

Cloud Connect

User Guide

Issue 01
Date 2024-08-23



Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Cloud Computing Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI 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 Central Network Operation Guide.....	1
1.1 Overview.....	1
1.2 Managing Central Networks.....	2
1.3 Managing Policies.....	4
1.4 Managing Attachments.....	5
1.5 Managing Cross-Site Connection Bandwidths.....	7
1.6 Auditing.....	8
1.6.1 Key Operations Recorded by CTS.....	9
1.6.2 Viewing Traces.....	10
2 Global Connection Bandwidth Operation Guide.....	11
2.1 Overview.....	11
2.2 Buying a Global Connection Bandwidth.....	15
2.3 Binding a Global Connection Bandwidth.....	16
2.4 Unbinding a Global Connection Bandwidth.....	18
2.5 Modifying a Global Connection Bandwidth.....	19
2.6 Deleting a Global Connection Bandwidth.....	19
2.7 Auditing.....	20
2.7.1 Key Operations Recorded by CTS.....	20
2.7.2 Viewing Traces.....	20
3 Permissions Management.....	22
3.1 Creating a User and Granting Permissions.....	22
3.2 Custom Policy.....	23
4 Quotas.....	25

1 Central Network Operation Guide

1.1 Overview

What Is a Central Network?

Relying on the cloud backbone network, Central Network allows you to easily build a reliable, intelligent enterprise-grade network and manage global network resources on premises and on the cloud. By building 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 different regions.

Application Scenarios

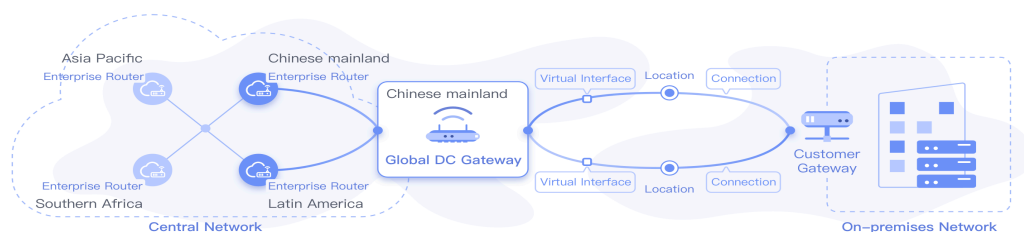
- Cross-region communication on the cloud: Enterprise routers in different regions are added to a central network as attachments so that resources in these regions can communicate with each other over one network.

Figure 1-1 Cross-region communication between enterprise routers



- Communication between on-premises data centers and the cloud across regions: Enterprise routers and global DC gateways are added to a central network as attachments, so that on-premises data centers can access the cloud over the cloud backbone network.

Figure 1-2 Connectivity between enterprise routers and an on-premises data center

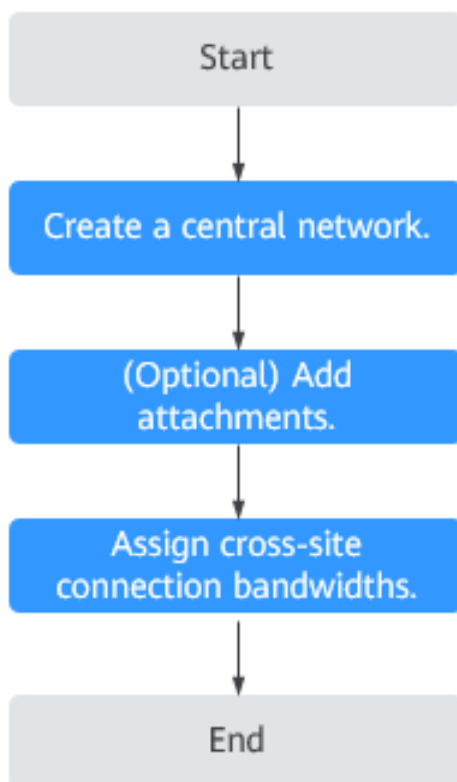


- Global network: By flexibly changing the central network policies, you can build a global network more conveniently.

Process for Using a Central Network to Manage Network Resources

Figure 1-3 shows the process of configuring a central network to manage global network resources.

Figure 1-3 Configuration process



1.2 Managing Central Networks

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

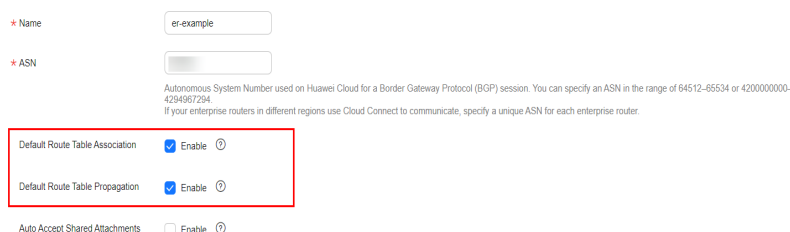
communicate with each other across regions, and network resources in each region can be managed centrally.

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.

Figure 1-4 Enabling **Default Route Table Association** and **Default Route Table Propagation** for enterprise routers



- To enable communication between on-premises data centers and the cloud, you need to create global DC gateways and add them to the central network as attachments.

NOTE

You can check the regions where global DC gateways are available on the Direct Connect console.

Creating a Central Network

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Click **Create Central Network**.
5. Enter the name and description and then configure policies for the central network. [Table 1-1](#) lists the parameters required for creating a central network.

Table 1-1 Parameters for creating a central network

Parameter	Setting
Name	Enter a name for the central network.
Description	Describe the central network for easy identification.
Policy	

Parameter	Setting
Region	Add a policy to record your configuration. You need to select a region for the policy.
Enterprise Router	Add only one enterprise router for a region. All added enterprise routers can communicate with each other by default. 10 kbit/s of bandwidth is provided for testing connectivity between enterprise routers.

6. Click **OK**.

Follow-up Operations

- Add attachments.
For details, see [Managing Attachments](#).
- Assign cross-site connection bandwidths.
For details, see [Managing Cross-Site Connection Bandwidths](#).

1.3 Managing Policies

Scenarios

Policies record the enterprises routers that have been added to a central network to allow you to better manage your network. You can apply policies of any version.

Constraints

- 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.

Creating a Policy

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. Switch to the **Policies** tab and click **Add Policy**.
6. Select the target region and the enterprise router in this region.
You can click **Add Enterprise Router** to add an enterprise router in another region.

7. Click **OK**.

Applying a Policy

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. On the **Policies** tab, locate the policy you want to apply and click **Apply** on the right.
6. In the **Policy Changes** area on the right, check the change of the enterprise router in the policy.
7. Click **OK**.

Deleting a Policy

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. On the **Policies** tab, locate the policy you want to delete and click **Delete** on the right.
6. In the displayed dialog box, click **OK**.

1.4 Managing Attachments

Scenarios

You can add network instances such as global DC gateways to a central network as attachments to enterprise routers in given regions, so that network instances in different regions can communicate with each other.

This topic describes how to manage attachments on a central network.

Constraints

- Only existing global DC gateways can be added to a central network as attachments.

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 quota, submit a service ticket.
- Up to five attachments can be added on the console at a time on the console. To add more attachments, click **OK** and then click **Add Attachment**.

Adding Attachments

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. Switch to the **Attachments** tab and click **Add Attachment**.
6. Add network instances such as global DC gateways to the central network. [Table 1-2](#) describes the parameters.

Table 1-2 Parameters for adding a network instance to a central network as an attachment

Parameter	Setting
Name	Enter a name for the attachment.
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 as attachment. Currently, 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.

7. Click **OK**.

Deleting an Attachment

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. Switch to the **Attachments** tab, locate the attachment you want to delete, and click **Delete** in the **Operation** column.
6. Click **OK**.

1.5 Managing Cross-Site Connection Bandwidths

Scenarios

Enterprise routers and global DC gateways in different regions added to the same policy can communicate with each other after you purchase a global connection bandwidth and assign cross-site connection bandwidths for these network resources.

Constraints

- [Changing a Cross-Site Connection Bandwidth](#) and [Deleting a Cross-Site Connection Bandwidth](#) cannot be performed when a cross-site connection is being created, updated, deleted, frozen, unfrozen, or recovered.
- 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. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. Switch to the **Cross-Site Connection Bandwidths** tab, locate the cross-site connection, and click **Assign now** in the **Global Connection Bandwidth** column.
6. 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.

7. Enter the bandwidth.
8. Click **OK**.

Viewing Monitoring Metrics of Cross-Site Connection Bandwidths

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

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. Switch to the **Cross-Site Connection Bandwidths** tab and click the icon in the **Monitoring** column to view the monitoring data.

NOTE

- For more information about Enterprise Router monitoring, see [Supported Metrics](#).
- If a global DC gateway is attached to an enterprise router, only metrics of the enterprise router can be viewed.

Changing a Cross-Site Connection Bandwidth

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. Switch to the **Cross-Site Connection Bandwidths** tab, locate the cross-site connection, and click **Change Bandwidth** in the **Operation** column.
6. On the **Change Bandwidth** page, change the global connection bandwidth or modify the cross-site connection bandwidth.
7. Click **OK**.

Deleting a Cross-Site Connection Bandwidth

1. Log in to the management console.
2. In the service list, choose **Networking > Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. Locate the central network and click its name.
5. Switch to the **Cross-Site Connection Bandwidths** tab, locate the cross-site connection, and click **Delete Bandwidth** in the **Operation** column.
6. In the displayed dialog box, click **OK**.

1.6 Auditing

1.6.1 Key Operations Recorded by CTS

Scenarios

With Cloud Trace Service (CTS), you can record operations associated with cloud connections and central networks for later query, audit, and backtracking.

Prerequisites

You have enabled CTS.

Key Operations Recorded by CTS

Table 1-3 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



1.6.2 Viewing Traces

Scenarios

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

This topic describes how to query or export 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 and select the desired region and 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.
If you select **Trace name** for **Search By**, select a trace name.
If you select **Resource ID** for **Search By**, select or enter a resource ID.
If you select **Resource name** for **Search By**, select or enter a resource name.
 - **Operator**: Select a specific operator (a user other than an account).
 - **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 arrow on the left of the required trace to expand its details.
7. Locate the required trace and click **View Trace** in the **Operation** column.
A dialog box is displayed, showing the trace content.

2 Global Connection Bandwidth Operation Guide

2.1 Overview

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

NOTE

- In Cloud Connect, global connection bandwidths are mainly used by central networks.
- By default, global connection bandwidths cannot be used by cloud connections. Only some existing users can bind global connection bandwidths to cloud connections.

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. Geographic-region and cross-geographic-region bandwidths are often bound to cloud connections for communications on the cloud.

Table 2-1 Global connection bandwidth types

Bandwidth Type	Instance Type	Description	Scenario
Multi-city	Global EIPs	Select this type of bandwidth if you need communications 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)

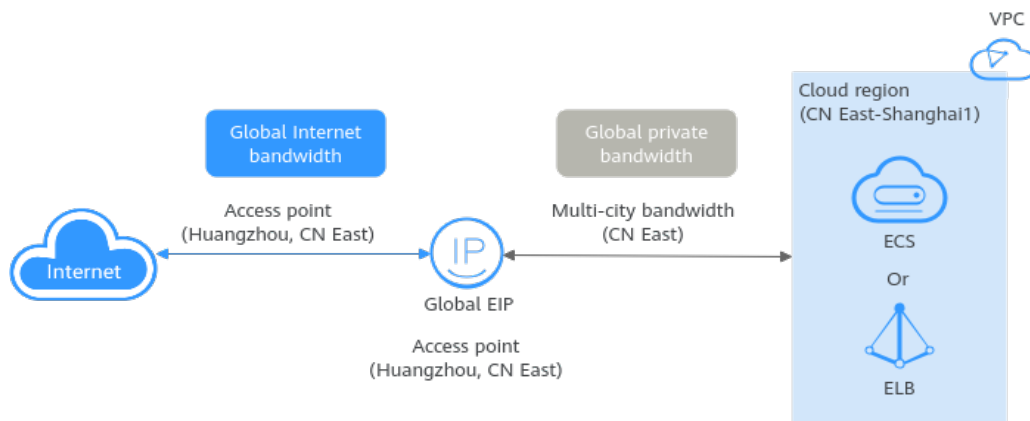
Bandwidth Type	Instance Type	Description	Scenario
Geographic-region	Global EIPs Cloud connections	Select this type of bandwidth if you need communications within a geographic region. Geographic regions include the Chinese mainland, Asia Pacific, and Southern Africa. For example, CN East-Shanghai1 and CN South-Guangzhou are regions in the Chinese mainland. For details about the relationship between geographic regions and Huawei Cloud regions, see .	<ul style="list-style-type: none"> 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/Cross-geographic-region Bandwidth Application Scenario (Central Network)
Cross-geographic-region	Global EIPs Cloud connections	Select this type of bandwidth if you need communications across geographic regions. Geographic regions include the Chinese mainland, Asia Pacific, and Southern Africa. For example, CN East-Shanghai1 and CN-Hong Kong are from different geographic regions. For details about the relationship between geographic regions and cloud regions, see .	<ul style="list-style-type: none"> 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/Cross-geographic-region Bandwidth Application Scenario (Central Network)

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 2-1 Multi-city bandwidth application scenario (global EIP)

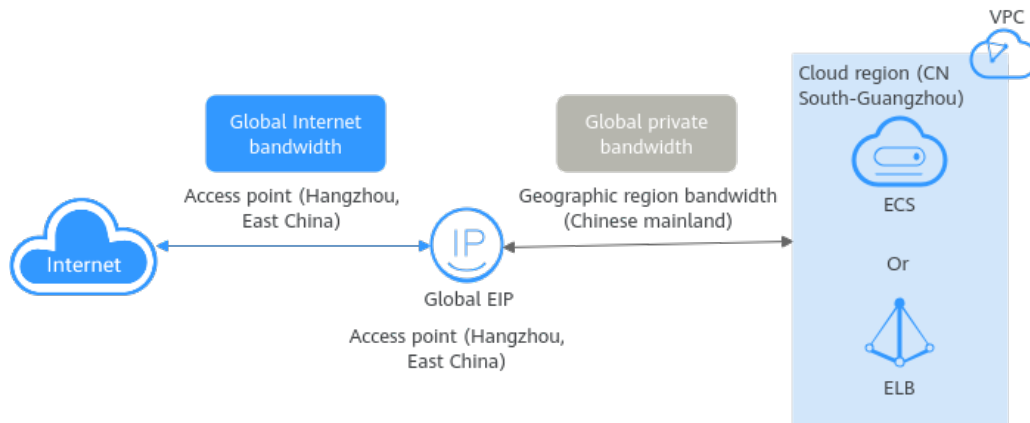


Geographic-region Bandwidth Application Scenario (Global EIP)

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



Cross-geographic-region Bandwidth Application Scenario (Global EIP)

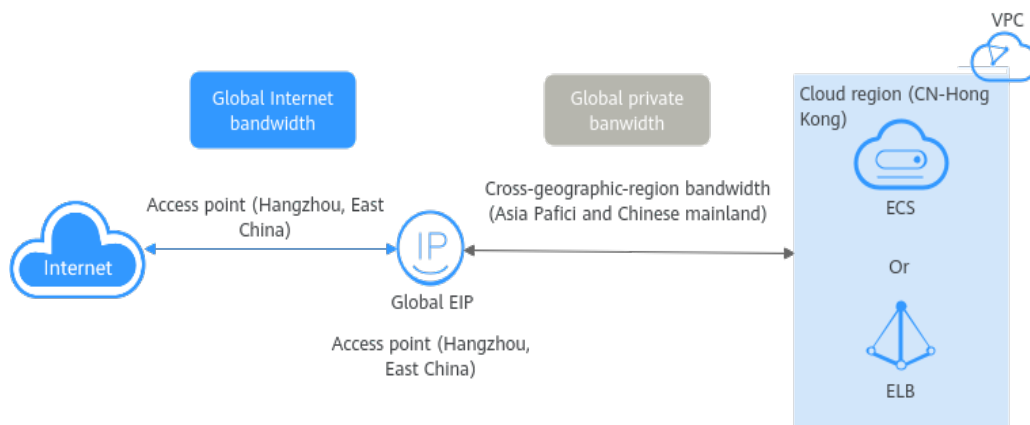
In this example, a global EIP is bound to an ECS.

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 2-3 Cross-geographic-region bandwidth application scenario (global EIP)

Geographic-region/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 communications 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 communications 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 communications 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

2.2 Buying a Global Connection Bandwidth

Scenarios

This section describes how to buy a global connection bandwidth for communication on a private network.

Procedure

1. Log in to the management console.
2. On the console homepage, choose > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.
4. In the cloud connection list, click the name of the cloud connection.
5. On the basic information page, click the **Global Connection Bandwidths** tab.
6. Click **Buy Global Connection Bandwidth**.
7. Configure the parameters based on [Table 2-2](#).

Table 2-2 Parameters required for buying a global connection bandwidth

Parameter	Description
Billing Mode	Mandatory Pay-per-use: a postpaid subscription. You are charged based on the usage duration of the global connection bandwidth. Your global connection bandwidth is billed by second, and you are charged for a minimum of 60 seconds each time. If the usage is less than an hour, you are charged based on the actual duration, accurate to seconds.
Bandwidth Type	Mandatory 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 after your purchase. Learn about the application scenarios of different types of bandwidths. You can decide whether to use a geographic-region bandwidth or cross-geographic-region bandwidth based on service scenarios.

Parameter	Description
Billed By	Mandatory The price of a global connection bandwidth varies by its size. <ul style="list-style-type: none">• 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	Mandatory Select the size of the bandwidth in Mbit/s.
Bandwidth Name	Mandatory Enter the name of the bandwidth. The name: <ul style="list-style-type: none">• Must contain 1 to 64 characters.• Can contain letters, digits, underscores (_), hyphens (-), and periods (.).

8. Click **Next**.
9. Confirm the configurations and click **Submit**.
The global connection bandwidth list page is displayed.
10. In the global connection bandwidth list, view the status of the bandwidth.
If the bandwidth status is **Normal**, the purchase is successful.

2.3 Binding a Global Connection Bandwidth

Scenarios

You can bind a global connection bandwidth to a global EIP or a cloud connection.

Constraints

- Instances that a global connection bandwidth is to be bound to must be from the same region as the bandwidth.
- A global connection bandwidth can only be bound to instances of the same type. If you want to add other type of instances to a global connection bandwidth with instances bound, you need to remove the bound instances first.
 - Global EIPs: You can add or remove global EIPs in batches.
 - Cloud connections: You can bind one global connection bandwidth to or unbind it from one cloud connection at a time.
- If use a global connection bandwidth on a central network, you need to configure cross-site connections by performing the following operations:
 - [Creating a Central Network](#)

- [Managing Policies](#)
- [Managing Attachments](#)
- Global connection bandwidths of different types can be used with different instances. For details, see the following table.

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

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

Using a Global Connection Bandwidth on a Central Network

1. Log in to the management console.
2. On the console homepage, choose > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Central Networks**.
4. In the central network list, click the name of the target central network.
5. Switch to the **Cross-Site Connection Bandwidths** tab.
6. Locate the cross-site connection, and click **Assign now** in the **Global Connection Bandwidth** column.
7. On the **Assign Cross-Site Connection Bandwidth** page, select the global connection bandwidth.
8. Specify the bandwidth and click **OK**.

Binding Global EIPs to a Global Connection Bandwidth

1. Log in to the management console.
2. On the console homepage, choose > **Cloud Connect**.
3. In the navigation pane on the left, choose **Intra-Cloud > Global Connection Bandwidths**.
4. Locate the global connection bandwidth and click **Add** in the **Operation** column.
5. In the **Add** dialog box, set **Instance Type** to **Global EIP**.
For a multi-city global connection bandwidth, select the two regions where the bandwidth will be used.
6. Search for global EIPs using keywords.
7. Select one or more global EIPs and click **OK**.

2.4 Unbinding a Global Connection Bandwidth

Scenarios

You can unbind a global connection bandwidth from a global EIP or a cloud connection.

Constraints

- Before a global connection bandwidth is unbound from a resource, ensure that the resource is not used for running workloads or establishing connectivity. If the resource is used, workloads will be unavailable or the network will be interrupted.
- A global connection bandwidth can only be bound to instances of the same type. If you want to add other type of instances to a global connection bandwidth with instances bound, you need to remove the bound instances first by referring to [Binding a Global Connection Bandwidth](#).
- If inter-region bandwidths have been assigned from a global connection bandwidth, the global private bandwidth cannot be unbound from the cloud connection. You need to delete the inter-region bandwidths first.

Deleting a Cross-Site Connection Bandwidth

1. Log in to the management console.
2. On the console homepage, choose > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**.
4. Switch to the **Cross-Site Connection Bandwidths** tab, locate the cross-site connection, and click **Delete Bandwidth** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

Unbinding a Global EIP from a Global Connection Bandwidth

1. Log in to the management console.
2. On the console homepage, choose > **Cloud Connect**.
3. In the navigation pane on the left, choose **Intra-Cloud** > **Global Connection Bandwidths**.
4. Locate the global connection bandwidth.
 - 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:
 - i. On the details page of the bandwidth, click **Associated Instances**.
 - ii. Select the instances.
 - iii. Click **Remove** above the instance list.
 - iv. In the displayed dialog box, click **OK**.

2.5 Modifying a Global Connection Bandwidth

Scenarios

You can increase or decrease a global connection bandwidth. The new bandwidth takes effect immediately.

Procedure

1. Log in to the management console.
2. On the console homepage, choose > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Cloud Connections**.
4. In the cloud connection list, click the name of the cloud connection.
5. On the basic information page, click the **Global Connection Bandwidths** tab.
6. Locate the target bandwidth and choose **More > Modify Bandwidth** in the **Operation** column.
7. Modify the bandwidth name and size as prompted, and click **Next**.
8. Confirm the information and click **Submit**.

2.6 Deleting a Global Connection Bandwidth


Scenarios

If your pay-per-use global connection bandwidth is no longer required, delete the bandwidth in a timely manner to avoid unnecessary fees.

Constraints

A global connection bandwidth with an instance bound cannot be deleted. To delete such a bandwidth, unbind its instance first. For details, see [Unbinding a Global Connection Bandwidth](#).

Procedure

1. Log in to the management console.
2. On the console homepage, choose > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect > Cloud Connections**.
4. In the cloud connection list, click the name of the cloud connection.
5. On the basic information page, click the **Global Connection Bandwidths** tab.
6. Locate the bandwidth you want to delete and click its name to view its settings.
7. In the upper left corner of the page, click  .

- In the global connection bandwidth list, search for the bandwidth.
- Choose **More > Delete** in the **Operation** column.
- Click **OK**.

2.7 Auditing

2.7.1 Key Operations Recorded by CTS

Scenarios

With Cloud Trace Service (CTS), you can record operations associated with global connection bandwidths for later query, audit, and backtracking.

Prerequisites

You have enabled CTS.

Key Operations Recorded by CTS

Table 2-4 Global connection bandwidth operations recorded by CTS

Operation	Resource	Trace
Creating a global connection bandwidth	globalConnectionBandwidth	createGcBandwidth
Updating a global connection bandwidth	globalConnectionBandwidth	updateGcBandwidth
Deleting a global connection bandwidth	globalConnectionBandwidth	deleteGcBandwidth
Binding a global connection bandwidth to an instance	globalConnectionBandwidth	bindGcBandwidth
Unbinding a global connection bandwidth from an instance	globalConnectionBandwidth	unbindGcBandwidth



2.7.2 Viewing Traces

Scenarios

After CTS is enabled, CTS starts recording operations on cloud resources. The CTS management console stores the last seven days of operation records.

This section describes how to query or export the last seven days of operation records on the management console.

Procedure

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 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.
If you select **Trace name** for **Search By**, select a trace name.
If you select **Resource ID** for **Search By**, select or enter a resource ID.
If you select **Resource name** for **Search By**, select or enter a resource name.
 - **Operator**: Select a specific operator (a user other than an account).
 - **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 arrow on the left of the required trace to expand its details.
7. Locate the required trace and click **View Trace** in the **Operation** column.
A dialog box is displayed, showing the trace content.

3 Permissions Management

3.1 Creating a User and Granting Permissions

Use [IAM](#) to implement fine-grained permissions control for your Cloud Connect resources. With IAM, you can:

- Create IAM users for employees based on your enterprise's organizational structure. Each IAM user will have their own security credentials for accessing Cloud Connect resources.
- Grant only the permissions required for users to perform a specific task.
- Delegate a Huawei Cloud account to manage your Cloud Connect resources or a cloud service to access your Cloud Connect resources.

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

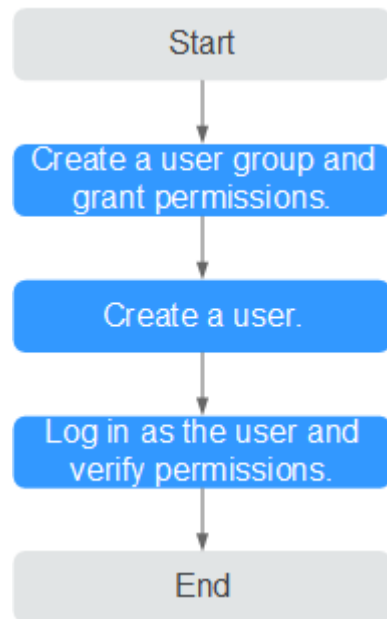
[Figure 3-1](#) shows the process of granting permissions.

Prerequisites

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

Process Flow

Figure 3-1 Process of granting Cloud Connect permissions



1. **Create a user group and assign permissions.**
Create a user group on the IAM console and assign the **Cross Connect Administrator** policy to the group.
2. **Create an IAM user and add it to the user group.**
Create a user on the IAM console and add the user to the group created in **1**.
3. **Log in** and verify permissions.
Log in to the Cloud Connect console using the user's credentials and verify that the user has all permissions for Cloud Connect.
 - In the service list, choose **Networking > Cloud Connect**. Click **Create Cloud Connection** in the upper right corner. If the cloud connection can be created, 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.

3.2 Custom Policy

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

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

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

For details, see [Creating a Custom Policy](#). The following are examples custom policies created for Cloud Connect.

Example Custom Policies

- Example 1: Allowing users to delete cloud connections

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

- Example 2: Denying bandwidth package deletion

A policy with only "Deny" permissions must be used in conjunction with other policies to take effect. If the policies assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

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 topics. Create a custom policy for denying topic deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on Cloud Connect except deleting topics. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cc:bandwidthPackages: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": [
        "cc:bandwidthPackages:create",
        "cc:cloudConnections:create",
        "cc:bandwidthPackages:delete",
        "cc:cloudConnections:delete"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "eps:enterpriseProjects:enable",
        "eps:enterpriseProjects:update",
        "eps:enterpriseProjects:create",
        "eps:enterpriseProjects:delete"
      ]
    }
  ]
}
```


4 Quotas

What Is Quota?

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

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

How Do I View My Quotas?

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