics of attachments on the enterprise routers in a central network policy on the Cloud Eye console.

Procedure

Step 1 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Enterprise Router**.

The enterprise router list is displayed.

Step 2 View the real-time metrics of enterprise router attachments.

1. In the enterprise router list, click **View Metric** in the **Operation** column of the target attachment.

   The metrics are displayed.

2. View metrics of the attachment.

----End

4.1.3 Creating an Alarm Rule

Scenarios

This section describes how to create alarm rules and notifications for enterprise router attachments.

The alarm function provides the alarm service for monitoring data. By creating alarm rules, you define how the alarm system checks monitoring data and sends alarm notifications when monitoring data meets alarm policies.

After creating alarm rules for important metrics, you can timely know metric data exceptions and quickly rectify the faults.

Procedure

Step 1 In the navigation pane on the left, choose **Cloud Service Monitoring** > **Enterprise Router ER**.

The enterprise router list is displayed.

Step 2 Create an alarm rule and notification for an enterprise router attachment.

1. In the enterprise router list, choose **More** > **Create Alarm Rule** in the **Operation** column of the target attachment.

   The **Create Alarm Rule** page is displayed.

2. On the **Create Alarm Rule** page, configure the parameters as prompted.

----End

4.2 Using CTS to Record Key Operations on Central Networks

4.2.1 Key Central Network Operations

Scenarios

With CTS, you can record operations associated with central networks and global connection bandwidths for later query, audit, and backtracking.

Prerequisites

You have enabled CTS.

Key Operations Recorded by CTS

Table 4-2 Central network operations that can be recorded by CTS

Operation	Resource	Trace
Creating a central network	centralNetwork	createCentralNetwork
Updating a central network	centralNetwork	updateCentralNetwork
Deleting a central network	centralNetwork	deleteCentralNetwork
Adding a central network policy	centralNetworkPolicy	createCentralNetworkPolicy
Applying a central network policy	centralNetworkPolicy	applyCentralNetworkPolicy
Deleting a central network policy	centralNetworkPolicy	deleteCentralNetworkPolicy
Adding a global DC gateway to a central network as an attachment	centralNetworkAttachment	createCentralNetworkGdgwAttachment
Updating a global DC gateway on a central network	centralNetworkAttachment	updateCentralNetworkGdgwAttachment
Removing an attachment from a central network	centralNetworkAttachment	deleteCentralNetworkAttachment
Updating a central network connection	centralNetworkConnection	updateCentralNetworkConnection
Adding a tag to a central network	createCentralNetworkTags	centralNetworkTags
Deleting a tag from a central network	deleteCentralNetworkTags	centralNetworkTags

Table 4-3 Global connection bandwidth operations recorded by CTS

Operation	Resource	Trace
Creating a global connection bandwidth	globalConnectionBandwidth	createGcBandwidth
Updating a global connection bandwidth	globalConnectionBandwidth	updateGcBandwidth

Operation	Resource	Trace
Deleting a global connection bandwidth	globalConnectionBand-width	deleteGcBandwidth
Binding a global connection bandwidth to an instance	globalConnectionBand-width	bindGcBandwidth
Unbinding a global connection bandwidth from an instance	globalConnectionBand-width	unbindGcBandwidth

4.2.2 Viewing Central Network Audit Logs

Scenarios

After CTS is enabled, it starts recording operations on cloud resources. You can view the operation records of the last seven days on the CTS console.

This section describes how you can query or export the operation records of the last seven days on the CTS console.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner to select a region and a project.
3. In the upper left corner of the page, click ☰ to go to the service list. Under **Management & Deployment**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**
5. Specify filters as needed. The following filters are available:
   - **Trace Type**: Set it to **Management** or **Data**.
   - **Trace Source**, **Resource Type**, and **Search By**

     Select filters from the drop-down list.

     After you select **Trace name** for **Search By**, you also need to select a trace name.

     After you select **Resource ID** for **Search By**, you also need to select or enter a resource ID.

     After you select **Resource name** for **Search By**, you also need to select or enter a resource name.
   - **Operator**: Select a specific operator (at the user level rather than the tenant level).
   - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
   - Search time range: In the upper right corner, choose **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
6. Click the arrow on the left of the required trace to expand its details.

7. Click **View Trace** in the **Operation** column to view trace details.

5 Quotas

What Is Quota?

Quotas can limit the number 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 a region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.

   The **Service Quota** 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 **Service Quota** 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**.