

Alibaba Cloud Express Connect

Peering connections

Issue: 20190814

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 due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall 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 the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. 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 bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, 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 content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, 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 the Alibaba Cloud website, product programs, or content 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 contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information 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.
	This warning information 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 restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	It is used for commands.	Run the <code>cd / d C :/ windows</code> command to enter the Windows system folder.
<i>Italics</i>	It is used for parameters and variables.	<code>bae log list --instanceid Instance_ID</code>
[] or [a b]	It indicates that it is an optional value, and only one item can be selected.	<code>ipconfig [-all -t]</code>

Style	Description	Example
<code>{}</code> or <code>{a b}</code>	It indicates that it is a required value, and only one item can be selected.	<code>swich {stand slave}</code>

Contents

Legal disclaimer.....	I
Generic conventions.....	I
1 What is a peering connection?.....	1
2 Billing of peering connections.....	3
3 Limits.....	5
4 Manage Pay-As-You-Go-billed instances.....	6
5 Delete a peering connection.....	7
6 Interconnect two VPCs.....	8
7 Interconnect a VPC and a VBR.....	11
8 Interconnect two VPCs under the same account.....	13
9 Interconnect two VPCs under different accounts.....	17
10 Access multiple VPCs through one physical connection.....	23

1 What is a peering connection?

You can establish a peering connection between two VPCs or between a VPC and a Virtual Border Router (VBR).

Initiator and acceptor

When you establish a peering connection, one end (VPC or VBR) of the connection is the initiator, and the other end is the acceptor. Only the initiator can initiate a connection. The acceptor can only wait for the initiator to initiate a connection. The initiator and the acceptor are only used to control the process of connection establishment. After the connection is established, the communication link is bidirectional and there is no difference between the initiator and the acceptor.

For interconnections between VPCs under the same account, Express Connect provides an option to create the initiator and the acceptor at the same time. You do not need to manually initiate the connection. The system will automatically initiate and establish the connection. For interconnections between VPCs under different accounts, you must manually initiate a connection.

The following table compares the initiator and acceptor.

Item	Initiator	Acceptor
Is this end charged when VPCs are interconnected in the same region?	No	No
Is this end charged when VPCs are interconnected between different regions ?	Yes	No
Is it required to configure peer information before initiating a connection?	Yes	Yes
Can this end initiate a connection?	Yes	No
Can this end send messages to the peer end after a connection is established?	Yes	Yes

Connection process and status

In the peering connection process, the initiator initiates a connection. The acceptor then receives the connection, after which the connection is established successfully.

During different stages of the connection process, the status of a peering connection is also different, as shown in the following table.



Note:

If you choose to create both ends at the same time when establishing a peering connection, the system automatically initiates and establishes a connection. In this case, the initiator and the acceptor become activated after being created.

Connection process	Initiator status	Acceptor status
The initiator initiates a connection.	Connecting	Accepting
The connection is established.	Activated	Activated
The connection is suspended.	Suspending	Suspending
The connection is broken.	Suspended	Suspended
A connection is re-initiated.	Activating	Activating
The connection is established.	Activated	Activated

2 Billing of peering connections

When you set a peering connection, Alibaba Cloud charges fees for the initiator instance, but does not charge fees for the acceptor instance.

Billing method

Billing method	Description	Upgrade or downgrade	Overdue payment process
Subscription	Monthly or yearly subscription with the billing unit of USD/month	Renewal is supported.	<ul style="list-style-type: none"> When payment for the peering connection is overdue, the initiator instance stops forwarding data 15 days after the date at which the payment is due, and the instance is automatically released after 15 days of downtime. Reminders are sent on the 8th, 12th, and 14th days after the expiration date and downtime date. After you renew the peering connection, the initiator instance is restored immediately. If the initiator instance is locked for more than 15 days after the date at which the payment is due, it is reclaimed by Alibaba Cloud. The configuration is then cleared and the connection cannot be restored.

Peering connection fee

When you set a peering connection, Alibaba Cloud charges fees for the initiator instance, but does not charge fees for the acceptor instance. The fee depends on the bandwidth of the initiator instance and the distance between the two instances. The fee for interconnected VPCs in the same region is lower than that of VPCs connected across different regions.

- Cross-region interconnections are charged according to the prices displayed on the [purchase page](#). If you have any issues, open a ticket.



Note:

Peering connections that are established between the China (Beijing) region and the China (Zhangjiakou) region with a bandwidth value of 2 Gbit/s or less than 2 Gbit/s are free of charge before December 31, 2020.

- Same-region interconnections are charged according to the price listed in the following table. This fee will not be charged until December 31, 2020.

Table 2-1: Same-region peering connection fee in Mainland China

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

3 Limits


Before you use peering connections, note the following limits.

Item	Quota	Can I apply for an increase to the quota?
The maximum number of peering connections that can be created for a VPC	5	Yes. You can use the quota management function to apply for an increase to the quota.
The maximum number of peering connections that can be created for a Virtual Border Router (VBR)	5	Yes. You can use the quota management function to apply for an increase to the quota.
The maximum number of peering connections that can be created under an account	10	Yes. You can use the quota management function to apply for an increase to the quota.

4 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 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.

5 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.

6 Interconnect two VPCs

You can interconnect two VPCs by creating a peering connection between them.

Context




Note:

If this is the first time that you use Express Connect to interconnect two VPCs, we recommend that you use Cloud Enterprise Network (CEN). For more information, see [Tutorial overview](#).

Procedure

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

Configuration	Description
Account type	<p>Select whether the VPCs you want to connect belong to the same account.</p> <ul style="list-style-type: none">· Same as Peer's: If the VPCs to be connected belong to the same account, the system creates an initiator instance and an acceptor instance at the same time, and automatically establishes a connection between them.· Different from Peer's: If the VPCs to be connected belong to different accounts, you must create an initiator instance and an acceptor instance separately before initiating the connection from the initiator instance.

Configuration	Description
Connection Type	<p>Select the peering connection type.</p> <ul style="list-style-type: none"> · VPC-to-VPC: Establish a peering connection between two VPCs. · VBR-to-VPC: Establish a peering connection between a VPC and a VBR. For more information, see Interconnect a VPC and a VBR. <p>In this example, select VPC-to-VPC.</p>
Routers to Create	<p>Select the instances to be created.</p> <ul style="list-style-type: none"> · Initiator and Acceptor: Both an initiator instance and an acceptor instance are created. After the creation, the initiator instance automatically connects to the acceptor instance. <p>This option applies only to connections under the same account.</p> <ul style="list-style-type: none"> · Create Initiator: An initiator instance is created and the initiator instance can initiate the connection actively. <p>The initiator router type can be VPC or VBR. If VBR-to-VPC is selected for the peering connection type, only VBR is available for the initiator router type.</p> <p>This option applies only to connections between different accounts.</p> <ul style="list-style-type: none"> · Acceptor Only: An acceptor instance is created. <p>Only VPC is available for the acceptor router type.</p> <p>This option applies only to connections between different accounts.</p> <div data-bbox="600 1704 1434 1951" style="background-color: #f0f0f0; padding: 10px;"> <p> Note: Only Pay-As-You-Go billing supports creating an acceptor separately. The acceptor instance is free of charge.</p> </div>
Local VPC ID	Select the ID of the local VPC (the initiator or the acceptor of the connection).

Configuration	Description
Local Region	Select the region of the local VPC.
Peer VPC ID	Select the ID of the peer VPC (the initiator or the acceptor of the connection).
Peer Region	Select the region of the peer VPC.
Bandwidth	Select a bandwidth value for the connection. Use the default bandwidth for the acceptor instance.
Validity	Select a validity period for your subscription. If you want the subscription to automatically renew when it expires, select the Auto Renew check box.

7 Interconnect a VPC and a VBR

You can fulfill intercommunication between a VPC and a Virtual Border Router (VBR) by creating a peering connection.

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. Configure the peering connection.

Configuration	Description
Account Type	<p>Select whether the VPC and the VBR you want to connect belong to the same account.</p> <ul style="list-style-type: none"> · Same as Peer's : If the VPC and VBR to be connected belong to the same account, the system creates an initiator instance and an acceptor instance at the same time, and automatically establishes a connection between them. · Different from Peer's: If the VPC and VBR to be connected belong to different accounts, you need to create an initiator instance and an acceptor instance respectively before initiating the connection from the initiator instance.
Connection Type	<p>Select the peering connection type:</p> <ul style="list-style-type: none"> · VPC-to-VPC: Establish a peering connection between two VPCs. · VBR-to-VPC: Establish a peering connection between a VPC and a VBR. <p>In this example, select VBR-to-VPC.</p>

Configuration	Description
Routers to Create	<p>Select the instances to be created:</p> <ul style="list-style-type: none"> · Initiator and Acceptor: Both an initiator instance and an acceptor instance are created. After the creation, the initiator instance automatically connects to the acceptor instance. This option applies only to connections under the same account. · Initiator Only: The initiator instance is created and the initiator instance can initiate the connection actively. If VBR-to-VPC is selected for the connection type, only VBR is available for the route type of the initiator. This option applies only to connections between different accounts. · Acceptor Only: An acceptor instance is created. Only VPC is available for the acceptor router type. This option applies only to connections between different accounts.
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 VBR to which you want to establish the connection ·
Peer Region	Select the region of the peer VPC.
Peer VPC ID	Select the ID of the peer VPC.
Bandwidth	Select a bandwidth for the connection. Use the default bandwidth for the acceptor instance.
Validity	Select a validity period for your subscription. If you want the subscription to automatically renew when it expires, select Auto Renew.

8 Interconnect two VPCs under the same account

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



Note:

- If this is the first time that you are using Express Connect to interconnect two VPCs, we recommend that you use CEN. For more information, see [Tutorial overview](#).

Example

This topic uses the following two VPCs as an example to show you how to fulfill VPC intercommunication by using Express Connect.

Prerequisites

The CIDR blocks of the VPCs or VSwitches that you want to interconnect do not conflict with each other.

Step 1: Create a peering connection

To create a 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.

In this example, select China (Qingdao).

4. Click Create Peering Connection.

5. Configure the peering connection.

Use the following configurations:

- **Account Type:** Select Same as Peer's.
- **Connection Type:** Select VPC-to-VPC.
- **Routers to Create:** Select Initiator and Acceptor.

The system sets the selected local VPC as the connection initiator, sets the peer VPC as the acceptor, and automatically connects the initiator and the acceptor.

- **Local Region:** Select the region of the local VPC. In this example, select China (Qingdao).
- **Local VPC ID:** Select the local VPC, that is, the initiator of the connection. In this example, select VPC1.
- **Peer Region:** Select the region of the peer VPC. In this example, select China (Beijing).
- **Peer VPC ID:** Select the peer VPC to be connected. In this example, select VPC2.
- **Bandwidth:** Select a bandwidth value for the interconnection. In this example, select 2 Mb.

6. Click Buy Now and complete the payment.

7. Go back to the VPC-to-VPC page to check the created peering connection.

When the initiator and the acceptor are both in the activated state, the connection is established.

Step 2: Configure routes

After establishing the peering connection, you need to add a route for each of the two interconnected VPCs.

To configure the routes, follow these steps:

1. On the VPC-to-VPC page, find the peering connection you created.
2. Click Route Settings under the initiator instance.
3. Click Add Route, enter the destination CIDR block of the VPC or VSwitch that you want to connect, and then click Confirm.

In this example, enter the CIDR block of the peer VPC: 172.16.0.0/16.

4. Click Route Settings under the acceptor instance.
5. Click Add Route, enter the destination CIDR block, that is, the CIDR block of the local VPC or its VSwitch, and then click Confirm.

Step 3: Configure security groups

After establishing the peering connection between the two VPCs, you need to configure security groups to enable the intercommunication of ECS instances in these two VPCs.

This topic uses the ECS instances and security groups in the following table as an example.

Configuration	Account A	Account A
Account ID	AccountID_A	AccountID_A
ECS instance ID	InstanceID_A	InstanceID_B
Security group ID	SecurityGroupID_A	SecurityGroupID_B

You can view the account ID in the [Account Center](#).

To configure the security group rule, follow these steps:

1. Log on to the [ECS console](#).
2. In the left-side navigation pane, choose Networks and Security > Security Groups.
3. Select the region of the instance.
4. Find the target security group and then click Add Rules.
5. On the Security Group Rules page, click Add Security Group Rule.
6. Configure the security group rule, select the protocol type, and enter the port range.



Notice:

For cross-region VPC interconnection, select the CIDR block authorization type and enter the CIDR block of the peer VPC.

If you select the security group authorization type, make sure that the VPCs are in the same region.

In this example, select the CIDR block authorization type.

Step 4: Test the connection

After establishing the peering connection and adding the routes, you can log on to an ECS instance of either VPC and ping the IP address of an ECS instance in the other VPC. If the ping succeeds, the connection between the two VPCs is successful.

9 Interconnect two VPCs under different accounts

This topic describes how to use Express Connect to connect two VPCs under different accounts.



Note:

- If this is the first time you are using Express Connect to interconnect two VPCs, we recommend that you use CEN. For more information, see [Tutorial overview](#).

Example

In cross-account VPC interconnections, you need to create an initiator and an acceptor separately, establish a peering connection, and then configure routes. This topic uses the following two VPCs as an example. VPC1 under account A acts as the initiator and VPC2 under account B acts as the acceptor.

Prerequisites

- You have obtained the Alibaba Cloud account ID of the peer VPC and the VRouter ID of the VPC.
- The Classless Inter-Domain Routing (CIDR) blocks of the VPCs or VSwitches that you want to interconnect do not conflict.

Step 1: Create an initiator

To create an initiator, 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 VPC Peering Connections > VPC-to-VPC.
3. Click Create Peering Connection.

4. Configure the peering connection.

Use the following configurations:

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

Only the initiator can initiate the connection to the acceptor.

- **Local Region:** Select the region of the VPC. In this example, select **China (Qingdao)**.
- **Local VPC ID:** Select the VPC for which the initiator instance is created. In this example, select **VPC1**.
- **Peer Region:** Select the region to which the VPC to be connected belongs. In this example, select **China (Beijing)**.
- **Specification:** Select a bandwidth value for the interconnection. In this example, select **2 Mb**.

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

6. Go back to the **VPC Peering Connections** page to check the created initiator instance.

Step 2: Create an acceptor

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 > VPC-to-VPC**.
3. Click **Create Peering Connection**.
4. Configure the peering connection.

Use the following configurations:

- Select **Pay-As-You-Go** as the billing method.



Note:

Only the Pay-As-You-Go billing method supports creating an acceptor separately. The acceptor instance is free of charge.

- **Account type:** Select Different from Peer's.
 - **Connection Type:** Select VPC-to-VPC.
 - **Routers to Create:** Select Acceptor Only.
 - **Local Region:** Select the region of the VPC. In this example, select China (Beijing).
 - **Local VPC ID:** Select the VPC for which the acceptor instance is created. In this example, select VPC2.
 - **Peer Region:** Select the region to which the VPC to be connected belongs. In this example, select China (Qingdao).
 - **Bandwidth:** The acceptor bandwidth depends on the initiator bandwidth. In this example, select Default.
5. Click Buy Now and complete the payment.
 6. On the VPC Peering Connections page, check the created acceptor instance and note down its ID. In this example, the acceptor instance ID is ri-2zeix2q86uoyisagyz0pn.

Step 3: Add the initiator

After creating an initiator and an acceptor, you must add the initiator for the acceptor

.

To add the initiator for the 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 > VPC-to-VPC.
3. Select the region of the acceptor.

In this example, select China (Beijing).

4. Find the created acceptor instance and click Add Initiator.
5. On the Add Instance page, select Another Account and enter the initiator router interface. In this example, enter ri-m5e33r3n78zyi5573kf85. Click OK.

Step 4: Add the acceptor and establish a peering connection

After you add the initiator and the acceptor, the initiator can actively initiate and establish a peering connection between the two VPCs.

In this example, the connection initiator is VPC1 under account A. To establish a peering connection, 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 VPC Peering Connections > VPC-to-VPC.
3. Select the region of the initiator instance.

In this example, select China (Qingdao).

4. Click Add Acceptor.
5. On the Add Instance page, select Another Account and enter the acceptor router interface. In this example, enter ri-2zeix2q86uoyisagyz0pn. Click OK.
6. Choose > Initiate Connection.

When the connection is established, the initiator and the acceptor enter the activated state.

Step 5: Configure routes

After establishing a peering connection, you need to add a route for each of the two VPCs.

To configure the routes, follow these steps:

1. Log on to the [Express Connect console](#) by using the credentials of account A.
2. On the VPC Peering Connections page, find the created peering connection.
3. Find the initiator instance and click Route Settings.
4. Click Add Route, enter the CIDR block of the VPC or VSwitch to be connected, and click Confirm.

In this example, enter the CIDR block of the peer VPC: 172.16.0.0/16.

5. Log on to the [Express Connect console](#) by using the credentials of account B.

6. Find the acceptor instance and click Route Settings.
7. Click Add Route, enter the destination CIDR block, and then click Confirm.

In this example, enter the CIDR block of the peer VPC: 192.168.0.0/16.

Step 6: Configure security groups

After establishing a peering connection between two VPCs, you need to configure security groups to enable the intercommunication of ECS instances in these two VPCs

This topic uses the ECS instances and security groups in the following table as an example.


Configuration	Account A	Account B
Account ID	AccountID_A	AccountID_B
ECS instance ID	InstanceID_A	InstanceID_B
Security group ID	SecurityGroupID_A	SecurityGroupID_B

You can view the account ID in the [Account Center](#).

To configure the security group rule, follow these steps:

1. Log on to the [ECS console](#).
2. In the left-side navigation pane, choose Networks and Security > Security Groups.
3. Select the region of the instance.
4. Find the target security group and then click Add Rules.
5. On the Security Group Rules page, click Add Security Group Rule.
6. Configure the security group rule, select the protocol type, and enter the port range. Then select the authorization type according to the following information.

Scenario	Authorization type	Description
Cross-region VPC interconnection	CIDR block	The CIDR block of the peer VPC.

Scenario	Authorization type	Description
Same-region VPC interconnection	Security group	<p>The ID of the security group associated with the peer ECS instance.</p> <div style="background-color: #f0f0f0; padding: 5px;">  Note: If the VPCs to be interconnected belong to different accounts, select Allow Other Accounts and in the Account ID field, enter the peer account ID. </div>

**Notice:**

- If the VPCs to be interconnected are in different regions, select the CIDR block authorization type and enter the CIDR block of the peer VPC. In this example, select the CIDR block authorization type.
- If the VPCs to be interconnected belong to the same region, select the security group authorization type. In cross-account interconnection, select Allow Other Accounts and in the Account ID field, enter the peer account ID.

Step 7: Test the connection

After establishing the peering connection and adding routes, you can log on to an ECS instance of either VPC and ping the IP address of an ECS instance in the other VPC. If the ping succeeds, the connection between the two VPCs is successful.

10 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. For more information, see [Connect an on-premises data center to a VPC through a physical connection](#).

Step 1: Create an initiator

To create an initiator, 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 VPC Peering Connections > VBR-to-VPC and then click Create Peering Connection.
3. Configure the peering connection.

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

- **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.

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

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.

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

- **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.

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.
 - a. **Account:** Select Another Account.
 - b. **Initiator Router Interface:** Enter the router interface ID of the created initiator, for example, ri-1234567.
 - c. 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.
 - a. Account: Select Another Account.
 - b. Acceptor Router Interface: Enter the ID of the created acceptor router interface, for example, ri-1234567.
 - c. 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.

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:
 - a. Destination Subnet: the CIDR block of the on-premises data center. In this topic, enter 172.16.0.0/12.
 - b. Next Hop Type: Select Physical Connection Interface.
 - c. Next hop: Select the created physical connection.
 - d. 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.
 - a. Destination Subnet: Enter the IP address range of VPC-B. In this topic, enter 192.168.0.0/16.
 - b. Next Hop Type: Select VPC.
 - c. Next Hop: Select the VPC to be connected. In this topic, select VPC-B.
 - d. 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:

- a. Log on to the [Express Connect console](#) by using the credentials of account B.
- b. In the left-side navigation pane, choose VPC Peering Connections > VBR-to-VPC.
- c. Select the peer connection region, find the acceptor, and then click Route Settings.
- d. 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 VPC-B is connected to the on-premises data center, test the speed of the physical connection to ensure that your service needs are met. For more information, see [Method for testing the network performance of a physical connection](#).