

ALIBABA CLOUD

阿里云

高速通道
最佳实践

文档版本：20201027

 阿里云

法律声明

阿里云提醒您在使用或阅读本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
Courier字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
斜体	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录

1.物理专线网络性能测试方法	05
2.通过物理专线就近接入和一点接入连接全球	12
3.本地IDC通过专线访问云服务器ECS	14
4.配置BGP与BFD联动实现路由快速收敛	18
5.使用OpenAPI Explorer终止和恢复VBR来确认冗余物理专线	20

1.物理专线网络性能测试方法

物理专线接入完成后，您需要对链路的性能进行测试，确保物理专线可以满足您的业务需求。

前提条件

在测试前，确保您完成以下环境准备：

- 完成物理专线的接入和路由配置，本地IDC与阿里云通过物理专线连通。
- 准备1台本地IDC服务器：作为Netperf或iperf3测试中的客户端或服务器端。
本操作中，IDC网络设备的IP地址为：192.168.100.1。
- 准备8台专有网络ECS实例：作为Netperf或iperf3测试中的客户端或服务器端。与本地IDC网络接入设备之间建立控制连接，传递测试配置相关的信息，以及测试结果。

本操作中使用8台规格为ecs.se1.2xlarge 镜像为centos_7_2_64_40G_base_20170222.vhd的ECS实例，IP地址为172.16.0.2 - 172.16.0.9。

搭建测试环境

安装Netperf

Netperf是一个网络性能的测量工具，主要针对基于TCP或UDP传输。

完成以下操作，分别在IDC网络设备和8台ECS实例上安装Netperf：

1. 执行以下命令下载Netperf。

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

2. 执行以下命令安装Netperf。

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

3. 执行 `netperf -h` 和 `netserver -h` 验证安装是否成功。

安装iPerf3

iperf3是一个网络性能测试工具。iperf3可以测试最大TCP和UDP带宽性能。

完成以下操作，分别在IDC网络设备和8台ECS实例上安装iPerf3：

1. 执行以下命令下载iPerf3。

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

2. 执行以下命令安装iPerf3。

```

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

```

3. 执行命令 `iperf3 -h`，验证安装是否成功。

开启多队列功能

在IDC网络接入设备内部执行以下命令，开启多队列功能。（假设与物理专线相连的接口为eth0。）

```

ethtool -L eth0 combined 4
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

```

使用Netperf工具测试物理专线的包转发性能

Netperf安装完成后会创建两个命令行工具：netserver（服务器端）和netperf（客户端）。两个工具的主要参数说明如下表所示。

工具名称	主要参数	参数说明
Netserver（服务器端：接收端工具）	-p	监听的端口号。
netperf（客户端：发送端工具）	-H	IDC网络接入设备或VPC服务器的IP地址。
	-p	IDC网络接入设备或VPC服务器的端口。
	-l	运行时间。
	-t	发送报文的协议类型：TCP_STREAM或UDP_STREAM。 建议使用UDP_STREAM。
	-m	数据包大小。 <ul style="list-style-type: none"> 测试pps（packet per second）时，建议设置为1。 测试bps（bit per second）时，建议设置为1400。

测试收方向

1. 在IDC网络接入设备内启动netserver进程，指定不同端口，如下所示：

```
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. 在VPC内的8台ECS实例上启动netperf进程，分别指定到IDC网络接入设备的不同netserver端口。

```
netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第一台
netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1 #第二台
netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1 #第三台
netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1 #第四台
netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1 #第五台
netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1 #第六台
netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1 #第七台
netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1 #第八台
```

3. 如果需要测试bps，将上述命令修改为：

```
netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1400 #第一台
netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1400 #第二台
netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1400 #第三台
netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1400 #第四台
netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1400 #第五台
netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1400 #第六台
netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1400 #第七台
netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1400 #第八台
```

测试发方向

1. 在8台VPC ECS实例内启动netserver进程，指定端口，如下所示：

```
netserver -p 11256
```

2. 在IDC网络接入设备内启动8个netperf进程，指定为不同IP地址。

```
netperf -H 172.16.0.2 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第一台ECS实例
netperf -H 172.16.0.3 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第二台ECS实例
netperf -H 172.16.0.4 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第三台ECS实例
netperf -H 172.16.0.5 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第四台ECS实例
netperf -H 172.16.0.6 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第五台ECS实例
netperf -H 172.16.0.7 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第六台ECS实例
netperf -H 172.16.0.8 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第七台ECS实例
netperf -H 172.16.0.9 -p 11256 -t UDP_STREAM -l 300 -- -m 1 #第八台ECS实例
```

3. 如果需要测试bps，将上述命令修改为：

```
netperf -H 192.168.100.1 -p 11256 -t UDP_STREAM -l 300 -- -m 1400 #第一台ECS实例
netperf -H 192.168.100.1 -p 11257 -t UDP_STREAM -l 300 -- -m 1400 #第二台ECS实例
netperf -H 192.168.100.1 -p 11258 -t UDP_STREAM -l 300 -- -m 1400 #第三台ECS实例
netperf -H 192.168.100.1 -p 11259 -t UDP_STREAM -l 300 -- -m 1400 #第四台ECS实例
netperf -H 192.168.100.1 -p 11260 -t UDP_STREAM -l 300 -- -m 1400 #第五台ECS实例
netperf -H 192.168.100.1 -p 11261 -t UDP_STREAM -l 300 -- -m 1400 #第六台ECS实例
netperf -H 192.168.100.1 -p 11262 -t UDP_STREAM -l 300 -- -m 1400 #第七台ECS实例
netperf -H 192.168.100.1 -p 11263 -t UDP_STREAM -l 300 -- -m 1400 #第八台ECS实例
```

分析测试结果

客户端的netperf进程执行完毕后，会显示如下结果。

```
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
```

显示结果中各字段含义如下表所示。

字段	含义
Socket Size	缓冲区大小
Message Size	数据包大小 (Byte)
Elapsed Time	测试时间 (s)
Message Okay	发送成功的报文数
Message Errors	发送失败的的报文数
Throughput	网络吞吐量 (Mbit/s)

通过发送成功的报文数除以测试时间，即可算出测试链路的pps，即pps=发送成功的报文数/测试时间。

使用iPerf3测试物理专线的带宽

iPerf3的主要参数说明如下表所示。

工具名称	主要参数	参数说明
iPerf3	-s	表示作为服务器端接收数据。
	-i	设置每次报告之间的时间间隔，单位为秒。
	-p	指定服务端的监听端口。
	-u	表示使用UDP协议发送报文。若不指定该参数则表示使用TCP协议。
	-l	设置读写缓冲区的长度。通常测试包转发性能是建议该值设为16，测试带宽是建议该值设为1400。
	-b	UDP模式使用的带宽，单位bits/s。
	-t	设置传输的总时间。Iperf在指定的时间内，重复的发送指定长度的数据包，默认值为10秒。
	-A	设置CPU亲和性，可以将的iPerf3进程绑定对应编号的逻辑CPU，避免iPerf3的进程在不同的CPU间被调度。

测试收方向

1. 在IDC网络接入设备中以server模式启动iperf3进程，指定不同端口，如下所示：

```
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. 在VPC ECS实例上以client模式启动iperf3进程，分别指定到IDC网络接入设备的不同端口。

```
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16001 -A 1
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16002 -A 2
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16003 -A 3
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16004 -A 4
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16005 -A 5
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16006 -A 6
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16007 -A 7
iperf3 -u -l 16 -b 100m -t 120 -c 192.168.100.1 -i 1 -p 16008 -A 8
```

测试发方向

1. 在每个VPC ECS实例上server模式启动iperf3进程并指定端口。

```
iperf3 -s -i 1 -p 16001
```

2. 在IDC接入设备上以client模式启动8个iperf3进程，`-c` 的值为各个陪练机的IP地址。

```
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
```

分析测试结果


客户端的iPerf3进程执行完毕后，会显示如下结果。

```
[ 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
```

显示结果中各字段含义如下表所示。

字段	含义
Transfer	传输的总数据量
Bandwidth	带宽大小
Jitter	抖动
Lost/Total Datagrams	丢失报文数/总报文数（丢包率）

PPS=对端收到的包 / 时间

 **说明** 建议您在server端运行 `sar` 命令来统计实际收到的包并作为实际结果，例如：`sar -n DEV 1 320`。

阿里云侧速率限制

除了物理专线的带宽限制外，VPC与本地数据中心之间的通信还受到以下限制。

- OSS的读写速率上限为5Gbit/s。
- 为了提高可靠性，从VPC到边界路由器（VBR）方向的单个hash流，在阿里云内部被限速为“高速通道规格带宽/12（或/4、/8和/16等）”。例如VBR到VPC的带宽为large1，即1Gbps带宽，则单个hash流的最大带宽为85Mbps。

hash流定义：源IP地址、源端口、传输层协议、目的IP地址和目的端口，这五个量组成的一个集合所定义的数据流。例如：“192.168.1.1 10000 TCP 121.14.**.* 80”就构成了一个hash流。即一个IP地址为192.168.1.1的终端通过端口10000，利用TCP协议，和IP地址为121.14.**.*，端口为80的终端进行的连接就是一个hash流。

2.通过物理专线就近接入和一点接入连接全球

高速通道物理专线可以帮助您在本地IDC和部署在各地域的阿里云VPC之间建立高质量、高可靠的内网通信。

功能概述

您可以通过物理专线在物理层面上连接您的本地数据中心到阿里云，然后建立边界路由器和路由器接口来连接数据中心与阿里云VPC。详情参见[专线上云方案介绍](#)。

就近接入

用户在使用专线将本地IDC和阿里云VPC互连时，选择距离本地IDC最近的接入点即可，无需在本地IDC和VPC所在地域间建立专线。其中接入点分为阿里云自有接入点和合作伙伴接入点。

- 阿里云自有接入点

您可以通过高速通道控制台的[专线接入点信息](#)来获取阿里云自有接入点的信息。如果您的本地IDC位于接入点所在的城市，您可以直接申请专线接入到这些接入点。



- 合作伙伴接入点

合作伙伴的接入点已经提前和阿里云建立了专线连接，您只需要在本地IDC和合作伙伴接入点间建立专线连接就可以实现本地IDC和云上VPC间的内网互连。您可以参考高速通道控制台的[合作伙伴信息](#)，并联系阿里云合作伙伴获取专线接入的相关信息。

如果您的本地IDC所在城市既没有阿里云自有接入点，也没有阿里云合作伙伴接入点，您可以自行选择一个距离您的本地IDC较近的接入点，在IDC和该接入点之间建立连接即可。

例如，一个用户在北京、天津和廊坊各有一个本地IDC，那么该用户可以根据以下策略进行专线接入：

- 由于北京有阿里云的自有接入点，该用户只需使用专线把位于北京的IDC和阿里云北京接入点连接即可。
- 由于天津没有阿里云的自有接入点，但有合作伙伴接入点，该用户可以使用专线把位于天津的IDC和天津的合作伙伴接入点连接起来即可。
- 廊坊既没有阿里云的自有接入点，也没有合作伙伴接入点，由于位于廊坊的IDC距离阿里云北京接入点距离较近，该用户可以使用专线把位于廊坊的IDC和阿里云北京接入点连接。


 **说明** 下图中只有黄色的专线是该用户需要找运营商或者合作伙伴施工的线路。



一点接入连接全球

您只需要接入任何一个接入点，就可以通过该接入点和阿里云遍布全球各地域的VPC连接起来。

例如，一个用户需要将位于北京的IDC通过专线接入到位于北京和深圳的VPC。此时，该用户只需要用一条专线将IDC连接到阿里云北京接入点，然后在边界路由器（VBR）上创建两个分别连接至两个VPC的路由器接口（RI）即可。

 **说明** 下图中只有黄色的专线是该用户需要找运营商或者合作伙伴施工的线路。



3.本地IDC通过专线访问云服务器ECS

本文介绍本地数据中心如何通过高速通道连接阿里云，打通云上VPC和本地IDC的网络，通过本地IDC的一台服务器访问云上VPC的一台ECS。

背景信息

当您需要从本地数据中心通过物理专线访问VPC中的云服务时，需要在边界路由器（VBR）中将100.64.0.0/10网段的路由条目指向VPC方向的路由器接口，并在本地数据中心的网关设备上将100.64.0.0/10网段的路由指向VBR的阿里云侧互联IP。

100.64.0.0/10是专有网络的保留地址，用于VPC中DNS、OSS或SLS等云服务使用。

说明 由于100.64.0.0/10网段属于VPC中的保留网段，因此不能直接在VBR中添加目的网段为100.64.0.0/10的路由条目。需要将该网段拆分成100.64.0.0/11和100.96.0.0/11，在VBR中配置两个路由条目。

教程介绍

本操作以下图的VPC和IDC配置为例，假设您在华东1（杭州）分别有一个VPC（私网网段：172.16.0.0/16）和本地IDC机房（私网网段：172.17.1.0/24），需要自主申请一条物理专线使本地IDC服务器（IP地址：172.17.1.2）和VPC中的ECS服务器（IP地址：172.16.1.1）互通。

参数	地址段
云上VPC网段	172.16.0.0/16
云上交换机网段	172.16.0.0/24
云上ECS的IP地址	172.16.1.1/24
本地IDC网段	172.17.1.0/24
互联IP	<ul style="list-style-type: none"> 云端VBR地址：10.0.0.1/30 本地IDC端：10.0.0.2/30
本地服务器IP地址	172.17.1.2/24
健康检查	<ul style="list-style-type: none"> 源IP：172.16.1.2 目的IP：10.0.0.2

步骤一：创建专线连接

您可以通过高速通道控制台自主创建专线连接（独享端口方式）或通过合作伙伴共享专线方式创建专线连接。具体操作请参见[创建独享专线连接](#)或[共享合作伙伴专线连接](#)。

本教程中和专线连接的云上网关设备边界路由器的配置如下：

边界路由器配置项	配置详情
VLANID	0

边界路由器配置项	配置详情
阿里云侧互联IP	10.0.0.1
客户侧互联IP	10.0.0.2
子网掩码	255.255.255.252

步骤二：加入CEN

 **注意** 在完成专线接入后，确保专线关联的VBR和要互通的VPC加入到同一个云企业网CEN（Cloud Enterprise Network）。

参考以下操作，加入云企业网：

1. 登录[云企业网控制台](#)。
2. 在云企业网实例页面，单击CEN实例ID链接。如果需要创建云企业网实例，请参见[创建云企业网实例](#)。
3. 在网络实例管理页面，单击[加载网络实例](#)加载专线关联的VBR和要互通的VPC。详细说明，请参见[加载网络实例](#)。




4. 单击[再次加载](#)，加载需要连接的VPC。
□
5. 单击[确定](#)。

步骤三：配置VBR路由

您需要在VBR上分别配置指向本地数据中心和物理专线接口的路由。

参考以下操作，配置VBR路由：

1. 登录[高速通道管理控制台](#)。
2. 在左侧导航栏，选择[边界路由器（VBR）](#)，然后单击目标边界路由器的ID链接。
3. 在边界路由器详情页面，单击[路由条目](#)，然后单击[添加路由条目](#)。
4. 在添加路由条目页面，根据以下信息配置路由条目。
 - **目标网段**：输入本地数据中心的网段，本操作中输入 *172.17.1.0/24*。
 - **下一跳类型**：选择[物理专线接口](#)。
 - **下一跳**：选择要自主申请的物理专线。

 **说明** 默认情况下，阿里云上的ECS实例无法ping通VBR的IP地址。如需进行ping测试，您需要添加指向物理专线接口的路由，其中使用VBR的互联IP地址段10.0.0.0/30作为本地IDC的网段。

5. 单击[确定](#)。

步骤四：配置健康检查

参考以下操作，配置健康检查：

1. 登录[云企业网控制台](#)。
2. 在左侧导航栏，单击[健康检查](#)。

3. 选择云企业网实例的地域**华东1（杭州）**，然后单击**设置健康检查**。
4. 在**设置健康检查**页面，配置健康检查。
 - **云企业网实例**：选择边界路由器加载的云企业网实例。
 - **边界路由器（VBR）**：选择要监控的边界路由器。
 - **源IP**：选择自定义源IP，输入所连接的VPC中交换机下的一个空闲IP，例如172.16.1.2。
 - **目标IP**：输入本地IDC网络设备的接口IP地址，例如10.0.0.2。
 - **发包时间间隔（秒）**：设置发包时间间隔为2秒。
 - **探测报文个数（个）**：设置探测报文个数为8个。
5. 单击**确定**。

步骤五：配置本地数据中心的路由

至此，已完成阿里云上的路由配置。您还需要在专线接入设备上配置指向VPC的路由。您可以选择配置静态路由或配置BGP路由将本地数据中心的数据转发至VBR。

参考以下操作，配置本地路由：

1. 本地网关设备配置到云上VPC的路由，您可以选择配置静态路由或配置BGP动态路由将本地数据中心的数据转发至VBR。
 - 静态路由示例仅供参考，不同厂商的不同设备可能会有所不同：

```
ip route 172.16.0.0 255.255.0.0 10.0.0.1
```

- 您也可以通过配置BGP来转发本地数据中心与VBR之间的数据，详情请参见[配置BGP](#)。
宣告网段为需要和本地数据中心通信的VPC的网段，下一跳云上边界路由器IP地址10.0.0.1。本案例中VPC网段为 172.16.0.0/16。
2. 本地网关设备ping云上VBR连通性测试。执行ping命令，`ping 10.0.0.1`，如果能ping通，表示本地网关到云上的专线连接成功。
 3. 执行如下命令，将本地IDC的服务器添加默认路由指向本地网关。

```
route add default gw 172.17.1.1
```

步骤六：专线连通性测试


参考以下操作，测试专线是否接入成功：

1. 打开本地IDC服务器的命令行窗口。
2. 执行ping命令，ping云上VBR**10.0.0.1**，如果能ping通，表示本地服务器到云上的专线连接成功。

 **说明** ECS无法ping通VBR互联地址。

步骤七：ECS连通性测试

您可以通过ping云上ECS实例的IP地址测试云上和本地数据中心的网络通信是否正常。

 **说明** 确保您要测试的ECS实例已经配置了安全组规则，允许本地IDC访问。

因为ECS的IP地址是动态分配的，请以实际ECS实例的内网IP进行配置，本案例中ECS实例的内网IP为 172.16.1.1 。

1. 打开本地IDC服务器的命令行窗口，执行ping命令，ping阿里云ECS实例的内网IP。

```
ping 172.16.1.1
```

2. 登录阿里云ECS实例并打开命令行窗口。
3. 执行**ping**命令，ping本地服务器的IP地址。如果能ping通，表示通过高速通道云下服务器到云上ECS已经连接成功。

```
ping 172.17.1.2
```

4. 配置BGP与BFD联动实现路由快速收敛

通过在本地IDC中心的网络设备上启动BGP路由协议，以及在云企业网边界路由器上配置双向转发检测（BFD），实现本地IDC与专有网络之间的路由快速收敛。

前提条件

配置BGP和BFD前，您必须确保以下操作已完成：

- 您已经在IDC与阿里云专有网络之间建立BGP对接，且BGP邻居状态是Established。
- 您已提交工单申请并获得使用BFD白名单权限。

背景信息

本操作以下图的VPC和IDC配置为例。



网络拓扑信息如下：

参数	地址段
互联IP	<ul style="list-style-type: none"> • 云端VBR地址：10.101.1.2/30 • 本地IDC端：10.101.1.1/30

步骤1：在边界路由器上配置BFD

1. 登录[高速通道管理控制台](#)。
2. 在左侧导航栏，单击**边界路由器（VBR）**。
3. 单击要修改参数的VBR实例操作列下的**编辑**。
4. 在显示的**修改边界路由器**面板，设置边界路由器参数。本实例中使用默认参数。



5. 单击**确定**。
6. 返回**边界路由器（VBR）**详情页面，单击目标VBR实例。



7. 在VBR实例配置页面，单击**BGP邻居**页签。
8. 单击要启动BFD的BGP邻居操作列下的**编辑**。



9. 在**修改BGP邻居**面板，选中**启用BFD**复选框。



说明 BFD功能支持自定义单跳或多跳会话。您可以根据真实的物理链路因素来配置不同的跳数。

10. 单击**确定**。

步骤2：在CE设备上与边界路由器建立BGP对接

1. 登录CE设备后执行下列命令（本示例采用H3C-6820设备）：

```
System-view
Bgp 32168
Peer 10.101.1.2 bfd
```

2. 运行 `display bfd session verbose` 验证BFD配置。

```
<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
```

以上显示信息表明CE和VBR之间已经建立了BGP连接，而且BFD协议运行正常。

如果本地IDC与VPC之间有多条专线连接，重复执行以上配置操作。

5.使用OpenAPI Explorer终止和恢复VBR来确认冗余物理专线

本文介绍本地IDC通过冗余专线接入阿里云后，您如何使用白屏化的OpenAPI工具调用API来完成专线故障演练。

背景信息

当本地IDC通过冗余物理专线正常接入阿里云后，您需要通过单条专线故障演练来确认冗余物理专线。您可以通过终止和恢复边界路由器VBR（Virtual Border Router）来完成故障演练，确认冗余物理专线的状态。

您通过冗余物理专线接入阿里云后，可以通过配置健康检查和设置路由权重来实现专线故障时业务流量的自动切换。当一条物理专线发生故障后，健康检查辅助系统自动将业务流量切换到另外一条正常的物理专线上，从而保障您的业务高可用。自动切换的时间周期受您的VPC路由条目数量的影响。通常情况下，您的业务可以在12秒内完成自动切换。

下表列出本地IDC通过冗余物理专线接入阿里云的VPC和IDC侧的参数配置信息：

参数	地址段
云上VPC网段	172.16.0.0/16
云上ECS的IP地址	172.16.1.25/24
本地IDC网段	172.17.1.0/24
主VBR互联IP	<ul style="list-style-type: none"> 云端VBR地址：10.0.0.1/30 本地IDC端：10.0.0.2/30
备VBR互联IP	<ul style="list-style-type: none"> 云端VBR地址：10.0.1.1/30 本地IDC端：10.0.1.2/30
本地服务器IP地址	172.17.1.2/24
主VBR健康检查	<ul style="list-style-type: none"> 源IP：172.16.1.2 目的IP：10.0.0.2
备VBR健康检查	<ul style="list-style-type: none"> 源IP：172.16.1.3 目的IP：10.0.1.2

步骤一：确认主VBR状态为正常

1. 登录[高速通道管理控制台](#)。
2. 在左侧导航栏，选择[独享物理专线](#)。
3. 单击目标物理专线实例ID，打开物理专线详情页面，确认关联的VBR实例状态为正常。

物理专线详情页面



步骤二：管理员终止VBR

1. 登录OpenAPI，在搜索框输入TerminateVirtualBorderRouter。
2. 单击TerminateVirtualBorderRouter。
3. 选择物理专线实例所在的地域，然后输入物理专线实例关联的主VBR实例ID。

4. 单击发起调用。

此时，VBR实例的状态为终止接入中，等待状态变为已终止。

 **说明** 您也可以单击物理专线详情页面目标VBR操作列下的终止接入来终止接入VBR。

步骤三：验证主专线故障以及云上VPC与本地IDC的网络连通性

1. 在本地IDC侧，ping主物理专线关联的VBR的互联IP地址10.0.0.1。结果显示网络不通，说明主物理专线已断开。

2. 在本地服务器侧，ping ECS服务器，结果显示网络正常。


3. 在本地服务器侧，通过curl访问云上ECS的Web端口。结果显示可以访问ECS Web页面内容。

步骤四：恢复VBR

1. 登录OpenAPI，在搜索框输入RecoverVirtualBorderRouter。
2. 单击RecoverVirtualBorderRouter。
3. 选择物理专线实例所在的地域，然后输入物理专线实例关联的主VBR实例ID。

4. 单击发起调用。

此时，VBR实例的状态为恢复中，等待状态变为正常。

 **说明** 您也可以单击物理专线详情页面VBR操作列下的恢复来重新连接VBR。

步骤五：验证主物理专线状态

在本地IDC侧，ping主物理专线关联的VBR的互联IP地址10.0.0.1。

更多信息

您可以使用OpenAPI工具通过DeleteVirtualBorderRouter接口删除状态为已终止的VBR实例。详细信息，请参见DeleteVirtualBorderRouter。