Alibaba Cloud
Virtual Private Cloud

User Guide

Issue: 20181129

Legal disclaimer

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

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company, or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed due to product version upgrades, adjustments, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and the updated versions of this document will be occasionally released through Alibaba Cloud-authorized channels. You shall pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides the document in the context that Alibaba Cloud products and services are provided on an "as is", "with all faults" and "as available" basis. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not bear any liability for any errors or financial losses incurred by any organizations, companies, or individuals arising from their download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, bear responsibility for any indirect, consequential, exemplary, incidental, special, or punitive damages, including lost profits arising from the use or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.
5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade

secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).

6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 **Danger:** Resetting will result in the loss of user configuration data.
	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 **Warning:** Restarting will cause business interruption. About 10 minutes are required to restore business.
	This indicates warning information, supplementary instructions, and other content that the user must understand.	 **Note:** Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	 **Note:** You can use **Ctrl** + **A** to select all files.
>	Multi-level menu cascade.	**Settings** > **Network** > **Set network type**
Bold	It is used for buttons, menus, page names, and other UI elements.	Click **OK**.
`Courier font`	It is used for commands.	Run the `cd /d C:/windows` command to enter the Windows system folder.
Italics	It is used for parameters and variables.	`bae log list --instanceid` *Instance_ID*
[] or [a|b]	It indicates that it is a optional value, and only one item can be selected.	`ipconfig` *[-all|-t]*
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

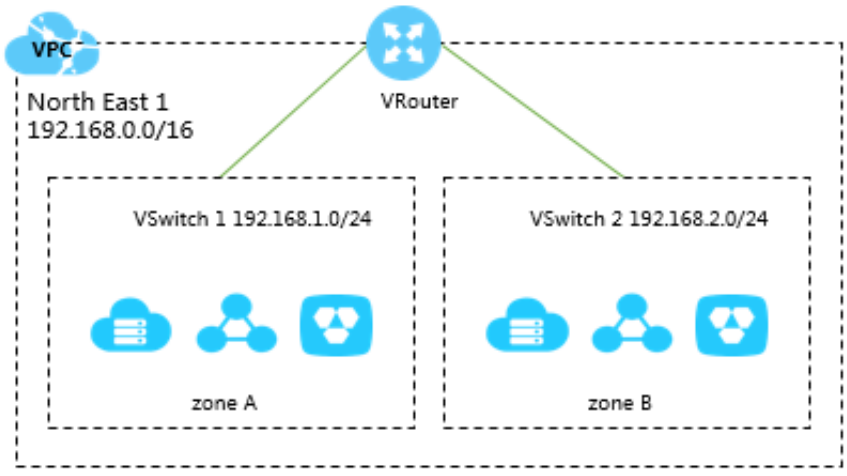
1 Manage a VPC

Virtual Private Cloud (VPC) is a private network dedicated to you in Alibaba Cloud. You have full control over your VPC, such as specifying its IP address range, and configuring route tables and network gateways. You can also use Alibaba Cloud resources such as ECS, RDS, and SLB in your own VPC.

VPC components

VRouter and VSwitch are two basic components of VPC:

- *VRouter* connects VSwitches in a VPC and serves as the gateway connecting the VPC with other networks. A VRouter is automatically created after a VPC is created. Each VRouter associates with a route table. For more information, see *Routing*.
- *VSwitch* is a basic network module in a VPC, used to connect different cloud product instances. After creating a VPC, you can further segment your virtual private network to one or more subnets by creating VSwitches. You can deploy different applications to different VSwitches that are located in different zones to improve the service availability. VSwitches in different zones of a VPC can communicate with each other through the intranet by default. For more information, see *Manage VSwitches*.



IP address range (CIDR block)

When creating a VPC, you must specify the IP address range for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block. Use the following standard private CIDR blocks or

their subsets as the IP address range. The IP address range is related to your network design. For more information, see *Plan and design VPC*.

If you want to use a subset of a standard CIDR block as the IP address range, you must use the *CreateVpc* API to create a VPC.

CIDR block	Number of available private IPs
192.168.0.0/16	65,532
172.16.0.0/12	1,048,572
10.0.0.0/8	16,777,212

Create a VPC and a VSwitch

To deploy cloud resources in a VPC, you must create at least a VSwitch. To create a VPC and a VSwitch, complete these steps:

1. Log on to the *VPC console*.
2. Select the region of the VPC.

   The VPC and the cloud resources to deploy must locate in the same region.
3. Click **Create VPC**, configure the VPC according to the following information and click **OK**.

Configuration	Description
VPC configurations	
Name	Enter a name for the VPC. The name can contain 2 to 128 characters. It must begin with English or Chinese characters and can contain numbers, hyphens (-) and underlines (_).
Destination CIDR Block	Select a CIDR block for the VPC. Limitations on the VPC CIDR blocks are as follows: • You can use the standard CIDR blocks: 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8, or their subsets as the IP address range of the VPC. If you want to use a subnet of a standard CIDR block as the IP address range, you must use the CreateVpc API to create a VPC. • If you want to connect a VPC to another VPC, or to a local network to build a hybrid cloud, it is recommended that you use the subset

Configuration	Description
	of the standard CIDR blocks, and make sure that the network mask is no longer than /16. • If you only have one VPC and it does not need to communicate with your local network, you can use any of the standard CIDR blocks or their subsets. **Note:** After the VPC is created, you cannot change its CIDR block.
VSwitch configurations	
Name	Enter a name for the VSwitch. The name can contain 2 to 128 characters. It must begin with English letters or Chinese characters and can contain numbers, hyphens (-) and underlines (_).
Zones	Select the zone of the VSwitch. In a VPC, VSwitches in different zones can communicate with each other through the intranet.
CIDR Block	Enter the CIDR block of the VSwitch. Note the following when specifying the VSwitch CIDR block: • The CIDR block of the VSwitch can be the same as that of the VPC to which it belongs, or a subset of the VPC CIDR block. For example, if the CIDR block of the VPC is 192.168.0.0/16, the CIDR block of the VSwitch in the VPC can be 192.168.0.0/16, 192.168.0.0/17, …, till 192.168.0.0/29. **Note:** If the CIDR block of the VSwitch is the same as that of the VPC to which it belongs, you can only create one VSwitch in the VPC. • The size of the subnet mask for the VSwitch can be /16 to /29, which can provide 8 to 65536 IP addresses. • The first and last three IP addresses are reserved by the system. Take the IP address range 192.168.1.0/24 as an example, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system.

Configuration	Description
	• Make sure the CIDR block does not conflict with that of the VSwitch in another VPC or the local data center that the VSwitch connects to. **Note:** After the VSwitch is created, you cannot change its CIDR block.

Delete a VPC

Make sure that you have deleted all switches in the VPC. After the VPC is deleted, the associated VRouters and route tables are also deleted.

To delete a VPC, complete these steps:

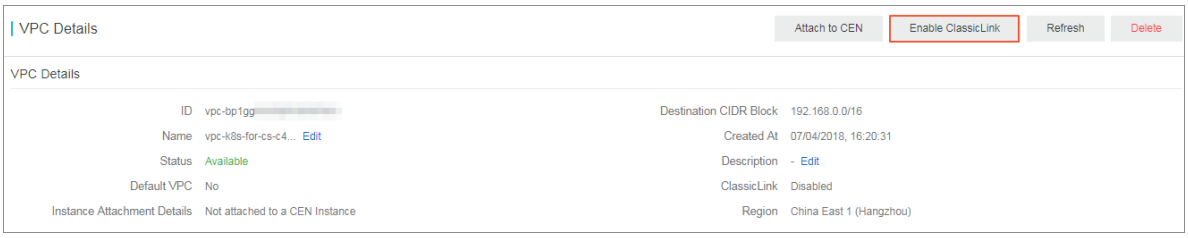
1. On the VPC console, select the region of the VPC.
2. Locate the target VPC and click **Delete**.
3. In the displayed dialog box, click **OK**.

Enable ClassicLink

With ClassicLink, ECS instances in the classic network can communicate with the cloud resource in the connected VPC. For more information, see *ClassicLink overview*.

To enable the ClassicLink function, complete these steps:

1. On the VPC console, select the region of the VPC.
2. Click the ID of the target VPC.
3. On the**VPC Details**page, click**Enable the ClassicLink**.



4. Click **OK**.
5. Create a ClassicLink connection.

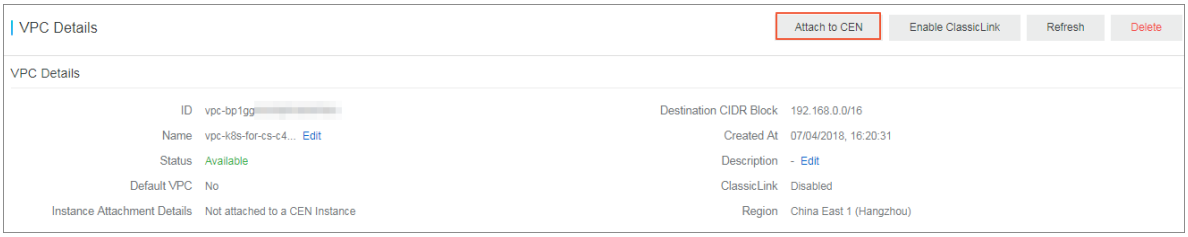
   For more information, see *Build a ClassicLink connection*.

Attach to a CEN instance

You can attach a VPC to a CEN instance, so that the VPC can communicate with other VPCs in the CEN instance or local data centers. For more information, see *What is Cloud Enterprise Network*.

To quickly attach a VPC to a CEN instance in the same account, complete these steps:

1. On the VPC console, select the region of the VPC.
2. Click the ID of the target VPC.
3. On the **VPC Details** page, click **Attach to CEN**.



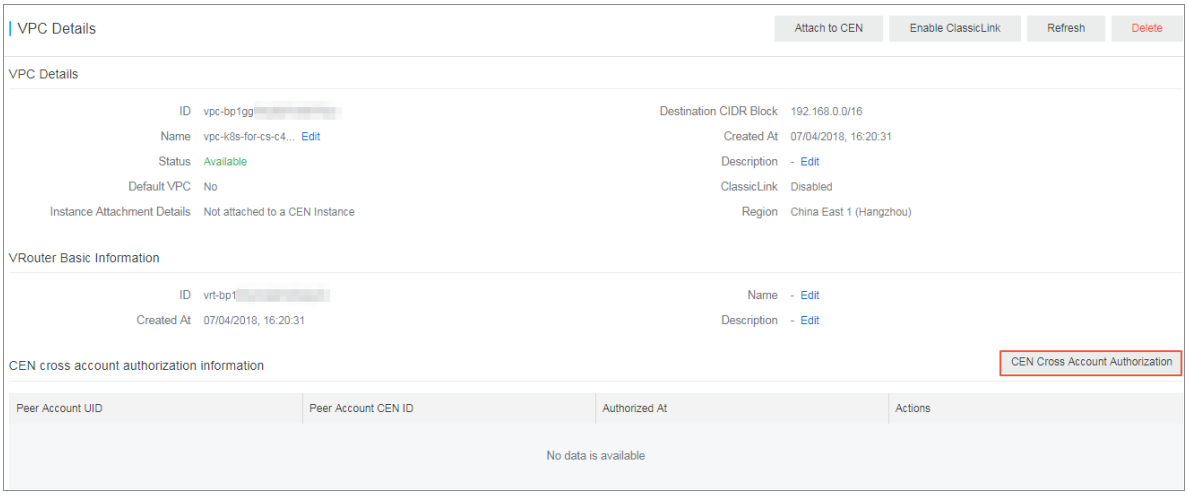
4. Select a CEN instance and click **OK**.

Authorize CEN

If you want the VPC to be attached to a CEN instance in a different account, authorize the CEN instance to attach it.

To authorize a CEN instance in a different account to attach your VPC, complete these steps:

1. On the VPC console, select the region of the VPC.
2. Click the ID of the target VPC to attach.
3. On the **VPC Details** page, click **CEN Cross Account Authorization**.



4. In the **Attach to CEN** dialog box, enter the ID of the account that the CEN instance belongs to and the ID of the CEN Instance, and then click **OK**.

Related APIs

CreateVpc

DeleteVpc

DescribeVpcs

ModifyVpcAttribute

2 Manage VSwitches

A VSwitch is a basic network module in a VPC network, used to connect different cloud product instances in the VPC.

After creating a VPC, you can further segment your virtual private network to one or more subnets by creating VSwitches. The VSwitches within a VPC are interconnected by default. You can deploy different applications to the VSwitches that are located in different zones to improve the service availability.

Note:
A VSwitch does not support multicast or broadcast. You can achieve multicast proxy by using the multicast agent tool provided by Alibaba Cloud. For more information, see *Configure multicast for Linux kernel*.

Create VSwitch

To create a VSwitch, complete these steps:

1. Log on to the *VPC console*.
2. Select the region of the VPC to which the VSwitch belongs.
3. In the left-side navigation pane, click **VSwitches**.
4. Click **Create VSwitch**, configure the VSwitch according to the following information and click **OK**.

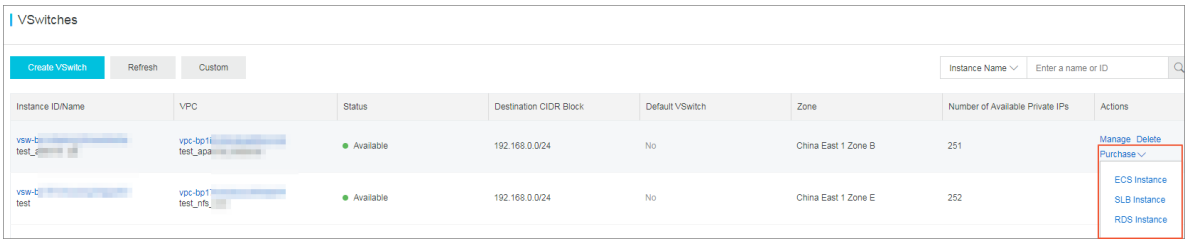
Configuration	Description
VPC	Select the VPC to which the VSwitch belongs.
CIDR Block	Display the CIDR block of the VPC.
Name	Enter the name of the VSwitch. The name can contain 2 to 128 characters. It must begin with English letters or Chinese characters and can contain numbers, hyphens, and underlines.
Zones	Select the zone of the VSwitch. In a VPC, VSwitches in different zones can communicate with each other through the intranet.
Zone Resource	Display the cloud resources that can be used in the selected zone.
CIDR	Enter the CIDR block of the VSwitch. Note the following when specifying the VSwitch CIDR block:

Configuration	Description
	• The CIDR block of the VSwitch can be the same as that of the VPC to which it belongs, or a subset of the VPC CIDR block. For example, if the CIDR block of the VPC is 192.168.0.0/16, the CIDR block of the VSwitch in the VPC can be 192.168.0.0/16, 192.168.0.0/17, …, till 192.168.0.0/29. **Note:** If the CIDR block of the VSwitch is the same as that of the VPC to which it belongs, you can only create one VSwitch in the VPC. • The size of the subnet mask for the VSwitch can be /16 to /29, which can provide 8 to 65536 IP addresses. • The first and last three IP addresses are reserved by the system. Take the IP address range 192.168.1.0/24 as an example, IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved by the system. • Make sure the CIDR block does not conflict with that of the VSwitch in another VPC or the local data center that the VSwitch connects to.
Number of Available Private IPs	Display the number of available private IPs of the VSwitch.
Description	Enter a description of the VSwitch. The name can contain 2 to 256 characters, but cannot begin with `http://` and `https://`.

Create cloud resources in a VSwitch

To create cloud resources in a VSwitch, complete these steps:

1. Log on to the VPC console.
2. Select the region of the VPC.
3. In the left-side navigation pane, click **VSwitches**.
4. Locate the target VSwitch, click **Purchase** and select the cloud resources to create.



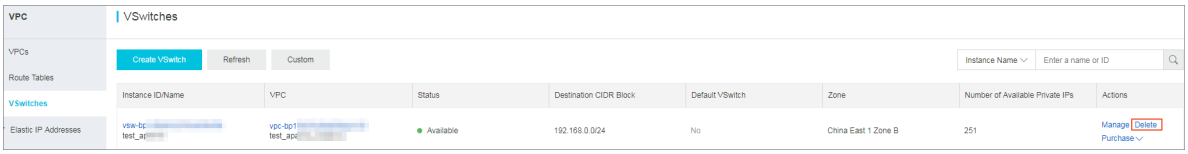
5. Complete the configuration.

Delete a VSwitch

> **Note:**
> Before deleting a VSwitch, make sure that:
>
> - You have deleted all cloud resources in the VSwitch, such as ECS, SLB, and RDS.
> - If the VSwitch has configured an SNAT entry, VPN Gateway, or HAVIP, delete these associated resources.

To delete a VSwitch, complete these steps:

1. Log on to the VPC console.
2. Select the region of the VPC.
3. In the left-side navigation pane, click **VSwitches**.
4. Locate the target VSwitch, and click **Delete**.



5. In the displayed dialog, click **OK**.

Related APIs

CreateVSwitch

DeleteVSwitch

DescribeVSwitches

ModifyVSwitchAttribute

3 Create a default VPC and VSwitch

If there is no available VPC and VSwitch to use when creating a cloud resource with the VPC network, you can choose to use the default VPC and VSwitch. A default VPC and VSwitch are created along with the creation of the instance. This document takes ECS as an example to introduce how to create a default VPC and VSwitch.

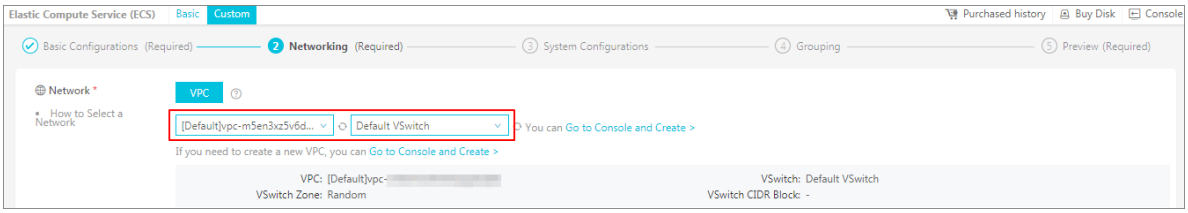
Context

A region can only have one default VPC but many default VSwitches. Because VPC is a region-based resource while VSwitch is a zone-based resource. Each zone can have a default VSwitch. The properties of default VPC and VSwitch are as follows:

Default VPC	Default VSwitch
The default VPC in each region is unique.	The default VSwitch in each zone is unique.
The netmask for a default VPC is /16, such as 172.31.0.0/16, providing up to 65536 private IP addresses.	The netmask for a default VSwitch is /20, such as 172.31.0.0/20, providing up to 4096 private IP addresses.
The default VPC does not take up the VPC quota.	The default VSwitch does not take up the VSwitch quota.
The default VPC is created by the system, and all VPCs created by you are non-default VPCs.	The default VSwitch is created by the system , and all VSwitches created by you are non-default VSwitches.
The operations and specifications for the default VPC and non-default VPCs are the same.	The operations and specifications for the default VSwitch and non-default VSwitches are the same.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, click **Instances** and then click **Create Instance**.
3. Select **Advanced Purchase**.
4. On the **Basic Configurations** page, configure ECS instance and click **Next: Networking**.
5. On the **Networking** page, select **default VPC** and the **default VSwitch**. Click **Next: System Configurations**.



6. Configure the login credential and instance name, and click **Create Order**.

   After the instance is created, a default VPC and a default VSwitch will be created in the region.

Figure 3-1: Default VPC

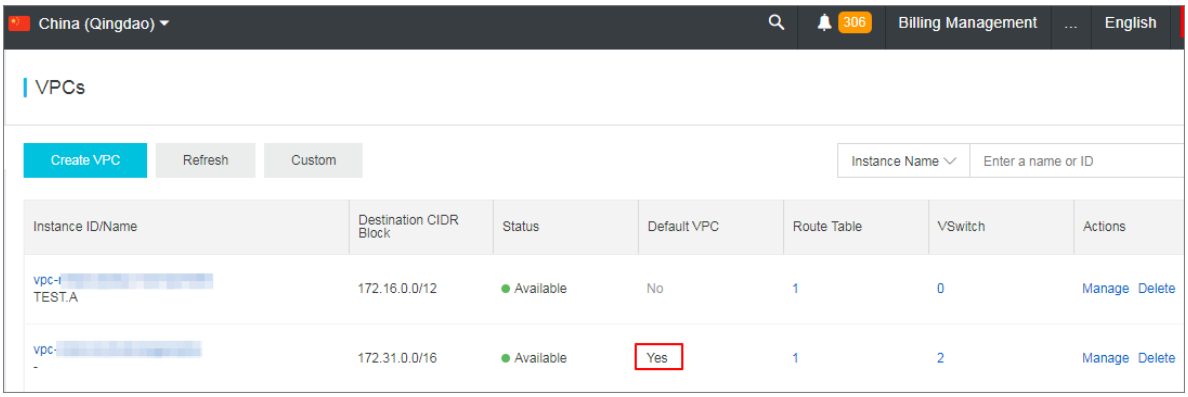
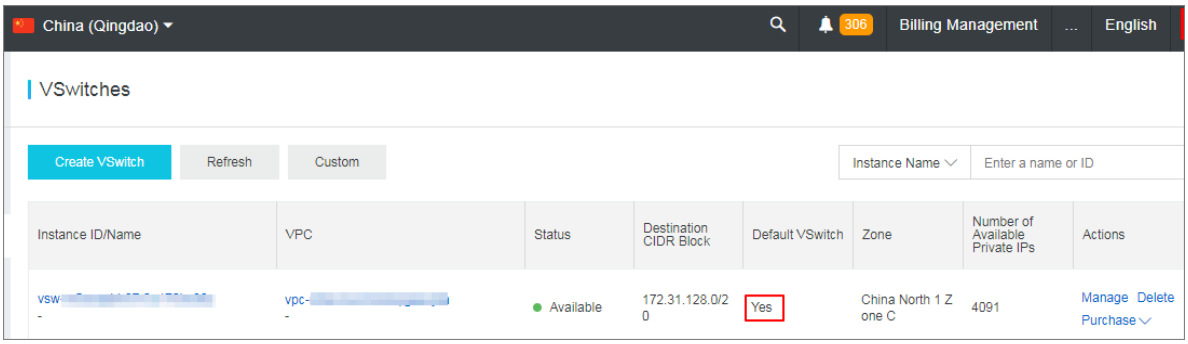


Figure 3-2: Default VSwitch



4 Route table

A route table consists of one or more route entries. Each route entry specifies the destination for the specified traffic. In addition to the default route table, you can create custom route tables for a VPC to route traffic through subnets.

System route table and custom route table

After creating a VPC, Alibaba Cloud automatically creates a route table to control the VPC routing . All VSwitches in the VPC use this route table by default. You cannot create a default route table, nor delete the default route table, but you can create a custom route table and associate it with a VSwitch to control the subnet routing.

Note the following when you manage route tables:

- A VPC can have up to 10 route tables, including the system route table.
- One VSwitch can only associate with one route table. The routing of a VSwitch (subnet) is managed by the route table associated with the VSwitch.
- After a VSwitch is created, the VSwitch is associated with the system route table by default.
- If you want to replace the custom route table associated with a VSwitch with the system route table, unbind the custom route table directly. Then, the VSwtich is automatically associated with the system route table. If you want to replace the custom route table associated with a VSwitch with another custom route table, unbind the custom route table and then associate it with the custom route table that you want to use.
- Currently, customized route tables are available in most regions apart from China (Beijing), China (Hangzhou), and China (Shenzhen) regions.

Create a custom route table

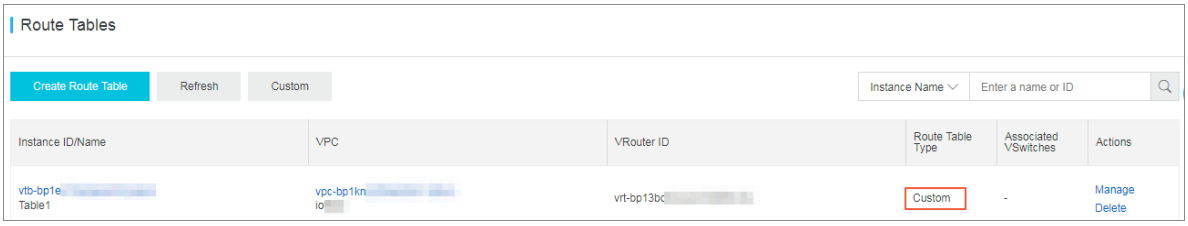
To create a custom route table, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click **Route Tables**.
3. On the **Route Tables** page, click **Create Route Table**.
4. Configure the route table according to the following information, and then click **OK**.

Configuration	Description
Name	Enter a name for the route table.

Configuration	Description
	The name can contain 2 to 128 characters. It must begin with English or Chinese characters and can contain numbers, hyphens (-) and underscores (_).
VPC	Select the VPC that the route table belongs to.
Description	Enter a description for the route table. The description can contain 2 to 256 characters, but cannot begin with `http://` and `https://`.

You can view and manage custom route tables on the **Route Tables** page.

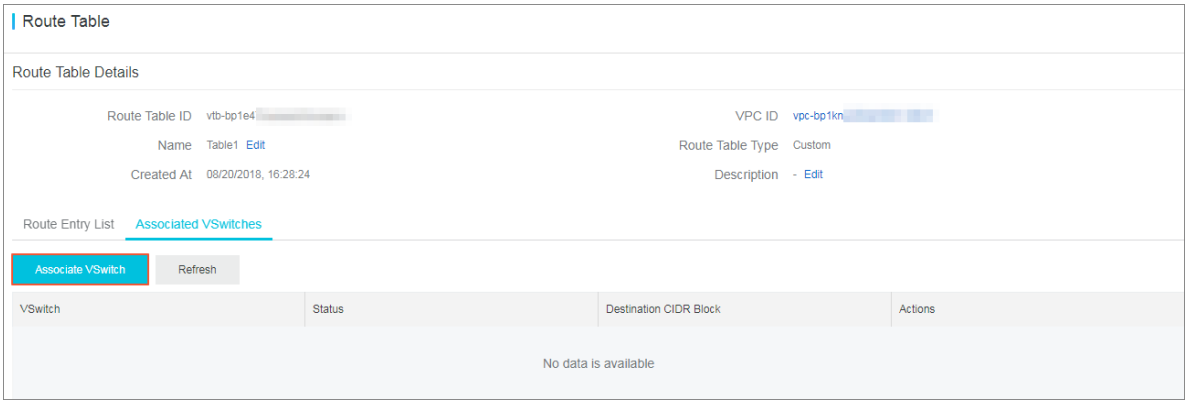


Associate a custom route table with a VSwitch

You can associate a custom route table with a VSwitch to control the traffic through it. A VSwitch can only associate with one route table, including the system route table.

To associate a custom route table with a VSwitch, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click **Route Tables**.
3. On the **Route Tables** page, locate the target custom route table.
4. Click the **Associated VSwitches** tab, and then click **Associate VSwitch**.



5. In the displayed dialog box, select the VSwitch to bind, and then click **OK**.
6. Click the **Route Entry List** tab, add custom route entries.

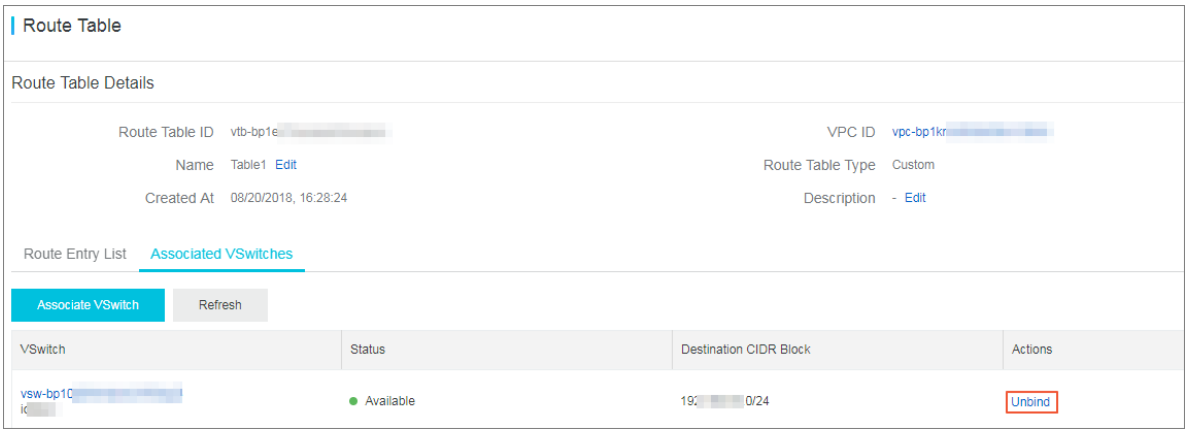
For more information, see *Add custom route entry*.

Unbind a custom route table from a VSwitch

You can unbind a custom route table with a VSwitch. Then the VSwitch uses the default route table if you do not associate it with another custom route table.

To unbind a custom route table from a VSwitch, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click **Route Tables**.
3. On the **Route Tables** page, click the ID of the target custom route table.
4. On the **Associated VSwitches** page, locate the target VSwitch.
5. Click **Unbind**. In the displayed dialog box, click **OK**.



Edit the custom route table

To modify the name and description of a custom route table, complete these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click **Route Tables**.
3. On the **Route Tables** page, click the ID of the target custom route table.
4. In the **Route Table Details** area, modify the name and description accordingly.

Related operations

Add custom route entry

5 Routing

Alibaba Cloud automatically creates a default route table and adds system route entries to it after you create a VPC. You cannot create system route entries, nor delete system route entries, but you can create custom route entries to override system route entries, routing the traffic from specific IP address to the specified destination.

You can add custom route entries to both system route tables and custom route tables. For more information about route tables, see *Route table*.

Each entry in the route table is a *route entry*. A route entry defines the next hop of the network traffic destined for a specific IP address. Route entries include system route entries and custom route entries.

System route entries

The following system route entries are added to the route table after you create a VPC.

- A route entry destined for 100.64.0.0/10. It is used for cloud resource communication in the VPC.
- A route entry destined for the IP address range of a VSwitch. It is used for cloud resource communication in the VSwitch.

For example, you have created a VPC with the IP address range of 192.168.0.0/16, and two VSwitches with the IP address ranges of 192.168.1.0/24 and 192.168.0.0/24. The following system route entries are automatically added to the route table of the VPC:

CIDR Block	Next Hop Type	Type
100.64.0.0/10	-	System
192.168.1.0/24	-	System
192.168.0.0/24	-	System

Custom route entries

You can add custom route entries to override system route entries or route traffic destined for specific IP address range to a target destination. You can specify the following next hop types when creating a custom route entry:

- ECS instance: route traffic destined for a specific IP address range to an ECS instance in the VPC.

Select this type when you want to access the Internet through the application deployed on the ECS instance.

- VPN Gateway: Route traffic destined for a specific IP address range to a VPN Gateway.

  Select this type when you want to connect to a VPC or a local IDC through the VPN Gateway.
- Router Interface (To VPC): Route traffic destined for a specific IP address range to a VPC.

  Select this type when you want to connect two VPCs through router interfaces of Express Connect.
- Router Interface (To VBR): Route traffic destined for a specific IP address range to a VBR.

  Select this type when you want to connect to a local IDC through a dedicated connection of Express Connect.
- Secondary ENI: Route traffic destined for a specific IP address range to a secondary ENI.

Routing rules

The longest prefix match algorithm is used to route traffic when more than one route entries match the destination IP address range. The route entry with the longest subnet mask (the most specific route) is used.

Here is an example of a route table of a VPC.

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	ECS instance	i-12345678	Custom
10.0.0.0/24	ECS instance	i-87654321	Custom

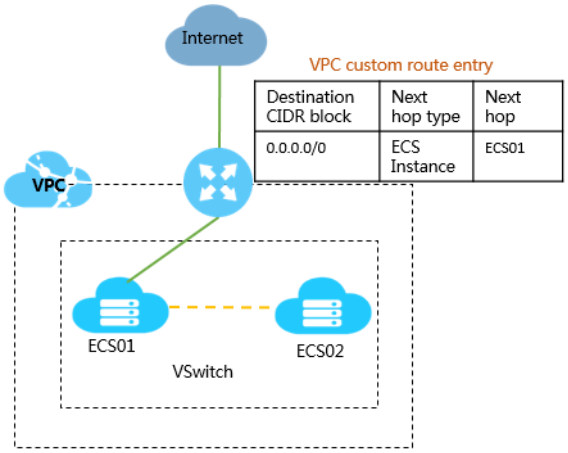
The route entries with the destination of `100.64.0.0/10` and `192.168.0.0/24` are system route entries. The route entries with the destination of`0.0.0.0/0` and `10.0.0.0/24` are custom route entries. Traffic destined for `0.0.0.0/0` will be routed to the ECS instance `i-12345678`, and traffic destined for `10.0.0.0/24` will be routed to the ECS instance `i-87654321`. According to the longest prefix match algorithm, traffic destined for `10.0.0.1` will be routed to the ECS instance `i-87654321`, while traffic destined for `10.0.1.1` will be routed to the ECS instance `i-12345678`.

Routing examples

- Routing within a VPC

  As shown in the following figure, a self-built NAT gateway is deployed on an ECS instance (ECS01), add the following route entry to the route table if you want other ECS instances to access the Internet through this ECS instance:

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



- VPC interconnection (Express Connect)

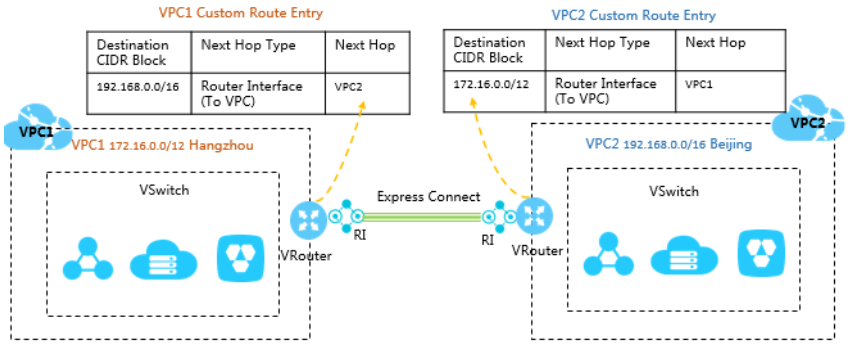
  As shown in the following figure, when using Express Connect to connect VPC 1 (172.16.0.0/12) and VPC 2 (192.168.0.0/16), you must add the following route entries in the VPC after creating route interfaces:

  — Custom route entry added in VPC1

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface (To VPC)	VPC 2

  — Custom route entry added in VPC2

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	Router interface (To VPC)	VPC 1



- VPC interconnection (VPN Gateway)

  As shown in the following figure, when using Express Connect to connect VPC 1 (172.16.0.0/12) and VPC 2 (10.0.0.0/8), you must add the following route entries in the VPC after configuring VPN Gateway:

  - Custom route entry added in VPC 1

Destination CIDR block	Next hop type	Next hop
10.0.0.0/8	VPN metric reference	VPN Gateway 1

  - Custom route entry added in VPC 2

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	VPN metric reference	VPN Gateway 2

- Local IDC connection (Express Connect)

  As shown in the following figure, when using Express Connect to connect a VPC to a local network, you must add the following route entries after configuring the leased line and the VBR:

  — Custom route entry added in VPC

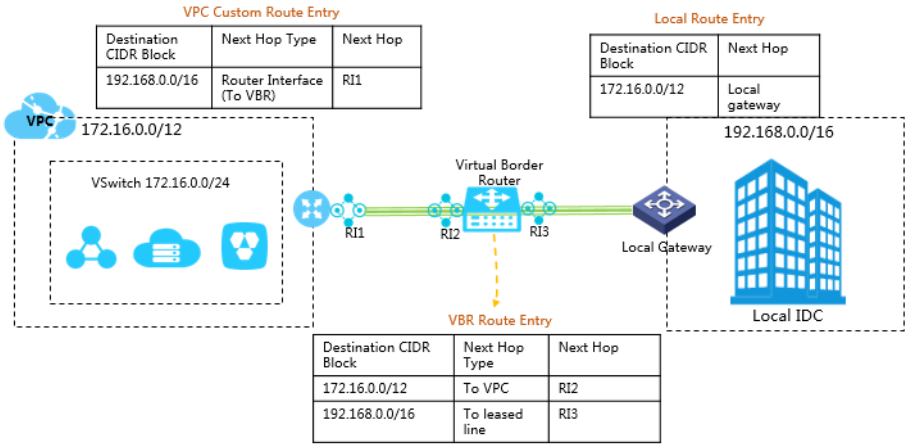
Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface (To VBR/ General Routing)	Router interface (RI 1)

  — Custom route entry added in VBR

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	To leased line	Router interface (RI 3)
172.16.0.0/12	To VPC	Router interface (RI 2)

  — Custom route entry added in the local network

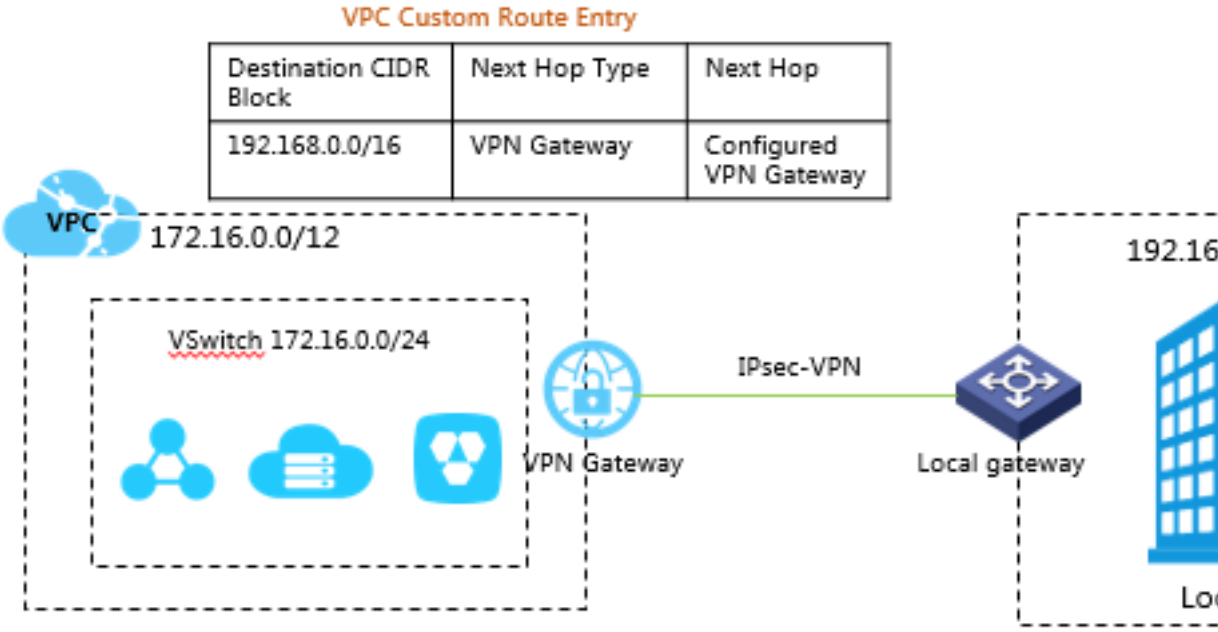
Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	—	Local gateway



- Local connection (VPN Gateway)

  As shown in the following figure, when using a VPN Gateway to connect a VPC (172.16.0.0/12) to a local network (92.168.0.0/16), you must add the following custom route entries:

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	VPN metric reference	VPN Gateway



Add custom route entry

To add a custom route entry, complete these steps:

1. Log on to the *VPC console*.
2. Select the region of the VPC.
3. In the left-side navigation pane, click **Route Tables**.
4. Click the ID of the target route table, and then click the **Route Entry List** tab.
5. Click **Add Route Entry**.
6. In the displayed dialog box, configure the route entry according to the following information and click **OK**.

Configuration	Description
Destination CIDR Block	The traffic from which IP address range to route.
Next hop type and next hop	Select the next hop type and the corresponding next hop: • **ECS Instance**: Route the traffic destined for the specified IP address range to the selected ECS instance. Applicable to the scenario where traffic destined for the specified network is routed to an ECS instance for unified traffic forwarding and management. For example, configure an ECS instance as an Internet gateway to control the Internet access for other ECS instances. • **VPN Gateway**: Route the traffic destined for the specified IP address range to the selected VPN Gateway. • **Secondary ENI**: Route the traffic destined for the specified IP address range to the selected secondary ENI. • **Router Interface (To VPC)**: Route the traffic destined for the specified IP address range to the selected VPC. Applicable to the scenario where Express Connect is used to connect VPCs. • **Router Interface (To VBR)**: Route the traffic destined for the specified IP address range to the selected router interface of which the peer router interface is a VBR.

Configuration	Description
	Applicable to the scenario where Express Connect is used to connect a VPC to a local IDC. You need to further select a routing method when this type is selected: — **General Routing**: Route the traffic to the specified route interface. — **Active/Standby Routing**: Choose two router interfaces as the next hop. The weight for the active route entry is 100 and for the standby route entry is 0. The standby route entry takes over traffic routing when the health check for the active route entry fails. — **Load Balancing Routing**: Choose at least two router interfaces or four router interfaces at most as the next hop. Set a weight value between 1 and 255 for each added route interface. The default value is 100. The weights must be identical. Therefore, the system will distribute the traffic evenly among these router interfaces.

6 VPC connections

Alibaba Cloud provides a lot of connectivity options to you to connect a VPC to the Internet, other VPCs, and local data centers.

Connect to the Internet

The following table lists the products or functions that you can use to connect a VPC to the Internet.

Product	Feature	Benefit
The public IP of an ECS instance of the VPC network	The public IP allocated by Alibaba Cloud when creating an ECS instance of the VPC network. With this public IP, the ECS instance can access the Internet (SNAT) and also can be accessed from the Internet (DNAT).	You can use Data Transfer Plan. After changing a public IP to an EIP, you can also use *Internet Shared Bandwidth*.
Elastic IP Address (EIP)	With an EIP, the ECS instance can access the Internet (SNAT) and also can be accessed from the Internet (DNAT).	You can bind and unbind an EIP from an ECS instance at any time. You can use *Internet Shared Bandwidth* and *Data Transfer Plan* to reduce Internet cost.
NAT Gateway	NAT Gateway is an enterprise-class Internet gateway, supporting multiple ECS instances accessing the Internet with one EIP (SNAT) and being accessed from the Internet (DNAT). **Note:** Compared to Server Load Balancer, NAT Gateway itself does not provide the traffic balancing function.	The core difference between NAT Gateway and EIP is that NAT Gateway supports Internet access of multiple ECS instances but EIP can only be used by an ECS instance.
Server Load Balancer	Port-based load balancing, Server Load Balancer provides Layer-4 (TCP and UDP protocols) and Layer-7 (HTTP and HTTPS protocols) load balancing. Server Load Balancer can forward the client requests from	In DNAT, Server Load Balancer supports forwarding an Internet request to multiple ECS instances. Server Load Balancer is a traffic distribution control service that distributes the incoming traffic among multiple ECS instances according

Product	Feature	Benefit
	the Internet to the backend ECS instances. **Note:** The ECS instance without a public IP cannot access the Internet (SNAT) through Server Load Balancer.	to the configured forwarding rules . It expands application service capabilities and enhances application availability. After binding with an EIP, you can use *Internet Shared Bandwidth* and *Data Transfer Plan* to reduce the Internet cost.

Connect to a VPC

The following table lists the products or functions that you can use to connect a VPC to another VPC.

Product	Feature	Benefit
VPN Gateway	VPN Gateway allows you to create an IPsec-VPN connection to build an encrypted communication between two VPCs. For more information, see *##VPC# VPC##*.	• Low cost, secure and simple configuration. However, the quality of the network depends on the Internet. • IPsec-VPN supports IKEv1 and IKEv2 protocols. Any device that supports these two protocols can connect to Alibaba Cloud VPN Gateway. Supported devices include: Huawei, H3C, SANGFOR , Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.
CEN	CEN allows you to connect VPCs in different regions and different accounts to build an interconnected network. For more information, see *####*.	• Simple configuration, and automatic route learning and distribution. • Low latency and fast speed. • The networks (VPCs/VBRs) attached to a CEN instance are connected with each other.

Product	Feature	Benefit
		• The network connection in the same region is free of charge.

Connect a VPC to a local IDC

The following table lists the products or functions that you can use to connect a VPC to a local IDC.

Product	Feature	Benefit
Express Connect	Express Connect allows you to connect a VPC to a local data center. For more information, see ######.	• Based on the backbone network, low latency. • The leased line access features higher security and reliability, faster speed, and lower latency.
VPN Gateway	• VPN Gateway allows you to create an IPsec-VPN connection to connect a VPC to a local IDC. • Connect multiple local IDCs The VPN-Hub function of VPN Gateway allows you to connect multiple local sites to the VPC. The connected sites can communicate with the VPC, but also can communicate with one another. • Remote access VPN Gateway allows you to create an SSL-VPN connection to let clients access the VPC from a remote computer.	• Low cost, secure and simple configuration. However, the quality of the network depends on the Internet. • IPsec-VPN supports IKEv1 and IKEv2 protocols. Any device that supports these two protocols can connect to Alibaba Cloud VPN Gateway. Supported devices include: Huawei, H3C, SANGFOR, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia. • SSL-VPN connection supports connecting a VPC from a remote computer using the Linux, Windows, and Mac operating systems.

Product	Feature	Benefit
CEN	• Connect to a local data center CEN allows you to attach the VBR associated with a local data center to a CEN instance to build an interconnected network. • Connect multiple VPCs with local IDCs CEN allows you to attach multiple networks (VPC/VBR) to a CEN instance. All the attached networks are connected with one another.	• Simple configuration, and automatic route learning and distribution. • Low latency and fast speed. • The networks (VPCs/VBRs) attached to a CEN instance are connected with one another. • The network connection in the same region is free of charge.
Smart Access Gateway	• Smart Access Gateway allows you to connect local branches to the Alibaba Cloud to build a hybrid cloud for large organizations. • Connect local branches.	• Highly automated configuration , out-of-box experience, and automatically and quickly adapts to network topology changes. • Access is provided from a nearby point within the city over the Internet. Additionally, multiple local branches can access Alibaba Cloud using the Smart Access Gateway devices with master-slave links. • The local branches and the Alibaba Cloud are connected through an encrypted private network and encryption authentica tion is implemented during the Internet transmission.

7 Access control

7.1 Access control

VPC does not comes with an independent access control policy. Access control in the VPC relies on the access control capabilities of each cloud product. For example, ECS instances use security groups to achieve access control, while SLB and RDS use whitelists to achieve access control.

ECS security group

A security group is a virtual firewall that provides the stateful packet inspection feature. A security group is a virtual firewall that provides the stateful inspection packet filtration feature. Security groups are used to set network access control for one or more ECS instances. As an important measure to isolate networks, security groups are used to divide security domains in the cloud.

When you create an ECS instance of the VPC network, you can use the default security group rule provided by the system. You can change the security rules in the default security group but you cannot delete the default security group.

RDS whitelist

You can use the whitelist feature of ApsaraDB for RDS to set IP addresses that are allowed to access the RDS instances. Access from other IP addresses are denied. When using RDS in a VPC, add the IP address of the ECS instance to the whitelist of the RDS so that the ECS instance can access the RDS instance.

SLB whitelist

SLB is a traffic distribution control service that distributes access traffic to multiple backend ECS instances based on forwarding rules. You can configure whitelists for Server Load Balancer listeners thereby only the IP addresses in the whitelists can access the listeners. It is useful when the application only allows access from certain IP addresses.

7.2 ECS security group configurations

When creating an ECS instance of the VPC network, you can use the default security group or other security groups of the VPC. A security group is a virtual firewall to control the inbound and outbound traffic through the ECS instances.

This document lists some common security group scenarios for the ECS instances of the VPC network.

Case 1: Intranet communication

Communication between ECS instances of the VPC network includes the following two kinds:

- Within the same VPC, ECS instances in the same security group can communicate with each other by default.
- Two ECS instances in different VPCs cannot communicate with each other. To achieve communication between the two ECS instances in different VPCs, use Express Connect or VPN Gateway to connect them and make sure that security group rules for the ECS instances allow mutual access, as shown in the following table.

Security group rules	Rule directi	Autho ion policy	Protocol type and port range	Authoriza ion type	Authorization object
Security group configurations for the ECS instance in VPC 1	Inbound	Allow	Windows: RDP 3389/3389	Address field access	Enter the private IP address to access the ECS instance. To allow the access of any ECS instance, enter 0.0.0.0 /0.
	Inbound	Allow	Linux: SSH 22/22	Address field access	
	Inbound	Allow	Custom TCP Custom	Address field access	
Security group configurations for the ECS instance in VPC 2	Inbound	Allow	Windows: RDP 3389/3389	Address field access	Enter the private IP address to access the ECS instance. To allow the access of any ECS instance, enter 0.0.0.0 /0.
	Inbound	Allow	Linux: SSH 22/22	Address field access	
	Inbound	Allow	Custom TCP Custom	Address field access	

Case 2: Deny access of specific IPs or ports

You can configure security groups to deny the access of specific IPs or ports to the ECS instance in a VPC.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Deny access of a specific IP address range to all ports of the ECS instance	Inbound	Drop	All -1	Address field access	Enter the IP address range to block, in the form of CIDR block, such as 10.0.0.1/32.
Deny access of a specific IP address range to port 22 of the ECS instance	Inbound	Drop	SSH (22) 22/22	Address field access	Enter the IP address range to block, in the form of CIDR block, such as 10.0.0.1/32.

Case 3: Allow access of a specific IP

If you have configured a public IP for the ECS instance in a VPC, you can add the following security group rules to allow Windows remote logon or Linux SSH logon.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Allow Windows remote logon	Inbound	Allow	RDP 3389/3389	Address field access	To allow the logon of any public IP address, enter 0.0.0.0/0. To allow only the remote logon of a specific IP address, enter the IP address.
Allow Linux SSH logon	Inbound	Allow	SSH 22/22	Address field access	To allow the logon of any public IP address, enter 0.0.0.0/0. To allow only the remote logon of a specific IP address, enter the IP address.

Case 4: Allow access from the Internet to the HTTP/HTTPS service deployed on the ECS instance

If you have deployed a website on the ECS instance in a VPC and configured an EIP or NAT gateway to provide services, configure the following security group rules to allow access from the Internet.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Allow access to port 80	Inbound	Allow	HTTP 80/80	Address field access	0.0.0.0/0
Allow access to port 443	Inbound	Allow	HTTPS 443/443	Address field access	0.0.0.0/0
Allow access to port 80	Inbound	Allow	TCP 80/80	Address field access	0.0.0.0

8 ClassicLink

8.1 Build a ClassicLink connection

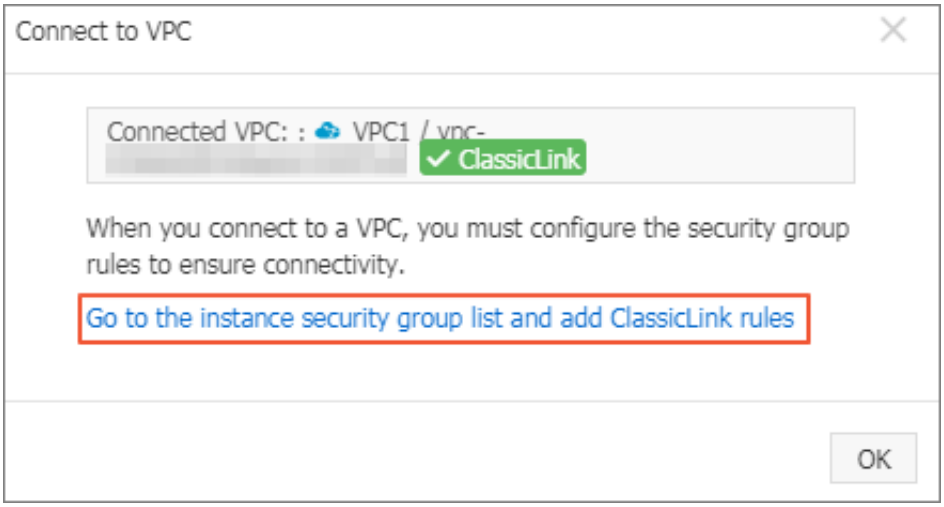
You can set up a ClassicLink connection to let the ECS instance of the classic network access the resources deployed in a VPC network.

Prerequisites

Make sure that you are aware of the limitations of ClassicLink. For more information, see *ClassicLink overview*.

Procedure

1. Log on to the *VPC console*.
2. Select the region of the target VPC, and click the ID of the target VPC.
3. On the **VPC Details** page, click **Enable ClassicLink**. In the displayed dialog box, click **OK**.
4. Go to the ECS console.
5. In the left-side navigation pane, click **Instances**.
6. Select a region, and then locate the target classic ECS instance.
7. Click **More** > **Network and Security Group** > **Connect to VPC**.
8. In the displayed dialog box, select the target VPC and click **OK**. Then click the security group configuration link.



9. Click **Add ClassicLink Rules** and configure the security rule according to the following information. Then, click **OK**.

Configuration	Description
Classic Security Group	Display the classic network security group.
Select VPC Security Group	Select a security group to use. Up to 5 security groups can be selected.
Mode	Select one of the following modes: • Classic <=> VPC: The connected resources can access each other (recommended). • Classic => VPC: Authorize the classic ECS instance to access cloud resources in the connected VPC. • Classic <= VPC: Authorize the cloud resources in the connected VPC to access the classic ECS instance.
Protocol Type and Port Range	Select the protocol and port used for the communication. The port must be in the form of xx/xx. For example, if port 80 is used, enter 80 /80.
Priority	Set the priority for the rule. A smaller number represents a higher priority.
Description	Enter a description for the security rule.

10. On the ECS instances page, click the Column Filter icon on the upper-right corner, and then select the **Connection Status** check box. Click **OK**.

Figure 8-1: Column Filter

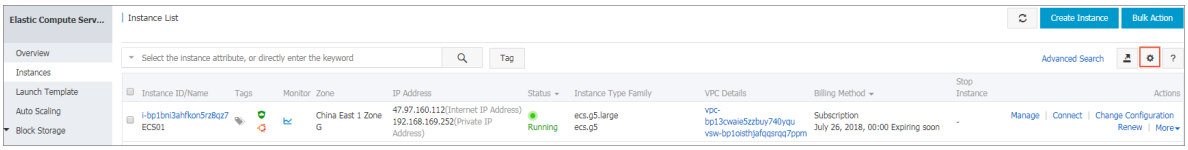


Figure 8-2: Connection Status

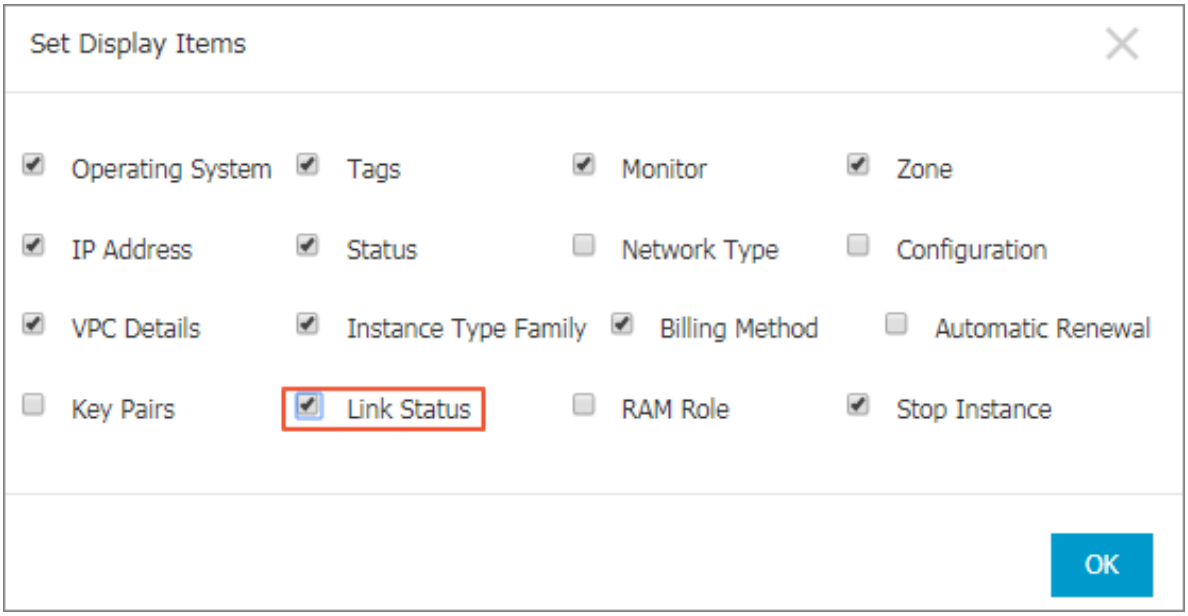
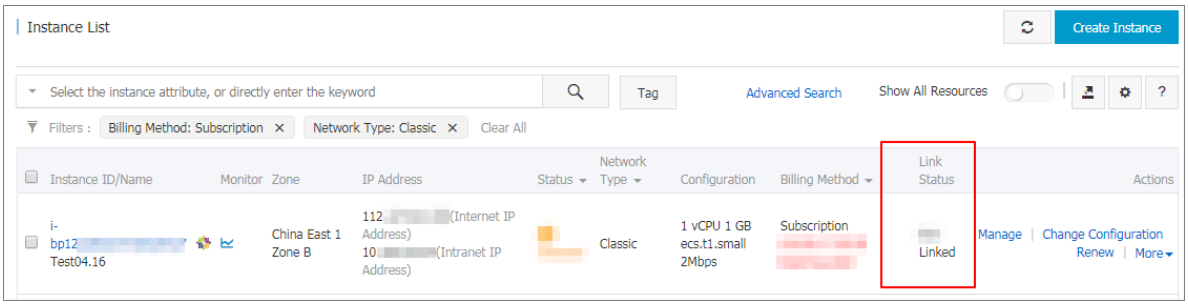


Figure 8-3: Connected to a VPC



8.2 ClassicLink overview

VPC provides the ClassicLink function, allowing you to connect an ECS instance of the classic network to cloud resources in a VPC through the intranet.

Limits

Note the following before using the ClassicLink function:

- Up to 1,000 ECS instances of the classic network can be connected to the same VPC.
- An ECS instance of the classic network can be connected to only one VPC (belong to the same account and the same region).

  For cross-account connection such as connecting an ECS instance of account A to a VPC of account B, the ECS instance can be transferred from account A to account B.

- To enable the ClassicLink function of a VPC, the following conditions must be met:

VPC CIDR block	Limitations
172.16.0.0/12	There is no custom route entry destined for 10.0.0.0/8 in the VPC.
10.0.0.0/8	• There is no custom route entry destined for 10.0.0.0/8 in the VPC. • Make sure that the CIDR block of the VSwitch to communicate with the ECS instance in the classic network is within 10.111.0.0/16.
192.168.0.0/16	• There is no custom route entry destined for 10.0.0.0/8 in the VPC. • Add a route entry, of which the destination CIDR block is 192.168.0.0/16 and the next hop is the private NIC, to the ECS instance of the classic network. You can use the provided script to add the route. Click *Here* to download the route script. **Note:** Before running the script, read the readme file in the script carefully.

Connection scenarios

The following table lists the scenarios of connecting an ECS instance in the classic network to a VPC network.

Network type of the initiator	Region/ account	Network type of the receiver/intranet communication	
		Classic network	VPC
Classic network	Same region Same account	Add a same-account authorization rule in the security group.	Build a ClassicLink connection.
	Same region	Add an across-account authorization rule in the security group.	• Solution A:

	Different accounts		1. Migrate the ECS instance of the classic network to the VPC network 2. Connect the VPCs • Solution B: 1. Transfer the ECS instance of the classic network to the account of the VPC 2. Build a ClassicLink connection
	Different regions Same account	1. Migrate both ECS instances to the VPC network. 2. Connect the two VPCs.	1. Migrate the initiator ECS instance to the VPC network. 2. Connect the two VPCs.
	Different regions Different accounts		
VPC	Same region Same account	Build a ClassicLink connection	Connect the VPCs
	Same-region Cross-account	• Solution A: 1. Migrate the ECS instance of the classic network to the VPC 2. Connect the VPCs • Solution B: 1. Migrate the ECS instance of the classic network to the account of the VPC. 2. Build a ClassicLink connection	
	Cross-region Same-account	1. Migrate the receiver ECS instance of the classic network to the VPC 2. Connect the VPCs	

	Cross-region Cross-account		

Introduction to ClassicLink

The bottom layer implementation of the intercommunication between a classic network and VPC is consistent with that of the intercommunication between two different classic networks. Therefore , the intranet latency and bandwidth limit remain unchanged. Operations like downtime migration , hot migration, stopping, starting, restarting, and system disk replacement will not change the established ClassicLink link.

The classic network and VPC are two different network planes. ClassicLink establishes a private communication channel between these two network planes through routing. Therefore, to use the ClassicLink function, you must plan the network properly to avoid network conflicts.

The IP address range of the classic network in Alibaba Cloud is 10.0.0.0/8 (excluding 10.111.0. 0/16). As long as the IP address range of the VPC does not conflict with 10.0.0.0/8, you can use ClassicLink to establish a private communication. The IP address ranges of the VPC that can communicate with the classic network through ClassicLink are 172.16.0.0/12, 10.111.0.0/16 and 192.168.0.0/16.

Principle of ClassicLink

After an ECS instance of the classic network is connected to a VPC through ClassicLink:

- The ECS instance in the classic network can access the cloud resources in the VPC.

  For example, an ECS instance in the classic network is connected to a VPC of the IP address range 10.0.0.0/8, and the VPC has a VSwitch of the IP address range 10.111.1.0/24. If you have deployed cloud resources such as ECS instances and RDS in the VSwitch, then the ECS instance in the classic network can access these resources through ClassicLink.
- After the ClassicLink connection is successfully established, ECS instances in the VPC can only access the ECS instances in the classic network that is connected to the VPC, and cannot access the ECS instances in the classic network that is not connected to the VPC or other cloud resources in the classic network.

8.3 Cancel ClassicLink connection

You can cancel the ClassicLink connection whenever the intranet connection between an ECS instance of the classic network and a VPC is not needed.

Procedure

1. Log on to the ECS console.
2. In the left-side navigation pane, click **Instances**.
3. Select the region of the instance, and then locate the target instance.
4. Click **More** > **Network and Security Group** > **Disconnect from VPC**.
5. In the displayed dialog box, click **OK**.

8.4 Disable ClassicLink

After cancelling the ClassicLink connection, you can disable the ClassicLink function.

Procedure

1. Log on to the *VPC console*.
2. Select the region of the target VPC and click the ID of the target VPC.
3. On the **VPC Details** page, click **Disable ClassicLink**, and then click **OK** in the displayed dialog box.

9 Configure multicast for Linux kernel

The Linux multicast tool is mainly used in the Alibaba Cloud VPC network and the classic network. A Linux kernel module and a command line are included in the client and server of the multicast tool. The kernel module is used to convert multicast packets and unicast packets to adapt to the current network environment. The command line is used to configure multicast groups.

Prepare the environment

The multicast tool depends on the `kernel-devel` and `rpm-build` packages. Run the following command to check if `kernel-devel` and `rpm-build` are installed:

```
#rpm -qa | grep kernel-devel-`uname -r
#rpm -qa | grep rpm-build
```

If not, run the following command to install:

```
#yum install kernel-devel-`uname -r` -y
#yum install rpm-build -y
```

Install the multicast agent tool

To install the multicast agent tool, complete these steps:

1. Download the multicast agent tool.

   Download address: *https://github.com/aliyun/multicast_proxy*

   Select the *`multicast_kernel`* folder.

2. Run the following command to check the kernel version.

   ```
   uname -r
   ```

   Note: If the kernel version is greater than or equal to 4.0, you need to install a patch by executing the following command in the code directory:

   ```
   patch -p1 &lt; multicast_kernel/patch/kernel_v4.0.patch
   ```

3. Run the following command to generate the installation package.

   ```
   sh tmcc_client_auto_rpm.sh;sh tmcc_server_auto_rpm.sh
   ```

4. Run the following command to install the agent tool.

   ```
   rpm -Uvh multi_server-1.1-1.x86_64.rpm
   ```

```
rpm -Uvh multi_client-1.1-1.x86_64.rpm
```

5. Run the following command to set the auto-startup `multis` and `multic` services.

> **Note:**
> The service is automatically stopped when the agent is stopped.

```
chkconfig multis on --level 2345
chkconfig multis off --level 016

chkconfig multic on --level 2345
chkconfig multic off --level 016
```

Start and stop the agent service

- Start the agent service

  The multicast tool starts the client and the server through the service. The starting process includes loading the kernel module and loading configurations from the configuration files. In this tutorial, JSON format is used to store configuration files.

  > **Note:**
  > Configuration files are not required for the first-time start up. The runtime configuration files are automatically saved.

  — Server (root permission)

  Run **`service multis start`**

  — Client (root permission)

  Run **`service multic start`**

- Stop the agent service

  The stopping process is to save the configuration and uninstall the corresponding kernel module. The configuration is saved as the configuration file for next-time startup by default, that is, the configuration is automatically restored by default when the agent is restarted. If you do not want to save the configuration, clear the configuration using command line before stopping the service.

  — Server (root permission)

  Run **`service multis stop`**

  — Client (root permission)

Run **service multic stop**

- Restart the agent service
  - Server (root permission)

    Run **service multis restart**
  - Client (root permission)

    Run **service multic restart**

Configure the multicast agent by using the script

You can also use the provided script for multicast configuration. Click *Here* to obtain the script.

Note:
We recommend that you use an automated script for multicast configuration. Read the readme before running the script.

Server configuration

You must configure multicast groups on the server and add multicast members to the groups. Each server supports 10 multicast groups. Each multicast group supports 128 server multicast members. The command line is installed under the */usr/local/sbin* directory by default.

Use the **multis_admin** command to configure the server and run **multis_admin -help** to view detailed description.

```
multis_admin -- This command can be used to configure multicast server
.
Usage:
multis_admin -A -m {multi_ip} -j {ip1,ip2,ip3...}
multis_admin -A -m {multi_ip} -q {ip1,ip2,ip3...}
multis_admin -D -m {multi_ip}
multis_admin -C
multis_admin -P -m {multi_ip}
multis_admin -L -m {multi_ip}
multis_admin -S
multis_admin -H
Options:
-A/-- Add add multicast group
-D/--delete del multicast group
-C/--clear clear multicast group
-P/--stats packets statistic
-S/--show show multicast group
-L/--list list multicast group member
-H/--help help info
-j/--join vm join multicast group
-q/--quit vm quit multicast group
```

```
-m/--multiip multicast ip
```

Client configuration

You must configure the information of the multicast groups that the client is added to. A client server can belong to 10 different multicast groups at most.

Configure the client with the multic_admin command, and execute multic_admin-help to view detailed instructions.

```
multic_admin -- This command can be used to configure multicast client
.
Usage:
multic_admin -A -i {ip} -p {port} -m {multi_ip}
multic_admin -D -i {ip} -p {port}
multic_admin -C
multic_admin -P -i {ip} -p {port}
multic_admin -L
multic_admin -H
Options:
-A/--add add multicast server ip and port
-D/--delete del multicast server ip and port
-C/--clear clear multicast server information
-P/--stats recv packets statistic
-L/--list list all multicast server ip and port
-H/--help help info
-i/--ip multicast server ip, the ip of multicast provider
-P/-- Port UDP port, the multicast Port
-m/--multi_ip multicast ip
```