ALIBABA CLOUD

Alibaba Cloud

Express Connect

Best Practices

Document Version: 20220615

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Test the performance of an Express Connect circuit ---- 05
2.Create connections over Express Connect circuits to access reso... ---- 13
3.Establish active/active connections between a data center and... ---- 16
4.Establish active/standby connections between a data center an... ---- 20
5.Create active/standby connections and configure BGP routing ---- 26
6.Configure ECMP between a data center and Alibaba Cloud ---- 33
7.Connect to an ECS instance from a data center by using an Ex... ---- 39
8.Configure BGP and BFD to accelerate route convergence ---- 44
9.Enable and disable a VBR to test the connectivity of a second... ---- 47

1.Test the performance of an Express Connect circuit

After an Express Connect circuit is deployed, you must test its network performance to ensure that the Express Connect circuit can meet your business requirements. This topic describes how to test the performance of an Express Connect circuit by using Netperf and iPerf3.

Prerequisites

- An Express Connect circuit is deployed and configured. Your data center is connected to Alibaba Cloud through the Express Connect circuit.
- An on-premises device is prepared to serve as the client or server in the Netperf or iPerf3 test.

  In this example, the IP address of the on-premises device is 192.168.100.1.
- Eight Elastic Compute Service (ECS) instances that are deployed in virtual private clouds (VPCs) are created. The ECS instances serve as clients or servers in the Netperf or iPerf3 test. The ECS instances are connected to the on-premises device to transmit configuration information and test results.

  In this example, the ECS instances use the ecs.se1.2xlarge type. The image is centos_7_2_64_40G_base_20170222.vhd and the IP address range is 172.16.0.2 to 172.16.0.9.

Set up the test environment

To install Netperf and iPerf3 on the on-premises device and ECS instances, perform the following operations:

> **Note** The following operations describe how to install Netperf and iPerf3 on an ECS instance.

1.
2. Install Netperf.
   i. Run the following command to download the Netperf installation package:

   ```
   wget -c "https://codeload.github.com/HewlettPackard/netperf/tar.gz/netperf-2.5.0" -O netperf-2.5.0.tar.gz
   ```

   ii. Run the following commands in sequence to install Netperf.

   ```
   tar -zxvf netperf-2.5.0.tar.gz
   cd netperf-netperf-2.5.0
   ./configure
   make
   make install
   ```

   iii. Run `netperf -V` or `netserver -V` to check whether Netperf is installed.

   If the system returns the following information, it indicates that Netperf is installed.

   ```
   Netperf version 2.5.0
   ```
3. Install iPerf3.

i. Run the following commands to download iPerf3.

```
yum install git -y
git clone https://github.com/esnet/iperf
```

ii. Run the following commands to install iPerf3.

```
cd iperf
./configure && make && make install && cd ..
cd src
ADD_PATH="$(pwd)"
PATH="${ADD_PATH}:${PATH}"
export PATH
```

iii. Run the `iperf3 -v` command to check whether iPerf3 is installed.

If the system returns the following information, it indicates that Netperf is installed.

```
iperf 3.10.1+ (cJSON 1.7.13)
Linux iZbp15y0zrhx2ry6vo1b4wZ 3.10.0-957.21.3.el7.x86_64 #1 SMP Tue Jun 18 16:35:19
UTC 2019 x86_64
```

Assume that the interface eth0 is connected to the Express Connect circuit. Run the `ethtool -L eth0 combined 4` command on the on-premises device to enable the multi-queue feature.

In this example, the following information is returned.

```
echo "ff" > /sys/class/net/eth0/queues/rx-0/rps_cpus
echo "ff" > /sys/class/net/eth0/queues/rx-1/rps_cpus
echo "ff" > /sys/class/net/eth0/queues/rx-2/rps_cpus
echo "ff" > /sys/class/net/eth0/queues/rx-3/rps_cpus
```

Install Netperf and iPerf3

Enable the multi-queue feature

Use Netperf to test the packet forwarding performance of the Express Connect circuit.

After Netperf is installed, two command line interface (CLI) tools are created: netserver (server) and netperf (client). The following table describes the main parameters.

Tool	Main parameter	Parameter description
netserver	-p	The port number of the listener.
	-H	The IP address of the on-premises device or ECS instance.
	-p	The port of the on-premises device or ECS instance.
	-l	The duration for which the tool runs.

Tool	Main parameter	Parameter description
netperf	-t	The protocol used to send packets. Valid values: TCP_STREAM and UDP_STREAM. We recommend that you use UDP_STREAM.
	-m	The size of the packets. • We recommend that you set the value to 1 when you test packets per second (PPS). • We recommend that you set the value to 1400 when you test bits per second (BPS).

1. Run the following commands to start the netserver process on the on-premises device and specify different ports.

```
netserver -p 11256
netserver -p 11257
netserver -p 11258
netserver -p 11259
netserver -p 11260
netserver -p 11261
netserver -p 11262
netserver -p 11263
```

2. Run the `netperf -H server_ip -p port 6 -t UDP_STREAM -l 300 -- -m 1` command on the eight ECS instances to start the netperf process and specify the ports of netserver as ports of the ECS instances.
   - Run the following commands to test PPS:

```
netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The first ECS instanc
e
netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1 #The second ECS instan
ce
netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1 #The third ECS instanc
e
netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1 #The fourth ECS instan
ce
netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1 #The fifth ECS instanc
e
netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1 #The sixth ECS instanc
e
netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1 #The seventh ECS insta
nce
netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1 #The eighth ECS instan
ce
```

   - Run the following commands to test BPS:

```
netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1400 #The first ECS instance
netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1400 #The second ECS instance
netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1400 #The third ECS instance
netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1400 #The fourth ECS instance
netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1400 #The fifth ECS instance
netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1400 #The sixth ECS instance
netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1400 #The seventh ECS instance
netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1400 #The eighth ECS instance
```

1. Run the `netserver -p 11256` command on the ECS instances to start the netserver process and specify ports.
2. Run the `netperf -H ECS_ip -p port -t UDP_STREAM -l 300 -- -m 1` command on the on-premises device to start eight netperf processes and specify different IP addresses for the ECS instances.
   - Run the following commands to test PPS:

     ```
     netperf -H 172.16.0.2 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The first ECS instance
     netperf -H 172.16.0.3 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The second ECS instance
     netperf -H 172.16.0.4 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The third ECS instance
     netperf -H 172.16.0.5 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The fourth ECS instance
     netperf -H 172.16.0.6 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The fifth ECS instance
     netperf -H 172.16.0.7 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The sixth ECS instance
     netperf -H 172.16.0.8 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The seventh ECS instance
     netperf -H 172.16.0.9 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #The eighth ECS instance
     ```

   - Run the following commands to test BPS:

     ```
     netperf -H 172.16.0.2 -p 11256 -t UDP_STREAM -l 300 -- -m 1400 #The first ECS instance
     netperf -H 172.16.0.3 -p 11257 -t UDP_STREAM -l 300 -- -m 1400 #The second ECS instance
     netperf -H 172.16.0.4 -p 11258 -t UDP_STREAM -l 300 -- -m 1400 #The third ECS instance
     netperf -H 172.16.0.5 -p 11259 -t UDP_STREAM -l 300 -- -m 1400 #The fourth ECS instance
     netperf -H 172.16.0.6 -p 11260 -t UDP_STREAM -l 300 -- -m 1400 #The fifth ECS instance
     netperf -H 172.16.0.7 -p 11261 -t UDP_STREAM -l 300 -- -m 1400 #The sixth ECS instance
     netperf -H 172.16.0.8 -p 11262 -t UDP_STREAM -l 300 -- -m 1400 #The seventh ECS instance
     netperf -H 172.16.0.9 -p 11263 -t UDP_STREAM -l 300 -- -m 1400 #The eighth ECS instance
     ```

The following result is displayed when netperf processes are complete on the client side. You can use the following formula to calculate the PPS: PPS = Number of packets that are sent/Duration of the test.

```
Socket  Message  Elapsed      Messages
Size    Size     Time         Okay Errors   Throughput
bytes   bytes    secs            #      #   10^6bits/sec
124928       1   10.00     4532554      0       3.63
212992           10.00     1099999              0.88
```

The following table describes the fields in the test result.

Field	Description
Socket Size	The buffer size.
Message Size	The packet size. Unit: bytes.
Elapsed Time	The duration of the test. Unit: seconds.
Message Okay	The number of packets that are sent.
Message Errors	The number of packets that fail to be sent.
Throughput	The network throughput. Unit: Mbit/s.

Overview of Netperf

Test the packet forwarding performance of the on-premises device as a server

Test the packet forwarding performance of the on-premises device as a client

Analyze the test result

Use iPerf3 to test the bandwidth of the Express Connect circuit

The following table describes the main parameters of iPerf3.

Main parameter	Parameter description
-s	Applies to only the server, which specifies that iPerf3 runs in server mode.
-c	Applies to only the client, which specifies that iPerf3 runs in client mode.
-i	Specifies the interval between two reports. Unit: seconds.

Main parameter	Parameter description
-p	• Specifies the port of the server listener. By default, the port number is 5201 and TCP and UDP are used. • Specifies the port of the client. By default, the port number is 5201. If the -u parameter is also set, it indicates that UDP is used to initiate connections. Otherwise, TCP is used.
-u	Uses UDP to send packets. If this parameter is not set, TCP is used.
-l	Specifies the length of the read/write buffer. We recommend that you set the value to 16 when you test the packet forwarding performance. When you test the bandwidth, we recommend that you set the value to 1400.
-b	Specifies the bandwidth used in UDP mode. Unit: bit/s.
-t	Specifies the duration of transmission. iPerf3 repeatedly sends packets of the specified length in the specified duration. The default duration is 10 seconds.
-A	The CPU affinity. You can associate an iPerf3 process with the logical CPU of the corresponding number to avoid cross-CPU scheduling of the iPerf3 process.

1. Run the following commands on the on-premises device to start the iPerf3 process in server mode and specify different ports.

```
iperf3 -s -i 1 -p 16001
iperf3 -s -i 1 -p 16002
iperf3 -s -i 1 -p 16003
iperf3 -s -i 1 -p 16004
iperf3 -s -i 1 -p 16005
iperf3 -s -i 1 -p 16006
iperf3 -s -i 1 -p 16007
iperf3 -s -i 1 -p 16008
```

2. Run the `iperf3 -u -l 16 -b 100m -t 120 -c server_ip -i 1 -p port -A 1` command on the ECS instances to start the iPerf3 process in client mode and specify the ports of the on-premises device as the ports of the ECS instances.

   Run the following commands:

```
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16001 -A 1 #The first ECS instance
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16002 -A 2 #The second ECS instance
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16003 -A 3 #The third ECS instance
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16004 -A 4 #The fourth ECS instance
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16005 -A 5 #The fifth ECS instance
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16006 -A 6 #The sixth ECS instance
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16007 -A 7 #The seventh ECS instance
 iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16008 -A 8 #The eighth ECS instance
```

1. Run the `iperf3 -s -i 1 -p 16001` command on the ECS instances to start the iPerf3 process in server mode and specify ports.
2. Run the following commands on the on-premises device to start eight iPerf3 processes in client mode.

```
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.2 -i 1 -p 16001 -A 1
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.3 -i 1 -p 16001 -A 2
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.4 -i 1 -p 16001 -A 3
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.5 -i 1 -p 16001 -A 4
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.6 -i 1 -p 16001 -A 5
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.7 -i 1 -p 16001 -A 6
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.8 -i 1 -p 16001 -A 7
iperf3 -u -l 16 -b 100m -t 120 -c 172.16.0.9 -i 1 -p 16001 -A 8
```

The following result is displayed when iPerf3 processes are complete on the client side. You can use the following formula to calculate the PPS: PPS = Number of packets that are received by the peer/Duration of the test.

```
[ ID]  Interval        Transfer    Bandwidth      Jitter    Lost/Total Datagrams
[  4]  0.00-10.00 sec  237 MBytes  199 Mbits/sec  0.027 ms  500/30352 (1.6%)
[  4]  Sent 30352  datagrams
```

Note We recommend that you run the `sar` command on the server side to count the packets that are actually received. Example: `sar -n DEV 1 320` .

The following table describes the fields in the test result.

Field	Description
Transfer	The total amount of data that is transmitted.
Bandwidth	The bandwidth.
Jitter	The network jitter.

Field	Description
Lost/Total Datagrams	The packet loss rate, which is calculated by the following formula: Packet loss rate = Number of dropped packets/Total number of packets.

Overview of iPerf3

Test the bandwidth of the on-premises device as a server

Test the bandwidth of the on-premises device as a client

Analyze the test result

2.Create connections over Express Connect circuits to access resources on Alibaba Cloud

This topic describes how to use Express Connect circuits to create high-quality, reliable, and private connections between a data center and virtual private clouds (VPCs) in different regions.

Description

You can use the following features of Express Connect to create a private connection between a data center and a VPC on Alibaba Cloud.

- Express Connect circuits

  Connect to Alibaba Cloud through the nearest access point by using an Express Connect circuit. For more information, see Physical connection solutions.

- Peering connections

  Create a router interface to connect a virtual border router (VBR) and a VPC. This way, the data center and the VPC can communicate with each other through a private connection. For more information, see What is a peering connection.

Connect to Alibaba Cloud through the nearest access point

Before you use an Express Connect circuit to connect to Alibaba Cloud, you must choose an access point. Express Connect provides access points in different regions on a global scale. You can choose an access point of Alibaba Cloud or an Express Connect partner.

- Alibaba Cloud access points

  You can view information about the access points of Alibaba Cloud on the Apply for an Express Connect page. For more information about the access point locations, see Locations of access points.

- Access points of Express Connect partners

  The access points of Express Connect partners are already connected to Alibaba Cloud through Express Connect circuits. You need only to connect your data center to an access point of an Express Connect partner. For more information about the access points of Express Connect partners, see Express Connect partners.

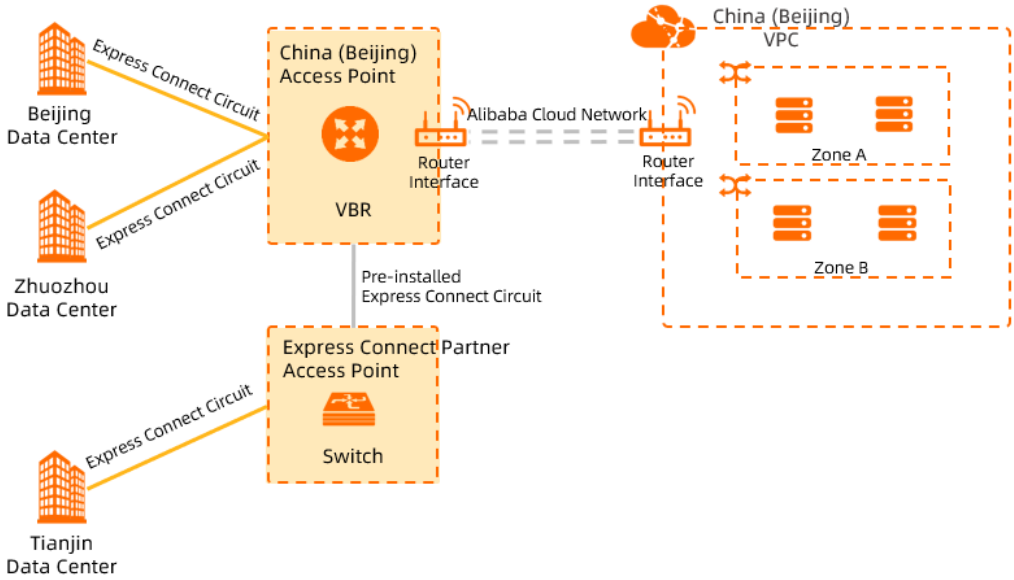
Choose an access point based on the location of your data center:

- Choose an access point in the city where your data center is located.
- If no access point is deployed in the city where your data center is located, choose one that is nearest to your data center.

  For example, a company has a data center in Beijing, a data center in Tianjin, and a data center in Zhuozhou, the company can choose access points based on the following rules:

  - Alibaba Cloud provides access points in the China (Beijing) region. To connect the data center in Beijing to Alibaba Cloud through an Express Connect circuit, the company can choose an access point in the China (Beijing) region.

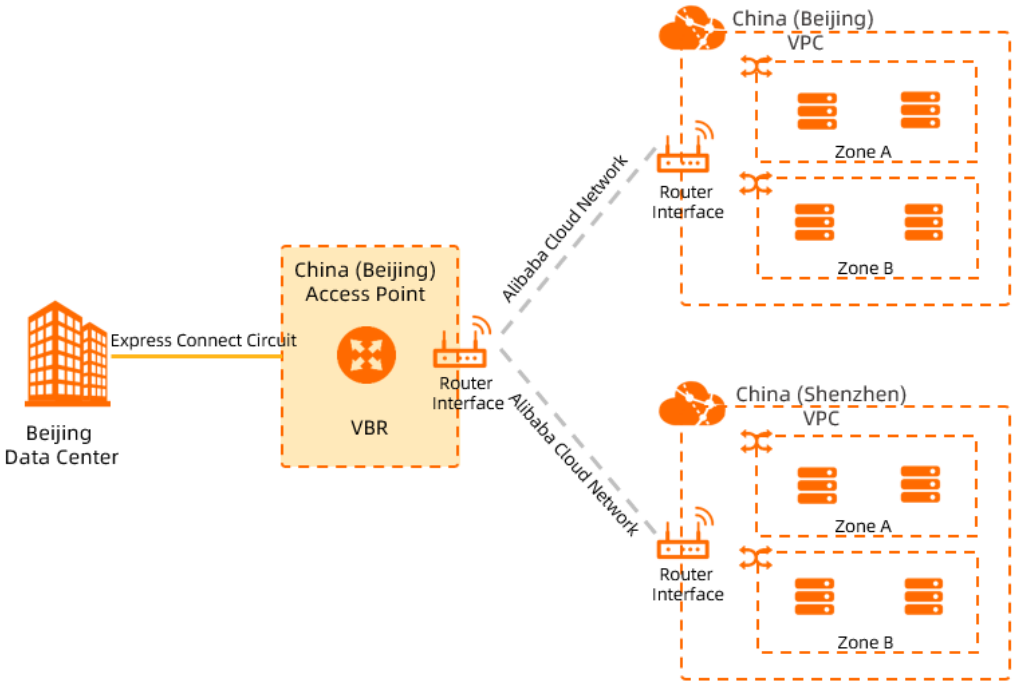
- Alibaba Cloud does not provide access points in the China (Tianjin) region. However, Express Connect partners provide access points in Tianjin. To connect the data center in Tianjin to Alibaba Cloud through an Express Connect circuit, the company can choose an access point provided by an Express Connect partner.
- Neither Alibaba Cloud nor Express Connect partners provide access points in Zhuozhou. In this case, the company can choose an access point in the China (Beijing) region, which is the nearest access point to Zhuozhou.



Enable communication between a data center and services on Alibaba Cloud

After you connect a data center to Alibaba Cloud through an Express Connect circuit, you can create peering connections to VPCs deployed in different regions. This way, the data center and the VPCs can communicate with each other.

For example, a company wants its data center in Beijing to communicate with a VPC in the China (Shenzhen) region and a VPC in the China (Beijing) region, the company must perform the following operations: Connect the data center to Alibaba Cloud through an Express Connect circuit. Then, create two router interfaces for the VBR that is associated with the Express Connect circuit. The router interfaces are used to enable communication between the VBR and the VPC. For more information, see Create and manage a VBR-to-VPC connection.


China (Beijing)
VPC
Zone A
Zone B
Router Interface
Alibaba Cloud Network
China (Beijing) Access Point
Express Connect Circuit
Router Interface
VBR
Beijing Data Center
Alibaba Cloud Network
China (Shenzhen)
VPC
Zone A
Zone B
Router Interface

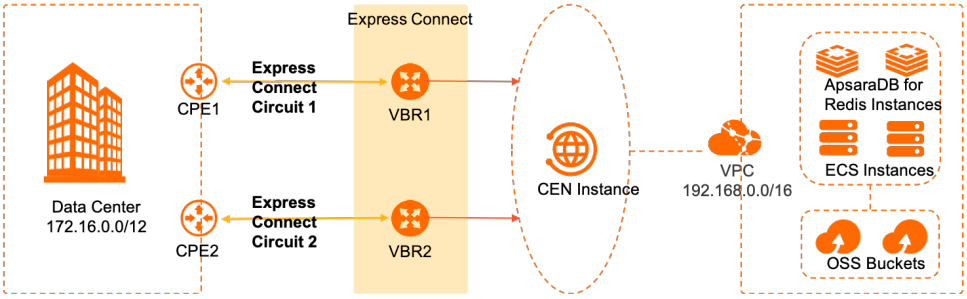
3.Establish active/active connections between a data center and Alibaba Cloud

This topic describes how to use two Express Connect circuits to establish active/active connections between a data center and Alibaba Cloud. If your data center is connected to Alibaba Cloud through two Express Connect circuits, network traffic is distributed across both connections by default. If one of the Express Connect circuits is down, the other Express Connect circuit takes over to serve your workloads. This ensures service availability.

Scenario

The following scenario is used as an example to show how to use two Express Connect circuits to establish active/active connections.

A company has a data center in Shanghai and a virtual private cloud (VPC) in the China (Shanghai) region. The private CIDR block of the data center is 172.16.0.0/12, and the CIDR block of the VPC is 192.168.0.0/16. To prevent single points of failure (SPOFs), the company plans to lease two Express Connect circuits from different connectivity providers to configure active-active failover.



The following table describes the configurations of the virtual border routers (VBRs) connected to the Express Connect circuits.

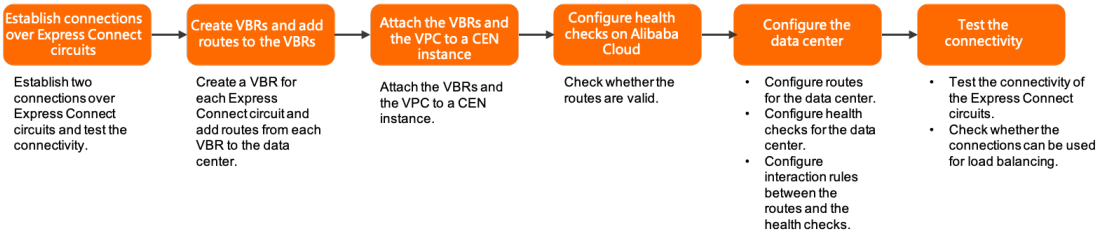
Configuration item	VBR1 (connected to Express Connect circuit 1)	VBR2 (connected to Express Connect circuit 2)
VLAN ID	0	0
Peer IPv4 Address of Gateway at Alibaba Cloud Side	10.0.0.1	10.0.0.5
Peer IPv4 Address of Gateway at Customer Side	10.0.0.2	10.0.0.6
Subnet Mask (IPv4 Address)	255.255.255.252	255.255.255.252

Prerequisites

- A VPC is created in the China (Shanghai) region and cloud resources such as Elastic Compute Service (ECS) instances that host your business systems are deployed in the VPC.

-

Procedure



Step 1: Create two connections over Express Connect circuits

In this example, two dedicated connections are created. For more information, see Create a dedicated connection over an Express Connect circuit.

When you apply for the second Express Connect circuit, you may need to specify a redundant Express Connect circuit based on the access point.

- If you want to connect the Express Connect circuits to the same access point, you must specify the redundant Express Connect circuit. Set **Redundant Connection ID** to the first Express Connect circuit. This way, the Express Connect circuits will be connected to different access devices.
- If you want to connect the Express Connect circuits to different access points, you do not need to specify the redundant Express Connect circuit. In this case, you do not need to specify **Redundant Connection ID**.

  In this example, the Express Connect circuits are connected to different access points.

Step 2: Create VBRs and configure routing

You must create a VBR for each Express Connect circuit and add a route to each VBR. Set the destination of both routes to the data center.

1.
2. Create a VBR for Express Connect Circuit 1.
   i.
   ii.
   iii. In the **Create VBR** panel, set the following parameters and click **OK**:
      - **Account**: Specify the type of account for which you want to create the VBR. In this example, **Current Account** is selected.
      - **Name**: Enter a name for the VBR. In this example, **VBR1** is entered.
      - **Physical Connection Interface**: In this example, **Dedicated Physical Connection** is selected and then Express Connect Circuit 1 is selected.
      - **VLAN ID**: Enter the VLAN ID of the VBR. In this example, **0** is entered.
      - **Peer IPv4 Address of Gateway at Alibaba Cloud Side**: Specify an IPv4 address for the VBR. In this example, **10.0.0.1** is entered.
      - **Peer IPv4 Address of Gateway at Customer Side**: Specify an IPv4 address for the gateway device in the data center. In this example, **10.0.0.2** is entered.
      - **Subnet Mask (IPv4 Address)**: Enter the IPv4 subnet mask of the specified IP addresses. In this example, **255.255.255.252** is entered.

3. Add a route whose destination is the data center to VBR1.
   i.
   ii. On the **Virtual Border Routers (VBRs)** page, click the ID of VBR1.
   iii. On the details page of VBR1, click the **Routes** tab and click **Add Route**.
   iv. In the **Add Route Entry** panel, set the following parameters and click **OK**:
      - **Next Hop Type**: In this example, **Physical Connection Interface** is selected.
      - **Destination Subnet**: Enter the CIDR block of the data center. In this example, **172.16.0.0/12** is entered.
      - **Next Hop**: Select an Express Connect circuit. In this example, Express Connect Circuit 1 is selected.
4. Repeat the preceding steps to create VBR2 for Express Connect Circuit 2 and add a route to VBR2. Set the destination of the route to the data center.

Step 3: Attach the VBR and VPC to a CEN instance

To enable communication between the data center and the VPC, you must attach the VBRs and the VPC to a Cloud Enterprise Network (CEN) instance.

Step 4: Configure health checks on Alibaba Cloud

By default, after you configure health checks, Alibaba Cloud sends a probe packet every 2 seconds over the Express Connect circuits from the source IP address to the destination IP address in the data center. If no responses are returned for eight consecutive probe packets over one of the Express Connect circuits, the other Express Connect circuit takes over.

Step 5: Configure routes and health checks in the data center

You must configure routes and health checks in the data center, and then configure the gateway device to route network traffic based on health check results to achieve network redundancy.

1. Configure routes in the data center.

   The configuration may vary based on the gateway device. For more information about the configuration commands, consult the vendor of your gateway device.

   ```
   #Configure routes in the data center to route network traffic to the VPC.
   ip route 192.168.0.0 255.255.0.0 10.0.0.1
   ip route 192.168.0.0 255.255.0.0 10.0.0.5
   #Configure routes to return probe packets.
   ip route <The source IP address for health checks> 255.255.255.255 10.0.0.1
   ip route <The source IP address for health checks> 255.255.255.255 10.0.0.5
   ```

2. Configure health checks in the data center.

   You can configure Bidirectional Forwarding Detection (BFD) or Network Quality Analyzer (NQA) on the gateway device in the data center to monitor the reachability of routes destined for the VBRs. For more information about the configuration commands, consult the vendor of your gateway device.

3. Configure the gateway device to route network traffic based on health check results.

   The configuration may vary based on the network environment. For more information about the configuration commands, consult the vendor of your gateway device.

Step 6: Test the connectivity

After you complete the preceding configurations, you must test the connectivity of the Express Connect circuits.

1. Open the command-line interface (CLI) on a computer in the data center.
2. Run the **ping** command to test the connectivity between the data center and an ECS instance in the VPC. The CIDR block of the VPC is 192.168.0.0/16.

   If echo reply packets are returned, it indicates that the destination is reachable.
3. To check whether active/active connections are established between the data center and Alibaba Cloud, run the **tracert** command to query the routes through which packets are sent.

References

- For more information about how to troubleshoot connectivity issues between a data center and an ECS instance, see Troubleshooting.
- For more information about Express Connect circuit installation FAQ, see FAQ about physical connection construction.
- For more information about how to resolve issues in Express Connect circuit connections, see Express Connect circuits.

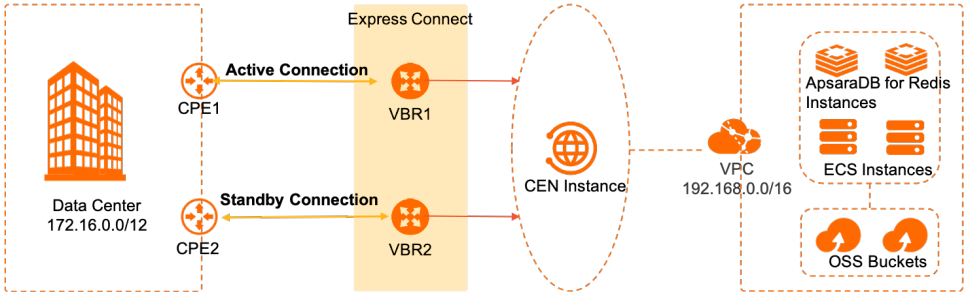
4.Establish active/standby connections between a data center and Alibaba Cloud

This topic describes how to establish active/standby connections between a data center and Alibaba Cloud by using two Express Connect circuits. If the primary Express Connect circuit is up, data is transmitted only through the primary Express Connect circuit. To ensure service availability, you can configure health checks to monitor the status of your Express Connect circuits. Probe packets are sent at the specified health check internal. If the primary Express Connect circuit is down, the secondary Express Connect circuit takes over.

Scenarios

The following example shows how to establish active/standby connections between a data center and Alibaba Cloud by using two Express Connect circuits.

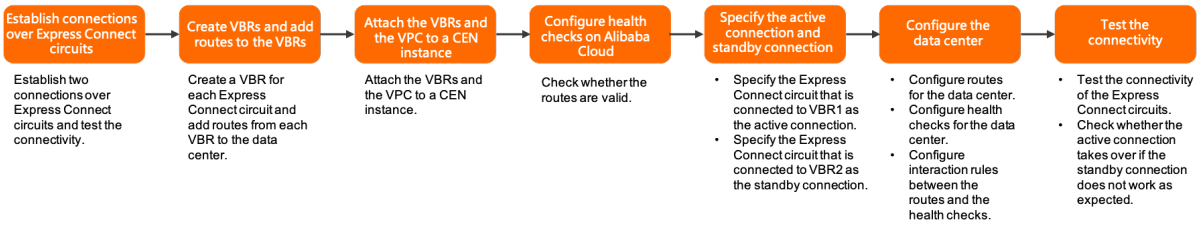
A company has a data center in Shanghai and a virtual private cloud (VPC) in the China (Shanghai) region. The private CIDR block of the data center is 172.16.0.0/12, and the CIDR block of the VPC is 192.168.0.0/16. To prevent single points of failure (SPOFs), the company plans to lease two Express Connect circuits from different connectivity providers to establish active/standby connections between the data center and Alibaba Cloud.



The following table describes the configurations of the virtual border routers (VBRs) connected to the Express Connect circuits.

Configuration item	VBR1 (connected to the primary Express Connect circuit)	VBR2 (connected to the secondary Express Connect circuit)
VLAN ID	0	0
Peer IPv4 Address of Gateway at Alibaba Cloud Side	10.0.0.1	10.0.0.5
Peer IPv4 Address of Gateway at Customer Side	10.0.0.2	10.0.0.6
Subnet Mask (IPv4 Address)	255.255.255.252	255.255.255.252

Procedure



Step 1: Create two connections over Express Connect circuits

Express Connect supports dedicated connections and hosted connections.

- Dedicated connection: If you want to create two dedicated connections, you must apply for two Express Connect circuits in the console. For more information, see Create a dedicated connection over an Express Connect circuit.

  When you apply for the second Express Connect circuit in the console, you may need to specify a redundant Express Connect circuit based on the access point.

  - If you want to connect the Express Connect circuits to the same access point, you must specify the redundant Express Connect circuit. Set **Redundant Connection ID** to the first Express Connect circuit that you applied. Make sure that the initial installation fee for the first Express Connect circuit is paid. Then, the Express Connect circuits will be connected to different access devices.
  - If you want to connect the Express Connect circuits to different access points, you do not need to specify the redundant Express Connect circuit. Therefore, you can leave the **Redundant Connection ID** parameter empty.

- Hosted connection: Contact two Express Connect partners and request them to create two hosted connections for you. For more information, see Overview.

Step 2: Create VBRs and configure routing

You must create a VBR for each Express Connect circuit and add a route to each VBR. Set the destination of both routes to the data center.

1.
2. Create a VBR for the first Express Connect circuit.
   i.
   ii.

iii. In the **Create VBR** panel, set the following parameters and click **OK**:

- **Account**: Specify the type of account for which you want to create the VBR. In this example, **Current Account** is selected.
- **Name**: Enter a name for the VBR. In this example, **VBR1** is entered.
- **Physical Connection Interface**: Select the Express Connect circuit that you want to associate with the VBR. The Express Connect circuit must be enabled and work as expected. In this example, the first Express Connect circuit is selected.
- **VLAN ID**: Enter the VLAN ID of the VBR. In this example, **0** is entered.
- **Peer IPv4 Address of Gateway at Alibaba Cloud Side**: Specify an IPv4 address for the VBR. In this example, **10.0.0.1** is entered.
- **Peer IPv4 Address of Gateway at Customer Side**: Specify an IPv4 address for the gateway device in the data center. In this example, **10.0.0.2** is entered.
- **Subnet Mask (IPv4 Address)**: Enter the IPv4 subnet mask of the specified IP addresses. In this example, **255.255.255.252** is entered.

3. Add a route whose destination is the data center to VBR1.
   i.
   ii. On the **Virtual Border Routers (VBRs)** page, click the ID of VBR1.
   iii. On the details page of VBR1, click the **Routes** tab and click **Add Route**.
   iv. On the **Add Route** page, set the following parameters and click **OK**:
   - **Next Hop Type**: In this example, **Physical Connection Interface** is selected.
   - **Destination Subnet**: Enter the CIDR block of the data center. In this example, **172.16.0.0/12** is entered.
   - **Next Hop**: Select an Express Connect circuit. In this example, the first Express Connect circuit is selected.
4. Repeat the preceding steps to create VBR2 for the second Express Connect circuit and add a route whose destination is the data center to VBR2.

Step 3: Attach the VBRs and VPC to a CEN instance

To enable communication between the VBRs and the VPC, you must attach the VBRs and the VPC to a Cloud Enterprise Network (CEN) instance.

1.
2. On the **Instances** page, click the ID of the CEN instance that you want to manage.

   If you do not have a CEN instance, create one. For more information, see .
3. Click the **Networks** tab and then click **Attach Network**.
4. In the **Attach Network** panel, click the **Your Account** tab to attach VBR1 and then click **OK**.
   - **Network Type**: Select the type of network instance that you want to attach. In this example, **Virtual Border Router (VBR)** is selected.
   - **Region**: Select the region where VBR1 is deployed.
   - **Networks**: Select the ID of VBR1.
5. Repeat the preceding steps to attach VBR2 and the VPC to the CEN instance.

> **Notice** If you have created routes that point to ECS instances, VPN gateways, or high-availability IP addresses (HAVIPs) in the VPC, you must advertise these routes to the CEN instance in the VPC console. For more information, see .

Step 4: Configure health checks on Alibaba Cloud

By default, after you configure health checks, Alibaba Cloud sends a probe packet every 2 seconds over the Express Connect circuits from the specified source IP address to the destination IP address in the data center. If no responses are returned for eight consecutive probe packets over one of the Express Connect circuits, the other Express Connect circuit takes over.

1.
2. In the left-side navigation pane, click **Health Check**.
3. Select the region where VBR1 is deployed and click **Set Health Check**.

   In this example, **China (Shanghai)** is selected.
4. On the **Set Health Check** page, set the parameters of the health check and click **OK**.

5. Repeat the preceding steps to configure health checks for VBR2.

Step 5: Specify the primary and secondary Express Connect circuits

To specify the primary and secondary Express Connect circuits, you must configure routing policies in CEN. In this example, the primary Express Connect circuit is connected to VBR1. The secondary Express Connect circuit is connected to VBR2.

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

Parameter	Description
Routing Policy Priority	Set a priority for the routing policy. A smaller value indicates a higher priority. You cannot specify the same priority for routing policies that apply in the same region and direction. The system evaluates routes against the match conditions of routing policies in descending order of priority. A smaller value indicates a higher priority. You must set the priorities to proper values. In this example, **20** is entered.
Description	Enter a description for the routing policies.
Region	Select the region in which the routing policy applies. In this example, **China (Shanghai)** is selected.

Parameter	Description
Direction	Select the direction in which the routing policy applies. ○ Import to Regional Gateway: If you select this option, the routing policy applies to routes that are advertised to the regional gateway. For example, routes are advertised to a regional gateway from a network instance in the same region, or from a network instance in a different region. ○ Export from Regional Gateway: If you select this option, the routing policy applies to routes that are advertised from the regional gateway. For example, routes are advertised from a regional gateway to a network instance in the same region or to a regional gateway in a different region. In this example, **Import to Regional Gateway** is selected.
Match Conditions	Select a match condition for the routing policy. In this example, **Source Instance IDs** is selected and VBR1 is selected. This way, the routing policy applies to all routes of VBR1. **Note** Click **+ Add Match Condition** to add more match conditions.
Routing Policy Action	Select **Permit** for **Action Policy** and set a priority for the routing policy. Preference: Click **Add Policy Entry**, select **Preference**, and then set a priority for routes that match the conditions. A lower value indicates a higher priority. In this example, **Preference** is set to **10**. **Note** In this example, Associated Priority is not set for VBR1.

6. Repeat the preceding steps to specify the Express Connect circuit that is associated with VBR2 as the secondary Express Connect circuit.
   - **Route Map Priority**: A lower value indicates a higher priority. The priority value of the routing policy for VBR2 must be greater than that of the routing policy for VBR1. In this example, **30** is entered.
   - **Match Conditions**: In this example, **Source Instance IDs** is selected and VBR2 is selected. This way, the routing policy applies to all routes of VBR2.
   - **Action Policy**: Select **Permit** for **Action Policy**, and set a priority for the routing policy.
     - A lower value indicates a higher priority. The priority of the routing policy for VBR1 must be higher than the priority of the routing policy for VBR2. In this example, **Preference** is set to **20**.
     - In this example, Associated Priority is not set for VBR2.

   After you create the routing policies, you can view two 172.16.0.0/12 routes on the **Routes** tab, which are destined for the data center. One of the routes is the secondary route.

Step 6: Configure health checks in the data center

You must configure routes and health checks in the data center, and then configure the gateway device to route network traffic based on health check results to achieve connection redundancy.

1. Configure routes in the data center.

   The following example is only for reference. Route configurations may vary based on the gateway device.

   ```
   ip route 192.168.0.0 255.255.0.0 10.0.0.1 preference 10
   ip route 192.168.0.0 255.255.0.0 10.0.0.5 preference 20
   ```

2. Configure health checks in the data center.

   You can configure Bidirectional Forwarding Detection (BFD) or Network Quality Analyzer (NQA) on the gateway device in the data center to monitor the reachability of routes destined for the VBRs. For more information about the configuration commands, consult the vendor of your gateway device. BFD can detect a link failure within milliseconds. Therefore, we recommend that you configure BFD on your gateway device.

3. Configure the gateway device to route network traffic based on health check results.

   Configurations may vary based on the gateway device. For more information, consult the vendor of your gateway device.

Step 7: Test network connectivity

You must verify the connectivity of both Express Connect circuits to ensure that your service is not interrupted when one of the Express Connect circuits is down.

1. Open the command-line interface on a computer in the data center.
2. Run the **ping** command to verify the connectivity between the data center and an ECS instance in the VPC whose CIDR block is 192.168.0.0/16.

   If echo reply packets are returned, it indicates that the ECS instance is reachable from the data center.

3. Disable the primary Express Connect circuit and run the **ping** command to verify the connectivity between the data center and an ECS instance in the VPC whose CIDR block is 192.168.0.0/16.

   If echo reply messages are returned, it indicates that the secondary Express Connect circuit can serve your workloads when the primary Express Connect is down.

References

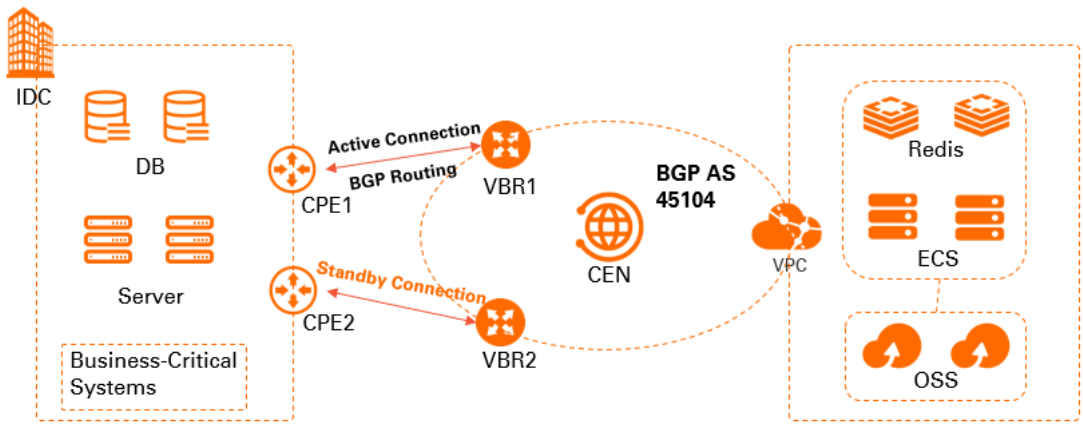
- For more information about how to troubleshoot connectivity issues between a data center and an ECS instance, see Troubleshooting.
- For more information about Express Connect circuit installation FAQ, see FAQ about physical connection construction.
- For more information about how to resolve issues in Express Connect circuit connections, see Express Connect circuits.

5.Create active/standby connections and configure BGP routing

This topic describes how to use Express Connect circuits and Cloud Enterprise Network (CEN) to create active/standby connections between a data center and a virtual private cloud (VPC) and configure Border Gateway Protocol (BGP) routing for the connections.

Scenario

The following scenario is used as an example to show how to use Express Connect circuits to create active/standby connections between a data center and a VPC and configure BGP routing for the connections. A company has a data center in Hangzhou and deployed business-critical systems such as database clusters in the data center. In addition, the company created a VPC in the China (Hangzhou) region and deployed applications on Elastic Compute Service (ECS) instances in the VPC. To ensure the stability of data transfer, the company plans to lease two Express Connect circuits to connect the customer-premises equipment (CPE) and virtual border routers (VBRs). Each Express Connect circuit connects to a separate piece of CPE in the data center. Then, attach the VBRs and the VPC to a CEN instance. This way, the data center and the VPC can communicate with each other. The data center is connected to the VPC through a primary Express Connect circuit and a secondary Express Connect circuit. The company configured BGP routing and Bidirectional Forwarding Detection (BFD). This accelerates network convergence and improves service availability.



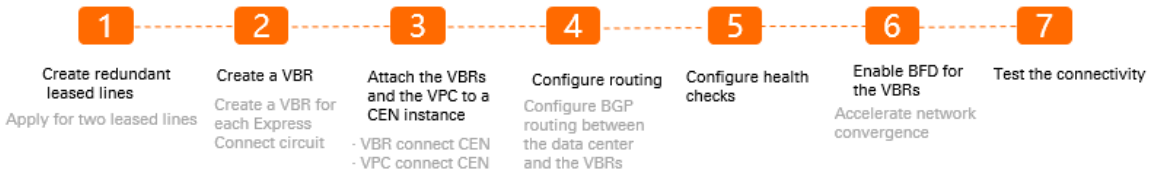
Preparations

Before you start, make sure that the following prerequisites are met:

-
- A VPC is created and applications are deployed in the VPC. For more information, see 创建和管理专有网络.
- A ticket is submitted and permissions to use the BFD feature are acquired.
- The following table describes how networks are planned in this example. You can plan CIDR blocks based on your business requirements. Make sure that the CIDR blocks do not overlap with each other.

Entity	CIDR block	Server or client IP address
Data center	10.1.1.0/24	Client IP address: 10.1.1.1
VPC	192.168.20.0/24	Server IP address: 192.168.20.161
VBR1	○ VLAN: 110 ○ IPv4 CIDR block for the VBR: 172.16.1.2/30 ○ IPv4 CIDR block for the gateway device in the data center: 172.16.1.1/30	N/A
VBR2	○ VLAN: 120 ○ IPv4 CIDR block for the VBR: 172.16.2.2/30 ○ IPv4 CIDR block for the gateway device in the data center: 172.16.2.1/30	N/A

Procedure



Step 1: Create redundant leased lines

Apply for two leased lines in the China (Shanghai) region. In this example, name the leased line that connects to the local CPE1 as leasedline1, and the leased line that connects to the local CPE2 as leasedline2. For more information, see Create a dedicated connection over an Express Connect circuit.

Step 2: Create a VBR

Create a VBR for each Express Connect circuit. A VBR is used to transmit data from the VPC to the data center.

1.
2.
3. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.
4. In the top navigation bar, select the region where you want to create a VBR.

   In this example, the **China (Hangzhou)** region is selected.
5. On the **Virtual Border Routers (VBRs)** page, click **Create VBR**.
6. In the **Create VBR** panel, set the following parameters and click **OK**:

- **Account**: Select **Current account**.
- **Name**: VBR1 is used in this example.
- **Physical Connection Interface**: Select an Express Connect circuit.
- **VLANID**: 110.
- **Peer IPv4 Address of Gateway at Alibaba Cloud Side**: Enter 172.16.1.2.
- **Peer IPv4 Address of Gateway at Customer Side**: Enter 172.16.1.1.
- **Subnet Mask (IPv4 Address)**: Set this parameter to 255.255.255.252.

7. Repeat the preceding steps to create a VBR for the other Express Connect circuit.

   Set the following parameters:

   - **Account**: Select **Current account**.
   - **Name**: VBR2 is used in this example.
   - **Physical Connection Interface**: Select the other Express Connect circuit.
   - **VLANID**: 120.
   - **Peer IPv4 Address of Gateway at Alibaba Cloud Side**: Enter 172.16.2.2.
   - **Peer IPv4 Address of Gateway at Customer Side**: Enter 172.16.2.1.
   - **Subnet Mask (IPv4 Address)**: Set this parameter to 255.255.255.252.

Step 3: Attach the VBRs and the VPC to a CEN instance

After the connections are established, you must attach the VBRs that are associated with the Express Connect circuits and the VPC that you want to access to a CEN instance.

> **Note** In this example, the previous version of the CEN console is used.

1. Log on to the CEN console.
2. On the **Instances** page, click Create CEN Instance. For more information, see Create a CEN instance.
3. On the **Instances** page, find the CEN instance that you want to manage and click **Manage** in the **Actions** column.
4. On the **CEN** page, click the **Networks** tab and then click **Attach Network** to attach the VBRs and the VPC to the CEN instance.

   In this example, VBR1, VBR2, and the VPC are attached to the same CEN instance. After the VBRs and the VPC are attached to the CEN instance, the routes of the VPC and those of the VBRs are automatically advertised to the CEN instance. The VPC and the VBRs can learn routes from each other through the CEN instance. For more information, see Attach a network instance.
5. If you have added routes that point to ECS instances, VPN gateways, or high-availability virtual IP addresses (HAVIPs) in the VPCs, advertise the routes to the CEN instance.

   For more information, see Advertise routes to CEN.

Step 4: Configure routing

Configure BGP routing between the data center and the VBRs. You can use the Autonomous System (AS) path attribute to configure route priorities in the data center.

1. Set the data center and the VBRs as BGP peers and advertise routes. For more information, see Configure BGP.

The Autonomous System Number (ASN) of Alibaba Cloud is 45104. The data center can use 2-byte or 4-byte ASNs.

2. When you configure BGP routing in the data center, set the destination CIDR block of the BGP routes that you want to advertise to Alibaba Cloud. In this example, the CIDR block is 10.1.1.0/24. To establish active/standby connections from Alibaba Cloud to the data center, set the AS path length to configure route priorities.

The primary Express Connect circuit connects to CPE1. The secondary Express Connect circuit connects to CPE2. You can set the AS path length to configure route priorities. A shorter AS path indicates a higher priority. The following table describes how BGP routing is configured on the two pieces of CPE in the data center. For more information about the commands, contact the service provider of the CPE.

Configuration	CPE1	CPE2
Vlan Tag	110	120
Network	10.1.1.0/24	10.1.1.0/24
BGP ASN	6***3	6***4
Interface IP	172.16.1.1/24	172.16.2.1/24
AS-Path	B, A	C, B, A

CEN automatically learns and advertises routes. After you configure BGP routing, CEN automatically learns routes based on the route priorities. The following table describes the route learning details.

- BGP routing information of the VBRs

Item	VBR1	VBR2
Destination CIDR block	10.1.1.0/24	10.1.1.0/24
Next hop	172.16.1.1	172.16.2.1

The preceding table describes the routing information that the VBRs learn from the BGP peers. The VBRs are attached to a CEN instance. Therefore, routing information such as the AS path that the VBRs learn is automatically advertised to the CEN instance.

- Global route configurations

CPE route configurations		
Configuration	CPE1	CPE2
Vlan Tag	110	120
Network	10.1.1.0/24	10.1.1.0/24
BGP ASN	6***3	6***4
Interface IP	172.16.1.1/24	172.16.2.1/24
AS-Path	B, A	C, B, A

CPE route configurations		
Route configurations of the VBRs		
Configuration	VBR1	VBR2
Destination CIDR block	10.1.1.0/24	10.1.1.0/24
Next hop	172.16.1.1	172.16.2.1
Route configurations in the data center		
Destination CIDR block	192.168.20.0/24	
Next hop	i. 172.16.1.2 ii. 172.16.2.2	
Route configurations of the CEN instance		
Destination CIDR block	10.1.1.0/24	
Next hop	VBR1	

The VBRs and the VPC are attached to the same CEN instance. Therefore, the BGP routes that the VBRs learn are automatically advertised to CEN. CEN learns routes based on configurations such as route priorities.

The BGP routes that the VBRs learn from the data center share the same destination CIDR block but have different priorities. The Express Connect circuit that is connected to VBR1 serves as the primary link (the AS path is shorter). The Express Connect circuit that is connected to VBR2 serves as the secondary link (the AS path is longer). After the BGP routes are advertised to CEN, network instances such as the VPC attached to the CEN instance can learn the routes. The 10.1.1.0/24 routes whose next hop is VBR1 are displayed in the route table of the VPC.

CEN also advertises its routes to the BGP route table in the data center. Routes that point to the IP addresses of the interfaces on the VBRs are displayed in the BGP route table in the data center. The interfaces are the ones that you set as the BGP peers of the data center.

To specify a primary and a secondary routing path from the data center to the VPC (192.168.20.0/24), you can set the priorities of routes learned by VBR1 and VBR2 by using the AS path attribute.

Step 5: Configure health checks

You must configure health checks for the Express Connect circuits. After health checks are configured, probe packets are sent at the specified time interval. If no response is returned from one of the Express Connect circuits after the specified number of probe packets are sent, CEN automatically switches to the other Express Connect circuit.

1. Return to the **Instances** page.
2. In the left-side navigation pane, click **Health Check**.
3. Select the region to which the VBR belongs and click **Set Health Check**.
4. In the **Set Health Check** panel, set the following parameters and click **OK**:

- **Instances**: Select the CEN instance to which the VBR is attached.
- **Virtual Border Router (VBR)**: Select the VBR that you want to monitor.
- **Source IP**: Select **Custom IP Address** and enter an idle IP address of a vSwitch in the VPC where the VBR is deployed.
- **Destination IP**: Enter the interface IP address of the CPE.
- **Probe Interval (Seconds)**: Default value: 2. Unit: seconds. In this example, the default value is used.
- **Probe Packets**: Default value: 8. In this example, the default value is used.

5. Repeat the preceding operations to configure health checks for the other VBR.

Step 6: Enable BFD for the VBRs

Enable BFD for the VBRs to accelerate network convergence.

1.
2. In the left-side navigation pane, click **Virtual Border Routers (VBRs)**.
3. On the **Virtual Border Routers (VBRs)** page, click **Edit** in the **Actions** column.
4. In the **Edit VBR** panel, set the following parameters to configure BFD and click **OK**:
   - **Interval to Send**: Specify the time interval at which BFD packets are sent. Unit: milliseconds. Default value: 1000. In this example, the default value is used.
   - **Interval to Receive**: Specify the time interval at which BFD packets are received. Unit: milliseconds. Default value: 1000. In this example, the default value is used.
   - **Detection Time Multiple**: Specify the detection time multiplier that is used to determine the maximum number of packets to be sent. Default value: 3. In this example, the default value is used.
5. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR that you want to manage.
6. On the details page of the VBR, click the **BGP Peers** tab.
7. Find the BGP peer that you want to manage and click **Edit** in the **Actions** column.
8. In the **Modify BGP Peer** panel, select the **Enable BFD** check box, specify **BFD hop count**, and then click **OK**.

> **Note** BFD supports single-hop and multi-hop authentication. You can set hops based on your network configuration.

Step 7: Test the connectivity

To test the connectivity of the primary and secondary Express Connect circuits, perform the following operations:

> **Note**

1. Open the Command Prompt window of your computer at the on-premises data center.
2. Run the `ping` command to connect to an ECS instance that belongs to the 192.168.0.0/24 CIDR block in the VPC. If the ping request is successful, the connection between the on-premises data center and Alibaba Cloud is established.

3. Disconnect a leased line (for example, from VBR1 to CPE1) and run the `tracert` command. You can see that the CEN instance switches routes and that all traffic from Alibaba Cloud to the on-premises data center is forwarded over VBR2.

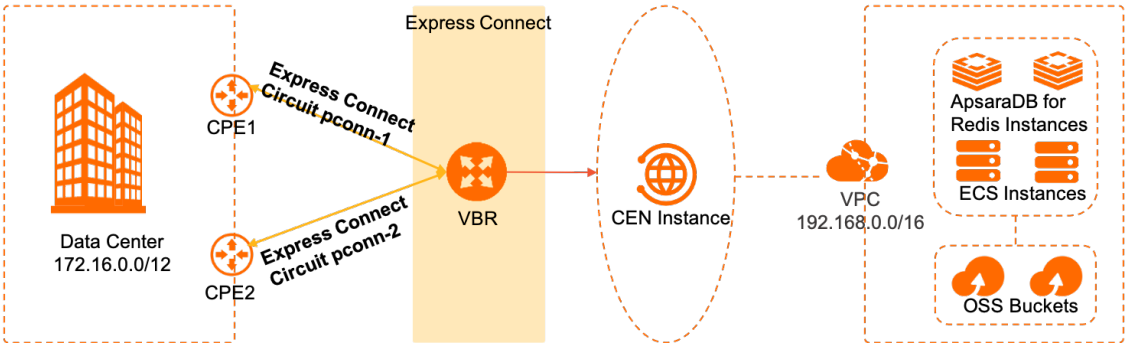
6.Configure ECMP between a data center and Alibaba Cloud

This topic describes how to configure equal-cost multi-path routing (ECMP). If a 100 Gbit/s Express Connect circuit cannot handle the traffic spikes to your workloads, you can use multiple Express Connect circuits to configure ECMP. This increases the bandwidth of your service and simplifies how you establish connections between your data center and Alibaba Cloud. ECMP allows network traffic with the same source and destination to be distributed across multiple paths. This prevents network congestion and optimizes resource utilization.

Scenario

The following example shows how to configure ECMP between a data center and Alibaba Cloud:

A company has a data center in Shanghai and a virtual private cloud (VPC) in the China (Shanghai) region. The private CIDR block of the data center is 172.16.0.0/12, and the CIDR block of the VPC is 192.168.0.0/16. To prevent bandwidth bottlenecks, the company applies for two Express Connect circuits from different connectivity providers to connect the data center to Alibaba Cloud.



The following table describes the configurations of the virtual border router (VBR) that is associated with the Express Connect circuits.

Configuration	Express Connect circuit pconn-1	Express Connect circuit pconn-2
VLAN ID	0	0
Peer IPv4 Address of Gateway at Alibaba Cloud Side	10.4.4.1	10.4.5.1
Peer IPv4 Address of Gateway at Customer Side	10.4.4.2	10.4.5.2
Subnet Mask (IPv4 Address)	255.255.255.252	255.255.255.252

Background information

Cloud Enterprise Network (CEN) automatically learns and distributes routes. After you configure routes, CEN automatically learns and advertises the routes to attached network instances. The following content describes how CEN learns routes:

> **Note** You can create static routes or configure Border Gateway Protocol (BGP) routing based on your network requirements. The configuration varies based on the routing option that you select:
>
> - To add a static route to the VBR, you must set the destination CIDR block of the route to the CIDR block of the data center. To configure BGP routing in the VBR, set the IP address of the BGP peer to the IPv4 address of the data center-side gateway.
> - To create a static route in the data center, you must set the destination CIDR block of the route to the CIDR block of the VPC. To configure BGP routing in the data center, set the IP address of the BGP peer to the IPv4 address of the Alibaba Cloud-side gateway.
>
> This topic describes how to configure BGP routing.

- BGP route configuration on the VBR

Destination CIDR block	Next hop
VBR route 1	
172.16.0.0/12	10.4.4.2
VBR route 2	
172.16.0.0/12	10.4.5.2

The preceding table describes the routes that the VBR learns from the BGP peer. After you attach the VBR to a CEN instance, the routes that the VBR learns from the data center are automatically advertised to the CEN instance.

- Global route configuration

Destination CIDR block	Next hop
VBR route 1	
172.16.0.0/12	10.4.4.2
VBR route 2	
172.16.0.0/12	10.4.5.2
CEN route table	
172.16.0.0/12	VBR
192.168.0.0/16	VPC

  - After you attach the VBR and the VPC to a CEN instance, the routes that the VBR learns from the data center are automatically advertised to the CEN instance. Then, network instances such as the VPC attached to the CEN instance can learn the routes.
  - CEN also advertises its routes to BGP. Therefore, you can view the CEN routes in the BGP route table in the data center. For example, you can view the routes whose next hops are the two interfaces on the VBR.

Prerequisites

Your data center is connected to Alibaba Cloud through Express Connect circuits. The Express Connect circuits must meet the following requirements. For more information, see Create a dedicated connection over an Express Connect circuit.

- The Express Connect circuits are associated with the same VBR.
- The Express Connect circuits are enabled.
- The bandwidth limits of the Express Connect circuits are the same.

Step 1: Create a VBR for the Express Connect circuits

1.
2.
3. On the **Physical Connections** page, click the ID of the Express Connect circuit for which you want to create a VBR. Make sure that the Express Connect circuit is enabled. In this example, pconn-1 is selected.
4. On the details page of the Express Connect circuit, click **Create VBR**.
5. In the **Create VBR** panel, set the following parameters and click **OK**:
   - **Account**: Specify the type of account for which you want to create the VBR. In this example, **Current Account** is selected.
   - **Name**: Enter a name for the VBR.
   - **Physical Connection Interface**: Select the Express Connect circuit that you want to associate with the VBR. The Express Connect circuit must be enabled and work as expected. In this example, **pconn-1** is selected.
   - **VLAN ID**: Enter the VLAN ID of the VBR. In this example, **0** is entered.
   - **Peer IPv4 Address of Gateway at Alibaba Cloud Side**: Specify an IPv4 address for the VBR. In this example, **10.4.4.1** is entered.
   - **Peer IPv4 Address of Gateway at Customer Side**: Specify an IPv4 address for the gateway device in the data center. In this example, **10.4.4.2** is entered.
   - **Subnet Mask (IPv4 Address)**: Enter the subnet mask of the specified IPv4 addresses. In this example, **255.255.255.252** is entered.

Step 2: Associate the VBR with another Express Connect circuit

1.
2.
3. On the **Physical Connections** page, click the ID of the Express Connect circuit that is already associated with the VBR. In this example, pconn-1 is selected.
4. On the details page of the Express Connect circuit, click the ID of the VBR.
5. On the **Physical Connection Interfaces** tab, click **Add Physical Connection Interface**.
6. In the **Add Physical Connection Interface** panel, set the following parameters to add another Express Connect circuit and click **OK**:
   - **Physical Connection Interface**: Select another Express Connect circuit that you want to associate with the VBR. The Express Connect circuit must be enabled and work as expected. In this example, **pconn-2** is selected.

- **VLAN ID**: Enter the VLAN ID of the VBR. In this example, **0** is entered.
- **Peer IPv4 Address of Gateway at Alibaba Cloud Side**: Specify another IPv4 address for the VBR. In this example, **10.4.5.1** is entered.
- **Peer IPv4 Address of Gateway at Customer Side**: Specify another IPv4 address for the gateway device in the data center. In this example, **10.4.5.2** is entered.
- **Subnet Mask (IPv4 Address)**: Enter the subnet mask of the specified IPv4 addresses. In this example, **255.255.255.252** is entered.

Step 3: Configure BGP routing in the VBR

To configure BGP routing between the data center and the VBR, you must add the BGP peer that communicates with the VBR to a BGP group, and then advertise the BGP CIDR block to the VBR.

1.
2.
3.
4. Create a BGP group.
   i. Click the **BGP Groups** tab and click **Create BGP Group**.
   ii. Set the following parameters of the BGP group and click **OK**.

Parameter	Description
Support IPv6	Specify whether to enable IPv6 support. In this example, **No** is selected.
Name	Enter a name for the BGP group.
Peer ASN	Enter the Autonomous System Number (ASN) of the data center.
BGP Key	Enter the key of the BGP group.
Description	Enter a description for the BGP group.

5. Create a BGP peer.
   i. Click the **BGP Peers** tab and click **Create BGP Peer**.
   ii. Set the parameters of the BGP peer and click **OK**.

Parameter	Description
BGP group	Select the BGP group that you created.
BGP peer IP address	Enter the IP address of the BGP peer. In this example, a data center-side gateway IP address is entered, which is 10.4.4.2.
Enable BFD	In this example, Bidirectional Forwarding Detection (BFD) is disabled.

6. Repeat the steps in to create a BGP peer for pconn-2.

   In this example, the IP address of the BGP peer for pconn-2 is set to 10.4.5.2 and BFD is disabled.

Step 4: Attach the VPC and the VBR to a CEN instance

You must attach the VPC and the VBR to the same CEN instance.

1.
2. On the **Instances** page, click the ID of the CEN instance that you want to manage.

   If you do not have a CEN instance, create one. For more information, see .
3. Click the **Networks** tab and click **Attach Network**.
4. In the **Attach Network** panel, click the **Your Account** tab to attach the VBR, and then click **OK**.
   - **Network Type**: Select the type of network instance that you want to attach. In this example, **Virtual Border Router (VBR)** is selected.
   - **Region**: Select the region where the VBR is deployed.
   - **Networks**: Select the ID of the VBR.
5. Repeat the preceding steps to attach the VPC to the CEN instance.

> **Notice** If you have created routes that point to Elastic Compute Service (ECS) instances, virtual private network (VPN) gateways, or high-availability virtual IP addresses (HAVIPs), you must advertise these routes to the CEN instance in the VPC console. For more information, see .

Step 5: Configure routing in the data center

You must configure BGP routing in the data center so that BGP routes can be advertised to Alibaba Cloud. The CIDR block of the data center is 172.16.0.0/12. The following table describes how to configure BGP routing on the two pieces of customer-premises equipment (CPE) in the data center. For more information about the configurations, contact the CPE vendor.

Configuration	CPE1	CPE2
VLAN ID	0	0
Network	172.16.0.0/12	172.16.0.0/12
BGP ASN	65000	65000
PEER BGP ASN	45104	45104
Interface IP	10.4.4.2/30	10.4.5.2/30

Step 6: Verify network connectivity

After you establish the connections, you must verify the reachability of the connections.

1. Open the command-line interface on a computer in the data center.
2. Run the **ping** command to verify the connectivity between the data center and an ECS instance in the VPC whose CIDR block is 192.168.0.0/16.

   If echo reply packets are returned, it indicates that the connection is reachable.
3. To check whether active/active connections are established between the data center and Alibaba Cloud, run the **tracert** command to query the routes through which packets are sent.

   The tracert command varies based on the device. For more information about the command,

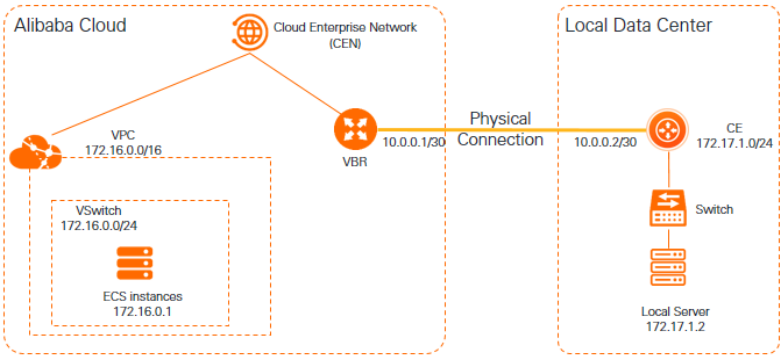
contact the vendor.

7.Connect to an ECS instance from a data center by using an Express Connect circuit

This topic describes how to connect a data center to a virtual private cloud (VPC) by using an Express Connect circuit. This allows servers in the data center to access the Elastic Compute Service (ECS) instances in the VPC.

Scenarios

The following figure shows an example of the network configurations for connecting a VPC and a data center. The data center is located in Hangzhou and the VPC is deployed in the China (Hangzhou) region. The private CIDR block of the VPC is 172.16.0.0/16. The private CIDR block of the data center is 172.17.1.0/24. You want to connect a server in the data center to an ECS instance in the VPC by using an Express Connect circuit. The IP address of the on-premises server is 172.17.1.2. The IP address of the ECS instance is 172.16.0.1.



Configuration item	IP address/CIDR block
VPC CIDR block	172.16.0.0/16
vSwitch CIDR block	172.16.0.0/24
ECS instance IP address	172.16.0.1
Data center CIDR block	172.17.1.0/24
IP addresses used by the gateways to connect the on-premises network and Alibaba Cloud	• IP addresses for the VBR: 10.0.0.1/30 • IP addresses for the gateway device in the data center: 10.0.0.2/30
On-premises server IP address	172.17.1.2
Health check IP addresses	• Source IP address: 172.16.0.2 • Destination IP address: 10.0.0.2

Step 1: Create a connection over an Express Connect circuit

You can create a dedicated connection over an Express Connect circuit by applying for a dedicated Express Connect circuit in the Express Connect console. You can also use a hosted connection over a shared Express Connect circuit provided by an Express Connect partner. For more information, see Create a dedicated connection over an Express Connect circuit or Overview.

The following table describes the configurations of the VBR that is associated with the Express Connect circuit in this example.

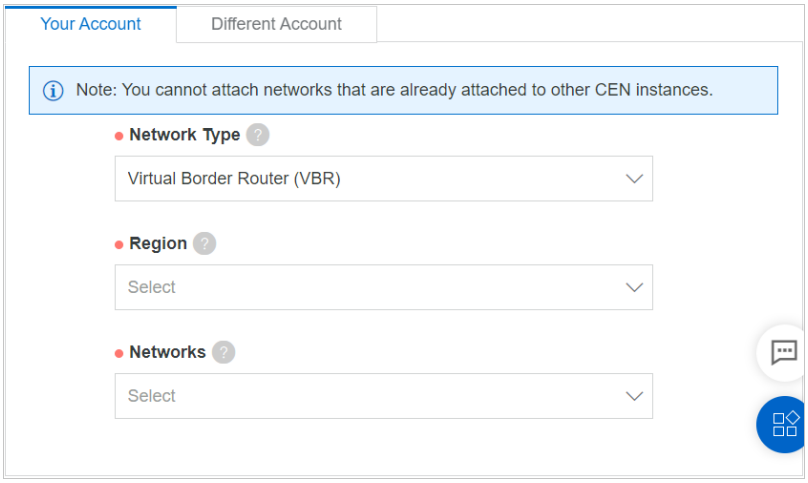
Configuration item	Configuration details
VLAN ID	0
Peer IPv4 Address of Gateway at Alibaba Cloud Side	10.0.0.1
Peer IPv4 Address of Gateway at Customer Side	10.0.0.2
Subnet Mask (IPv4 Address)	255.255.255.252

Step 2: Attach the VPC and the VBR to a CEN instance

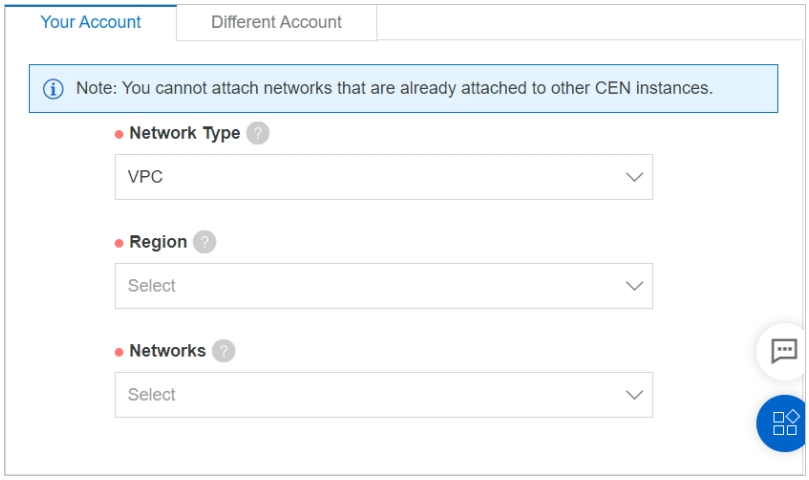
After the data center is connected to the VPC, you must attach the VPC and the VBR to the same Cloud Enterprise Network (CEN) instance. The CEN instance automatically learns and distributes the routes of the attached network instances to enable private communication.

1. Log on to the CEN console.
2. On the **Instances** page, find the CEN instance that you want to manage and click its ID.

   For more information about how to create a CEN instance, see Create a CEN instance.
3. On the **Networks** tab, click **Attach Network** to attach the VBR that is associated with the Express Connect circuit to the CEN instance. In the panel that appears, set the parameters and click **OK**.



   - **Network Type**: Select **Virtual Border Routers (VBRs)**.
   - **Region**: Select the region where the VBR is deployed.
   - **Networks**: Select the VBR that is associated with the Express Connect circuit.
4. Click **Attach More**, attach the VPC that you want to access and click **OK**.



Step 3: Configure routes on the VBR

After you attach the VBR and the VPC to the CEN instance, you must add a route that points to the data center and a route that points to the Express Connect circuit to the VBR. The following procedure shows how to add a route that points to the Express Connect circuit to the VBR.

1.
2.
3. On the **Virtual Border Routers (VBRs)** page, click the ID of the VBR.
4. On the VBR details page, click the **Routes** tab, and click **Add Route**.
5. In the **Add Route** panel, set the following parameters and click **OK**:
   - **Next Hop Type**: Select **Physical Connection Interface**.
   - **Destination Subnet**: Enter the CIDR block of the data center. In this example, *172.17.1.0/24* is entered.
   - **Next Hop**: Select the Express Connect circuit associated with the VBR.

> **Note** By default, if you **ping** the IP address of the VBR from an ECS instance, you cannot reach the VBR. You must first add a route to the VBR, and then set the next hop of the route to the Express Connect circuit and the destination CIDR block to 10.0.0.1/30.

Step 4: Configure health checks

CEN provides the health check feature to monitor the status of connections to the data center.

1. Log on to the CEN console.
2. In the left-side navigation pane, click **Health Check**.
3. On the **Health Check** page, select the region where the VBR is deployed. In this example, **China (Hangzhou)** is selected. Click **Set Health Check**.
4. In the **Set Health Check** panel, set the following parameters and click **OK**.
   - **Instances**: Select the CEN instance to which the VBR is attached.
   - **Virtual Border Router (VBR)**: Select the VBR that you want to monitor.
   - **Source IP**: Select **Custom IP Address** and enter an idle IP address that belongs to a vSwitch of the connected VPC. In this example, 172.16.0.2 is entered.

- **Destination IP**: Enter the IP address of the gateway device in the data center. In this example, 10.0.0.2 is entered.
- **Probe Interval (Seconds)**: Set the time interval at which probe packets are sent. In this example, the time interval is set to 2 seconds.
- **Probe Packets**: Specify the number of probe packets to be sent for a health check. In this example, the value of this parameter is set to 8.

> **Note** The system sends probe packets at the specified intervals. If the number of consecutively dropped packets reaches the specified value, the health check fails.

Step 5: Configure routes on the gateway device of the data center

After you complete the previous steps, you must log on to the gateway device of the data center and configure routes that point to the VPC. You can create a static route or configure Border Gateway Protocol (BGP) routing to forward network traffic from the data center to the VBR.

1. Create a static route or configure BGP routing on the gateway device to route traffic to the VPC.
   - The following static route is used as an example.

     > **Note** The route in this example is provided only for reference. Route configurations may vary based on the gateway device.

     ```
     ip route 172.16.0.0 255.255.0.0 10.0.0.1
     ```

   - Configure BGP routing. For more information, see Configure BGP.

     The CIDR block to be advertised is the CIDR block of the VPC connected to the data center. In this example, the CIDR block of the VPC is 172.16.0.0/16.
2. Run the **ping** command to ping the IP address of the VBR from the gateway device to verify network connectivity.

   Run the **ping** command to ping the IP address `10.0.0.1`. If you can reach the destination, it indicates that the gateway device in the data center is connected to Alibaba Cloud over the Express Connect circuit.
3. Run the following command to configure the default route on a server in the data center. The route points to the gateway device in the data center.

   ```
   route add default gw 172.17.1.1
   ```

Step 6: Verify the connectivity of the Express Connect circuit

To verify the connectivity of the Express Connect circuit, you can ping the IP address of the VBR.

1. Open the command prompt on a server in the data center.
2. Run the **ping** command to ping the IP address of the VBR: **10.0.0.1**. If the ping succeeds, it indicates that the server in the data center is connected to Alibaba Cloud over the Express Connect circuit.

> **Note** If you **ping** the IP address of the VBR from an ECS instance, you cannot reach the VBR.

Step 7: Test the connectivity to an ECS instance

You can ping the IP address of an ECS instance to verify the connectivity between Alibaba Cloud and the data center. IP addresses of ECS instances are dynamically allocated. You must ping the private IP address of an ECS instance. In this example, the private IP address of the ECS instance is 172.16.0.1.

> **Note** Before you ping the private IP address, make sure that the security group rules configured for the ECS instance accept network traffic from the data center. For more information, see Query security group rules.

1. Open the command prompt on a server in the data center. Run the following command to **ping** the private IP address of the ECS instance:

   ```
   ping 172.16.0.1
   ```

2. Log on to the ECS instance and open the command prompt.
3. Run the **ping** command to ping the IP address of the server in the data center. If you can reach the IP address, it indicates that the server in the data center is connected to the ECS instance on Alibaba Cloud.

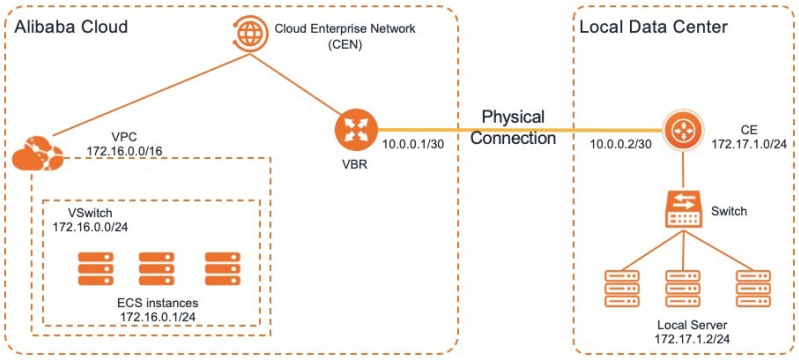
   ```
   ping 172.17.1.2
   ```

8.Configure BGP and BFD to accelerate route convergence

You can enable Border Gateway Protocol (BGP) on the network device in a data center and configure Bidirectional Forwarding Detection (BFD) on the virtual border router (VBR) to accelerate route convergence between the data center and a virtual private cloud (VPC).

Scenario

The following scenario is used as an example. A company has a data center in Hangzhou and a VPC in the China (Hangzhou) region. The company wants to connect a customer edge (CE) router to a VBR and then use Cloud Enterprise Network (CEN) to enable communication between the data center and the VPC. To accelerate route convergence, the company wants to configure BGP routing and BFD on the router in the data center and the VBR. This improves network availability.



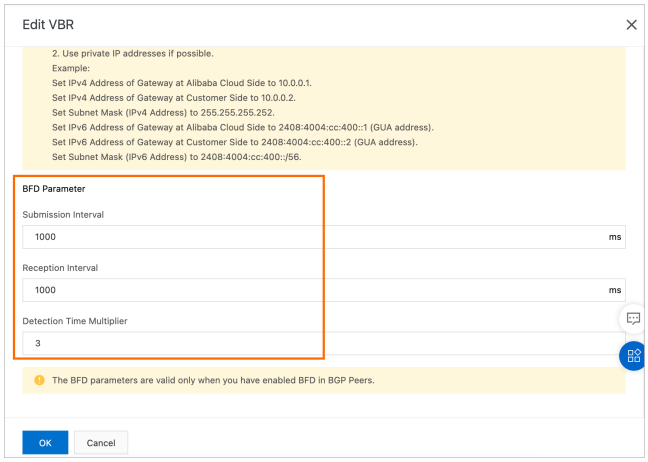
Prerequisites

- The data center is connected to Alibaba Cloud through an Express Connect circuit. For more information, see Connect to an ECS instance from a data center by using an Express Connect circuit.
- A BGP connection is established between the data center and the VPC. The **BGP peer** is in the **Established** state. For more information, see Configure BGP.
- Your account is included in the BFD whitelist. To use this feature, .

Step 1: Configure BFD on the VBR

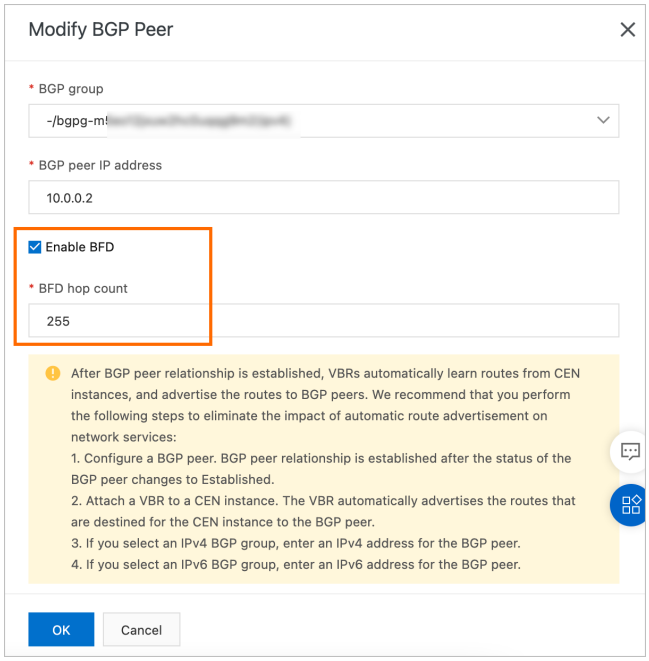
1.
2.
3. On the **Virtual Border Routers (VBRs)** page, find the VBR that you want to manage and click **Edit** in the **Actions** column.
4. In the **Edit VBR** panel, set the BFD parameters and click **OK**.

   In this example, the default settings are used.



5. Enable BFD.
   i.
   ii. Click the **BGP Groups** tab, find the BGP peer that you want to manage and click **Edit** in the **Actions** column.
   iii. In the **Modify BGP Peer** panel, select **Enable BFD**, specify **BFD hop count**, and then click **OK**.

   BFD hop count: specifies the maximum number of devices between a source and a destination. You can specify the hop count based on your network topology. Valid values: 1 to 255.



Step 2: Configure BFD between the CE router and the VBR

> **Note** In this example, an H3C-6820 device is used. The configuration may vary based on the device. For more information, contact the service provider of your CE router.

1. Log on to the CE router and run the following command to configure BFD:

```
System-view
Bgp <Autonomous System Number (ASN) of the CE router>
Peer <IP address that the VBR uses to communicate with the data center> bfd
```

> **Note** In this example, *10.101.1.2* is used by the VBR.

2. To verify the BFD configurations, run the `display bfd session verbose` command.

   The following output is displayed. **Session State: Up** indicates that a BGP connection is established between the CE router and the VBR and BFD is enabled.

```
<CE> display bfd session verbose
Total Session Num: 1 Up Session Num: 1 Init Mode: Active
IPv4 Session Working Under Ctrl Mode:
Local Discr: 513 Remote Discr: 513
Source IP: 10.101.1.1 Destination IP: 10.101.1.2
Session State: Up
Interface: N/A
Min Tx Inter: 500ms Act Tx Inter: 500ms
Min Rx Inter: 500ms Detect Inter: 2500ms
Rx Count: 135 Tx Count: 135
Connect Type: Indirect Running Up for: 00:00:58
Hold Time: 2457ms Auth mode: None
Detect Mode: Async Slot: 0
Protocol: BGP
Version:1
Diag Info: No Diagnostic
```

3. If multiple connections over Express Connect circuits are established between the data center and the VPC, repeat the preceding operations.

FAQ

- Can I configure BFD on one VBR to accelerate route convergence when two VBRs are attached to a CEN instance?

  Yes, you can configure BFD on one VBR to accelerate route convergence when two VBRs are attached to a CEN instance.

- If BFD detects failures on one of two VBRs attached to a CEN instance, can the other VBR immediately take over?

  Yes, a VBR can take over immediately after the other VBR is down. However, you must add the VBRs to a failover group to reduce the route convergence time. For more information about failover groups, see Configure a failover group.

9.Enable and disable a VBR to test the connectivity of a secondary Express Connect circuit by using OpenAPI Explorer

This topic describes how to use OpenAPI Explorer to test the connectivity of an Express Connect circuit. OpenAPI Explorer provides web-based operations. You can call APIs in OpenAPI Explorer to test the connectivity of an Express Connect circuit that is used to connect your data center to Alibaba Cloud.

Context

If your data center is connected to Alibaba Cloud through a primary and a secondary Express Connect circuit, you can test the connectivity of the secondary Express Connect circuit by disabling the primary Express Connect circuit for a limited time. To perform the test, you can enable and disable the VBR that is associated with the primary Express Connect circuit.

If your data center is connected to Alibaba Cloud through two Express Connect circuits, you can configure health checks and routes for the Express Connect circuits to enable automatic failover. When one of the Express Connect circuits is declared unhealthy, the system automatically routes network traffic through the other Express Connect circuit that works as expected. This ensures the high availability of your service. The time that is required to switch network traffic is affected by the number of routes in the virtual private cloud (VPC) that is connected to your data center. The process normally takes less than 12 seconds.

The following table describes the configurations of a primary Express Connect circuit and a secondary Express Connect circuit that are used to connect a data center to a VPC.

Parameter	IP address/CIDR block
CIDR block of the VPC	172.16.0.0/16
IP addresses of the Elastic Compute Service (ECS) instance	172.16.1.25/24
CIDR block of the data center	172.17.1.0/24
Peer IP addresses configured on the primary VBR	• IP addresses used by the VBR: 10.0.0.1/30 • IP addresses used by the data center: 10.0.0.2/30
Peer IP addresses configured on the secondary VBR	• IP addresses used by the VBR: 10.0.1.1/30 • IP addresses used by the data center: 10.0.1.2/30
IP addresses of the on-premises server	172.17.1.2/24

Parameter	IP address/CIDR block
Health check configurations for the primary VBR	• Source IP address: 172.16.1.2 • Destination IP address: 10.0.0.2
Health check configurations for the secondary VBR	• Source IP address: 172.16.1.3 • Destination IP address: 10.0.1.2

Step 1: Check whether the primary VBR is active

1.
2. In the left-side navigation pane, click **Exclusive Physical Connection**.
3. Click the ID of the primary Express Connect circuit. On the details page of the Express Connect circuit, check whether the primary VBR is active.

Step 2: Disable the primary VBR

1. Log on to OpenAPI Explorer and enter TerminateVirtualBorderRouter in the search bar.
2. Click **TerminateVirtualBorderRouter**.
3. Select the region where the primary Express Connect circuit is created, and enter the ID of the associated VBR.
4. Click **Submit Request**.

   The state of the VBR switches to Terminating. After the operation is successful, the state of the VBR switches to Terminated.

   > **Note** You can also click **Terminate Connection** in the Actions column of the VBR on the details page of the Express Connect circuit.

Step 3: Test the connectivity between the VPC and the data center when the primary Express Connect circuit is down

1. In the data center, **ping** the peer IP address used by the VBR that is associated with the primary Express Connect circuit: 10.0.0.1. The result shows that the connection fails. This indicates that the primary Express Connect circuit is out of service.
2. In the data center, **ping** an ECS instance that is deployed in the VPC. The result shows that the connection is active.
3. In the data center, use **curl** to access the web port of the ECS instance. The result shows that the data center can access the web page of the ECS instance.

Step 4: Enable the primary VBR

1. Log on to OpenAPI Explorer, and enter RecoverVirtualBorderRouter in the search bar.
2. Click **RecoverVirtualBorderRouter**.
3. Select the region where the primary Express Connect circuit is created and enter the ID of the associated VBR.
4. Click **Submit Request**.

The state of the VBR switches to Enabling. After the operation is successful, the state of the VBR switches to Active.

> **Note** You can also click **Recover** in the Actions column of the VBR on the details page of the Express Connect circuit.

Step 5: Test the connectivity of the primary Express Connect circuit

In the data center, **ping** the peer IP address used by the VBR that is associated with the primary Express Connect circuit: 10.0.0.1.

Additional information

You can call the DeleteVirtualBorderRouter operation to delete a disabled VBR in OpenAPI Explorer. For more information, see DeleteVirtualBorderRouter.