Cloud Connect

FAQ

Issue 01

Date 2022-06-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

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

Contents

1 Popular Questions 1
1.1 How Do I Configure Cloud Connect? 1
1.2 What Can I Do If Cross-Region Network Communications Fail? 1
1.3 What Tools Can I Use to Test Network Connectivity After All Configurations Are Complete? 2
1.4 What Can I Do If There Is a Route Conflict When I Load a Network Instance to a Cloud Connection? 2
1.5 How Can I Modify the Bandwidth of a Purchased Bandwidth Package? 2
1.6 Do I Need to Create Another Cloud Connection If Network Instances in One Region Need to Communicate with Network Instances in Two Other Regions That Have Already Been Loaded to a Cloud Connection? 3
1.7 Why Do I Need Cloud Connect If the Network Latency Is the Same as on the Internet? 3
2 General Consulting and Service Use 7
2.1 What Can I Do with Cloud Connect? 7
2.2 How Do I Configure Cloud Connect? 7
2.3 What Are the Differences Between Cloud Connect and VPC Peering? 8
2.4 What Tools Can I Use to Test Network Connectivity After All Configurations Are Complete? 8
2.5 What Network Instance Types Does Cloud Connect Support? 9
2.6 How Many Bandwidth Packages Can I Bind to a Cloud Connection? 9
2.7 Are the Uplink and Downlink Rates of the Configured Inter-Region Bandwidth the Same? 9
2.8 Are There Any Limits on the Traffic for Cross-Region Network Communications? 9
2.9 What Are the Metrics for Traffic Monitoring? 10
2.10 What Are the Restrictions of Using Cloud Connect? 10
2.11 Where Can I Add Routes for a Cloud Connection on the Management Console? 10
2.12 Do I Need to Bind an EIP to Each ECS in the VPCs Connected over a Cloud Connection? 11
2.13 How Can I Modify the Bandwidth of a Purchased Bandwidth Package? 11
2.14 Will the Modified Inter-Region Bandwidth Take Effect Immediately? 12
2.15 How Can I Modify Inter-Region Bandwidth? 12
2.16 Do I Need to Create Another Cloud Connection If Network Instances in One Region Need to Communicate with Network Instances in Two Other Regions That Have Already Been Loaded to a Cloud Connection? 12
2.17 Are Network Circuits Physically Isolated? 12
2.18 Is Cloud Connect an Out-Of-The-Box Service? 12
2.19 How Can Cloud Connect Offer High Availability? 13
3 Console Operations 14

3.1 How Do I Configure Cloud Connect?.....14
3.2 What Can I Do If There Is a Route Conflict When I Load a Network Instance to a Cloud Connection?.....14
3.3 How Many Bandwidth Packages Can I Bind to a Cloud Connection?.....15
3.4 What Are the Restrictions of Using Cloud Connect?.....15
3.5 How Can I Apply for a Cross-Border Permit?.....15
3.6 Where Can I Add Routes for a Cloud Connection on the Management Console?.....16
3.7 How Can I Modify the Bandwidth of a Purchased Bandwidth Package?.....16
3.8 How Can I Modify Inter-Region Bandwidth?.....17
3.9 What Tool Can I Used to Test the Bandwidth Rate of a Cloud Connection?.....17
3.10 Will the Modified Inter-Region Bandwidth Take Effect Immediately?.....17

4 Bandwidth Packages.....18
4.1 How Many Bandwidth Packages Can I Bind to a Cloud Connection?.....18
4.2 How Can I Modify the Bandwidth of a Purchased Bandwidth Package?.....18
4.3 How Do I Decrease the Bandwidth of a Bandwidth Package?.....19

5 Bandwidth, Latency and Packet Loss.....20
5.1 What Can I Do If Cross-Region Network Communications Fail?.....20
5.2 Will the Modified Inter-Region Bandwidth Take Effect Immediately?.....20
5.3 How Can I Troubleshoot Network Connectivity for a Hybrid Cloud Built Using Cloud Connect and Direct Connect?.....21
5.4 Do I Need a Bandwidth Package for Testing Network Connectivity?.....21
5.5 Why Do I Need Cloud Connect If the Network Latency Is the Same as on the Internet?.....21
5.6 Are the Uplink and Downlink Rates of the Configured Inter-Region Bandwidth the Same?.....24
5.7 Are There Any Limits on the Traffic for Cross-Region Network Communications?.....24
5.8 How Can I Modify an Inter-Region Bandwidth?.....24
5.9 Are Network Circuits Physically Isolated?.....25
5.10 How Can Cloud Connect Offer High Availability?.....25

6 Cross-Border Permit.....26
6.1 Why Do I Need a Cross-Border Permit?.....26
6.2 Who Approves Cross-Border Permits?.....26
6.3 How Can I Apply for a Cross-Border Permit?.....26
6.4 When Would I Need to Apply for a Cross-Border Permit?.....27
6.5 How Long Will a Cross-Border Permit Be Approved?.....27
6.6 Why Is Additional Real-Name Authentication Required After I Have Completed Huawei Cloud Real-Name Authentication?.....27
6.7 Can I Modify the Content of the *Cloud Connect Cross-Border Circuit Service Agreement*?.....28
6.8 Can I Download the Materials for My Cross-Border Permit Application on the Console After I Delete Them from My PC?.....28
6.9 Does Huawei Cloud Need to Sign and Stamp the Seal on the Materials for Cross-Border Permit Application?.....28

7 Networking and Cloud Connect Scenarios.....29
7.1 Can Cloud Connect Link VPCs in the Same Region?.....29

7.2 Can I Load the VPCs of Other Accounts to My Cloud Connection? 29

8 Cross-Account Authorization 30

8.1 Does the Other User Need to Buy a Bandwidth Package If I Want to Load This Other User's VPCs to My Cloud Connection? 30

8.2 Does the Other User Need to Create a Cloud Connection If I Want to Load This Other User's VPCs to My Cloud Connection? 30

8.3 How Do I Load VPCs Across Accounts? 30

8.4 Can a VPC Be Loaded to More than One Cloud Connection? 31

9 Permissions 32

9.1 How Can I Grant Cloud Connect Permissions to IAM Users? 32

10 Monitoring 34

10.1 Why Is the Bandwidth Monitoring Data on the Cloud Eye Console Incomplete? 34

10.2 How Do I View the Bandwidth Monitoring Data of a Cloud Connection? 34

10.3 Is There Monitoring Data Immediately After I Assign an Inter-region Bandwidth? 34

10.4 What Are the Metrics for Traffic Monitoring? 34

11 Quotas 36

11.1 How Can I Increase Resource Quotas? 36

1 Popular Questions

1.1 How Do I Configure Cloud Connect?

To configure Cloud Connect, perform the following steps on the management console:

1. Create a cloud connection, which will connect all the network instances loaded to it and allow the instances to communicate with each other over a private network.
2. Load the network instances that need to communicate with each other to the cloud connection. Two types of network instances are supported, VPC and virtual gateway.
3. If network instances are in different regions, buy a bandwidth package and bind it to the cloud connection.
4. Assign inter-region bandwidths for cross-region network communications.

1.2 What Can I Do If Cross-Region Network Communications Fail?

After you complete all the required configuration, you can use ICMP or Telnet to test network connectivity. If network communications fail, do the following to locate the fault:

- Check whether the security group containing the ECSs in the destination VPC allows ICMP or Telnet traffic over the corresponding port in the inbound direction. If ICMP or Telnet traffic is not allowed, the packets will be blocked by the security group.
- Check whether a network ACL is configured for the subnet in the destination VPC to deny the communications between the source and destination VPCs. If such an ACL exists, the packets will be blocked by the ACL.
- Check whether there are overlapping subnets in the source and destination VPCs. If they have overlapping subnets, the packets will not be sent to the subnet of the destination VPC.

- Check whether an inter-region bandwidth is assigned between source and destination regions. If you have a bandwidth package but there is no inter-region bandwidth between different regions, the default 10 kbit/s of bandwidth may fail to transmit large ICMP packets or Telnet packets.

1.3 What Tools Can I Use to Test Network Connectivity After All Configurations Are Complete?

Use ICMP or Telnet to test whether the VPCs in different regions can communicate with each other.

1.4 What Can I Do If There Is a Route Conflict When I Load a Network Instance to a Cloud Connection?

When you are loading a VPC, the system may display a message "A routing conflict has occurred in this VPC. This route is already being used in other scenarios, such as VPC Peering or VPN." If this happens, check whether the VPC is used by:

- Custom CIDR block
- Direct Connect
- VPN
- VPC peering connection

If the VPC is used by any of the above, there may be route conflicts. In this case, disassociate the VPC from the resource and then load the VPC to the cloud connection or select another VPC based on your network plan.

1.5 How Can I Modify the Bandwidth of a Purchased Bandwidth Package?

Cloud Connect allows you to modify the bandwidth of a purchased bandwidth package.

To modify the bandwidth, perform the following operations:

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

NOTE

You can increase or decrease the bandwidth. In the following steps, increasing the bandwidth is used as an example.

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

5. Select **Increase bandwidth** and click **Continue**.
6. Specify the new bandwidth and click **OK**.
7. Confirm the configuration and click **Submit**.
8. Select a payment method and click **Pay**.

NOTE

- Modifying the bandwidth does not interrupt services, but unsubscribing from a bandwidth package that has been bound to a cloud connection or unbinding a bandwidth package from a cloud connection will. Before you unsubscribe from a bandwidth package that has been bound to a cloud connection, unbind it from the cloud connection.
- If bandwidth package is going to expire within the next 24 hours, you cannot increase or decrease the bandwidth.

1.6 Do I Need to Create Another Cloud Connection If Network Instances in One Region Need to Communicate with Network Instances in Two Other Regions That Have Already Been Loaded to a Cloud Connection?

No.

Load the network instances in first region to the cloud connection used by network instances in the other two regions and assign inter-region bandwidth between each pair of regions.

In this way, network instances in the three regions can communicate with each other.

1.7 Why Do I Need Cloud Connect If the Network Latency Is the Same as on the Internet?

Consider the following when you are using Cloud Connect:

- **Network performance**
- **Transmission distance**
- **Advantages of Cloud Connect**

Network Performance Measuring Metrics

- Packet loss rate: the proportion of packets lost during network transmission

  This metric measures the network's packet forwarding capabilities. The difference between the number of packets from the sender and the number of packets to the receiver is the number of packets lost during network transmission. The percentage of the packets that are lost is the packet loss rate.

- Jitter: fluctuation in the latency of the packets flowing through the network

  Physical devices, such routers, that forward data packets on the network have buffers. When an amount of data that exceeds the transmission capacity of the cable is transmitted, physical devices will buffer excess packets. Packets that are not buffered or buffered for a short time arrive faster than those buffered for longer. This variation is called network jitter.

- Latency: the average round-trip time for transmitting packets between two network nodes

  For a store-and-forward device, the delay starts when the last bit of the last data frame enters the device and ends when the first bit of the data frame appears on the outbound interface. The time difference is the delay of the storage and forwarding device.

  Generally, there are the following types of delay:

  – Propagation delay: the time taken to transmit a packet in the transmission medium. Propagation delay is directly proportional to the physical distance between the two ends and the packet size. The longer the physical distance and the larger the packet, the longer the transmission delay.

  – Device delay: the time taken by a physical device, such as a router, to forward a data packet. The device delay is related to the forwarding performance of the switching device.

  – Packet conversion delay: the time taken for encoding and decoding data packets at both ends.

  – Jitter buffer delay: Generally, with IP communications for a voice service, a buffer is configured to eliminate the network jitter to prevent the voice quality from being discontinuous. The buffer also causes a certain delay.

Transmission Distance

Cloud Connect uses a DCI backbone network for communications, and the latency depends on the transmission distance and transmission loss.

- A longer distance results in more loss and higher latency.
- A shorter distance results in less loss and lower latency.

NOTE

To ensure connection reliability, inter-region services are usually carried by multiple connections. The length of each connection varies slightly. Therefore, Cloud Connect does not guarantee the latency.

Advantages of Cloud Connect Compared with the Internet

Two scenarios are presented here to compare the network performance of Cloud Connect and the Internet.

Table 1-1 Scenario details

ECS Specification	2 vCPUs and 4 GB memory
Bandwidth	4 Mbit/s
Regions of the VPCs that need to communicate with each other	CN North-Beijing4 (AZ1) and CN-Hong Kong (AZ1)
	CN East-Shanghai1 (AZ1) and CN-Hong Kong (AZ1)
Test Time	From 2020/09/09 18:30 to 2020/09/10 09:30 (15 hours in total)
How This Works	Internet: Bind EIPs to the servers in the VPCs. Cloud Connect: Load the VPCs in CN North-Beijing1, CN East-Shanghai1, and CN-Hong Kong to one cloud connection.

Quality of network between CN North-Beijing4 and CN-Hong Kong

Figure 1-1 Internet test results

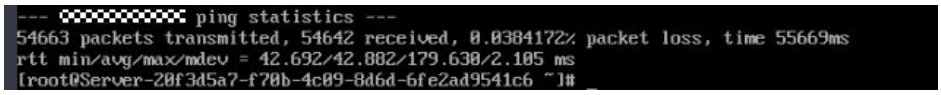


Figure 1-2 Cloud Connect test results

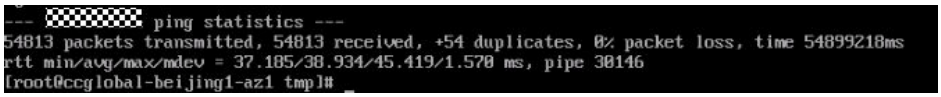


Table 1-2 Test comparison

Item	Packet Loss	Average Latency	Jitter
Cloud Connect	0%	38.9 ms	1.57 ms
Internet	0.04%	42.882 ms	2.105 ms

Quality of network connection between CN East-Shanghai1 and CN-Hong Kong

Figure 1-3 Internet test results

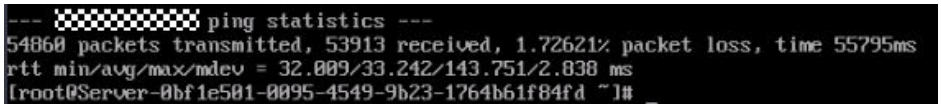


Figure 1-4 Cloud Connect test results

Table 1-3 Test comparison

Item	Packet Loss	Average Latency	Jitter
Cloud Connect	0%	32.14 ms	0.514 ms
Internet	1.73%	33.24 ms	2.838 ms

You can see from the test results that the performance of Cloud Connect is better than that of the Internet in terms of network latency. Cloud Connect outperforms the Internet in terms of packet loss and jitter.

In summary, Cloud Connect can provide more accurate data transmission and more stable network communications.

2 General Consulting and Service Use

2.1 What Can I Do with Cloud Connect?

Cloud Connect is a cloud service that allows you to connect VPCs in different regions to build a globally connected cloud network where instances can communicate with each other over a private network. With Cloud Connect, you can

- Connect VPCs in a single region.
- Connect VPCs in different regions.
- Connect multiple on-premises data centers to multiple VPCs in different regions after you connect the on-premises data centers to the cloud through Direct Connect or VPN.
- Reduce the network latency for access to backend services.

2.2 How Do I Configure Cloud Connect?

To configure Cloud Connect, perform the following steps on the management console:

1. Create a cloud connection, which will connect all the network instances loaded to it and allow the instances to communicate with each other over a private network.
2. Load the network instances that need to communicate with each other to the cloud connection. Two types of network instances are supported, VPC and virtual gateway.
3. If network instances are in different regions, buy a bandwidth package and bind it to the cloud connection.
4. Assign inter-region bandwidths for cross-region network communications.

2.3 What Are the Differences Between Cloud Connect and VPC Peering?

Cloud Connect differs from VPC Peering in the following ways:

- Interworking capabilities: VPC Peering can only connect two VPCs in the same region, but Cloud Connect can connect multiple VPCs either in the same region or in different regions.
- Network capabilities: After you create a VPC peering connection, you need to manually configure routes. With Cloud Connect, you do not need to configure routes.
- The bearer network: VPC Peering uses the data center network, but Cloud Connect uses a DCI backbone network.
- Billing: VPC Peering is free. With Cloud Connect, communications between VPCs in the same region is also free, but cross-region communications require a bandwidth package, which is not free.

Table 2-1 compares these differences.

Table 2-1 Differences between Cloud Connect and VPC Peering

Item		VPC Peering	Cloud Connect
Interworking capability	VPCs within a region	Supported	Supported
	VPCs across regions	Not supported	Supported
	Cross-border compliance	Not supported	Supported
Networking capability		Manual routing configuration	Automatic routing configuration
Bearer network		Data center network in the region	Inter-region DCI backbone network
Pricing		Free of charge	Free of charge within a region and billed based on standard pricing across regions

2.4 What Tools Can I Use to Test Network Connectivity After All Configurations Are Complete?

Use ICMP or Telnet to test whether the VPCs in different regions can communicate with each other.

2.5 What Network Instance Types Does Cloud Connect Support?

Currently, only VPCs and Direct Connect virtual gateways can be connected using Cloud Connect. VPNs will be supported soon.

2.6 How Many Bandwidth Packages Can I Bind to a Cloud Connection?

One cloud connection can only have one bandwidth package regardless of if the cloud connection is used for communications within a geographic region or between geographic regions.

For example, you have created a cloud connection and bound a 50 Mbit/s bandwidth package to the cloud connection for communications within the Chinese mainland. Before you unbind the bandwidth package from the cloud connection, you cannot bind another bandwidth package to the cloud connection for communications within the Chinese mainland. However, you can bind a bandwidth package to the cloud connection for communications in another geographic region or between geographic regions.

2.7 Are the Uplink and Downlink Rates of the Configured Inter-Region Bandwidth the Same?

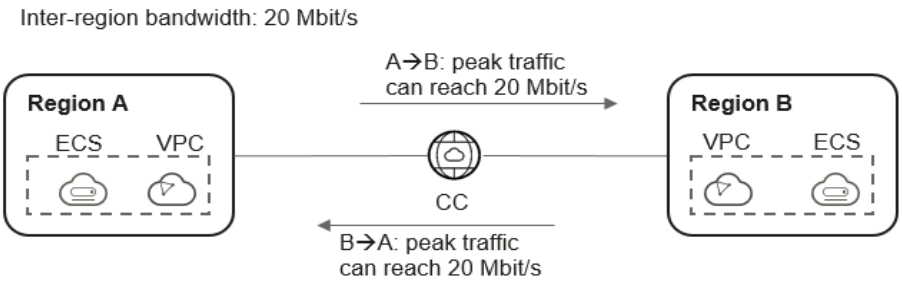
Yes.

If you purchase a 10 Mbit/s bandwidth package for network communications between the Chinese mainland and Asia Pacific and assign 5 Mbit/s of bandwidth between the CN East-Shanghai region and the CN-Hong Kong region, the maximum bandwidth from the CN East-Shanghai region to the CN-Hong Kong region and from the CN-Hong Kong region to the CN East-Shanghai region is 5 Mbit/s.

2.8 Are There Any Limits on the Traffic for Cross-Region Network Communications?

The traffic required when you are using Cloud Connect depends on the assigned inter-region bandwidth. The peak inbound or outbound traffic cannot exceed the inter-region bandwidth.

If you assign 20 Mbit/s bandwidth between regions, the peak traffic from region A and the peak traffic from region B cannot exceed 20 Mbit/s.



2.9 What Are the Metrics for Traffic Monitoring?

There are two metrics used to monitor the traffic: **Incoming Traffic** and **Outgoing Traffic**.

Incoming Traffic is the traffic from the other region to the current region.
Outgoing Traffic is the traffic from the current region to the other region.

2.10 What Are the Restrictions of Using Cloud Connect?

When you use Cloud Connect, note that:

- CIDR blocks of the network instances loaded to a cloud connection cannot overlap.
- Each account can create up to six cloud connections. A cloud connection can be used by network instances from up to six regions. In each region, a cloud connection can be used by up to six network instances.
- There are up to 50 routes for a cloud connection in all the regions where the cloud connection is used.

2.11 Where Can I Add Routes for a Cloud Connection on the Management Console?

If you load a VPC to a cloud connection, a route will be automatically assigned for each subnet you select. If you load a virtual gateway to a cloud connection, routes will be automatically assigned for the local and remote subnets. If you need a special route, you can add a custom CIDR block when loading the network instance.

You can view the routes in the default route tables of other VPCs loaded to the cloud connection or in the default route tables of the VPCs associated with other virtual gateways loaded to the cloud connection.

2.12 Do I Need to Bind an EIP to Each ECS in the VPCs Connected over a Cloud Connection?

If the ECSs are used only within the VPCs, you do not need EIPs.

If you want to access the ECSs from the Internet or use the ECSs to provide services accessible from the Internet, you need to purchase an EIP for each ECS.

2.13 How Can I Modify the Bandwidth of a Purchased Bandwidth Package?

Cloud Connect allows you to modify the bandwidth of a purchased bandwidth package.

To modify the bandwidth, perform the following operations:

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

   NOTE

   You can increase or decrease the bandwidth. In the following steps, increasing the bandwidth is used as an example.

   - If you increase the bandwidth, you need to pay for the increased bandwidth. The new bandwidth will take effect after you make the payment.
   - If you decrease the bandwidth, the system will refund the overpayment to your account. The new bandwidth takes effect immediately.
5. Select **Increase bandwidth** and click **Continue**.
6. Specify the new bandwidth and click **OK**.
7. Confirm the configuration and click **Submit**.
8. Select a payment method and click **Pay**.

NOTE

- Modifying the bandwidth does not interrupt services, but unsubscribing from a bandwidth package that has been bound to a cloud connection or unbinding a bandwidth package from a cloud connection will. Before you unsubscribe from a bandwidth package that has been bound to a cloud connection, unbind it from the cloud connection.
- If bandwidth package is going to expire within the next 24 hours, you cannot increase or decrease the bandwidth.

2.14 Will the Modified Inter-Region Bandwidth Take Effect Immediately?

No. It takes about 1 to 2 minutes before the new inter-region bandwidth can take effect.

2.15 How Can I Modify Inter-Region Bandwidth?

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

2.16 Do I Need to Create Another Cloud Connection If Network Instances in One Region Need to Communicate with Network Instances in Two Other Regions That Have Already Been Loaded to a Cloud Connection?

No.

Load the network instances in first region to the cloud connection used by network instances in the other two regions and assign inter-region bandwidth between each pair of regions.

In this way, network instances in the three regions can communicate with each other.

2.17 Are Network Circuits Physically Isolated?

No. Cloud Connect leverages the Huawei Cloud backbone network, and network circuits are logically isolated.

2.18 Is Cloud Connect an Out-Of-The-Box Service?

All operations that you perform on Cloud Connect take effect immediately, except for the cross-border permit, which takes effect only after it is approved by China Unicom.

2.19 How Can Cloud Connect Offer High Availability?

- If Cloud Connect is used to connect VPCs in the same region, Cloud Connect is deployed in clusters, and multiple clusters are deployed across AZs.
- If Cloud Connect is used to connect VPCs in different regions, the Huawei Cloud backbone network is used to connect the VPCs. The network between every two regions has at least two links that are configured in active/standby mode.
- Cloud Connect has a dedicated dialing test platform to monitor the status of clusters and links in real time.

3 Console Operations

3.1 How Do I Configure Cloud Connect?

To configure Cloud Connect, perform the following steps on the management console:

1. Create a cloud connection, which will connect all the network instances loaded to it and allow the instances to communicate with each other over a private network.
2. Load the network instances that need to communicate with each other to the cloud connection. Two types of network instances are supported, VPC and virtual gateway.
3. If network instances are in different regions, buy a bandwidth package and bind it to the cloud connection.
4. Assign inter-region bandwidths for cross-region network communications.

3.2 What Can I Do If There Is a Route Conflict When I Load a Network Instance to a Cloud Connection?

When you are loading a VPC, the system may display a message "A routing conflict has occurred in this VPC. This route is already being used in other scenarios, such as VPC Peering or VPN." If this happens, check whether the VPC is used by:

- Custom CIDR block
- Direct Connect
- VPN
- VPC peering connection

If the VPC is used by any of the above, there may be route conflicts. In this case, disassociate the VPC from the resource and then load the VPC to the cloud connection or select another VPC based on your network plan.

3.3 How Many Bandwidth Packages Can I Bind to a Cloud Connection?

One cloud connection can only have one bandwidth package regardless of if the cloud connection is used for communications within a geographic region or between geographic regions.

For example, you have created a cloud connection and bound a 50 Mbit/s bandwidth package to the cloud connection for communications within the Chinese mainland. Before you unbind the bandwidth package from the cloud connection, you cannot bind another bandwidth package to the cloud connection for communications within the Chinese mainland. However, you can bind a bandwidth package to the cloud connection for communications in another geographic region or between geographic regions.

3.4 What Are the Restrictions of Using Cloud Connect?

When you use Cloud Connect, note that:

- CIDR blocks of the network instances loaded to a cloud connection cannot overlap.
- Each account can create up to six cloud connections. A cloud connection can be used by network instances from up to six regions. In each region, a cloud connection can be used by up to six network instances.
- There are up to 50 routes for a cloud connection in all the regions where the cloud connection is used.

3.5 How Can I Apply for a Cross-Border Permit?

Preparing for Materials

You need to provide the following materials and ensure that all materials are stamped with your company's official seal:

- A scanned copy of your company's business license
- A scanned copy of the *Cloud Connect Cross-Border Circuit Service Agreement*
- A scanned copy of *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*

Applying for a Cross-Border Permit

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

The **Cross-Border Service Application System** page is displayed.

5. Fill in the enterprise and representative information, and upload the prepared materials.
6. Click **Submit**.

   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.

3.6 Where Can I Add Routes for a Cloud Connection on the Management Console?

If you load a VPC to a cloud connection, a route will be automatically assigned for each subnet you select. If you load a virtual gateway to a cloud connection, routes will be automatically assigned for the local and remote subnets. If you need a special route, you can add a custom CIDR block when loading the network instance.

You can view the routes in the default route tables of other VPCs loaded to the cloud connection or in the default route tables of the VPCs associated with other virtual gateways loaded to the cloud connection.

3.7 How Can I Modify the Bandwidth of a Purchased Bandwidth Package?

Cloud Connect allows you to modify the bandwidth of a purchased bandwidth package.

To modify the bandwidth, perform the following operations:

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

   NOTE

   You can increase or decrease the bandwidth. In the following steps, increasing the bandwidth is used as an example.

   - If you increase the bandwidth, you need to pay for the increased bandwidth. The new bandwidth will take effect after you make the payment.
   - If you decrease the bandwidth, the system will refund the overpayment to your account. The new bandwidth takes effect immediately.
5. Select **Increase bandwidth** and click **Continue**.
6. Specify the new bandwidth and click **OK**.
7. Confirm the configuration and click **Submit**.

8. Select a payment method and click **Pay**.

NOTE

- Modifying the bandwidth does not interrupt services, but unsubscribing from a bandwidth package that has been bound to a cloud connection or unbinding a bandwidth package from a cloud connection will. Before you unsubscribe from a bandwidth package that has been bound to a cloud connection, unbind it from the cloud connection.
- If bandwidth package is going to expire within the next 24 hours, you cannot increase or decrease the bandwidth.

3.8 How Can I Modify Inter-Region Bandwidth?

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

3.9 What Tool Can I Used to Test the Bandwidth Rate of a Cloud Connection?

You can use iPerf to send packets to an ECS in each VPC loaded to the cloud connection and test the bandwidth rate between regions.

3.10 Will the Modified Inter-Region Bandwidth Take Effect Immediately?

No. It takes about 1 to 2 minutes before the new inter-region bandwidth can take effect.

4 Bandwidth Packages

4.1 How Many Bandwidth Packages Can I Bind to a Cloud Connection?

One cloud connection can only have one bandwidth package regardless of if the cloud connection is used for communications within a geographic region or between geographic regions.

For example, you have created a cloud connection and bound a 50 Mbit/s bandwidth package to the cloud connection for communications within the Chinese mainland. Before you unbind the bandwidth package from the cloud connection, you cannot bind another bandwidth package to the cloud connection for communications within the Chinese mainland. However, you can bind a bandwidth package to the cloud connection for communications in another geographic region or between geographic regions.

4.2 How Can I Modify the Bandwidth of a Purchased Bandwidth Package?

Cloud Connect allows you to modify the bandwidth of a purchased bandwidth package.

To modify the bandwidth, perform the following operations:

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

NOTE

You can increase or decrease the bandwidth. In the following steps, increasing the bandwidth is used as an example.

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

5. Select **Increase bandwidth** and click **Continue**.
6. Specify the new bandwidth and click **OK**.
7. Confirm the configuration and click **Submit**.
8. Select a payment method and click **Pay**.

NOTE

- Modifying the bandwidth does not interrupt services, but unsubscribing from a bandwidth package that has been bound to a cloud connection or unbinding a bandwidth package from a cloud connection will. Before you unsubscribe from a bandwidth package that has been bound to a cloud connection, unbind it from the cloud connection.
- If bandwidth package is going to expire within the next 24 hours, you cannot increase or decrease the bandwidth.

4.3 How Do I Decrease the Bandwidth of a Bandwidth Package?

To decrease the bandwidth, perform the following operations:

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

5 Bandwidth, Latency and Packet Loss

5.1 What Can I Do If Cross-Region Network Communications Fail?

After you complete all the required configuration, you can use ICMP or Telnet to test network connectivity. If network communications fail, do the following to locate the fault:

- Check whether the security group containing the ECSs in the destination VPC allows ICMP or Telnet traffic over the corresponding port in the inbound direction. If ICMP or Telnet traffic is not allowed, the packets will be blocked by the security group.
- Check whether a network ACL is configured for the subnet in the destination VPC to deny the communications between the source and destination VPCs. If such an ACL exists, the packets will be blocked by the ACL.
- Check whether there are overlapping subnets in the source and destination VPCs. If they have overlapping subnets, the packets will not be sent to the subnet of the destination VPC.
- Check whether an inter-region bandwidth is assigned between source and destination regions. If you have a bandwidth package but there is no inter-region bandwidth between different regions, the default 10 kbit/s of bandwidth may fail to transmit large ICMP packets or Telnet packets.

5.2 Will the Modified Inter-Region Bandwidth Take Effect Immediately?

No. It takes about 1 to 2 minutes before the new inter-region bandwidth can take effect.

5.3 How Can I Troubleshoot Network Connectivity for a Hybrid Cloud Built Using Cloud Connect and Direct Connect?

- Ensure that the route table of your on-premises network have routes to send traffic to cloud resources.
- Ensure that the routes used by the on-premises network are included in the custom CIDR blocks configured for the VPCs connected through the cloud connection and Direct Connect connection.

5.4 Do I Need a Bandwidth Package for Testing Network Connectivity?

Cloud Connect provides you with 10 kbit/s of bandwidth for ping tests.

You do not need to purchase bandwidth packages for network communications within a region, but you need to purchase them and assign inter-region bandwidths for network instances in different regions.

5.5 Why Do I Need Cloud Connect If the Network Latency Is the Same as on the Internet?

Consider the following when you are using Cloud Connect:

- **Network performance**
- **Transmission distance**
- **Advantages of Cloud Connect**

Network Performance Measuring Metrics

- Packet loss rate: the proportion of packets lost during network transmission

  This metric measures the network's packet forwarding capabilities. The difference between the number of packets from the sender and the number of packets to the receiver is the number of packets lost during network transmission. The percentage of the packets that are lost is the packet loss rate.
- Jitter: fluctuation in the latency of the packets flowing through the network

  Physical devices, such routers, that forward data packets on the network have buffers. When an amount of data that exceeds the transmission capacity of the cable is transmitted, physical devices will buffer excess packets. Packets that are not buffered or buffered for a short time arrive faster than those buffered for longer. This variation is called network jitter.
- Latency: the average round-trip time for transmitting packets between two network nodes

  For a store-and-forward device, the delay starts when the last bit of the last data frame enters the device and ends when the first bit of the data frame

appears on the outbound interface. The time difference is the delay of the storage and forwarding device.

Generally, there are the following types of delay:

- Propagation delay: the time taken to transmit a packet in the transmission medium. Propagation delay is directly proportional to the physical distance between the two ends and the packet size. The longer the physical distance and the larger the packet, the longer the transmission delay.
- Device delay: the time taken by a physical device, such as a router, to forward a data packet. The device delay is related to the forwarding performance of the switching device.
- Packet conversion delay: the time taken for encoding and decoding data packets at both ends.
- Jitter buffer delay: Generally, with IP communications for a voice service, a buffer is configured to eliminate the network jitter to prevent the voice quality from being discontinuous. The buffer also causes a certain delay.

Transmission Distance

Cloud Connect uses a DCI backbone network for communications, and the latency depends on the transmission distance and transmission loss.

- A longer distance results in more loss and higher latency.
- A shorter distance results in less loss and lower latency.

NOTE

To ensure connection reliability, inter-region services are usually carried by multiple connections. The length of each connection varies slightly. Therefore, Cloud Connect does not guarantee the latency.

Advantages of Cloud Connect Compared with the Internet

Two scenarios are presented here to compare the network performance of Cloud Connect and the Internet.

Table 5-1 Scenario details

ECS Specification	2 vCPUs and 4 GB memory
Bandwidth	4 Mbit/s
Regions of the VPCs that need to communicate with each other	CN North-Beijing4 (AZ1) and CN-Hong Kong (AZ1)
	CN East-Shanghai1 (AZ1) and CN-Hong Kong (AZ1)
Test Time	From 2020/09/09 18:30 to 2020/09/10 09:30 (15 hours in total)

How This Works	Internet: Bind EIPs to the servers in the VPCs. Cloud Connect: Load the VPCs in CN North-Beijing1, CN East-Shanghai1, and CN-Hong Kong to one cloud connection.

Quality of network between CN North-Beijing4 and CN-Hong Kong

Figure 5-1 Internet test results

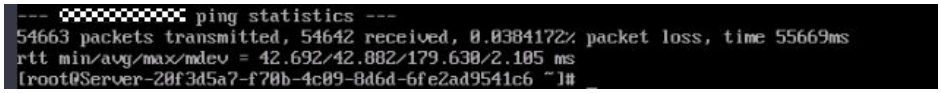


Figure 5-2 Cloud Connect test results

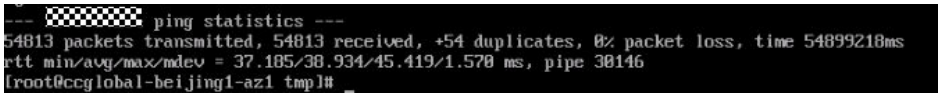


Table 5-2 Test comparison

Item	Packet Loss	Average Latency	Jitter
Cloud Connect	0%	38.9 ms	1.57 ms
Internet	0.04%	42.882 ms	2.105 ms

Quality of network connection between CN East-Shanghai1 and CN-Hong Kong

Figure 5-3 Internet test results

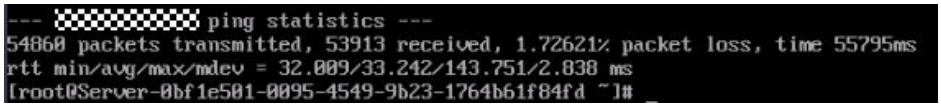


Figure 5-4 Cloud Connect test results

Table 5-3 Test comparison

Item	Packet Loss	Average Latency	Jitter
Cloud Connect	0%	32.14 ms	0.514 ms
Internet	1.73%	33.24 ms	2.838 ms

You can see from the test results that the performance of Cloud Connect is better than that of the Internet in terms of network latency. Cloud Connect outperforms the Internet in terms of packet loss and jitter.

In summary, Cloud Connect can provide more accurate data transmission and more stable network communications.

5.6 Are the Uplink and Downlink Rates of the Configured Inter-Region Bandwidth the Same?

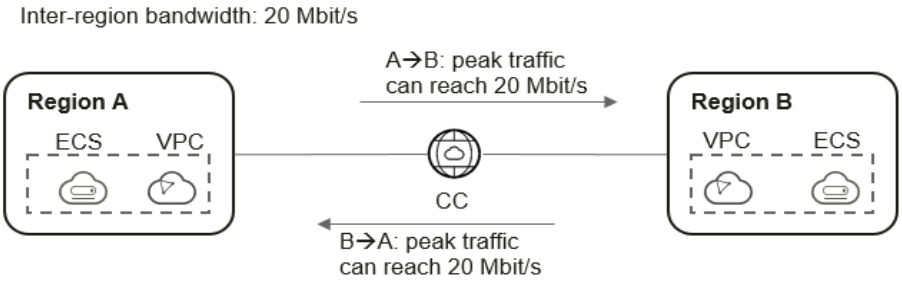
Yes.

If you purchase a 10 Mbit/s bandwidth package for network communications between the Chinese mainland and Asia Pacific and assign 5 Mbit/s of bandwidth between the CN East-Shanghai region and the CN-Hong Kong region, the maximum bandwidth from the CN East-Shanghai region to the CN-Hong Kong region and from the CN-Hong Kong region to the CN East-Shanghai region is 5 Mbit/s.

5.7 Are There Any Limits on the Traffic for Cross-Region Network Communications?

The traffic required when you are using Cloud Connect depends on the assigned inter-region bandwidth. The peak inbound or outbound traffic cannot exceed the inter-region bandwidth.

If you assign 20 Mbit/s bandwidth between regions, the peak traffic from region A and the peak traffic from region B cannot exceed 20 Mbit/s.



5.8 How Can I Modify an Inter-Region Bandwidth?

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

5.9 Are Network Circuits Physically Isolated?

No. Cloud Connect leverages the Huawei Cloud backbone network, and network circuits are logically isolated.

5.10 How Can Cloud Connect Offer High Availability?

- If Cloud Connect is used to connect VPCs in the same region, Cloud Connect is deployed in clusters, and multiple clusters are deployed across AZs.
- If Cloud Connect is used to connect VPCs in different regions, the Huawei Cloud backbone network is used to connect the VPCs. The network between every two regions has at least two links that are configured in active/standby mode.
- Cloud Connect has a dedicated dialing test platform to monitor the status of clusters and links in real time.

6 Cross-Border Permit

6.1 Why Do I Need a Cross-Border Permit?

This is a legal requirement. In accordance with the laws and administrative regulations of the Ministry of Industry and Information Technology (MIIT) of the People's Republic of China, only three major operators in the Chinese mainland are allowed for cross-border network communications. To carry out business outside the Chinese mainland, you need to apply for a cross-border permit from China Unicom because Huawei Cloud cooperates with China Unicom to centrally manage user profiles for cross-border businesses. Huawei Cloud provides cloud services and resources, and China Unicom provides the cross-border circuit services.

6.2 Who Approves Cross-Border Permits?

China Unicom approves cross-border permits and provides you with the cross-border circuit services.

6.3 How Can I Apply for a Cross-Border Permit?

Preparing for Materials

You need to provide the following materials and ensure that all materials are stamped with your company's official seal:

- A scanned copy of your company's business license
- A scanned copy of the *Cloud Connect Cross-Border Circuit Service Agreement*
- A scanned copy of *China Unicom Letter of Commitment to Information Security of the Cross-Border Circuit Service*

Applying for a Cross-Border Permit

1. Log in to the management console.

2. Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**.
3. In the navigation pane on the left, choose **Cloud Connect** > **Bandwidth Packages**.
4. On the displayed page, click **apply now**.

   The **Cross-Border Service Application System** page is displayed.
5. Fill in the enterprise and representative information, and upload the prepared materials.
6. Click **Submit**.

   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.

6.4 When Would I Need to Apply for a Cross-Border Permit?

To comply with China's laws and regulations on cross-border network communications, you need to apply for a cross-border permit before you can buy a bandwidth package for communications 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:

- Network communications between the Chinese mainland and Asia Pacific
- Network communications between the Chinese mainland and Southern Africa
- Network communications 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 on the Cloud Connect console. China Unicom will review and approve the application within one working day. After the application is approved, you can buy bandwidth packages.

6.5 How Long Will a Cross-Border Permit Be Approved?

Cross-border permits are approved within one working day.

6.6 Why Is Additional Real-Name Authentication Required After I Have Completed Huawei Cloud Real-Name Authentication?

- Huawei Cloud real-name authentication information is used for billing and issuing invoices.
- Cloud Connect real-name authentication is required for China Unicom to approve your application for the cross-border permit, which is required if you want to access a VPC or on-premises data center outside the Chinese mainland. China Unicom will archive your information for auditing if necessary.

6.7 Can I Modify the Content of the *Cloud Connect Cross-Border Circuit Service Agreement*?

No.

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

6.8 Can I Download the Materials for My Cross-Border Permit Application on the Console After I Delete Them from My PC?

No, you cannot.

Keep your application materials safe and secure.

6.9 Does Huawei Cloud Need to Sign and Stamp the Seal on the Materials for Cross-Border Permit Application?

No.

Huawei Cloud works with China Unicom to enable network communications 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).

7 Networking and Cloud Connect Scenarios

7.1 Can Cloud Connect Link VPCs in the Same Region?

Yes. After you load the VPCs in the same region to a cloud connection, they can communicate with each other by default. No bandwidth packages are required. If you require lower network latency, use VPC Peering instead of Cloud Connect.

7.2 Can I Load the VPCs of Other Accounts to My Cloud Connection?

Yes. You can load the VPCs of other users as long as you have obtained their permission to load these VPCs to your cloud connection.

8 Cross-Account Authorization

8.1 Does the Other User Need to Buy a Bandwidth Package If I Want to Load This Other User's VPCs to My Cloud Connection?

No.

If you want to load the VPCs of other users to your cloud connection, you need to request other users to grant you the permissions to load their VPCs. These other users do not need to buy a bandwidth package in their accounts.

8.2 Does the Other User Need to Create a Cloud Connection If I Want to Load This Other User's VPCs to My Cloud Connection?

No.

If you want to load the VPCs of other users to your cloud connection, you need to request other users to grant you the permissions to load their VPCs. These other users do not need to create a cloud connection in their accounts.

8.3 How Do I Load VPCs Across Accounts?

Scenarios

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

Procedure

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

3. In the navigation pane, choose **Cloud Connect** > **Cross-Account Authorization**.
4. Click **Network Instances Authorized by Me**.
5. Click **Authorize Network Instance**.

   Select a region and a VPC, and enter the peer account ID and peer cloud connection ID.
6. Click **OK**.

Helpful Links

For details, see **Connecting the VPCs in Your Account to the VPCs in Another User's Account**.

8.4 Can a VPC Be Loaded to More than One Cloud Connection?

No.

A VPC can only be loaded to one cloud connection.

9 Permissions

9.1 How Can I Grant Cloud Connect Permissions to IAM Users?

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

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

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

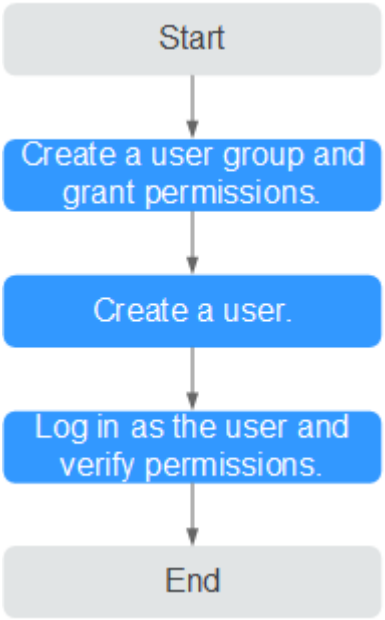
Figure 9-1 shows the process for granting permissions.

Prerequisites

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

Process Flow

Figure 9-1 Process for granting Cloud Connect permissions



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

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

2. **Create an IAM user**.

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

3. **Log in** and verify permissions.

   Log in to the Cloud Connect console using the created user and verify that the user only has the assigned permissions for Cloud Connect.

   - Hover on the upper left corner to display **Service List** and choose **Networking** > **Cloud Connect**. Click **Create Cloud Connection** in the upper right corner. If the cloud connection can be created, the **Cross Connect Administrator** policy has taken effect.
   - Choose any other service in the **Service List**. A message will appear indicating that you have sufficient permissions to access the service.

Helpful Links

Cloud Connect Permission Management

10 Monitoring

10.1 Why Is the Bandwidth Monitoring Data on the Cloud Eye Console Incomplete?

Cloud Eye collects data every 5 minutes, which is called a metric collection point. During data collection, about 5% of data is lost. However, all the data will be collected after another 2 hours.

10.2 How Do I View the Bandwidth Monitoring Data of a Cloud Connection?

- Navigate to the Cloud Eye console, choose **Cloud Service Monitoring** > **Cloud Connect** in the navigation pane, locate the cloud connection, and click **View Metric** in the **Operation** column to view its monitoring data.
- On the **Inter-Region Bandwidths** tab page, click the icon in the **Monitoring** column.

  For detailed operations, see **Viewing Metrics**.

10.3 Is There Monitoring Data Immediately After I Assign an Inter-region Bandwidth?

No.

Each time you assign or modify inter-region bandwidth, data needs to be synchronized. Data synchronization requires about one day. The monitoring data will be updated one day later.

10.4 What Are the Metrics for Traffic Monitoring?

There are two metrics used to monitor the traffic: **Incoming Traffic** and **Outgoing Traffic**.

Incoming Traffic is the traffic from the other region to the current region.
Outgoing Traffic is the traffic from the current region to the other region.

11 Quotas

11.1 How Can I Increase Resource Quotas?

What Is Quota?

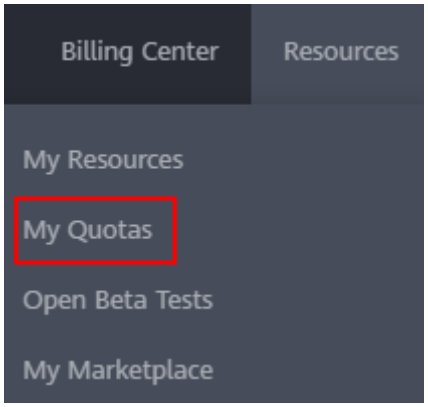
Quotas can limit the number or amount of resources available to users, such as the maximum number of ECSs or EVS disks that can be created.

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

How Do I View My Quotas?

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

   Figure 11-1 My Quotas

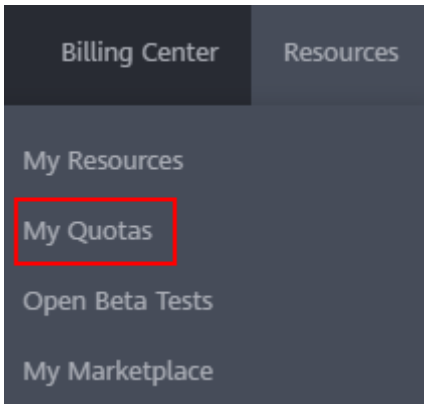
   

4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

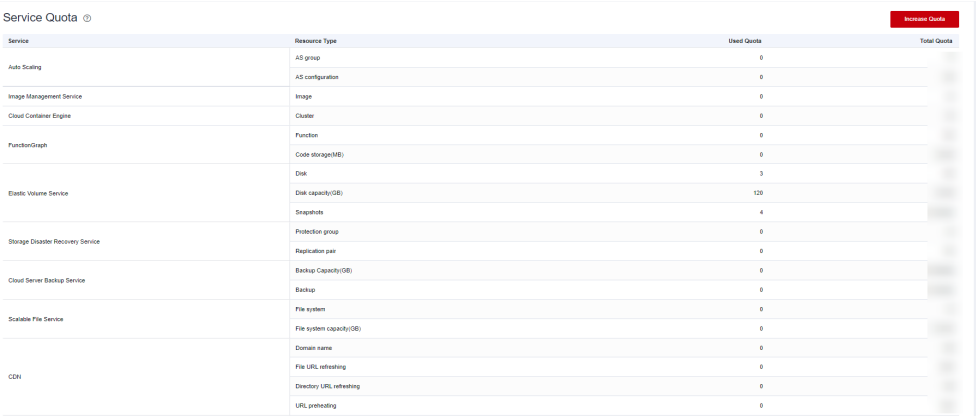
1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 11-2 My Quotas

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

   Figure 11-3 Increasing quota

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**.

