ALIBABA CLOUD

Alibaba Cloud

云企业网

Best Practices

Document Version: 20220401

Alibaba Cloud

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.

2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.

3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.

4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).

5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.

6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions

Style	Description	Example
Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	**Danger:** Resetting will result in the loss of user configuration data.
Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	**Warning:** Restarting will cause business interruption. About 10 minutes are required to restart an instance.
Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	**Notice:** If the weight is set to 0, the server no longer receives new requests.
Note	A note indicates supplemental instructions, best practices, tips, and other content.	**Note:** You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click **Settings**> **Network**> **Set network type**.
Bold	Bold formatting is used for buttons , menus, page names, and other UI elements.	Click **OK**.
`Courier font`	Courier font is used for commands	Run the `cd /d C:/window` command to enter the Windows system folder.
Italic	Italic formatting is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	This format is used for an optional value, where only one item can be selected.	`ipconfig [-all|-t]`
{} or {a|b}	This format is used for a required value, where only one item can be selected.	`switch {active|stand}`

Table of Contents

1.Migrate Express Connect peering connections to CEN

1.1. Migration overview

This topic describes how to migrate virtual private clouds (VPCs) and virtual border routers (VBRs) that use Express Connect peer connections to a Cloud Enterprise Network (CEN) instance. You can use CEN to establish private connections between VPCs, and between VPCs and data centers. CEN uses automatic route learning and distribution to accelerate network convergence and improve the quality of cross-network communication. This way, all network instances attached to CEN can communicate with each other.

Procedure

After you prepare a CEN instance, you can attach VPCs and VBRs that use peer connections to the CEN instance, and then configure routes.

The CEN instance automatically learns and distributes the routes of the attached network instances. After a VPC or VBR that uses a peer connection is attached to a CEN instance, the static route of the peer connection has a higher priority than the dynamic route of the CEN instance. If a route from the CEN instance is more specific than or the same as the static route of the peer connection, the route cannot be learnt. To ensure a successful migration, we recommend that you split a route that points to a large CIDR block into multiple child routes. After the CEN instance learns the child routes, you can delete them. For more information about how to migrate VPCs and VBRs to a CEN instance, see Migrate a VPC from a peering connection to a CEN instance and Migrate a VBR from a peering connection to a CEN instance.

Differences between connections of CEN and peer connections of Express Connect

You can establish private connections between VPCs that are attached to a CEN instance, and between VPCs and data centers. CEN is developed with more flexible and simplified configurations than peer connections of Express Connect. In addition, connections that are established through CEN are more stable. The following table describes the differences in detail.

Item	CEN	Express Connect
Network connection	Network-wide interconnection All networks (VPCs and Virtual Border Routers) associated with a CEN instance are interconnected with each other. A secure, reliable, and high-speed intranet communication channel can be established between any two networks.	Single point interconnection Express Connect connections cannot be extended. Specifically, the VPCs or on-premises data centers that are connected through Express Connect can only communicate with the peer VPCs.

Item	CEN	Express Connect
Route management	Dynamic learning Based on the Fullmesh link, CEN dynamically learns and distributes routes, which improves the convergence of routes, and the quality and security of network communication.	Manual configuration Express Connect requires end-to-end manual route configuration.
Bandwidth management	Cross-region shared bandwidth package CEN provides bandwidth packages which are sold by region to facilitate cross-region bandwidth adjustments. Bandwidth packages also help optimize resource allocation and save costs.	Point-to-point purchase The bandwidth of an Express Connect connection must be specified when you create the connection. You can adjust the bandwidth value after you create an Express Connect connection, but you cannot change the connected regions.

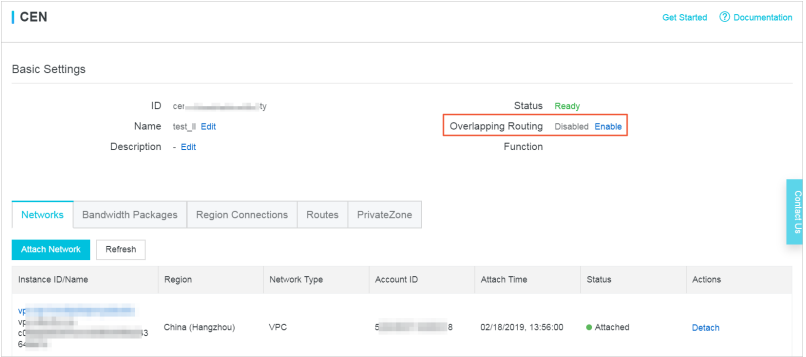
1.2. Migrate a VPC from a peering connection to a CEN instance

This topic describes how to migrate a virtual private cloud (VPC) from a peering connection in Express Connect to a Cloud Enterprise Network (CEN) instance. CEN allows you to establish private network connections between VPCs or between a VPC and a data center. CEN can automatically advertise and learn routes to accelerate network convergence and improve network quality in inter-network communication scenarios. This enables networks to communicate with each other.

Warning Before you suspend or delete the router interfaces of a peering connection, make sure that the routes for both the virtual border router (VBR) and the connected VPC from the peering connection are migrated.

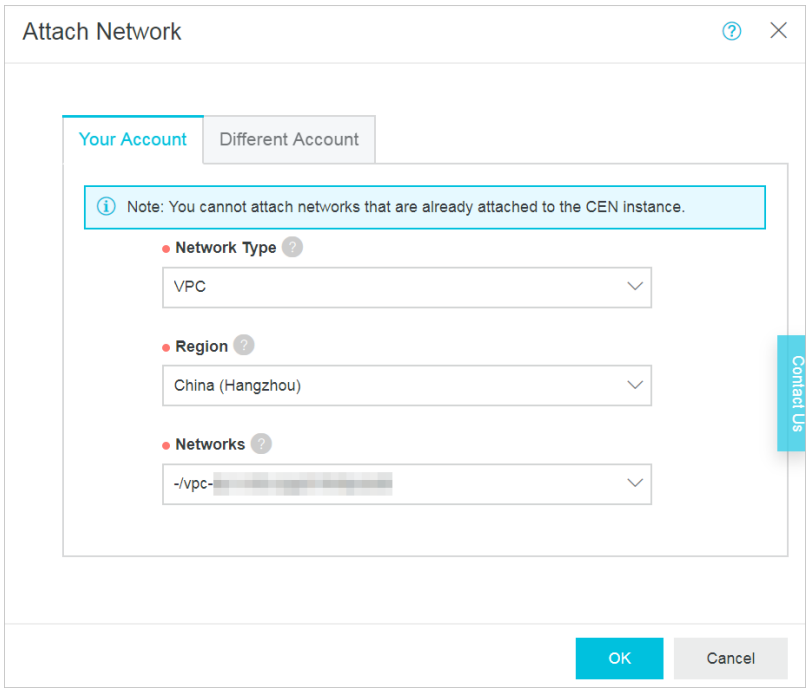
Prerequisites

Overlapping routing is enabled for the CEN instance that you want to use, as shown in the following figure. For more information, see Enable overlapping routing.



Procedure

1. If you do not have a CEN instance, create one and attach the VPC that you want to migrate to the CEN instance. For more information, see Create a CEN instance.
2. Attach the VPCs that you want to migrate to the CEN instance. For more information, see Attach a network instance.



3. If you want to enable inter-region network communication, purchase a bandwidth plan and allocate bandwidth to inter-region connections. For more information, see Purchase a bandwidth plan and Configure bandwidth for cross-region connections.
4. If you have added routes that point to Elastic Compute Service (ECS) instances, virtual private network (VPN) gateways, or high-availability virtual IP addresses (HAVIPs), you must advertise these routes to the CEN instance in the CEN console. For more information, see Advertise routes to CEN.
5. Check the routes of the VPC.

   The static routes of a peering connection have higher priorities than the dynamic routes of the CEN instance. If static routes of the peering connection are retained on the CEN instance, the CEN instance cannot learn duplicate static routes or routes that are longer than the static routes. The system prompts you if overlapped routes are detected.

After you attach the VPC to the CEN instance, you can log on to the CEN console, click the ID of the CEN instance on the **Instances** page, and then click the **Routes** tab to check whether routes of the VPC are overlapped.

If routes are overlapped, you can migrate the VPC by using the following methods:

- Delete the routes

  Delete the routes of the peering connection in the VPC console. The CEN instance then automatically learns and advertises routes. The deletion of the routes causes transient connections. For more information, see Add and delete route entries.

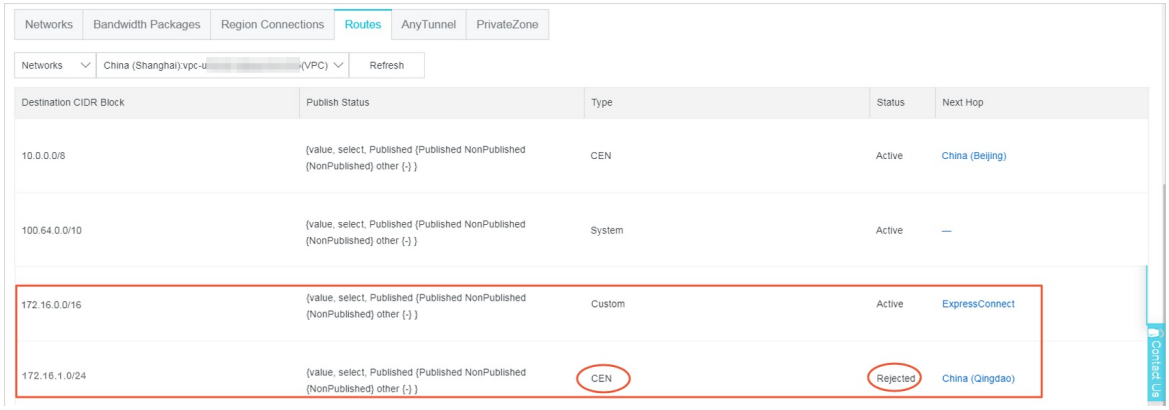
  > **Notice** The duration of the transient connection varies based on the number of CEN routes. For important business scenarios, we recommend that you use the following method to smoothly migrate the VPC.

- Split the routes

  Split the routes of the peering connection into several routes. After the CEN instance learns the routes of the peering connection, delete the routes that are split from the original routes. This method ensures smooth migration.

6. Migrate the overlapped routes.

   The following figure shows how to migrate overlapped routes. After you attach the VPC to the CEN instance, the VPC retains the route that points to 172.16.0.0/16. However, the route of the peering connection that points to 172.16.1.0/24 cannot be learned because the route is longer than the one that points to 172.16.0.0/16. The routes are overlapped.



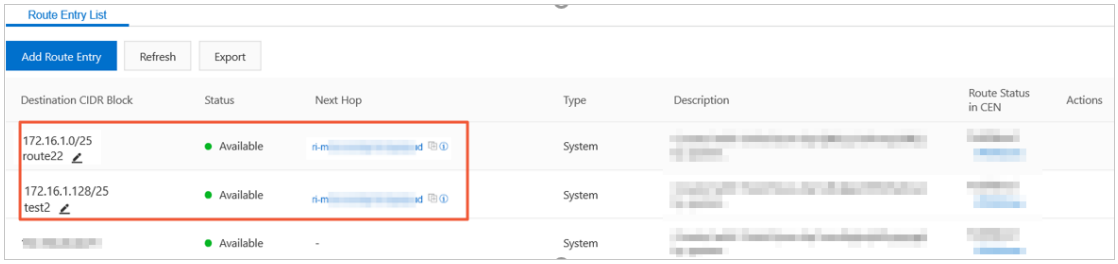
   In this case, you must split the route that points to 172.16.0.0/16 into longer routes that point to the following CIDR blocks: 172.16.1.0/25 and 172.16.1.128/25.

   i. Log on to the VPC console.

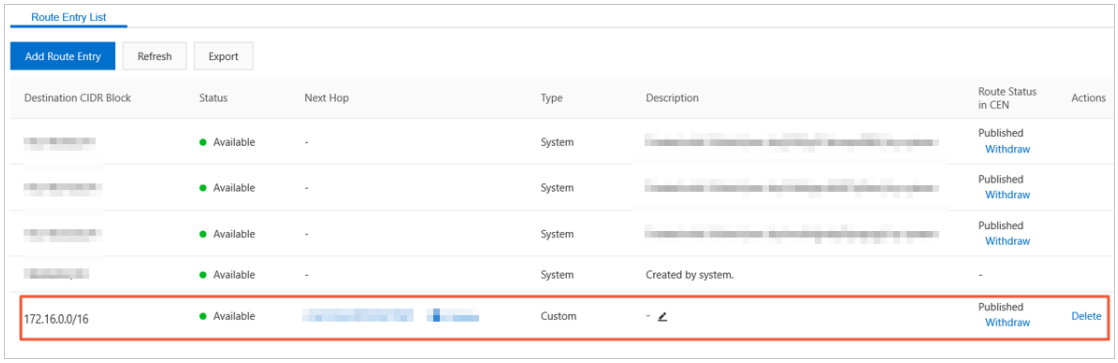
   ii. In the top navigation bar, select the region where the VPC is deployed.

   iii. In the left-side navigation pane, click **Route Tables**. On the **Route Tables** page, click the ID of the route table that you want to manage.

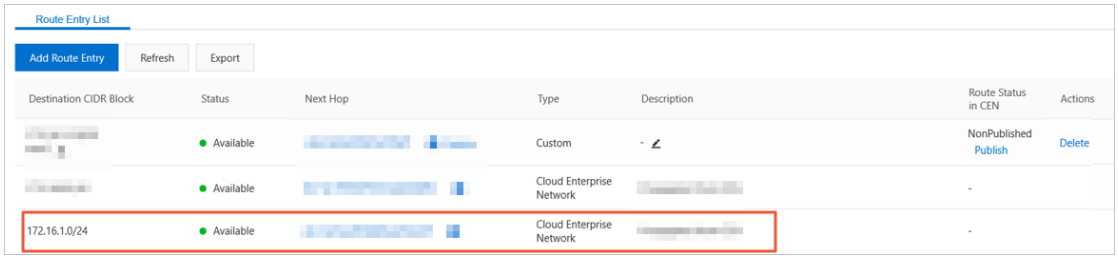
iv. On the **Custom Route** tab, click **Add Route Entry** to add two routes whose destination CIDR blocks are 172.16.1.0/25 and 172.16.1.128/25. The next hops are the router interface of the peering connection.



v. After you add the preceding two routes, delete the route that points to 172.16.0.0/16.



vi. Refresh the CEN route list to check whether the route that points to 172.16.1.0/24 is learned.



vii. After the routes in the CEN instance take effect, delete the routes that point to 172.16.1.0/25 and 172.16.1.128/25. The VPC is smoothly migrated to the CEN instance.

1.3. Migrate a VBR from a peering connection to a CEN instance

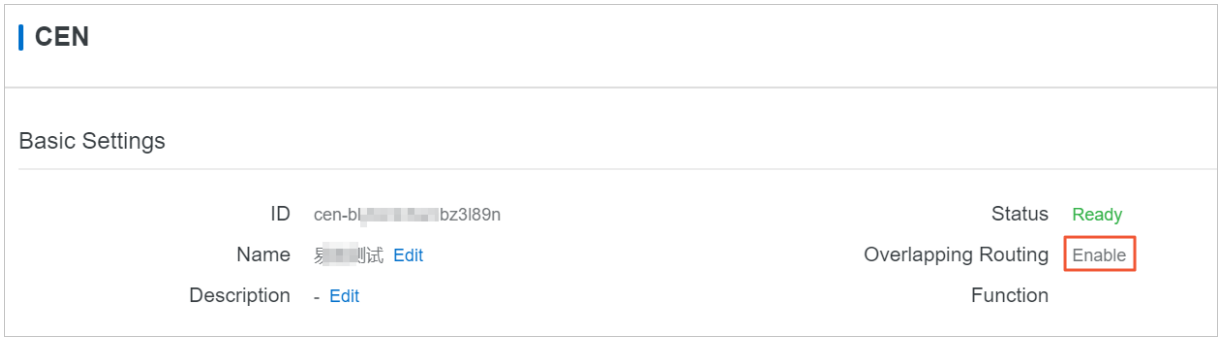
This topic describes how to migrate a virtual border router (VBR) from a peering connection in Express Connect to a Cloud Enterprise Network (CEN) instance. CEN allows you to enable communication between VPCs and between VPCs and on-premises data centers by using internal network connections. CEN automatically learns and distributes routes to quickly adapt to network changes. This improves the quality of cross-network communication.

Warning Before you freeze or delete the router interfaces of the peering connection, make sure that the routes for both the VBR and the connected VPC in the peering connection are migrated.

Preparations

If you want to migrate the VBR to an existing CEN instance, make sure that the overlapping routing function is enabled for the CEN instance.

> **Note** If the overlapping routing function is not enabled, enable it first.



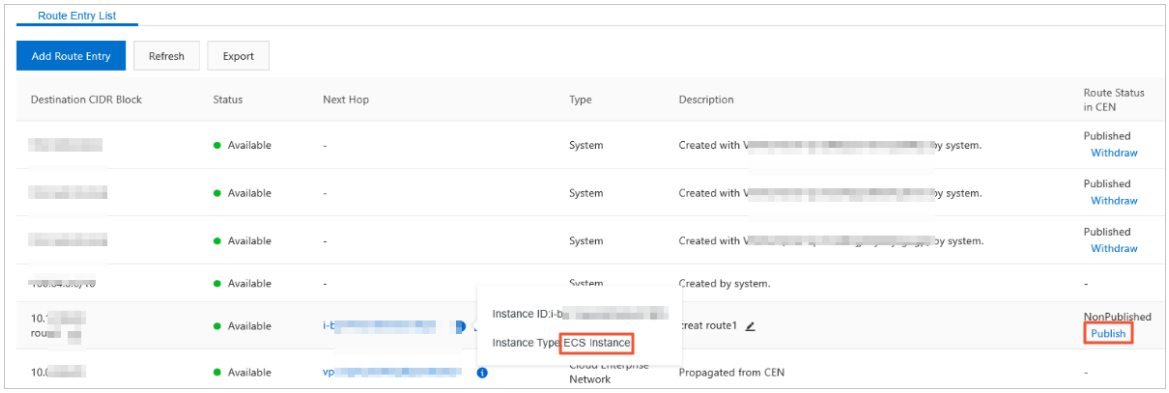
Procedure

To migrate a VBR from a peering connection to a CEN instance, perform the following steps:

> **Note** Before the migration, make sure that you complete the preparations.

1. If you have configured health checks for the VBR, delete the health check settings in the Express Connect console.
2. Log on to the CEN console.
3. On the **Instances** page, find the required CEN instance and click its ID.
4. On the **Networks** tab, click **Attach Network** to attach the VBR that you want to migrate and the VPC that is connected to the VBR. For more information, see Attach a network instance.
5. If you want to communicate across regions, purchase a bandwidth plan and configure bandwidth for the communication.

   For more information, see Manage bandwidth for cross-region connections.
6. If you have added routes that point to high-availability virtual IP addresses (HAVIPs) or IP addresses of ECS instances and VPN gateways, go to the VPC console and advertise these routes to the CEN instance based on your connection requirements.



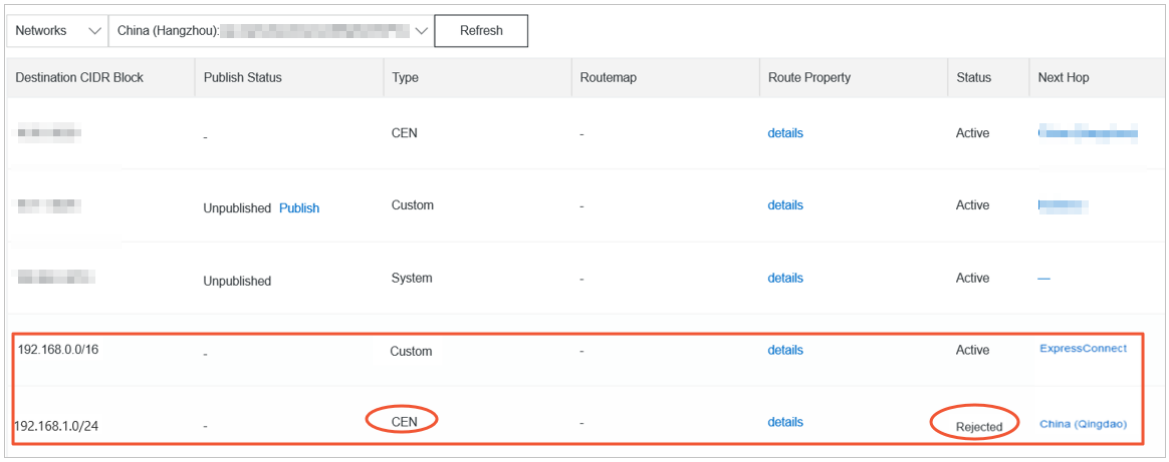
7. If your on-premises data center needs to access Alibaba Cloud services, such as Object Storage Service (OSS) and PrivateZone, configure the connections in the CEN console.

   For more information, see Access PrivateZone.

8. Log on to the CEN console and click the ID of the required CEN instance. Then, click the **Routes** tab to view the route information. Make sure that the routes do not conflict after you attach the VBR and VPC to the CEN instance.

   The static routes configured in the peering connection have higher priorities than the dynamic routes of the CEN instance. Specifically, if a static route is configured in the peering connection, CEN does not learn routes that are more specific than the static route and have the same destination as the static route. We recommend that you split static routes in the peering connection and delete them after CEN learns the routes. This ensures smooth migration.

   In the following figure, the route to 192.168.1.0/24 in the CEN instance is more specific than the route to 192.168.0.0/16 in the peering connection. Therefore, the two routes are in conflict.



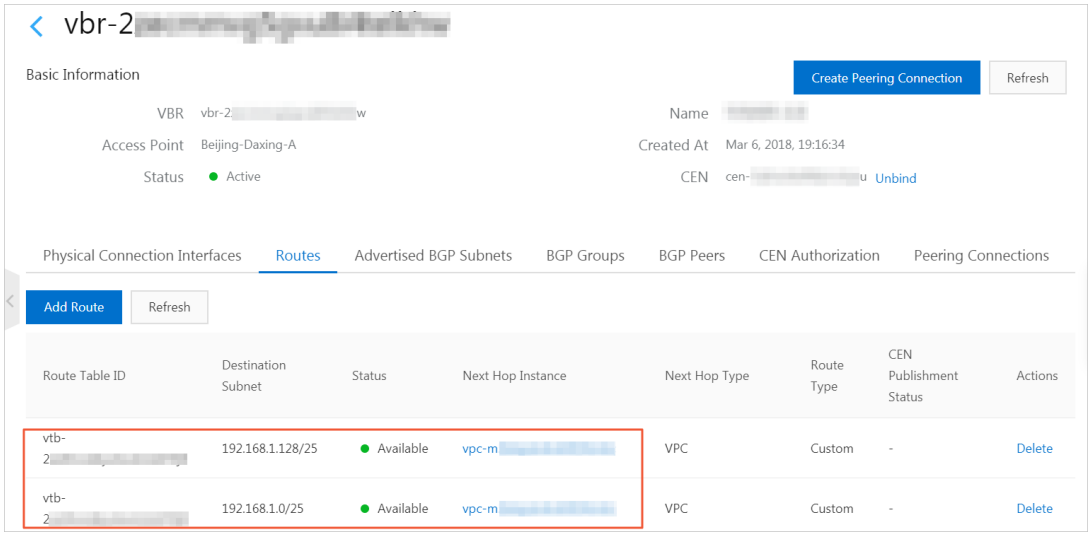
   - If you can tolerate a transient network interruption during the migration, delete the route to 192.168.0.0/16. Then, the route in the CEN instance automatically takes effect.

     The duration of the network interruption varies based on the number of CEN routes. For important business scenarios, we recommend that you use the following method to smoothly migrate the VBR.

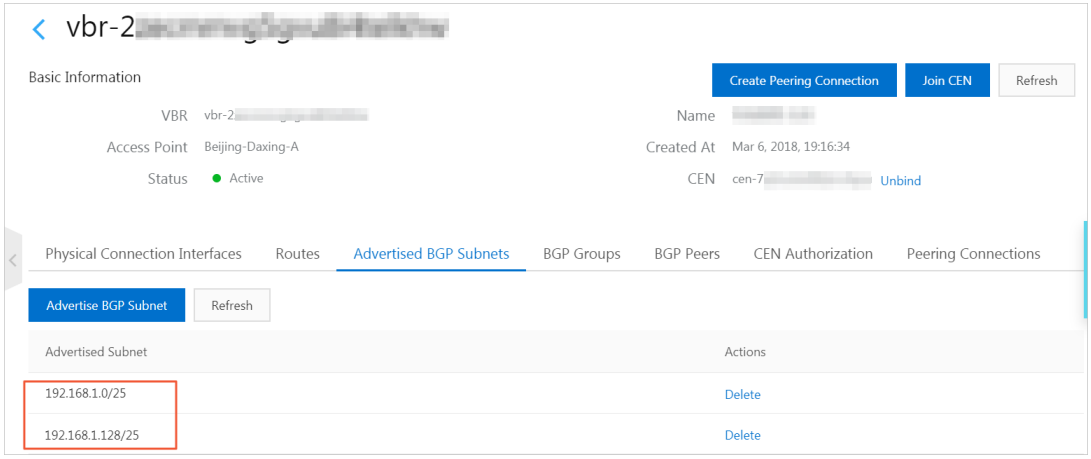
   - If you want to smoothly migrate the VBR, split the route in the peering connection into routes more specific than the route to 192.168.1.0/24 in the CEN instance. For example, split the route to 192.168.0.0/16 in the peering connection into routes to 192.168.1.0/25 and 192.168.1.128/25.

     a. In the Express Connect console, click Virtual Border Routers (VBRs). Find the required VBR, click its ID, and click the **Routes** tab.

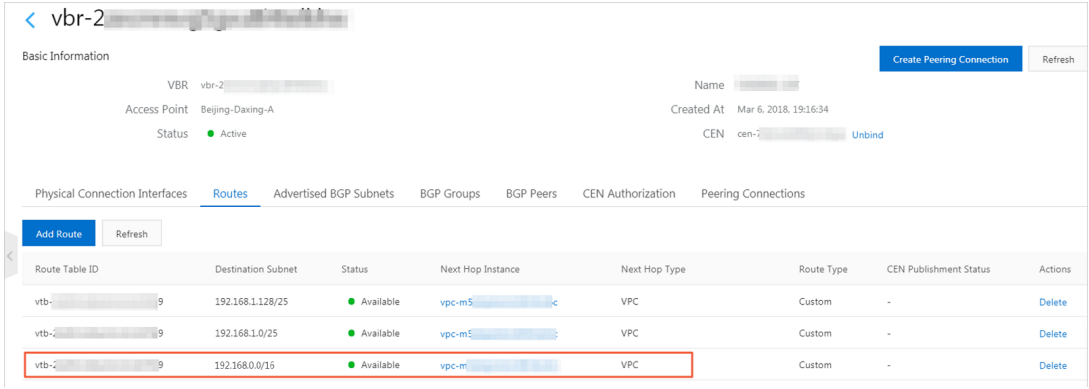
b. Click **Add Route** to add two routes in which the destination CIDR blocks are 192.168.1.0/25 and 192.168.1.128/25 and the next hops are the VPC to which the VBR is connected.



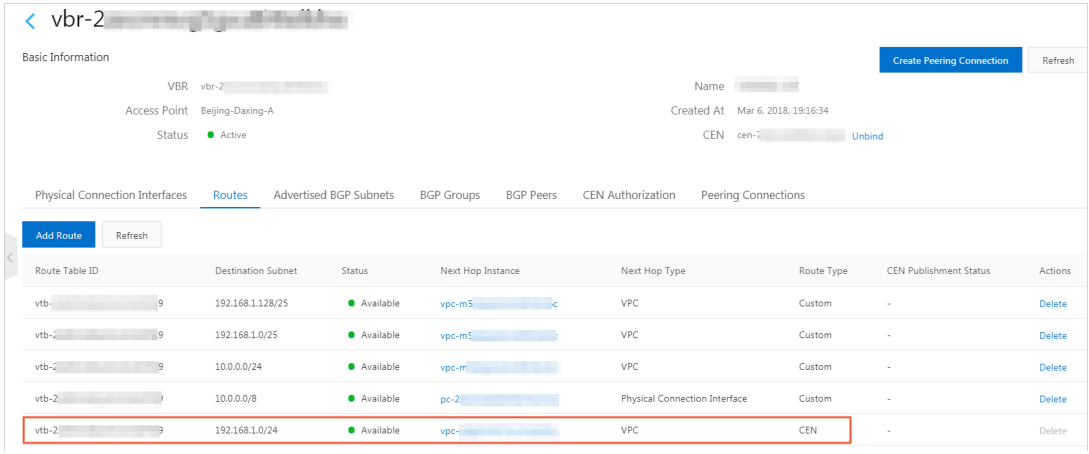
c. If BGP is used, advertise the routes to 192.168.1.0/25 and 192.168.1.128/25.



d. Delete the route to 192.168.0.0/16 in the peering connection.



e. Click **Refresh** to check whether the routes in the CEN instance take effect.



f. Delete the routes to 192.168.1.0/25 and 192.168.1.128/25 in the VBR route table and the advertised BGP routes.

g. In the CEN console, configure health checks for the VBR. For more information, see Configure health checks.

1.4. Roll back the migration

This topic describes how to roll back your migration by modifying the routes.

Rollback solutions depend on the migration methods you have adopted. The available rollback solutions are as follows:

- Migration with intermittent disconnections: Re-add the deleted static route of the peering connection. All the routes that are more detailed than or equals the re-added peering connection route are automatically deleted.
- Smooth migration: Re-add the deleted detailed routes directly.

> **Note** If the migrated Virtual Border Router (VBR) is configured with BGP routes, you need to re-advertise the related CIDR blocks.

2.Best practices for route maps

2.1. Stop the communication between a VPC and other networks attached to a CEN instance

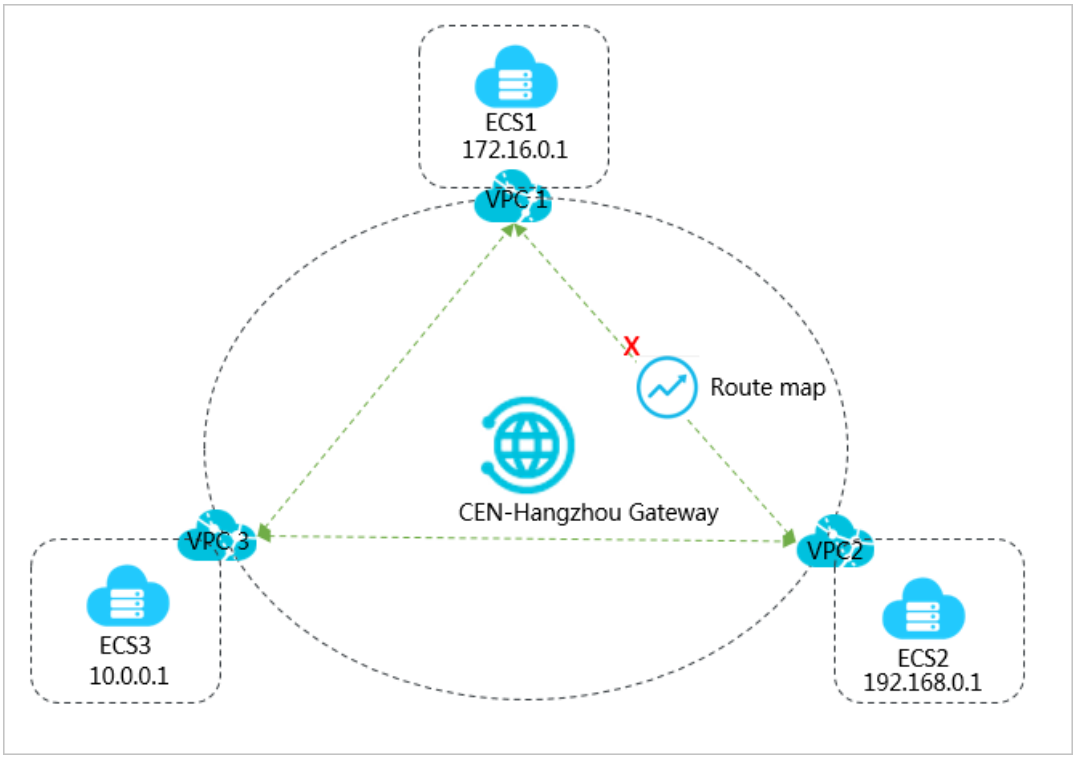
This topic describes how to use route maps to stop the communication between a Virtual Private Cloud (VPC) and other networks that are attached to the same Cloud Enterprise Network (CEN) instance.

Prerequisites

A CEN instance is created and the required networks are attached to the CEN instance. For more information, see Create a CEN instance and Attach a network instance.

Context

VPCs can communicate with VPCs, Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs) that are attached to the same CEN instance by default. However, you may need to block the communication between two VPCs, or between a VPC and a VBR or CCN. In this topic, two VPCs are used as an example to show you how to stop the communication between two VPCs by using route maps.

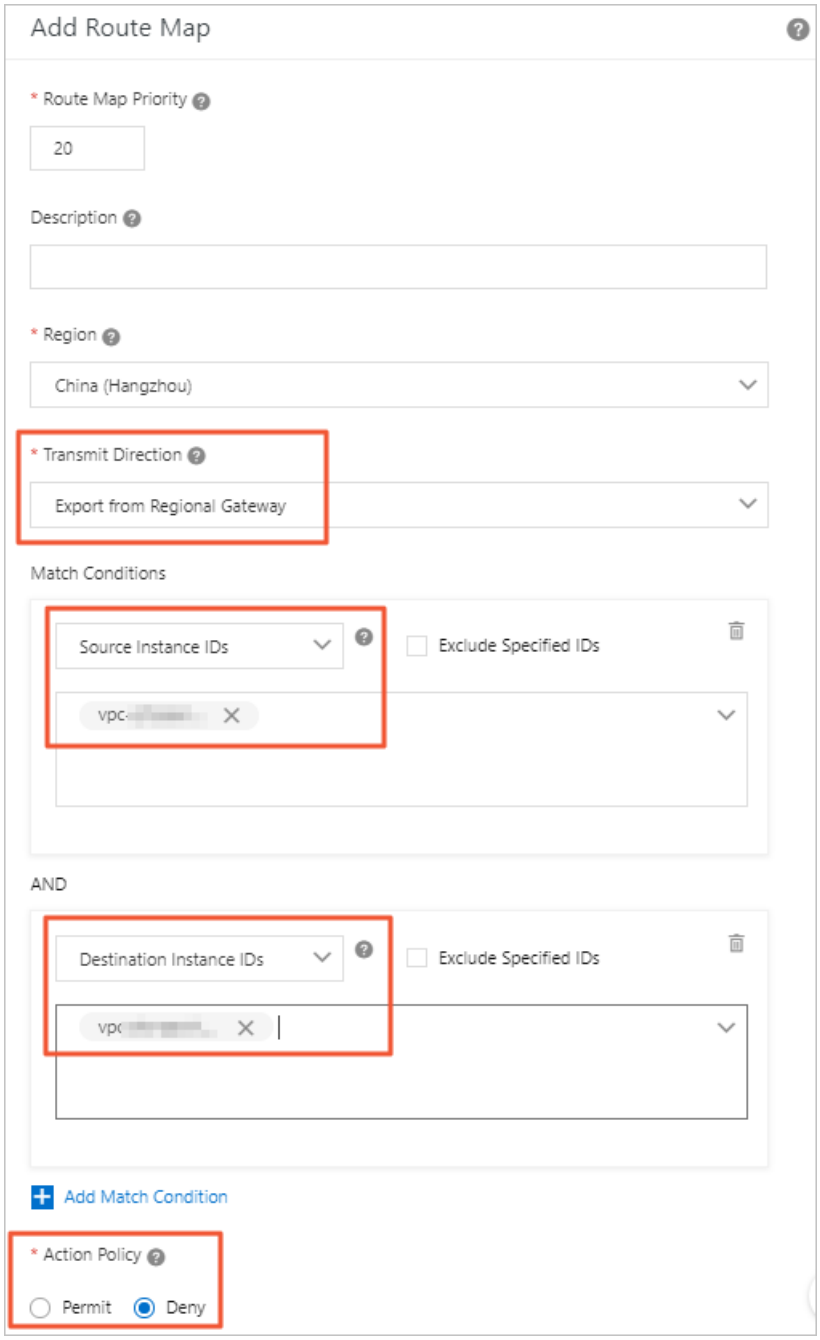


As shown in the preceding figure, VPC1, VPC2, and VPC3 are attached to CEN. By default, VPC1, VPC2, and VPC3 are all connected and can communicate with each other. By using route maps, you can block the communication between VPC1 and VPC2 while VPC1 and VPC2 can still communicate with VPC3.

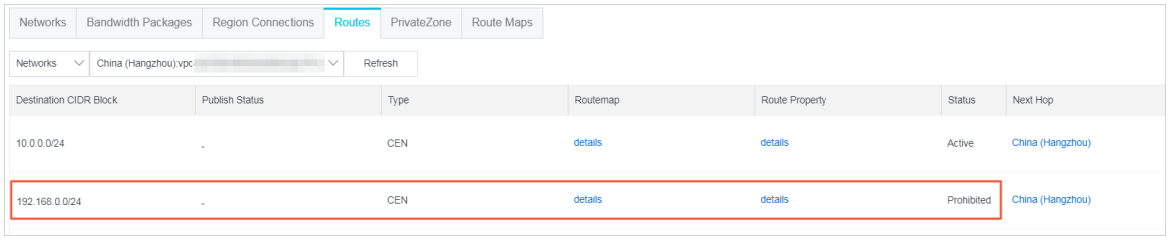
Step 1: Set a route map to deny access from VPC1 to VPC2

To set a route map to deny access from VPC1 to VPC2, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the target CEN instance and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
5. On the **Add Route Map** page, configure the route map according to the following information and then click **OK**.
   - **Route Map Priority**: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter **20**.
   - **Region**: Select the region to which the route map is applied. In this example, select **China (Hangzhou)**.
   - **Transmit Direction**: Select the direction in which the route map is applied. In this example, select **Export from Regional Gateway**.
   - **Match Conditions**: Set the match conditions of the route map. In this example, add a match condition and set the source instance ID to the ID of VPC2 and the destination instance ID to the ID of VPC1.
   - **Action Policy**: Select the action that is performed to a route if the route meets all the match conditions. In this example, select **Deny**.



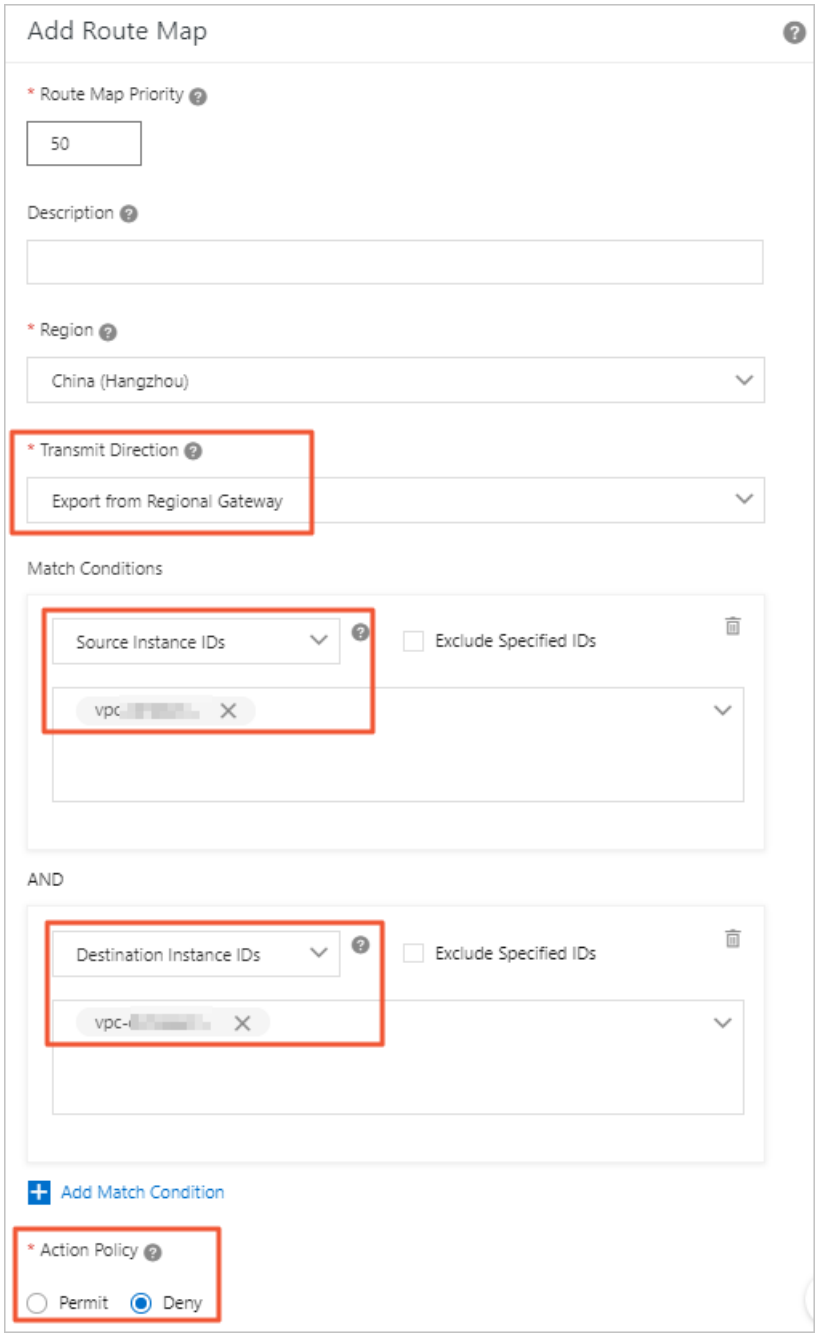
After you add the route map, you can view the route that denies access from VPC1 to VPC2 on the **Routes** tab.



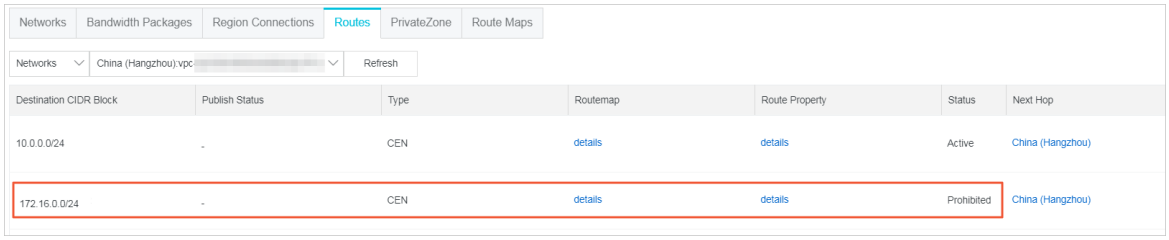
Step 2: Set a route map to deny access from VPC2 to VPC1

To set a route map to deny access from VPC2 to VPC1, follow these steps:

1. In the left-side navigation pane, click **Instances**.
2. On the **Instances** page, find the target CEN instance and click **Manage** in the **Actions** column.
3. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
4. On the **Add Route Map** page, configure the route map according to the following information and then click **OK**.
   - **Route Map Priority**: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter **50**.
   - **Region**: Select the region to which the route map is applied. In this example, select **China (Hangzhou)**.
   - **Transmit Direction**: Select the direction in which the route map is applied. In this example, select **Export from Regional Gateway**.
   - **Match Conditions**: Set the match conditions of the route map. In this example, add a match condition and set the source instance ID to the ID of VPC1 and the destination instance ID to the ID of VPC2.
   - **Action Policy**: Select the action that is performed to a route if the route meets all the match conditions. In this example, select **Deny**.



After you add the route map, you can view the route that denies access from VPC2 to VPC1 on the **Routes** tab.



Step 3: Test the network connectivity

To test the network connectivity between VPC1 and VPC2, follow these steps:

1. Log on to the ECS instance ECS1 in VPC1.
2. Use the **ping** command to **ping** the IP address of the ECS instance ECS2 in VPC2.

   The output shows that ECS1 cannot access ECS2, which means VPC1 cannot access VPC2.

```
[root@                    ~]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.



^C
--- 192.168.0.1 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 15999ms
```

3. Log on to ECS2 in VPC2.
4. Use the **ping** command to **ping** the IP address of ECS1 in VPC1.

   The output shows that ECS2 cannot access ECS1, which means VPC2 cannot access VPC1.

```
[root@                    ~]# ping 172.16.0.1
PING 172.16.0.1 (172.16.0.1) 56(84) bytes of data.



^C
--- 172.16.0.1 ping statistics ---
6 packets transmitted, 0 received, 100% packet loss, time 5000ms
```

To test the network connectivity between VPC1 and VPC3, follow these steps:

1. Log on to ECS1 in VPC1.
2. Use the **ping** command to **ping** the IP address of ECS3 in VPC3.

   The output shows that ECS1 can access ECS3, which means VPC1 can access VPC3.

```
C:\Users\Administrator>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Log on to ECS3 in VPC3.
4. Use the **ping** command to **ping** the IP address of ECS1 in VPC1.

   The output shows that ECS3 can access ECS1, which means VPC3 can access VPC1.

```
C:\Users\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

To test the network connectivity between VPC2 and VPC3, follow these steps:

1. Log on to ECS2 in VPC2.
2. Use the **ping** command to **ping** the IP address of ECS3 in VPC3.

   The output shows that ECS2 can access ECS3, which means VPC2 can access VPC3.

```
C:\Users\Administrator>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128
Reply from 10.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Log on to ECS3 in VPC3.
4. Use the **ping** command to **ping** the IP address of ECS2 in VPC2.

   The output shows that ECS3 can access ECS2, which means VPC3 can access VPC2.

```
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2.2. Stop the communication between a VPC and a CIDR block in CEN

The topic describes how to use route maps to stop the communication between a VPC and a CIDR block in Cloud Enterprise Network (CEN).

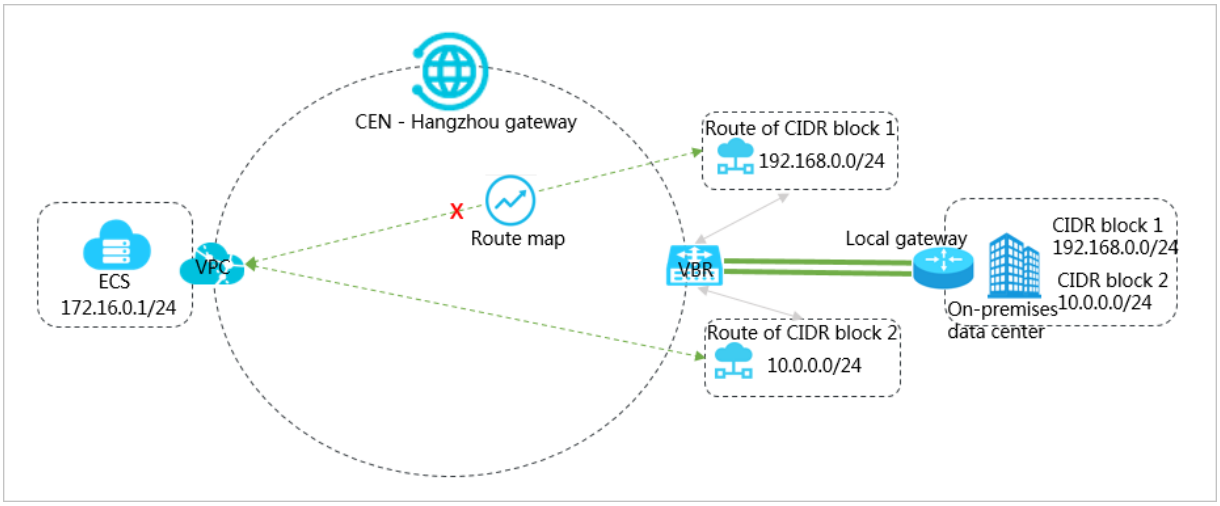
Prerequisites

Before you add a route map, make sure that the following conditions are met:

- The on-premises data center is connected to Alibaba Cloud through a leased line. For more information, see Create a dedicated connection over an Express Connect circuit.
- A CEN instance is created and the required networks are attached to the CEN instance. For more information, see Create a CEN instance and Attach a network instance.

Context

VPCs can communicate with the CIDR blocks of VPCs, Virtual Border Routers (VBRs), and Cloud Connect Networks (CCNs) that are attached to the same CEN instance by default. However, you may need to stop a VPC from communicating with a certain CIDR block of a VPC, VBR, or CCN.

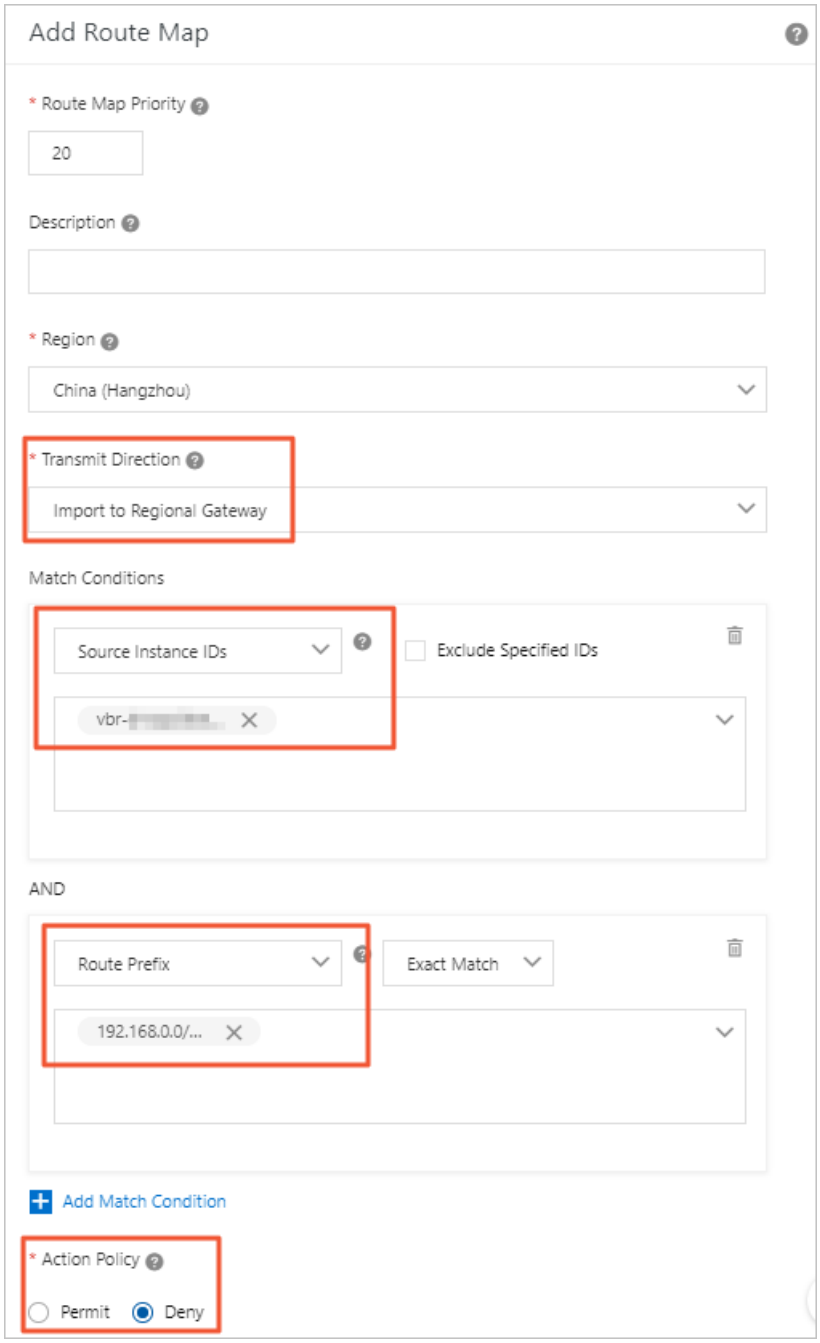


As shown in the preceding figure, a VPC and a VBR are attached to CEN. The VBR learns the routes pointing to CIDR block 1 and CIDR block 2 of the on-premises data center through BGP. By default, the VPC can communicate with CIDR block 1 and CIDR block 2 of the on-premises data center, too. If you want to stop the VPC from communicating with CIDR block 1, you can use route maps. By using route maps, you can stop the VPC from communicating with CIDR block 1 while the VPC can still communicate with CIDR block 2.

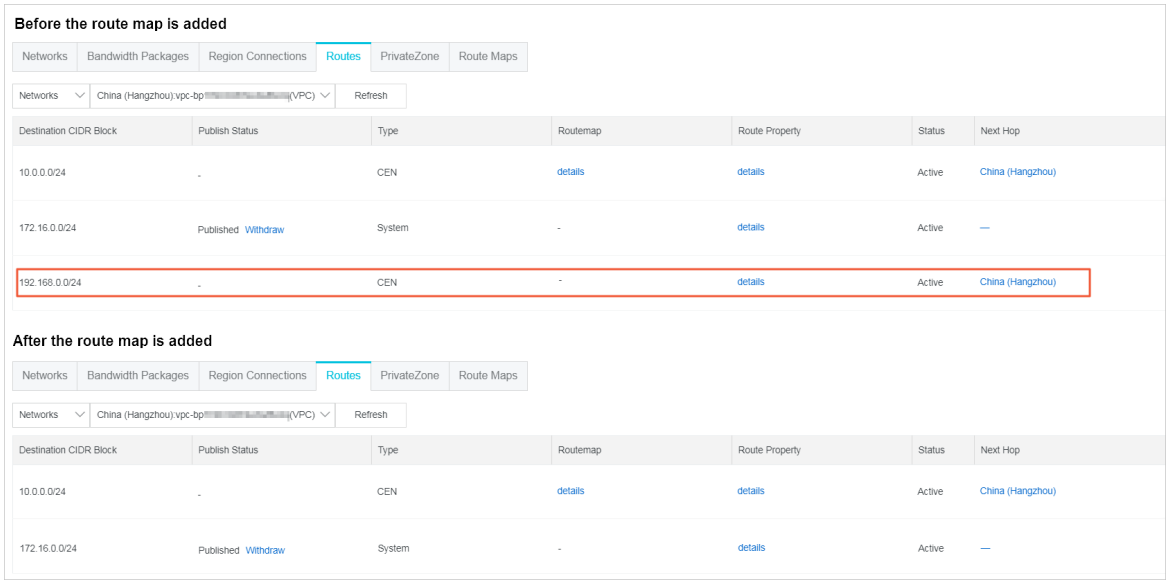
Step 1: Set a route map to deny the route of CIDR block 1

To set a route map to deny the route of CIDR block 1, follow these steps:

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the target CEN instance and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
5. On the **Add Route Map** page, configure the route map according to the following information and then click **OK**.
   - **Route Map Priority**: Enter the priority of the route map. A smaller number represents a higher priority. In this example, enter **20**.
   - **Region**: Select the region to which the route map is applied. In this example, select **China (Hangzhou)**.
   - **Transmit Direction**: Select the direction in which the route map is applied. In this example, select **Import to Regional Gateway**.
   - **Match Conditions**: Set the match conditions of the route map. In this example, add two match conditions:
     - **Source Instance IDs**: Enter the instance ID of the VBR.
     - **Route Prefix**: Enter 192.168.0.0/24. Select **Exact Match** as the **matching method**.
   - **Action Policy**: Select the action that is performed to a route if the route matches all the matching conditions. In this example, select **Deny**.



After you add the route map, you can see that the route pointing to CIDR block 1, 192.168.0.0/24, is deleted from the VPC on the **Routes** tab.



Step 2: Test the network connectivity

To test the network connectivity between the VPC and CIDR block 1 of the on-premises data center, follow these steps:

1. Log on to an ECS instance in the VPC.
2. Use the **ping** command to **ping** the IP address of CIDR block 1.

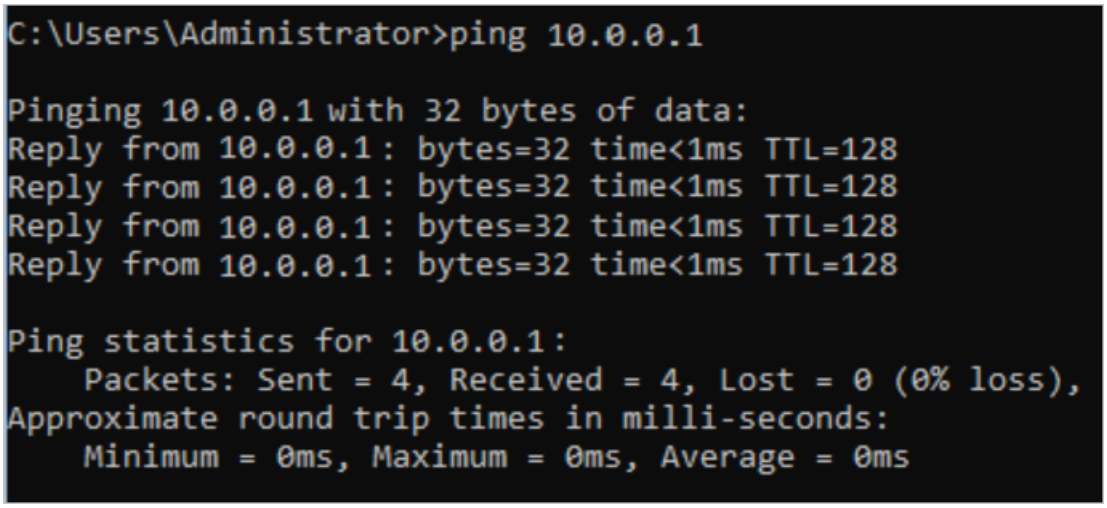
   The output shows that the ECS instance in the VPC cannot access the IP address of CIDR block 1.

```
[root@ ~]# ping 192.168.0.1
PING 192.168.0.1 (192.168.0.1) 56(84) bytes of data.



^C
--- 192.168.0.1 ping statistics ---
17 packets transmitted, 0 received, 100% packet loss, time 15999ms
```

To test the network connectivity between the VPC and CIDR block 2 of the on-premises data center, follow these steps:

1. Log on to the ECS instance in the VPC.
2. Use the **ping** command to **ping** the IP address of CIDR block 2.

   The output shows that the ECS instance in the VPC can access the IP address of CIDR block 2.



2.3. Connect data centers through CEN

This topic describes how to connect data centers by using route maps of Cloud Enterprise Network (CEN).

Prerequisites

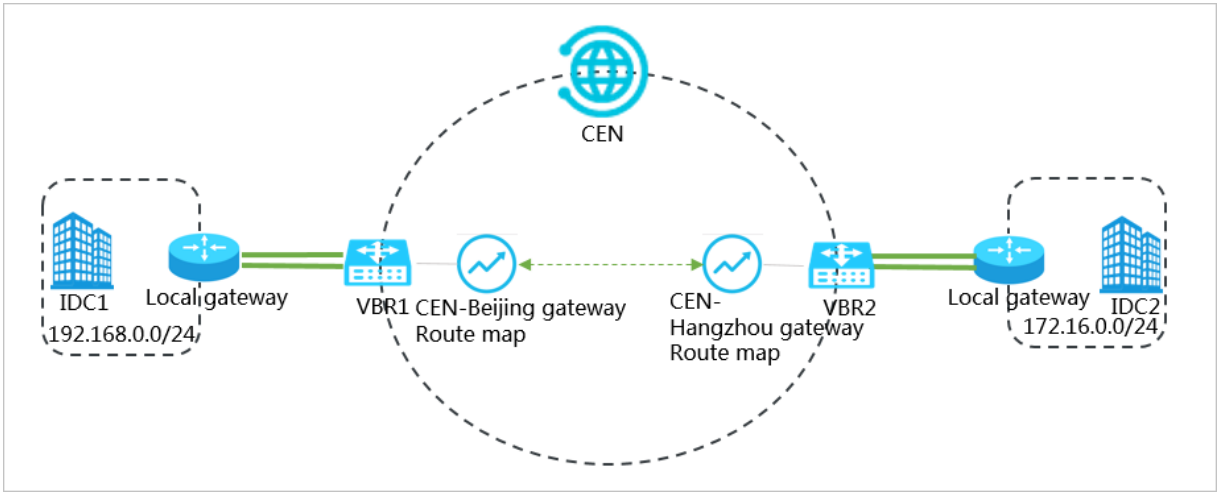
Before you configure route maps, make sure that the following requirements are met:

- The data centers are connected to Alibaba Cloud through leased lines. For more information, see Create a dedicated connection over an Express Connect circuit.
- A CEN instance is created and network instances that you want to connect are attached to the CEN instance. For more information, see Create a CEN instance and Attach a network instance.
- A bandwidth plan is purchased and the bandwidth for cross-region communication is allocated. For more information, see Use a bandwidth plan and Manage bandwidth for cross-region connections.

Context

After you create a CEN instance, the system automatically creates a route map for the regional gateways of the CEN instance. The priority of the route map is 5000 and the action policy of the route map is Deny. The route map forbids virtual border routers (VBRs) and Cloud Connect Network (CCN) instances to communicate with other VBRs and CCN instances that are attached to the CEN instance. In some scenarios, you may need to allow the VBRs and CCN instances to communicate with other VBRs and CCN instances that are attached to the CEN instance.

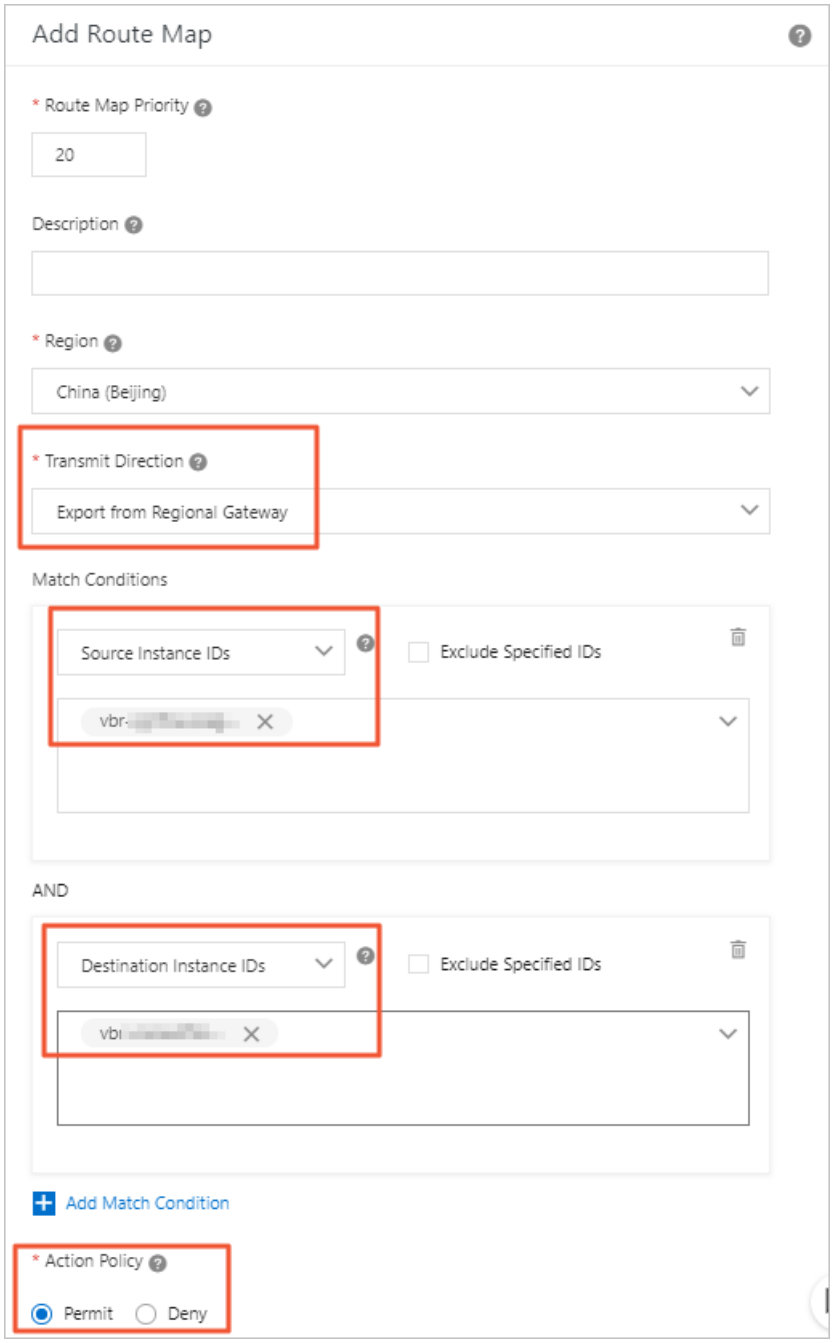
> **Notice** If you delete the default route map, routing loops may occur. Proceed with caution.



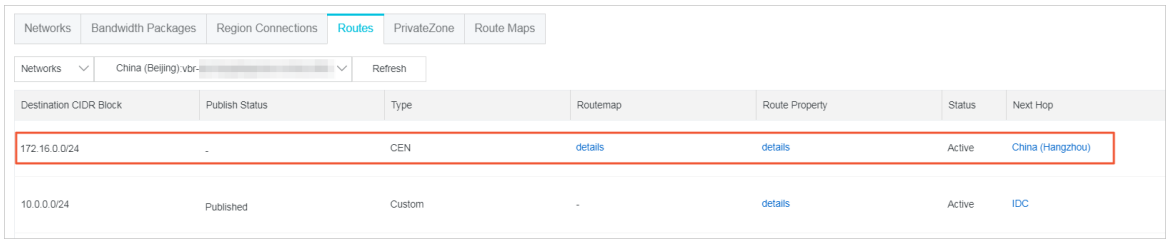
Data center 1 is located in the China (Beijing) region and connected to Alibaba Cloud through VBR 1. Data center 2 is located in the China (Hangzhou) region and connected to Alibaba Cloud through VBR 2, as shown in the preceding figure. VBR 1 and VBR 2 are attached to a CEN instance. By default, Data center 1 and Data center 2 cannot communicate with each other. To enable intercommunication between Data center 1 and Data center 2, you must configure route maps for the VBRs by performing the following operations:

Step 1: Add a route map that allows Date center 1 to access Data center 2

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the CEN instance that you want to manage, and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab, and then click **Add Route Map**.
5. On the **Add Route Map** page, set the following parameters and click **OK**:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **20** is entered.
   - **Description**: Enter a description for the route map. This parameter is optional.
   - **Region**: Select the region to which the route map is applied. In this example, **China (Beijing)** is entered.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to Regional Gateway** is selected.
   - **Match Conditions**: Set match conditions for routes. In this example, the following conditions are set:
     - **Source Instance IDs**: Select the ID of VBR 2.
     - **Destination Instance IDs**: Select the ID of VBR 1.
   - **Action Policy**: Select the action that you want to perform to a route when the route meets all match conditions. In this example, **Permit** is selected.

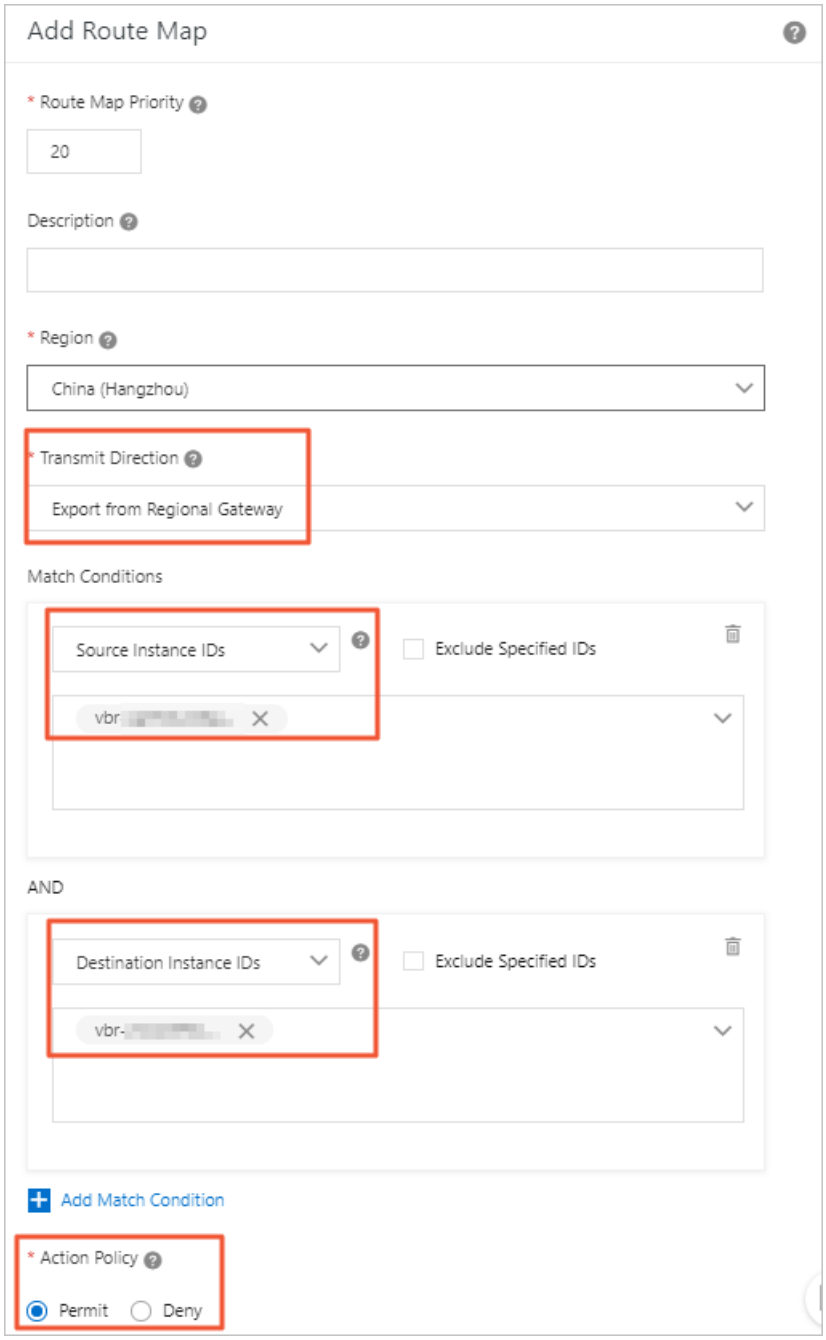


After you add the route map, you can view the route that allows Data center 1 to access Data center 2 on the **Routes** tab.

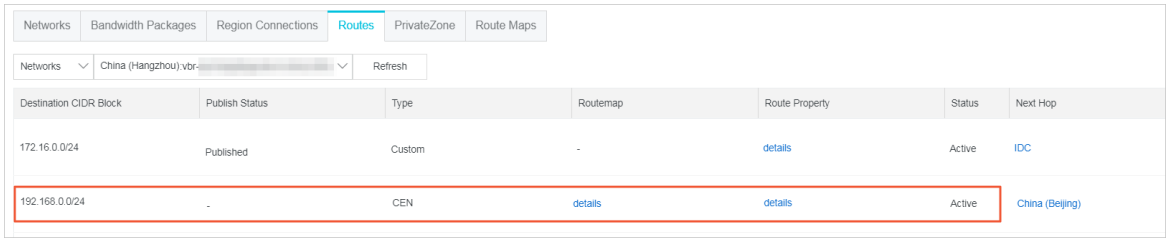


Step 2: Add a route map that allows Data center 2 to access Data center 1

1. In the left-side navigation pane, click **Instances**.
2. On the **Instances** page, find the CEN instance that you want to manage. In the **Actions** column, click **Manage**.
3. On the **CEN** page, click the **Route Maps** tab, and then click **Add Route Map**.
4. In the **Add Route Map** panel, set the following parameters and then click **OK**:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **20** is entered.
   - **Description**: Enter a description for the route map. This parameter is optional.
   - **Region**: Select the region to which the route map is applied. In this example, **China (Hangzhou)** is entered.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to Regional Gateway** is selected.
   - **Match Conditions**: Set match conditions for routes. In this example, the following conditions are set:
     - **Source Instance IDs**: Select the ID of VBR 1.
     - **Destination Instance IDs**: Select the ID of VBR 2.
   - **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Permit** is selected.



After you add the route map, you can view the route that allows Data center 2 to access Data center 1 on the **Routes** tab.



Step 3: Test the connectivity between Data center 1 and Data center 2

1. Open the command prompt on a PC in Data center 1.
2. Run the **ping** command to **ping** the IP address of a PC in Data center 2 to test the connectivity.

   The test result shows that the PC in Data center 1 can access the PC in Data center 2.

```
C:\Users\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Open the command prompt on a PC in Data center 2.
4. Run the **ping** command to **ping** the IP address of a PC in Data center 1 to test the connectivity.

   The test result shows that the PC in Data center 2 can access the PC in Data center 1.

```
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

2.4. Connect branches to a data center through CEN

This topic describes how to use route maps of Cloud Enterprise Network (CEN) to connect the branches of a company to its data center.

Prerequisites

Before you configure route maps, make sure that the following requirements are met:

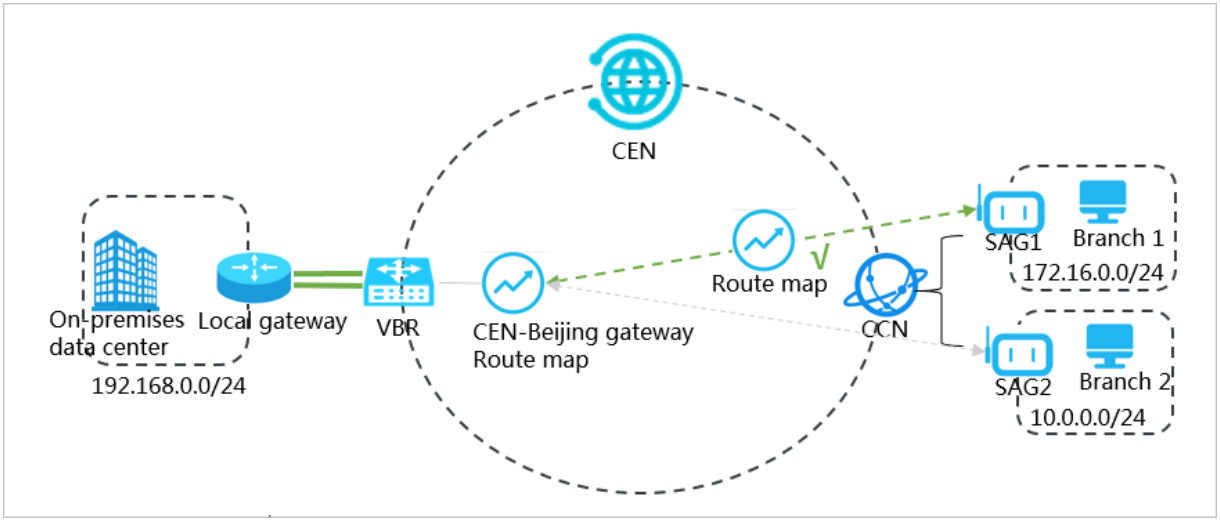
- A Cloud Connect Network (CCN) instance is created. Smart Access Gateway (SAG) instances that are created for the branches are attached to the CCN instance. For more information, see Create a CCN instance and Attach a network instance.

- A CEN instance is created. Network instances to be connected are attached to the CEN instance. For more information, see Create a CEN instance and Attach a network instance.
- A bandwidth plan is purchased and the bandwidth for cross-region communication is allocated. For more information, see Use a bandwidth plan and Manage bandwidth for cross-region connections.

Context

The system automatically adds a default route map to the regional gateway of a CEN instance. The priority value of the default route map is 5000 and the action policy is deny. This route map forbids virtual border routers (VBRs) and CCN instances that are attached to the CEN instance to communicate with each other. However, in some scenarios, you may need to allow the VBRs and CCN instances that are attached to the CEN instance to communicate with each other.

Notice If you delete the default route map, routing loops may occur. Proceed with caution.



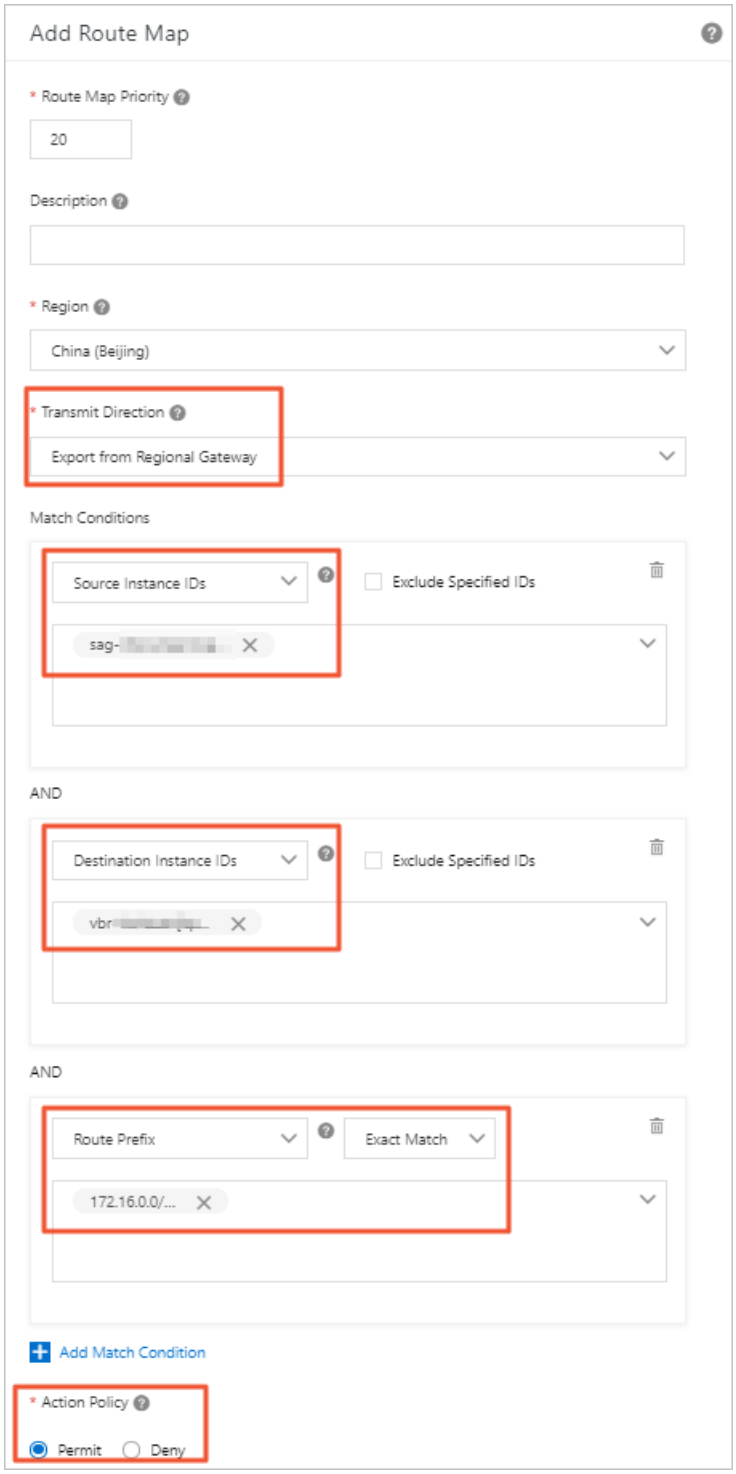
The data center of a company is deployed in the China (Beijing) region as shown in the preceding figure. The data center is connected to Alibaba Cloud through a VBR. A branch of the company (Branch 1) is located in the China (Shanghai) region. Another branch of the company (Branch 2) is located in the China (Hangzhou) region. Branch 1 is connected to a CCN instance through an SAG instance (SAG 1). Branch 2 is connected to the same CCN instance through another SAG instance (SAG 2). By default, the data center cannot communicate with Branch 1 and Branch 2. You can configure a route map to allow the data center and Branch 1 to communicate with each other.

Step 1: Configure a route map to allow the data center to access Branch 1

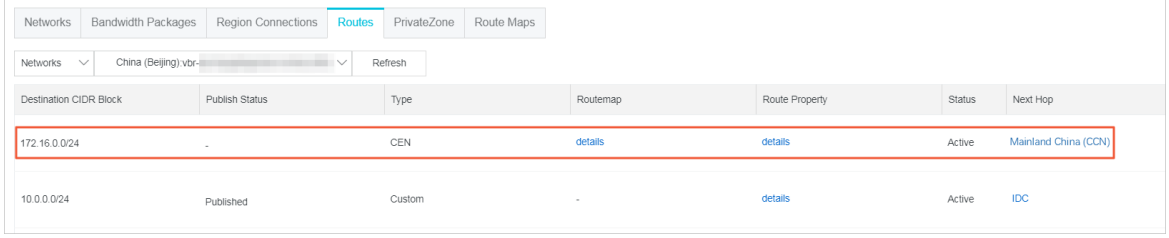
Perform the following operations to configure a route map to allow the data center to access Branch 1:

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
5. In the **Add Route Map** panel, set the following parameters and click **OK** to create a route map:

- **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **20** is entered.
- **Region**: Select the region to which the route map is applied. In this example, **China (Beijing)** is selected.
- **Transmit Direction**: Select the direction of the route map. In this example, **Export from Regional Gateway** is selected.
- **Match Conditions**: Set the match conditions of routes. The following conditions are set in this example:
  - **Source Instance IDs**: Select the ID of SAG 1.
  - **Target Instance IDs**: Select the ID of the VBR.
  - **Route Prefix**: Enter 172.16.0.0/24.
- **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Permit** is selected.



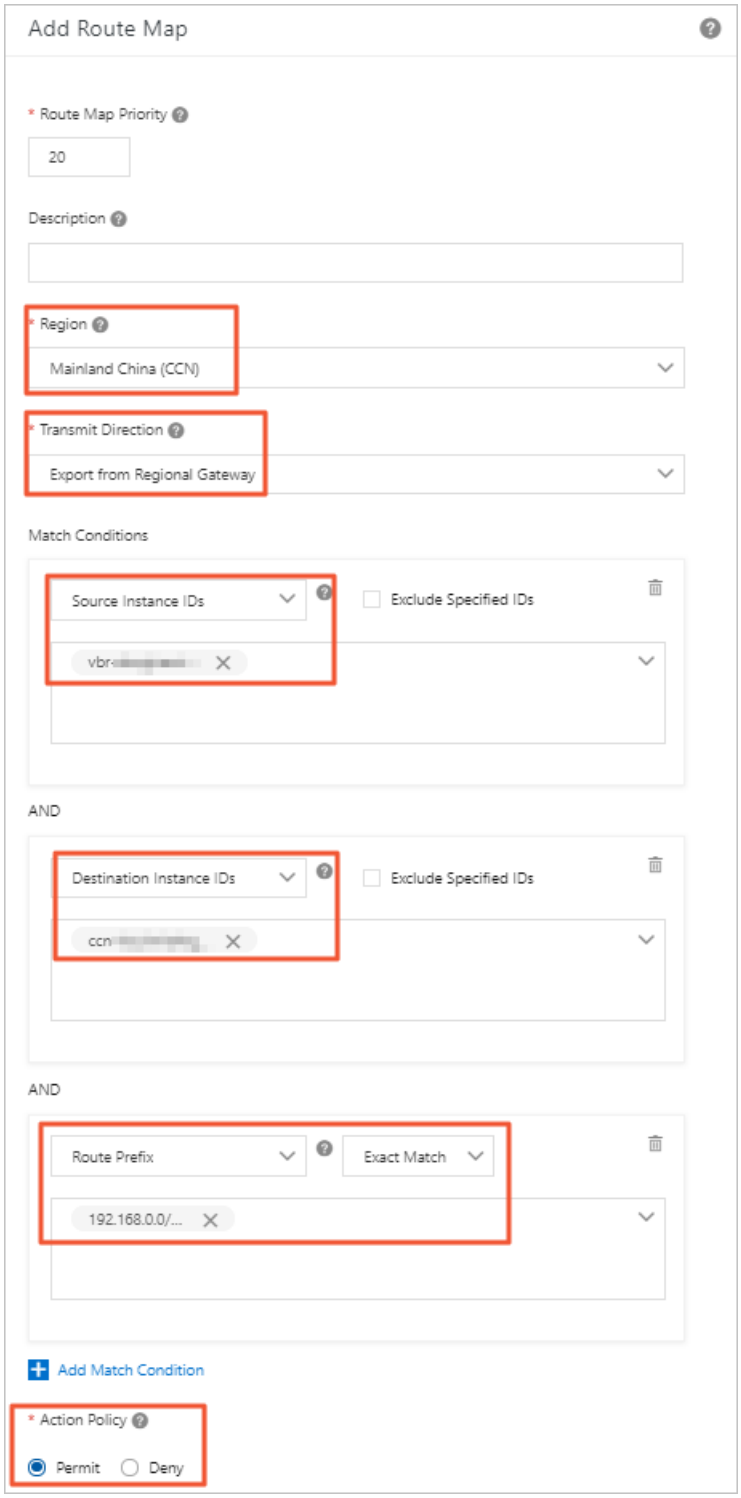
After you configure the route map, you can view the route that allows the data center to access Branch 1 on the **Routes** tab.



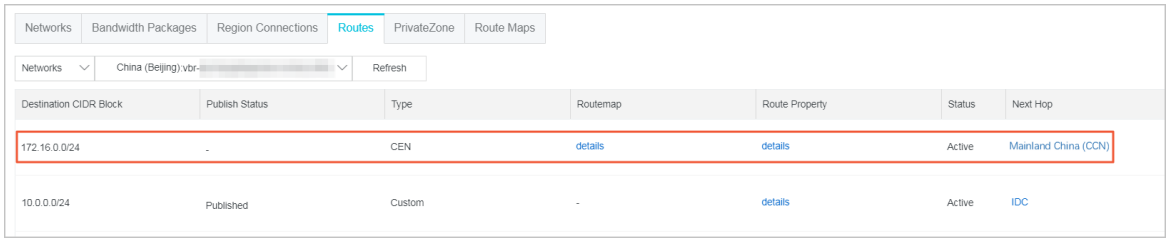
Step 2: Configure a route map to allow the CCN instance to access the data center

Perform the following operations to configure a route map to allow the CCN instance to access the data center:

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
5. In the **Add Route Map** panel, set the following parameters and click **OK** to create a route map:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **20** is entered.
   - **Region**: Select the region to which the route map is applied. In this example, **Mainland China CCN** is selected.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Export from Regional Gateway** is selected.
   - **Match Conditions**: Set the match conditions of routes. The following match conditions are set:
     - **Source Instance IDs**: Select the ID of VBR.
     - **Target Instance IDs**: Select the ID of the CCN instance.
     - **Route Prefix**: Enter 192.168.0.0/24.
   - **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Permit** is selected.



After you add the route map, you can view the route that allows the CCN instance to access the data center on the **Routes** tab.



Step 3: Test the connectivity

Perform the following operations to test the connectivity between the data center and Branch 1:

1. Open the command prompt on a PC in the data center.
2. Run the **ping** command to **ping** the IP address of a PC in Branch 1.

   The result shows that the data center can access Branch 1.

```
C:\Users\Administrator>ping 172.16.0.1

Pinging 172.16.0.1 with 32 bytes of data:
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128
Reply from 172.16.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 172.16.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

3. Open the command prompt on a PC in Branch 1.
4. Run the **ping** command to **ping** the IP address of a PC in the data center.

   The result shows that Branch 1 can access the data center.

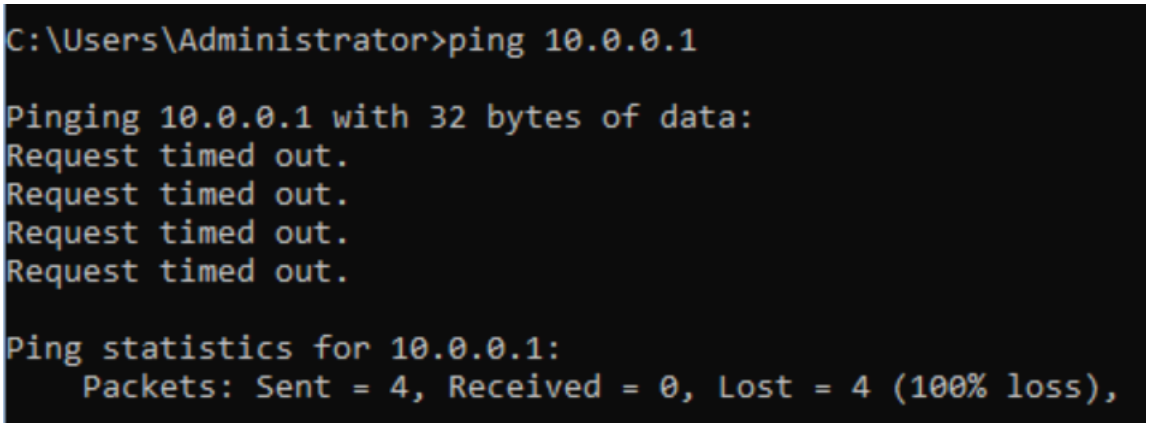
```
C:\Users\Administrator>ping 192.168.0.1

Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128
Reply from 192.168.0.1 : bytes=32 time<1ms TTL=128

Ping statistics for 192.168.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Perform the following operations to test the connectivity between the data center and Branch 2:

1. Open the command prompt on a PC in the data center.

2. Run the **ping** command to **ping** the IP address of a PC in Branch 2.

   The result shows that the data center cannot access Branch 2.



2.5. Configure active/standby static routes for VBRs in the same region by using route maps

This topic describes how to configure active/standby static routes for virtual border routers (VBRs) in the same region by using route maps of Cloud Enterprise Network (CEN).

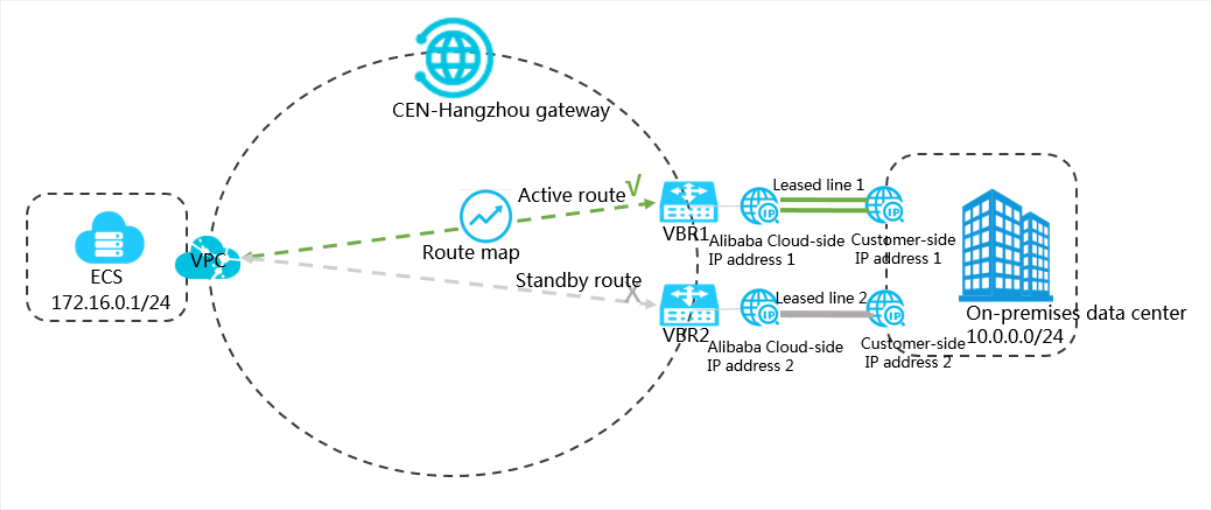
Prerequisites

Before you configure route maps, make sure that the following requirements are met:

- The data center is connected to Alibaba Cloud through leased lines. For more information, see Create a dedicated connection over an Express Connect circuit.
- A CEN instance is created and network instances to be connected are attached to the CEN instance. For more information, see Create a CEN instance and Attach a network instance.

Context

Route maps permit or deny routes based on match conditions. You can set match conditions to specify the attributes of routes that you want to permit.



A company has a data center located in the China (Hangzhou) region. The company connects the data center to Alibaba Cloud by using two leased lines from two ISPs, as shown in the preceding figure. The port of Leased line 1 is 10 Gbit/s, whereas the port of Leased line 2 is 1 Gbit/s. VBR 1, VBR 2, and the virtual private cloud (VPC) are attached to the CEN instance. The company uses the leased lines to connect the data center to Alibaba Cloud through load balancing. However, the company needs to use Leased line 2 as a standby connection because the port of Leased line 2 is slower than that of Leased line 1. When Leased line 1 is down, network traffic is automatically transmitted through Leased line 2.

You can add a route map with a higher priority for VBR 1 that is connected to Leased line 1, and then add a route map with a lower priority for VBR 2 that is connected to Leased line 2. This way, Leased line 1 functions as the active connection and Leased line 2 functions as the standby connection.

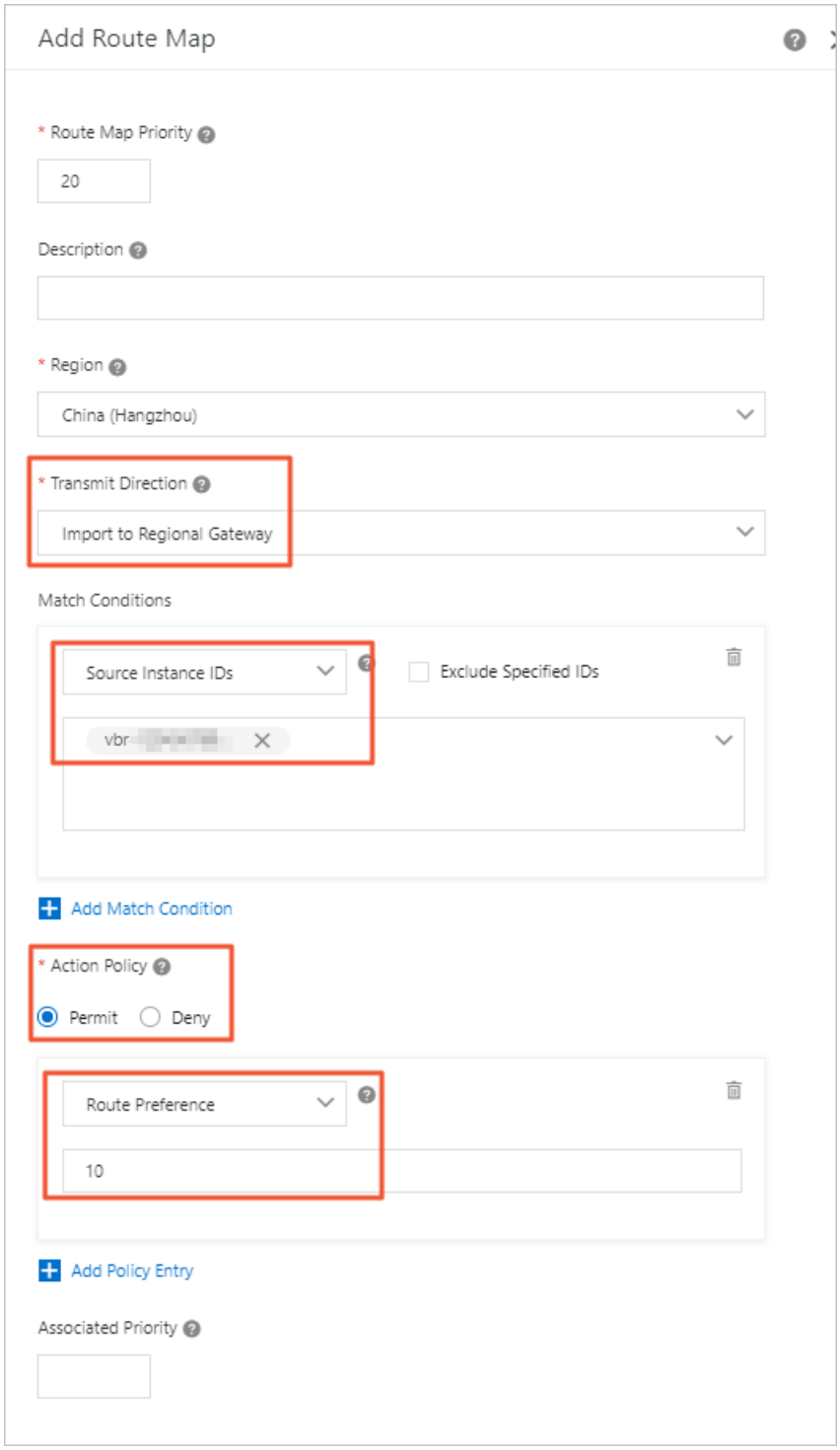
Step 1: Set Leased line 1 that is connected to VBR 1 as the active connection

Perform the following operations to set Leased line 1 as the active connection:

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the CEN instance that you want to manage, and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab, and click **Add Route Map**.
5. In the **Add Route Map** panel, set the following parameters and click **OK**:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **20** is entered.
   - **Region**: Select the region to which the route map is applied. In this example, **China (Hangzhou)** is entered.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to Regional Gateway** is selected.
   - **Match Condition**: Set the matching conditions for routes. In this example, **Source Instance IDs** is selected and the ID of VBR 1 is entered.
   - **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Permit** is selected.
   - **Add Policy Entry**: Select Preference and then set the priorities of the routes that are

permitted. In this example, the priority value is set to 10.

> **Note** By default, the priorities of the permitted routes are 50. You can set a value from 1 to 100. A lower value indicates a higher priority.

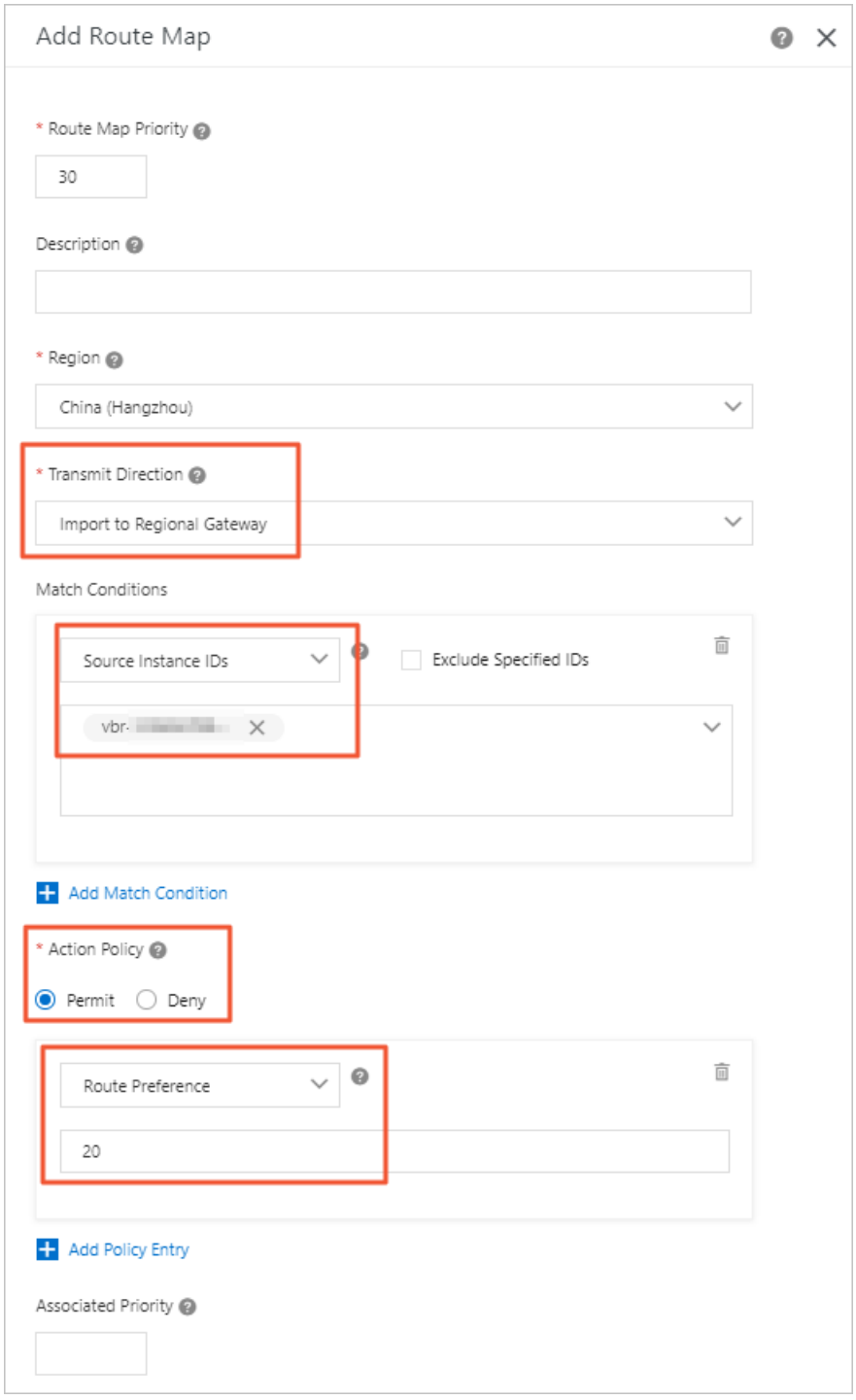


Step 2: Set Leased line 2 that is connected to VBR 2 as the standby connection

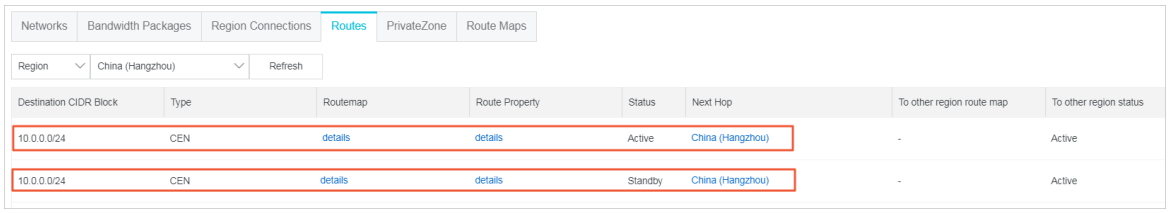
Perform the following operations to set Leased line 2 as the standby connection:

1. In the left-side navigation pane, click **Instances**.
2. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
3. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
4. On the **Add Route Map** page, set the following parameters and click **OK**:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **30** is entered.
   - **Region**: Select the region to which the route map is applied. In this example, **China (Hangzhou)** is entered.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to Regional Gateway** is selected.
   - **Match Condition**: Set the match conditions for routes. In this example, **Source Instance IDs** is selected and the ID of VBR 2 is entered.
   - **Action Policy**: Select the action that you want to perform to a route if the route meets all matching conditions. In this example, **Permit** is selected.
   - **Add Policy Entry**: Select Preference and then set the priorities of the routes that are permitted. In this example, the priority value is set to 20.

     Note By default, the priorities of the permitted routes are 50. You can set a value from 1 to 100. A lower value indicates a higher priority.



After you add the route maps, you can find two routes that point to 10.0.0.0/24 on the **Routes** tab. One of the routes is used as the standby route.



2.6. Use route maps to allow specified VPCs to communicate with each other

This topic describes how to configure route maps to allow specified virtual private clouds (VPCs) that are attached to a Cloud Enterprise Network (CEN) instance to communicate with each other. This improves the network security. We recommend that you use this method to manage routes in CEN instances.

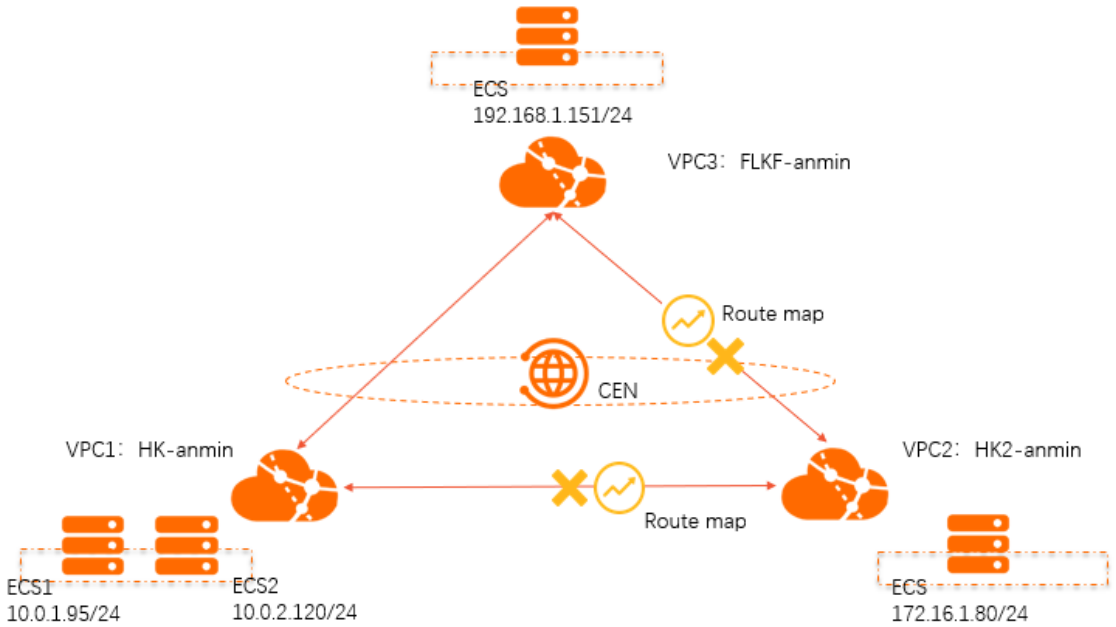
Prerequisites

Before you configure route maps, make sure that the following conditions are met:

- A CEN instance is created. For more information, see Create a CEN instance.
- Network instances that need to communicate with each other are attached to the same CEN instance. For more information, see Attach a network instance.
- A bandwidth plan is purchased and the bandwidth for cross-region connections is allocated. For more information, see Use a bandwidth plan and Manage bandwidth for cross-region connections.

Context

By default, VPCs that are attached to a CEN instance can communicate with other network instances that are attached to the same CEN instance. These network instances are VPCs, virtual border routers (VBRs), and Cloud Connect Network (CCN) instances. If you have a large number of VPCs, VBRs, and CCN instances attached to a CEN instance, it is difficult to manage the connections. In this case, we recommend that you configure low-priority route maps to forbid all the attached network instances to communicate with each other. Then, configure high-priority route maps to allow only specified network instances to communicate with each other.



The VPCs in the preceding figure are attached to a CEN instance. VPC 1 and VPC 2 are deployed in the China (Hong Kong) region, and VPC 3 is deployed in the Germany (Frankfurt) region. By default, VPC 1, VPC 2, and VPC 3 can communicate with each other. To facilitate network management and maintenance in case you want to expand the network, you can use route maps to allow specified VPCs to communicate with each other. To perform this task, you can configure low-priority route maps to block routes from the China (Hong Kong) regional gateways and the Germany (Frankfurt) regional gateway. This forbids VPC 1, VPC 2, and VPC 3 to communicate with each other. Then, configure high-priority route maps to allow VPC 1 and VPC 3 to communicate with each other.

CIDR blocks

The following table describes the CIDR blocks of VPC 1, VPC 2, and VPC 3.

Network instance	CIDR block	ECS instance IP address
VPC1	VPC 1: 10.0.0.0/8 VSwitch 1: 10.0.1.0/24 VSwitch 2: 10.0.2.0/24	ECS 1: 10.0.1.95 ECS 2: 10.0.2.120
VPC2	VPC 2: 172.16.0.0/12 VSwitch: 172.16.1.0/24	ECS: 172.16.1.80
VPC3	VPC 3: 192.168.0.0/16 VSwitch: 192.168.1.0/24	ECS: 192.168.1.151

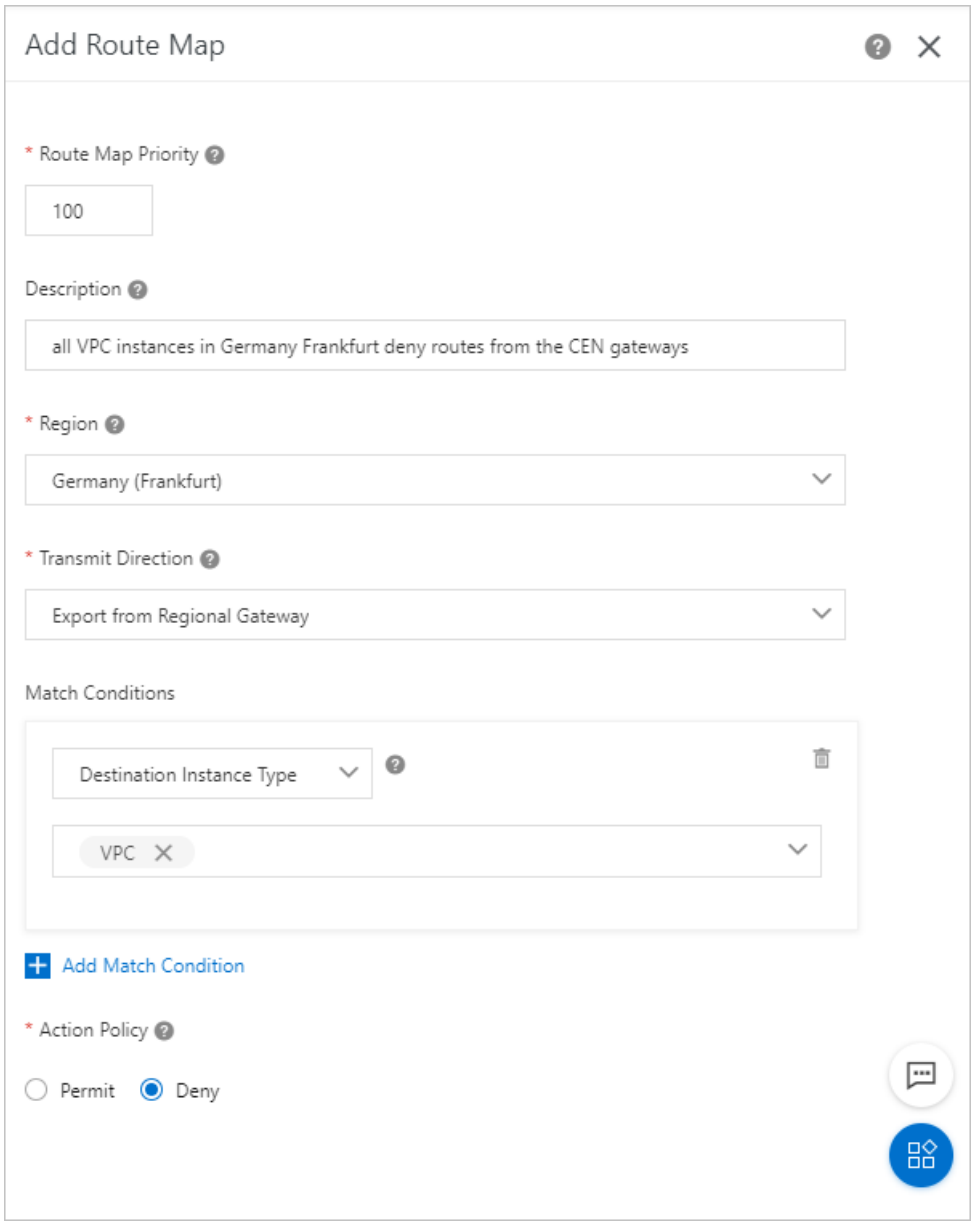
Step 1: Configure route maps to block routes from the regional gateways to all network instances

Perform the following operations to configure route maps to block routes from the regional gateways deployed in the China (Hong Kong) and Germany (Frankfurt) regions to VPC 1, VPC 2, and VPC 3:

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Instances**.
3. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
5. In the **Add Route Map** panel, set the following parameters and click **OK** to add a route map for the regional gateway deployed in the Germany (Frankfurt) region:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **100** is entered.
   - **Description**: Enter a description for the route map. This parameter is optional. In this example, *All VPCs in the Germany (Frankfurt) region deny routes from the regional gateway* is entered.
   - **Region**: Select the region to which the route map is applied. In this example, **Germany (Frankfurt)** is selected.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to**

Regional Gateway is selected.

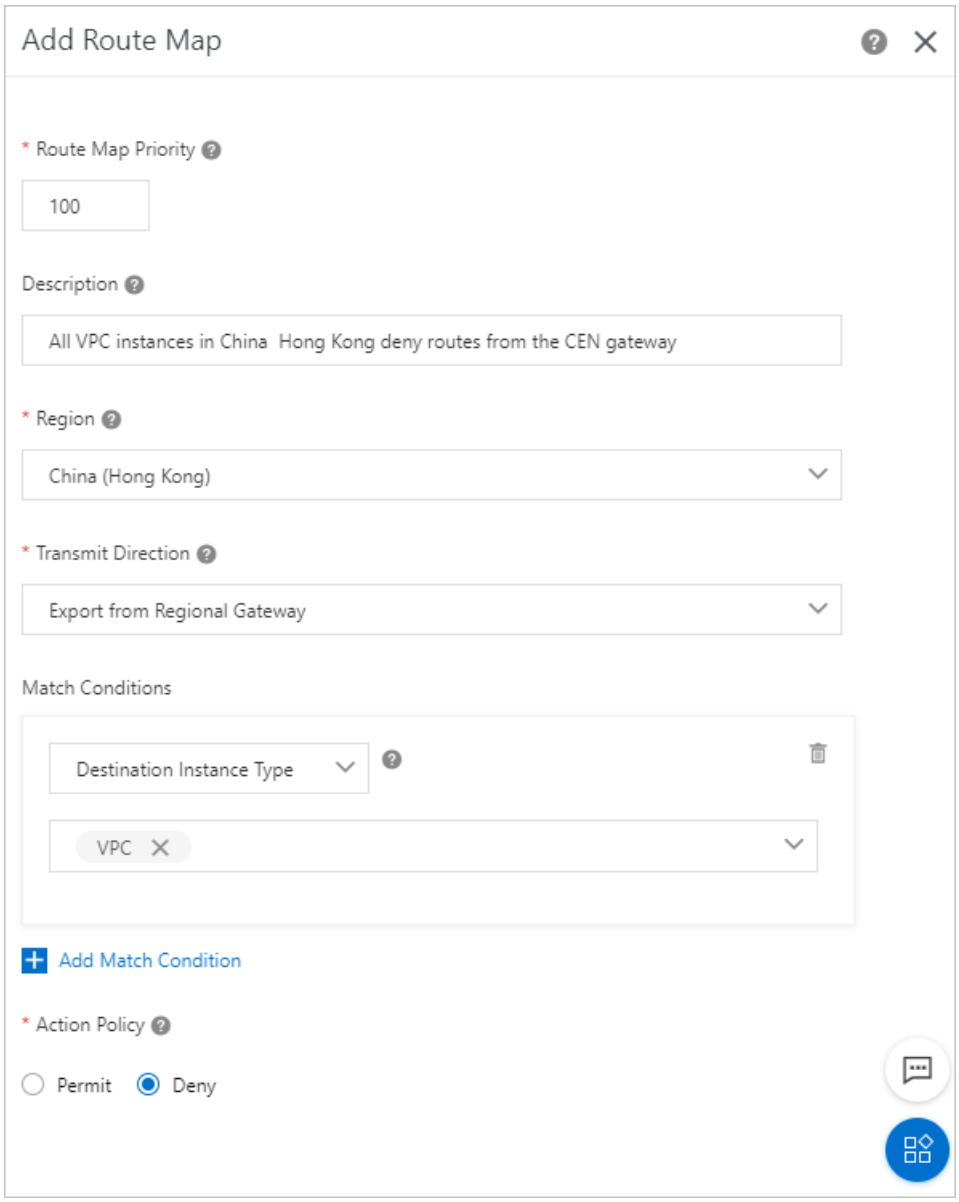
- **Match Conditions**: Set the match conditions of routes. In this example, **VPC** is specified as **Destination Instance Type**.
- **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Deny** is selected.



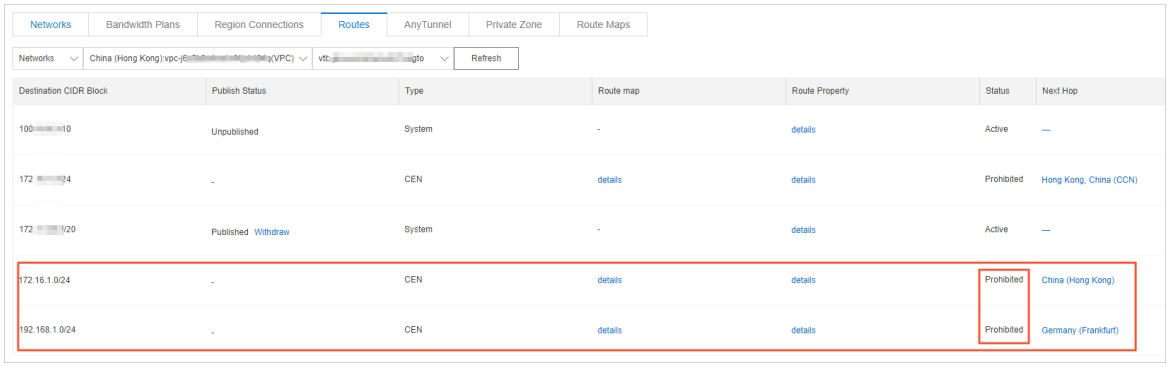
6. On the **Add Route Map** page, set the following parameters and click **OK** to add a route map for the regional gateway in the China (Hong Kong) region:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **100** is entered.
   - **Description**: Enter a description for the route map. This parameter is optional. In this example, *All VPCs in the China (Hong Kong) region deny routes from the regional gateway* is entered.
   - **Region**: Select the region to which the route map is applied. In this example, **China (Hong Kong)** is selected.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to**

Regional Gateway is selected.

- **Match Conditions**: Set the match conditions of routes. In this example, **VPC** is specified as **Destination Instance Type**.
- **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Deny** is selected.



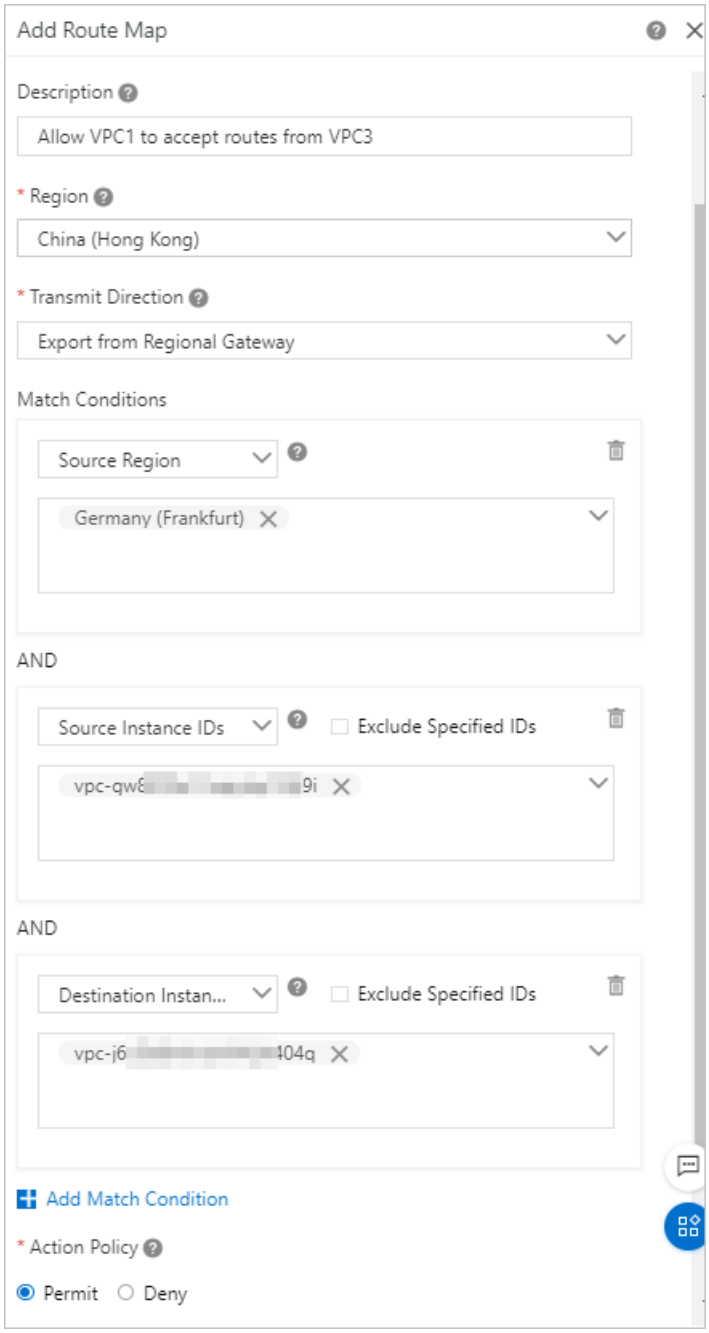
After you add the route maps, navigate to the **Routes** tab. You can find that VPC 1, VPC 2, and VPC 3 have denied routes from the regional gateways. The following figure shows that VPC 1 has denied routes from the regional gateways.



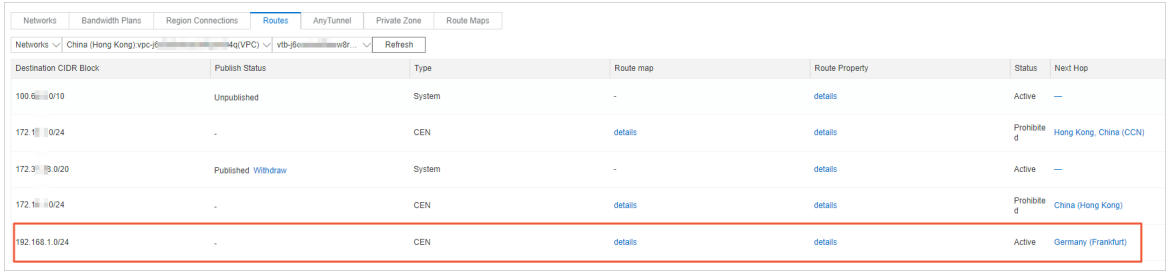
Step 2: Configure a route map that allows VPC 1 to permit routes from VPC 3

Perform the following operations to allow VPC 1 to permit routes from VPC 3:

1. In the left-side navigation pane, click **Instances**.
2. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
3. On the **CEN** page, click the **Route Maps** tab, and then click **Add Route Map**.
4. In the **Add Route Map** panel, set the following parameters and click **OK** to create a route map:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **50** is entered.
   - **Description**: Enter a description for the route map. This parameter is optional. In this example, *Allow VPC 1 to permit routes from VPC 3* is entered.
   - **Region**: Select the region to which the route map is applied. In this example, **China (Hong Kong)** is selected.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to Regional Gateway** is selected.
   - **Match Condition**: Set the match conditions of routes. In this example, the following match conditions are set:
     - **Source Region**: **Germany (Frankfurt)** is selected.
     - **Source Instance IDs**: The ID of VPC 3 is selected.
     - **Target Instance IDs**: The ID of VPC 1 is selected.
   - **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Permit** is selected.



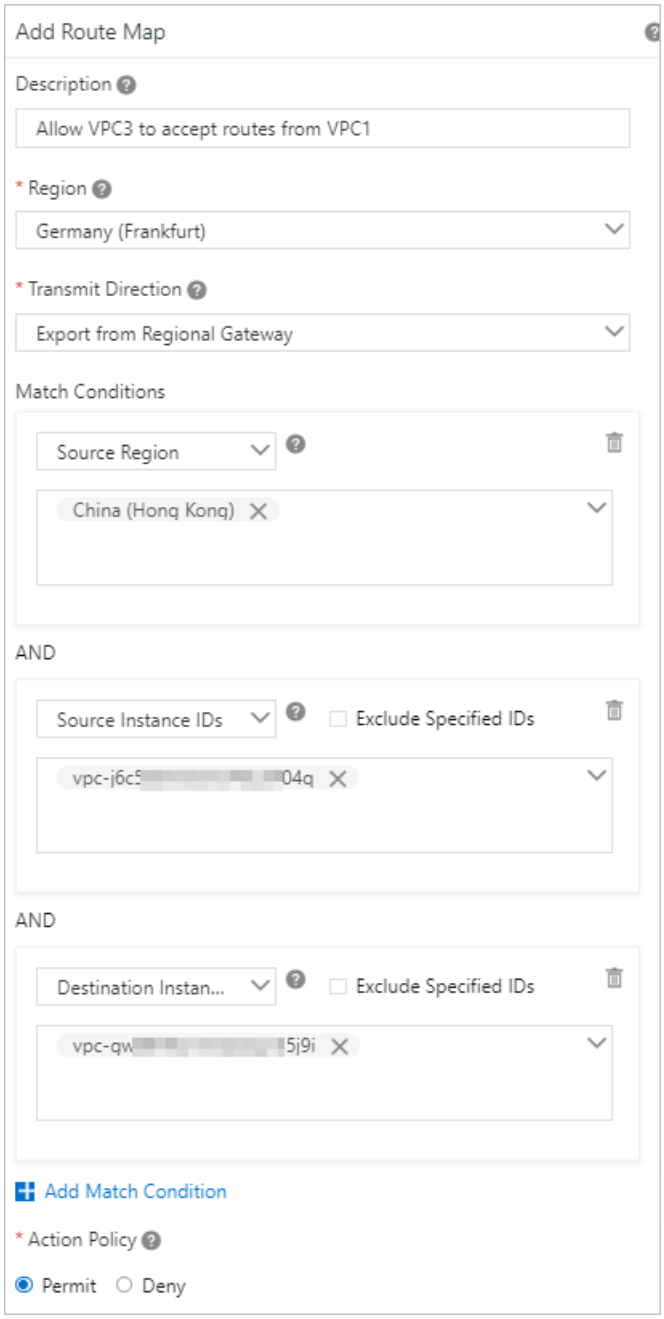
After you add the route map, navigate to the **Routes** tab. You can check whether VPC 1 has permitted routes from VPC 3.



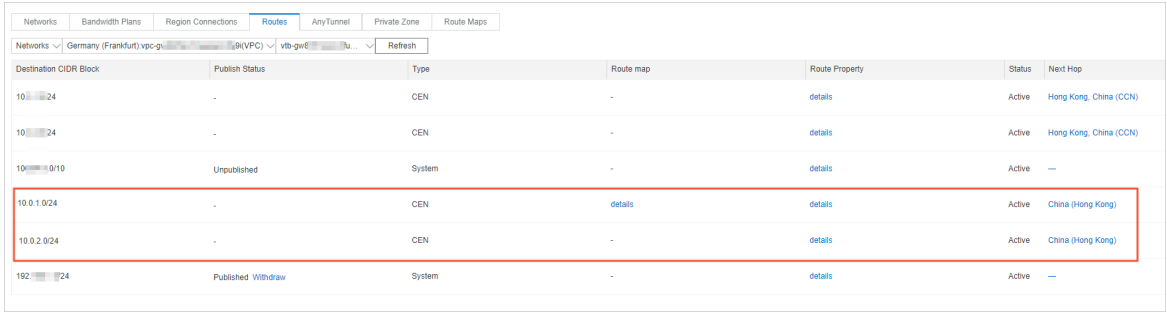
Step 3: Configure a route map that allows VPC 3 to permit routes from VPC 1

Perform the following operations to allow VPC 3 to permit routes from VPC 1:

1. In the left-side navigation pane, click **Instances**.
2. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
3. On the **CEN** page, click the **Route Maps** tab and then click **Add Route Map**.
4. On the **Add Route Map** page, set the following parameters and click **OK** to create a route map:
   - **Route Map Priority**: Enter a priority value for the route map. A lower value indicates a higher priority. In this example, **50** is entered.
   - **Description**: Enter a description for the route map. This parameter is optional. In this example, *Allow VPC 3 to permit routes from VPC 1* is entered.
   - **Region**: Select the region to which the route map is applied. In this example, **Germany (Frankfurt)** is selected.
   - **Transmit Direction**: Select the direction of the route map. In this example, **Import to Regional Gateway** is selected.
   - **Match Conditions**: Set the match conditions of routes.
     - **Source Region**: **China (Hong Kong)** is selected.
     - **Source Instance IDs**: The ID of VPC 1 is selected.
     - **Target Instance IDs**: The ID of VPC 3 is selected.
   - **Action Policy**: Select the action that you want to perform to a route if the route meets all match conditions. In this example, **Permit** is selected.



After you add the route map, navigate to the **Routes** tab. You can check whether VPC 3 has permitted routes from VPC 1.

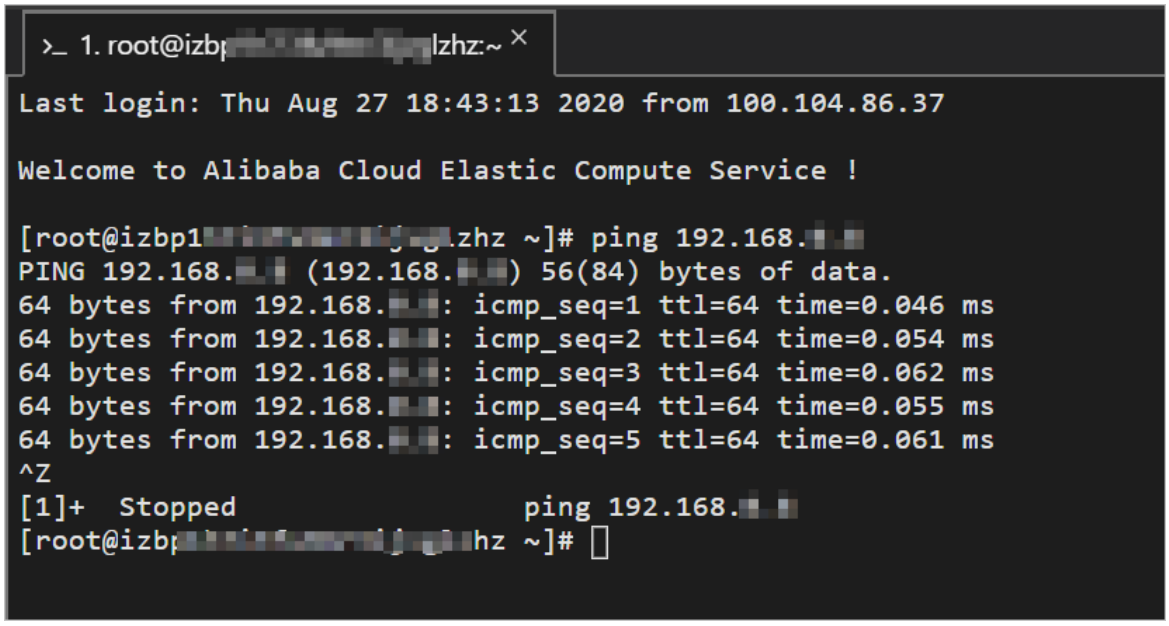


Step 4: Test the connectivity

Perform the following operations to test the connectivity between the VPCs:

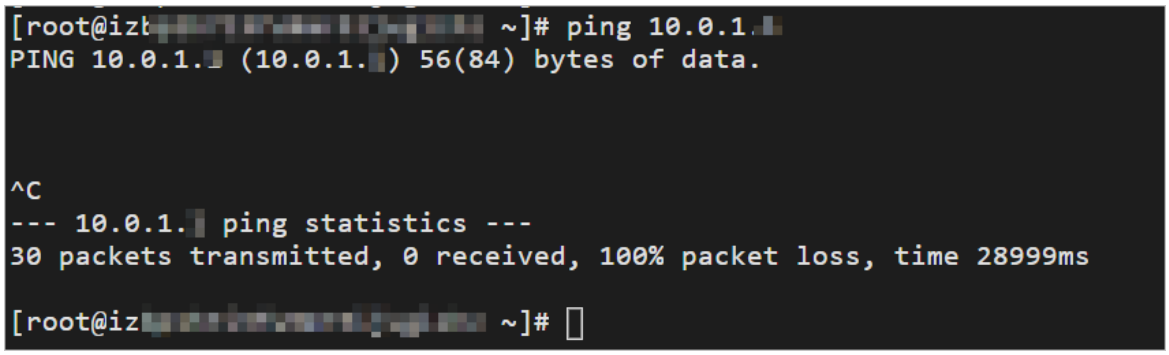
1. Log on to ECS 1 in VPC 1.
2. Run the **ping** command to **ping** the IP address of the ECS instance in VPC 3 to test the connectivity.

   The result shows that VPC 1 can access the ECS instance in VPC 3. This indicates that VPC 1 and VPC 3 can communicate with each other.



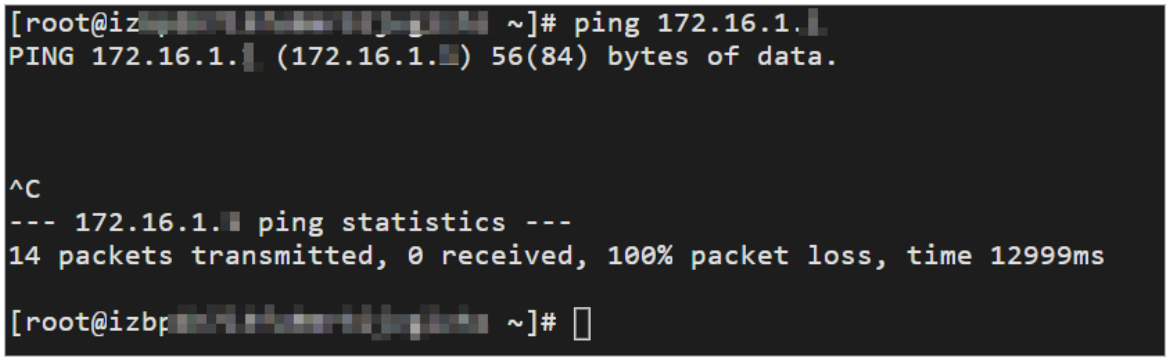
3. Log on to the ECS instance in VPC 2.
4. Run the **ping** command to **ping** the IP address of ECS 1 in VPC 1 to test the connectivity.

   The result shows that VPC 2 fails to access VPC 1. This indicates that VPC 1 and VPC 2 cannot communicate with each other.



5. Log on to the ECS instance in VPC 3.
6. Run the **ping** command to **ping** the IP address of the ECS instance in VPC 2 to test the connectivity.

   The result shows that VPC 3 fails to access VPC 2. This indicates that VPC 2 and VPC 3 cannot communicate with each other.


[root@iz ~]# ping 172.16.1.
PING 172.16.1. (172.16.1.) 56(84) bytes of data.
^C
--- 172.16.1. ping statistics ---
14 packets transmitted, 0 received, 100% packet loss, time 12999ms
[root@izbp ~]#

3.Best practices for hybrid cloud

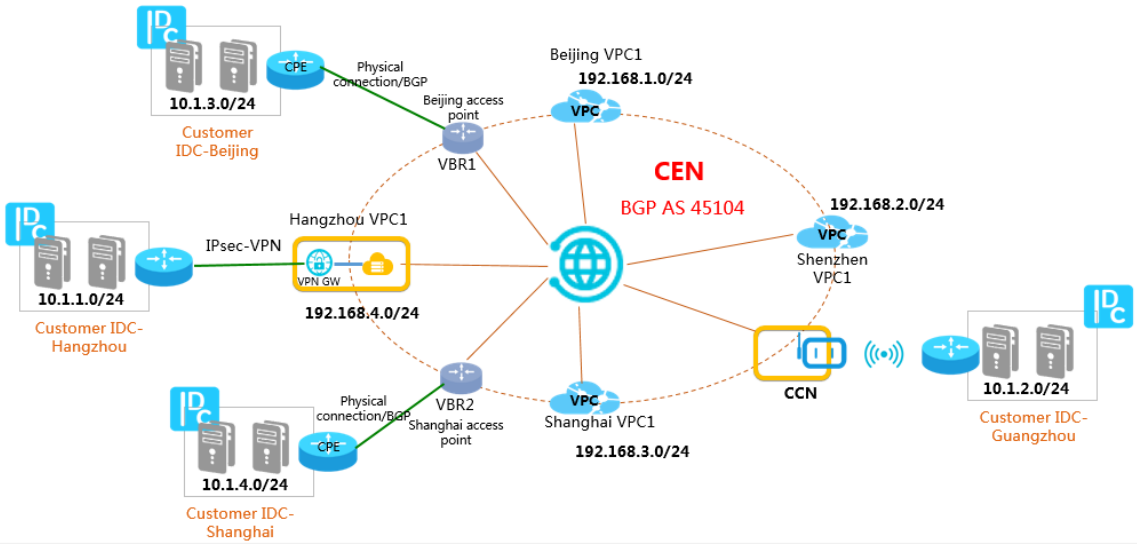
3.1. Build an enterprise-class hybrid cloud by combining multiple connection services

Cloud Enterprise Network (CEN) helps you build a high-quality network environment. CEN provides a simplified networking method to build a hybrid cloud with a scale and communication capability at the enterprise level. This topic describes how to build a hybrid cloud by combining leased lines, VPN gateways, and Smart Access Gateway (SAG) instances.

Network topology

The following network topology is used in this example:

- A company has deployed data centers in the China (Beijing), China (Shanghai), China (Hangzhou), and China (Guangzhou) regions.
- In addition, the company has created virtual private clouds (VPCs) in the China (Beijing), China (Shanghai), China (Hangzhou), and China (Shenzhen) regions.
- The data centers in China (Beijing) and China (Shanghai) are connected to Alibaba Cloud through leased lines. The virtual border routers (VBRs) of the leased lines are attached to a CEN instance.
- The data center in China (Hangzhou) is connected to the VPC in China (Hangzhou) through a VPN gateway.
- The data center in China (Guangzhou) is connected to Alibaba Cloud through an SAG instance. The Cloud Connect Network (CCN) instance to which the SAG instance belongs is attached to the CEN instance.
- The VPCs of the company in China (Beijing), China (Shanghai), China (Shenzhen), and China (Hangzhou) are attached to the CEN instance.



Subnetting

To build a hybrid cloud, make sure that the CIDR blocks to be connected do not overlap with each other. The following table describes the CIDR blocks in this example.

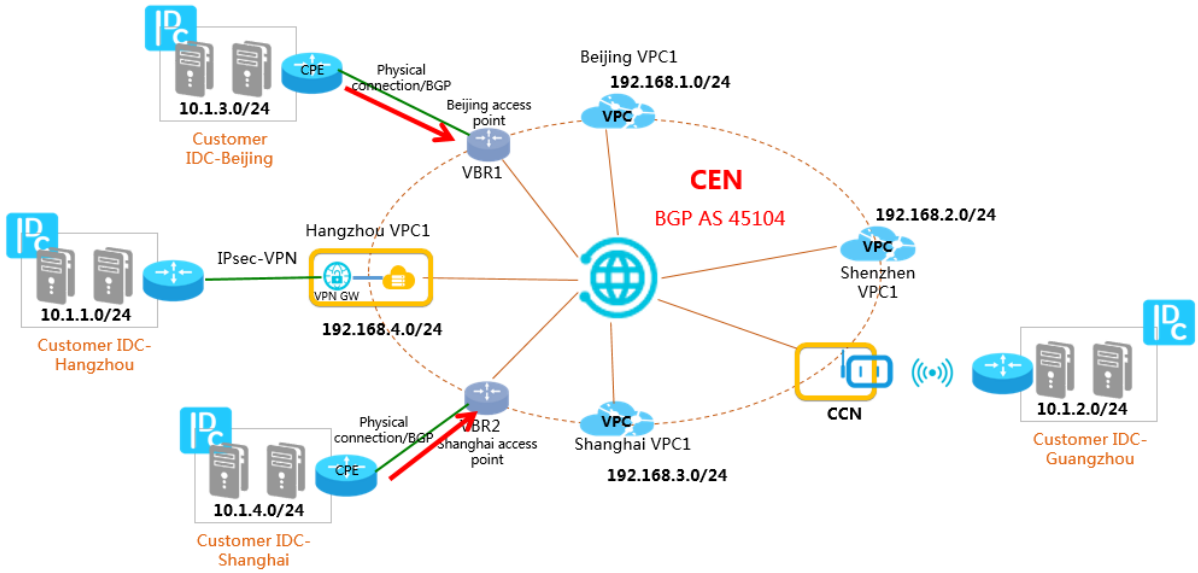
Network	CIDR block
Data center in China (Hangzhou)	10.1.1.0/24
Data center in China (Guangzhou)	10.1.2.0/24
Data center in China (Beijing)	10.1.3.0/24
Data center in China (Shanghai)	10.1.4.0/24
VPC in China (Beijing)	192.168.1.0/24
VPC in China (Shenzhen)	192.168.2.0/24
VPC in China (Shanghai)	192.168.3.0/24
VPC in China (Hangzhou)	192.168.4.0/24

Services for connecting data centers to Alibaba Cloud

The data centers are connected to Alibaba Cloud in the following ways:

- Connect the data centers in China (Beijing) and China (Shanghai) to Alibaba Cloud through leased lines
- Connect the data center in China (Hangzhou) to Alibaba Cloud through a VPN gateway
- Connect the data center in China (Guangzhou) to Alibaba Cloud through an SAG instance

Connect the data centers in China (Beijing) and China (Shanghai) to Alibaba Cloud through leased lines



Procedure

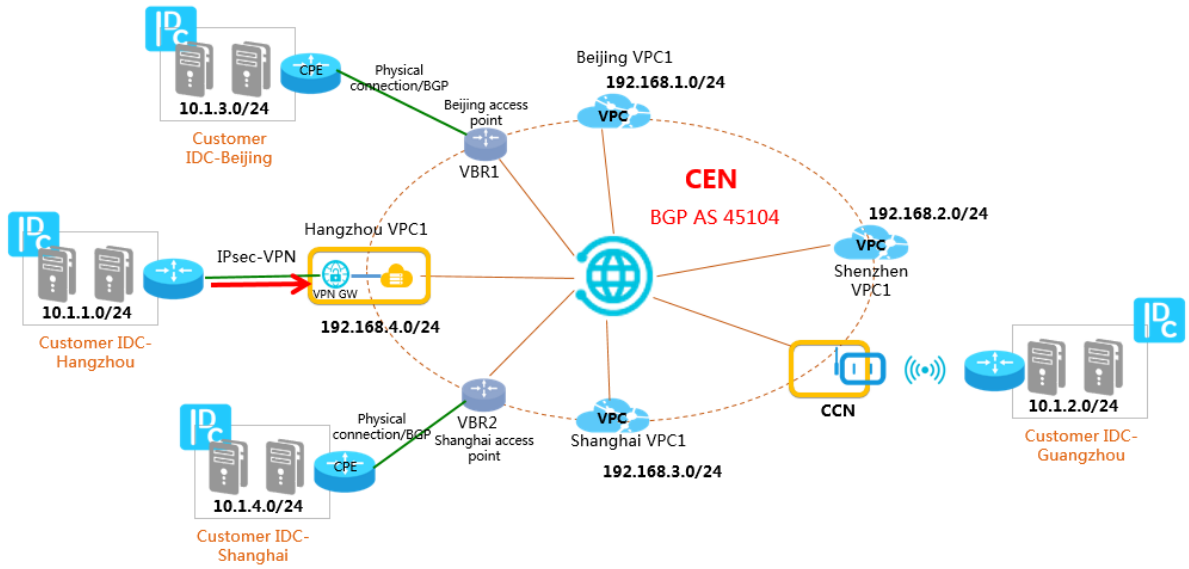
1. Connect the data centers in China (Beijing) and China (Shanghai) to VBRs through leased lines. Then, configure the data centers and the connected VBRs as BGP peers. For more information, see Configure BGP.
2. Use the customer-premises equipment (CPE) of the data centers in China (Beijing) and China (Shanghai) to advertise the CIDR blocks of the data centers to the CEN instance through BGP. The

following table describes the configurations of the CPE in China (Beijing) and China (Shanghai).

Configuration	CPE in China (Beijing)	CPE in China (Shanghai)
Local BGP ASN	A	B
Peer BGP ASN	45104	45104
Network	10.1.3.0/24	10.1.4.0/24

After the data centers and the VBRs are configured as BGP peers, the data centers and the VBRs can learn routes from each other.

Connect the data center in China (Hangzhou) to Alibaba Cloud through a VPN gateway



Procedure:

1. Create an IPsec-VPN connection to connect the data center in China (Hangzhou) to the VPC in China (Hangzhou). For more information, see Connect a data center to a VPC.
2. Configure a specific route or default route that points to Alibaba Cloud.

   Configure a specific route.

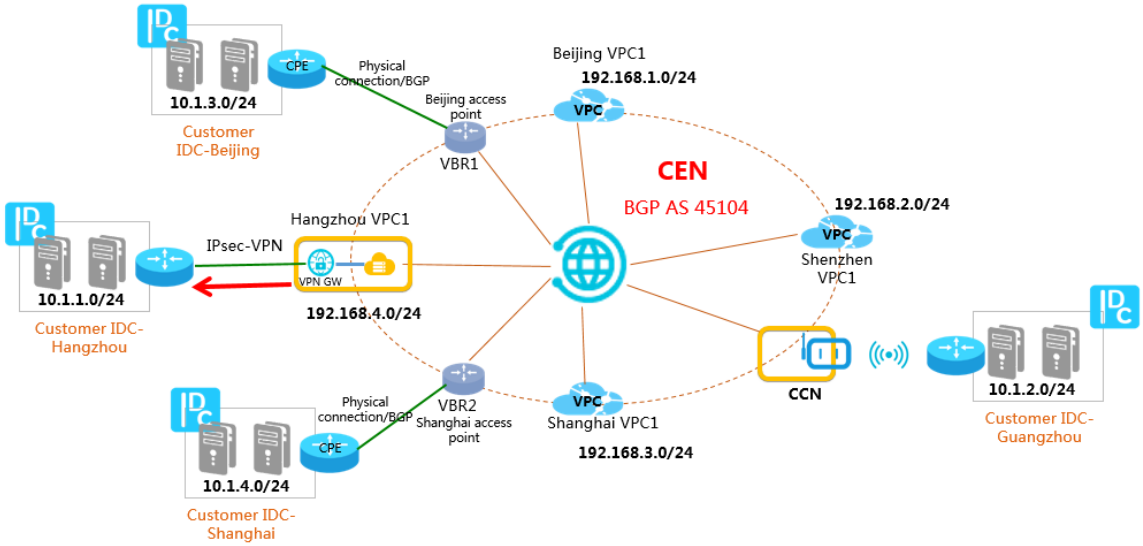
Destination CIDR block	Next hop
10.1.2.0/24	VPN gateway
10.1.3.0/24	VPN gateway
10.1.4.0/24	VPN gateway
192.168.1.0/24	VPN gateway
192.168.2.0/24	VPN gateway

Destination CIDR block	Next hop
192.168.3.0/24	VPN gateway
192.168.4.0/24	VPN gateway

Configure the default route

Destination CIDR block	Next hop
0.0.0.0/0	VPN gateway

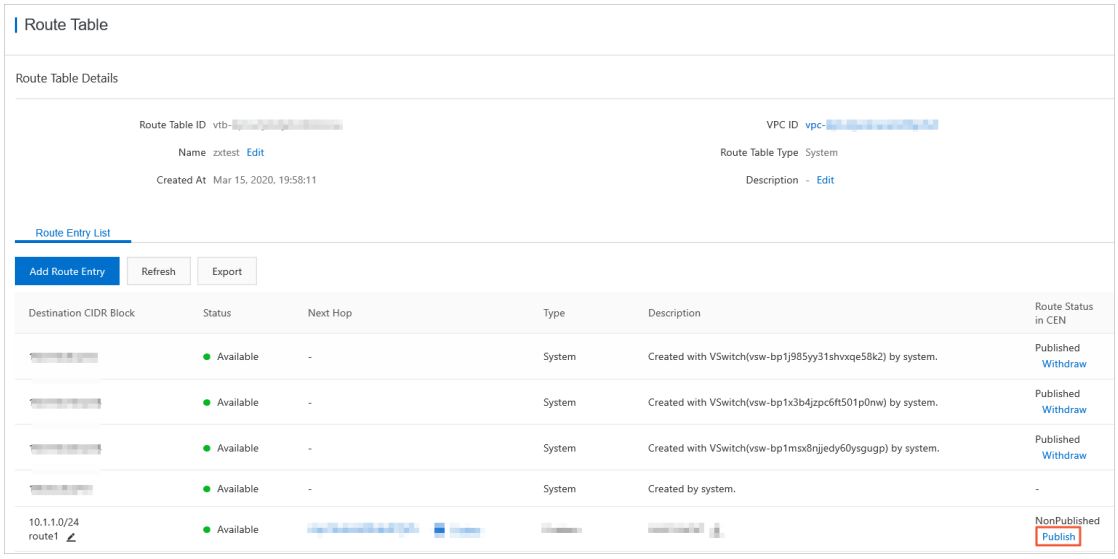
3. To allow the data center to communicate with the network instances that are attached to the CEN instance, you must add a route to the VPC that is associated with the VPN gateway and advertise the route to the CEN instance. The route must point to the data center.



Configure the route based on the following information:

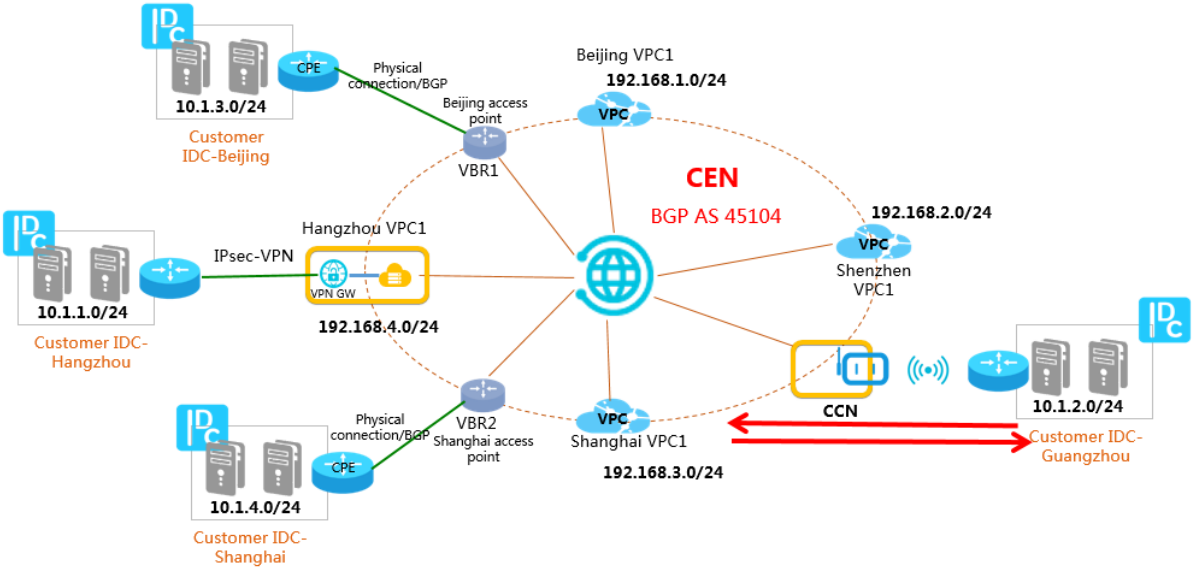
i. Add a route to the route table of the VPC in China (Hangzhou). The destination CIDR block is set to 10.1.1.0/24 and the next hop is set to the VPN gateway that is created for the VPC.

ii. Advertise the route from the VPC in China (Hangzhou) to the CEN instance.



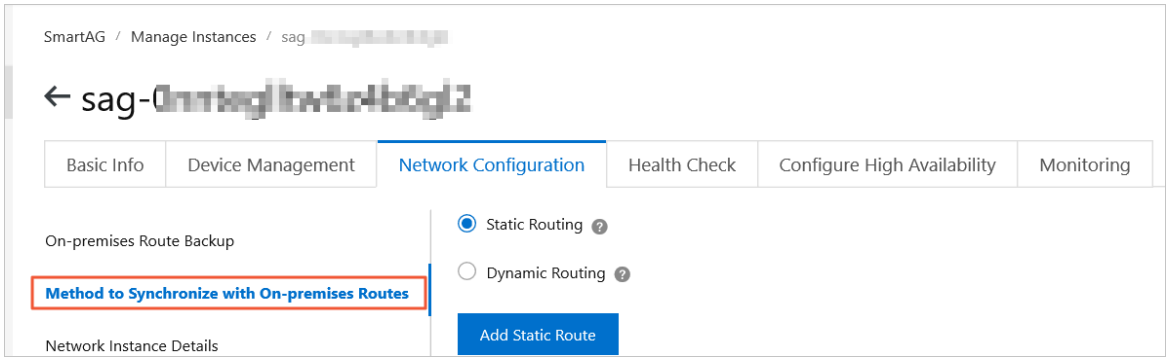
After you advertise the route to the CEN instance, the network instances that are attached to the CEN instance can learn the route. This way, the data center in China (Hangzhou) can communicate with all attached network instances.

Connect the data center in China (Guangzhou) to Alibaba Cloud through an SAG instance

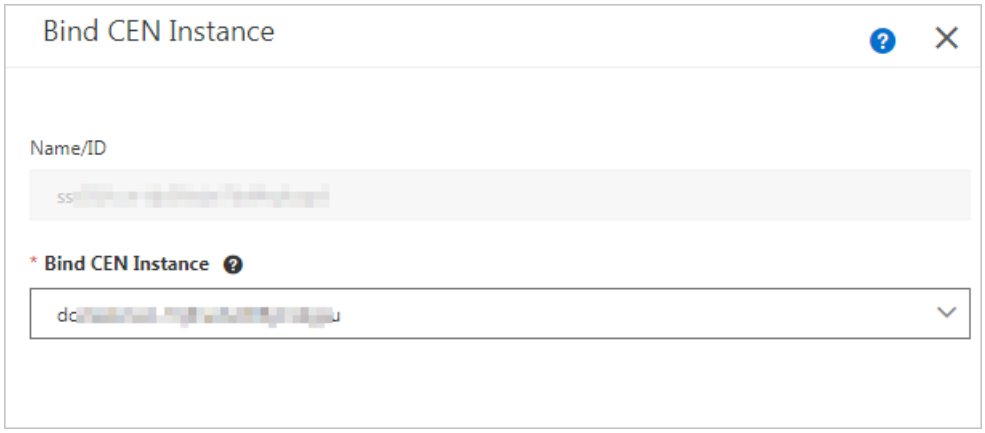


Procedure:

1. Log on to the SAG console, select an SAG instance to connect to the data center in China (Guangzhou), and then configure a route for the connection.



2. Attach the CCN instance that is associated with the SAG instance to the CEN instance. This way, the data center in China (Guangzhou) can communicate with the network instances attached in the CEN instance.

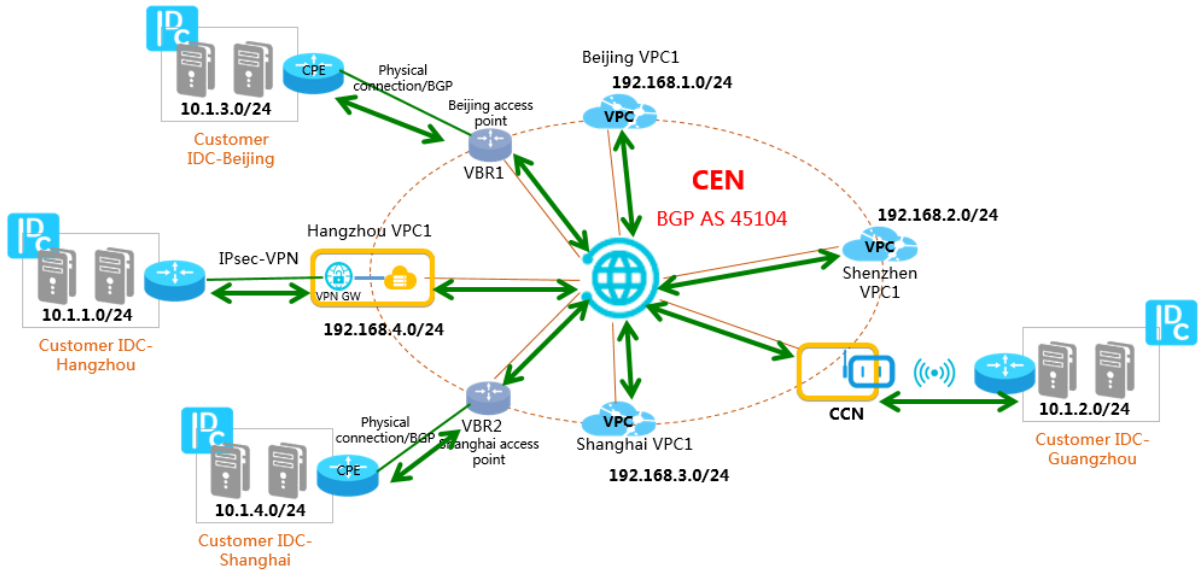


Connect the data centers in all regions

Repeat the preceding procedures to connect all data centers through CEN.

- The data centers in China (Beijing) and China (Shanghai) are connected to Alibaba Cloud through BGP leased lines. Therefore, attach the VBRs to the CEN instance.
- The data center in China (Hangzhou) is connected to Alibaba Cloud through a VPN gateway. Therefore, attach the VPC for which the VPN gateway is created to the CEN instance.
- The data center in China (Guangzhou) is connected to Alibaba Cloud through an SAG instance. Therefore, attach the CCN instance that is associated with the SAG instance to the CEN instance.

The CEN instance dynamically advertises the routes from the attached network instances to avoid route overlapping. This builds a hybrid cloud through which the data centers and the attached network instances can communicate with each other.



For example, the following tables describe the route tables of the CPE in China (Beijing), the VBR in China (Beijing), and the VPC in China (Shenzhen).

CPE in China (Beijing)

Destination CIDR block	Next hop	Route type
10.1.1.0/24	BGP peer: VBR in China (Beijing)	BGP route
10.1.2.0/24	BGP peer: VBR in China (Beijing)	BGP route
10.1.4.0/24	BGP peer: VBR in China (Beijing)	BGP route
192.168.1.0/24	BGP peer: VBR in China (Beijing)	BGP route
192.168.2.0/24	BGP peer: VBR in China (Beijing)	BGP route
192.168.3.0/24	BGP peer: VBR in China (Beijing)	BGP route
192.168.4.0/24	BGP peer: VBR in China (Beijing)	BGP route

VBR in China (Beijing)

Destination CIDR block	Next hop	Route type
10.1.3.0/24	BGP peer: CPE in China (Beijing)	BGP route
10.1.1.0/24	VPC in China (Hangzhou)	CEN route
10.1.2.0/24	CCN	CEN route
10.1.4.0/24	VBR in China (Shanghai)	CEN route

Destination CIDR block	Next hop	Route type
192.168.1.0/24	VPC in China (Beijing)	CEN route
192.168.2.0/24	VPC in China (Shenzhen)	CEN route
192.168.3.0/24	VPC in China (Shanghai)	CEN route
192.168.4.0/24	VPC in China (Hangzhou)	CEN route

VPC in China (Shenzhen)

Destination CIDR block	Next hop	Route type
10.1.1.0/24	VPC in China (Hangzhou)	CEN route
10.1.2.0/24	CCN	CEN route
10.1.3.0/24	VBR in China (Beijing)	CEN route
10.1.4.0/24	VBR in China (Shanghai)	CEN route
192.168.1.0/24	VPC in China (Beijing)	CEN route
192.168.3.0/24	VPC in China (Shanghai)	CEN route
192.168.4.0/24	VPC in China (Hangzhou)	CEN route