

**Cloud Connect**

# **User Guide**

**Issue**            01  
**Date**             2026-03-06



**Copyright © Huawei Cloud Computing Technologies Co., Ltd. 2026. All rights reserved.**

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

## **Trademarks and Permissions**



HUAWEI and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

## **Notice**

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

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

---

# Contents

---

<b>1 Cloud Connection Operation Guide.....</b>	<b>1</b>
1.1 Using IAM to Grant Access to Cloud Connect.....	1
1.1.1 Using IAM Roles or Policies to Grant Access to Cloud Connections.....	1
1.1.2 Using IAM Identity Policies to Grant Access to Cloud Connections.....	4
1.2 Cloud Connections.....	6
1.2.1 Cloud Connection Overview.....	7
1.2.2 Creating a Cloud Connection.....	9
1.2.3 Managing Cloud Connections.....	11
1.2.4 Binding or Unbinding a Bandwidth Package to and from a Cloud Connection.....	12
1.2.5 Changing the Capacity of a Bandwidth Package Bound to a Cloud Connection.....	13
1.2.6 Managing Cloud Connection Tags.....	14
1.3 Cross-Border Permits.....	15
1.3.1 Cross-Border Permit Overview.....	16
1.3.2 Applying for a Cross-Border Permit.....	16
1.3.3 Querying the Progress of the Cross-Border Permit Application.....	20
1.4 Network Instances.....	21
1.4.1 Network Instance Overview.....	21
1.4.2 Loading a Network Instance to a Cloud Connection.....	22
1.4.3 Managing Network Instances.....	24
1.5 Bandwidth Packages.....	25
1.5.1 Bandwidth Package Overview.....	26
1.5.2 Buying a Bandwidth Package.....	27
1.5.3 Binding or Unbinding a Bandwidth Package to and from a Cloud Connection.....	30
1.5.4 Managing Bandwidth Packages.....	31
1.5.5 Managing Bandwidth Package Tags.....	32
1.6 Inter-Region Bandwidths.....	34
1.6.1 Inter-Region Bandwidth Overview.....	34
1.6.2 Assigning an Inter-Region Bandwidth.....	35
1.6.3 Managing Inter-Region Bandwidths.....	37
1.6.4 Viewing Monitoring Data of an Inter-Region Bandwidth.....	37
1.7 Cross-Account Authorization.....	38
1.7.1 Cross-Account Authorization Overview.....	38
1.7.2 Authorizing Network Instances.....	38

1.7.3 Managing Cross-Account Authorization.....	40
1.8 Route Information.....	41
1.8.1 Route Overview.....	42
1.8.2 Modifying the VPC CIDR Block.....	46
1.8.3 Viewing Cloud Connection Routes.....	46
1.9 Monitoring and Auditing.....	47
1.9.1 Using Cloud Eye to Monitor Cloud Connections.....	47
1.9.1.1 Overview.....	47
1.9.1.2 Cloud Connection Metrics.....	47
1.9.1.3 Viewing Cloud Connection Metrics.....	51
1.9.1.4 Creating an Alarm Rule.....	51
1.9.2 Using CTS to Record Cloud Connection Operations.....	51
1.9.2.1 Key Cloud Connection Operations.....	52
1.9.2.2 Viewing Cloud Connection Audit Logs.....	53
1.10 Quotas.....	54
<b>2 Central Network Operation Guide.....</b>	<b>56</b>
2.1 Using IAM to Grant Access to Central Networks.....	56
2.1.1 Using IAM Roles or Policies to Grant Access to Central Networks.....	56
2.1.2 Using IAM Identity Policies to Grant Access to Central Networks.....	59
2.2 Central Networks.....	61
2.2.1 Overview.....	62
2.2.2 Creating a Central Network.....	64
2.2.3 Managing Policies.....	67
2.2.4 Managing Central Network Attachments.....	70
2.2.5 Managing Cross-Site Connection Bandwidths.....	72
2.2.6 Managing Central Network Tags.....	73
2.3 Global Connection Bandwidths.....	74
2.3.1 Overview.....	75
2.3.2 Buying a Global Connection Bandwidth.....	80
2.3.3 Adding Instances to a Global Connection Bandwidth.....	82
2.3.4 Removing Instances from a Global Connection Bandwidth.....	83
2.3.5 Managing a Global Connection Bandwidth.....	84
2.4 Monitoring and Auditing.....	85
2.4.1 Using Cloud Eye to Monitor Central Network Metrics.....	85
2.4.1.1 Central Network Metrics.....	85
2.4.1.2 Viewing Central Network Metrics.....	87
2.4.1.3 Creating an Alarm Rule.....	88
2.4.2 Using Cloud Eye to Monitor Metrics on Global Connection Bandwidths.....	88
2.4.2.1 Monitoring Metrics Supported by Global Connection Bandwidths.....	89
2.4.2.2 Viewing Monitoring Metrics of a Global Connection Bandwidth.....	90
2.4.2.3 Creating an Alarm Rule.....	90
2.4.3 Using CTS to Record Key Operations on Central Networks.....	91

---

2.4.3.1 Key Central Network Operations.....	91
2.4.3.2 Viewing Central Network Audit Logs.....	92
2.5 Quotas.....	93

# 1 Cloud Connection Operation Guide

---

## 1.1 Using IAM to Grant Access to Cloud Connect

### 1.1.1 Using IAM Roles or Policies to Grant Access to Cloud Connections

System-defined permissions in [role/policy-based authorization](#) provided by [IAM](#) let you control access to Cloud Connect resources. With IAM, you can:

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

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

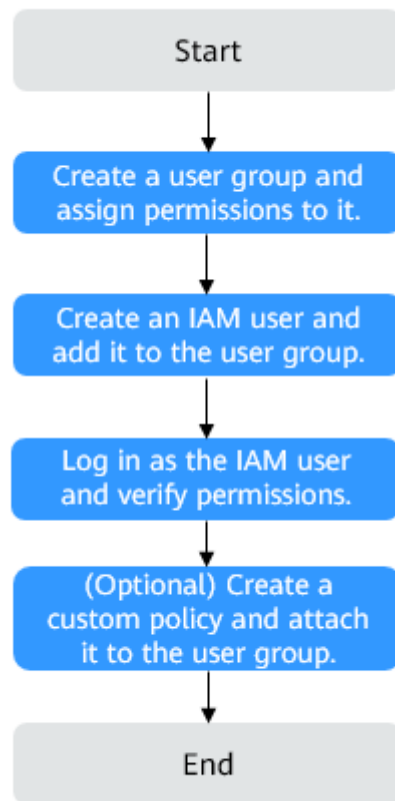
[Figure 1-1](#) shows the process of authorization with policies/roles.

#### Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in [Role/Policy-based Authorization](#) for Cloud Connect. To grant permissions for other services, learn about all [system-defined policies/roles](#) supported by IAM.

## Process Flow

**Figure 1-1** Process of granting Cloud Connect permissions using role/policy-based authorization



1. On the IAM console, **create a user group and grant it permissions** (the **Cross Connect Administrator** role as an example).
2. **Create an IAM user and add the user to the created user group.**
3. **Log in to the Cloud Connect console as the IAM user** and verify that the user only has read permissions for Cloud Connect.
  - In the service list, choose **Networking** > **Cloud Connect**. Click **Create Cloud Connection** in the upper right corner. If the cloud connection can be created, the **Cross Connect Administrator** role has taken effect.
  - Choose any other service in the service list. If a message appears indicating that you have insufficient permissions to access the service, the **Cross Connect Administrator** role is in effect.

## Example Custom Policies

Custom policies can be created to supplement system-defined policies. For the actions supported by custom policies, see [Actions Supported by Policy-based Authorization](#) in the *Cloud Connect API Reference*.

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

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

For details, see [Creating a Custom Policy](#). The following are examples of common 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 resources except deleting bandwidth packages. The following is an example of a deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "cc:bandwidthPackages:delete"
      ]
    }
  ]
}
```

- Example 3: Creating a custom policy containing multiple actions

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is a custom policy containing multiple actions:

```
{
  "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"  
    ]  
}  
]  
}
```

## 1.1.2 Using IAM Identity Policies to Grant Access to Cloud Connections

System-defined permissions [in identity policy-based authorization](#) provided by [IAM](#) let you control access to your Cloud Connect resources. With IAM, you can:

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

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

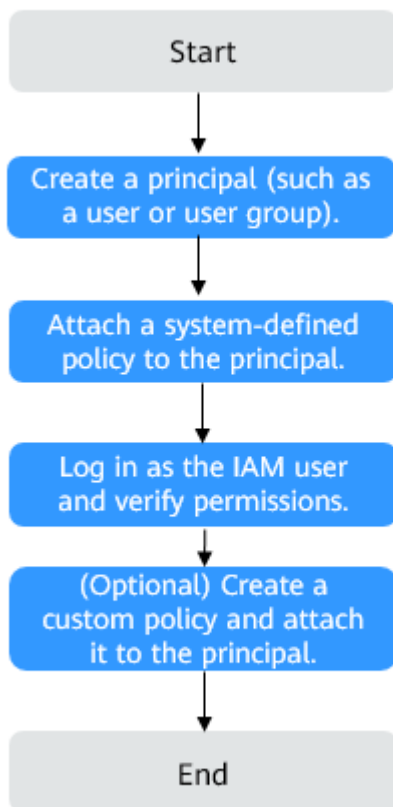
[Figure 1-2](#) shows the process flow of identity policy-based authorization.

### Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in [Identity Policy-based Authorization](#) for Cloud Connect. To grant permissions for other services, learn about all [system-defined permissions](#) supported by IAM.

## Process Flow

**Figure 1-2** Process of granting Cloud Connect permissions using identity policy-based authorization



1. On the IAM console, [create an IAM user](#) or [create a user group](#).
2. [Attach a system-defined policy](#) (**CCReadOnlyPolicy** as an example) to the user or user group.
3. [Log in as the IAM user](#) and verify permissions.  
In the authorized region, perform the following operations:
  - In the service list, choose **Networking** > **Cloud Connect**. Click **Create Cloud Connection** in the upper right corner. If the cloud connection can be created, the **CCReadOnlyPolicy** policy has taken effect.
  - Choose any other service in the service list. If a message appears indicating that you have insufficient permissions to access the service, the **CCReadOnlyPolicy** policy is in effect.

## Example Custom Policies

You can create custom identity policies to supplement the system-defined identity policies of Cloud Connect. For the actions supported for custom policies, see "Identity Policy-based Authorization" in the [Cloud Connect API Reference](#).

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

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

For details, see [Creating a Custom Policy and Attaching It to a Principal](#).

When creating a custom policy, use the Resource element to specify the resources the policy applies to and use the Condition element (condition keys) to control when the policy is in effect. For the supported resource types and condition keys, see "Identity Policy-based Authorization" in the [Cloud Connect API Reference](#).

The following are examples of common custom policies.

- Example 1: Granting permissions to create and delete cloud connections

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:cloudConnections:create",
        "cc:cloudConnections:delete"
      ]
    }
  ]
}
```

- Example 2: Creating a custom policy containing multiple actions

A custom policy can contain the actions of one or multiple services. The following is a custom policy containing multiple actions:

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:cloudConnections:create",
        "cc:cloudConnections:delete"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "vpc:vpcs:create",
        "vpc:vpcs:list"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ecs:cloudServers:createServers",
        "ecs:cloudServers:listServersDetails"
      ]
    }
  ]
}
```

## 1.2 Cloud Connections

## 1.2.1 Cloud Connection Overview

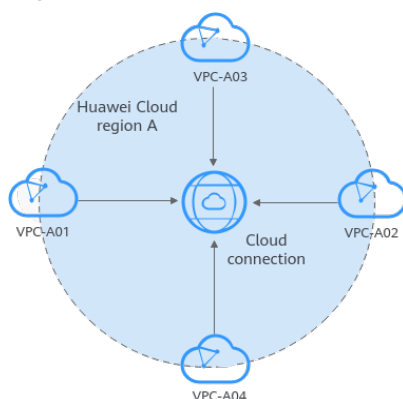
### What Is a Cloud Connection?

A cloud connection enables communication between VPCs in different regions and between VPCs and on-premises data centers.

### Cloud Connection Application Scenarios

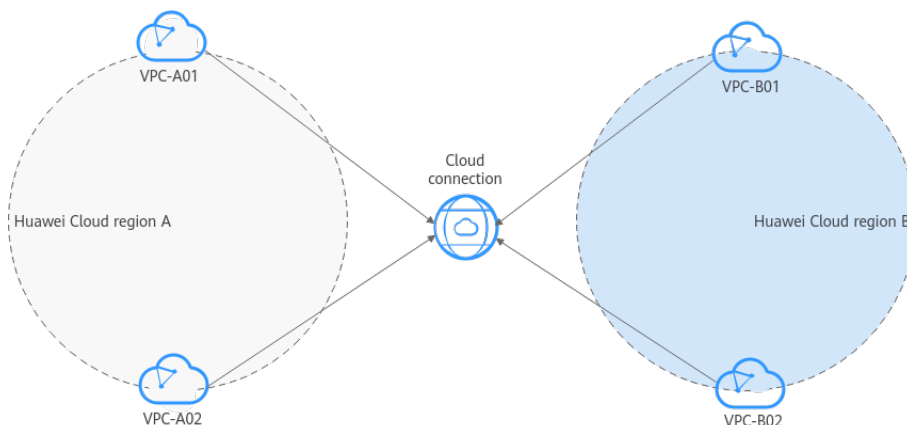
- Connecting VPCs in the same region to set up a single private network  
By default, VPCs in the same region can communicate with each other after they are loaded to a cloud connection.

**Figure 1-3** Communication between VPCs in the same region



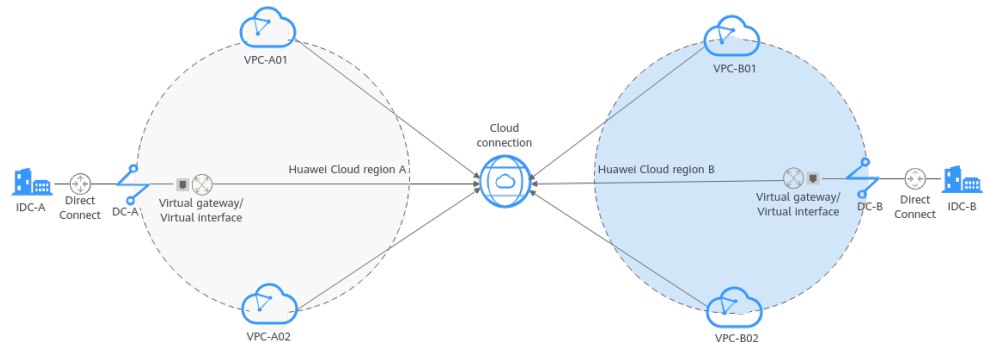
- Connecting VPCs in different regions to set up a single private network  
A cloud connection helps realize secure and reliable private network communications among VPCs in different regions in addition to improving network topology flexibility.

**Figure 1-4** Communication between VPCs in different regions



- Connecting on-premises data centers to VPCs in different regions to set up a hybrid cloud network  
If you want to establish connectivity between multiple on-premises data centers and VPCs in different regions, you can use Direct Connect to connect each data center to the corresponding VPC and then load all the virtual gateways and VPCs to a cloud connection.

**Figure 1-5** Communication between on-premises data centers and VPCs across regions



## Cloud Connection Quotas

**Table 1-1** Cloud connection quotas

Quota Type	Default Quota	Adjustable
Cloud connections allowed in each account	6	Yes <a href="#">Submit a service ticket.</a>
Regions where a cloud connection can be used	6	Yes <a href="#">Submit a service ticket.</a>
Network instances allowed in each region	6	Yes For cross-region communication, the quota can be increased to 10. <a href="#">Submit a service ticket.</a>
Bandwidth packages for each cloud connection	1	No
Routes per cloud connection	50	Yes <a href="#">Submit a service ticket.</a>

## Cloud Connection Constraints

- A cloud connection cannot be used to connect VPCs that have overlapping CIDR blocks, or communication will fail.
- If you load a VPC to a cloud connection created using the same account, you cannot enter loopback addresses, multicast addresses, or broadcast addresses for the custom CIDR block.
- If a NAT gateway has been created for any VPC you have loaded to a cloud connection, a custom CIDR block needs to be added and set to 0.0.0.0/0.
- Multiple bandwidth packages with different billing modes can be bound to a cloud connection.
- A cloud connection can only have one bandwidth package bound if the geographic region and billing mode of the bandwidth packages are the same.

## Cloud Connection Configuration Process

Figure 1-6 shows the process of connecting VPCs using a cloud connection.

Figure 1-6 Cloud connection configuration process



Table 1-2 Steps for configuring a central network

No.	Step	Description	Reference
1	Applying for a cross-border permit	If a VPC you want to connect is outside the Chinese mainland, you need to apply for a cross-border permit. Skip this step if communication across geographic regions is not required.	<a href="#">Applying for a Cross-Border Permit</a>
2	Creating a cloud connection	To enable VPCs to communicate with each other, create a cloud connection first.	<a href="#">Creating a Cloud Connection</a>
3	Loading network instances	Load the VPCs to the created cloud connection based on your network plan.	<a href="#">Loading a Network Instance to a Cloud Connection</a>
4	Buying bandwidth packages	To enable normal communication between regions in the same geographic region or different geographic regions, you need to purchase at least one bandwidth package and bind them to the cloud connection. Skip this step if communication across regions or geographic regions is not required.	<a href="#">Buying a Bandwidth Package</a>
5	Assigning inter-region bandwidths		<a href="#">Assigning an Inter-Region Bandwidth</a>

## 1.2.2 Creating a Cloud Connection

### Scenarios

To enable VPCs to communicate with each other, create a cloud connection first.

#### NOTE

For details about the regions where cloud connections are available, see [Region Availability](#).

## Creating a Cloud Connection

1. Go to the [Cloud Connections](#) page.
2. In the upper right corner of the page, click **Create Cloud Connection**.
3. Configure the parameters based on [Table 1-3](#).

**Table 1-3** Parameters for creating a cloud connection

Parameter	Description	Example Value
Name	Specifies the cloud connection name.	cc-test
Enterprise Project	Specifies the enterprise project for managing the cloud connection. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is <b>default</b> . For details about creating and managing enterprise projects, see the <a href="#">Enterprise Management User Guide</a> .	default
Scenario	Specifies whether the cloud connection is used to connect VPCs or enterprise routers. If you select <b>VPC</b> 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 up to 20 tags to a cloud connection. The tag key and value must meet the requirements listed in <a href="#">Table 1-4</a> . <b>NOTE</b> 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.	-
Description	(Optional) Provides supplementary information about the cloud connection. The description can contain no more than 255 characters and cannot contain angle brackets (<>).	-

**Table 1-4** Tag naming requirements

Parameter	Requirements	Example Value
Tag key	<p>For each resource, each tag key must be unique, and each tag key can only have one tag value.</p> <ul style="list-style-type: none"><li>• Cannot be left blank.</li><li>• Can contain no more than 128 characters.</li><li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li><li>• Cannot start with <code>_sys_</code> or a space or end with a space.</li></ul>	cc_key 1
Tag value	<ul style="list-style-type: none"><li>• Can be left blank.</li><li>• Can contain no more than 255 characters.</li><li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), slashes (/), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li><li>• Cannot start or end with a space.</li></ul>	cc-01

4. Click **OK**.

## 1.2.3 Managing Cloud Connections

### Scenarios

You can perform the following operations to manage your cloud connections:

- [Viewing a Cloud Connection](#)
- [Modifying a Cloud Connection](#)
- [Deleting a Cloud Connection](#)

### Viewing a Cloud Connection

You can view details about a cloud connection you have created.

1. Go to the [Cloud Connections](#) page.
2. View all cloud connections you have created.
3. Locate the cloud connection you want to view and click its name to view the details, such as the basic information, network instances, bandwidth packages, inter-region bandwidths, routes, and tags.

### Modifying a Cloud Connection

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

1. Go to the [Cloud Connections](#) page.
2. Locate the cloud connection you want to modify and click **Modify** in the **Operation** column.
3. In the displayed dialog box, modify the name and description of the cloud connection.
4. Click **OK**.

## Deleting a Cloud Connection

You can delete a cloud connection you no longer need.

1. Go to the [Cloud Connections](#) page.
2. Locate the cloud connection you want to delete and click **Delete** in the **Operation** column.



If network instances have been loaded to a cloud connection, it cannot be deleted. Delete all network instances loaded to the cloud connection first. For details about how to delete network instances, see [Removing a VPC from a Cloud Connection](#) and [Removing a Virtual Gateway from a Cloud Connection](#).

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

## 1.2.4 Binding or Unbinding a Bandwidth Package to and from a Cloud Connection

### Scenarios

This section describes how to bind or unbind a bandwidth package to and from a cloud connection.

Currently, Cloud Connect provides only 1 kbit/s of bandwidth for testing network connectivity. If no bandwidth package is bound, cross-region networks cannot be connected.

### Constraints

- Multiple bandwidth packages with different billing modes can be bound to a cloud connection.
- A cloud connection can only have one bandwidth package bound if the geographic region and billing mode of the bandwidth packages are the same.

### Binding a Bandwidth Package to a Cloud Connection

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Bandwidth Packages** tab.

4. Click **Bind Bandwidth Package** and select the bandwidth package to be bound.

If you have not purchased a bandwidth package, click **Buy Bandwidth Package** and then select a cloud connection. For details about how to purchase a bandwidth package, see [Buying a Bandwidth Package](#).

## Unbinding a Bandwidth Package from a Cloud Connection

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

---

**CAUTION**

Before unbinding a bandwidth package, delete all inter-region bandwidths assigned based on the bandwidth package. For details about how to delete an inter-region bandwidth, see [Deleting an Inter-Region Bandwidth](#).

---

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Bandwidth Packages** tab.
4. Locate the bandwidth package you want to unbind and click **Unbind** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

## 1.2.5 Changing the Capacity of a Bandwidth Package Bound to a Cloud Connection

### Scenarios

You can change the capacity of a bandwidth package bound to a cloud connection.

### Procedure

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Bandwidth Packages** tab.
4. Locate the bandwidth package and click **Modify Bandwidth** in the **Operation** column.
5. Set the bandwidth size as needed.
6. Confirm the configurations and select **I acknowledge the price change and agree to proceed**.
7. Click **Submit**.

## 1.2.6 Managing Cloud Connection Tags

### Scenarios

A tag is the identifier of a cloud connection and consists of a key and a value.

You can perform the following operations to manage your cloud connection tags:

- [Adding a Tag](#)
- [Editing a Tag](#)
- [Deleting a Tag](#)

### Constraints

- You can add up to 20 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. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Tags** tab.
4. In the displayed dialog box, enter a key and a value.

[Table 1-5](#) describes the tag key and value requirements.

**Table 1-5** Tag naming requirements

Parameter	Requirements	Example Value
Tag key	<p>For each resource, each tag key must be unique, and each tag key can only have one tag value.</p> <ul style="list-style-type: none"> <li>• Cannot be left blank.</li> <li>• Can contain no more than 128 characters.</li> <li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li> <li>• Cannot start with <code>_sys_</code> or a space or end with a space.</li> </ul>	cc_key1

Parameter	Requirements	Example Value
Tag value	<ul style="list-style-type: none"><li>• Can be left blank.</li><li>• Can contain no more than 255 characters.</li><li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), slashes (/), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li><li>• Cannot start or end with a space.</li></ul>	cc-01

5. Click **OK**.

## Editing a Tag

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

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Tags** tab.
4. Locate the tag and click **Edit** in the **Operation** column.
5. Enter a new value.
6. Click **OK**.

## Deleting a Tag

Delete a tag from a cloud connection.

---

**⚠ CAUTION**

Deleted tags cannot be recovered.

---

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Tags** tab.
4. Locate the tag and click **Delete** in the **Operation** column.
5. Click **OK**.

## 1.3 Cross-Border Permits

## 1.3.1 Cross-Border Permit Overview

### What Is a Cross-Border Permit?

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 communication. A cross-border permit is required if resources outside the Chinese mainland need to access your resources in the Chinese mainland.

To comply with China's laws and regulations on cross-border communication, you need to apply for a cross-border permit before you can buy a bandwidth package for communication between the Chinese mainland and another country or region. Cloud Connect is now live in four geographic regions, and a cross-border permit is required in the following scenarios:

- Communication between the Chinese mainland and Asia Pacific
- Communication between the Chinese mainland and Southern Africa
- Communication between the Chinese mainland and western Latin America

To apply for a cross-border permit, you need to prepare the required materials stamped with your company's official seal and submit an application. China Unicom will review and approve the application within one working day. After the cross-border permit is approved, you can buy bandwidth packages.

### Constraints on Cross-Border Permits

- The content of the contract for applying for the cross-border permit cannot be changed.

The *Cloud Connect Cross-Border Circuit Service Agreement* is a standard contract confirmed with China Unicom Shenzhen Branch and cannot be modified.

- The application materials cannot be downloaded, so you must keep them properly in your local PC.
- The application materials for the cross-border permit do not need to be signed and sealed by Huawei Cloud.

Huawei Cloud works with China Unicom to enable communication across borders. China Unicom provides the network circuit services and reviews and archives the application materials for cross-border permits under the requirements of the Ministry of Industry and Information Technology (MIIT).

## 1.3.2 Applying for a Cross-Border Permit

### Scenarios

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

### Constraints

- The content of the contract for applying for the cross-border permit cannot be changed.

The *Cloud Connect Cross-Border Circuit Service Agreement* is a standard contract confirmed with China Unicom Shenzhen Branch and cannot be modified.

- If the application materials for the cross-border permit are lost and cannot be retrieved locally, they must be kept properly.

## Procedure

1. Go to the [Bandwidth Packages](#) page.
2. On the displayed page, click **apply now**.

If the registered address of your business entity is in the Chinese mainland, click [here](#) to go to the **Cross-Border Service Application System** page.

If the registered address of your business entity is outside the Chinese mainland, click [here](#) to go to the **Cross-Border Service Application System** page.

### NOTE

Select the address for applying for the cross-border permit based on the registration address of your business entity.

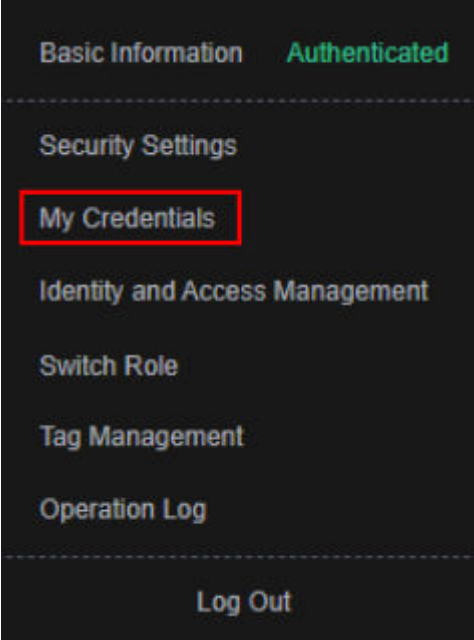
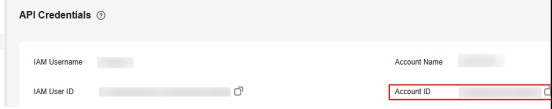
3. On the displayed page, select an applicant type, configure the parameters as prompted, and upload the required materials.

### NOTE

Prepare and upload the materials required on the application page.

**Table 1-6** Online cross-border permit application

Parameter	Description
Applicant Name	The applicant name that must be the same as the company name in the <i>Letter of Commitment to Information Security</i> .

Parameter	Description
<p>Huawei Cloud UID</p>	<p><b>The account ID, rather than the user ID or project ID. It is used to log in to the management console.</b></p> <p>You can perform the following operations to obtain your account ID.</p> <ol style="list-style-type: none"> <li>1. Log in to the management console.</li> <li>2. Move your cursor over the username in the upper right corner and select <b>My Credentials</b> from the drop-down list.</li> </ol> <p><b>Figure 1-7 My credentials</b></p>  <p><b>Figure 1-8 Obtaining the account ID</b></p>  <ol style="list-style-type: none"> <li>3. On the displayed <b>API Credentials</b> page, view <b>Account ID</b> and obtain the ID.</li> </ol>
<p>Bandwidth(M)</p>	<p>The bandwidth size, which must be the same as the bandwidth in the <i>Letter of Commitment to Information Security</i>.</p> <p>The information is for reference only and does not affect the actual service bandwidth.</p>
<p>Start Date</p>	<p>For reference only.</p>
<p>Termination Date</p>	<p>For reference only.</p>

Parameter	Description
Customer Type	The customer type. Select a type as required.
Country of the Customer	The country where the applicant is located.
Contact Name	-
Contact Number	-
Type of ID	-
ID Number	-
Scope of Business	Briefly describe the main business.
Number of Employees	For reference only.
Branch Location Country	The country where the applicant branch is located. Set this parameter as required.

**Table 1-7** Required materials

Parameter	Description	Required Material	Signature	Company Seal
Business License	Upload a photo of the business license with the official seal. For the position of the seal, see the template.	A scanned copy of your company's business license	-	√
Service Agreement	Download the <i>Huawei Cloud Cross-Border Circuit Service Agreement</i> , fill in the blank, upload the copy of agreement with the signature and official seal. <ul style="list-style-type: none"> <li>• Sign the material on the signature block.</li> <li>• Stamp the seal over the signature.</li> </ul>	A scanned copy of the <i>Huawei Cloud Cross-Border Circuit Service Agreement</i>	√	√

Parameter	Description	Required Material	Signature	Company Seal
Letter of Commitment to Information Security	<p>Download the <i>China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service</i>, fill in the blank, and upload the copy of the letter with the signature and seal.</p> <ul style="list-style-type: none"> <li>• Sign the material on the signature block.</li> <li>• Stamp the seal over the signature.</li> <li>• Specify the bandwidth you estimated and your company name.</li> </ul>	A scanned copy of the <i>China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service</i>	√	√

4. Click **Submit**.

 **NOTE**

After you submit the application, the status will change to **Pending approval**. The review takes about one working day. When the status changes to **Approved**, you can buy bandwidth packages.

### 1.3.3 Querying the Progress of the Cross-Border Permit Application

#### Scenarios

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

#### Constraints

- The application materials for the cross-border permit do not need to be signed and sealed by Huawei Cloud.

Huawei Cloud works with China Unicom to enable communication across borders. China Unicom provides the network circuit services and reviews and archives the application materials for cross-border permits under the requirements of the Ministry of Industry and Information Technology (MIIT).

#### Procedure

1. Go to the [Bandwidth Packages](#) page.

2. 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.
3. On the **Self-inquiry System** page, enter the **Huawei Cloud ID** and **Contact Number** as prompted, and click **Query**.

**NOTE**

China Unicom approves cross-border permits and provides you with the cross-border circuit services. Generally, the application for the cross-border permit will be handled within one working day.

## 1.4 Network Instances

### 1.4.1 Network Instance Overview

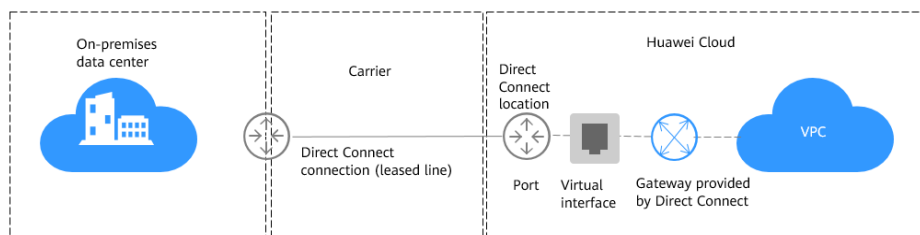
#### What Is a Network Instance?

A network instance can be a VPC or virtual gateway.

- VPCs can be connected using a cloud connection.
- If VPCs are connected by a cloud connection, virtual gateways associated with each VPC can be loaded to this cloud connection to allow the on-premises data center to communicate with these VPCs.

In Direct Connect, a virtual gateway associates a virtual interface with a VPC so that the on-premises data center can access this VPC. For more information about Direct Connect, see [What Is Direct Connect?](#)

**Figure 1-9** How Direct Connect works



#### Constraints on Network Instances

- If network instances are in the same region, they can communicate with each other by default after they are loaded to a cloud connection.
- If network instances are in different regions, purchase a bandwidth package and assign inter-region bandwidths. For details, see [Buying a Bandwidth Package](#) and [Assigning an Inter-Region Bandwidth](#).
- You can only load one network instance to a cloud connection.
- If a VPC is loaded, the associated virtual gateway cannot be loaded.
- To load a network instance in another account, you must ask that account to grant you the permission to load the network instance to your cloud connection.

- Loading 100.64.0.0/10 to a cloud connection may cause services such as OBS, DNS, and API Gateway to become unavailable.

## 1.4.2 Loading a Network Instance to a Cloud Connection

### Scenarios

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

### Constraints

- You can only load one network instance to a cloud connection.
- If a VPC is loaded, the associated virtual gateway cannot be loaded.
- To load a network instance in another account, you must ask that account to grant you the permission to load the network instance to your cloud connection.
- Loading 100.64.0.0/10 to a cloud connection may cause services such as OBS, DNS, and API Gateway to become unavailable.

### Procedure

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Network Instances** tab.
4. Click **Load Network Instance**.
  - If the network instance to be loaded is in the same account as the cloud connection, select **Current account**.

Configure the parameters based on [Table 1-8](#) and click **OK**.

**Table 1-8** Parameters for loading network instances in the current account

Parameter	Description	Example Value
Account	Specifies the account that provides the network instance. Select <b>Current account</b> .	Current account
Region	Specifies the region where the VPC you want to load is located.	CN-Hong Kong
Instance Type	Specifies the type of the network instance that needs to be loaded to the cloud connection. There are two options: <ul style="list-style-type: none"><li>• <b>VPC</b></li><li>• <b>Virtual gateway</b></li></ul> Select <b>VPC</b> .	VPC

Parameter	Description	Example Value
VPC	Specifies the VPC you want to load to the cloud connection. This parameter is mandatory if you have set <b>Instance Type</b> to <b>VPC</b> .	VPC-A
VPC CIDR Block	Specifies the subnets in the VPC you want to load and the custom CIDR blocks. If you have set <b>Instance Type</b> to <b>VPC</b> , you need to configure the following two parameters: <ul style="list-style-type: none"> <li>• <b>Subnet</b></li> <li>• <b>Other CIDR Block</b>: Add one or more custom CIDR blocks as needed.</li> </ul>	Subnet-A01
Remarks	Provides supplementary information about the network instance.	-

- If the network instance is in another account, select **Peer account**. Configure the parameters based on [Table 1-9](#) and click **OK**.

**Table 1-9** Parameters for loading a network instance in another account

Parameter	Description	Example Value
Account	Specifies the account that provides the network instance. Select <b>Peer account</b> .	Peer account
Peer Account ID	Specifies the ID of the other account.	-
Region	Specifies the region where the VPC you want to load is located.	CN-Hong Kong
Peer Project ID	Specifies the project ID of the VPC in the other account.	-
Instance Type	Specifies the type of the network instance that needs to be loaded to the cloud connection.	VPC
Peer VPC	Specifies the VPC to be loaded.	-
VPC CIDR Block	Specifies the subnets in the VPC you want to load and custom CIDR blocks.	Subnet-B01
Remarks	Provides supplementary information about the network instance.	-

5. Click **Continue Loading** to continue loading the VPCs that need to communicate with each other. Then click the **Network Instances** tab to view the VPCs you loaded.

## 1.4.3 Managing Network Instances

### Scenarios

You can perform the following operations to manage your network instances:

- [Viewing a Network Instance](#)
- [Modifying the VPC CIDR Block](#)
- [Modifying the Virtual Gateway CIDR Block](#)
- [Removing a VPC from a Cloud Connection](#)
- [Removing a Virtual Gateway from a Cloud Connection](#)

### Viewing a Network Instance

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

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Network Instances** tab.
4. Click the name of the loaded network instance. In the lower right area of the page, view its details.

### Modifying the VPC CIDR Block

You can modify the subnets in the VPC that has been loaded to a cloud connection and custom CIDR blocks.

---

**CAUTION**

Modifying the VPC CIDR block may affect the communication between the cloud connection and external networks.

When you load a VPC to a cloud connection, you can select the subnets in the VPC and specify custom CIDR blocks.

Only the subnets you select and the custom CIDR blocks you specify can be used for communication.

- 
1. Go to the [Cloud Connections](#) page.
  2. Click the name of the cloud connection to go to the **Basic Information** tab.
  3. Click the **Network Instances** tab.
  4. Locate the VPC you want to modify and click its name.
  5. In the lower right area of the page, click **Modify VPC CIDR Block**.
  6. Modify the VPC subnets or add custom CIDR blocks.

7. Click **OK**.

## Modifying the Virtual Gateway CIDR Block

You can modify the local and remote subnets configured for a virtual gateway that has been loaded to a cloud connection.

---

**CAUTION**

Modifying the virtual gateway CIDR block may affect the communication between the cloud connection and external networks.

---

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Network Instances** tab.
4. Locate the virtual gateway you want to modify and click its name.
5. In the lower right area of the page, click **Modify Virtual Gateway CIDR Block**.
6. Modify the CIDR blocks.
7. Click **OK**.

## Removing a VPC from a Cloud Connection

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

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Network Instances** tab.
4. Locate the VPC you want to remove and click its name.
5. In the lower right area of the page, click **Remove**.
6. In the displayed dialog box, click **OK**.

## Removing a Virtual Gateway from a Cloud Connection

If an on-premises data center does not need to communicate with a VPC in another region, you can remove the virtual gateway associated with the VPC.

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Network Instances** tab.
4. Locate the virtual gateway you want to remove and click its name.
5. In the lower right area of the page, click **Remove**.
6. In the displayed dialog box, click **OK**.

# 1.5 Bandwidth Packages

## 1.5.1 Bandwidth Package Overview

### What Is a Bandwidth Package?

A bandwidth package is required for communications between network instances across regions. You can assign inter-region bandwidths from a bandwidth package to enable cross-region communications.

- A bandwidth package is required for inter-region communications regardless of whether:
  - The two regions are within the same geographic region.
  - The two regions are in different geographic regions.
- Bandwidth packages are not required for communications among network instances in the same region.

#### NOTE

For details about regions and geographic regions, see [Geographic Regions and Huawei Cloud Regions](#).

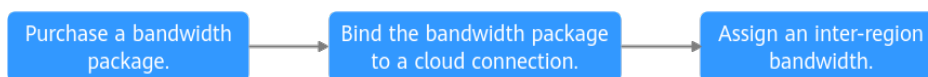
### Constraints on Bandwidth Packages

- A bandwidth package can only be bound to one cloud connection.
- A cloud connection can only have one bandwidth package bound if the geographic region and billing mode of the bandwidth packages are the same.
- 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.
- The geographic regions of a bandwidth package cannot be changed after it is purchased.

### Bandwidth Package Usage Process

**Figure 1-10** shows the process of using a bandwidth package. A bandwidth package cannot be used independently. You need to bind it to a cloud connection and assign inter-region bandwidths.

**Figure 1-10** Process of using a bandwidth package



**Table 1-10** Process of using a bandwidth package

No.	Step	Description	Reference
1	Purchase a bandwidth package.	A bandwidth package is required by a cloud connection to provide inter-region bandwidths for communications between network instances in different regions. Bandwidth packages are not required for communications between network instances in the same region.	<a href="#">Buying a Bandwidth Package</a>
2	Bind the bandwidth package to a cloud connection.	Bind the purchased bandwidth package to a cloud connection to prepare for assigning inter-region bandwidths.	<a href="#">Binding or Unbinding a Bandwidth Package to and from a Cloud Connection</a>
3	Assign an inter-region bandwidth.	Assign inter-region bandwidths for communications between network instances in different regions. If there is more than one inter-region bandwidth, the sum of all inter-region bandwidths cannot exceed the total bandwidth of the bandwidth package.	<a href="#">Assigning an Inter-Region Bandwidth</a>

## 1.5.2 Buying a Bandwidth Package

### Scenarios

To enable normal communication between regions in the same geographic region or different geographic regions, you need to purchase at least one bandwidth package and bind them to a cloud connection.

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

### Constraints

- 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.
- The geographic regions of a bandwidth package cannot be changed after it is purchased.

## Buying a Bandwidth Package

**Step 1** Go to the [Buy Bandwidth Package](#) page.

**Step 2** Configure the parameters based on [Table 1-11](#) and click **Next**.

**Table 1-11** Parameters for buying a bandwidth package

Parameter	Description	Example Value
<b>Basic Information</b>		
Billing Mode	The only option is <b>Yearly/Monthly</b> . You can purchase it by year or month as needed.	Yearly/ Monthly
Name	Specifies the bandwidth package name. The name can contain 1 to 64 characters. Only digits, letters, underscores (_), hyphens (-), and periods (.) are allowed.	bandwidthpackage-test
Enterprise Project	Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default
Tag (Optional)	Identifies the bandwidth package. A tag consists of a key and a value. You can add 20 tags to a bandwidth package. The tag key and value must meet the requirements listed in <a href="#">Table 1-12</a> . <b>NOTE</b> 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 <a href="#">Predefined Tags</a> .	-
<b>Bandwidth Details</b>		
Billed By	Specifies how you want the bandwidth package to be billed.	Bandwidth
Applicability	Specifies whether you want to use the bandwidth package for communication within a geographic region or between geographic regions. There are two options: <ul style="list-style-type: none"> <li>• <b>Single geographic region:</b> Use the bandwidth package between regions in the same geographic region.</li> <li>• <b>Across geographic regions:</b> Use the bandwidth package between regions in different geographic regions.</li> </ul>	Single geographic region
Geographic Region	Specifies the geographic regions.	Chinese mainland

Parameter	Description	Example Value
Bandwidth (Mbit/s)	Specifies the bandwidth you require for communication between 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. Unit: Mbit/s	10
Required Duration	Specifies how long you require the bandwidth package for. Auto renewal is supported.	1
Cloud Connection	Specifies the cloud connection you want to bind the bandwidth package to. There are two options: <ul style="list-style-type: none"> <li>• <b>Bind now</b></li> <li>• <b>Bind later</b></li> </ul>	Bind later

**Table 1-12** Tag naming requirements

Parameter	Requirements	Example Value
Tag key	For each resource, each tag key must be unique, and each tag key can only have one tag value. <ul style="list-style-type: none"> <li>• Cannot be left blank.</li> <li>• Can contain no more than 128 characters.</li> <li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li> <li>• Cannot start with _sys_ or a space or end with a space.</li> </ul>	bandwidthpackage_key1
Tag value	<ul style="list-style-type: none"> <li>• Can be left blank.</li> <li>• Can contain no more than 255 characters.</li> <li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), slashes (/), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li> <li>• Cannot start or end with a space.</li> </ul>	bandwidthpackage-01

**Step 3** Confirm the configuration and submit your order.

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 the cloud connection.

After purchasing a bandwidth package, you must bind it to the corresponding cloud connection by referring to [Binding or Unbinding a Bandwidth Package to and from a Cloud Connection](#).

----End

## 1.5.3 Binding or Unbinding a Bandwidth Package to and from a Cloud Connection

### Scenarios

Bind a bandwidth package to a cloud connection or unbind a bandwidth package from a cloud connection.

- [Binding a Bandwidth Package to a Cloud Connection](#)
- [Unbinding a Bandwidth Package from a Cloud Connection](#)

### Constraints

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

### Binding a Bandwidth Package to a Cloud Connection

1. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package you want to bind and click **Bind** in the **Operation** column.
3. Select the cloud connection you want to bind the bandwidth package to.
4. Click **OK**.

After a bandwidth package is bound to a cloud connection, you need to assign inter-region bandwidths. For details, see [Assigning an Inter-Region Bandwidth](#).

### Unbinding a Bandwidth Package from a Cloud Connection

If you no longer need a bandwidth package, you can unbind it from the cloud connection.

---

**CAUTION**

All inter-region bandwidths assigned based on the bandwidth package have been deleted. For details about how to delete an inter-region bandwidth, see [Deleting an Inter-Region Bandwidth](#).

---

1. Go to the [Bandwidth Packages](#) page.

2. Locate the bandwidth package you want to unbind and click **Unbind** in the **Operation** column.
3. In the displayed dialog box, click **OK**.

## 1.5.4 Managing Bandwidth Packages

You can perform the following operations to manage your bandwidth packages:

- [Changing the Capacity of a Bandwidth Package](#)
- [Changing a Pay-per-Use Bandwidth Package to a Yearly/Monthly Bandwidth Package](#)
- [Unsubscribing from a Yearly/Monthly Bandwidth Package](#)
- [Deleting a Pay-per-Use Bandwidth Package](#)

### Changing the Capacity of a Bandwidth Package

After a bandwidth package is purchased, you can modify its bandwidth.

1. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package and click **Modify Bandwidth** in the **Operation** column.
3. Set the bandwidth size as needed.
4. Confirm the configurations and select **I acknowledge the price change and agree to proceed**.
5. Click **Submit**.

Once you modify the bandwidth package, modify the inter-region bandwidths on the central network to apply these changes to the cross-region network communications. For details, see [Assigning an Inter-Region Bandwidth](#).

---

**CAUTION**

- Modifying the bandwidth does not interrupt services.
  - If bandwidth package is going to expire within 24 hours, you cannot increase or decrease the bandwidth.
- 

### Changing a Pay-per-Use Bandwidth Package to a Yearly/Monthly Bandwidth Package

You can change the billing mode of a bandwidth package from pay-per-use to yearly/monthly.

1. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package and click **More > Change Billing Mode**.
3. In the displayed dialog box, click **OK**.
4. On the **Change Subscription** page, set the required duration and click **Pay**.
5. On the displayed page, select a payment method and click **OK**.

## Unsubscribing from a Yearly/Monthly Bandwidth Package

You can unsubscribe from a yearly/monthly bandwidth package if you no longer need it.

---

**CAUTION**

Before unsubscribing from a yearly/monthly bandwidth package, you need to unbind it from the cloud connection. For details, see [Unbinding a Bandwidth Package from a Cloud Connection](#).

1. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package you want to unsubscribe from and choose **More > Unsubscribe** in the **Operation** column.
3. On the displayed page, confirm the resource and refund amount, select the unsubscription reason, and select **I've backed up the data or confirmed that the unsubscribed resources are no longer needed. I understand that only resources in the recycle bin can be restored after unsubscription.**
4. Click **Unsubscribe**.
5. In the displayed dialog box, click **Unsubscribe** to unsubscribe from the bandwidth package.

## Deleting a Pay-per-Use Bandwidth Package

Currently, pay-per-use bandwidth packages are only for trial use. You can delete a bandwidth package if you no longer need it.

---

**CAUTION**

Before deleting a pay-per-use bandwidth package, unbind it from the cloud connection. For details, see [Unbinding a Bandwidth Package from a Cloud Connection](#).

1. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package you want to delete and choose **More > Delete** in the **Operation** column.
3. In the displayed dialog box, click **OK**.

## 1.5.5 Managing Bandwidth Package Tags

### Scenarios

A tag is an identifier of a bandwidth package and consists of a key and a value.

You can perform the following operations to manage your bandwidth package tags:

- [Adding a Tag](#)

- [Editing a Tag](#)
- [Deleting a Tag](#)

## Constraints

- You can add up to 20 tags to a bandwidth package.
- 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. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package and click its name to go to the details page.
3. Click the **Tags** tab.
4. Click **Add Tag**.
5. In the displayed dialog box, enter a key and a value.

[Table 1-13](#) describes the tag key and value requirements.

**Table 1-13** Tag naming requirements

Parameter	Requirements	Example Value
Tag key	<p>For each resource, each tag key must be unique, and each tag key can only have one tag value.</p> <ul style="list-style-type: none"><li>• Cannot be left blank.</li><li>• Can contain no more than 128 characters.</li><li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li><li>• Cannot start with <code>_sys_</code> or a space or end with a space.</li></ul>	bandwidthpackage_key1
Tag value	<ul style="list-style-type: none"><li>• Can be left blank.</li><li>• Can contain no more than 255 characters.</li><li>• Can contain letters in any language, digits, spaces, underscores (_), periods (.), colons (:), slashes (/), equal signs (=), plus signs (+), minus signs (-), and at signs (@).</li><li>• Cannot start or end with a space.</li></ul>	bandwidthpackage-01

6. Click **OK**.

## Editing a Tag

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

1. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package and click its name to go to the details page.
3. Click the **Tags** tab.
4. Locate the tag and click **Edit** in the **Operation** column.
5. In the displayed dialog box, modify the tag value as needed.
6. Click **OK**.

## Deleting a Tag

Delete a tag from a bandwidth package.



Deleted tags cannot be recovered.

---

1. Go to the [Bandwidth Packages](#) page.
2. Locate the bandwidth package and click its name to go to the details page.
3. Click the **Tags** tab.
4. Locate the tag and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

# 1.6 Inter-Region Bandwidths

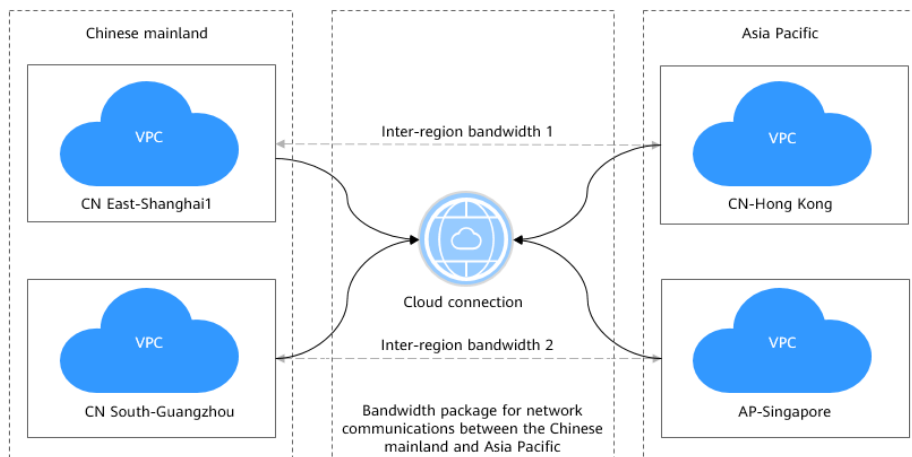
## 1.6.1 Inter-Region Bandwidth Overview

### What Is an Inter-Region Bandwidth?

An inter-region bandwidth is used for communications between regions. Inter-region bandwidths are assigned from a bandwidth package for cross-region communications. If there is more than one inter-region bandwidth, the sum of all inter-region bandwidths cannot exceed the total bandwidth of the bandwidth package.

In [Figure 1-11](#), two inter-region bandwidths are assigned from the bandwidth package for communications between the Chinese mainland and Asia Pacific. The sum of the two inter-region bandwidths cannot exceed the maximum bandwidth of the bandwidth package.

**Figure 1-11** Bandwidth packages and inter-region bandwidths for communications between geographic regions



### Constraints on Inter-Region Bandwidths

- To allow you to test network connectivity between regions, Cloud Connect provides 10 kbit/s by default. To test network connectivity, you can ping an ECS in one VPC from an ECS in the other VPC.
- If network instances are in the same region, they can communicate with each other by default after they are loaded to one cloud connection.

### Process of Using an Inter-Region Bandwidth

**Figure 1-12** shows the process of using an inter-region bandwidth. An inter-region bandwidth is used for communications between network instances across regions. After you purchase a bandwidth package and bind it to a cloud connection, you need to assign an inter-region bandwidth.

**Figure 1-12** Process of using an inter-region bandwidth



## 1.6.2 Assigning an Inter-Region Bandwidth

### Scenarios

By default, a cloud connection provides 10 kbit/s of bandwidth for testing cross-region network connectivity.

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

## Constraints

- If network instances are in the same region, they can communicate with each other by default after they are loaded to one cloud connection.
- To allow cross-region communications, you need to assign an inter-region bandwidth. Before assigning an inter-region bandwidth, ensure that you have purchased a bandwidth package and bound it to the target cloud connection. For details, see [Buying a Bandwidth Package](#) and [Binding or Unbinding a Bandwidth Package to and from a Cloud Connection](#).

## Assigning an Inter-Region Bandwidth

- Step 1** Go to the [Cloud Connections](#) page.
- Step 2** Click the name of the cloud connection to go to the **Basic Information** tab.
- Step 3** Click the **Inter-Region Bandwidths** tab.
- Step 4** Click **Assign Inter-Region Bandwidth** and configure the parameters based on [Table 1-14](#).

**Table 1-14** Parameters required for assigning an inter-region bandwidth

Parameter	Description	Example Value
Regions	Specifies the regions of the network instances that need to communicate with each other. Select two regions.	CN-Hong Kong CN North-Ulanqab1
Bandwidth Package	Specifies the purchased bandwidth package that will be bound to the cloud connection.	bandwidthpackage-test
Bandwidth	Specifies the bandwidth you require for communication between regions, in Mbit/s. The sum of all inter-region bandwidths you assign cannot exceed the total bandwidth of the bandwidth package. Plan the bandwidth in advance.	10

- Step 5** Click **OK**.

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

### NOTE

The default security group rules deny all the inbound traffic. Ensure that security group rules in both directions are correctly configured for resources in the regions to ensure normal communication.

----End

## 1.6.3 Managing Inter-Region Bandwidths

### Scenarios

You can perform the following operations to manage your inter-region bandwidths:

- [Viewing Inter-Region Bandwidths](#)
- [Modifying an Inter-Region Bandwidth](#)
- [Deleting an Inter-Region Bandwidth](#)

### Viewing Inter-Region Bandwidths

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

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Inter-Region Bandwidths** tab.
4. View the inter-region bandwidths assigned for the cloud connection.

### Modifying an Inter-Region Bandwidth

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

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Inter-Region Bandwidths** tab.
4. Locate the inter-region bandwidth you want to modify and click **Modify** in the **Operation** column.
5. Modify the bandwidth and click **OK**.

### Deleting an Inter-Region Bandwidth

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

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Inter-Region Bandwidths** tab.
4. Locate the inter-region bandwidth you want to delete and click **Delete** in the **Operation** column.
5. In the displayed dialog box, click **OK**.

## 1.6.4 Viewing 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. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Inter-Region Bandwidths** tab.
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.

# 1.7 Cross-Account Authorization

## 1.7.1 Cross-Account Authorization Overview

### Cross-Account Authorization

Cross-account authorization allows an account (account A) to authorize another account (account B) to use its cloud service resources. Even if account A does not allow access to a specific cloud service, account B can still use the cloud service resources that have been authorized by account A. For example, you can share the resources through Random Access Memory (RAM) or access the resources through cross-account authorization. This authorization mechanism allows different accounts to share and collaborate on using cloud resources while maintaining independence and security.

### Constraints on Cross-Account Authorization

- You can share your network instances with other accounts, or have them share theirs with you.
- Only VPCs can be authorized. A VPC can only be loaded to one cloud connection.

## 1.7.2 Authorizing Network Instances

### Scenarios

Allow another account to use network instances in your account or load network instances authorized by another account to the cloud connection in your account.

### Constraints

- You can share your network instances with other accounts, or have them share theirs with you.
- Only VPCs can be authorized. A VPC can only be loaded to one cloud connection.

## Authorizing Another Account to Use Network Instances in Your Account

You can grant other accounts the permissions to load the VPCs in your account to their cloud connection.

- Step 1** Go to the [Cross-Account Authorization](#) page.
- Step 2** On the **Network Instances Authorized by Me** tab, click **Authorize Network Instance**.
- Step 3** Configure the parameters based on [Table 1-15](#).

**Figure 1-13** Cross-account authorization

**Authorize Network Instance** [Close]

**!** Each VPC can be authorized only to one peer account and peer cloud connection. The peer account can load the authorized VPC onto the specified cloud connection, allowing communication between your network and the peer account's network.

\* Region: [Dropdown]

\* VPC <sup>?</sup>: [--Select--] [Search]

\* Peer Account ID <sup>?</sup>: [Text Input]

\* Peer Cloud Connection ID: [Text Input]

Remarks: [Text Area] 0/64

[Cancel] [OK]

**Table 1-15** Parameters for cross-account authorization

Parameter	Description	Example Value
Region	Specifies the region where the VPC is located.	CN-Hong Kong
VPC	Specifies the VPC you want to authorize.	VPC-A
Peer Account ID	Specifies the ID of the peer account. To obtain the account ID, log in to the management console using the peer account. In the drop-down list of the username in the upper right corner, click <b>My Credentials</b> . On the <b>API Credentials</b> page, copy the account ID.	-
Peer Cloud Connection ID	Specifies the ID of the peer cloud connection that the VPC is to be loaded to. For details about how to obtain the cloud connection ID, see <a href="#">Viewing a Cloud Connection</a> .	-
Remarks	Provides supplementary information about cross-account authorization.	-

**Step 4** Click **OK**.

----End

## Loading Network Instances in Other Accounts to the Cloud Connection in Your Account

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

1. Go to the [Cross-Account Authorization](#) page.
2. Click the **Network Instances Authorized to Me** tab.
3. Locate the network instance and click **Load to Cloud Connection** in the **Operation** column.
4. Configure the parameters based on [Table 1-16](#).

**Table 1-16** Parameters for loading a VPC to a cloud connection

Parameter	Description	Example Value
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.	CN-Hong Kong
Instance Type	Specifies the type of the network instance you can load. Only VPCs can be loaded.	VPC
Peer VPC	Specifies the ID of the VPC to be loaded. For details about how to obtain the VPC ID, see <a href="#">Obtaining a VPC ID</a> .	-
VPC CIDR Block	Specifies the subnets of the VPC you want to load and the custom CIDR blocks.	-

5. Click **OK**.

You can view the loaded VPC on the **Network Instances** tab. For details, see [Managing Network Instances](#).

### 1.7.3 Managing Cross-Account Authorization

#### Scenarios

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

If you do not want other accounts to use the network instances in your account, you can cancel the authorization.

You can perform the following operations:

- [Viewing the VPCs that Can Be Loaded to the Cloud Connections in Other Accounts](#)
- [Viewing the VPCs that Other Accounts Allow You to Load](#)
- [Canceling Cross-Account Authorization](#)

## Viewing the VPCs that Can Be Loaded to the Cloud Connections in Other Accounts

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

1. Go to the [Cross-Account Authorization](#) page.
2. In the search area above the list, you can search for network instances by attribute or enter a keyword to search for the target network instance.

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

You can view the VPCs that other accounts have allowed you to load to your cloud connection.

1. Go to the [Cross-Account Authorization](#) page.
2. Click the **Network Instances Authorized to Me** tab.
3. In the search area above the list, you can search for network instances by attribute or enter a keyword to search for the target network instance.

## Canceling Cross-Account Authorization

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

1. Go to the [Cross-Account Authorization](#) page.
2. On the **Network Instances Authorized by Me** tab, locate the network instance and click **Cancel Authorization** in the **Operation** column.
3. In the displayed dialog box, click **OK**.

### NOTE

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

## 1.8 Route Information

## 1.8.1 Route Overview

### What Is a Route?

You can add routes to both default and custom route tables and configure the destination, next hop type, and next hop for the routes to determine where network traffic is directed. Routes are classified into system routes and custom routes.

- **System route:** A system route is automatically added by the VPC service or other services (such as VPN and Direct Connect) and cannot be deleted or modified.

Each route table comes with routes whose next hops are Local. Generally, a route table contains the following local routes:

- Routes whose destination is 100.64.0.0/10, which is used to deploy public services, for example, the DNS servers. The route directs instances in a subnet to access these services.
- Routes whose destination is 198.19.128.0/20 (IP address range used by internal services, such as VPC Endpoint).
- Routes whose destination is 127.0.0.0/8 (local loopback addresses)
- Routes whose destination is a subnet CIDR block that enables instances in a VPC to communicate with each other.

If you enable IPv6 when creating a subnet, the system automatically assigns an IPv6 CIDR block to the subnet. Then, you can view IPv6 routes in its route table. Example destinations of subnet CIDR blocks are as follows:

- IPv4: 192.168.2.0/24
  - IPv6: 2407:c080:802:be7::/64
- **Custom route:** After a route table is created, you can add custom routes and configure information such as the destination and next hop in the route to determine where network traffic is directed. In addition to manually added custom routes, there are custom routes added by other cloud services, such as Cloud Container Engine (CCE) or NAT Gateway.

Route tables include default route tables and custom route tables. They support the next hop types described in [Table 1-17](#) and [Table 1-18](#). The default route table supports fewer next hop types than a custom route table. This is because services like VPN, Direct Connect, and Cloud Connect automatically add routes to the default table.

**Table 1-17** Next hop types supported by the default route table

Next Hop Type	Description
Server	Traffic intended for the destination is forwarded to an ECS in the VPC.
Extended network interface	Traffic intended for the destination is forwarded to the extended network interface of an ECS in the VPC.

Next Hop Type	Description
Supplementary network interface	Traffic intended for the destination is forwarded to the supplementary network interface of an ECS in the VPC.
NAT gateway	Traffic intended for the destination is forwarded to a NAT gateway.
VPC peering connection	Traffic intended for the destination is forwarded to a VPC peering connection.
Virtual IP address	Traffic intended for the destination is forwarded to a virtual IP address and then sent to active and standby ECSs to which the virtual IP address is bound.
VPC endpoint	Traffic intended for the destination is forwarded to a VPC endpoint.
Cloud container	Traffic intended for the destination is forwarded to a cloud container.
Enterprise router	Traffic intended for the destination is forwarded to an enterprise router.
Cloud firewall	Traffic intended for the destination is forwarded to a cloud firewall.
Global internet gateway	Traffic intended for the destination is forwarded to a global internet gateway.

**Table 1-18** Next hop types supported by a custom route table

Next Hop Type	Description
Server	Traffic intended for the destination is forwarded to an ECS in the VPC.
Extended network interface	Traffic intended for the destination is forwarded to the extended network interface of an ECS in the VPC.
BMS user-defined network	Traffic intended for the destination is forwarded to a BMS user-defined network.
VPN gateway	Traffic intended for the destination is forwarded to a VPN gateway.
Gateway provided by Direct Connect	Traffic intended for the destination is forwarded to a gateway provided by Direct Connect.
Cloud connection	Traffic intended for the destination is forwarded to a cloud connection.

Next Hop Type	Description
Supplementary network interface	Traffic intended for the destination is forwarded to the supplementary network interface of an ECS in the VPC.
NAT gateway	Traffic intended for the destination is forwarded to a NAT gateway.
VPC peering connection	Traffic intended for the destination is forwarded to a VPC peering connection.
Virtual IP address	Traffic intended for the destination is forwarded to a virtual IP address and then sent to active and standby ECSs to which the virtual IP address is bound.
VPC endpoint	Traffic intended for the destination is forwarded to a VPC endpoint.
Cloud container	Traffic intended for the destination is forwarded to a cloud container.
Enterprise router	Traffic intended for the destination is forwarded to an enterprise router.
Cloud firewall	Traffic intended for the destination is forwarded to a cloud firewall.
Global internet gateway	Traffic intended for the destination is forwarded to a global internet gateway.

#### NOTE

If you specify the destination when creating a resource, a system route is delivered. If you do not specify a destination when creating a resource, a custom route that can be modified or deleted is delivered.

For example, when you create a NAT gateway, a custom route is automatically delivered without a specific destination (0.0.0.0/0 is used by default). In this case, you can change the destination. However, when you create a VPN gateway, you need to specify the remote subnet, which is the destination of a route. A system route will be delivered. Do not modify the route destination on the **Route Tables** page. If you do, the destination will be inconsistent with the configured remote subnet. To modify the route destination, go to the specific resource page and modify the remote subnet, then the route destination will be changed accordingly.

You cannot add a route whose next hop type is **VPC endpoint** or **Cloud container** to a route table. These routes are automatically added by the VPC Endpoint or CCE service.

## Constraints on Routes

When you create a VPC, a default route table is automatically generated for the VPC. You can also create a custom route table.

- A VPC can be associated with a maximum of five route tables, including the default route table and four custom route tables.

- All route tables in a VPC can have a maximum of 1,000 routes. System routes do not occupy the quota.

In each VPC route table, there are local routes and custom routes.

- Generally, the destination of a custom route cannot overlap with that of a local route. The destination of a local route can be a subnet CIDR block and CIDR blocks that are used for internal communications.
- You cannot add two routes with the same destination to a VPC route table even if their next hop types are different.
- When adding routes to a VPC route table, remember the route priority described in [Table 1-19](#).

**Table 1-19** Route priorities

Route Priority	Description
Local routes preferentially matched	A local route is the default route for communications within a VPC. They have the highest priority.
Most accurate route (longest prefix match)	<p>If there are multiple routes that match the request destination, the longest prefix match routing is used. This means the route that has the longest subnet mask is preferentially used to determine the next hop.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• A request is destined for 192.168.1.12/32.</li> <li>• The destination of route A is 192.168.0.0/16, with an ECS (ECS-A) as the next hop.</li> <li>• The destination of route B is 192.168.1.0/24, with a VPC peering connection as the next hop.</li> </ul> <p>According to the longest prefix match routing rule, the request preferentially matches route B and will be forwarded to the VPC peering connection.</p>
EIP	<p>If the default route in the route table points to 0.0.0.0/0 and an ECS in the subnet has an EIP bound, the EIP has a higher priority. In this case, the EIP is used to access the Internet by default.</p> <p>Example:</p> <ul style="list-style-type: none"> <li>• The destination of route A is 0.0.0.0/0, with a NAT gateway as the next hop.</li> <li>• An ECS in a VPC subnet has an EIP bound.</li> </ul> <p>In this case, the ECS will use the EIP to access the Internet instead of using the NAT gateway.</p>

## 1.8.2 Modifying the VPC CIDR Block

### Scenarios

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

### Precautions

Modifying the VPC CIDR block may affect the communication between the cloud connection and external networks. Exercise caution when performing this operation.

When you load a VPC to a cloud connection, you can select the subnets in the VPC and specify custom CIDR blocks.

Only the subnets you select and the custom CIDR blocks you specify can be used for communication.

The following uses an example to explain this.

Suppose that there are two VPCs (VPC-A and VPC-B), each in a separate region. A cloud connection has been created to enable communication between the two VPCs. VPC-A has two subnets: subnet 1 and subnet 2. If only subnet 1 is selected when VPC-A is loaded to the cloud connection, only subnet 1 can communicate with VPC-B, and subnet 2 cannot communicate with VPC-B. To enable communication between subnet 2 in VPC-A and VPC-B, you need to select subnet 2 and deselect subnet 1 for VPC-A. In this way, subnet 2 can communicate with VPC-B, and subnet 1 cannot communicate with VPC-B.

### Procedure

1. Go to the [Cloud Connections](#) page.
2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Network Instances** tab.
4. Locate the VPC you want to modify.
5. In the lower right area of the page, click **Modify VPC CIDR Block**.
6. Modify the VPC subnets or add custom CIDR blocks.
7. Click **OK**.

## 1.8.3 Viewing Cloud Connection Routes

### Scenarios

You can view the routes of a cloud connection.

### Procedure

1. Go to the [Cloud Connections](#) page.

2. Click the name of the cloud connection to go to the **Basic Information** tab.
3. Click the **Route Information** tab. All routes of the cloud connection are displayed.
4. In the search area above the list, you can search for routes by attribute or enter a keyword to search for the target route.

## 1.9 Monitoring and Auditing

### 1.9.1 Using Cloud Eye to Monitor Cloud Connections

#### 1.9.1.1 Overview

Monitoring is key to ensuring the performance, reliability, and availability of a cloud service. Monitoring provides you with data on cloud connections. You can use Cloud Eye to track the status of cloud connections. 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 connections.

For more information, see the following:

- [Monitoring Metrics](#)
- [Setting an Alarm Rule](#)
- [Viewing Cloud Connection Metrics](#)

#### 1.9.1.2 Cloud Connection Metrics

##### Description

The table describes monitored metrics reported by cloud connections 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 connections.

##### Namespace

SYS.CC

## Metrics

**Table 1-20** Cloud connection metrics

ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval
network_incoming_bits_rate	Network Incoming Bandwidth	Bit rate for inbound data to a region from another region of a cloud connection	$\geq 0$	bits/s	1000 (SI)	Inter-region bandwidth	1 minute
network_outgoing_bits_rate	Network Outgoing Bandwidth	Bit rate for outbound data from a region to another region of a cloud connection	$\geq 0$	bits/s	1000 (SI)	Inter-region bandwidth	1 minute
network_incoming_bytes	Network Incoming Traffic	Number of bytes for inbound data to a region from another region of a cloud connection	$\geq 0$	bytes	1024 (IEC)	Inter-region bandwidth	1 minute
network_outgoing_bytes	Network Outgoing Traffic	Number of bytes for outbound data from a region to another region of a cloud connection	$\geq 0$	bytes	1024 (IEC)	Inter-region bandwidth	1 minute

ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval
network_incoming_packets_rate	Network Incoming Packet Rate	Packet rate for inbound data to a region from another region of a cloud connection	$\geq 0$	packets/s	N/A	Inter-region bandwidth	1 minute
network_outgoing_packets_rate	Network Outgoing Packet Rate	Packet rate for outbound data from a region to another region of a cloud connection	$\geq 0$	packets/s	N/A	Inter-region bandwidth	1 minute
network_incoming_packets	Network Incoming Packets	Number of packets for inbound data to a region from another region of a cloud connection	$\geq 0$	packets	N/A	Inter-region bandwidth	1 minute
network_outgoing_packets	Network Outgoing Packets	Number of packets for outbound data from a region to another region of a cloud connection	$\geq 0$	packets	N/A	Inter-region bandwidth	1 minute
network_bandwidth_usage	Network Bandwidth Usage	Utilization of an inter-region bandwidth assigned to a cloud connection	0-100	%	N/A	Inter-region bandwidth	1 minute

ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval
network_bandwidth	Network Bandwidth	Inter-region bandwidth of a cloud connection	≥ 0	bits/s	1000 (SI)	Inter-region bandwidth	1 minute

 **NOTE**

Metrics in certain regions are monitored every 5 minutes. Check the console for the exact monitoring interval.

## Dimensions

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

If a monitored object has multiple dimensions, all dimensions are mandatory when you use APIs to query the metrics.

- Query a single metric:

```
dim.0=cloud_connect_id%2Ca92ab2f75d844dbebbc3fcc7871d1136&dim.1=bwp_id%2C625db750db7b1447d0c9d1a447c11903&dim.2=region_bandwidth_id%2Ce2cc9dc0b4954fbbaf1299f2727fe1ca.
```
- Query multiple metrics:

```
"dimensions": [
  {
    "name": "cloud_connect_id",
    "value": "a92ab2f75d844dbebbc3fcc7871d1136"
  },
  {
    "name": "bwp_id",
    "value": "625db750db7b1447d0c9d1a447c11903"
  },
  {
    "name": "region_bandwidth_id",
    "value": "e2cc9dc0b4954fbbaf1299f2727fe1ca"
  }
],
```

### 1.9.1.3 Viewing Cloud Connection Metrics

#### Scenarios

You can view cloud connection metrics on the Cloud Eye console.

#### Procedure

**Step 1** Go to the [Overview](#) page.

**Step 2** In the navigation pane on the left, choose **Cloud Service Monitoring**. Then click **Cloud Connect CC**.

The page that shows the Cloud Connect monitoring details is displayed.

**Step 3** On the **Resources** tab, locate the cloud connection and click **View Metric** in the **Operation** column to view the metrics.

#### NOTE

For details about querying metrics, see [Querying Cloud Service Monitoring Metrics](#).

----End

### 1.9.1.4 Creating an Alarm Rule

#### Scenarios

This section describes how to create alarm rules and notifications for cloud connections.

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

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

#### Procedure

1. Go to the [Alarm Rules](#) page.
2. Click **Create Alarm Rule** or modify an existing alarm rule.
3. Configure the parameters and then click **Create**.

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

#### NOTE

For more information about cloud connection alarm rules, see [Cloud Eye User Guide](#).

## 1.9.2 Using CTS to Record Cloud Connection Operations

## 1.9.2.1 Key Cloud Connection Operations

### Scenarios

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

### Prerequisites

You have enabled CTS.

### Key Operations Recorded by CTS

**Table 1-21** 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
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

Operation	Resource	Trace
Unbinding a bandwidth package	bandwidthPackage	disassociateBandwidth-Package
Creating cross-account authorization	authorisation	createAuthorisation
Updating cross-account authorization	authorisation	updateAuthorisation
Canceling cross-account authorization	authorisation	deleteAuthorisation



## 1.9.2.2 Viewing Cloud Connection Audit Logs

### 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.

## 1.10 Quotas

### What Is Quota?

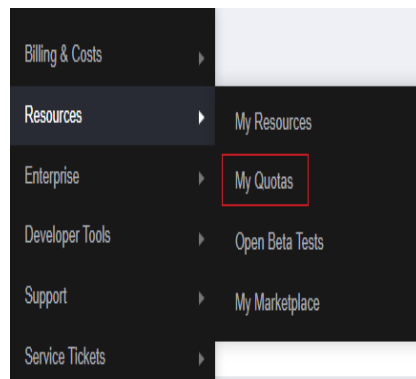
Quotas can limit the number of resources available to users, such as the maximum number of ECS or EVS disks that can be created.

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

### How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**. The **Quotas** page is displayed.

**Figure 1-14** My Quotas

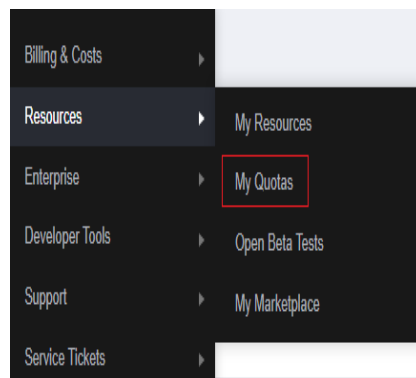


3. View the used and total quota of each type of resources on the displayed page.  
If a quota cannot meet service requirements, apply for a higher quota.

### How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**. The **Quotas** page is displayed.

**Figure 1-15** My Quotas



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

**Figure 1-16** Increasing quota

Service	Resource Type	Used Quota	Total Quota
Elastic Cloud Server	ECSs	1	
	VCPUs	4	
	Memory (MB)		
Dedicated Host	c3_pro	0	
	s6	0	
	c6_pro	0	
	s6_pro	0	
Image Management Service	m3	0	
	Images	1	
FunctionGraph	Function	0	
	Code storage(MB)	0	
Auto Scaling	Auto scaling groups	0	
	Auto scaling configuration	0	

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**.

# 2 Central Network Operation Guide

---

## 2.1 Using IAM to Grant Access to Central Networks

### 2.1.1 Using IAM Roles or Policies to Grant Access to Central Networks

System-defined permissions in [role/policy-based authorization](#) provided by [IAM](#) let you control access to central networks. With IAM, you can:

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

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

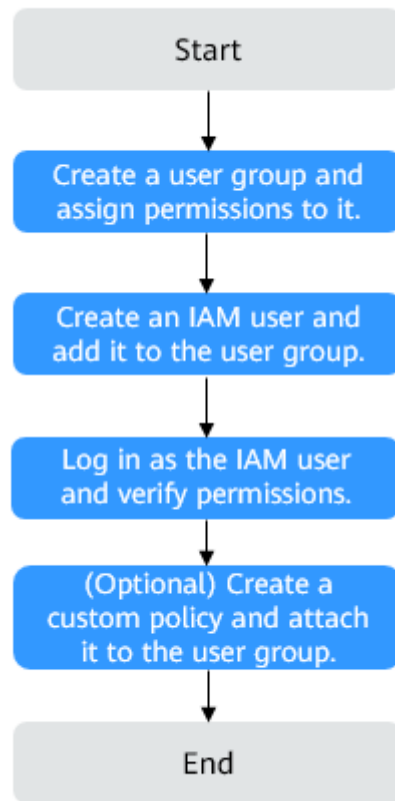
[Figure 2-1](#) shows the process of authorization with policies/roles.

#### Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in [Role/Policy-based Authorization](#) for Cloud Connect. To grant permissions for other services, learn about all [system-defined permissions](#) supported by IAM.

## Process Flow

**Figure 2-1** Process of granting Cloud Connect permissions using role/policy-based authorization



1. **Create a user group and grant 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 and add it to the created user group.**  
On the IAM console, create a user and add it to the user group created in 1.
3. **Log in as the IAM user** and verify permissions.  
In the authorized region, perform the following operations:
  - In the service list, choose **Networking > Cloud Connect**. Click **Create Cloud Connection** in the upper right corner. If a message appears indicating that you have insufficient permissions to perform the operation, the **Cross Connect Administrator** policy is in effect.
  - Choose any other service in the service list. If a message appears indicating that you have insufficient permissions to access the service, the **Cross Connect Administrator** policy is in effect.

## Example Custom Policies

Custom policies can be created to supplement system-defined policies. For the actions supported by custom policies, see [Actions Supported by Policy-based Authorization](#) in the *Cloud Connect API Reference*.

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

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

For details, see [Creating a Custom Policy](#). The following section contains examples of common custom policies.

- Example 1: Grant permission to delete central networks.

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

- Example 2: Grant permission to deny the deletion of central network policies.  
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.

Assume that you want to grant the **CC FullAccess** policy to a user but want to prevent them from deleting central networks. You can create a custom policy for denying central network deletion, and attach this policy together with the **CC FullAccess** policy to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on central networks excepting deleting them. The following is an example of a deny policy:

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

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

A custom policy can contain the actions of one or multiple services that are of the same type (global or project-level). The following is a custom policy containing multiple actions:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetwork:create",

```

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

## 2.1.2 Using IAM Identity Policies to Grant Access to Central Networks

System-defined permissions [in identity policy-based authorization](#) provided by [IAM](#) let you control access to your central networks. With IAM, you can:

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

If your Huawei Cloud account meets your permissions requirements, you can skip this section.

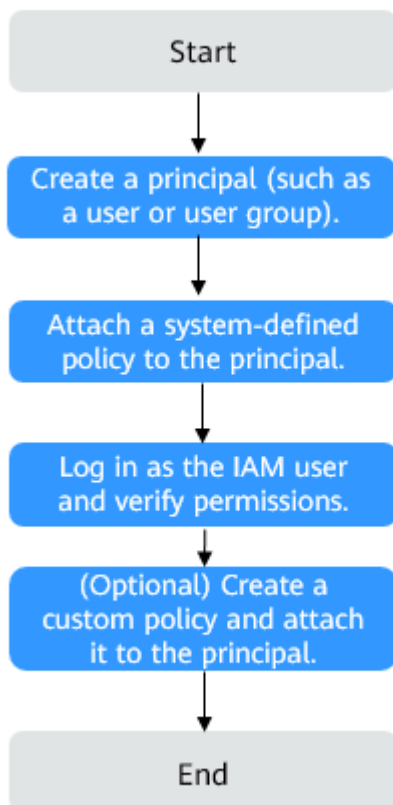
[Figure 2-2](#) shows the process flow of identity policy-based authorization.

### Prerequisites

Before granting permissions to user groups, learn about system-defined permissions in [Identity Policy-based Authorization](#) for Cloud Connect. To grant permissions for other services, learn about all [system-defined permissions](#) supported by IAM.

## Process Flow

**Figure 2-2** Process of granting Cloud Connect permissions using identity policy-based authorization



1. On the IAM console, [create an IAM user](#) or [create a user group](#).
2. [Attach a system-defined identity policy](#) (CCReadOnlyPolicy) to the user or user group.
3. [Log in as the IAM user](#) and verify permissions.  
In the authorized region, perform the following operations:
  - In the service list, choose **Networking > Cloud Connect**. Click **Create Cloud Connection** in the upper right corner. If the cloud connection can be created, the **CCReadOnlyPolicy** policy has taken effect.
  - Choose any other service in the service list. If a message appears indicating that you have insufficient permissions to access the service, the **CCReadOnlyPolicy** policy is in effect.

## Example Custom Policies

You can create custom identity policies to supplement the system-defined identity policies of Cloud Connect. For the actions supported for custom policies, see "Identity Policy-based Authorization" in the [Cloud Connect API Reference](#).

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

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

For details, see [Creating a Custom Policy and Attaching It to a Principal](#).

When creating a custom policy, use the Resource element to specify the resources the policy applies to and use the Condition element (condition keys) to control when the policy is in effect. For the supported resource types and condition keys, see "Identity Policy-based Authorization" in the [Cloud Connect API Reference](#).

The following are examples of common custom policies.

- Example 1: Granting permissions to create and delete central networks

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetwork:create",
        "cc:centralNetwork:delete"
      ]
    }
  ]
}
```

- Example 2: Creating a custom policy containing multiple actions

A custom policy can contain the actions of one or multiple services. The following is a custom policy containing multiple actions:

```
{
  "Version": "5.0",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cc:centralNetwork:create",
        "cc:centralNetwork:update",
        "cc:centralNetwork:delete",
        "cc:centralNetwork:get"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "er:instances:create",
        "er:instances:update",
        "er:instances:delete",
        "er:instances:get"
      ]
    }
  ]
}
```

## 2.2 Central Networks

## 2.2.1 Overview

### Central Network

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

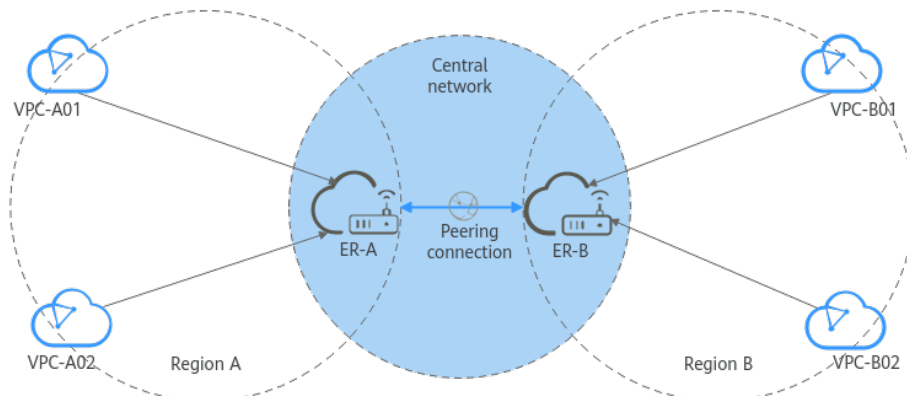
**NOTE**

For details about the regions where central networks are available, see [Region Availability](#).

### Application Scenarios

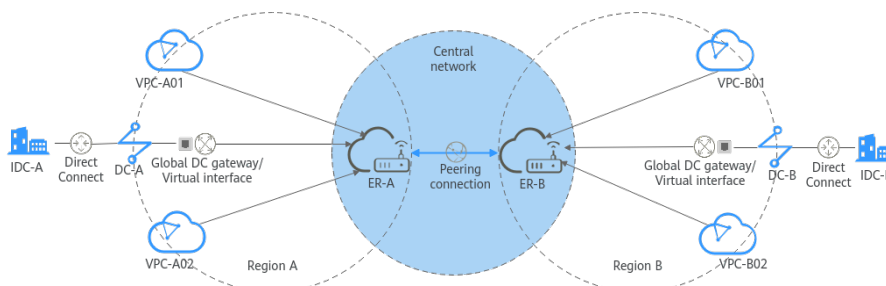
- Cross-region communication on the cloud: Enterprise routers in different regions are added to a central network as attachments so that resources in these regions can communicate with each other over one network.

**Figure 2-3** Cross-region communication between enterprise routers



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

**Figure 2-4** Communication between enterprise routers and on-premises data centers



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

## Central Network Quotas

**Table 2-1** Central network quotas

Quota Type	Default Quota	Adjustable
Central networks in an account	6	Yes <a href="#">Submit a service ticket.</a>
Policies for a central network	500	Yes <a href="#">Submit a service ticket.</a>
Policy document size (KB)	10	No
Enterprise routers on a central network as attachments in a region	1	No
Global DC gateways on a central network as attachments in a region	3	Yes <a href="#">Submit a service ticket.</a>

## Constraints on Central Networks

- To use a central network, the following resources must have been created:
  - Enterprise router: used to build a central network
  - Global DC gateway: attached to an enterprise router for allowing on-premises data centers to access the cloud across regions
- Policy management
  - A central network can only have one policy. If you apply another policy for this central network, the policy that was previously applied will be automatically cancelled.
  - In each policy, only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default.
  - A policy that is being applied or cancelled cannot be deleted.
- Cross-site connection bandwidth management
  - A cross-site connection bandwidth cannot be changed or deleted when it is being created, updated, deleted, frozen, unfrozen, or is recovering.
  - The total of cross-site connection bandwidths cannot exceed the global connection bandwidth.
  - If a cross-site connection bandwidth is deleted, you will still be billed for the global connection bandwidth.

## Configuration Process

**Figure 2-5** shows the process of configuring a central network to manage global network resources.

**Figure 2-5** Central network configuration process



**Table 2-2** Steps for configuring a central network

N o.	Step	Description	Reference
1	Create a central network.	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.	<a href="#">Creating a Central Network</a>
2	(Optional) Add attachments.	Attach global DC gateways to the enterprise routers in a specific region of the central network to enable resources to communicate with each other across regions.	<a href="#">Adding Attachments</a>
3	Assign a cross-site connection bandwidth.	After adding enterprise routers or global DC gateways in different regions to the same policy, purchase a global connection bandwidth and assign bandwidths for cross-site connections.	<a href="#">Assigning a Cross-Site Connection Bandwidth</a>

## Concepts

- Attachment  
 Attachments are any resources that you want to add to a central network. You can attach a global DC gateway to the enterprise routers in specified regions to connect the cloud and on-premises networks.
- Cross-site connection bandwidth  
 A cross-site connection bandwidth enables network instances at different sites to communicate with each other over cross-site connections. They are used to control the rate at which network instances in different sites communicate with each other. The total capacity of cross-site connection bandwidths cannot exceed that of the global connection bandwidth.

## 2.2.2 Creating a Central Network

### Scenarios

After an enterprise router is created, you can create a central network and add the enterprise router to a policy of the central network. In this way, resources can

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

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

## Constraints

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

**Figure 2-6** Enabling **Default Route Table Association** and **Default Route Table Propagation** for enterprise routers

\* Name

\* ASN

Autonomous System Number used on Huawei Cloud for a Border Gateway Protocol (BGP) session. You can specify an ASN in the range of 64512-65534 or 4200000000-4294967294.  
If your enterprise routers in different regions use Cloud Connect to communicate, specify a unique ASN for each enterprise router.

Default Route Table Association  Enable ⓘ

Default Route Table Propagation  Enable ⓘ

Auto Accept Shared Attachments  Enable ⓘ

- If you need to connect your on-premises network to the cloud, you need to create a global DC gateway and attach it to an enterprise router in a specified region.

### NOTE

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

## Creating a Central Network

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

**Table 2-3** Parameters for creating a central network

Parameter	Setting
<b>Basic Information</b>	
Name	Enter a name for the central network.

Parameter	Setting
Add Enterprise Router	<p>Add an enterprise router to enable VPCs in the same region to communicate with each other. By working with global DC gateways provided by Direct Connect, enterprise routers enable the VPCs and on-premises data centers to communicate with each other. Enterprise routers in different regions can be connected over a central network to allow for cross-region communication between VPCs and between on-premises data centers and VPCs.</p> <p>Click <b>Add Enterprise Router</b> and select the region and route table.</p> <p>Before using the central network, you need to add enterprise routers. Only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default.</p> <p>10 kbit/s of free bandwidth is provided for testing the connectivity between enterprise routers.</p> <p>If no enterprise router is available for your services, click <b>Create Enterprise Router</b> to create one.</p>
<b>Connection Settings (Optional)</b>	
Full-Mesh Peering	This function is enabled by default. Expand the advanced settings to see the full-mesh peering connection list.
Full-Mesh Peering Connections	<p>If this option is enabled, a peering connection will be automatically created between every two enterprise routers you select. The number of enterprise routers you select determines the number of peering connections in the full-mesh peering connection list. You can remove unnecessary peering connections as needed.</p> <ul style="list-style-type: none"> <li>• Removing a peering connection: Click <b>Remove</b> in the <b>Operation</b> column of the target peering connection.</li> <li>• Connecting a peering connection: Click <b>Connect</b> in the <b>Operation</b> column of the target peering connection.</li> <li>• A numerical value that is used to identify a peering connection between two enterprise routers. For full-mesh peering connections, the value can only be 0.</li> </ul>
<b>Advanced Settings (Optional)</b>	
Description	Describe the central network for easy identification.

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

## Follow-up Operations

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

## 2.2.3 Managing Policies

### Scenarios

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

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

- [Creating a Policy](#)
- [Applying a Policy](#)
- [Deleting a Policy](#)

### Constraints

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

### Creating a Policy

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

**Table 2-4** Parameters for adding a policy

Parameter	Description	Example Value
<b>Basic Information</b>		

Parameter	Description	Example Value
Add Enterprise Router	<p>Add an enterprise router to enable VPCs in the same region to communicate with each other. By working with global DC gateways provided by Direct Connect, enterprise routers enable the VPCs and on-premises data centers to communicate with each other. Enterprise routers in different regions can be connected over a central network to allow for cross-region communication between VPCs and between on-premises data centers and VPCs.</p> <p>Click <b>Add Enterprise Router</b> and select the region and route table.</p> <p>Only one enterprise router can be added for a region. All added enterprise routers can communicate with each other by default.</p> <p>10 kbit/s of free bandwidth is provided for testing the connectivity between enterprise routers.</p> <p>If no enterprise router is available for your services, click <b>Create Enterprise Router</b> to create one.</p>	<ul style="list-style-type: none"> <li>• ER-01</li> <li>• ER-02</li> </ul>
<b>Connection Settings (Optional)</b>		
Full-Mesh Peering	This function is enabled by default. Expand <b>Advanced Settings</b> to check the full-mesh peering connections.	-
Full-Mesh Peering Connections	<p>If this option is enabled, a peering connection will be automatically created between every two enterprise routers you select. The number of selected enterprise routers determines the number of peering connections that will be displayed in the list. You can remove unnecessary peering connections as needed.</p> <ul style="list-style-type: none"> <li>• Removing a peering connection: Click <b>To be removed</b> in the <b>Operation</b> column of the target peering connection.</li> <li>• Connecting a peering connection: Click <b>Peering Connection</b> in the <b>Operation</b> column of the target peering connection.</li> <li>• A numerical value that is used to identify a peering connection between two enterprise routers. For full-mesh peering connections, the value can only be 0.</li> </ul>	-

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

## Applying a Policy

1. Go to the [central network list page](#).
2. Locate the central network and click its name.
3. Choose the **Policies** tab and click **Apply** on the right of the target policy version. On the **Apply Policy** page, confirm the information shown in [Table 2-5](#) and click **Submit**.

**Table 2-5** Parameters for applying a policy

Parameter	Description
<b>Existing Policy Details</b>	
Existing Policy Name	<ul style="list-style-type: none"> <li>• <b>Version 1</b>: the name of the existing policy.</li> <li>• <b>Enterprise Routers</b>: the enterprise routers on the central network that the existing policy is applied to.</li> <li>• <b>Peering Connections</b>: the peering connections that connect the enterprise routers in the existing policy.</li> </ul>
<b>New Policy Details</b>	
New Policy Name	<ul style="list-style-type: none"> <li>• Version 2: name of the new policy to be applied.</li> <li>• <b>Enterprise Routers</b>: the enterprise routers on the central network that the new policy will be applied to.</li> <li>• <b>Peering Connections</b>: the peering connections that connect the enterprise routers in the new policy.</li> </ul>
<b>Policy Change Details</b>	
Enterprise Routers	The enterprise routers on the central network that the new policy will be applied to.
Peering Connections	The peering connections that connect the enterprise routers in the new policy.
<b>Confirm</b>	
Current Configuration	<b>Existing Policy Name: Version 1</b>
New Configuration	<b>New Policy Name: Version 2</b>
Enterprise router attachment change	Price for changing the policy of a central network.

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

## Deleting a Policy

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

## 2.2.4 Managing Central Network Attachments

### Scenarios

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

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

- [Adding Attachments](#)
- [Deleting an Attachment](#)

### Constraints

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

#### NOTE

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

- By default, you can add up to three attachments to a central network. To increase the default quota, [submit a service ticket](#).
- Up to five attachments can be added on the console at a time.

### Adding Attachments

1. Go to the [central network list page](#).
2. Locate the central network and click its name.
3. On the **Attachments** tab, click **Add Attachment**.
4. Add network instances such as global DC gateways or enterprise router route tables to the central network. [Table 2-6](#) describes the parameters.

**Table 2-6** Parameters for adding a network instance to a central network as an attachment

Parameter	Setting
Name	Enter a name for the attachment.

Parameter	Setting
<b>Region where the enterprise router on the central network is located</b>	
Region	Select the region of the enterprise router that the network instance is attached to.
Enterprise Router	Select an enterprise router in the selected region. The network instance will be attached to the selected enterprise router.  If there are no enterprise routers for you to choose from, click <b>Create Enterprise Router</b> to create one first.
<b>Network instance that will be added to a central network</b>	
Attachment Type	Specify the type of the network instance that will be added to the central network as attachment.  Only global DC gateways are supported.  A global DC gateway can work with enterprise routers in the same region or different regions to build a central network so that your on-premises data center can access the VPCs over the Huawei backbone network. This can reduce network latency, simplify network topology, and improve O&M efficiency.
Region	Select the region where the global DC gateway is located.  This region may be different from that of the enterprise router.
Global DC Gateway	Select the global DC gateway that will be attached to the selected enterprise router, so that they can communicate with each other and the on-premises data center can communicate with the cloud network.  If there are no global DC gateways for you to choose from, click <b>Create Global DC Gateway</b> to create one first.

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

5. Click **OK**.

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

## Deleting an Attachment

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

1. Go to the [central network list page](#).
2. Locate the central network and click its name.

3. On the **Attachments** tab, locate the attachment you want to delete and click **Delete** in the **Operation** column.
4. Click **OK**.

## 2.2.5 Managing Cross-Site Connection Bandwidths

### Scenarios

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

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

- [Assigning a Cross-Site Connection Bandwidth](#)
- [Viewing Monitoring Metrics of Cross-Site Connection Bandwidths](#)
- [Changing Cross-Site Connection Bandwidth](#)
- [Deleting a Cross-Site Connection Bandwidth](#)

### Constraints

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

### Assigning a Cross-Site Connection Bandwidth

1. Go to the [central network list page](#).
2. Locate the central network and click its name.
3. Click the **Cross-Site Connection Bandwidths** tab.
4. Locate the cross-site connection and click **Assign** in the **Global Connection Bandwidth** column.
5. On the **Assign Cross-Site Connection Bandwidth** page, select the global connection bandwidth.  
You can also click **Buy Now** to purchase one if there are no available global connection bandwidths.
6. Enter the bandwidth.
7. Click **OK**.

### Viewing Monitoring Metrics of Cross-Site Connection Bandwidths

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

1. Go to the [central network list page](#).

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

 **NOTE**

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

## Changing Cross-Site Connection Bandwidth

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

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

 **NOTE**

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

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

6. Click **OK**.

## Deleting a Cross-Site Connection Bandwidth

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

## 2.2.6 Managing Central Network Tags

### Scenarios

Tags help you identify, classify, and search for central networks. This section shows you how to:

- Add central network tags.

- Modify central network tags.
- Delete central network tags.

For details about central network tag requirements, see [Table 2-7](#).

**Table 2-7** Central network tag requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"><li>• For each resource, each tag key must be unique, and each tag key can only have one tag value.</li><li>• Cannot be left blank.</li><li>• Can contain a maximum of 128 characters.</li><li>• Cannot start or end with a space.</li></ul>	gcb_key1
Value	<ul style="list-style-type: none"><li>• Can be left blank.</li><li>• Can contain a maximum of 255 characters.</li><li>• Cannot start or end with a space.</li></ul>	gcb_value1

## Constraints

Each cloud resource can have a maximum of 20 tags.

## Procedure

1. Go to the [central network list page](#).
2. In the central network list, click the name of the target central network.  
The central network details page is displayed.
3. On the **Tags** tab, click **Edit Tag** in the upper left corner above the tag list.  
The **Edit Tag** dialog box is displayed.
4. Perform the following operations on the tags as required:
  - Adding a tag: Click **+ Add** , enter a tag key and value, and click **OK**.
  - Modifying a tag: Click **×** next to the target tag key or value to delete the original value, enter a new value, and click **OK**.
  - Deleting a tag: Click **Delete** next to the target tag and click **OK**.

## 2.3 Global Connection Bandwidths

## 2.3.1 Overview

### What Is a Global Connection Bandwidth?

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

 **NOTE**

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

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

**Table 2-8** Global connection bandwidth types

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

Bandwidth Type	Instance Type	Description	Scenario
Geographic - region	<ul style="list-style-type: none"> <li>Global EIPs</li> <li>Central network</li> </ul>	<p>Select this type of bandwidth if you need communication within a geographic region. Geographic regions include the Chinese mainland, Asia Pacific, and Southern Africa. For example, CN East-Shanghai1 and CN South-Guangzhou are regions in the Chinese mainland. For details about the relationship between geographic regions and Huawei Cloud regions, see <a href="#">Geographic Regions and Huawei Cloud Regions</a>.</p>	<ul style="list-style-type: none"> <li>A global EIP and its associated resource, such as an ECS or load balancer, have to be in the same geographic region. <a href="#">Geographic-Region Bandwidth Application Scenario (Global EIP)</a></li> <li>Enterprise routers on a central network are from the same geographic region. <a href="#">Geographic-Region or Cross-Geographic-Region Bandwidth Application Scenario (Central Network)</a></li> </ul>
Cross-geographic - region	<ul style="list-style-type: none"> <li>Global EIPs</li> <li>Central network</li> </ul>	<p>Select this type of bandwidth if you need communication across geographic regions. Geographic regions include the Chinese mainland, Asia Pacific, and Southern Africa. For example, CN East-Shanghai1 and CN-Hong Kong are regions in the Chinese mainland. For details about the relationship between geographic regions and Huawei Cloud regions, see <a href="#">Geographic Regions and Huawei Cloud Regions</a>.</p>	<ul style="list-style-type: none"> <li>A global EIP and its associated resource, such as an ECS or load balancer, are from different geographic regions. <a href="#">Cross-Geographic-Region Bandwidth Application Scenario (Global EIP)</a></li> <li>Enterprise routers on a central network are from different geographic regions. <a href="#">Geographic-Region or Cross-Geographic-Region Bandwidth Application Scenario (Central Network)</a></li> </ul>

### Constraints on Global Connection Bandwidths

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

- You can bind one global connection bandwidth to or unbind it from a central network at a time.
- To use a global connection bandwidth on a central network, you need to configure cross-site connections by referring to the following:
  - [Creating a Central Network](#)
  - [Managing Policies](#)
- Global connection bandwidths of different types can be used with different instances. For details, see [Table 2-9](#).

**Table 2-9** Instances that can use a global connection bandwidth

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

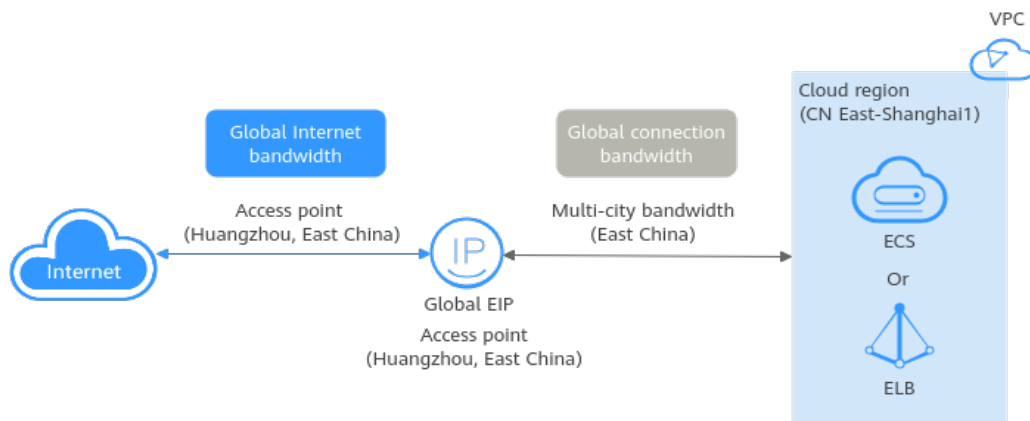
- Before an instance is removed from a global connection bandwidth, ensure the instance is not used to run workloads or establish network connectivity, or the workloads will be unavailable or the network will be interrupted.
- If a global connection bandwidth has been used to assign cross-site connection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

## Multi-city Bandwidth Application Scenario (Global EIP)

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

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

**Figure 2-7** Multi-city bandwidth application scenario (global EIP)

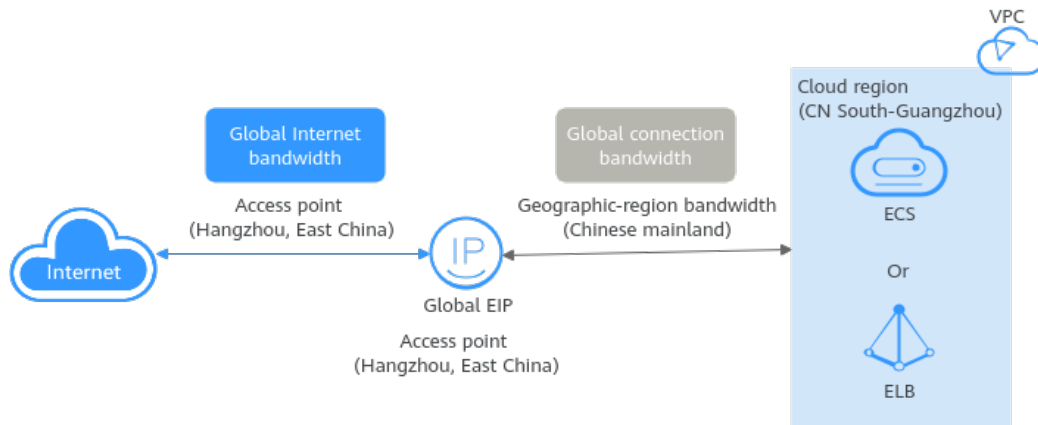


### Geographic-Region Bandwidth Application Scenario (Global EIP)

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

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

**Figure 2-8** Geographic-region bandwidth application scenario (global EIP)



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

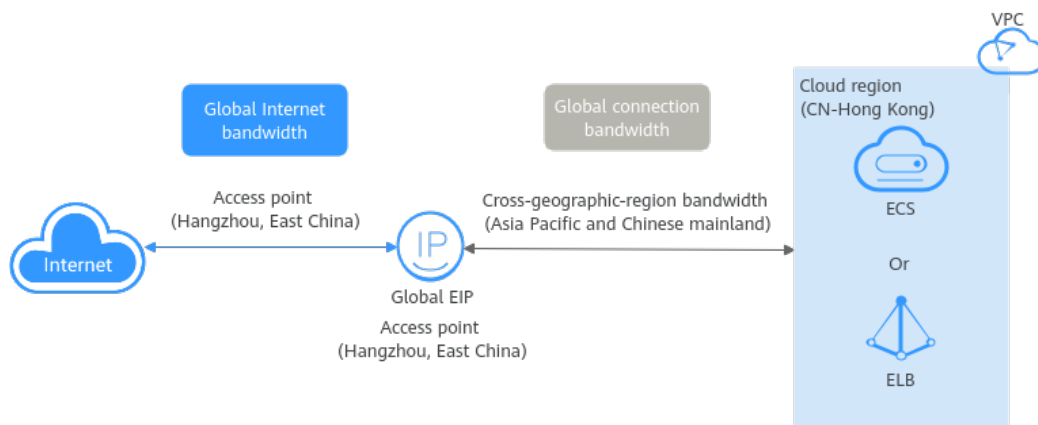
In this example, a global EIP is bound to an ECS.

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

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

**NOTE**

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

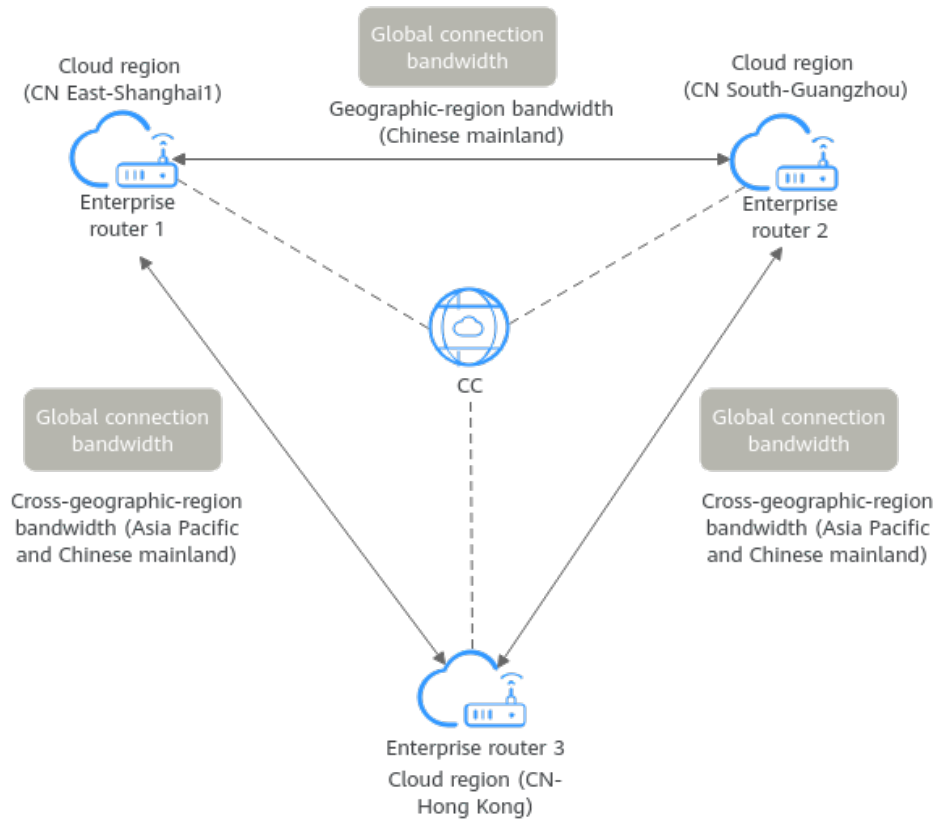
**Figure 2-9** Cross-geographic-region bandwidth application scenario (global EIP)

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

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

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

**Figure 2-10** Geographic-region or cross-geographic-region bandwidth application scenario (central network)



## 2.3.2 Buying a Global Connection Bandwidth

### Scenarios

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

### Procedure

1. Go to the [Create Global Connection Bandwidth](#) page.
2. Configure the parameters based on [Table 2-10](#).

**Table 2-10** Parameters required for buying a global connection bandwidth

Parameter	Setting	Example Value
Billing Mode	<p>Mandatory</p> <p><b>Pay-per-use:</b> a postpaid subscription. You are charged based on the usage duration of the global connection bandwidth. The usage of a global connection bandwidth is calculated by the second but billed by hour. If the usage is less than an hour, you are billed based on the actual duration.</p>	Pay-per-use
Bandwidth Type	<p>Mandatory</p> <p>Select a bandwidth type. There are different types of global connection bandwidths that are designed for different application scenarios, including multi-city, HomeZones, geographic-region, and cross-geographic-region bandwidths. The type of a bandwidth cannot be changed once it is created.</p> <p>For details, see <a href="#">Global Connection Bandwidth Overview</a>.</p> <p>You can decide whether to use a geographic-region bandwidth or cross-geographic-region bandwidth based on service scenarios.</p> <p>If you select a geographic-region, cross-geographic-region, or HomeZones bandwidth, you also need to select geographic regions and specify the regions that need to communicate with each other.</p>	Geographic-region
Billed By	<p>Mandatory</p> <p>The price of a global connection bandwidth varies by its size.</p> <ul style="list-style-type: none"> <li>After a bandwidth is purchased, the billing starts immediately regardless of whether the bandwidth is used.</li> <li>If a bandwidth is no longer required, delete it in a timely manner to avoid unnecessary fees.</li> </ul>	Bandwidth
Bandwidth	<p>Mandatory</p> <p>Select the bandwidth, in Mbit/s.</p>	100
Bandwidth Name	<p>Mandatory</p> <p>Enter the name of the bandwidth. The name:</p> <ul style="list-style-type: none"> <li>Must contain 1 to 64 characters.</li> <li>Can contain letters, digits, underscores (_), hyphens (-), and periods (.).</li> </ul>	bandwidth-test

Parameter	Setting	Example Value
Enterprise Project	Mandatory Provides a cloud resource management mode, in which cloud resources and members are centrally managed by project.	default

3. Click **Next**.
4. Confirm the configurations and click **Submit**.  
The global connection bandwidth list page is displayed.
5. In the global connection bandwidth list, view the status of the bandwidth.  
If the bandwidth status becomes **Normal**, the purchase is successful.

## 2.3.3 Adding Instances to a Global Connection Bandwidth

### Scenarios

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

- [Using a Global Connection Bandwidth on a Central Network \(Assigning Bandwidths to a Cross-Site Connection on a Central Network\)](#)
- [Adding Global EIPs to a Global Connection Bandwidth](#)

### Constraints

- Instances that can be added to a global connection bandwidth must be from the same region as the bandwidth.
- A global connection bandwidth can only be used by instances of the same type. If you want another type of instances to use a global connection bandwidth that already has instances, you need to remove the instances first.
  - You can add or remove global EIPs in batches.
  - You can bind one global connection bandwidth to or unbind it from a central network at a time.
- To use a global connection bandwidth on a central network, you need to configure cross-site connections by referring to the following:
  - [Creating a Central Network](#)
  - [Managing Policies](#)
  - [Managing Central Network Attachments](#)
- Global connection bandwidths of different types can be used with different instances. For details, see [Table 2-11](#).

**Table 2-11** Instances that can use a global connection bandwidth

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

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

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

### Adding Global EIPs to a Global Connection Bandwidth

1. Go to the [global connection bandwidth list page](#).
2. Locate the global connection bandwidth and click **Bind** in the **Operation** column.
3. In the displayed dialog box, select **Global EIP** for **Instance Type**.  
For a multi-city global connection bandwidth, select the two regions where the bandwidth will be used.
4. Search for global EIPs using keyword.
5. Select one or more global EIPs and click **OK**.

## 2.3.4 Removing Instances from a Global Connection Bandwidth

### Scenarios

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

### Constraints

- Before an instance is removed from a global connection bandwidth, the instance is not used to run workloads or establish network connectivity, or the workloads will be unavailable or the network will be interrupted.
- A global connection bandwidth can only be used by one type of instances. If you want to change the instance type, remove all the instances from the

global connection bandwidth and then add instances of another type by referring to [Adding Instances to a Global Connection Bandwidth](#).

- If a global connection bandwidth has been used to assign cross-site connection bandwidths for a central network, the global connection bandwidth cannot be unbound from the central network. You need to delete the cross-site connection bandwidths first.

## Deleting a Cross-site Connection Bandwidth from a Central Network

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

## Removing Instances from a Global Connection Bandwidth

1. Go to the [global connection bandwidth list page](#).
2. Locate the global connection bandwidth and click **Unbind** in the **Operation** column.
  - If the bandwidth is only bound to one instance, click **Remove** in the **Operation** column and then click **OK** in the displayed dialog box.
  - If the bandwidth is bound to more than one instance:
    - i. On the details page of the bandwidth, click **Associated Instances**.
    - ii. Select the instances.
    - iii. Click **Remove** above the instance list.
    - iv. In the displayed dialog box, click **OK**.

## 2.3.5 Managing a Global Connection Bandwidth

### Scenarios

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

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

- [Modifying a Global Connection Bandwidth](#)
- [Deleting a Global Connection Bandwidth](#)

### Constraints

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

## Modifying a Global Connection Bandwidth

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

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

## Deleting a Global Connection Bandwidth

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

## 2.4 Monitoring and Auditing

### 2.4.1 Using Cloud Eye to Monitor Central Network Metrics

#### 2.4.1.1 Central Network Metrics

##### Overview

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

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

##### Namespace

SYS.ER

## Metrics

**Table 2-12** Monitoring metrics of an enterprise router attachment

ID	Metric	Description	Value Range	Unit	Conversion Rule	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
attachm ent_byt es_in	Inbo und Traffi c	Network traffic going into the attachment	≥ 0	Byt e	1024 (IEC)	Enterprise router attachment	1 minute
attachm ent_byt es_out	Outb ound Traffi c	Network traffic going out of the attachment	≥ 0	Byt e	1024 (IEC)	Enterprise router attachment	1 minute
attachm ent_bits _rate_in	Inbo und Band width h	Network traffic per second going into the attachment	≥ 0	bit/ s	1000 (SI)	Enterprise router attachment	1 minute
attachm ent_bits _rate_o ut	Outb ound Band width h	Network traffic per second going out of the attachment	≥ 0	bit/ s	1000 (SI)	Enterprise router attachment	1 minute
attachm ent_pac kets_in	Inbo und PPS	Packets going into the attachment per second	≥ 0	pps	1000 (SI)	Enterprise router attachment	1 minute
attachm ent_pac kets_out	Outb ound PPS	Packets going out of the attachment per second	≥ 0	pps	1000 (SI)	Enterprise router attachment	1 minute

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

## Dimensions

Key	Value
er_attachment_id	Enterprise router attachment

### 2.4.1.2 Viewing Central Network Metrics

#### Scenarios

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

#### Procedure

**Step 1** Go to the [Overview](#) page.

**Step 2** In the navigation pane on the left, choose **Cloud Service Monitoring > Enterprise Router**.

The enterprise router list is displayed.

**Step 3** View the real-time metrics of enterprise router attachments.

1. In the enterprise router list, click **View Metric** in the **Operation** column of the target attachment.  
The metrics are displayed.
2. View metrics of the attachment.

 **NOTE**

For details about querying metrics, see [Querying Cloud Service Monitoring Metrics](#).

----End

### 2.4.1.3 Creating an Alarm Rule

#### Scenarios

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

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

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

#### Procedure

**Step 1** Go to the [Overview](#) page.

**Step 2** In the navigation pane on the left, choose **Cloud Service Monitoring > Enterprise Router ER**.

The enterprise router list is displayed.

**Step 3** Create an alarm rule and notification for an enterprise router attachment.

1. In the enterprise router list, choose **More > Create Alarm Rule** in the **Operation** column of the target attachment.  
The **Create Alarm Rule** page is displayed.
2. On the **Create Alarm Rule** page, configure the parameters as prompted.

 **NOTE**

For details about the parameters on the **Create Alarm Rule** page, see [Creating an Alarm Rule](#).

----End

## 2.4.2 Using Cloud Eye to Monitor Metrics on Global Connection Bandwidths

## 2.4.2.1 Monitoring Metrics Supported by Global Connection Bandwidths

### Overview

The table describes monitoring metrics reported by global connection bandwidths 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 global connection bandwidths.

### Namespace

SYS.GCB

### Metrics

**Table 2-13** Monitoring metrics supported by global connection bandwidths

ID	Metric	Description	Value Range	Unit	Monitored Object (Dimension)	Monitoring Interval (Raw Data)
network_bytes	Network Traffic	Traffic of a global connection bandwidth in a measurement period	$\geq 0$	Byte	Global connection bandwidth	1 minute
network_bandwidth	Network Bandwidth	Actually used global connection bandwidth in a measurement period	$\geq 0$	bit/s	Global connection bandwidth	1 minute
network_bandwidth_usage	Network Bandwidth Usage	Utilization of a global connection bandwidth in a measurement period	$\geq 0$	%	Global connection bandwidth	1 minute

### Dimensions

Key	Value
gcb_id	Global connection bandwidth

## 2.4.2.2 Viewing Monitoring Metrics of a Global Connection Bandwidth

### Scenarios

You can view the monitoring metrics of global connection bandwidths on the Cloud Eye console.

### Procedure

**Step 1** Go to the [Overview](#) page.

**Step 2** In the navigation pane on the left, choose **Cloud Service Monitoring > Global Connection Bandwidth**.

The global connection bandwidth list is displayed.

**Step 3** In the global connection bandwidth list, perform the following operations to view the monitoring metrics:

1. In the global connection bandwidth list, click **View Metric** in the **Operation** column of the target global connection bandwidth.

The metrics are displayed.

2. View metrics of the global connection bandwidth.

 **NOTE**

For details about querying metrics, see [Querying Cloud Service Monitoring Metrics](#).

----End

## 2.4.2.3 Creating an Alarm Rule

### Scenarios

This section describes how to create an alarm rule and notification for a global connection bandwidth.

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

Alarm rules for important metrics help you timely know metric data exceptions and quickly rectify the faults.

### Procedure

**Step 1** Go to the [Overview](#) page.

**Step 2** In the navigation pane on the left, choose **Cloud Service Monitoring > Global Connection Bandwidth**.

The global connection bandwidth list is displayed.

**Step 3** In the global connection bandwidth list, perform the following operations to create an alarm rule for the global connection bandwidth:

1. Locate the target global connection bandwidth, click **More** in the **Operation** column, and select **Create Alarm Rule**.

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

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

 **NOTE**

For details about the parameters on the **Create Alarm Rule** page, see [Creating an Alarm Rule](#).

----End

## 2.4.3 Using CTS to Record Key Operations on Central Networks

### 2.4.3.1 Key Central Network Operations

#### Scenarios

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

#### Prerequisites

You have enabled CTS.

#### Key Operations Recorded by CTS

**Table 2-14** 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

Operation	Resource	Trace
Adding a global DC gateway to a central network as an attachment	centralNetworkAttachment	createCentralNetworkGdgwAttachment
Updating a global DC gateway on a central network	centralNetworkAttachment	updateCentralNetworkGdgwAttachment
Removing an attachment from a central network	centralNetworkAttachment	deleteCentralNetworkAttachment
Updating a central network connection	centralNetworkConnection	updateCentralNetworkConnection
Adding a tag to a central network	createCentralNetworkTags	centralNetworkTags
Deleting a tag from a central network	deleteCentralNetworkTags	centralNetworkTags

**Table 2-15** Global connection bandwidth operations recorded by CTS

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



### 2.4.3.2 Viewing Central Network Audit Logs

#### Scenarios

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

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

## Procedure

1. Log in to the management console.
2. Click  in the upper left corner to select a region and a project.
3. In the upper left corner of the page, click  to go to the service list. Under **Management & 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.  
After you select **Trace name** for **Search By**, you also need to select a trace name.  
After you select **Resource ID** for **Search By**, you also need to select or enter a resource ID.  
After you select **Resource name** for **Search By**, you also need to select or enter a resource name.
  - **Operator**: Select a specific operator (at the user level rather than the tenant level).
  - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
  - Search time range: In the upper right corner, choose **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
6. Click the arrow on the left of the required trace to expand its details.
7. Click **View Trace** in the **Operation** column to view trace details.

## 2.5 Quotas

### What Is Quota?

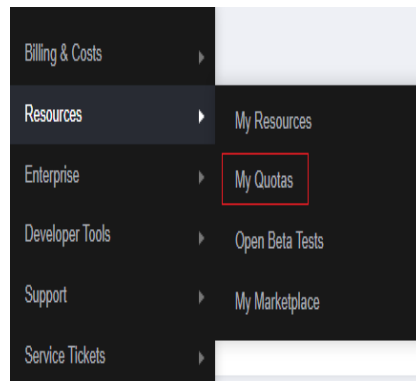
Quotas can limit the number of resources available to users, such as the maximum number of ECS or EVS disks that can be created.

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

### How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**.  
The **Service Quota** page is displayed.

**Figure 2-11 My Quotas**

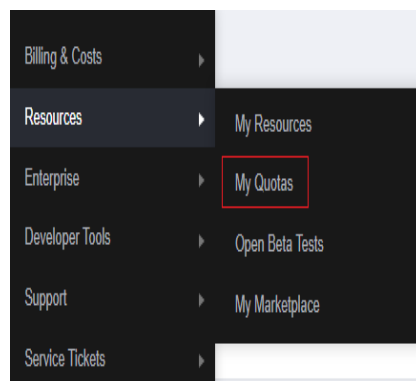


3. View the used and total quota of each type of resources on the displayed page.  
If a quota cannot meet service requirements, apply for a higher quota.

### 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 2-12 My Quotas**



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

**Figure 2-13 Increasing quota**

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

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**.