

Alibaba Cloud

Express Connect Peering connections

Document Version: 20210713

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 <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1.Migrate peering connections to CEN	05
1.1. Migrate a VPC from a peering connection to a CEN instan... ..	05
1.2. Migrate a VBR from a peering connection to a CEN instan... ..	07
1.3. Roll back the migration	11
2.What is a peering connection	12
3.Quotas related to peering connections	14
4.Billing of peering connections	15
5.Manage Subscription-billed instances	16
6.Manage Pay-As-You-Go-billed instances	17
7.Delete a peering connection	18
8.Connect two VPCs	19
9.Connect a VBR and a VPC	21
10.Connect two VPCs under the same Alibaba Cloud account	23
11.Access multiple VPCs through one physical connection	27
12.Configure a standby Express Connect circuit	32

1. Migrate peering connections to CEN

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

This topic describes how to migrate a VPC 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, and quickly adapts to network changes. This improves the quality of cross-network communication.

 **Warning** Before you freeze or delete the router interfaces, make sure that the routes for both the local and peer VPCs in the peering connection are migrated.

Preparations

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

 **Note** If the overlapping routing function is not enabled for the CEN instance, enable it first.

CEN

Basic Settings

ID	cen-bl-  bz3l89n	Status	Ready
Name	易测试 Edit	Overlapping Routing	<input checked="" type="checkbox"/> Enable
Description	- Edit	Function	

Procedure

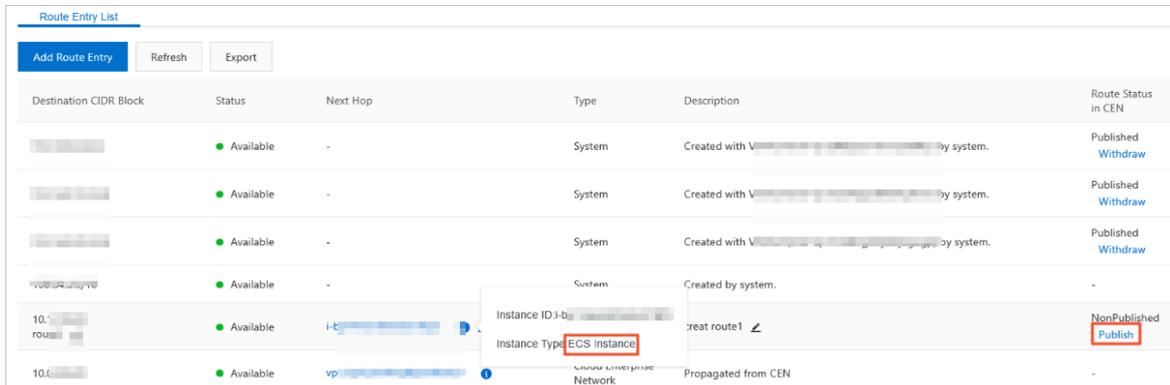
To migrate a VPC from a peering connection to a CEN instance, perform the following steps:

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

1. Log on to the [CEN console](#).
2. On the **Instances** page, find the required CEN instance and click its ID.
3. On the **Networks** tab, click **Attach Network** and attach the VPC that you want to migrate. For more information, see [Attach networks](#).
4. If you want to communicate across regions, purchase a bandwidth plan and configure the bandwidth for the communication.

For more information, see [Set a cross-region bandwidth](#).

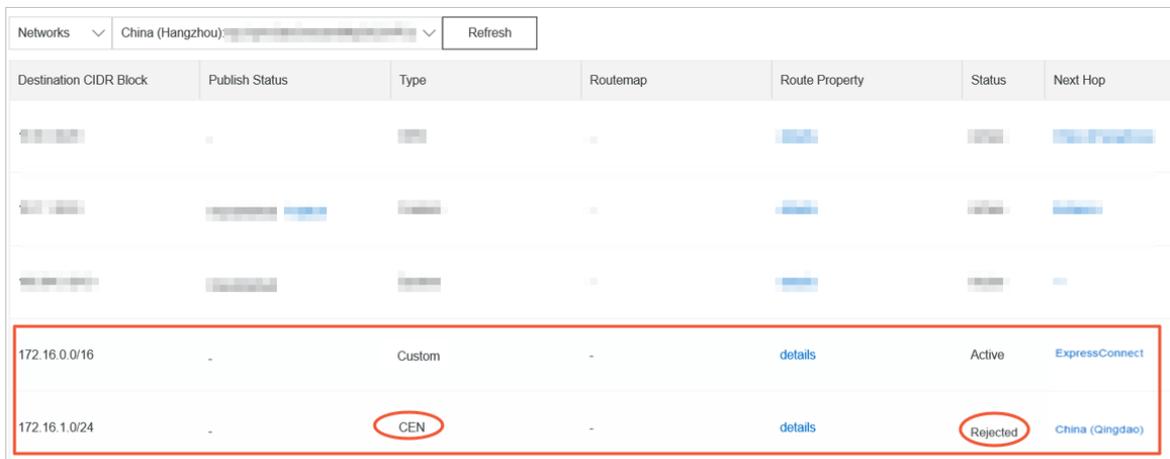
- If you have added routes that point to high-availability virtual IP addresses (HAVIPs) or IP addresses of ECS instances and VPN gateways, go to the VPC console and advertise these routes to the CEN instance based on your connection requirements.



- 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. After you attach the VPC to the CEN instance, make sure that the routes do not conflict.

The static routes that are 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 of the peering connection and delete them after CEN learns the routes. This ensures smooth migration.

In the following figure, the route to 172.16.1.0/24 in the CEN instance is more specific than the route to 172.16.0.0/16 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 172.16.0.0/16 in the VPC console. Then, the route in the CEN instance automatically takes effect.

The duration of the network interruption increases as the number of CEN routes increases. For important business scenarios, we recommend that you use the following method to smoothly migrate the VPC.

- If you want to smoothly migrate the VPC, split the route in the peering connection into routes more specific than the route to 172.16.1.0/24 in the CEN instance. For example, split the route to 172.16.0.0/16 in the peering connection into two routes, one to 172.16.1.0/25 and the other to 172.16.1.128/25.
 - Log on to the VPC console and find the route table to which the route you want to split

belongs.

- b. Click **Add Route Entry** to add two routes in which the destination CIDR blocks are 172.16.1.0/25 and 172.16.1.128/25 and the next hops are the router interface of the peering connection.

Destination CIDR Block	Status	Next Hop	Type	Description	Route Status in CEN	Actions
172.16.1.0/25 route22	Available	n-m-...-id	System			
172.16.1.128/25 test2	Available	n-m-...-id	System			
	Available	-	System			

- c. Find the route to 172.16.0.0/16 and click **Delete** in the Actions column.

Destination CIDR Block	Status	Next Hop	Type	Description	Route Status in CEN	Actions
	Available	-	System		Published	Withdraw
	Available	-	System		Published	Withdraw
	Available	-	System		Published	Withdraw
	Available	-	System	Created by system.	-	-
172.16.0.0/16	Available		Custom		Published	Withdraw Delete

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

Destination CIDR Block	Status	Next Hop	Type	Description	Route Status in CEN	Actions
	Available		Custom		NonPublished	Publish Delete
	Available		Cloud Enterprise Network		-	-
172.16.1.0/24	Available		Cloud Enterprise Network		-	-

- e. After the routes in the CEN instance take effect, delete the routes to 172.16.1.0/25 and 172.16.1.128/25. The smooth migration is complete.

1.2. 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.

CEN

Basic Settings

ID	cen-bl- ibz3l89n	Status	Ready
Name	易测试 Edit	Overlapping Routing Function	Enable
Description	- Edit		

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 networks](#).
5. If you want to communicate across regions, purchase a bandwidth plan and configure bandwidth for the communication.

For more information, see [Set a cross-region bandwidth](#).

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.

Destination CIDR Block	Status	Next Hop	Type	Description	Route Status in CEN
 	Available	-	System	Created with V by system.	Published Withdraw
 	Available	-	System	Created with V by system.	Published Withdraw
 	Available	-	System	Created with V by system.	Published Withdraw
 	Available	-	System	Created by system.	-
10.0.1.0/24	Available	i- 	Instance ID: Instance Type: ECS Instance	reat route 1 ↗	NonPublished Publish
10.0.1.0/24	Available	vpc- 	Network	Propagated from CEN	-

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 [Configure PrivateZone access](#).

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.

Destination CIDR Block	Publish Status	Type	Routemap	Route Property	Status	Next Hop
[Redacted]	-	CEN	-	details	Active	[Redacted]
[Redacted]	Unpublished Publish	Custom	-	details	Active	[Redacted]
[Redacted]	Unpublished	System	-	details	Active	—
192.168.0.0/16	-	Custom	-	details	Active	ExpressConnect
192.168.1.0/24	-	CEN	-	details	Rejected	China (Qingdao)

- o 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.

- o 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.

Basic Information

VBR vbr-2-...w
Access Point Beijing-Daxing-A
Status Active

Name ...
Created At Mar 6, 2018, 19:16:34
CEN cen-7-... Unbind

Physical Connection Interfaces Routes Advertised BGP Subnets BGP Groups BGP Peers CEN Authorization Peering Connections

Add Route Refresh

Route Table ID	Destination Subnet	Status	Next Hop Instance	Next Hop Type	Route Type	CEN Publication Status	Actions
vtb-2-...	192.168.1.128/25	Available	vpc-m-...	VPC	Custom	-	Delete
vtb-2-...	192.168.1.0/25	Available	vpc-m-...	VPC	Custom	-	Delete

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

Basic Information

VBR vbr-2-...w
Access Point Beijing-Daxing-A
Status Active

Name ...
Created At Mar 6, 2018, 19:16:34
CEN cen-7-... Unbind

Physical Connection Interfaces Routes Advertised BGP Subnets BGP Groups BGP Peers CEN Authorization Peering Connections

Advertise BGP Subnet Refresh

Advertised Subnet	Actions
192.168.1.0/25	Delete
192.168.1.128/25	Delete

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

Basic Information

VBR vbr-2-...w
Access Point Beijing-Daxing-A
Status Active

Name ...
Created At Mar 6, 2018, 19:16:34
CEN cen-7-... Unbind

Physical Connection Interfaces Routes Advertised BGP Subnets BGP Groups BGP Peers CEN Authorization Peering Connections

Add Route Refresh

Route Table ID	Destination Subnet	Status	Next Hop Instance	Next Hop Type	Route Type	CEN Publication Status	Actions
vtb-9	192.168.1.128/25	Available	vpc-m5-...	VPC	Custom	-	Delete
vtb-9	192.168.1.0/25	Available	vpc-m5-...	VPC	Custom	-	Delete
vtb-9	192.168.0.0/16	Available	vpc-m-...	VPC	Custom	-	Delete

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

Route Table ID	Destination Subnet	Status	Next Hop Instance	Next Hop Type	Route Type	CEN Publication Status	Actions
vtb-2-1	192.168.1.128/25	Available	vpc-m5-1	VPC	Custom	-	Delete
vtb-2-2	192.168.1.0/25	Available	vpc-m5-2	VPC	Custom	-	Delete
vtb-2-3	10.0.0.0/24	Available	vpc-m5-3	VPC	Custom	-	Delete
vtb-2-4	10.0.0.0/8	Available	pc-2	Physical Connection Interface	Custom	-	Delete
vtb-2-5	192.168.1.0/24	Available	vpc-m5-5	VPC	CEN	-	Delete

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](#).

1.3. 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. What is a peering connection

You can create a peering connection to connect two virtual private clouds (VPCs). In addition, you can create a peering connection to connect a VPC and a virtual border router (VBR).

Initiator and acceptor

When you establish a peering connection between two VPCs or between a VPC and a VBR, one end of the peering connection functions as the initiator. The other end of the peering connection functions as the acceptor. Only the initiator can initiate the peering connection. The acceptor must wait for the initiator to initiate the peering connection. The concepts of initiator and acceptor are only used to control how a peering connection is established. Data transmission between the initiator and acceptor is bidirectional. Therefore, after the peering connection is established, both the initiator and acceptor can send and receive data.

When you connect two VPCs under the same account, you can specify the initiator and acceptor in the Express Connect console. After you specify the initiator and acceptor, the system automatically initiates a connection request and then establishes a peering connection. You do not need to manually send a connection request. To connect two VPCs under different accounts, you must manually send a request to establish a peering connection.

The following table describes the differences between the initiator and acceptor.

Item	Initiator	Acceptor
Whether the configuration of the peer is required before a peering connection is initiated	Yes	Yes
Initiate connection requests	Yes	No
Send messages to the peer after the peering connection is established	Yes	Yes

Connection stages and states

The initiator sends a connection request to the acceptor to establish a peering connection. After the acceptor accepts the request, the peering connection is established.

The following table describes the states of a peering connection at different stages.

 **Note** If you specify the initiator and acceptor when you create a peering connection, the system automatically sends a connection request and establishes the peering connection. The peering connection is activated on both the initiator and acceptor after the peering connection is established.

Stage	State of the peering connection on the initiator	State of the peering connection on the acceptor
Send a connection request from the initiator	Connecting	Accepting
Successfully establish a peering connection	Active	Active

Stage	State of the peering connection on the initiator	State of the peering connection on the acceptor
Deactivate a peering connection	Deactivating	Deactivating
Close a peering connection	Inactive	Inactive
Resend a connection request	Activating	Activating

3. Quotas related to peering connections

This topic provides the quotas related to peering connections.

 Note

Item	Default quota	Limit on quota adjustment
Maximum number of peering connections that can be created for each VPC	5	You can change the quota on the Quota Management page in the Express Connect console.
Maximum number of peering connections that can be created for each VBR	5	You can change the quota on the Quota Management page in the Express Connect console.
Maximum number of peering connections that can be created in each Alibaba Cloud account	10	You can change the quota on the Quota Management page in the Express Connect console.

4. Billing of peering connections

Alibaba Cloud charges fees for the initiator instance of a peering connection and does not charge fees for the acceptor instance.

Billing method

Billing method	Description	Configuration change	Expiration and overdue payment
Subscription	You must pay for a peering connection on a monthly or yearly basis when you purchase it.	You can change the configuration of a peering connection when you renew it.	<ul style="list-style-type: none"> The initiator instance stops forwarding traffic 15 days after the peering connection expires. If you do not renew the peering connection, the initiator instance is locked. After the peering connection expires, Alibaba Cloud sends you reminders on the 8th, 12th, and 14th days. After the initiator instance is locked, Alibaba Cloud also sends you reminders on the 8th, 12th, and 14th days. After you clear the overdue payment, the initiator instance resumes forwarding traffic. The initiator instance is released 15 days after it is locked. Its configuration is cleared and cannot be restored.

Prices of peering connections

Alibaba Cloud charges fees for the initiator instance of a peering connection and does not charge fees for the acceptor instance. The prices vary based on the bandwidth of the initiator instance and the distance between the initiator and acceptor instances. The prices of peering connections between VPCs in the same region are lower than the prices of peering connections between VPCs across regions.

- The final prices of cross-region peering connections are subject to the amount displayed on the [buy page](#). If you have questions about the prices, consult your business manager.
- The following table provides the price of peering connections in the same region. However, Alibaba Cloud does not charge you for such peering connections until August 01, 2021.

Price of peering connections in the same region in mainland China

Bandwidth (Gbit/s)	Initiator instance (USD/month)
1	70

5. Manage Subscription-billed instances

You can change the bandwidth values of your Subscription-billed instances and pay for the change.

Procedure

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, choose **VPC Peering Connections > VPC-to-VPC** or **VPC Peering Connections > VBR-to-VPC**.
3. Select the region of the target peering connection and find the target peering connection.
4. Click



and select the operation you want to perform:

- **Renew**: When the initiator instance is overdue for more than 24 hours, the physical connection interface stops forwarding data and is locked. To avoid affecting your business, we recommend that you renew your instance in a timely manner.
- **Renew and Upgrade/Downgrade**: Change the bandwidth while you renew your instance. The change takes effect in the next billing cycle.
- **Upgrade**: Increase the bandwidth of the initiator.
- **Suspend Initiator/Acceptor**: Suspend the activated initiator or acceptor. Data is no longer forwarded after the suspension.
- **Activate Initiator/Acceptor**: Activate the suspended initiator or acceptor. Data forwarding is restored after the activation.
- **Temporarily Upgrade**: Temporarily increase the bandwidth of the initiator.

The upgrade interval is two hours. The price is charged by the hour. The upgrade takes effect immediately after the payment. Services are not interrupted during the upgrade.

When the upgrade duration ends, the initiator automatically returns to the original bandwidth. Your service will not be interrupted when the initiator returns to the original bandwidth, but intermittent disconnections may occur. We recommend that your applications have re-connection functionalities.

6. Manage Pay-As-You-Go-billed instances

You can delete your Pay-As-You-Go-billed instances, change their bandwidth values, or change their billing method to Subscription.

Procedure

1. Log on to the [Express Connect](#) console.
2. In the left navigation pane, choose **VPC Peering Connections > VPC-to-VPC** or **VPC Peering Connections > VBR-to-VPC**.
3. Select the region of the target peering connection and find the target peering connection.
4. Click



and select the operation you want to perform:

- **Initiate Connection:** When you create a peering connection between two different accounts, you must initiate the connection from the initiator or after adding the acceptor. The connection can be initiated only from the initiator.
- **Upgrade/Downgrade:** Change the bandwidth of the initiator.
- **Switch to Subscription:** Change the billing method of the initiator to Subscription.
- **Suspend Initiator/Acceptor:** Suspend the activated initiator or acceptor. No data is forwarded after suspension.
- **Activate Initiator/Acceptor:** Activate the suspended initiator or acceptor. Data forwarding is restored after activation.
- **Delete:** Delete the peering connection.

7.Delete a peering connection

Before you can delete a peering connection, you must delete the route entries of its initiator and acceptor.

Step 1: Delete route entries

To delete the custom route entries, follow these steps:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, choose **VPC Peering Connections > VPC-to-VPC**.
3. Select a region and find your target peering connection.
4. Click the VPC ID of the initiator. On the **VPC Details** page, click the VPC ID again.
5. In the **Network Resources** section, click the route table link. On the displayed **Route Tables** page, click the route table ID.
6. Find the custom route entry destined for the on-premises data center and then click **Delete**.
7. In the displayed dialog box, click **OK**.
8. Repeat the preceding steps to delete the route entries of the acceptor.

Step 2: Delete the peering connection

To delete the peering connection, follow these steps:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, choose **VPC Peering Connections > VPC-to-VPC**.
3. Select a region and find your target peering connection.
4. Choose  **> Suspend Initiator**. In the displayed dialog box, click **Confirm**.
5. Choose  **> Suspend Acceptor**. In the displayed dialog box, click **Confirm**.
6. Click  **> Delete**. In the displayed dialog box, click **Confirm**.

8. Connect two VPCs

This topic describes how to create a peering connection between two virtual private clouds (VPCs).

Context



Procedure

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, choose **VPC Peering Connections > VPC-to-VPC**.
3. Click **Create Peering Connection**.
4. Configure the parameters of the peering connection.

Parameter	Description
Account Type	<p>Specify whether the VPCs that you want to connect belong to the same Alibaba Cloud account.</p> <ul style="list-style-type: none">◦ Same-account: The VPCs belong to the same Alibaba Cloud account. In this case, the system creates the initiator and acceptor instances and automatically establishes a connection between them.◦ Cross-account: The VPCs belong to different Alibaba Cloud accounts. In this case, you must separately create the initiator and acceptor instances and initiate a connection request from the initiator instance.
Connection Type	<p>Select the type of the peering connection.</p> <ul style="list-style-type: none">◦ VPC-to-VPC: The peering connection connects two VPCs.◦ VBR-to-VPC: The peering connection connects a VPC and a virtual border router (VBR). For more information, see Connect a VBR and a VPC. <p>For this example, select VPC-to-VPC.</p>

Parameter	Description
Routers to Create	<p>Select the router interfaces to create.</p> <ul style="list-style-type: none"> ◦ Initiator and Acceptor: Both the initiator and acceptor instances are created. The initiator instance automatically connects to the acceptor instance. This option appears only when you set Account Type to Same-account. ◦ Initiator Only: Only the initiator instance is created. The initiator instance initiates a connection request. Router Type of the initiator instance can be VRouter or Virtual Border Router (VBR). For a VBR-to-VPC peering connection, Router Type of the initiator instance must be Virtual Border Router (VBR). This option appears only when you set Account Type to Cross-account. ◦ Acceptor Only: Only the acceptor instance is created. Router Type of the acceptor instance must be VRouter. This option appears only when you set Account Type to Cross-account. <div style="background-color: #e1f5fe; padding: 10px; border: 1px solid #cfcfcf;"> <p> Note You must set Product Type to PostPaid. The acceptor instance is free of charge.</p> </div>
Local VPC ID	Select the ID of the local VPC, which is the connection initiator.
Local Region	Select the region of the local VPC.
Peer VPC ID	Select the ID of the peer VPC, which is the connection acceptor.
Peer Region	Select the region of the peer VPC.
Bandwidth	<p>Specify the bandwidth of the peering connection.</p> <p>You do not need to specify the bandwidth for the acceptor instance. The default bandwidth is used.</p>
Validity	<p>Specify the subscription period.</p> <p>To enable automatic renewal upon expiration, select Auto-renewal.</p>

9. Connect a VBR and a VPC

This topic describes how to create a peering connection between a virtual border router (VBR) and a virtual private cloud (VPC).

Context



Notice

Procedure

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, choose **VPC Peering Connections > VBR-to-VPC**.
3. Click **Create Peering Connection**.
4. On the **Express Connect - Peering connections** page, configure the parameters of the peering connection.

Parameter	Description
Account Type	Specify whether the VBR and VPC that you want to connect belong to the same Alibaba Cloud account. Same-account : The VBR and VPC belong to the same Alibaba Cloud account. In this case, the system creates the initiator and acceptor instances and automatically establishes a connection between them.
Connection Type	Select the type of the peering connection. <ul style="list-style-type: none"> ◦ VPC-to-VPC: The peering connection connects two VPCs. ◦ VBR-to-VPC: The peering connection connects a VPC and a VBR. For this example, select VBR-to-VPC .
Routers to Create	Select the router interfaces to create. Initiator and Acceptor : Both the initiator and acceptor instances are created. The initiator instance automatically connects to the acceptor instance.
Local Region	Select the region of the VBR.
Local Access Point	Select the access point to which the VBR connects.
Local VBR ID	Select the ID of the VBR.
Peer Region	Select the region of the VPC.
Peer VPC ID	Select the ID of the VPC.

Parameter	Description
Bandwidth	Specify the bandwidth of the peering connection. You do not need to specify the bandwidth for the acceptor instance. The default bandwidth is used.
Validity	Specify the subscription duration. To enable automatic renewal upon expiration, select Auto-renewal .

5. Click **Buy Now**.
6. Read and select **I have read and agree to Express Connect -Peering Connections Agreement of Service**. Then, click **Pay**.

10.Connect two VPCs under the same Alibaba Cloud account

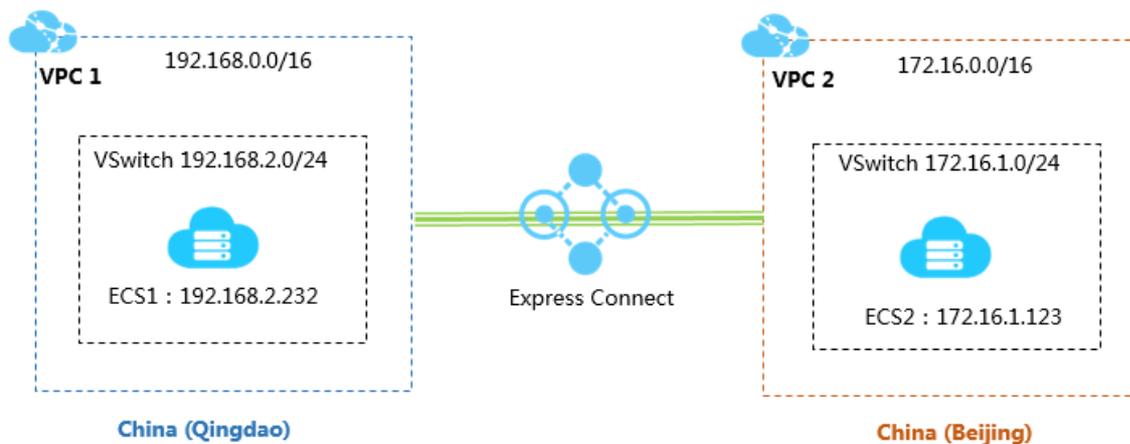
This topic describes how to use Express Connect to connect two VPCs under the same Alibaba Cloud account.

Note

If it is the first time that you use Express Connect to connect two VPCs, we recommend that you try Cloud Enterprise Network (CEN). For more information, see [Overview](#).

Example network architecture

The following figure shows the example network architecture that is used by Express Connect to connect two VPCs.



Prerequisites

The classless inter-domain routing (CIDR) blocks of the two VPCs or vSwitches in the VPCs do not conflict.

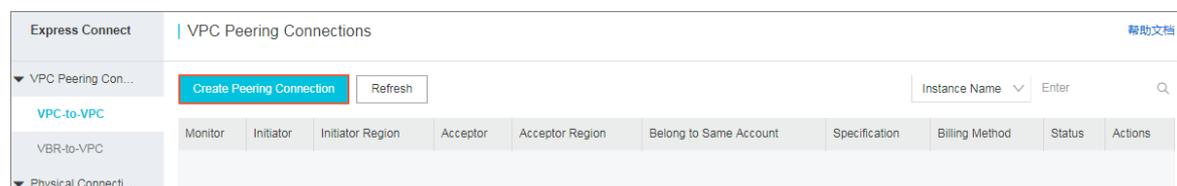
Step 1: Create a peering connection

To create a peering connection, perform the following steps:

1. Log on to the [Express Connect](#) console.
2. In the left-side navigation pane, choose **VPC Peering Connections > VPC-to-VPC**.
3. Select a region.

For this example, select **China (Qingdao)**.

4. On the page that appears, click **Create Peering Connection**.



5. Specify parameters of the peering connection.

For this example, use the following configuration:

- **Account Type:** Select **Same-account**.
- **Connection Type:** Select **VPC-to-VPC**.
- **Routers to Create:** Select **Initiator and Acceptor**.

The system configures the router of the local VPC as the initiator and the router of the peer VPC as the acceptor. It automatically connects the two routers.

- **Local Region:** Select the region of the local VPC. For this example, select **China (Qingdao)**.
- **Local VPC ID:** Select the ID of the local VPC. For this example, select **VPC1**.
- **Peer Region:** Select the region of the peer VPC. For this example, select **China (Beijing)**.
- **Peer VPC ID:** Select the ID of the peer VPC. For this example, select **VPC2**.
- **Bandwidth:** Select the bandwidth for the peering connection between the VPCs. For this example, select **2 Mbit/s**.
- **Validity:** Select the validity period of the peering connection. For this example, select **2 Months**.

6. Click **Buy Now** and complete the payment.

7. Return to the **VPC-to-VPC** page to view the created peering connection.

If both the initiator and acceptor instances are in the **Activated** state, the peering connection is established.

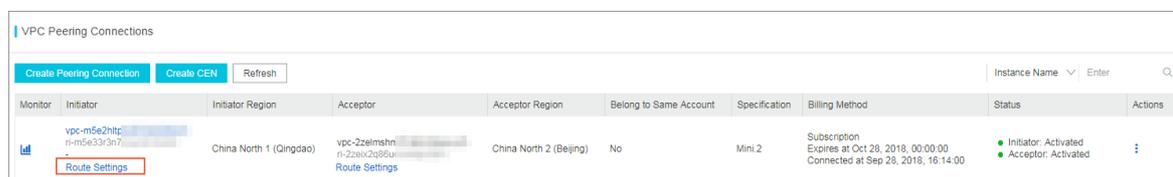


Step 2: Add routes

After the peering connection is established, add routes for the connected VPCs.

Perform the following steps:

1. On the **VPC-to-VPC** page, find the created peering connection.
2. Click **Route Settings** under the initiator instance.



3. Click **Add Route**, enter the CIDR block of the local VPC or the vSwitch that you want to connect in the VPC, and then click **Confirm**.

For this example, enter 172.16.0.0/16.

4. Click **Route Settings** under the acceptor instance.



5. Click **Add Route**, enter the CIDR block of the peer VPC or the vSwitch that you want to connect in the VPC, and then click **Confirm**.

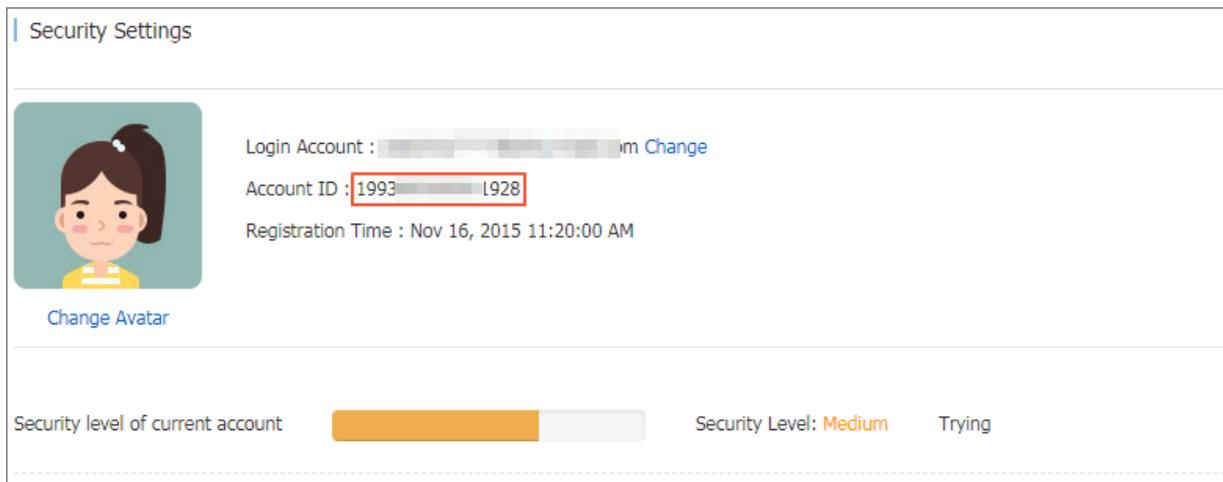
Step 3: Configure security group rules

After a peering connection is established between two VPCs, you must configure security group rules to enable communication between ECS instances in the VPCs.

In this example, the following ECS instances and security groups are configured.

Item	Account A	Account A
Alibaba Cloud account ID	AccountID_A	AccountID_A
ECS instance ID	InstanceID_A	InstanceID_B
Security group ID	SecurityGroupID_A	SecurityGroupID_B

You can view the ID of your Alibaba Cloud account in [Account Center](#).



Perform the following operations to configure security group rules:

1. Log on to the [ECS console](#).
2. In the left-side navigation pane, choose **Network & Security > Security Groups**.
3. Select the region of the ECS instance for which you want to configure security group rules.
4. Find the security group and click **Add Rules**.
5. On the **Security Group Rules** page, click **Add Security Group Rule**.
6. Specify the protocol type, port range, authorization object, and other parameters of the security group rule.

 **Notice** If the two VPCs are in different regions, set Authorization Type to IPv4 CIDR Block and enter the CIDR block of the peer VPC.

If the VPCs are in the same region, set Authorization Type to Security Group.

For this example, set Authorization Type to IPv4 CIDR Block.

7. Click **OK**.

Step 4: Test connectivity between the VPCs

After you establish the peering connection and add routes, log on to an ECS instance in one VPC and ping the private IP address of an ECS instance in the other VPC. If the IP address is reachable, the two VPCs are connected.

11. Access multiple VPCs through one physical connection

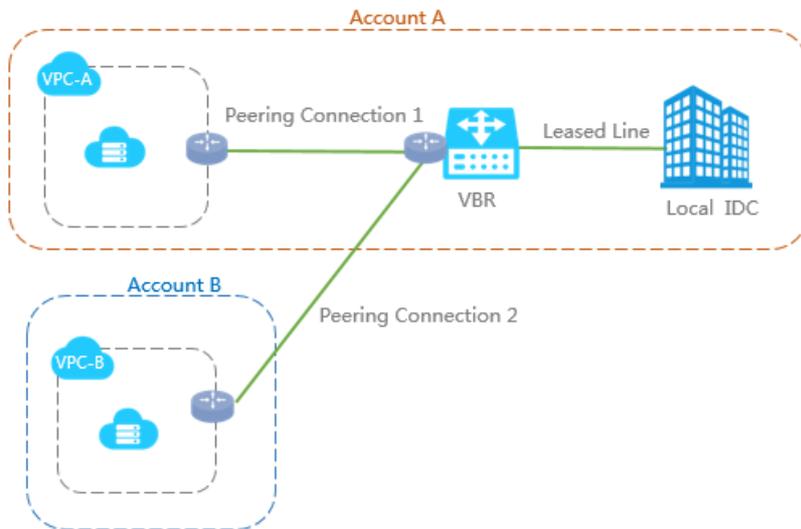
You can use a physical connection that is already connected to an access point of Alibaba Cloud to connect multiple VPCs. This topic describes how to use a physical connection to connect your on-premises data center with two VPCs that belong to different accounts.

Note Currently, a physical connection can be used by five VPCs at most. You can open a ticket to increase the quota.

Scenario

This topic takes the network architecture in the following figure as an example. A company registers account A on Alibaba Cloud and creates VPC-A. The company creates a physical connection under account A to connect its on-premises data center (172.16.0.0/12) with VPC-A. A subsidiary of the company registers account B on Alibaba Cloud and creates VPC-B under account B. The subsidiary wants to connect VPC-B to the on-premises data center.

Because the company has purchased a physical connection under account A and connected the on-premises data center to an access point of Alibaba Cloud, account B of the subsidiary can also use this physical connection to connect the VPC under account B to the on-premises data center.



In this topic, the VPC and physical connection configurations are as follows:

Account A	Account B
Account ID: 12345678	Account ID: 87654321
VPC <ul style="list-style-type: none"> Name: VPC-A Region: China (Beijing) VPC ID: vpc-12345678 CIDR block: 10.10.0.0/16 	VPC <ul style="list-style-type: none"> Name: VPC-B Region: China (Hangzhou) VPC ID: vpc-87654321 CIDR block: 192.168.0.0/16

Account A	Account B
Physical connection <ul style="list-style-type: none"> • VBR name: VPC-Beijing • VBR ID: vbr-12345678 • Physical connection ID: pc-AAA • VLAN ID: 1000 	None

Overview

To connect VPC-B under account B to the on-premises data center by using the physical connection and VBR of account A, you only need to establish a peering connection between the VBR and VPC-B.

1. Step 1: Create an initiator

In VBR-to-VPC peering connections, the VBR must be the initiator. In this topic, create a router interface for the VBR by using account A and use the router interface as the connection initiator.

2. Step 2: Create an acceptor

Create a router interface for the VRouter of the VPC to be connected and use the router interface as the connection acceptor.

3. Step 3: Add the acceptor and the initiator to establish a peering connection

Add the acceptor and the initiator respectively for the created router interfaces, and then initiate the connection from the initiator.

4. Step 4: Configure route entries

Add routes to the connection devices of the VPC, VBR, and on-premises data center respectively to forward traffic.

5. Step 5: Perform an acceptance test (optional)

After the network is connected, you can test the speed of the physical connection to check whether the bandwidth meets your service needs.

Prerequisites

The on-premises data center is connected with VPC-A of account A through the physical connection.

Step 1: Create an initiator

To create an initiator, follow these steps:

1. Log on to the
2. Log on to the [Express Connect console](#) by using the credentials of account A.
3. In the left-side navigation pane, choose **VPC Peering Connections > VBR-to-VPC** and then click **Create Peering Connection**.
4. Configure the peering connection.

The configurations in this topic are as follows. For more information, see [Connect a VBR and a VPC](#).

- **Account type:** Select **Different from Peer's**.
- **Connection Type:** Select **VBR-to-VPC**.

- **Routers to Create:** Select **Create Initiator**.
 - **Local Region:** Select the region of the created VBR. In this example, select **China (Beijing)**.
 - **Local Access Point:** Select the access point of the physical connection connected to the VBR.
 - **Local VBR ID:** Select the created VBR.
 - **Peer Region:** Select the region to which the target VPC belongs. In this topic, select **China (Hangzhou)**.
 - **Bandwidth:** Select the bandwidth for intranet communication. In this topic, select **2Mb**.
5. View the created initiator and record the initiator router interface ID.

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status
	vbr-2ze0ya5 vbr-2ze0ya5 Route Settings	Beijing-Daxing-A	Add Acceptor	China (Hangzhou)	-	2Mbps	Pay-As-You-Go Created at Jan 16, 2019, 18:48:04	● Initiator: Disconnected ● Acceptor: Disconnected

Step 2: Create an acceptor

After the initiator is created, you need to create an acceptor for the VPC to be connected under account B.

To create an acceptor, follow these steps:

1. Log on to the [Express Connect console](#) by using the credentials of account B.
2. In the left-side navigation pane, choose **VPC Peering Connections > VBR-to-VPC** and then click **Create Peering Connection**.
3. Configure the peering connection and then click **OK**.

The configurations in this topic are as follows. For more information, see [Connect a VBR and a VPC](#).

- **Account type:** Select **Different from Peer's**.
- **Connection Type:** Select **VBR-to-VPC**.
- **Routers to Create:** Select **Acceptor Only**.
- **Local Region:** Select the region to which the target VPC belongs. In this topic, select **China (Hangzhou)**.
- **Local VPC ID:** Select the target VPC to be connected. In this topic, select VPC-B.
- **Peer Region:** Select the region to which the created VBR belongs. In this topic, select **China (Beijing)**.
- **Peer Access Point:** Select the access point of the physical connection connected to the VBR.

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
	vbr-2ze0ya5 vbr-2ze0ya5 Route Settings	Beijing-Daxing-A	vpc-bp1pq4oyrau vpc-bp1pq4oyrau Route Settings	China (Hangzhou)	Yes	100Mbps	Pay-As-You-Go Created at Dec 28, 2018, 14:50:58 Connected at Dec 28, 2018, 14:51:47	● Initiator: Activated ● Acceptor: Activated	

4. View the created acceptor and record the acceptor router interface ID.

Step 3: Add the acceptor and the initiator to establish a peering connection

To establish a peering connection between VPC-B and the VBR, follow these steps:

1. Log on to the [Express Connect console](#) by using the credentials of account B.
2. In the left-side navigation pane, choose **VPC Peering Connections > VBR-to-VPC**.
3. Select the region of the acceptor, find the target acceptor, and click **Add Initiator**.

4. On the **Add Instance** page, complete the following configurations.
 - i. **Account** : Select **Another Account** .
 - ii. **Initiator Router Interface**: Enter the router interface ID of the created initiator, for example, ri-1234567.
 - iii. Click **OK**.
5. Log on to the **Express Connect console** by using the credentials of account A.
6. In the left-side navigation pane, choose **VPC Peering Connections > VBR-to-VPC**.
7. Select the region of the initiator, find the target initiator, and click **Add Acceptor**.
8. On the **Add Instance** page, complete the following configurations.
 - i. **Account** : Select **Another Account** .
 - ii. **Acceptor Router Interface**: Enter the ID of the created acceptor router interface, for example, ri-1234567.
 - iii. Click **OK**.
9. Click



in the **Actions** column and then choose **Initiate Connection**.

The peering connection is established if both the acceptor and the initiator are in the activated state.

Monitor	Initiator	Initiator Region	Acceptor	Acceptor Region	Belong to Same Account	Specification	Billing Method	Status	Actions
Route Settings	vbr-2zeofya5g ri-2zeokspzqbp4	Beijing-Daxing-A	vpc-bp1aeivy9ec ri-bp1meruzumw	China (Hangzhou)	No	2Mbps	Pay-As-You-Go Created at Jan 16, 2019, 18:48:04 Connected at Jan 16, 2019, 19:22:56	● Initiator: Activated ● Acceptor: Activated	

Step 4: Configure route entries

After establishing the peering connection, you must configure routes in the VPC, VBR, and on-premises data center.

Add route entries in VBR

To add a route entry to the on-premises data center and VPC respectively, follow these steps:

1. Log on to the **Express Connect console** by using the credentials of account A.
2. In the left-side navigation pane, choose **Physical Connections > Virtual Border Routers (VBRs)**.
3. Select the region of the VBR and then click the instance ID of the target VBR.
4. Click the **Routes** tab and then click **Add Route**.
5. Follow these steps to add a route that forwards the traffic destined for the on-premises data center (CIDR block: 172.16.0.0/12) from the VBR to the physical connection:
 - i. **Destination Subnet** : the CIDR block of the on-premises data center. In this topic, enter 172.16.0.0/12.
 - ii. **Next Hop Type**: Select **Physical Connection Interface**.
 - iii. **Next hop**: Select the created physical connection.
 - iv. Click **OK**.
6. Click **Add Route** to add one more route that forwards the traffic destined for the VPC (CIDR block: 192.168.0.0/16) from the VBR to the VPC.

- i. **Destination Subnet** : Enter the IP address range of VPC-B. In this topic, enter 192.168.0.0/16.
- ii. **Next Hop Type**: Select **VPC**.
- iii. **Next Hop**: Select the VPC to be connected. In this topic, select VPC-B.
- iv. Click **OK**.

Add a route in VPC

Follow these steps to add a route that forwards the traffic, destined for the on-premises data center (CIDR block: 172.16.0.0/12), from the VPC to the VBR:

1. Log on to the [Express Connect console](#) by using the credentials of account B.
2. In the left-side navigation pane, choose **VPC Peering Connections > VBR-to-VPC**.
3. Select the peer connection region, find the acceptor, and then click **Route Settings**.
4. Click **Add Route** and in the displayed dialog box, enter the CIDR block of the on-premises data center (172.16.0.0/12 in this topic). Click **Confirm**.

Configure a route for the on-premises data center

After you configure routes on Alibaba Cloud, you need to add a route entry for the VPC CIDR block in the physical connection device of the on-premises data center. The destination CIDR block is the Alibaba Cloud-side IP address. For example:

```
ip route 192.168.0.0/16 10.100.0.1
```

Step 5: Perform an acceptance test (optional)

After the VPC is connected to the local data center, test the speed of the physical connections to ensure that service needs are met. For more information, see [Test the network performance of a physical connection](#).

12. Configure a standby Express Connect circuit

This topic describes how to configure health checks and route weights for peering connections that are established on each virtual border router (VBR). This ensures that a standby Express Connect circuit can take over when the active Express Connect circuit is not working as expected.

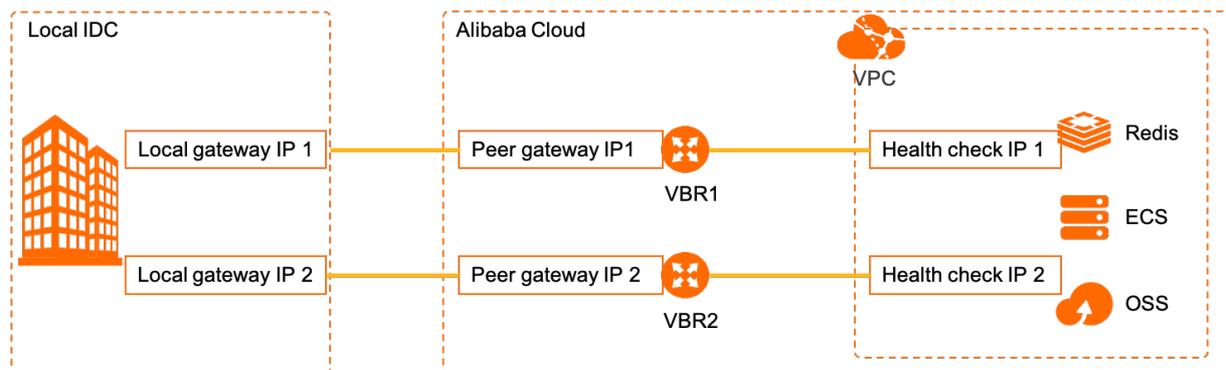
Prerequisites

- Two Express Connect circuits are requested and Alibaba Cloud is connected to a data center over an Express Connect circuit.
- Two peering connections are established between a VBR and a VPC. For more information, see [Create a dedicated connection over an Express Connect circuit](#) and [Connect a VBR and a VPC](#).
- Static routes are configured for the VBR and data center. Border Gateway Protocol (BGP) is not used.

Context

Alibaba Cloud sends a **ping** packet to the IP address of the data center from the source IP address every 2 seconds. If no response is returned for eight consecutive **ping** packets, the other Express Connect circuit takes over.

Note If Copp policies or anti-attack policies are configured for the network device of the data center, such as a Cisco device, probe packets of health checks may be dropped and oscillation may occur in health check connections. We recommend that you disable speed throttling for the network device of the data center.



The following table provides details of the network topology.

Configuration	IP address/CIDR block
VPC	192.168.0.0/16
Data center	172.16.0.0/16
Connection between the first VBR and the data center	<ul style="list-style-type: none"> • IP address of the VBR gateway: 10.10.10.1 • IP address of the data center gateway: 10.10.10.2 • Subnet mask: 255.255.255.252

Configuration	IP address/CIDR block
Connection between the second VBR and the data center	<ul style="list-style-type: none"> IP address of the VBR gateway: 10.10.11.1 IP address of the data center gateway: 10.10.11.2 Subnet mask: 255.255.255.252
Health checks for the first peering connection	<ul style="list-style-type: none"> Source IP address: 192.168.10.1 Destination IP address: 10.10.10.2
Second health check	<ul style="list-style-type: none"> Source IP address: 192.168.10.2 Destination IP address: 10.10.11.2

Step 1: Configure health checks

You must configure health checks for both peering connections.

- 1.
2. In the top navigation bar, select the region and choose **VPC Peering Connections > VBR-to-VPC** in the left-side navigation pane.
3. Find the peering connection and choose  **> Health Check** in the **Actions** column.
4. In the **Health Check** panel, click **Settings**.
5. In the **Modify VBR** panel, set the following parameters and click **OK**.

Parameter	Description
Source IP address	An idle private IP address of the connected VPC.
Destination IP address	The IP address of the network device interface in the data center. If you want to send ICMP packets from the data center to the VPC to perform health checks, we recommend that you enter the source IP address of the health check. Then, configure routes that point to the new destination IP address.

6. Repeat the preceding steps to configure health checks for the other peering connection.

 **Note** The source IP address for health checks of the second peering connection cannot be the same as that of the first peering connection.

Step 2: Configure route weights

In this example, load balancing routes are configured.

1. Log on to the [VPC console](#).
2. In the left-side navigation pane, click **Route Tables**.
3. On the **Route Tables** page, find the VPC where you want to configure load balancing routes and click its ID. Then, click the ID of the route table.

4. On the **Route Entry List** tab, click **Custom**, and then click **Add Route Entry**.
5. Set the following parameters and click **OK**.
 - **Destination CIDR Block**: Enter the destination CIDR block.
 - **Next Hop Type**: Select **Router Interface (To VBR)**. Traffic destined for IP addresses within the destination CIDR block is forwarded to the router interface of the VBR.

Select **Load Balancing Routing** as the routing method and specify the two VBRs that are connected to the VPC as the next hop. The weight must be an integer from 1 to 255. The default value is 100. The weights of the instances must be the same. This way, traffic can be evenly distributed to the next-hop instances.
6. Click **Add Route Entry** and set the following parameters to add a route from the first VBR to the data center.
 - **Destination CIDR Block**: Enter the destination CIDR block.
 - **Next Hop Type**: Select **Router Interface (To VBR)**. Traffic destined for IP addresses within the destination CIDR block is forwarded to the router interface of the VBR.

Select **General Routing** as the routing method and specify the first VBR interface as the next hop.
7. Click **Add Route Entry** and set the following parameters to add a route from the second VBR to the data center.
 - **Destination CIDR Block**: Enter the destination CIDR block.
 - **Next Hop Type**: Select **Router Interface (To VBR)**. Traffic destined for IP addresses within the destination CIDR block is forwarded to the router interface of the VBR.

Select **General Routing** as the routing method and specify the second VBR interface as the next hop.

Step 3: Configure static routes for the source IP addresses of health checks on the CPE device of the data center

Static routes are configured for the VBR and data center. If BGP is not used, you must configure the following static routes for the customer-premises equipment (CPE) of the data center.

- Set the next hop of the source IP address for the first peer connection health checks as the IP address of the first VBR.
- Set the next hop of the source IP address for the second peer connection health checks as the IP address of the second VBR.

Step 4: Test the network connectivity

Disable an Express Connect circuit and ping the cloud resources deployed in the VPC to test whether the standby Express Connect circuit can work as expected.

 **Note** If BGP is used on the VBRs and the CPE device of the data center, the VBR must advertise BGP CIDR blocks for the IP addresses used in health checks.

- 1.
2. In the top navigation bar, select the region and click **Virtual Border Routers (VBRs)** in the left-side navigation pane.

- 3.
4. On the details page of the VBR, click the **Routes** tab and click **Add Route**.
5. In the **Add Route** panel, set the following parameters and click **OK**.
 - **Destination CIDR Block**: Enter the source IP address of health check. 192.168.10.1/32 is used in this example.
 - **Next Hop Type**: Select **VPC**.
 - **Next Hop**: Select the VPC that you want to connect.
6. On the VBR details page, click **Advertised BGP Subnets**, and then click **Advertise BGP Subnet**.
7. On the **Advertise BGP Subnet** page, enter the source IP address of the health check.
8. Repeat the preceding steps to advertise BGP CIDR blocks for health checks of the second VBR.