Cloud Connect

# User Guide

**Issue** 15

**Date** 2024-03-15

HUAWEI TECHNOLOGIES CO., LTD.

## Trademarks and Permissions

## Notice

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

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

# Security Declaration

## Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

# Contents

# 1 Cloud Connection Operation Guide

## 1.1 Cloud Connections

### 1.1.1 Managing Cloud Connect Service Disclaimer

#### Scenarios

To provide cross-region network communications, Cloud Connect will obtain and transmit your credential and account ID from the Chinese mainland to the country or region where the network instances you want to connect to are running for identity verification and authentication.

The credential and account ID is required only for providing services for you. If you need to use Cloud Connect for network communications, please read and **agree to the Cloud Connect Service Disclaimer**.

If you do not need Cloud Connect for network communications, you can **reject the disclaimer**.

#### Agreeing to the Disclaimer

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. On the **Cloud Connections** page, click **Accept Disclaimer**.
4. Select **I have read and agree to the Cloud Connect Service Disclaimer**.
5. Click **OK**.

#### Rejecting the Disclaimer

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. On the **Cloud Connections** page, click **Reject Disclaimer**.

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

## 1.1.2 Creating a Cloud Connection

### Scenarios

You need a cloud connection to connect the VPCs that you want to access.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. On the **Cloud Connections** page, click **Create Cloud Connection**.
4. Configure the parameters.

**Table 1-1** Parameters for creating a cloud connection

| Parameter | Description | Example Value |
|---|---|---|
| Name | Specifies the cloud connection name. | CC-test |
| Enterprise Project | Specifies the enterprise project that cloud connection belongs to.<br>An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is **default**.<br>For details about creating and managing enterprise projects, see the **Enterprise Management User Guide**. | default |
| Scenario | Specifies whether the cloud connection is used to connect VPCs or enterprise routers.<br>If you select **VPC** here, only VPCs or virtual gateways can use this cloud connection. | VPC |
| Tag | Identifies the cloud connection. A tag consists of a key and a value. You can add 10 tags to a cloud connection.<br>**NOTE**<br>If you have configured tag policies for Cloud Connect, add tags to cloud connections based on the tag policies. If you add a tag that does not comply with the tag policies, cloud connections may fail to be created. Contact your administrator to learn more about tag policies. | • Key: cc_key1<br>• Value: cc-01 |

| Parameter | Description | Example Value |
|---|---|---|
| Description | (Optional) Provides supplementary information about the cloud connection.<br>The description can contain a maximum of 255 characters and cannot contain angle brackets (<>). | - |

5. Click **OK**.

# 1.1.3 Viewing a Cloud Connection

## Scenarios

You can view details about a cloud connection you created.

## Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name to view the details.

# 1.1.4 Modifying a Cloud Connection

## Modifying Cloud Connection Details

### Scenarios

You can modify the name and description of a cloud connection.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection, click **Modify** in the **Operation** column, and change the name and description.
4. Click **OK**.

## Modifying the Bandwidth

### Scenarios

You can modify the bandwidth of the bandwidth package that you have bound to a cloud connection.

### Procedure

1. Log in to the management console.

2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Bound Bandwidth Packages**.
4. Locate the bandwidth package and click **Modify Bandwidth** in the **Operation** column.
5. Modify the bandwidth and click **OK**.
6. Confirm the new bandwidth and click **Pay Now**.

## 1.1.5 Deleting a Cloud Connection

### Scenarios

You can delete a cloud connection you no longer need.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click **Delete** in the **Operation** column.

   A cloud connection used by network instances cannot be deleted. To delete the cloud connection, remove the network instances from it first.
4. Click **Yes**.

## 1.1.6 Unbinding a Bandwidth Package

### Scenarios

You can unbind a bandwidth package that you do not require from the cloud connection.

### Prerequisites

You have deleted the inter-region bandwidths that you have assigned based on this bandwidth package.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Bound Bandwidth Packages**.
4. Locate the bandwidth package and click **Unbind** in the **Operation** column.
5. Click **Yes**.

# 1.1.7 Managing Cloud Connection Tags

## Scenarios

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

A tag is the identifier of a cloud connection and consists of a key and a value. You can add 10 tags to a cloud connection.

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

**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 Tags**.

## Adding a Tag

Add a tag to an existing cloud connection.

1. Log in to the management console.
2. On the console homepage, click 📍 in the upper left corner and select the desired region and project.
3. Hover on ☰ to display **Service List** and choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.
5. Locate the connection and click its name.
6. Click **Tags**.
7. Click **Add Tag**.
8. In the displayed dialog box, enter a key and a value.

   **Table 1-2** describes the tag key and value requirements.

**Table 1-2** Tag key and value requirements

| Parameter | Requirements |
|---|---|
| Key | ● Cannot be left blank.<br>● Must be unique for each resource.<br>● Can contain a maximum of 36 characters.<br>● Can contain only letters, digits, hyphens, underscores, and Unicode characters from \u4e00 to \u9fff. |

| Parameter | Requirements |
|---|---|
| Value | ● Can be left blank.<br>● Can contain a maximum of 43 characters.<br>● Can contain only letters, digits, period, hyphens, underscores, and Unicode characters from \u4e00 to \u9fff. |

9. Click **OK**.

## Editing a Tag

Modify the value of a tag added to a cloud connection.

1. Log in to the management console.
2. On the console homepage, click 📍 in the upper left corner and select the desired region and project.
3. Hover on ≡ to display **Service List** and choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.
5. Locate the connection and click its name to switch to the details page.
6. Click **Tags**.
7. In the tag list, locate the tag you want to modify and click **Edit** in the **Operation** column.
8. Enter a new value.
9. Click **OK**.

## Deleting a Tag

Delete a tag from a cloud connection.

⚠ CAUTION

Deleted tags cannot be recovered.

1. Log in to the management console.
2. On the console homepage, click 📍 in the upper left corner and select the desired region and project.
3. Hover on ≡ to display **Service List** and choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.

5. Locate the connection and click its name to switch to the details page.
6. Click **Tags**.
7. In the tag list, locate the tag you want to delete and click **Delete** in the **Operation** column.
8. Click **Yes**.

# 1.2 Network Instances

## 1.2.1 Loading a Network Instance

### Scenarios

Load the VPCs and virtual gateways to the cloud connection based on your network plan.

### Constraints

To provide cross-region network communications, Cloud Connect will obtain and transmit your credential and account ID from the Chinese mainland to the country or region where the network instances you want to connect to are running for identity verification and authentication.

The credential and account ID is required only for providing services for you. If you need to use Cloud Connect for network communications, please read and **agree to the Cloud Connect Service Disclaimer**.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, click the name of the cloud connection.
4. Click **Network Instances**.
5. Click **Load Network Instance**.
6. In the **Load Network Instance** dialog box, specify the account.
   - If the network instance to be loaded is from your own account that is used to create the cloud connection, select **Current account**.

     Configure parameters based on **Table 1-3** and then click **OK**.
   - If the network instance is from the other user, select **Peer account**.

     Configure parameters based on **Table 1-4** and then click **OK**.

**Table 1-3** Parameters for loading network instances in the current account

| Parameter | Description |
|---|---|
| Account | Specifies whether network instances will be loaded across accounts.<br>Set it to **Current account**. |
| Region | Specifies the region where the VPC you want to connect is located. |
| Instance Type | Specifies the type of the network instance. Two options are available, **VPC** and **Virtual gateway**. |
| VPC | Specifies the VPC you want to load to the cloud connection.<br>This parameter is mandatory if you have set **Instance Type** to **VPC**. |
| VPC CIDR Block | Specifies the subnets of the VPC you want to load and the custom CIDR blocks.<br>If you have set **Instance Type** to **VPC**, configure the following two parameters:<br>● **Subnet**: Select one or all subnets of the VPC.<br>● **Other CIDR Block** |
| Virtual Gateway | Specifies the virtual gateway you want to load to the cloud connection. This parameter is mandatory if you have set **Instance Type** to **Virtual gateway**. |
| Virtual Gateway CIDR Block | Specifies the VPC and the network segment route of the remote user site in the virtual gateway you want to load to the cloud connection. If you have set **Instance Type** to **Virtual gateway**, you need to configure the following two parameters:<br>● Local Subnet<br>● **Remote Subnet** |
| Remarks | Provides supplementary information about the network instance. |

**Table 1-4** Parameters for loading network instances across accounts

| Parameter | Description |
|---|---|
| Account | Specifies whether network instances will be loaded across accounts.<br>Select **Peer account**. |
| Peer Account ID | Specifies the ID of this other user's account. |
| Region | Specifies the region where the VPC you want to connect is located. |
| Peer Project ID | Specifies the project ID of the VPC in the other user's account. |
| Instance Type | Specifies the type of the instance you want to load to the cloud connection. |
| Peer VPC | Specifies the ID of the VPC you want to load. |
| VPC CIDR Block | Specifies the subnets of the VPC you want to load and the custom CIDR blocks. |
| Remarks | Provides supplementary information about the network instance. |

NOTE

- A network instance can be loaded to only one cloud connection.
- If a VPC is loaded, the associated virtual gateway cannot be loaded.

7. Configure other parameters and click **OK**.
8. Click **Load Another Instance** if you want to continue loading network instances. Then click the **Network Instances** tab to view the network instances you loaded.

## 1.2.2 Viewing a Network Instance

### Scenarios

You can view details about a network instance that has been loaded to a cloud connection.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.

3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Network Instances**.
4. Click the name of the loaded network instance. In the lower right area of the page, view its details.

# 1.2.3 Modifying a Network Instance

## Modifying a VPC

### Scenarios

You can modify the subnets and custom CIDR blocks of a loaded VPC.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Network Instances**.
4. Locate the VPC and click its name.
5. In the lower right area of the page, click **Modify VPC CIDR Block**.
6. Modify the subnets and custom CIDR blocks.
7. Click **OK**.

## Modifying a Virtual Gateway

### Scenarios

You can modify local and remote subnets of a loaded virtual gateway.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Network Instances**.
4. Locate the virtual gateway and click its name.
5. In the lower right area of the page, click **Modify Virtual Gateway CIDR Block**.
6. Modify the local and remote subnets.
7. Click **OK**.

# 1.2.4 Removing a Network Instance

## Removing a VPC

### Scenarios

You can remove a VPC that does not need to communicate with other VPCs.

**Procedure**

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Network Instances**.
4. Locate the VPC and click its name.
5. In the lower right area of the page, click **Remove**.
6. Click **Yes**.

### Removing a Virtual Gateway

**Scenarios**

If an on-premises data center does not need to communicate with the VPCs, you can delete the loaded virtual gateway.

**Procedure**

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Network Instances**.
4. Locate the virtual gateway and click its name.
5. In the lower right area of the page, click **Remove**.
6. Click **Yes**.

# 1.3 Bandwidth Packages

## 1.3.1 Buying a Bandwidth Package

### Scenarios

To enable network communications between regions in the same geographic region or across geographic regions, you need to purchase a bandwidth package and bind it to a cloud connection.

Bandwidth packages are used when network instances to be loaded to a cloud connection are VPCs.

NOTE

To allow you to test network connectivity between regions, the system allocates 10 kbit/s by default. To test network connectivity, you can ping an ECS in one VPC from an ECS in the other VPC.

No bandwidth packages are required if two VPCs are in the same region because they can communicate with each other by default after they are loaded to the same cloud connection.

## Constraints

To provide cross-region network communications, Cloud Connect will obtain and transmit your credential and account ID from the Chinese mainland to the country or region where the network instances you want to connect to are running for identity verification and authentication.

The credential and account ID is required only for providing services for you. If you need to use Cloud Connect for network communications, please read and **agree to the Cloud Connect Service Disclaimer**.

## Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. Click **Buy Bandwidth Package**.
5. Configure the parameters based on **Table 1-5** and click **Buy Now**.

**Table 1-5** Parameters

| Parameter | Description |
|---|---|
| Billing Mode | Specifies how you want the bandwidth package to be billed. |
| Name | Specifies the bandwidth package name.<br>The name can contain 1 to 64 characters, including digits, letters, underscores (_), hyphens (-), and periods (.). |
| Billed By | Specifies by what you want the bandwidth package to be billed.<br>Only **Bandwidth** is available. |
| Applicability | Specifies whether the bandwidth package is used for communications within a geographic region, between geographic regions, or between specified regions. The following options are available:<br>● **Single geographic region**: Use the bandwidth package between regions in the same geographic region.<br>● **Across geographic regions**: Use the bandwidth package between regions in different geographic regions. |
| Geographic Region | Specifies the geographic region. |

| Parameter | Description |
|---|---|
| Bandwidth | Specifies the bandwidth you require for network communications across regions, in Mbit/s. The sum of all inter-region bandwidths you assign cannot exceed the total bandwidth of the bandwidth package. Assign the bandwidth based on your network plan. |
| Required Duration | Specifies how long you require the bandwidth package for.<br>Auto renewal is supported. |
| Cloud Connection | Specifies the cloud connection you want to bind the bandwidth package to.<br>Two options are available, **Bind now** and **Bind later**. |

6. Confirm the information and click **Pay Now**.
7. Click **Pay**.

   Go back to the bandwidth package list and locate the bandwidth package. If its status changes to **Normal**, you can bind the bandwidth package to a cloud connection.

## 1.3.2 Modifying a Bandwidth Package

### Scenarios

You can modify the bandwidth of a bandwidth package you have purchased. You can increase or decrease the bandwidth.

- If you increase the bandwidth, you need to pay for the increased bandwidth. The new bandwidth will take effect after you make the payment.
- If you decrease the bandwidth, the system will refund the overpayment to your account. The new bandwidth takes effect immediately.

The following procedure use bandwidth increase as an example.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. Locate the bandwidth package and click **Modify Bandwidth** in the **Operation** column.
5. Select **Increase bandwidth** and click **Continue**.
6. Specify the new bandwidth and click **OK**.

7. Confirm the configuration and click **Submit**.
8. Select a payment method and click **Pay**.

## 1.3.3 Binding a Bandwidth Package to a Cloud Connection

### Scenarios

Bind a purchased bandwidth package to a cloud connection.

NOTE

- One cloud connection can only have one bandwidth package regardless of if the cloud connection is used for communications within a geographic region or between geographic regions. For example, cloud connection A can only have one bandwidth package between the Chinese mainland and Asia Pacific.
- A bandwidth package can only be bound to one cloud connection.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. Locate the bandwidth package and click **Bind** in the **Operation** column.
5. Select the cloud connection you want to bind.
6. Click **OK**.

## 1.3.4 Unbinding a Bandwidth Package from a Cloud Connection

### Scenarios

If you do not need a bandwidth package any longer, you can unbind it from the cloud connection.

### Prerequisites

You have deleted the inter-region bandwidths that you have assigned based on this bandwidth package.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. Locate the bandwidth package and click **Unbind** in the **Operation** column.

5. Click **Yes**.

## 1.3.5 Unsubscribing from a Yearly/Monthly Bandwidth Package

### Scenarios

You can unsubscribe from a yearly/monthly bandwidth package if you do not need it any longer. After you unsubscribe from the package, you will stop being charged for it.

### Prerequisites

You have unbound the bandwidth package from the cloud connection by referring to **Unbinding a Bandwidth Package from a Cloud Connection**.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. Locate the bandwidth package and click **Unsubscribe** in the **Operation** column.
5. Select the bandwidth package, reason for unsubscription, and **I understand a handling fee will be charged for this unsubscription**.
6. Click **Confirm**.

## 1.3.6 Managing Bandwidth Package Tags

### Scenarios

After a bandwidth package is purchased, you can view its tags or add, edit or delete a tag.

A tag is the identifier of a bandwidth package and consists of a key and a value. You can add a maximum of 10 tags to a bandwidth package.

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 Tags**.

### Adding a Tag

Add a tag to an existing bandwidth package.

1. Log in to the management console.

2. On the console homepage, click 📍 in the upper left corner and select the desired region and project.
3. Hover on ☰ to display **Service List** and choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
5. Locate the bandwidth package and click its name to switch to the details page.
6. Click **Tags**.
7. Click **Add Tag**.
8. In the displayed dialog box, enter a key and a value.

   Table 1-6 describes the tag key and value requirements.

**Table 1-6** Tag key and value requirements

| Parameter | Requirements |
|---|---|
| Key | ● Cannot be left blank.<br>● Must be unique for each resource.<br>● Can contain a maximum of 36 characters.<br>● Can contain only letters, digits, hyphens, underscores, and Unicode characters from \u4e00 to \u9fff. |
| Value | ● Can be left blank.<br>● Can contain a maximum of 43 characters.<br>● Can contain only letters, digits, period, hyphens, underscores, and Unicode characters from \u4e00 to \u9fff. |

9. Click **OK**.

## Editing a Tag

Modify the value of a tag added to a bandwidth package.

1. Log in to the management console.
2. On the console homepage, click 📍 in the upper left corner and select the desired region and project.
3. Hover on ☰ to display **Service List** and choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
5. Locate the bandwidth package and click its name to switch to the details page.
6. Click **Tags**.

7. In the tag list, locate the tag you want to modify and click **Edit** in the **Operation** column.
8. Enter a new value.
9. Click **OK**.

### Deleting a Tag

Delete a tag from a bandwidth package.

⚠ **CAUTION**

Deleted tags cannot be recovered.

1. Log in to the management console.
2. On the console homepage, click 📍 in the upper left corner and select the desired region and project.
3. Hover on ☰ to display **Service List** and choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
5. Locate the bandwidth package and click its name to switch to the details page.
6. Click **Tags**.
7. In the tag list, locate the tag you want to delete and click **Delete** in the **Operation** column.
8. Click **Yes**.

# 1.4 Inter-Region Bandwidths

## 1.4.1 Assigning an Inter-Region Bandwidth

### Scenarios

If network instances are in the same region, they can communicate with each other by default after they are loaded to one cloud connection. If network instances are in different regions, you need to assign inter-region bandwidths to ensure normal network communications between the instances. By default, the system allocates 10 kbit/s of bandwidth for testing network connectivity across regions.

### Constraints

To provide cross-region network communications, Cloud Connect will obtain and transmit your credential and account ID from the Chinese mainland to the country or region where the network instances you want to connect to are running for identity verification and authentication.

The credential and account ID is required only for providing services for you. If you need to use Cloud Connect for network communications, please read and **agree to the Cloud Connect Service Disclaimer**.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, click the name of the cloud connection.
4. Click **Inter-Region Bandwidths**.
5. Click **Assign Inter-Region Bandwidth**.
6. Select the regions and the bandwidth package and enter the bandwidth.
7. Click **OK**.

   Now the network instances in the two regions can communicate with each other.

## 1.4.2 Viewing Inter-Region Bandwidths

### Scenarios

You can view details about inter-region bandwidths you have configured.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. Locate the cloud connection and click its name.
4. Click **Inter-Region Bandwidths** and view the inter-region bandwidths that you have assigned for the cloud connection.

## 1.4.3 Modifying an Inter-Region Bandwidth

### Scenarios

You can modify an inter-region bandwidth if it no longer meets your requirements.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Inter-Region Bandwidths**.
4. Locate the inter-region bandwidth and click **Modify** in the **Operation** column.
5. Modify the bandwidth and click **OK**.

## 1.4.4 Deleting an Inter-Region Bandwidth

### Scenarios

If you do not require network communications between two regions, you can delete the inter-region bandwidth assigned between them.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Inter-Region Bandwidths**.
4. Locate the inter-region bandwidth and click **Delete** in the **Operation** column.
5. Click **Yes**.

## 1.4.5 Viewing the Monitoring Data of an Inter-Region Bandwidth

### Scenarios

You can view the real-time monitoring data of an inter-region bandwidth to evaluate the network quality.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name. On the displayed page, click **Inter-Region Bandwidths**.
4. Locate the inter-region bandwidth and click the icon in the **Monitoring** column to view the metrics of the corresponding period, for example, metrics of the last hour, 3 hours, or 12 hours.

# 1.5 Routes

## 1.5.1 Adding a Custom CIDR Block

### Scenarios

If you use Cloud Connect together with another cloud service, such as NAT Gateway, Direct Connect, or VPN, you need to add a custom CIDR block to the cloud connection, so that the VPCs you load to the cloud connection can communicate with the service.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the cloud connection and click its name.
4. Click **Network Instances**.
5. Locate the network instance and click its name.
6. In the lower right area, click **Modify VPC CIDR Block**.
7. Click **Advanced Settings**.
8. Enter the CIDR block in the **Other CIDR Block** text box and click **Add**.
9. Click **OK**.

## 1.5.2 Viewing Route Information

### Scenarios

You can view the routes of a cloud connection.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the cloud connection list, locate the click the cloud connection and click its name. On the displayed page, click **Route Information**.
4. From the drop-down list, select the region.
5. View the routes in the list.

# 1.6 Cross-Account Authorization

## 1.6.1 Allowing Other Users to Load Your VPCs

### Scenarios

You can grant other users the permissions to load your VPCs to their cloud connections.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane, choose **Cloud Connect** > **Cross-Account Authorization**.
4. Click **Network Instances Authorized by Me**.

5. Click **Authorize Network Instance**.

   Select a region and a VPC, and enter the peer account ID and peer cloud connection ID.

6. Click **OK**.

## 1.6.2 Viewing Authorization

You can view the VPCs that you have allowed other users to load to their cloud connections and the VPCs that you are allowed to load to your cloud connection.

### Viewing the VPCs that Can Be Loaded to Other Users' Cloud Connections

**Scenarios**

You can view the VPCs that you have allowed other users to load to their cloud connections

**Procedure**

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane, choose **Cloud Connect** > **Cross-Account Authorization**.
4. Click **Network Instances Authorized by Me**.
5. In the search box in the upper right corner of the list, search the VPCs by name or ID.
6. In the displayed VPC list, view the VPCs.

### Viewing the VPCs that Other Users Allow You to Load

**Scenarios**

You can view the VPCs that other users have allowed you to load to their cloud connections.

**Procedure**

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane, choose **Cloud Connect** > **Cross-Account Authorization**.
4. Click **Network Instances Authorized to Me**.
5. In the search box in the upper right corner of the list, search the VPCs by peer account ID, VPC ID, or cloud connection ID.
6. In the displayed VPC list, view the VPCs.

## 1.6.3 Canceling Authorization

### Scenarios

You can cancel the authorization that allows other users to load your VPCs to their cloud connections.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane, choose **Cloud Connect** > **Cross-Account Authorization**.
4. Click **Network Instances Authorized by Me**.
5. In the search box in the upper right corner of the list, search the VPCs by name or ID.
6. Click **Cancel Authorization** in the **Operation** column.
7. Click **Yes**.

NOTE

After the authorization is canceled, other users can still use your VPCs that have been loaded to their cloud connections until these VPCs are removed from the cloud connection.

## 1.6.4 Loading a VPC in Another Account

### Scenarios

You can load the VPCs in other accounts to your cloud connection so that your VPCs can communicate with these VPCs.

### Prerequisites

You must have the permissions of **Tenant Guest**, **VPC Administrator**, and **Cross Connect Administrator** for the region where the other user's VPCs reside.

For details, see Permission Management.

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane, choose **Cloud Connect** > **Cross-Account Authorization**.
4. Click **Network Instances Authorized to Me**.
5. In the search box in the upper right corner of the list, search the VPCs by peer account ID, VPC ID, or cloud connection ID.
6. Select the VPC and click **Load to Cloud Connection** in the **Operation** column.

7. Configure the parameters.

**Table 1-7** Parameters for loading a VPC to a cloud connection

| Parameter | Description |
|---|---|
| Cloud Connection ID | Specifies the ID of the cloud connection to which the VPC you want to load. |
| Region | Specifies the region where the VPC you want to connect is located. |
| Instance Type | Specifies the type of the network instance you can load. Only VPCs can be loaded. |
| Peer VPC | Specifies the ID of the VPC to be loaded. |
| VPC CIDR Block | Specifies the subnets of the VPC you want to load and the custom CIDR blocks. |

8. Click **OK**.

   In the cloud connection list, locate the cloud connection and click its name. Under **Network Instances**, view the loaded VPC.

# 1.7 Cross-Border Permits

## 1.7.1 Applying for a Cross-Border Permit

### Scenarios

In accordance with the laws and administrative regulations of the Ministry of Industry and Information Technology (MIIT) of the People's Republic of China, only three major operators in the Chinese mainland are allowed for cross-border network communications, and a cross-border permit is required if you carry out business activities outside the Chinese mainland.

You need to apply for a cross-border permit only when a VPC to be connected is outside the Chinese mainland and other VPCs are inside the Chinese mainland.

### Procedure

1. Log in to the management console.
2. Hover on ☰ to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. On the displayed page, click **apply now**.

   The **Cross-Border Service Application System** page is displayed.
5. On the application page, set related parameters and upload related materials.

**Table 1-8** Online cross-border permit application

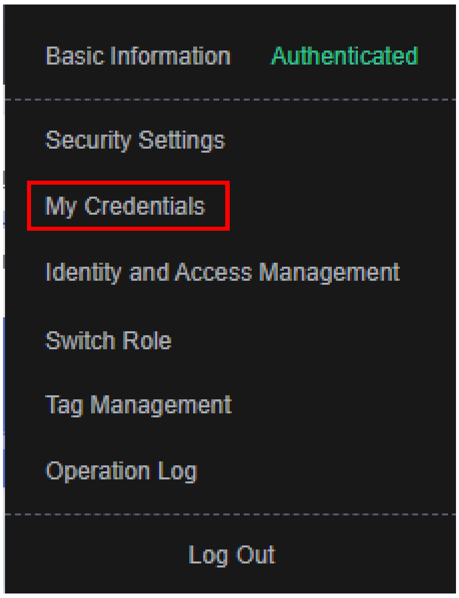
| Parameter |
|---|
| Applicant Name |
| Huawei Cloud UID |
| Type of Product |
| Bandwidth (M) |
| Start Date |
| Termination Date |
| Customer Type |
| Country of the Customer |
| Contact Name |
| Contact Number |
| Type of ID |
| ID Number |
| Scope of Business |
| Number of Employees |
| Per Capita Bandwidth |
| Branch Location Country |

NOTE

HUAWEI ID is your account ID. You can take the following steps to obtain your account ID.

1. Log in to the management console.
2. Click the username and select **My Credentials** from the drop-down list.

**Figure 1-1** My credentials



3. On the **API Credentials** page, view the **Account ID**.

**Figure 1-2** Obtaining an account ID

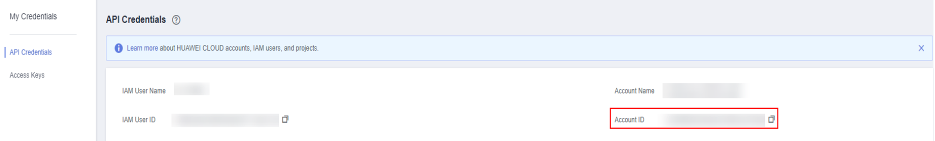


**Table 1-9** Required materials

| Material | Signature | Seal | Description |
|---|---|---|---|
| A scanned copy of your company's business license | - | √ | See the template Huawei Cloud provides for the position of the seal. |
| A scanned copy of *Huawei Cloud Cross-Border Circuit Service Agreement* | √ | √ | ● Sign the material on the signature block.<br>● Stamp the seal over the signature. |

| Material | Signature | Seal | Description |
|---|---|---|---|
| A scanned copy of *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service* | √ | √ | ● Sign the material on the signature block.<br>● Stamp the seal over the signature.<br>● Specify the bandwidth you estimated and your company name. |

6. Click **Submit**.

## 1.7.2 Querying the Application Progress

### Scenarios

You can query the progress of your cross-border permit application.

### Procedure

1. Log in to the management console.
2. Hover on ☰ to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. On the displayed page, click **you can view the approval progress** in the upper part of the page.

   Alternatively, on the application page, click **Application Progress Enquiry** in the upper right corner.
5. On the **Self-inquiry System** page, enter the **Huawei Cloud ID** and **Contact Number** as prompted, and click **Query**.

# 1.8 Monitoring

## 1.8.1 Overview

Monitoring is key to ensuring the performance, reliability, and availability of a cloud service. Monitoring provides you with data on your Cloud Connect resource usage. You can use Cloud Eye to track the status of your Cloud Connect resources. Cloud Eye automatically monitors resources in real time and enables you to manage alarms and notifications, so that you can keep track of performance of Cloud Connect.

For more information, see the following:

- Monitoring Metrics
- Setting an Alarm Rule
- Viewing Metrics

## 1.8.2 Supported Metrics

### Description

The table describes monitored metrics reported by Cloud Connect to Cloud Eye as well as their namespaces and dimensions. You can use the management console to query the metrics of the monitored objects and alarms generated for Cloud Connect.

### Namespace

SYS.CC

### Metrics

**Table 1-10** Cloud Connect metrics

| ID | Metric | Description | Value Range | Monitored Object | Monitoring Interval |
|---|---|---|---|---|---|
| network_incoming_bits_rate | Network Incoming Bandwidth | Bit rate for inbound data to a region from another region of a cloud connection<br>Unit: bit/s | ≥ 0 bits/s | Inter-region bandwidth | 5 minutes |
| network_outgoing_bits_rate | Network Outgoing Bandwidth | Bit rate for outbound data from a region to another region of a cloud connection<br>Unit: bit/s | ≥ 0 bits/s | Inter-region bandwidth | 5 minutes |
| network_incoming_bytes | Network Incoming Traffic | Number of bytes for inbound data to a region from another region of a cloud connection<br>Unit: byte | ≥ 0 bytes | Inter-region bandwidth | 5 minutes |

| ID | Metric | Description | Value Range | Monitored Object | Monitoring Interval |
|---|---|---|---|---|---|
| network_outgoing_bytes | Network Outgoing Traffic | Number of bytes for outbound data from a region to another region of a cloud connection<br>Unit: byte | ≥ 0 bytes | Inter-region bandwidth | 5 minutes |
| network_incoming_packets_rate | Network Incoming Packet Rate | Packet rate for inbound data to a region from another region of a cloud connection<br>Unit: Packet/s | ≥ 0 packets/s | Inter-region bandwidth | 5 minutes |
| network_outgoing_packets_rate | Network Outgoing Packet Rate | Packet rate for outbound data from a region to another region of a cloud connection<br>Unit: Packet/s | ≥ 0 packets/s | Inter-region bandwidth | 5 minutes |
| network_incoming_packets | Network Incoming Packets | Number of packets for inbound data to a region from another region of a cloud connection<br>Unit: Packet | ≥ 0 packets | Inter-region bandwidth | 5 minutes |
| network_outgoing_packets | Network Outgoing Packets | Number of packets for outbound data from a region to another region of a cloud connection<br>Unit: Packet | ≥ 0 packets | Inter-region bandwidth | 5 minutes |

| ID | Metric | Description | Value Range | Monitored Object | Monitoring Interval |
|---|---|---|---|---|---|
| network_bandwidth_usage | Network Bandwidth Usage | Utilization of an inter-region bandwidth assigned to a cloud connection<br>Unit: percent | 0-100% | Inter-region bandwidth | 5 minutes |

NOTE

In some regions, the monitoring period can be set to 1 minute. View the actual monitoring period on the console.

## Dimensions

| Key | Value |
|---|---|
| cloud_connect_id | Cloud connection ID |
| bwp_id | Bandwidth package ID |
| region_bandwidth_id | Inter-region bandwidth ID |

# 1.8.3 Setting Alarm Rules

## Scenarios

You can configure alarm rules to customize the monitored objects and notification policies and to learn Cloud Connect resource status at any time.

## Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Management & Governance** > **Cloud Eye**.
3. In the navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
4. On the **Alarm Rule** page, click **Create Alarm Rule** to create an alarm rule. You can also modify an existing alarm rule.
5. After configuring the parameters, click **Create**.

   After the alarm rule is set, the system automatically notifies you when an alarm is triggered.

NOTE

For more information about Cloud Connect alarm rules, see **Cloud Eye User Guide**.

## 1.8.4 Viewing Metrics

1. Log in to the management console.
2. Click in the upper left corner to select a region and a project.
3. Hover on the upper left corner to display **Service List** and choose **Management & Governance** > **Cloud Eye**.
4. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Cloud Connect**.
5. Click **View Metric** in the **Operation** column to view the cloud connection status.

   You can view data of the last one, three, 12, or 24 hours, or last 7 days.

# 1.9 Auditing

## 1.9.1 Key Operations Recorded by CTS

### Scenarios

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

### Prerequisites

You have enabled CTS.

### Key Operations Recorded by CTS

**Table 1-11** Cloud connection operations recorded by CTS

| Operation | Resource | Trace |
|---|---|---|
| Creating a cloud connection | cloudConnection | createCloudConnection |
| Updating a cloud connection | cloudConnection | updateCloudConnection |
| Deleting a cloud connection | cloudConnection | deleteCloudConnection |
| Loading a network instance | networkInstance | createNetworkInstance |
| Updating a network instance | networkInstance | updateNetworkInstance |

| Operation | Resource | Trace |
|---|---|---|
| Removing a network instance | networkInstance | deleteNetworkInstance |
| Assigning an inter-region bandwidth | interRegionBandwidth | createInterRegionBandwidth |
| Updating an inter-region bandwidth | interRegionBandwidth | updateInterRegionBandwidth |
| Deleting an inter-region bandwidth | interRegionBandwidth | deleteInterRegionBandwidth |
| Buying a bandwidth package | bandwidthPackage | createBandwidthPackage |
| Updating a bandwidth package | bandwidthPackage | updateBandwidthPackage |
| Deleting a bandwidth package | bandwidthPackage | deleteBandwidthPackage |
| Binding a bandwidth package to a cloud connection | bandwidthPackage | associateBandwidthPackage |
| Unbinding a bandwidth package | bandwidthPackage | disassociateBandwidthPackage |
| Allowing other users to load your VPCs | authorisation | createAuthorisation |
| Updating authorization | authorisation | updateAuthorisation |
| Canceling authorization | authorisation | deleteAuthorisation |

## 1.9.2 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 & Governance**, 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 Central Network Operation Guide

## 2.1 Overview

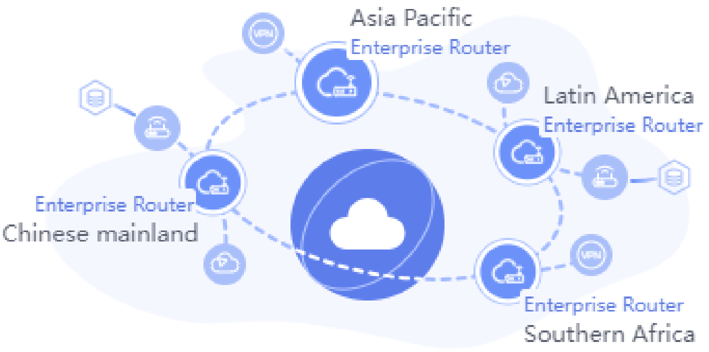
### What Is a Central Network?

Relying on the Huawei 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.

### Scenarios

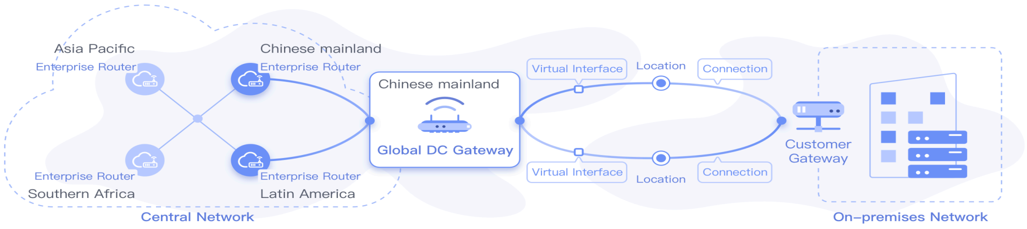
- Cross-region communication on the cloud: Enterprise routers in different regions are added to a central network as attachments so that resources in these regions can communicate with each other over one network.

**Figure 2-1** Cross-region communication between enterprise routers



- Communication between on-premises data centers and the cloud 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 Huawei Cloud backbone network.

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

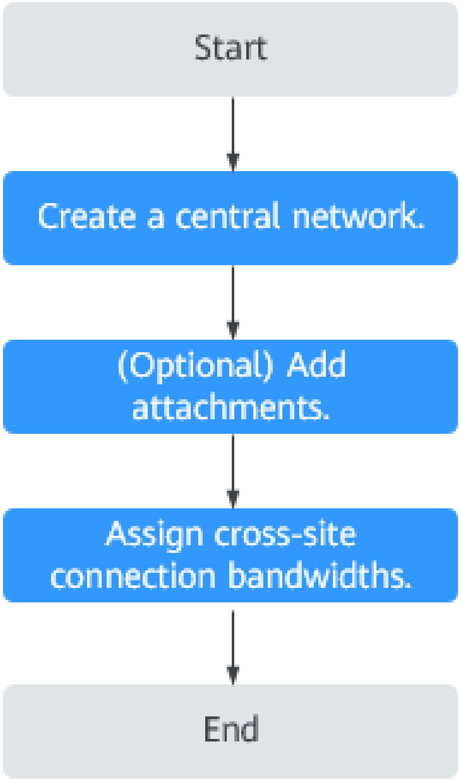


- Global network: By flexibly changing the central network policies, you can build a global network more conveniently.

## Process for Using a Central Network to Manage Network Resources

Figure 2-3 shows the process of configuring a central network to manage global network resources.

**Figure 2-3** Configuration process


Start
Create a central network.
(Optional) Add attachments.
Assign cross-site connection bandwidths.
End

# 2.2 Managing Central Networks

## Scenarios

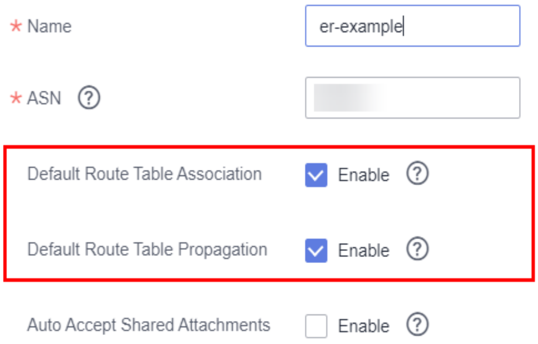
After an enterprise router is created, you can create a central network and add the enterprise router to a policy of the central network. In this way, resources can communicate with each other across regions, and network resources in each region can be managed centrally.

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 2-4** Enabling **Default Route Table Association** and **Default Route Table Propagation** for enterprise routers

  * Name: er-example
  * ASN: [redacted]
  Default Route Table Association ☑ Enable
  Default Route Table Propagation ☑ Enable
  Auto Accept Shared Attachments □ Enable

- 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

  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. Hover on the upper left corner to display **Service List** and 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 2-1** lists the parameters required for creating a central network.

**Table 2-1** 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 | |
| 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.<br>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**.

# 2.3 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. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**.
4. Locate the central network that you want to add a policy to 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. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**.
4. Locate the central network that you want to apply a policy to 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. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**.
4. Locate the central network that you want to delete a policy from 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**.

# 2.4 Managing Attachments

## Scenarios

To allow enterprise routers and global DC gateways to communicate with each other across regions, you need to add these network resources to a central network.

## Constraints

The global DC gateways you want to add to the central network have been created.

NOTE

Check the regions where global DC gateways are available on the Direct Connect console.

## Adding Attachments

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**.
4. Locate the central network that you want to add attachments to and click its name.
5. Switch to the **Attachments** tab and click **Add Attachment**.
6. Add network resources, such as enterprise routers and global DC gateways, to the central network as attachments. **Table 2-2** lists the parameters required for adding attachments.

**Table 2-2** Parameters for adding attachments

| Parameter | Setting |
|---|---|
| Name | Enter the name of the attachment. |
| Enterprise Router | Select the enterprise router you want to add to the central network.<br>You can also click **Create Enterprise Router** if there are no enterprise routers for you to select. |
| Select Global DC Gateway | |
| Region | Select the region of the global DC gateway. |

| Parameter | Setting |
|---|---|
| Global DC Gateway | Select the global DC gateway you want to add to the central network.<br>You can also click **Create Global DC Gateway** if there are no global DC gateways for you to select. |

7. Click **OK**.

### Deleting an Attachment

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**.
4. Locate the central network that you want to delete an attachment from 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**.

## 2.5 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 private 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 private bandwidth.
- After **Deleting a Cross-Site Connection Bandwidth**, you will still be billed if the global private bandwidth is not deleted.

### Assigning a Cross-Site Connection Bandwidth

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and 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 Private Bandwidth** column.
6. On the **Assign Cross-Site Connection Bandwidth** page, select the global private bandwidth.

   You can also click **Buy Now** to purchase one if there are no available global private 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. Hover on the upper left corner to display **Service List** and 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. Hover on the upper left corner to display **Service List** and 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 private 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. Hover on the upper left corner to display **Service List** and 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**.

# 2.6 Auditing

## 2.6.1 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 2-3** 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 |

| Operation | Resource | Trace |
|---|---|---|
| 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 |

## 2.6.2 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 & Governance**, 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 Global Private Bandwidth Operation Guide

## 3.1 Overview

A global private bandwidth is used by instances to allow communications over the Huawei Cloud backbone network.

NOTE

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

There are different types of global private 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 3-1** Global private 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.<br>**Multi-city Bandwidth Application Scenario (Global EIP)** |

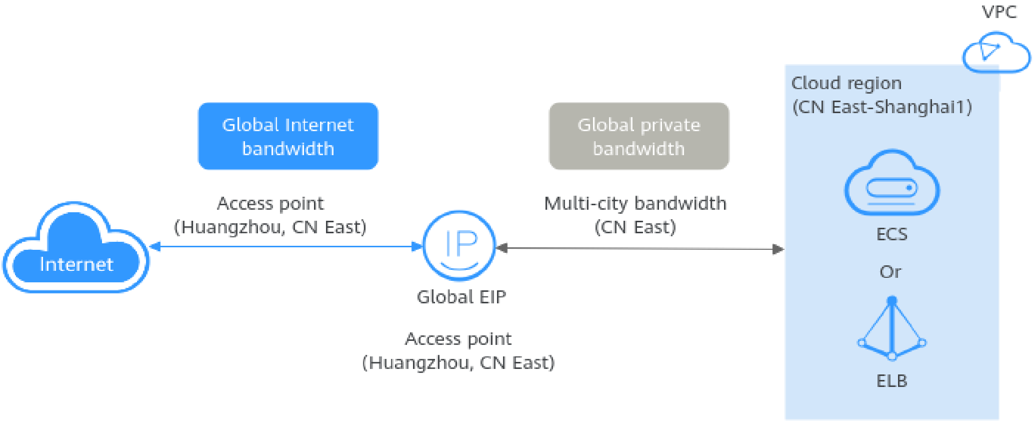
| Bandwidth Type | Instance Type | Description | Scenario |
|---|---|---|---|
| Geographic-region | Global EIPs<br>Cloud connections | Select this type of bandwidth if you need communications within a geographic region. Geographic regions include the Chinese mainland, Asia Pacific, and Southern Africa. 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 **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)**<br>● 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<br>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 **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)**<br>● 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 3-1** Multi-city bandwidth application scenario (global EIP)

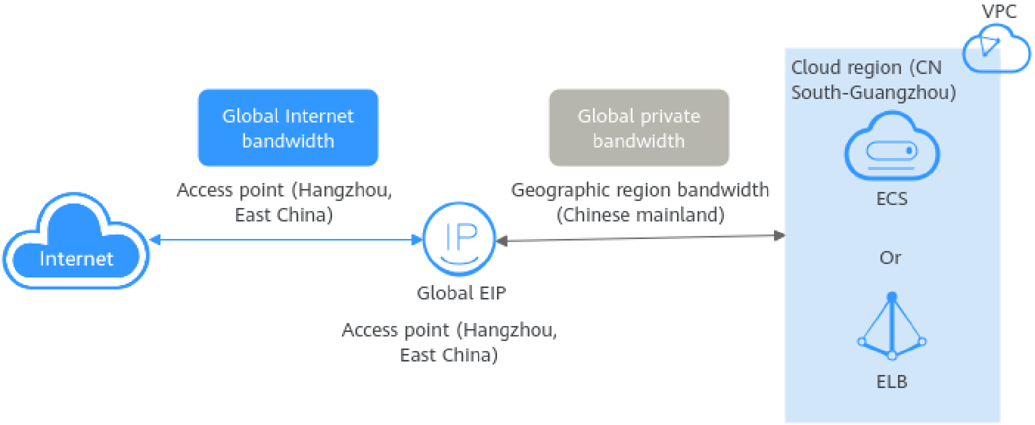


## Geographic-region Bandwidth Application Scenario (Global EIP)

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.

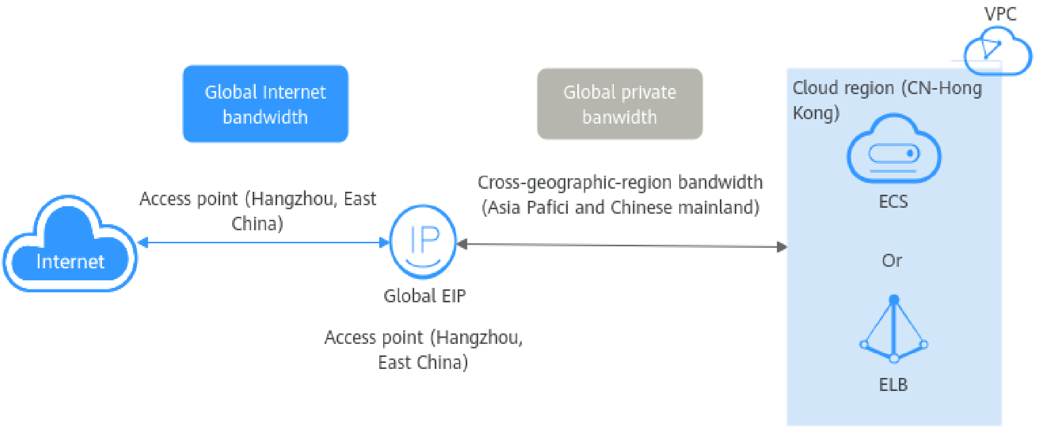
The ECS is in the CN-Hong Kong region, and the access point of the global EIP is in Hangzhou. CN-Hong Kong is a cloud region in Asia Pacific, but Hangzhou is a city on the Chinese mainland.

- 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 private banwidth
Cloud region (CN-Hong Kong)
Access point (Hangzhou, East China)
Cross-geographic-region bandwidth (Asia Pafici and Chinese mainland)
ECS
Internet
Or
Global EIP
Access point (Hangzhou, East China)
ELB

## 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

# 3.2 Buying a Global Private Bandwidth

## Scenarios

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

## Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.
5. In the cloud connection list, click the name of the cloud connection.
6. On the basic information page, click the **Global Private Bandwidths** tab.
7. Click **Buy Global Private Bandwidth**.
8. Configure the parameters based on **Table 3-2**.

**Table 3-2** Parameters required for buying a global private bandwidth

| Parameter | Description |
|---|---|
| Billing Mode | Mandatory<br>**Pay-per-use**: a postpaid subscription. You are charged based on the usage duration of the global private bandwidth. Your global private 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<br>There are different types of global private 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.<br>**Learn about the application scenarios of different types of bandwidths.**<br>You can decide whether to use a geographic-region bandwidth or cross-geographic-region bandwidth based on service scenarios. |

| Parameter | Description |
|---|---|
| Billed By | Mandatory<br>The price of a global private bandwidth varies by its size.<br>● After a bandwidth is purchased, the billing starts immediately regardless of whether the bandwidth is used.<br>● If a bandwidth is no longer required, delete it in a timely manner to avoid unnecessary fees. |
| Bandwidth | Mandatory<br>Select the size of the bandwidth in Mbit/s. |
| Bandwidth Name | Mandatory<br>Enter the name of the bandwidth. The name:<br>● Must contain 1 to 64 characters.<br>● Can contain letters, digits, underscores (_), hyphens (-), and periods (.). |

9. Click **Next**.
10. Confirm the configurations and click **Submit**.

    The global private bandwidth list page is displayed.
11. In the global private bandwidth list, view the status of the bandwidth.

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

# 3.3 Binding a Global Private Bandwidth

## Scenarios

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

## Constraints

- Instances that a global private bandwidth is to be bound to must be from the same region as the bandwidth.
- A global private bandwidth can only be bound to instances of the same type. If you want to add other type of instances to a global private 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 private bandwidth to or unbind it from one cloud connection at a time.
- If use a global private bandwidth on a central network, you need to configure cross-region connections by performing the following operations:
  - **Creating a Central Network**
  - **Managing Policies**
  - **Managing Attachments**

- Global private bandwidths of different types can be used with different instances. For details, see the following table.

**Table 3-3** Instances that can use a global private bandwidth

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

## Using a Global Private Bandwidth on a Central Network

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

## Binding Global EIPs to a Global Private Bandwidth

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Intra-Cloud** > **Global Private Bandwidths**.
5. Locate the global private bandwidth and click **Add** in the **Operation** column.
6. In the **Add** dialog box, set **Instance Type** to **Global EIP**.

   For a multi-city global private bandwidth, select the two regions where the bandwidth will be used.
7. Search for global EIPs using keywords.
8. Select one or more global EIPs and click **OK**.

# 3.4 Unbinding a Global Private Bandwidth

## Scenarios

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

## Constraints

- Before a global private 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 private bandwidth can only be bound to instances of the same type. If you want to add other type of instances to a global private bandwidth with instances bound, you need to remove the bound instances first by referring to **Binding a Global Private Bandwidth**.
- If inter-region bandwidths have been assigned from a global private 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. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Central Networks**.
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**.

## Unbinding a Global EIP from a Global Private Bandwidth

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Intra-Cloud** > **Global Private Bandwidths**.
5. Locate the global private 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**.

# 3.5 Modifying a Global Private Bandwidth

## Scenarios

Your can increase or decrease a global private bandwidth. The new bandwidth takes effect immediately.

## Procedure

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

# 3.6 Deleting a Global Private Bandwidth

## Scenarios

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

## Constraints

A global private bandwidth with an instance bound cannot be deleted. To delete such a bandwidth, unbind its instance first. For details, see **Unbinding a Global Private Bandwidth**.

## Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, choose **Networking** > **Cloud Connect**.
4. In the navigation pane on the left, choose **Cloud Connect** > **Cloud Connections**.
5. In the cloud connection list, click the name of the cloud connection.

6. On the basic information page, click the **Global Private Bandwidths** tab.
7. Locate the bandwidth you want to delete and click its name to view its settings.
8. In the upper left corner of the page, click < .
9. In the global private bandwidth list, search for the bandwidth.
10. Choose **More** > **Delete** in the **Operation** column.
11. Click **OK**.

# 3.7 Auditing

## 3.7.1 Key Operations Recorded by CTS

### Scenarios

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

### Prerequisites

You have enabled CTS.

### Key Operations Recorded by CTS

**Table 3-4** Global private bandwidth operations recorded by CTS

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

## 3.7.2 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 & Governance**, 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.

# 4 Permissions Management

## 4.1 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.

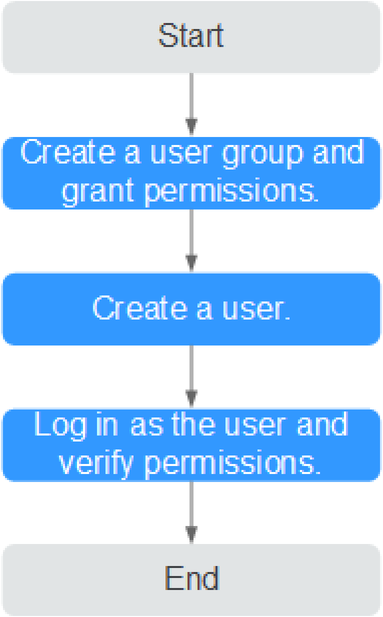
**Figure 4-1** shows the process for granting permissions.

### 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 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 4-1** Process for granting Cloud Connect 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** to it.

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

2. **Create an IAM user**.

   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.

   - Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**. Click **Create Cloud Connection** in the upper right corner. If the cloud connection is 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.

# 4.2 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"
              ]
          }
      ]
  }
  ```

# 4.3 Configuration Examples for Cloud Connect Permission Policy

You can configure permission policies for different IAM users based on service requirements.

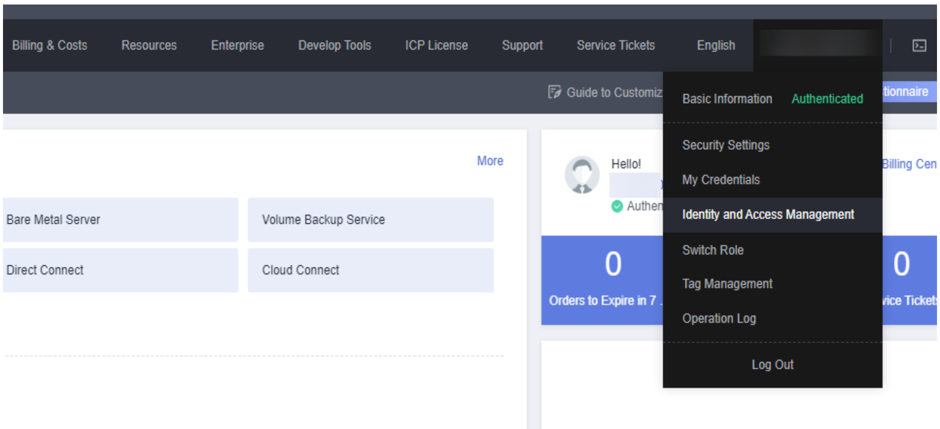
## Example 1: Allowing an IAM User Who Is Not in Any Enterprise Projects to Have All Cloud Connect Permissions

An IAM user who is not in any enterprise projects wants to have all Cloud Connect permissions, for example, performing operations on cloud connections, network instances, bandwidth packages, inter-region bandwidths, and routes, and operations such as cross-border permit application and cross-account authorization.

To grant the permissions to this IAM user, perform the following operations:

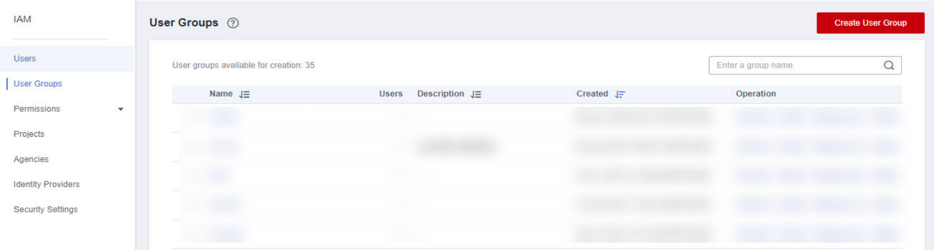
1. Log in to the management console.
2. On the homepage, hover over the username in the upper right corner and choose **Identity and Access Management** from the drop-down list.

**Figure 4-2** Identity and Access Management



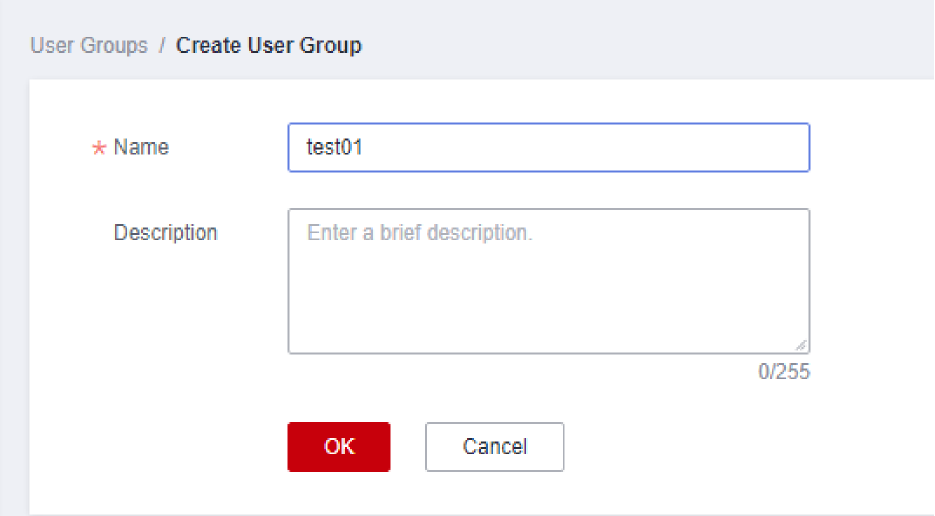
3. In the navigation pane on the left, choose **User Groups**.
4. In the upper right corner, click **Create User Group**.

**Figure 4-3** Creating a user group



5. Configure the parameters and click **OK**.

**Figure 4-4** Configuring user group parameters



User Groups / Create User Group

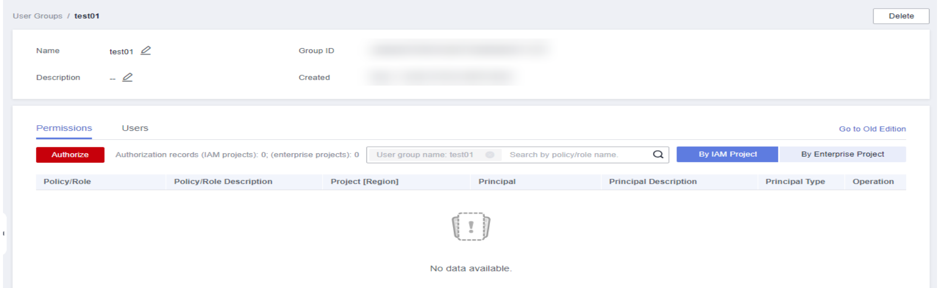
* Name: test01

Description: Enter a brief description.

0/255

6. Locate the created user group and click its name.
7. Click **By IAM Project** on the right and then click **Authorize**.

**Figure 4-5** Authorizing a user group



User Groups / test01

Name: test01

Description: --

Group ID: [redacted]

Created: [redacted]

Authorization records (IAM projects): 0; (enterprise projects): 0

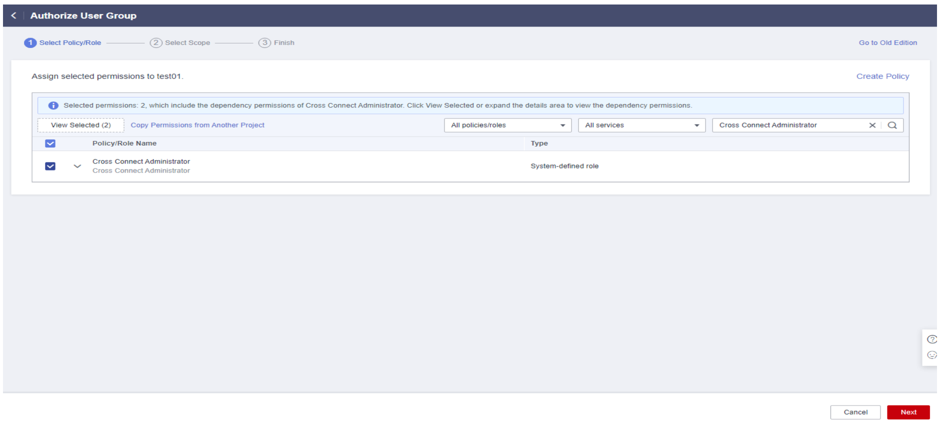
User group name: test01 | Search by policy/role name.

| Policy/Role | Policy/Role Description | Project [Region] | Principal | Principal Description | Principal Type | Operation |
|---|---|---|---|---|---|---|

No data available.

8. Enter **Cross Connect Administrator** in the text box and click the search icon.
9. In the search result, select **Cross Connect Administrator** and click **Next**.

**Figure 4-6** Selecting a system-defined role



Assign selected permissions to test01.

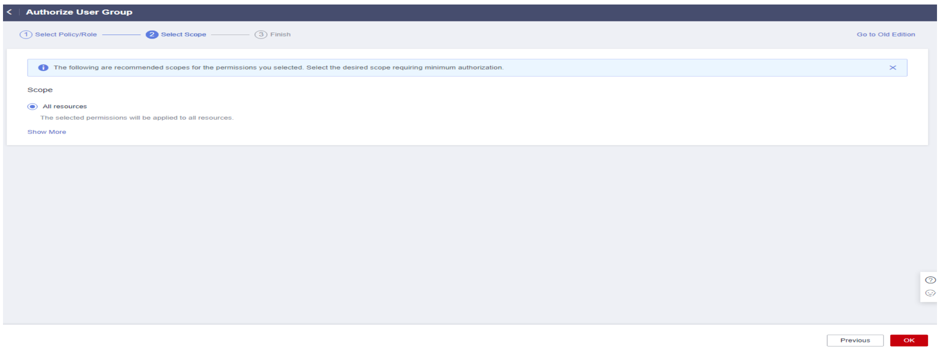
Selected permissions: 2, which include the dependency permissions of Cross Connect Administrator. Click View Selected or expand the details area to view the dependency permissions.

Cross Connect Administrator

| ☑ | Policy/Role Name | Type |
|---|---|---|
| ☑ | Cross Connect Administrator<br>Cross Connect Administrator | System-defined role |

10. Click **Show More**.

**Figure 4-7** Scope



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

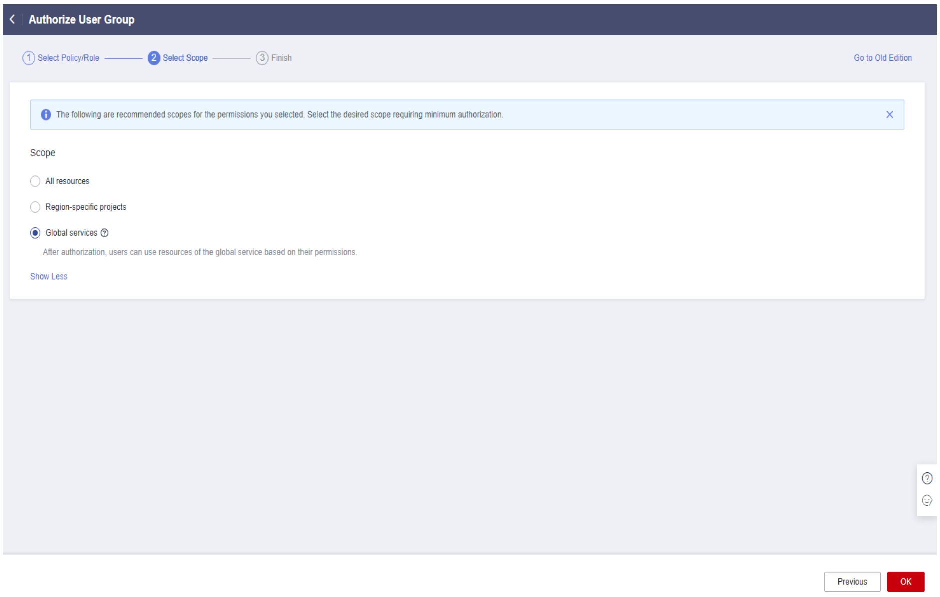
● All resources

The selected permissions will be applied to all resources.

Show More

11. Select **Global services** and click **OK**.

**Figure 4-8** Global services



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

○ All resources

○ Region-specific projects

● Global services

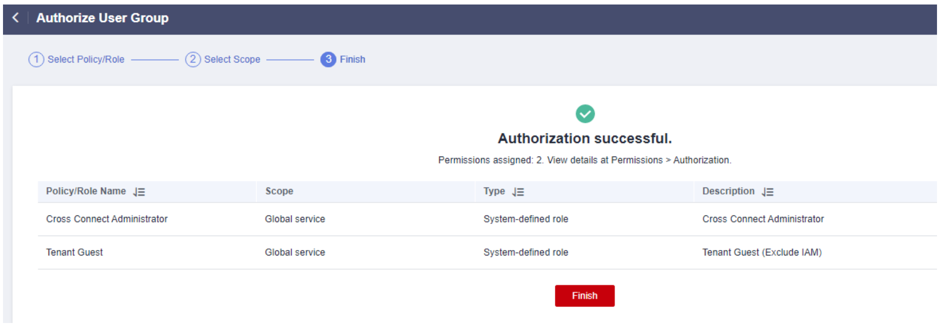
After authorization, users can use resources of the global service based on their permissions.

Show Less

NOTE

If "Authorization successful" is displayed, the authorization is complete. The authorization will take effect 15 to 30 minutes later.

**Figure 4-9** Authorization successful



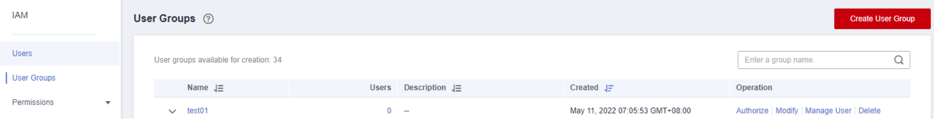
Authorization successful.

Permissions assigned: 2. View details at Permissions > Authorization.

| Policy/Role Name | Scope | Type | Description |
|---|---|---|---|
| Cross Connect Administrator | Global service | System-defined role | Cross Connect Administrator |
| Tenant Guest | Global service | System-defined role | Tenant Guest (Exclude IAM) |

12. Go back to the user group list, locate the created user group, and click **Manage User** in the **Operation** column.

**Figure 4-10** Manage User



13. Select the IAM user you want to add to the user group and click **OK**.

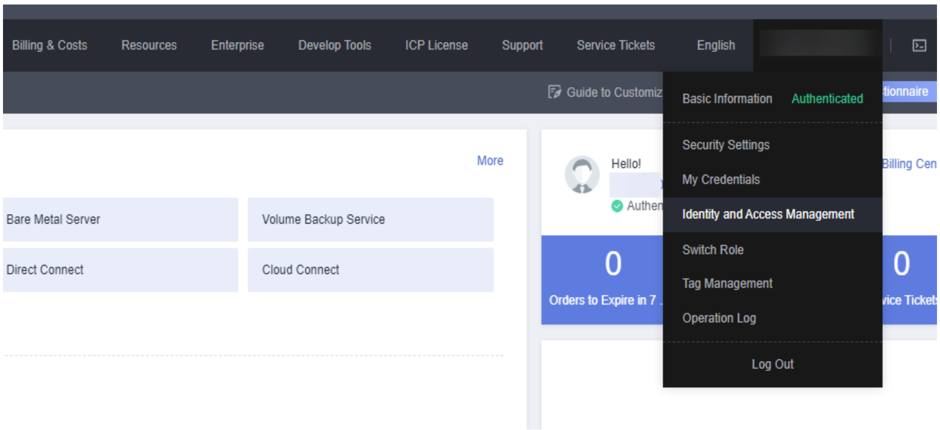
## Example 2: Authorizing an IAM User to Use Cloud Connect in All Enterprise Projects

An IAM user needs to perform operations on Cloud Connect resources, including network instances, bandwidth packages, inter-region bandwidths, and routes, in all enterprise projects. You can perform the operations below to grant the corresponding permissions to this IAM user.

To grant the permissions on cross-account authorization and cross-border permit application, perform the operations in **Example 1: Allowing an IAM User Who Is Not in Any Enterprise Projects to Have All Cloud Connect Permissions**.

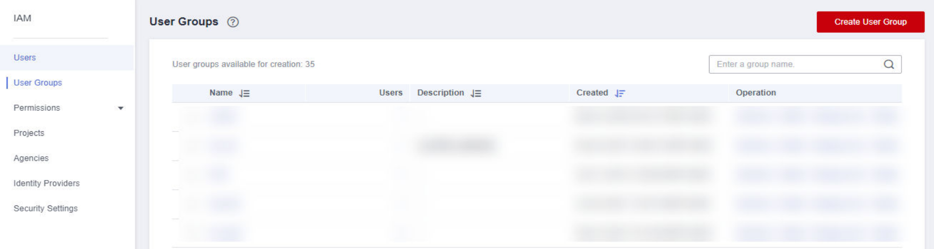
1. Log in to the management console.
2. On the homepage, hover over the username in the upper right corner and choose **Identity and Access Management** from the drop-down list.

**Figure 4-11** Identity and Access Management



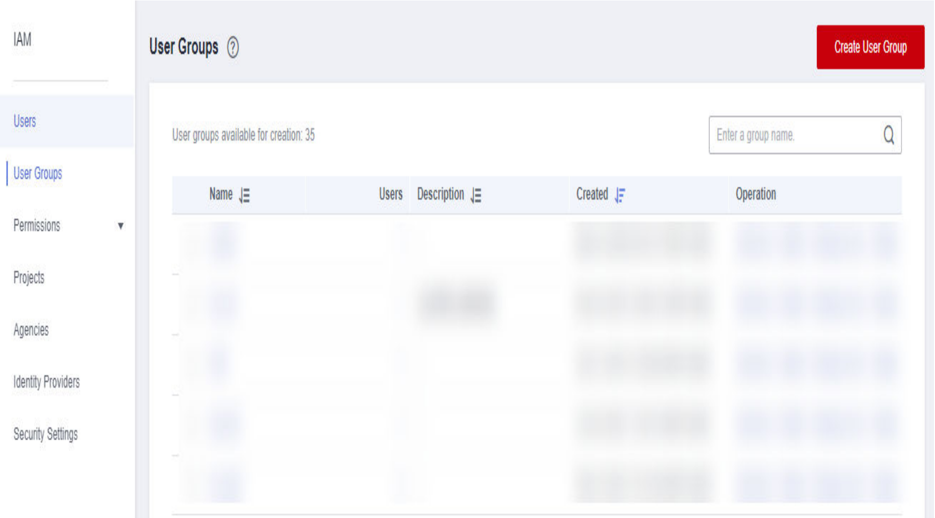
3. In the navigation pane on the left, choose **User Groups**.
4. In the upper right corner, click **Create User Group**.

**Figure 4-12** Creating a user group



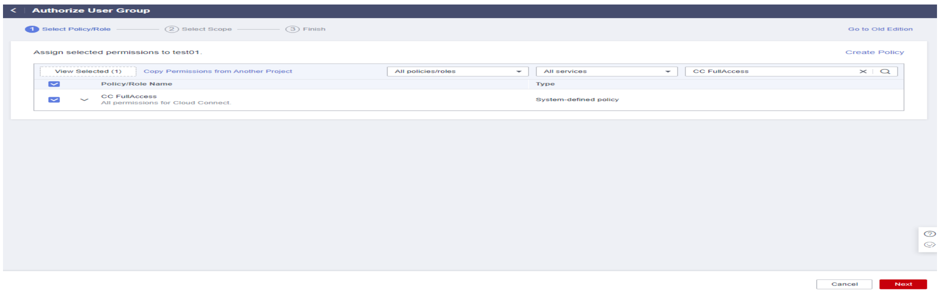
5. Configure the parameters and click **OK**.

**Figure 4-13** Configuring user group parameters



6. Locate the created user group and click its name.
7. Click **By IAM Project** on the right and then click **Authorize**.

**Figure 4-14** Authorizing a user group



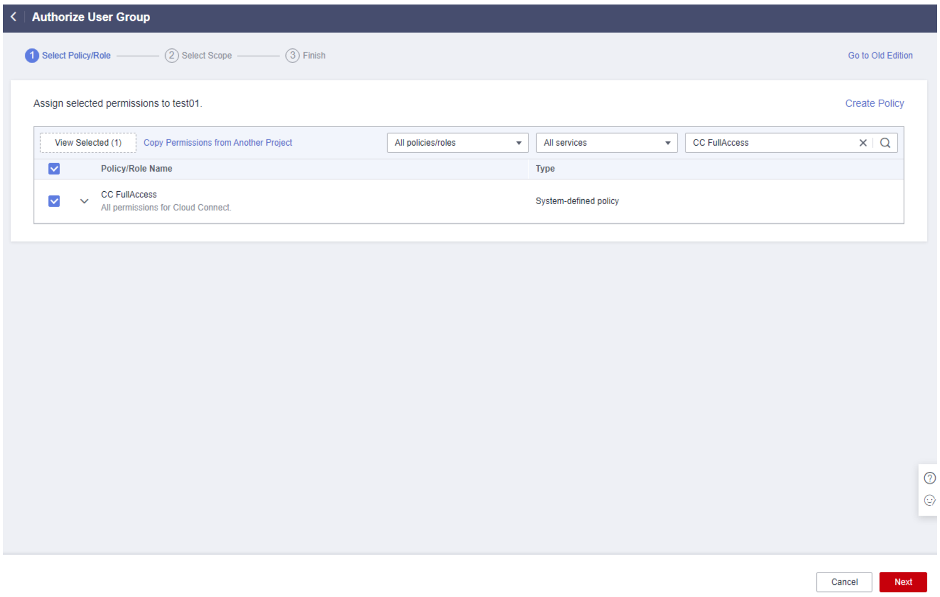
Assign selected permissions to test01.

All policies/roles | All services | CC FullAccess

| ☑ | Policy/Role Name | Type |
|---|---|---|
| ☑ | CC FullAccess<br>All permissions for Cloud Connect. | System-defined policy |

8. Enter **CC FullAccess** in the text box and click the search icon.
9. In the search result, select **CC FullAccess** and click **Next**.

**Figure 4-15** Selecting a system-defined policy



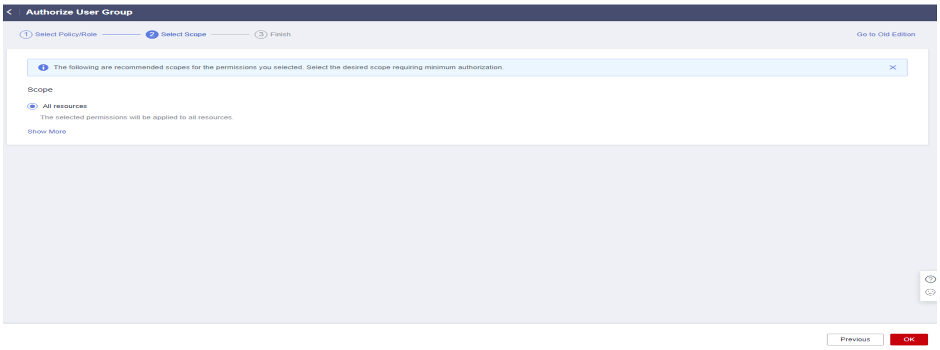
Assign selected permissions to test01.

All policies/roles | All services | CC FullAccess

| ☑ | Policy/Role Name | Type |
|---|---|---|
| ☑ | CC FullAccess<br>All permissions for Cloud Connect. | System-defined policy |

10. Click **Show More**.

**Figure 4-16** Scope



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

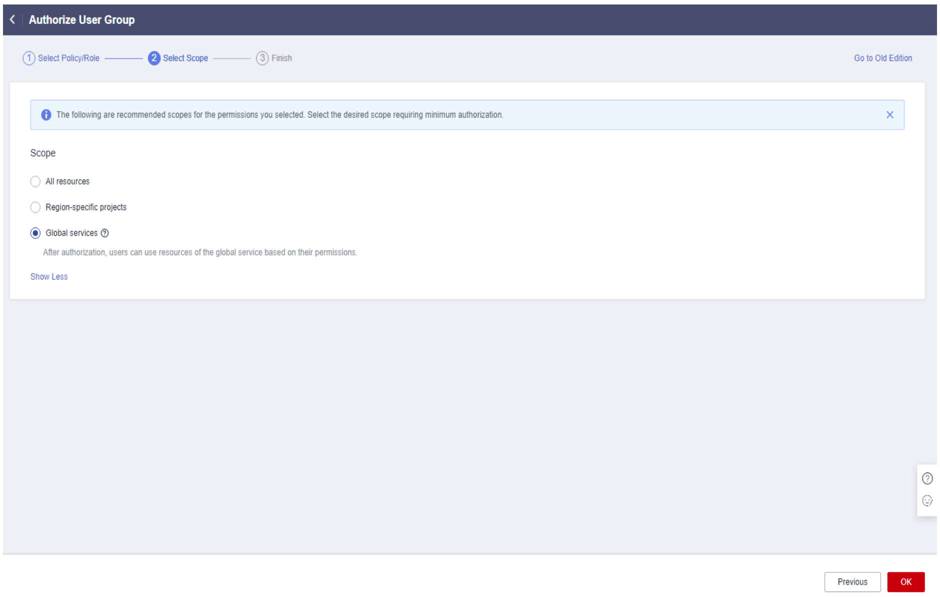
● All resources

The selected permissions will be applied to all resources.

Show More

11. Select **Global services** and click **OK**.

**Figure 4-17** Global services



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

○ All resources

○ Region-specific projects

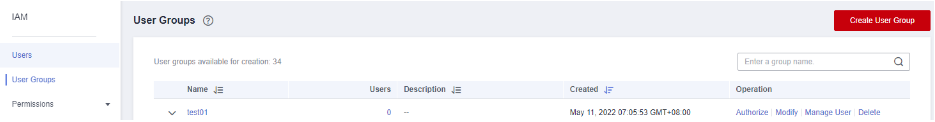
● Global services

After authorization, users can use resources of the global service based on their permissions.

Show Less

12. Go back to the user group list, locate the created user group, and click **Manage User** in the **Operation** column.

**Figure 4-18** Manage User



User groups available for creation: 34

| Name | Users | Description | Created | Operation |
|---|---|---|---|---|
| test01 | 0 | -- | May 11, 2022 07:05:53 GMT+08:00 | Authorize \| Modify \| Manage User \| Delete |

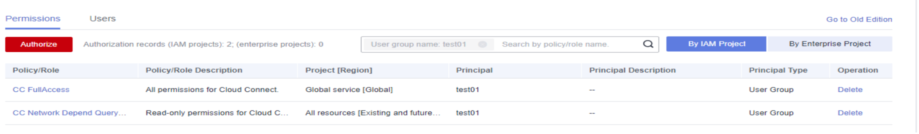
13. Select the IAM user you want to add to the user group and click **OK**.

NOTE

If the IAM user does not have VPC-related permissions, you can grant the **CC Network Depend QueryAccess** permissions for the user group that the IAM user belongs to and select **All resources** for **Scope**.

You can view the authorization in the **Permissions** tab.

**Figure 4-19** Permissions



Authorization records (IAM projects): 2; (enterprise projects): 0

| Policy/Role | Policy/Role Description | Project [Region] | Principal | Principal Description | Principal Type | Operation |
|---|---|---|---|---|---|---|
| CC FullAccess | All permissions for Cloud Connect. | Global service [Global] | test01 | -- | User Group | Delete |
| CC Network Depend Query... | Read-only permissions for Cloud C... | All resources [Existing and future... | test01 | -- | User Group | Delete |

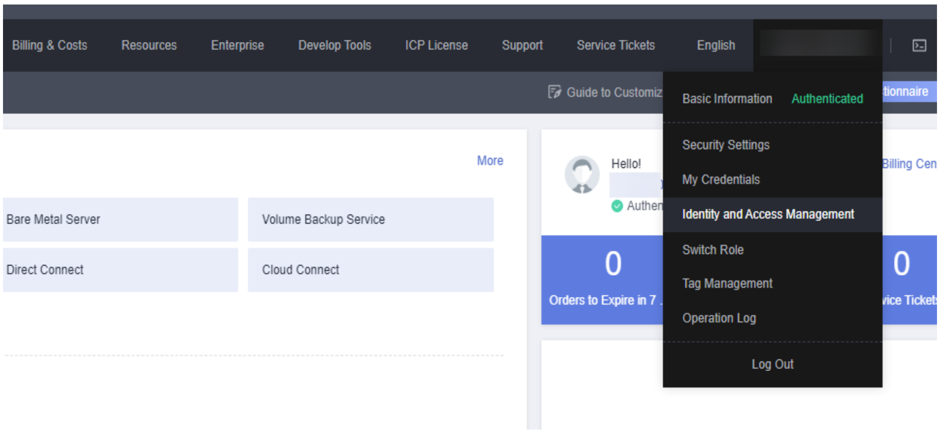
## Example 3: Authorizing an IAM User to Use Cloud Connect in a Specific Enterprise Project

An IAM user needs to perform operations on Cloud Connect resources, including network instances, bandwidth packages, inter-region bandwidths, and routes, in specific enterprise projects. You can perform the operations below to grant the corresponding permissions to this IAM user.

To grant the permissions on cross-account authorization and cross-border permit application, perform the operations in **Example 1: Allowing an IAM User Who Is Not in Any Enterprise Projects to Have All Cloud Connect Permissions**.

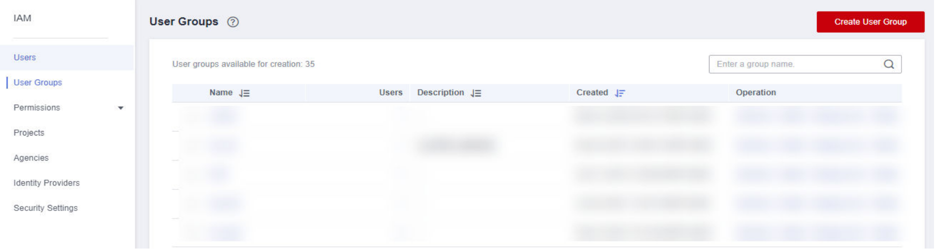
1. Log in to the management console.
2. On the homepage, hover over the username in the upper right corner and choose **Identity and Access Management** from the drop-down list.

**Figure 4-20** Identity and Access Management



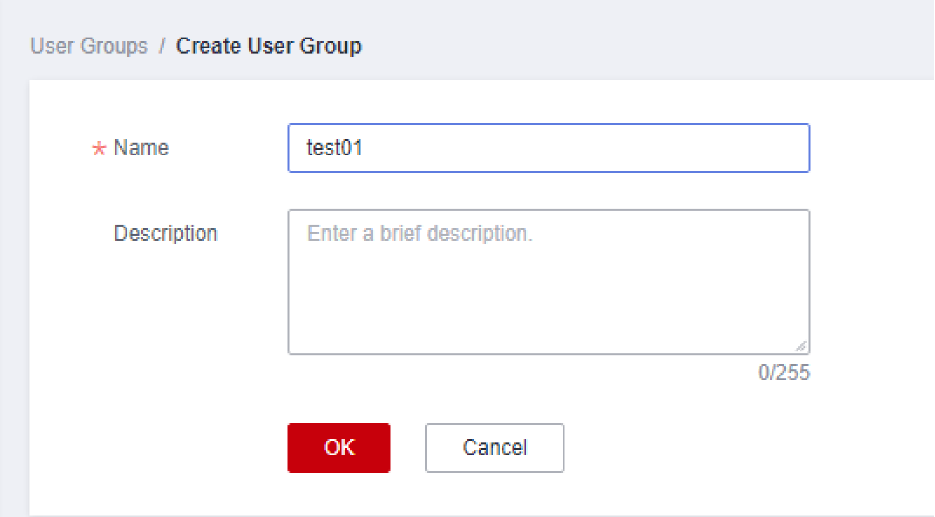
3. In the navigation pane on the left, choose **User Groups**.
4. In the upper right corner, click **Create User Group**.

**Figure 4-21** Creating a user group



5. Configure the parameters and click **OK**.

**Figure 4-22** Configuring user group parameters

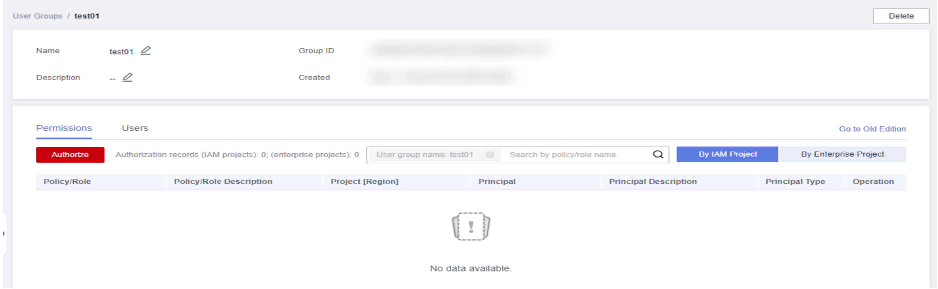


* Name: test01

Description:

6. Locate the created user group and click its name.
7. Click **By IAM Project** on the right and then click **Authorize**.

**Figure 4-23** Authorizing a user group



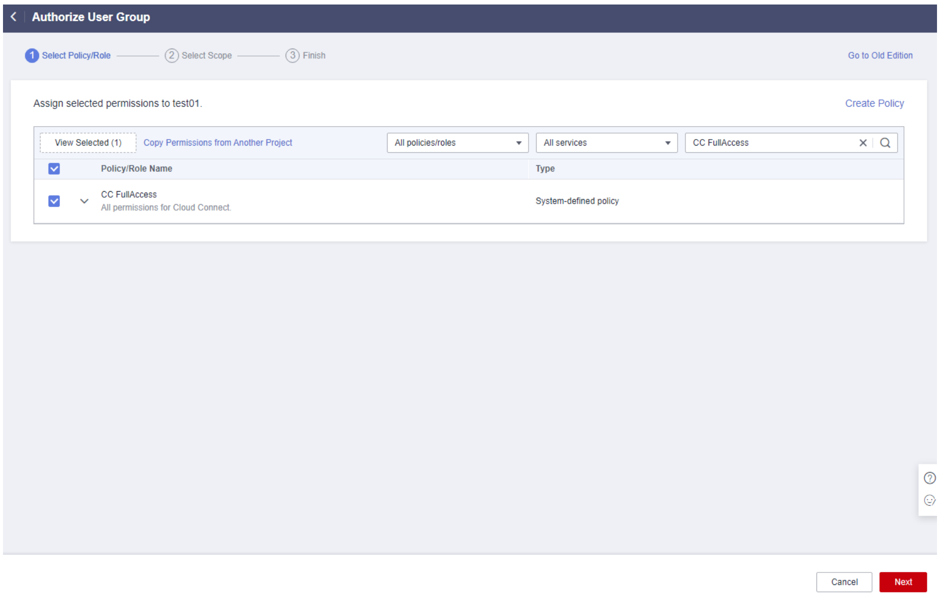
Name: test01

Description: --

Authorization records (IAM projects): 0; (enterprise projects): 0

8. Enter **CC FullAccess** in the text box and click the search icon.
9. In the search result, select **CC FullAccess** and click **Next**.

**Figure 4-24** Selecting a system-defined policy



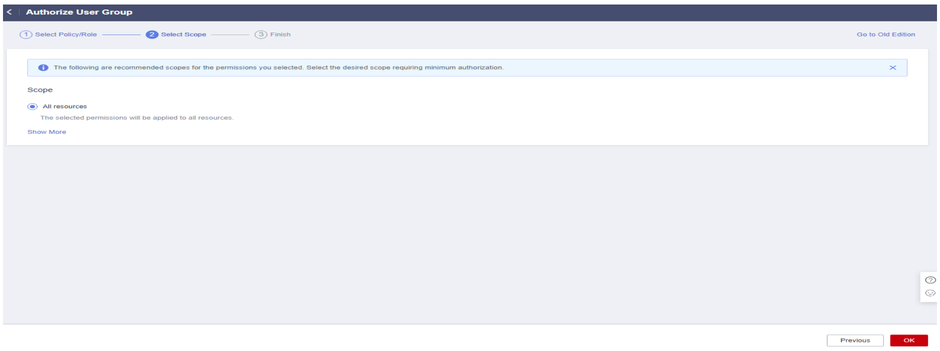
Assign selected permissions to test01.

CC FullAccess

| ☑ | Policy/Role Name | Type |
|---|---|---|
| ☑ | CC FullAccess<br>All permissions for Cloud Connect. | System-defined policy |

10. Click **Show More**.

**Figure 4-25** Scope



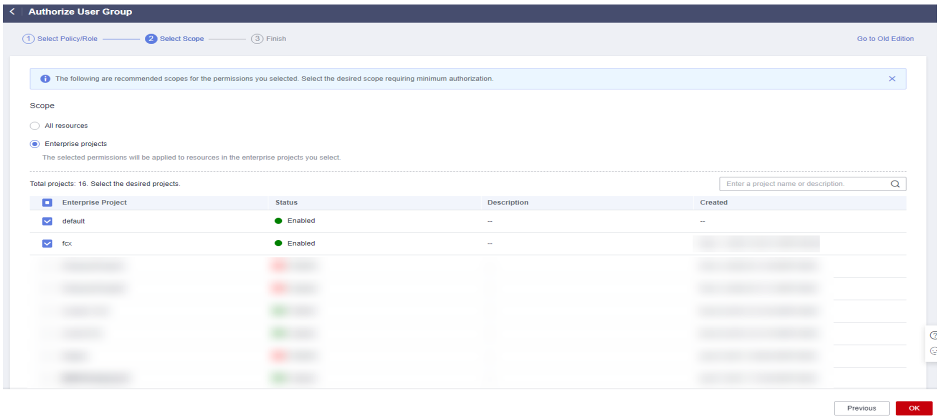
The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

● All resources
The selected permissions will be applied to all resources.

11. Select **Enterprise projects**.
12. Select an enterprise project and click **OK**.

**Figure 4-26** Enterprise projects



The following are recommended scopes for the permissions you selected. Select the desired scope requiring minimum authorization.

Scope

○ All resources

● Enterprise projects
The selected permissions will be applied to resources in the enterprise projects you select.

Total projects: 16. Select the desired projects.

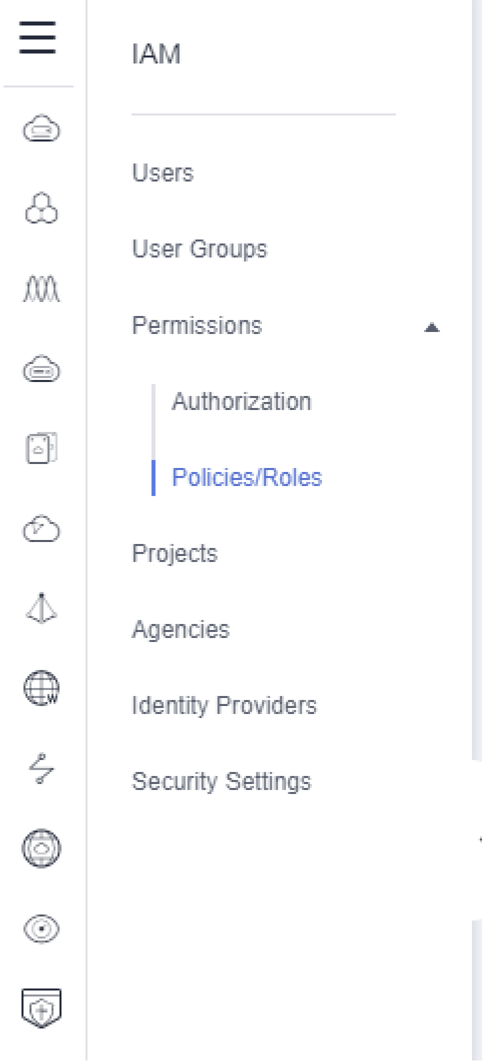
Enter a project name or description.

| ☐ | Enterprise Project | Status | Description | Created |
|---|---|---|---|---|
| ☑ | default | ● Enabled | -- | -- |
| ☑ | fcx | ● Enabled | -- | [redacted] |

[redacted]

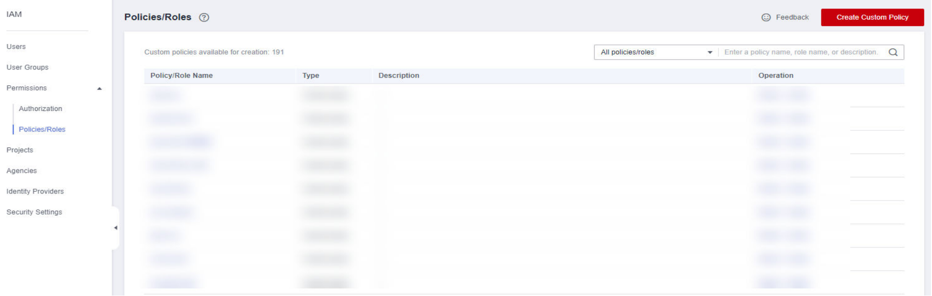
13. In the navigation pane on the left, choose **Permissions** > **Policies/Roles**.

**Figure 4-27** Policies/Roles



14. Click **Create Custom Policy**.

**Figure 4-28** Creating a custom policy



Custom policies available for creation: 191

| Policy/Role Name | Type | Description | Operation |
|---|---|---|---|

15. Configure the parameters based on **Configuration Examples for Cloud Connect Permission Policy**.

**Table 4-1** Custom policy parameters

| Parameter | Description |
|---|---|
| Policy Name | Specifies the name of the custom policy. |
| Policy View | ● (Recommended) Visual editor<br>● JSON |
| Policy Content | ● Select **Allow**.<br>● Cloud service: **Cloud Connect**<br>● Actions:<br>– ReadOnly: Select **cc:networkInstances:get**, **cc:interRegionBandwidths:get**, and **cc:cloudConnectionRoutes:get**.<br>– **ReadWrite**: Select the following: **cc:networkInstances:create**<br>**cc:interRegionBandwidths:update**<br>**cc:networkInstances:delete**<br>**cc:interRegionBandwidths:create**<br>**cc:interRegionBandwidths:delete**<br>**cc:networkInstances:update**<br>– ListOnly: Select **cc:cloudConnectionRoutes:list**, **cc:networkInstances:list**, and **cc:interRegionBandwidths:list**. |

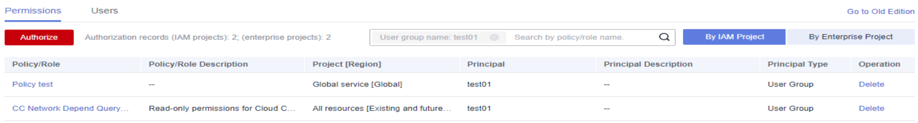
16. Configure other parameters and click **OK**.
17. Repeat steps **3** to **7**.
18. Search for the created custom policy by name.
19. Select the custom policy and click **Next**.
20. Click **Show More**.
21. Select **All resources** and click **OK**.

NOTE

If the IAM user does not have VPC-related permissions, you can grant the **CC Network Depend QueryAccess** permissions for the user group that the IAM user belongs to and select **All resources** for **Scope**.

You can view the authorization in the **Permissions** tab.

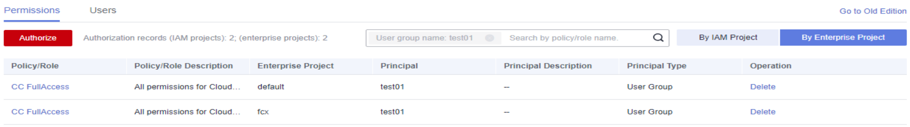
**Figure 4-29** Authorization records in the IAM project view



Authorization records (IAM projects): 2; (enterprise projects): 2

| Policy/Role | Policy/Role Description | Project [Region] | Principal | Principal Description | Principal Type | Operation |
|---|---|---|---|---|---|---|
| Policy test | -- | Global service [Global] | test01 | -- | User Group | Delete |
| CC Network Depend Query... | Read-only permissions for Cloud C... | All resources [Existing and future... | test01 | -- | User Group | Delete |

**Figure 4-30** Authorization records in the enterprise project view



Authorization records (IAM projects): 2; (enterprise projects): 2

| Policy/Role | Policy/Role Description | Enterprise Project | Principal | Principal Description | Principal Type | Operation |
|---|---|---|---|---|---|---|
| CC FullAccess | All permissions for Cloud... | default | test01 | -- | User Group | Delete |
| CC FullAccess | All permissions for Cloud... | fcx | test01 | -- | User Group | Delete |

# 5 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.

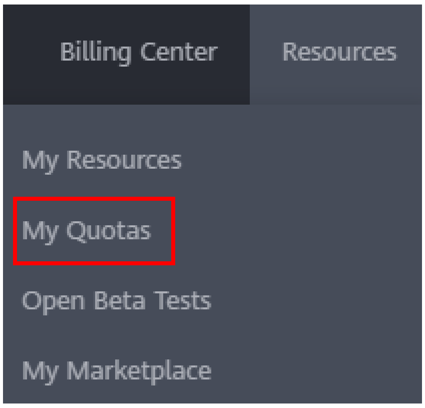
If the existing resource quota cannot meet your service requirements, you can apply for a higher quota.

## 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.

   **Figure 5-1** My Quotas

4. View the used and total quota of each type of resources on the displayed page.

   If a quota cannot meet service requirements, apply for a higher quota.

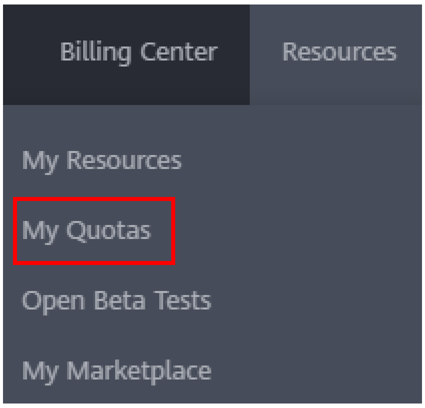
## How Do I Apply for a Higher Quota?

1. Log in to the management console.

2. In the upper right corner of the page, choose **Resources** > **My Quotas**.

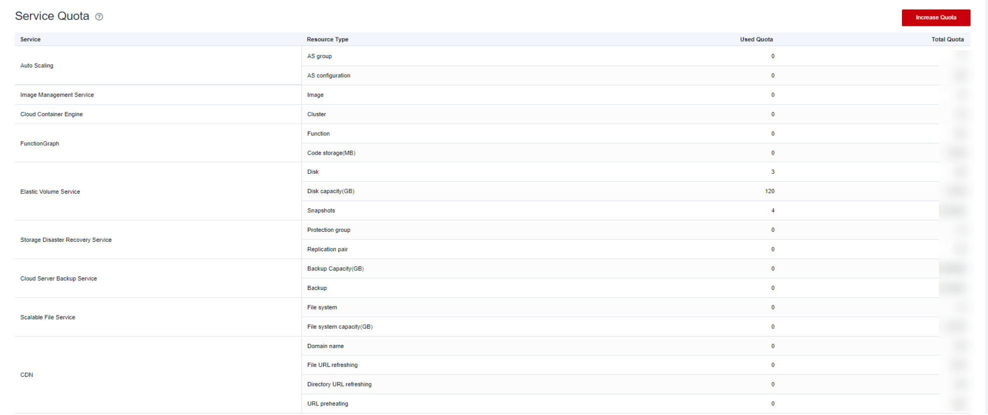
   The **Service Quota** page is displayed.

   **Figure 5-2** My Quotas

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

   **Figure 5-3** Increasing quota

| Service | Resource Type | Used Quota | Total Quota |
|---|---|---|---|
| Auto Scaling | AS group | 0 | [redacted] |
| | AS configuration | 0 | [redacted] |
| Image Management Service | Image | 0 | [redacted] |
| Cloud Container Engine | Cluster | 0 | [redacted] |
| FunctionGraph | Function | 0 | [redacted] |
| | Code storage(MB) | 0 | [redacted] |
| Elastic Volume Service | Disk | 3 | [redacted] |
| | Disk capacity(GB) | 120 | [redacted] |
| | Snapshots | 4 | [redacted] |
| Storage Disaster Recovery Service | Protection group | 0 | [redacted] |
| | Replication pair | 0 | [redacted] |
| Cloud Server Backup Service | Backup Capacity(GB) | 0 | [redacted] |
| | Backup | 0 | [redacted] |
| Scalable File Service | File system | 0 | [redacted] |
| | File system capacity(GB) | 0 | [redacted] |
| CDN | Domain name | 0 | [redacted] |
| | File URL refreshing | 0 | [redacted] |
| | Directory URL refreshing | 0 | [redacted] |
| | URL preheating | 0 | [redacted] |

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**.

# 6 Change History

| Release Date | Description |
|---|---|
| 2024-03-15 | This issue is the fifteenth official release, which incorporates the following changes:<br>Added the description of tag policies in **Creating a Cloud Connection** and **Managing Cloud Connection Tags**. |
| 2023-06-28 | This issue is the fourteenth official release, which incorporates the following changes:<br>Supported global private bandwidth. |
| 2022-06-30 | This issue is the thirteenth official release, which incorporates the following changes:<br>Tags can be used to identify cloud connections and bandwidths. |
| 2021-06-30 | This issue is the twelfth official release, which incorporates the following changes:<br>● Added information about new features in "What's New".<br>● Modified section "Billing" in chapter "Service Overview". |
| 2020-09-30 | This issue is the eleventh official release, which incorporates the following changes:<br>● Modified section "Billing" in chapter "Service Overview".<br>● Added section "Accelerating Access to a Website Across Regions" in chapter "Best Practices".<br>● Modified FAQs in "Product Consultation", "Bandwidth, Latency, and Packet Loss", and "Cross-account Authorization". |

| Release Date | Description |
|---|---|
| 2020-06-30 | This issue is the tenth official release, which incorporates the following changes:<br>● Updated section "Geographic Regions and Huawei Cloud Regions" in chapter "Service Overview".<br>● Added sections "Creating a Cloud Connection", "Loading a Network Instance", "Unsubscribing from a Yearly/Monthly Bandwidth Package", "Configuring an Inter-Region Bandwidth", "Adding a Custom CIDR Block", and "Authorizing a Network Instance" in chapter "User Guide".<br>● Optimized sections "Acceleration of Cross-Region Internet Access from an Intranet by Combining Cloud Connect with SNAT" and "Acceleration of Cross-Region Internet Access from an Intranet by Combining Cloud Connect with DNAT", and added section "Authorizing Network Instances Across Accounts" in chapter "Best Practices".<br>● Added FAQs about cross-account authorization. |
| 2020-05-30 | This issue is the ninth official release, which incorporates the following changes:<br>● Modified sections "Geographic Regions and Huawei Cloud Regions", "Available Regions", and "Billing" in chapter "Service Overview".<br>● Optimized chapter "Getting Started".<br>● Updated section "Acceleration of Cross-Region Internet Access".<br>● Classified FAQs. |
| 2020-04-30 | This issue is the eighth official release, which incorporates the following changes:<br>● Updated section "What Is Cloud Connect?" and added section "Billing" in chapter "Service Overview".<br>● Updated section "Communication Between Data Centers and VPCs in Different Regions" in chapter "Getting Started".<br>● Updated section "Acceleration of Cross-Region Internet Access".<br>● Added new FAQs. |
| 2020-03-30 | This issue is the seventh official release, which incorporates the following changes:<br>● Updated chapter "Best Practices."<br>● Added section "Billing."<br>● Optimized the entire document. |

| Release Date | Description |
|---|---|
| 2020-03-16 | This issue is the sixth official release, which incorporates the following changes:<br>Updated section "Acceleration of Cross-Region Internet Access". |
| 2019-12-30 | This issue is the fifth official release, which incorporates the following changes:<br>Added Latin America and LA-Santiago in sections "Geographic Regions and Huawei Cloud Regions" and "Available Regions". |
| 2019-11-30 | This issue is the fourth official release, which incorporates the following changes:<br>Optimized the entire document. |
| 2019-10-30 | This issue is the third official release, which incorporates the following changes:<br>Added operations for enabling communication between VPCs in the same region. |
| 2019-10-21 | This issue is the second official release, which incorporates the following changes:<br>Added FAQs about cross-border permits. |
| 2019-08-30 | This issue is the first official release. |