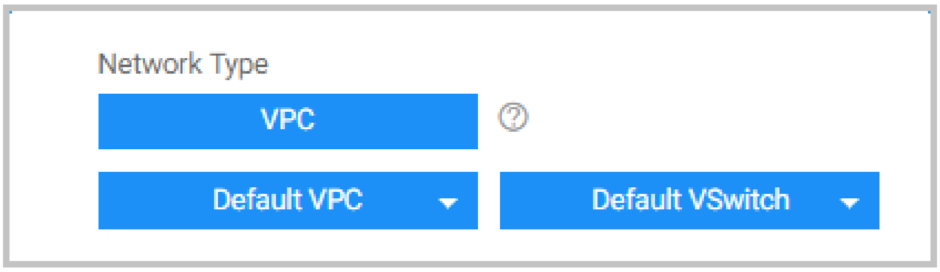
Virtual Private Cloud

User Guide

MORE THAN JUST CLOUD | Alibaba Cloud

User Guide

Alibaba Cloud provides a default VPC and VSwitch for you in the situation that you do not have any existing VPC and VSwitch to use when creating a cloud product instance. A default VPC and VSwitch will be created along with the creation of the instance.



Default VPC and VSwitch feature list

Default VPC	Default VSwitch
The default VPC in each region is unique.	The default VSwitch in each Availability Zone is unique.
The netmask for a default VPC is /16 such as 172.31.0.0/16, which provides up to 65536 private IP addresses.	The netmask for a default VSwitch is /20 such as 172.31.0.0/20, which provides up to 4096 private IP addresses.
The default VPC does not occupy the VPC quota that the Alibaba Cloud allocates to you.	The default VSwitch does not occupy the VSwitch quota that the Alibaba Cloud allocates to you.
The default VPC is created by the system, all the VPCs created by you are non-default VPCs.	The default VSwitch is created by the system, all the VSwitches created by you are non-default VSwitches.
The operations and restrictions for default and non-default VPCs are the same.	The operations and restrictions for default and non-default VSwitches are the same.

Build VPC

Prerequisite

Before creating a VPC, see Plan and design VPC network to design your private network.

Procedure

Log on to the VPC consoleVPC console.

In the left-side navigation pane, click **VPC**.

Choose the region where the VPC is located.

Click **Create VPC** in the upper-right corner.

In the dialog box, provide the following information:

Configuration	Description
VPC Name	Enter the name of the VPC.
Description(optional)	Add a description for the VPC.
CIDR block	Specify the IP address range for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block. Note the following when selecting a CIDR block: - Use the standard private CIDR blocks (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/1) or their subsets as the IP address ranges. **Note**: If you want to use the subset of the provided CIDR blocks as the IP address range, use the Open API to create a VPC. For more information, see Create a VPC. - If you have multiple VPCs, or you want to build a hybrid cloud consisting of multiple VPCs and on-premises IDCs, we recommend that you use the subset of the provided CIDR blocks, and ensure that the network mask is no larger than /16. - If you have one VPC and it does not need to communicate with the on-premises data center, you can use any of the provided

	CIDR blocks. - Consider the use of the classic network. If you plan to connect the cloud product instances in the classic network with a VPC, we recommend that you do not use the CIDR block 10.0.0.0/8, which is also used as CIDR block by the classic network. - **Note**: If you have special requirements on the IP address range, open a ticket or contact your customer manager.

Click **Create VPC**.

Related operations

Create a VSwitch

A VSwitch is a basic network device in a VPC network used to connect the cloud product instances in the VPC. You can further segment your virtual networks into subnets by adding VSwitches. For more information, see Create a VSwitch.

Manage a Route Table

A VRouter and a route table will be created after the VPC is created. You can add custom route entries in the route table, see Manage a route table.

Delete a VPC

On the VPC list page, locate the target VPC and click **Delete**.

> **Note**: Before deleting the VPC, make sure you have released or transferred all instances in the VSwitches of the VPC and VSwitches have been deleted.

Modify the name of a VPC

On the VPC list page, hover the mouse pointer on the target VPC ID. A pencil icon appears. Click the pencil icon to modify the VPC name.

Prerequisite

Plan and design VPC

Create a VPC

Procedure

Log on to the VPC console.

In the left-side navigation pane, click **VPC**.

Click the VPC region where the VSwitch to be created is located.

Click the target VPC ID.

Then you are directed to the **VPC Details** page.

Click **VSwitch** and then click **Create VSwitch**.

In the **Create VSwitch** dialog, provide the following information:

Configuration	Description
VPC	The ID of the VPC where the VSwitch is located.
VPC CIDR block	The CIDR block of the VPC. You can choose to click **Display Binary** to view the CIDR block in binary format.
Name	Enter the name of the VSwitch.
Zone	Select a zone of the VSwitch. Zones are physical areas with independent power grids and networks in one region. Zones in the same region are intranet connected. We recommend creating different VSwitches in different zones to achieve disaster recovery.
CIDR block	Specify the VSwitch IP address in the

	CIDR block form. Note the following when specifying a VSwtich CIDR block: - The allowed block size for a VSwitch is between a /16 netmask and /29 netmask, which can provide 8 to 65,536 IP addresses. - The CIDR block of the VSwitch can be the same as that of the VPC that it belongs to, or the subset of the VPC CIDR block. **Note**: If the CIDR block of the VSwitch is the same as that of the VPC, you can only create one VSwitch. - The first and the last three IP addresses are reserved by the system. For example, for the CIDR block 192.168.1.0/24, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. - You need to consider the number of the cloud product instances running in the VSwitch.
Number of Available Private IPs	The number of available IP addresses in the VSwitch.
Description (optional)	Add a description for the VSwitch.

7. Click **OK**.

Related operations

Create cloud product instances in a VPC

On the **VSwitch List** page, click **Create an Instance** to create an ECS, SLB, or RDS instance. For more details, refer to Create cloud service instance in a VPC.

Modify a VSwtich

On the **VSwitch List** page, find the target VSwitch and then click **Edit**. Or hover your mouse pointer over the VSwitch name to change the name of the VSwitch.

Delete a VSwitch

On the **VSwitch List** page, find the target VSwitch and then click **Delete**, click **Confirm** to delete the VSwitch.

Note: Before deleting a VSwitch, confirm that you have released or transferred all the cloud product instances under it.

Route table basics

A VRouter is a hub in a VPC that connects all VSwitches in the VPC and also serves as a gateway device that connects the VPC with other networks.

A VRouter and a route table are automatically created after you create a VPC. Each entry in the route table is a ***route entry***, which defines the next hop of the network traffic destined for a specific destination CIDR block. The network traffic is routed based on the configurations of the route entries in the route table.

> **Note**: You cannot create or delete a VRouter or a route table directly. They will be deleted automatically along with the deletion of the VPC. But you can add route entries to the route table to route network traffic.

There are two types of route entries:

- **System route entry**

  A system route entry is created by the system and cannot be deleted.

  - After you create a VPC, a system route entry will be automatically created.

    The destination CIDR block of this system route entry is 100.64.0.0/10, which is used for the communication within the VPC.

  - After you create a VSwitch, a system route entry will be automatically created.

    The destination CIDR block of this system route entry is the CIDR block of the VSwitch, which controls the routing for the VSwitch.

Custom route entry

You can create or delete custom route entries, and you can create up to 40 custom route entries in a route table.

> **Note**: In general, system route entries can meet your needs. But in some particular cases, you still need to add custom route entries. Before adding custom route entries, ensure that you have completed your network plan.

Routing policy

The longest prefix match algorithm is used to route the network traffic when more than one route entries match the destination IP address. That is, the route entry with the longest netmask (the most specific route) is used to determine the next hop.

Here is an example of a route table.

Destination CIDR block	Next Hop Type	Next Hop	Type
100.64.0.0/10			System
192.168.0.0/24			System
0.0.0.0/0	Instance	i-12345678	Custom
10.0.0.0/24	Instance	i-87654321	Custom

In this example, route entries with the destination CIDR blocks100.64.0.0/10 and 192.168.0.0/24 are the system route entries. Route entries with the destination CIDR blocks0.0.0.0/0 and 10.0.0.0/24 are custom route entries.

All traffic destined for 0.0.0.0/0 is routed to the ECS instance with the IDi-12345678 and all traffic destined for 10.0.0.0/24 is routed to the ECS instance with the IDi-87654321.

According to the longest prefix match algorithm, the traffic destined for 10.0.0.1 is routed to ECS instance with the IDi-87654321, while the traffic destined for 10.0.1.1 is routed to the ECS instance with the IDi-12345678.

Scenarios of adding custom router entries

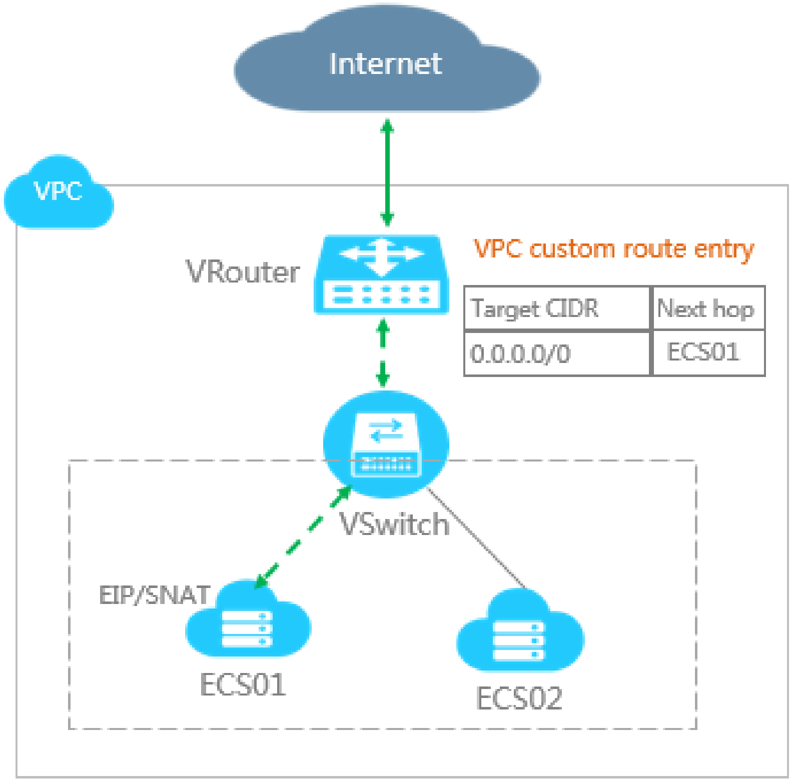
The custom route entries are needed in the following scenarios.

Traffic routing within a VPC

Assume that you have two ECS instances in your VPC: ECS01 and ECS02.

ECS01 is bounded with an Elastic IP (EIP) so that this ECS instance can communicate with the Internet. If you want ECS02 to communicate with the Internet without binding another EIP, you can add a custom route entry as follows.

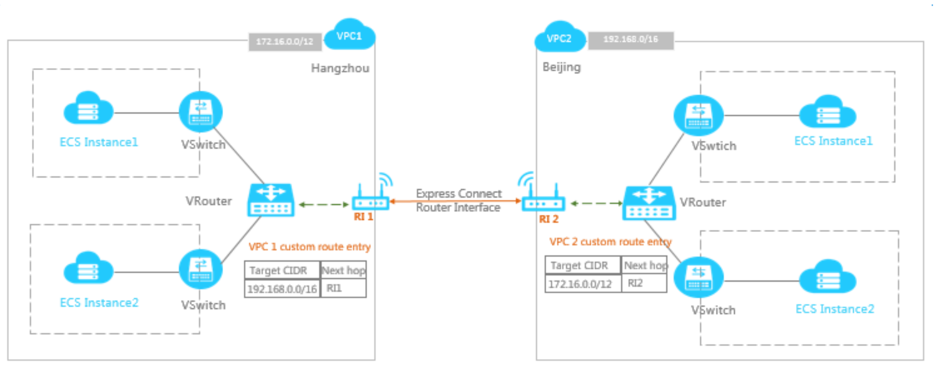
Destination CIDR	Next hop type	Next hop
0.0.0.0/0	ECS instance	ECS01



Interconnection between VPCs

Assume that you have two VPCs. VPC1 uses the CIDR block 172.16.0.0/12 and VPC2 uses the CIDR block 192.168.0.0/16.

By using the router interface function of the Express Connect product, you can create a connection between these two VPCs. Firstly, you need to create a router interface, and set VPC1 as the initiator and VPC2 as the receiver. Then, you need to add two custom route entries as follows.



- Custom route entry added in VPC1

Destination CIDR	Next hop type	Next hop
192.168.0.0/16	Route interface	RI1

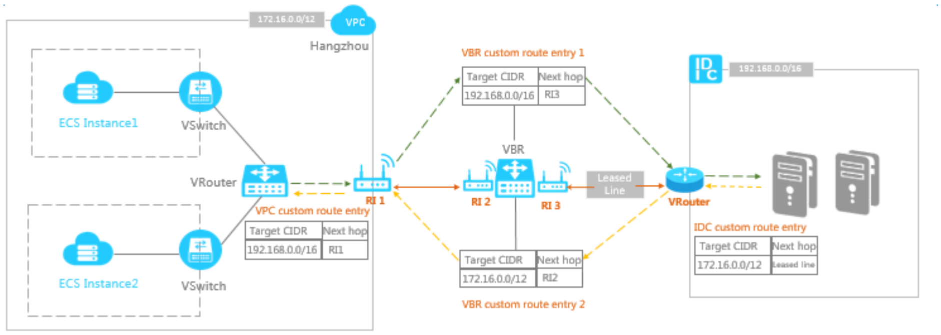
- Custom route entry added in VPC2

Destination CIDR	Next hop type	Next hop
172.16.0.0/12	Route interface	RI2

Interconnection between VPC and on-premises IDC

Assume that you have a VPC with the CIDR block 172.16.0.0/12, and an on-premises IDC with the CIDR block 192.168.0.0/16.

By using the physical connection (leased line) function of the Express Connect product, you can create a connection between the VPC and the IDC. Firstly, you need to create a Virtual Border Router (VBR) to connect the IDC with the VBR. Then, you need to create a router interface to connect the VBR with the VPC. Lastly, you need to add the following custom router entries:



- Custom route entry added in VPC

Destination CIDR block	Next hop type	Next hop

192.168.0.0/16	Route interface	RI1

- Custom route entry added in VBR

Destination CIDR	Next hop type	Next hop
192.168.0.0/16	Leased line	RI3
172.16.0.0/12	VPC	RI2

- Custom route entry added in IDC

Destination CIDR	Next hop type	Next hop
172.16.0.0/12	—	RI4

Add custom route entries

Log on to the VPC console.

In the left-side navigation pane, click **VPC**.

Choose the region where the VPC is created.

Click the ID of the target VPC.

In the left-side **VPC Details** pane, click **VRouter**, and then click **Add Route Entry**.

In the **Add Route Entry** dialog, provide the following information and click **OK**.

Configuration	Description
Destination CIDR Block	Enter the destination CIDR block. If you enter an IP address, the network mask /32 is used by default.
Next hop type	Choose a type of the next hop. - ECS instance: routes the traffic destined for the destination CIDR to an ECS instance. - Router interface: routes the traffic destined for the destination CIDR to a router

	interface. Then the router interface will route the traffic to its peer router interface. - VPN gateway: routes the traffic destined for the destination CIDR to the specified VPN gateway.
Next hop	The next hop that receives the routed traffic. **Note**: If you select ECMP-Routing, you must add at least two router interfaces, and the corresponding peer router interface must be a Virtual Boarder Interface (VBR).

Instance management in VPC

Overview

You can directly create a cloud product instance such as ECS, SLB or RDS under a specific VSwitch in the VPC console.

Prerequisite

Ensure that you have created a VPC and VSwitch.

Procedure

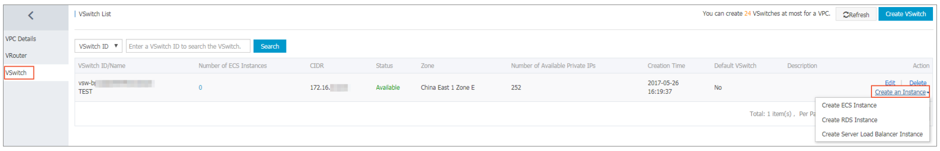
Log on to the VPC console.

In the left-side navigation pane, click **VPC**.

Click a region and then click the ID of the VPC where the VSwitch is created.

On the **VPC Details** page, click **VSwitch**.

Click **Create an Instance** for the target VSwitch, and click the type of instance you want to create.


VPC Details
VRouter
VSwitch
VSwitch List
You can create 24 VSwitches at most for a VPC.
Refresh
Create VSwitch
VSwitch ID ▼
Enter a VSwitch ID to search the VSwitch.
Search
Create ECS Instance
Create RDS Instance
Create Server Load Balancer Instance
Total: 1 item(s) , Per Pa

VSwitch ID/Name	Number of ECS Instances	CIDR	Status	Zone	Number of Available Private IPs	Creation Time	Default VSwitch	Description	Action
vsw-b[redacted] TEST	0	172.16.[redacted]	Available	China East 1 Zone E	252	2017-05-26 16:19:37	No		Edit | Delete Create an Instance

Complete the instance configuration on the corresponding purchase page. After creating a VPC ECS instance, you can change the private IP address and VSwitch of the ECS instance.

After creating a VPC ECS instance, you can change the private IP address and also can change the VSwitch of the ECS instance.

Procedure

Log on to the ECS console.

On the left-side navigation pane, click **Instances**.

Click a region and then click the ID of the target ECS instance.

On the **Instance Details** page, click **Stop** on the upper-right corner.

In the **Configuration Information** panel, click **More** > **Modify Private IP Address**.

In **Modify Private IP Address** dialog, modify the private IP by either of the following ways, and then click **Modify**.

VSwitch: Select a new VSwitch for the ECS instance from the list.

Because each VSwitch in a VPC has a unique CIDR block, the ECS instance's private IP address will be automatically changed along with the change of the VSwitch.

Private IP Address: Enter the new IP address if you do not want to change the VSwitch of the ECS instance.

Restart the ECS instance.

You can migrate an RDS instance from one VPC to another VPC. Firstly, you have to switch the network type of the RDS instance to the classic network, and then switch it to the VPC.

> **Note**:
>
> The VPC switch will cause an ephemeral disconnection for the RDS instance. Ensure that you have set an automatic reconnection mechanism for it.

Procedure

Log on to the RDS console.

Switch the network type to the classic network:

Click the ID of the target RDS instance.

On the left-side navigation pane, click **Database Connection**.

In the **Connection information** section, click **Switch to Classic**.

Click **OK** in the pop-up dialog.

Switch the network type to VPC:

Click **Refresh** to check the database status.

After the network type is changed to the classic network, click **Switch to VPC**.

In the pop-up dialog, select a new VPC and VSwitch for the RDS instance and then click **OK**.

Related operations

Add the new private IP address to the RDS whitelist, see Set whitelist.

Restart the RDS instance.

Currently, the Virtual Private Cloud (VPC) in Alibaba Cloud does not comes with a dedicated resource access management policy. Resource access management in the VPC relies on the access control capabilities of each cloud product. For example, resource access management for ECS is implemented using security groups, and that for SLB and RDS is implemented using whitelists.

ECS security group

A security group is a virtual firewall that provides the stateful packet inspection feature. Security groups are used to set network access control for one or more ECSs. An important means of security isolation, security groups are used to divide security domains on the cloud.

You can use the default security group rules provided by the system to a VPC-type ECS instance. You can change the rules in the default security group but you cannot delete the default security group.

Default security group 1: All outbound access is allowed. Inbound access is allowed from all ICMP ports and TCP ports 22, 3389, 80, and 443.

When you create an ECS instance using a non-default VPC and VSwitch, you can select this default security group rule.

Default security group 2: All outbound access is allowed. Inbound access is allowed from all ICMP ports and TCP ports 22 and 3389.

When you create an ECS instance using a default VPC and VSwitch, you can select this default security group rule.

For more security group configurations, see Security groups.

RDS whitelist

Using the whitelist feature of ApsaraDB for RDS, you can customize IP addresses that are allowed to access the RDS. All access from unspecified IP addresses are denied. When you use the RDS products in a VPC, add the IP address of the ECS to the whitelist for the required RDS so that the ECS can visit the RDS instance.

For more configuration on ApsaraDB for RDS whitelist, see Set whitelist.

SLB whitelist

You can configure the Server Load Balancer (SLB) listener to be only accessible by certain IP address. This configuration applies to scenarios where the application only allows access from certain IP addresses.

SLB is a traffic distribution control service that distributes access traffic to multiple backend ECSs based on forwarding policies. Access is usually available to Internet or intranet users. When the service is available only to specified users, or when only intranet access is available, the whitelist feature can perform effective resource access management on the service. To configure the whitelist, add the user’ s IP addresses or the cloud service IP addresses inside the VPC to be accessed over SLB to the access management whitelist of SLB.

For more SLB whitelist configurations, see Set whitelist access control.

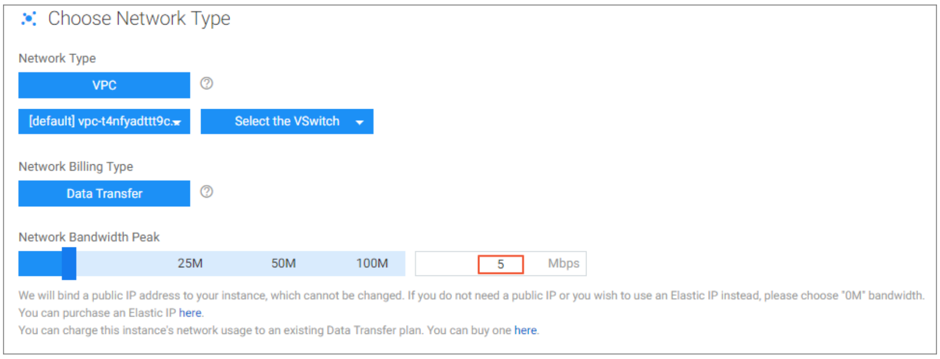
Connections from VPC to Internet

If a VPC ECS instance needs to access the Internet, you can choose to allocate a public IP for it when creating the ECS instance.

As shown in the following figure, after you have chosen the VPC and VSwitch where the ECS instance is created, you have to set a network bandwidth peak. The value must be larger than 0 so that a public IP will be allocated to the ECS instance after it is created.

Note:

> Only when the specified network bandwidth peak is larger than 0, a public IP will be allocated. Otherwise, no public IP is allocated. In this situation, you can bind an Elastic IP to the ECS instance as an alternative.
>
> You cannot unbind the system allocated IP from the ECS instance.



Choose Network Type

Network Type: VPC

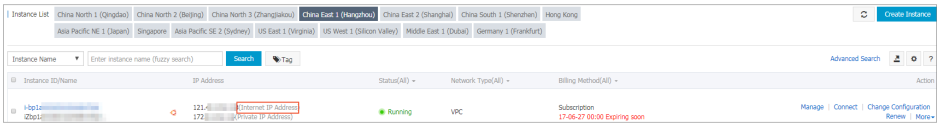
[default] vpc-t4nfyadttt9c. | Select the VSwitch

Network Billing Type: Data Transfer

Network Bandwidth Peak: 5 Mbps

We will bind a public IP address to your instance, which cannot be changed. If you do not need a public IP or you wish to use an Elastic IP instead, please choose "0M" bandwidth.
You can purchase an Elastic IP here.
You can charge this instance's network usage to an existing Data Transfer plan. You can buy one here.

After the ECS instance is created, you can view the public IP on the **Instance List** page. You can use this public IP to access the ECS instance in the public network.



Instance ID/Name	IP Address	Status(All)	Network Type(All)	Billing Method(All)	Action
i-bp1a[redacted] iZbp1[redacted]	121.[redacted](Internet IP Address) 172[redacted](Private IP Address)	Running	VPC	Subscription 17-06-27 00:00 Expiring soon	Manage | Connect | Change Configuration Renew | More

If the ECS instance does not have a system allocated public IP, you can bind an EIP to the ECS instance to access the Internet.

An EIP is a public IP address resource that you can purchase and possess independently. It can be dynamically bound to a VPC ECS instance without restarting the ECS instance. For more details, refer to EIP overview.

Procedure

Log on to the EIP console.

Click **Apply for Elastic IP**.

On the purchase page, configure the EIP and click **Buy Now**.

Go back to the EIP console after completing the purchase, and click **Bind** next to the target EIP.

In the **Bind** dialog, select the ECS instance to be bound and click **OK**.

> **Note**: Ensure the ECS instance is in the Running or Stopped status, and the ECS instance does not have a system allocated public IP or bound with any other EIPs.

After binding an EIP, the ECS instance can access the Internet through the EIP. You can unbind and release the EIP whenever the Internet access is not needed. For details, see Manage an EIP.

NAT Gateway is an enterprise-class public network gateway that provides NAT proxy services (SNAT and DNAT), up to 10 Gbps forwarding capacity, and cross-zone disaster recovery. For more information, see What is NAT gateway.

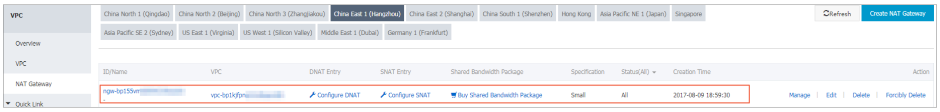
You can provide proxy services that access the Internet by using the SNAT feature of the NAT gateway for ECS instances that do not have public network IP in VPC.

Procedure

Log on to the VPC console.

In the left-side navigation pane, click **NAT Gateway**. In the upper-right corner of the NAT Gateway page, click **Create NAT Gateway**.

Click **Buy Now** and complete the creation.



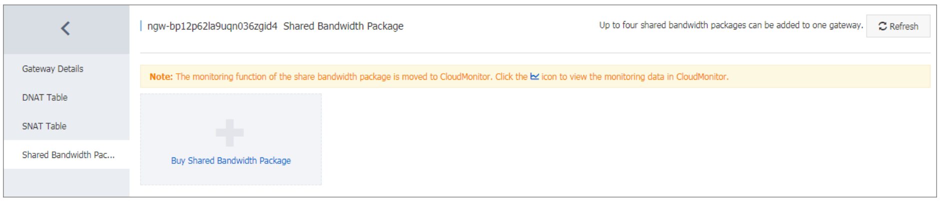
ID/Name	VPC	DNAT Entry	SNAT Entry	Shared Bandwidth Package	Specification	Status(All)	Creation Time	Action
ngw-bp155vm[redacted] -	vpc-bp1kjfpn[redacted]	Configure DNAT	Configure SNAT	Buy Shared Bandwidth Package	Small	All	2017-08-09 18:59:30	Manage | Edit | Delete | Forcibly Delete

For more information about the billing method of the NAT gateway, see billing.

Find the target NAT gateway, and click the **Buy Shared Bandwidth Package** link.

As a public network gateway, NAT Gateway must have configured with public IPs and bandwidth. The public IPs in the NAT Gateway are abstractly grouped into a shared bandwidth package.

On the **Shared Bandwidth Package** page, click **Buy Shared Bandwidth Package** again.



ngw-bp12p62la9uqn036zgid4 Shared Bandwidth Package

Up to four shared bandwidth packages can be added to one gateway.

Note: The monitoring function of the share bandwidth package is moved to CloudMonitor. Click the icon to view the monitoring data in CloudMonitor.

On the purchase page, configure the purchase information and click **Buy Now** complete the payment.

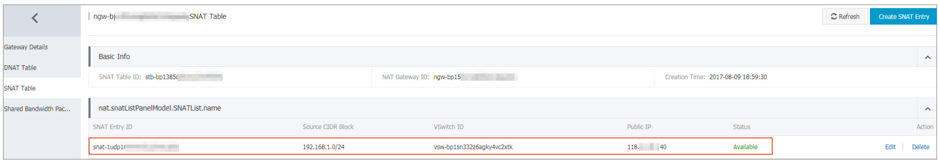
Return to the NAT gateway page, click the NAT gateway ID, and then click **SNAT Table** in the left-side navigation pane.

Click **Create SNAT entry**, configure the SNAT entry according to the following information, Click **Confirm**.

Configuration	Description
VSwtich	The VSwitch of the ECS instances that require the Internet access. By default, all ECS instances in the specified VSwitch can use the specified public IP to access the Internet.

	Note: If an ECS instance has already configured a public IP (such as an EIP), the previously configured public IP for the ECS instance is used to access the Internet, rather than using the SNAT proxy service.
VSwitch CIDR Block	Display the CIDR block of the selected VSwitch.
Public IP	The public IP that is used to access the Internet. **Note**: You cannot use a public IP that has already been added to a DNAT entry.

The status of the added SNAT entry is **Configuring**. Click **Refresh** to refresh the status. When the status is **Available**, the SNAT entry has been successfully added.



ngw-bp[redacted]SNAT Table

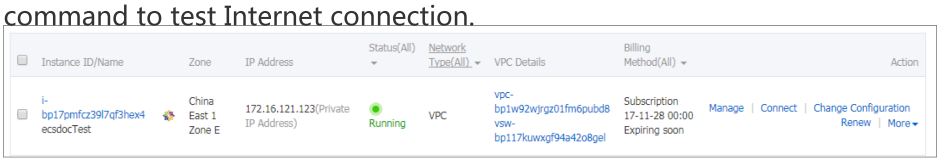
Basic Info

SNAT Table ID: stb-bp1385[redacted] NAT Gateway ID: ngw-bp15[redacted] Creation Time: 2017-08-09 18:59:30

nat.snatListPanelModel.SNATList.name

SNAT Entry ID	Source CIDR Block	VSwitch ID	Public IP	Status	Action
snat-1udp1r[redacted]	192.168.1.0/24	vsw-bp1sn332z6agky4vc2xtk	118.[redacted]40	Available	Edit | Delete

Now the ECS instance can access Internet. Log on to the ECS instance and use the ping command to test Internet connection.



☐	Instance ID/Name	Zone	IP Address	Status(All)	Network Type(All)	VPC Details	Billing Method(All)	Action
☐	i-bp17pmfcz39l7qf3hex4 ecsdocTest	China East 1 Zone E	172.16.121.123(Private IP Address)	● Running	VPC	vpc-bp1w92wjrgz01fm6pubd8 vsw-bp117kuwxgf94a42o8gel	Subscription 17-11-28 00:00 Expiring soon	Manage | Connect | Change Configuration Renew | More

Access from Internet to VPC

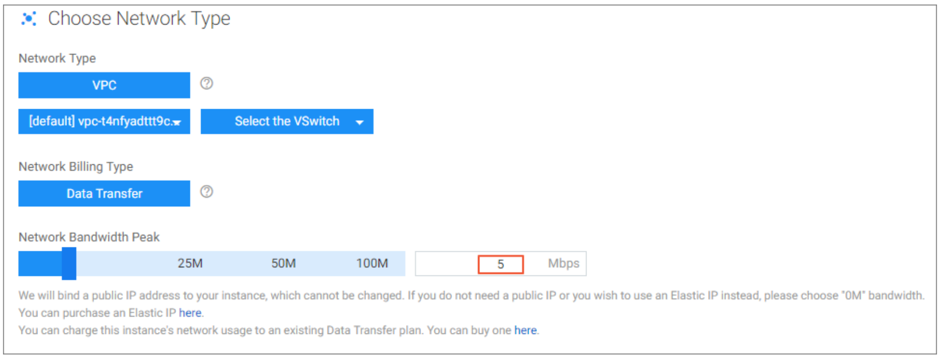
If an ECS instance in a VPC needs to provide external services, you can allocate a public IP for it when creating the ECS instance.

As shown in the following figure, after you have chosen the VPC and VSwitch where the ECS instance is created, you have to set a network bandwidth peak. The value must be larger than 0 so that a public IP will be allocated to the ECS instance after it is created.

Note:

Only when the specified network bandwidth peak is larger than 0, a public IP will be allocated. Otherwise, no public IP is allocated. In this situation, you can bind an EIP to the ECS instance.

You cannot unbind the system allocated IP from the ECS instance.



Choose Network Type

Network Type: VPC

[default] vpc-t4nfyadttt9c

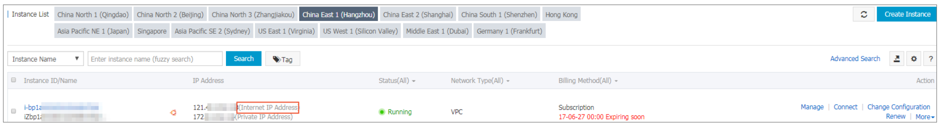
Select the VSwitch

Network Billing Type: Data Transfer

Network Bandwidth Peak: 5 Mbps

We will bind a public IP address to your instance, which cannot be changed. If you do not need a public IP or you wish to use an Elastic IP instead, please choose "0M" bandwidth.
You can purchase an Elastic IP here.
You can charge this instance's network usage to an existing Data Transfer plan. You can buy one here.

After the ECS instance is created, you can view the public IP on the **Instance List** page. You can resolve this public IP to a domain name to provide external services.



Instance ID/Name	IP Address	Status(All)	Network Type(All)	Billing Method(All)	Action
i-bp1a[redacted] iZbp1[redacted]	121.[redacted](Internet IP Address) 172[redacted](Private IP Address)	Running	VPC	Subscription 17-06-27 00:00 Expiring soon	Manage | Connect | Change Configuration Renew | More

If an ECS instance in a VPC needs to provide external services, you can bind an Elastic IP (EIP) to the ECS instance.

An EIP is a public IP address resource that you can purchase and possess independently. It can be dynamically bound to a VPC ECS instance without restarting the ECS instance. For more details, refer to EIP overview.

Procedure

Log on to the EIP console.

Click **Apply for Elastic IP**.

On the purchase page, configure the EIP and click **Buy Now**.

Go back to the Log on to the EIP console after completing the purchase, and click **Bind** next to the target EIP.

In the **Bind** dialog, select the ECS instance to be bound and then click **OK**.

Note: Ensure the ECS instance is in the Running or Stopped status, and the ECS instance does not have a system allocated public IP or is bound with any other EIPs.

After binding an EIP, the ECS instance can access the Internet through the EIP. You can unbind and release the EIP whenever there is no need to provide external services. For details, refer to Manage an EIP.

NAT Gateway is an enterprise-class public network gateway that provides NAT proxy services (SNAT and DNAT), up to 10 Gbps forwarding capacity, and cross-zone disaster recovery. For more information, see What is NAT gateway.

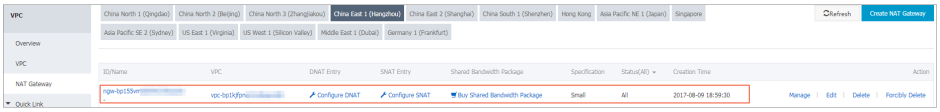
You can use the DNAT function to map a public IP to a private IP. By adding a DNAT entry, the Internet traffic through the public IP is forwarded to the mapped private IP.

Procedure

Log on to the VPC console.

In the left-side navigation pane, click **NAT Gateway**. In the upper-right corner of the NAT Gateway page, click **Create NAT Gateway**.

Click **Buy Now** and complete the creation.



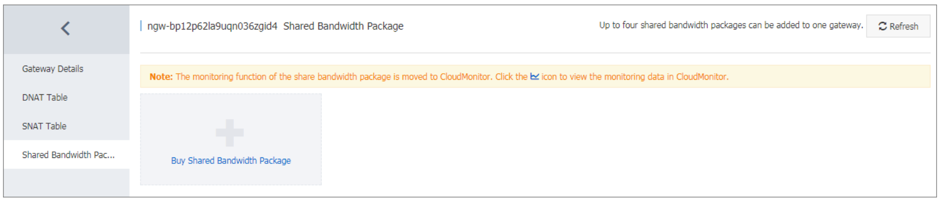
ID/Name	VPC	DNAT Entry	SNAT Entry	Shared Bandwidth Package	Specification	Status(All)	Creation Time	Action
ngw-bp155vm[redacted] -	vpc-bp1kjfpn[redacted]	Configure DNAT	Configure SNAT	Buy Shared Bandwidth Package	Small	All	2017-08-09 18:59:30	Manage | Edit | Delete | Forcibly Delete

For more information about the billing method of the NAT gateway, see billing.

Find the target NAT gateway, and click the **Buy Shared Bandwidth Package** link.

As a public network gateway, the NAT gateway must have configured with public IPs and bandwidth. The public IPs in the NAT Gateway are abstractly grouped into a shared bandwidth package.

On the **Shared Bandwidth Package** page, click **Buy Shared Bandwidth Package** again.



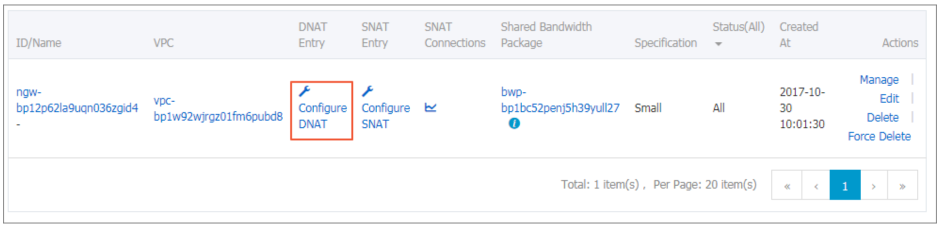
ngw-bp12p62la9uqn036zgid4 Shared Bandwidth Package

Up to four shared bandwidth packages can be added to one gateway.

Note: The monitoring function of the share bandwidth package is moved to CloudMonitor. Click the icon to view the monitoring data in CloudMonitor.

On the purchase page, configure the purchase information and click **Buy Now** complete the payment.

Return to the NAT gateway page, find the target NAT gateway, click **Configure DNAT**.



ID/Name	VPC	DNAT Entry	SNAT Entry	SNAT Connections	Shared Bandwidth Package	Specification	Status(All)	Created At	Actions
ngw-bp12p62la9uqn036zgid4 -	vpc-bp1w92wjrgz01fm6pubd8	Configure DNAT	Configure SNAT		bwp-bp1bc52penj5h39yull27	Small	All	2017-10-30 10:01:30	Manage | Edit | Delete | Force Delete

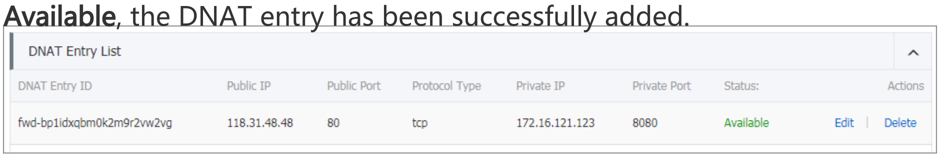
Total: 1 item(s) , Per Page: 20 item(s)

Configure the DNAT entry according to the following information.

Configuration	Description
Public IP	Select a public IP to forward the Internet traffic. **Note**: You cannot use the IP that is already being used in an SNAT entry.
Private IP	The private IP that you want to map. You can specify the private IP in the following ways: - Manually Input: Enter the private IP that you want to map. It must be within the private IP range of the VPC. - Auto Fill: Select an ECS instance in the VPC from the list. The private IP of the selected ECS instance is automatically entered in the field.
Port Settings	DNAT supports IP mapping and port mapping. Select a mapping method: - All Ports: Select this option to configure IP mapping. Using this method, the ECS instance with the specified private IP can receive any Internet requests using any protocol on any port. This is the same as binding an EIP to it.You do not need to configure the public port, private port, and IP protocol

	when configuring IP mapping. - Specific Port: Select this option to configure port mapping. Using this method, the NAT gateway will forward the received data from [ExternalIp:ExternalPort] using the specified protocol to [InternalIp:InternalPort], and send the response in the same.You must specify the public port, private port, and IP protocol when configuring port mapping.

Click **Confirm**. The status of the added DNAT entry is **Configuring**. When the status is **Available**, the DNAT entry has been successfully added.



DNAT Entry List

DNAT Entry ID	Public IP	Public Port	Protocol Type	Private IP	Private Port	Status:	Actions
fwd-bp1idxqbm0k2m9r2vw2vg	118.31.48.48	80	tcp	172.16.121.123	8080	Available	Edit | Delete

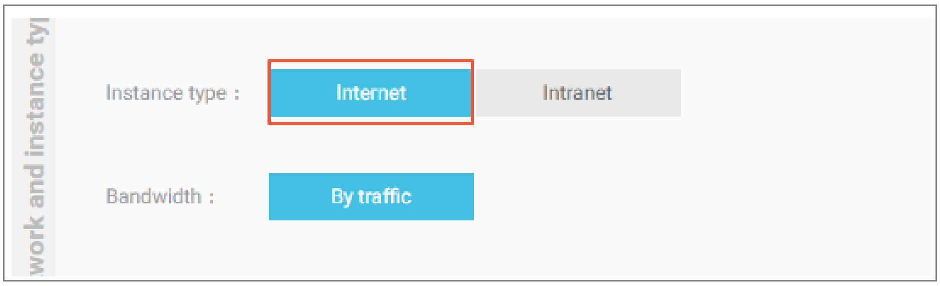
A Server Load Balancer (SLB) is a traffic distribution control service that distributes traffic based on forwarding rules and scheduling algorithms to multiple backend servers. For more information, see What is Server Load Balancer.

You can create an Internet-facing SLB instance, and add VPC ECS instances as the backend servers to process the distributed requests from the Internet. In this way, the VPC ECS instances can provide external services.

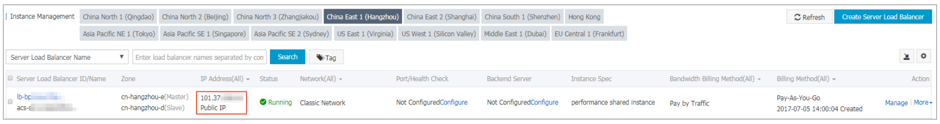
Two ECS instances with Apache static web pages deployed are used in this tutorial.

Procedure

Log on to the Server Load Balancer console and click **Create Server Load Balancer** to create an Internet-facing SLB instance.



A public IP address is allocated to the SLB instance after it is created. You can use this IP address to provide external services.



Instance Management
China North 1 (Qingdao)
China North 2 (Beijing)
China North 3 (Zhangjiakou)
China East 1 (Hangzhou)
China East 2 (Shanghai)
China South 1 (Shenzhen)
Hong Kong
Asia Pacific NE 1 (Tokyo)
Asia Pacific SE 1 (Singapore)
Asia Pacific SE 2 (Sydney)
US East 1 (Virginia)
US West 1 (Silicon Valley)
Middle East 1 (Dubai)
EU Central 1 (Frankfurt)
Refresh
Create Server Load Balancer
Server Load Balancer Name ▾
Enter load balancer names separated by con
Search
Tag

□ Server Load Balancer ID/Name	Zone	IP Address(All)	Status	Network(All)	Port/Health Check	Backend Server	Instance Spec	Bandwidth Billing Method(All)	Billing Method(All)	Action

□ lb-bp[redacted]
acs-s[redacted]
	cn-hangzhou-e(Master)
	cn-hangzhou-d(Slave)
		101.37[redacted]
		Public IP
			✓ Running	Classic Network	Not ConfiguredConfigure	Not ConfiguredConfigure	performance shared instance	Pay by Traffic	Pay-As-You-Go
									2017-07-05 14:00:04 Created
										Manage | More

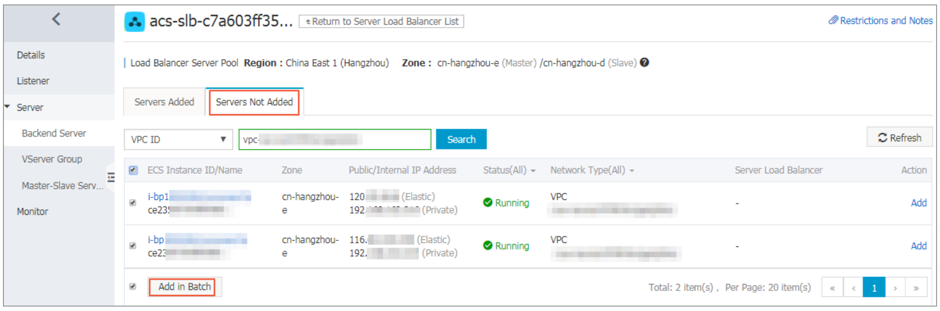
Add backend servers.

Click the ID of the created SLB instance.

In the left-side navigation pane, click **Server** > **Backend Server**.

Click the **Servers Not Added** tab.

Select the checkboxes next to the VPC ECS instances and then click **Add in Batch**. In the pop-up dialog, set the weight to 100 and click **Confirm** to add.



Load Balancer Server Pool **Region :** China East 1 (Hangzhou) **Zone :** cn-hangzhou-e (Master) /cn-hangzhou-d (Slave)

vpc-[redacted]

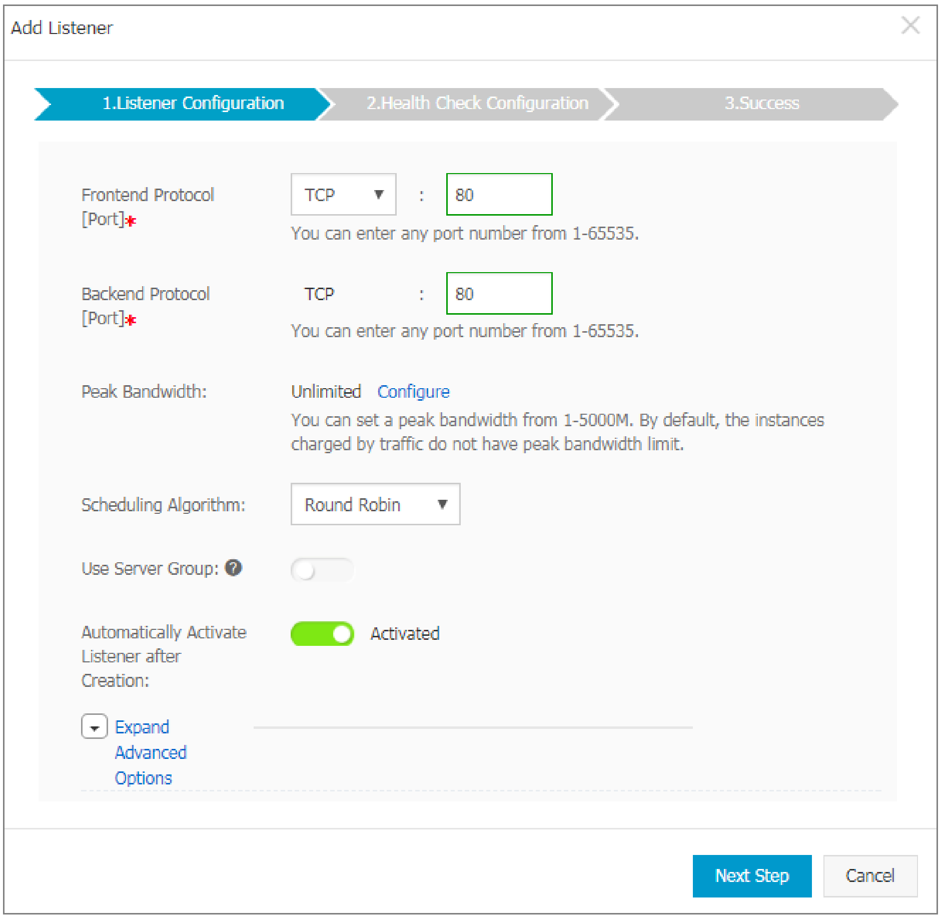
☑ ECS Instance ID/Name	Zone	Public/Internal IP Address	Status(All)	Network Type(All)	Server Load Balancer	Action
☑ i-bp1[redacted] ce23[redacted]	cn-hangzhou-e	120[redacted] (Elastic) 192[redacted] (Private)	✓ Running	VPC [redacted]	-	Add
☑ i-bp[redacted] ce23[redacted]	cn-hangzhou-e	116.[redacted] (Elastic) 192.[redacted] (Private)	✓ Running	VPC [redacted]	-	Add

Total: 2 item(s) , Per Page: 20 item(s) « ‹ 1 › »

Add a listener.

In the left-side navigation pane, click **Listener**, and then click **Add Listener**.

In the **Add Listener** dialog, refer to the following figure to configure the TCP listener.



Add Listener

Frontend Protocol [Port]*: TCP : 80
You can enter any port number from 1-65535.

Backend Protocol [Port]*: TCP : 80
You can enter any port number from 1-65535.

Peak Bandwidth: Unlimited Configure
You can set a peak bandwidth from 1-5000M. By default, the instances charged by traffic do not have peak bandwidth limit.

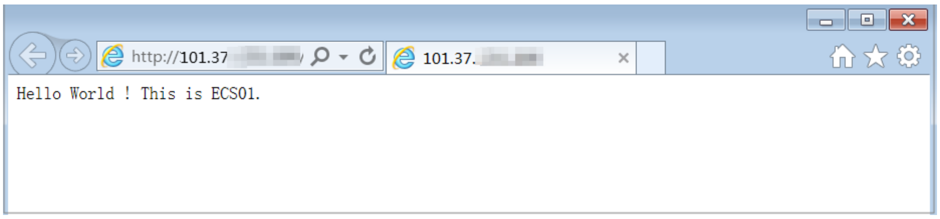
Scheduling Algorithm: Round Robin

Use Server Group:

Automatically Activate Listener after Creation: Activated

Click **Next Step** to configure the health check and select **TCP** with other settings unchanged. Click **Confirm** twice to finish the configuration.

Go back to the Server Load Balancer list page and refresh the page to check the instance status. When the instance is running and the health check is normal, you can use the public IP address of the SLB instance to provide external services.



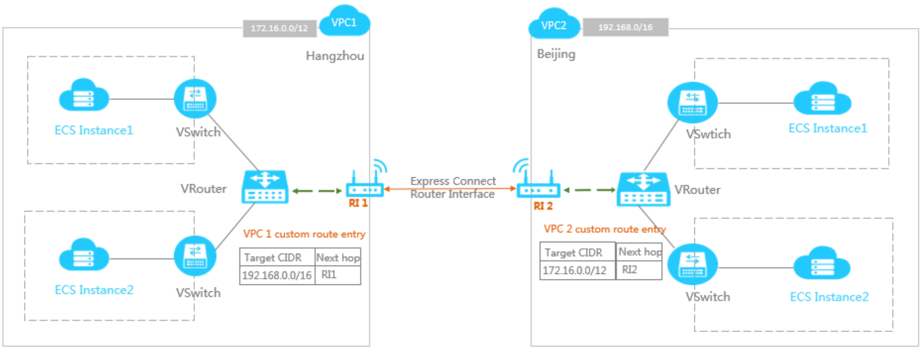
```
Hello World ! This is ECS01.
```

Interconnection between VPCs

Alibaba Cloud Express Connect can establish a dedicated private connection between two VPCs in any regions. The connection does not go through the Internet. This allows Express Connect to offer a fast, stable, secure, and dedicated network communication.

As shown in the following figure, assume that you have two VPCs: VPC1 with the CIDR block 172.16.0.0/16 and VPC2 with the CIDR block 192.168.0.0/16.

To establish a connection between VPC1 and VPC2, you need to use the router interface function of Express Connect. First, create a router interface, and set VPC1 as the initiator and VPC2 as the receiver. Then, add two custom route entries.



- Custom route entry added in VPC1

Destination CIDR	Next hop type	Next hop
192.168.0.0/16	Route interface	RI1

- Custom route entry added in VPC2

Destination CIDR	Next hop type	Next hop
172.16.0.0/12	Route interface	RI2

For more details, refer to:

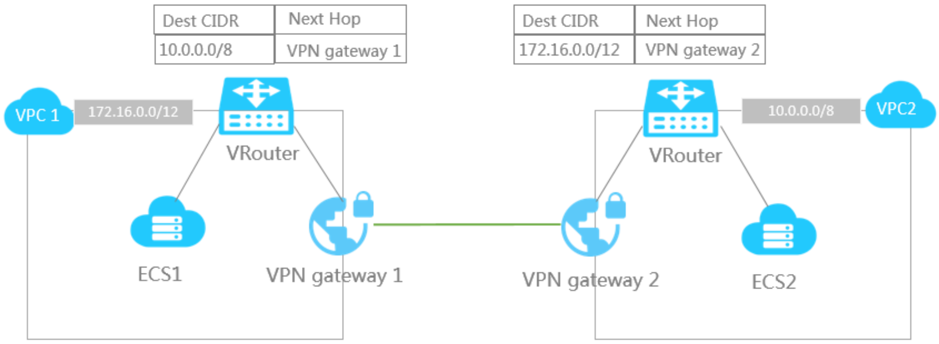
Establish a connection between VPCs under the same account

Establish a connection between VPCs under different accounts

VPN Gateway is an Internet-based service that establishes a safe and reliable connection using a VPN tunnel. You can use VPN Gateway to connect two VPCs quickly.

You can deploy VPN gateways so that the two VPCs can communicate with each other. First create a VPN gateway and a user gateway for each VPC, and then create a VPN connection to establish a VPN tunnel, and finally add a custom route entry in both VPCs. For more information, see Connect two

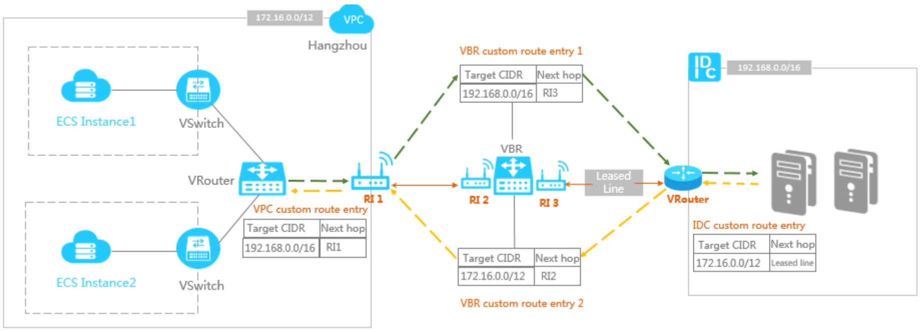
VPCs.



Interconnection between VPC and On-premises IDC

You can use the physical connection function of Express Connect to establish a connection between a VPC and an on-premises IDC.

Assume that you have a VPC with CIDR block 172.16.0.0/12, and an on-premises data center with CIDR block 192.168.0.0/16. When the cloud services needs to access the on-premises data center, you can apply for a leased line to create a connection between them.



Procedure

Apply for a leased line

A leased line is used to connect the IDC with the access point of Alibaba Cloud.

Create a virtual border router

A virtual border router (VBR) is a bridge between the IDC and the VPC for forwarding your data from your VPC to IDC.

After creating the VBR, the system will automatically establish a connection between the router interface (RI3 in the figure) and the IDC through the leased line.

Create a router interface

Create a router interface to connect the VPC and the VBR. When creating the router interface, set the router interface of the VBR as the local side, and the VPC as the peer side.

After creating the router interface, the system will automatically establish a connection between the VPC and VBR through two router interfaces (RI2 and RI3 in the figure).

Add route entries

Finally, you need to add route entries to route the network traffic between the VPC and IDC.

Custom route entries added in VPC

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface	RI1

Custom route entries added in VBR

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Leased line	RI3
172.16.0.0/12	VPC	RI2

Route in IDC

Add a route pointing to the leased line in the IDC router.

For more details, refer to Leased line access.

VPN Gateway is an Internet-based service that establishes a safe and reliable connection between a VPC and your on-premises data centers over an IPsec VPN tunnel.

Plan and preparation

Before deploying a VPN gateway, design your network to connect an on-premises IDC as follows:

The CIDR blocks of the on-premises IDC and VPC cannot be the same.

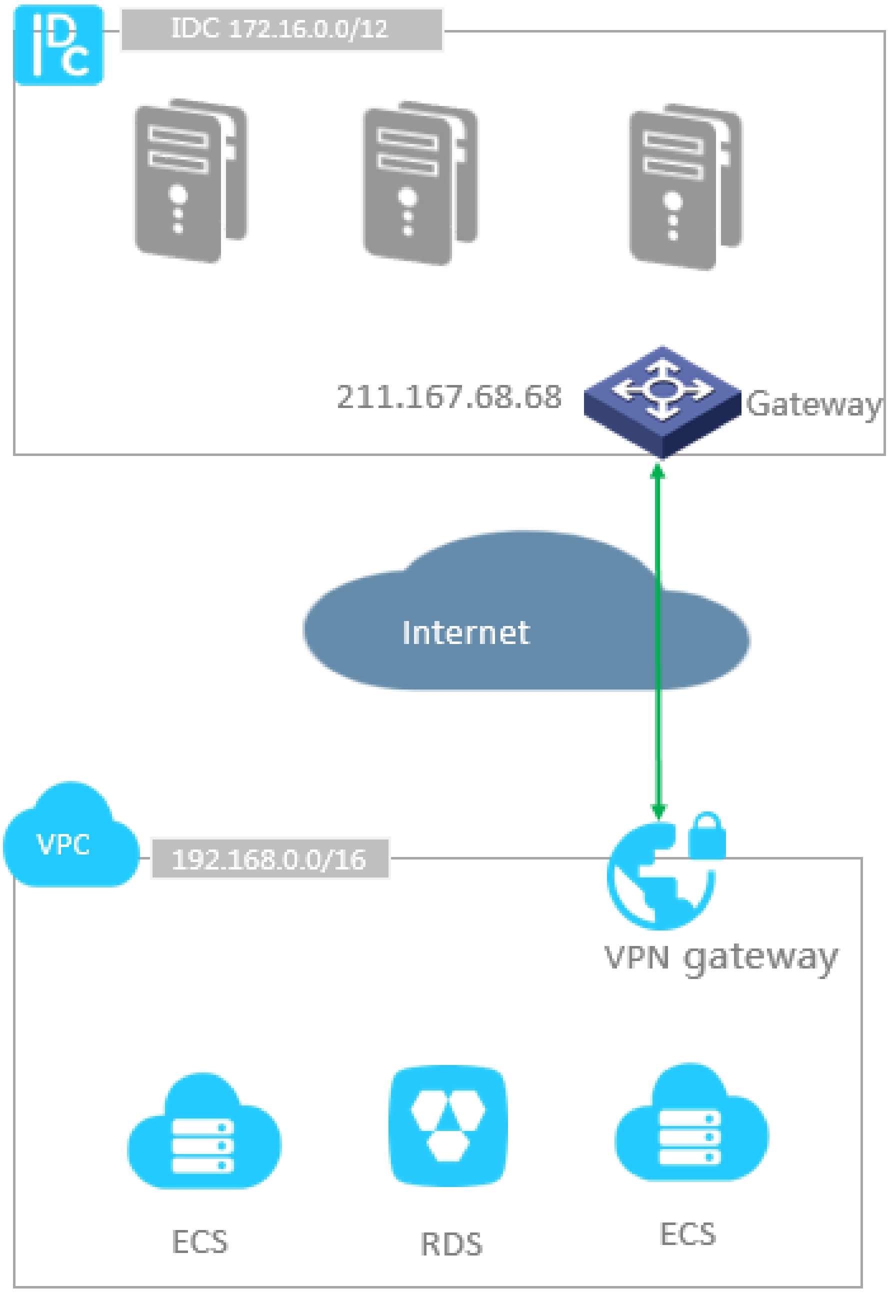
Create a VPC and a VSwitch that the on-premises IDC connects to.

Define which gateway device in the on-premises IDC is used to communicate with the VPC. Alibaba Cloud VPN Gateway supports IKEv1 and IKEv2. Therefore, any gateway device that supports IKEv1 or IKEv2 can be used. For example, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.

Scenario

Follow the tutorial in this document to build a hybrid cloud, using VPN gateway to establish communication between on-premises IDC and VPC through the VPN tunnel.

For this tutorial, assume that the CIDR block for VPC is 192.168.0.0/16, the CIDR block for on-premises IDC is 172.16.0.0/12, and the public IP of the gateway in the on-premises IDC is 211.167.68.68 as shown in the following figure.



Procedure

Step 1: Create a VPN gateway

Create a VPN gateway for the VPC.

Step 2: Create a customer gateway

A customer gateway is the VPN service deployed in the remote network (on-premises data center) of the VPN connection. Creating a customer gateway registers the public IP of the

IDC gateway to the system to establish a connection.

Step 3: Create a VPN connection

Create a VPN connection to connect the VPN gateway with the IDC gateway.

Step 4: Add the VPN connection configuration to the IDC gateway

Register the VPN gateway configuration of the VPC in the IDC gateway.

Step 5: Configure routing

VPN gateway configuration is complete. However, to enable communication with the on-premises IDC, you must add a customer route entry in the VPC.

Step 6: Test connection

Test whether the VPN gateway works.

Create a VPN gateway

Log on to the VPC console.

In the left-side navigation pane, click **VPN** > **VPN Gateway**.

Click **Create VPN Gateway**.

On the purchase page, configure the following:

Configuration	Description
Region	Select the region where the VPN gateway is created. **Note:** The VPN gateway and VPC must be in the same region.
VPC	Select a VPC to create the VPN gateway for.
Peak Bandwidth	Select a peak bandwidth. Two specifications are available, 10 MB and 100 MB.
Billing Method	You are charged based on the actual traffic usage.

Quantity	Select the number of VPN gateways to be created.
Billing Cycle	VPN gateways are billed on an hourly basis.

Click **Buy Now** to activate the VPN gateway service.

Note: The creation of a VPN gateway generally takes 1-5 minutes. A public IP is assigned to the VPN gateway.

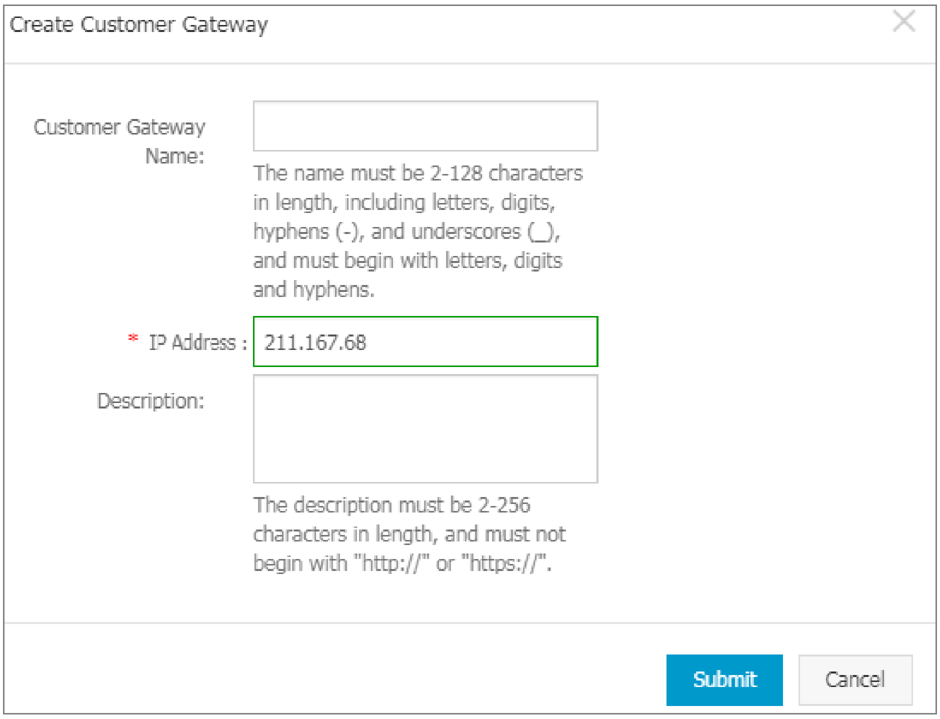
Step 2: Create a customer gateway

Log on to the VPC console.

In the left-side navigation pane, click **VPN** > **Customer Gateway**.

Click **Create Customer Gateway**.

In the **Create Customer Gateway** dialog box, enter the public address for the on-premises IDC gateway, and then click **Submit**.



Create Customer Gateway

Customer Gateway Name:

The name must be 2-128 characters in length, including letters, digits, hyphens (-), and underscores (_), and must begin with letters, digits and hyphens.

* IP Address : 211.167.68

Description:

The description must be 2-256 characters in length, and must not begin with "http://" or "https://".

Step 3: Create a VPN connection

Log on to the VPC console.

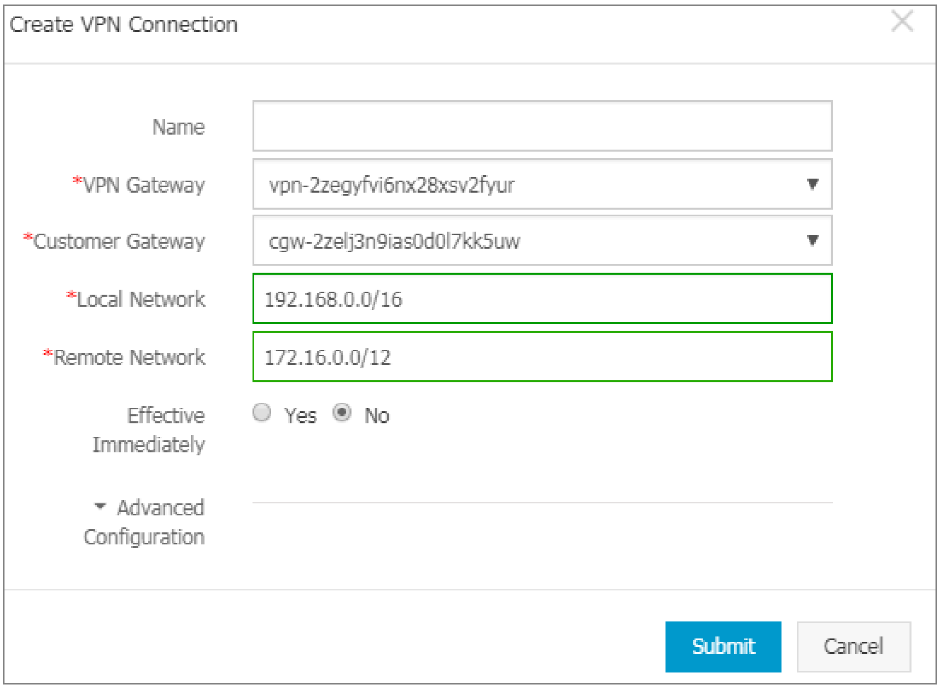
In the left-side navigation pane, click **VPN** > **VPN Connection**.

Click **Create VPN connection**.

In the **Create VPN Connection** dialog box, configure the following, and then click **Submit**.

- **Local Network:** The CIDR block of the VPC. In this tutorial, it is 192.168.0.0/16.

- **Remote Network:** The CIDR block of the on-premises IDC. In this tutorial, it is 172.16.0.0/12.



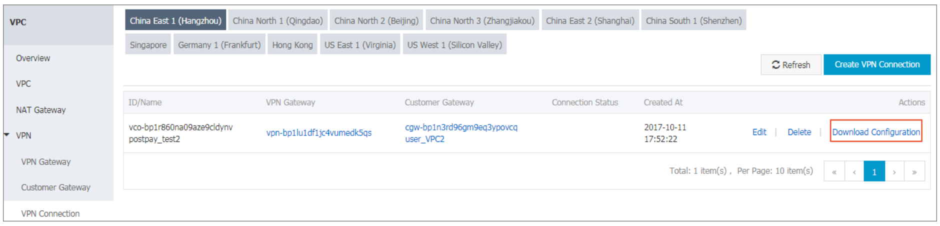
Create VPN Connection

Name	
*VPN Gateway	vpn-2zegyfvi6nx28xsv2fyur ▼
*Customer Gateway	cgw-2zelj3n9ias0d0l7kk5uw ▼
*Local Network	192.168.0.0/16
*Remote Network	172.16.0.0/12
Effective Immediately	○ Yes ● No

Step 4: Add the VPN connection configuration to the IDC gateway

On the VPN Connection page, select a region and find the target VPN connection.

Click **Download Configuration**.

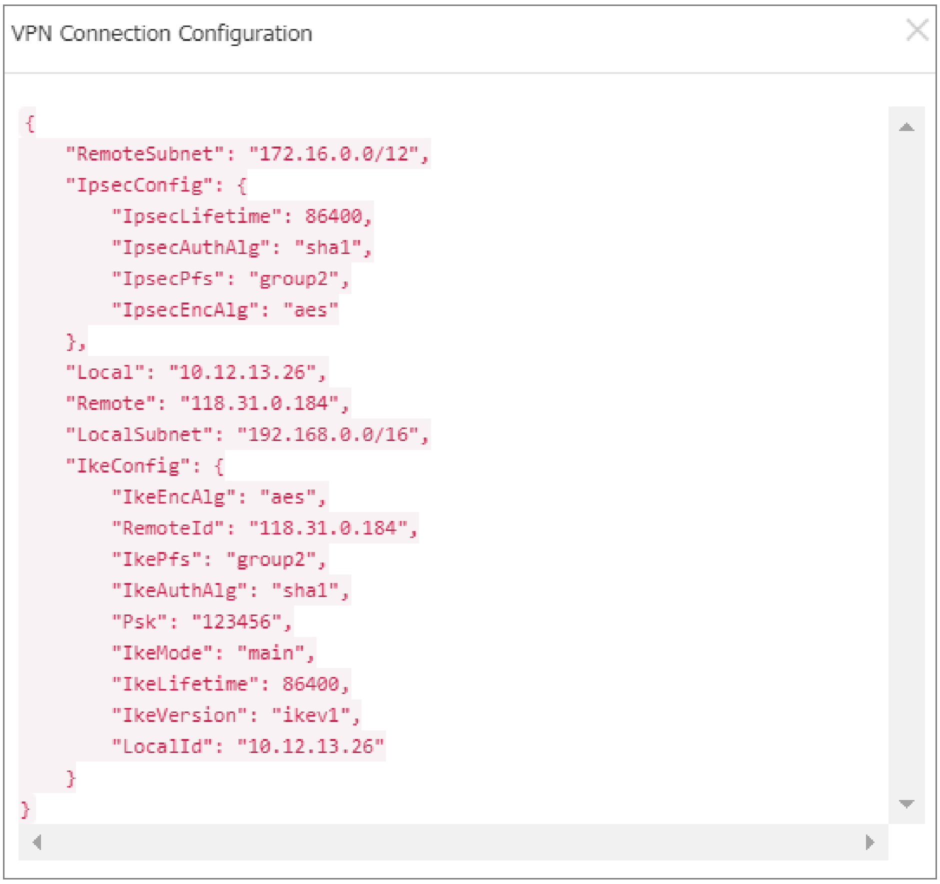


ID/Name	VPN Gateway	Customer Gateway	Connection Status	Created At	Actions
vco-bp1r860na09aze9cldynv postpay_test2	vpn-bp1lu1df1jc4vumedk5qs	cgw-bp1n3rd96gm9eq3ypovcq user_VPC2		2017-10-11 17:52:22	Edit | Delete | Download Configuration

Total: 1 item(s) , Per Page: 10 item(s) « ‹ 1 › »

Configure the on-premises IDC gateway based on the VPN connection configuration.

> **Note:** The RemotSubnet and LocalSubnet in the download configuration are the opposite of the local network and the remote network when creating a VPN connection. From the perspective of VPN gateway, the remote network is the on-premises IDC and the local network is the VPC; while from the perspective of on-premises IDC, the remote network is the VPC and the local network is the on-premises IDC.


VPN Connection Configuration

```
{
    "RemoteSubnet": "172.16.0.0/12",
    "IpsecConfig": {
        "IpsecLifetime": 86400,
        "IpsecAuthAlg": "sha1",
        "IpsecPfs": "group2",
        "IpsecEncAlg": "aes"
    },
    "Local": "10.12.13.26",
    "Remote": "118.31.0.184",
    "LocalSubnet": "192.168.0.0/16",
    "IkeConfig": {
        "IkeEncAlg": "aes",
        "RemoteId": "118.31.0.184",
        "IkePfs": "group2",
        "IkeAuthAlg": "sha1",
        "Psk": "123456",
        "IkeMode": "main",
        "IkeLifetime": 86400,
        "IkeVersion": "ikev1",
        "LocalId": "10.12.13.26"
    }
}
```

Step 5: Configure routing

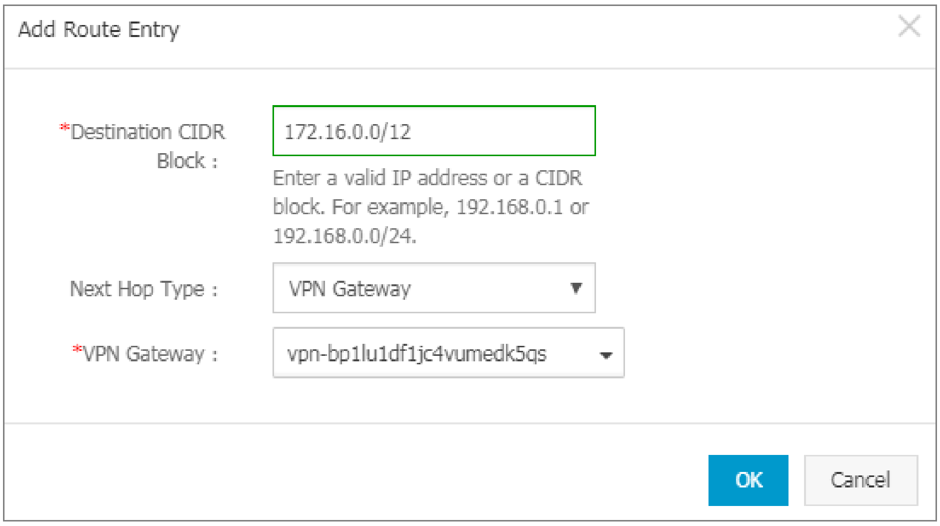
Log on to the VPC console.

In the left-side navigation pane, click **VPC**.

Select the region where the VPC is located and click the ID of the target VPC.

In the left-side navigation pane, click **VRouter**, and then click **Add Route Entry**.

In the **Add Route Entry** dialog box, configure the route entry, and then click **OK**.



Add Route Entry

*Destination CIDR Block : 172.16.0.0/12

Enter a valid IP address or a CIDR block. For example, 192.168.0.1 or 192.168.0.0/24.

Next Hop Type : VPN Gateway

*VPN Gateway : vpn-bp1lu1df1jc4vumedk5qs

Step 6: Test connection

Log on to an ECS instance without a public IP in the VPC, and ping the private IP of a server in the IDC to test the connection.