Alibaba Cloud
Virtual Private Cloud

User Guide

Issue: 20190516

Legal disclaimer

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

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

or trust in this document, even if Alibaba Cloud has been notified of the possibility of such a loss.

5. By law, all the content of the Alibaba Cloud website, including but not limited to works, products, images, archives, information, materials, website architecture, website graphic layout, and webpage design, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of the Alibaba Cloud website, product programs, or content shall be used, modified , reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates . The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates).
6. Please contact Alibaba Cloud directly if you discover any errors in this document.

Generic conventions

Table -1: Style conventions

Style	Description	Example
⛔	This warning information indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	⛔ Danger: Resetting will result in the loss of user configuration data.
⚠	This warning information indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	⚠ Warning: Restarting will cause business interruption. About 10 minutes are required to restore business.
📋	This indicates warning information, supplementary instructions, and other content that the user must understand.	❗ Notice: Take the necessary precautions to save exported data containing sensitive information.
	This indicates supplemental instructions, best practices, tips, and other content that is good to know for the user.	📋 Note: You can use Ctrl + A to select all files.
>	Multi-level menu cascade.	Settings > Network > Set network type
Bold	It is used for buttons, menus , page names, and other UI elements.	Click OK.
`Courier font`	It is used for commands.	Run the `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]*

Style	Description	Example
{} or {a|b}	It indicates that it is a required value, and only one item can be selected.	`swich` *{stand | slave}*

Contents

1 VPC and subnets

1.1 Overview of VPC and subnets

This topic describes Alibaba Cloud Virtual Private Clouds (VPCs) and VSwitches (indicated as subnets in this topic). You can create multiple VSwitches to divide a VPC into multiple subnets. By default, VSwitches in a VPC are connected through the intranet.

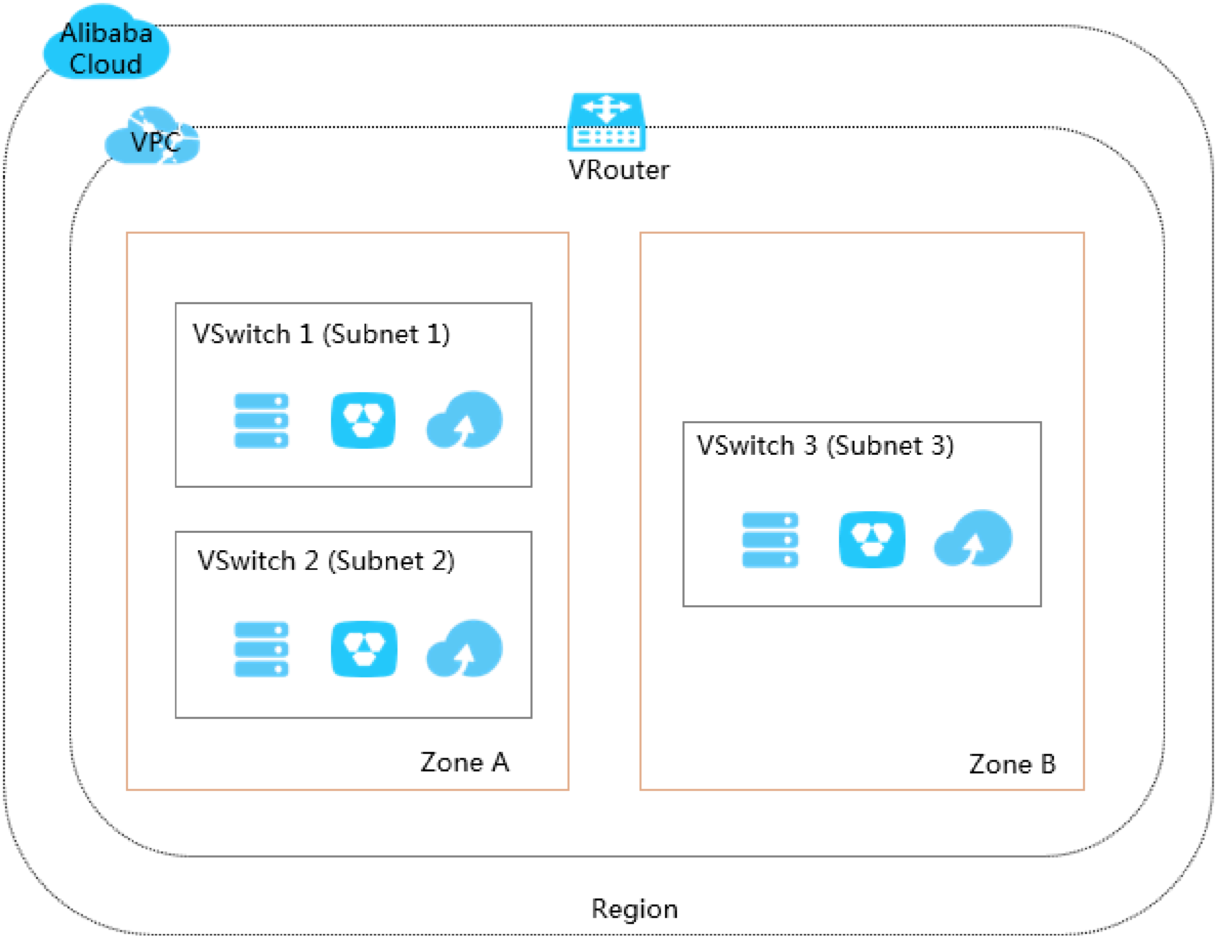
VPC and subnets

VPC is a virtual cloud network dedicated to you. You can deploy cloud products in your VPC.

Note:

You cannot deploy a cloud product in a VPC directly. You must deploy each cloud product in a VSwitch (subnet) of a VPC.

VSwitches are basic network devices that are used to form a VPC and connect different cloud product instances. VPCs are region-level resources. A VPC cannot be used across multiple regions, but it can contain all zones in a region. You can create one or more VSwitches in a zone to divide the zone into multiple subnets.



CIDR blocks and IP addresses

VPCs support both IPv4 and IPv6 addressing protocols. By default, each VPC uses the IPv4 addressing protocol. However, you can enable the IPv6 addressing protocol as needed.

VPCs can operate in dual-stack mode, whereby resources in a VPC can communicat e through IPv4 or IPv6 addresses. However, when you configure routes and security groups for IP addresses, you need to set the routes and security groups for IPv4 addresses and IPv6 addresses separately in a VPC.

The following table lists the differences between an IPv4 address and an IPv6 address.

IPv4 VPC	IPv6 VPC
32 bits, 4 groups. Each group consists of up to 3 numbers.	128 bits, 8 groups, each group consists of 4 hexadecimal numbers.
The IPv4 address protocol is enabled by default.	You can select to enable the IPv6 address protocol.

IPv4 VPC	IPv6 VPC
The size of the VPC CIDR block can range from /8 to /24.	The size of the VPC CIDR block is /56.
The size of the VSwitch CIDR block can range from /16 to /29.	The size of the VSwitch CIDR block is /64.
You can select the IPv4 CIDR block to use .	You cannot select the IPv6 CIDR block to use. The system allocates an IPv6 CIDR block from the IPv6 address pool to your VPC.
All types of instances support the IPv4 protocol.	Some types of instances do not support the IPv6 protocol. For more information, see *Instance type families*.
Configuring ClassicLink is supported.	Configuring ClassicLink is not supported.
Configuring elastic IPv4 addresses is supported.	Configuring elastic IPv6 addresses is not supported.
Configuring VPN Gateway and NAT Gateway is supported.	Configuring VPN Gateway or NAT Gateway is not supported.

By default, both IPv4 and IPv6 addresses of VPC only support intranet communication, which means products under different VSwitches in a VPC can only communicate with each other through the intranet. To connect a VPC to another VPC or an on-premises data center, you need to configure a Smart Access Gateway, Express Connect, a VPN Gateway or another related product to achieve communication. For more information, see *Connect an on-premises data center*.

To enable the VPC to communicate with the Internet, configure the VPC as follows:

- IPv4 Internet communication

  You can associate an EIP or NAT Gateway so that ECS instances in a VPC can communicate through the Internet by using IPv4 addresses.

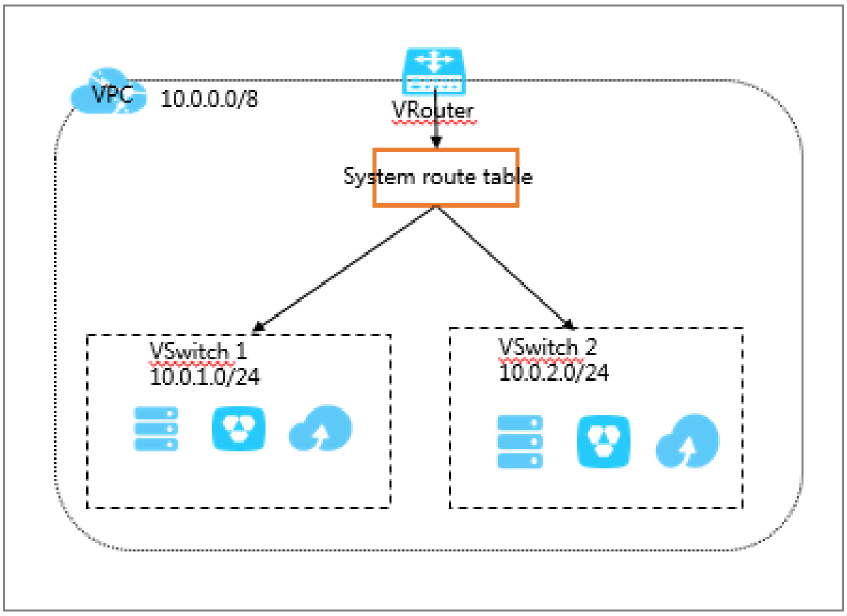
  For more information, see *Attach cloud resources* and *Configure NAT Gateway*.

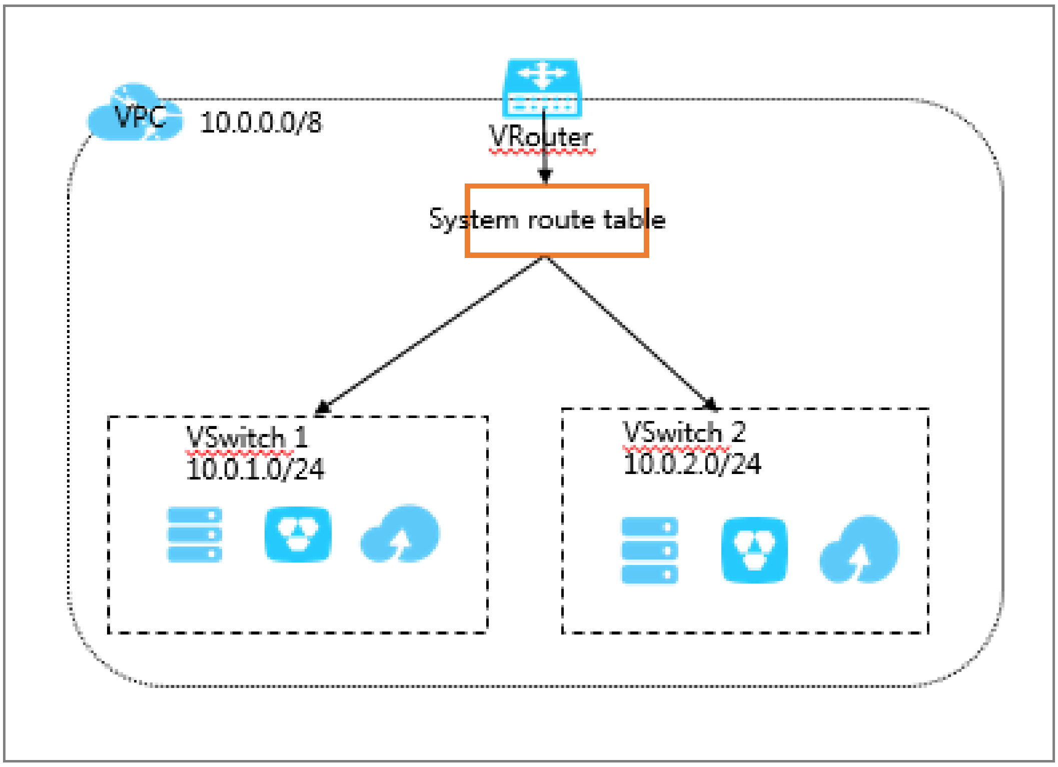
- IPv6 Internet communication

  You need to purchase an Internet bandwidth for the IPv6 address used for communication with the Internet. Then, you can configure an egress-only rule for the IPv6 address, so that cloud products in the VPC can only access the Internet by using the IPv6 address, and IPv6 clients can actively establish connections with other cloud products in the VPC.

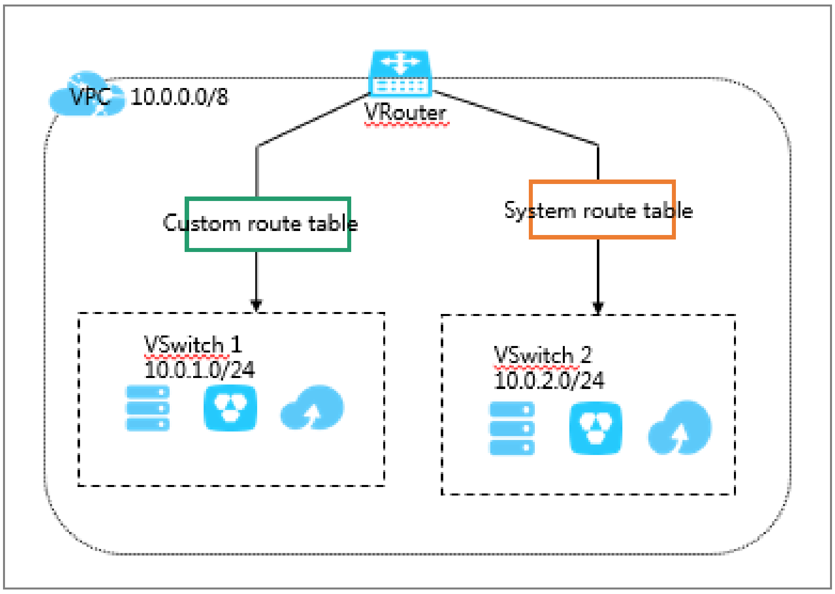
Routes

After a VPC is created, the system automatically creates one default route table (the system route table) and adds system routes to it to manage traffic. You cannot manually create or delete a default system route entry, or delete the system route table.





If you need to add custom subnet routes, you can create a custom route table in a target VPC and attach it to the corresponding VSwitch. Each VSwitch can only be associated with one route table. For more information, see *Manage route tables*.



Route tables implements the longest prefix match algorithm. Therefore, when multiple IP addresses match the destination IP address, the IP address with the longest mask is selected as the next hop. You can also add a custom route entry to route the traffic to the specified IP address. For more information, see *Add a custom route entry*.

1.2 Create a default VPC and VSwitch

If no VPC or VSwitch is available when you create an instance, you can use a default VPC or VSwitch. A default VPC and VSwitch can be created alongside a new instance. This topic describes how to create a default VPC or VSwitch when you create an instance by using an ECS instance as an example..

Context

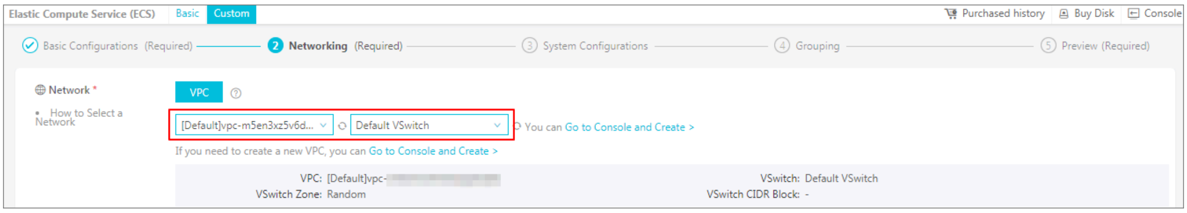
You can create only one default VPC in each region and only one default VSwitch in each zone of a VPC. The following table compares a default VPC with a default VSwitch:

Default VPC	Default VSwitch
The default VPC is unique in each region.	The default VSwitch is unique in each zone.

Default VPC	Default VSwitch
The mask for the default VPC is /16 (for example, 172.31.0.0/16), which provides up to 65,536 private IP addresses.	The mask for the default VSwitch is /20 (for example, 172.31.0.0/20), which provides up to 4,096 private IP addresses.
The default VPC is not included in the VPC quota.	The default VSwitch is not included in 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 the ECS instance and click Next: Networking.
5. On the Networking page, select the default VPC and default VSwitch. Then click Next: System Configurations.



[Default]vpc-m5en3xz5v6d... Default VSwitch

You can Go to Console and Create >

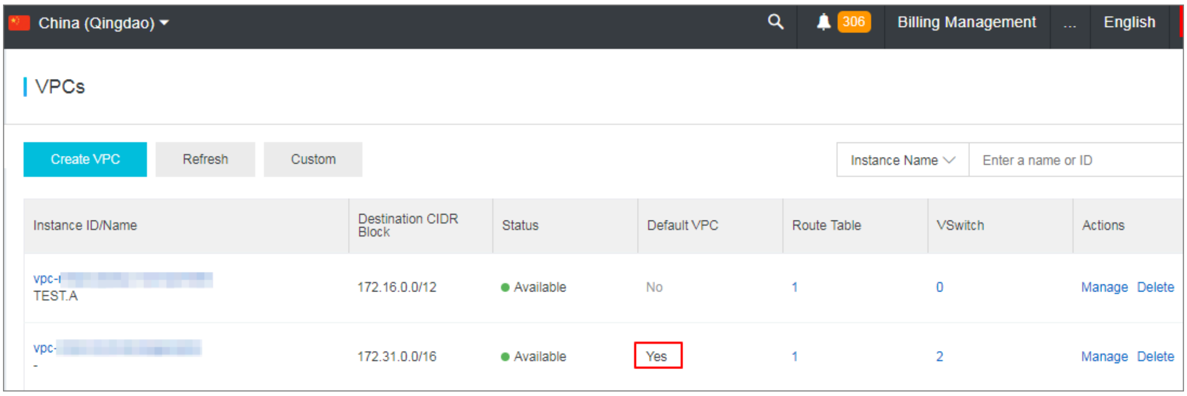
If you need to create a new VPC, you can Go to Console and Create >

VPC: [Default]vpc-[redacted]
VSwitch Zone: Random
VSwitch: Default VSwitch
VSwitch CIDR Block: -

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

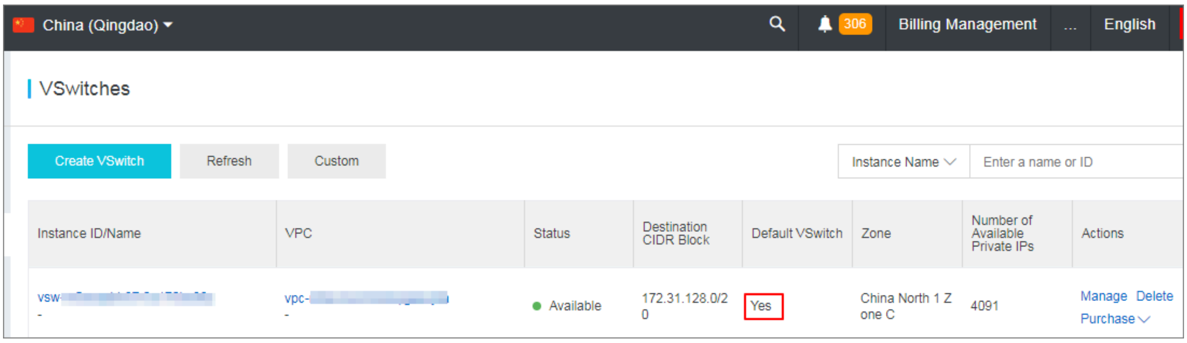
   After the instance is created, a default VPC and a default VSwitch will be created in the region.

Figure 1-1: Default VPC



Instance ID/Name	Destination CIDR Block	Status	Default VPC	Route Table	VSwitch	Actions
vpc-[redacted] TEST.A	172.16.0.0/12	● Available	No	1	0	Manage Delete
vpc-[redacted] -	172.31.0.0/16	● Available	Yes	1	2	Manage Delete

Figure 1-2: Default VSwitch



Instance ID/Name	VPC	Status	Destination CIDR Block	Default VSwitch	Zone	Number of Available Private IPs	Actions
vsw-[redacted] -	vpc-[redacted] -	● Available	172.31.128.0/20	Yes	China North 1 Zone C	4091	Manage Delete Purchase

1.3 Manage a VPC

This topic describes how to manage an Alibaba Cloud Virtual Private Cloud (VPC), including how to create a VPC and a VSwitch, enable ClassicLink, attach a VPC to a CEN instance, and how to delete a VPC.

Create a VPC and a VSwitch

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

1. Log on to the *VPC console*.
2. In the top menu bar, select the region to which the VPC will belong.

   The VPC and the cloud resources to deploy must be located in the same region.

3. Click Create VPC and then configure the VPC according to your requirements. The following table describes VPC configuration items. Then, click OK.

   Note:

   Currently, only the China (Hohhot) region supports enabling IPv6. After IPv6 is enabled, the system creates an IPv6 Gateway.

Configuration	Description
VPC	
Name	Enter a name for the VPC. The name must be 2 to 128 characters in length. It can contain letters, numbers, hyphens (-) and underscores (_) and must begin with a letter.
IPv4 CIDR Block	We recommend that you use an RFC private IP address range as the CIDR block of the VPC. · 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 subnets 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 of the VPC, you must call `CreateVpc` to create a VPC. · If you want to connect a VPC to another VPC, or to an on-premises data center to build a hybrid cloud, we recommend that you use a subnet of the standard CIDR blocks as the CIDR block of the VPC, and make sure that the mask is no longer than /16. · If you only have one VPC and it does not need to communicate with an on-premises data center, you can use any of the standard CIDR blocks or their subnets. Note: After a VPC is created, you cannot change its IPv4 CIDR block.

Configuration	Description
IPv6 CIDR block	Select whether to allocate an IPv6 CIDR block to the VPC. By default, no IPv6 CIDR block is allocated. If you enable IPv6 CIDR blocks, the sysem allocates an IPv6 CIDR block with the mask /56 for your VPC, such as 2001:db8::/56. Note: After the VPC is created, you cannot change its CIDR block.
Description	Enter a description for the VSwitch. The description must be 2 to 256 characters in length and cannot begin with http:// or https://.
Resource Group	Select the resource group to which the VPC belongs.
VSwitch	
Name	Enter a name for the VSwitch. The name must be 2 to 128 characters in length and can contain letters, numbers, hyphens (-) and underscores (_). The name must start with a letter.
Zone	Select the zone of the VSwitch. In a VPC, VSwitches in different zones can communicate with each other through the intranet.

Configuration	Description
IPv4 CIDR Block	Enter the IPv4 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 subnet 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 in the range of 192.168.0.0/16 to 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 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. For example, for the IP address range 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. · Make sure the CIDR block does not conflict with that of the VSwitch in another VPC or the on-premises data center to which the VSwitch connects. Note: After the VSwitch is created, you cannot change its CIDR block.

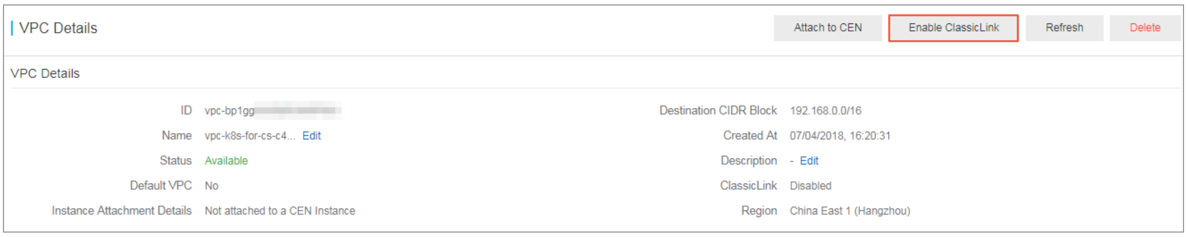
Configuration	Description
IPv6 CIDR Block	The IPv6 CIDR block of the VSwitch. The mask for the IPv6 CIDR block of the VSwitch is /64. You can enter a value from 0 to 255 to define the last 8 bits of the IPv6 CIDR block. If the IPv6 CIDR block of the VPC is 2001:db8::/64 and you enter 255 in the IPv6 CIDR block of the VSwitch (the corresponding hexadecimal representation is ff), the IPv6 CIDR block of the VSwitch is 2001:db8::ff/64. Note: After the VSwitch is created, you cannot change its CIDR block.
Description	Enter a description for the VSwitch. The description must be 2 to 256 characters in length and cannot start with http:// or https://.

Enable ClassicLink

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

To enable the ClassicLink function, follow these steps:

1. Log on to the VPC console.
2. Select the target region and click the ID of the target VPC.
3. In the upper-right corner of the page, click Enable the ClassicLink.



VPC Details

ID vpc-bp1gg[redacted]

Name vpc-k8s-for-cs-c4... Edit

Status Available

Default VPC No

Instance Attachment Details Not attached to a CEN Instance

Destination CIDR Block 192.168.0.0/16

Created At 07/04/2018, 16:20:31

Description - Edit

ClassicLink Disabled

Region China East 1 (Hangzhou)

4. Click OK.

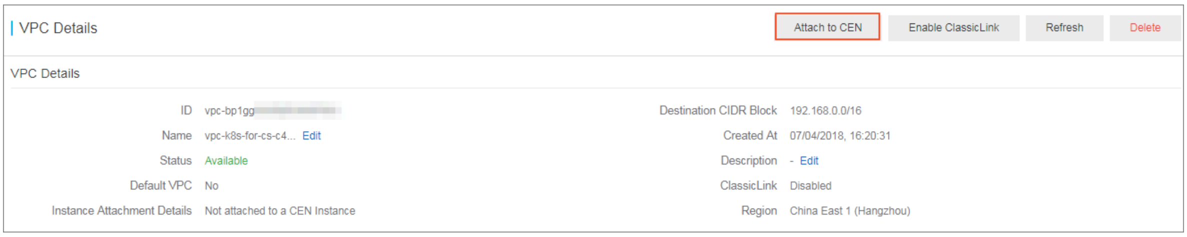
   For more information, see *Build a ClassicLink connection*.

Attach a VPC to a CEN instance

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

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

1. Log on to the VPC console.
2. Select the target region and click the ID of the target VPC.
3. In the upper-right corner of the page, click Attach to CEN.



VPC Details

ID	vpc-bp1gg[redacted]	Destination CIDR Block	192.168.0.0/16
Name	vpc-k8s-for-cs-c4... Edit	Created At	07/04/2018, 16:20:31
Status	Available	Description	- Edit
Default VPC	No	ClassicLink	Disabled
Instance Attachment Details	Not attached to a CEN Instance	Region	China East 1 (Hangzhou)

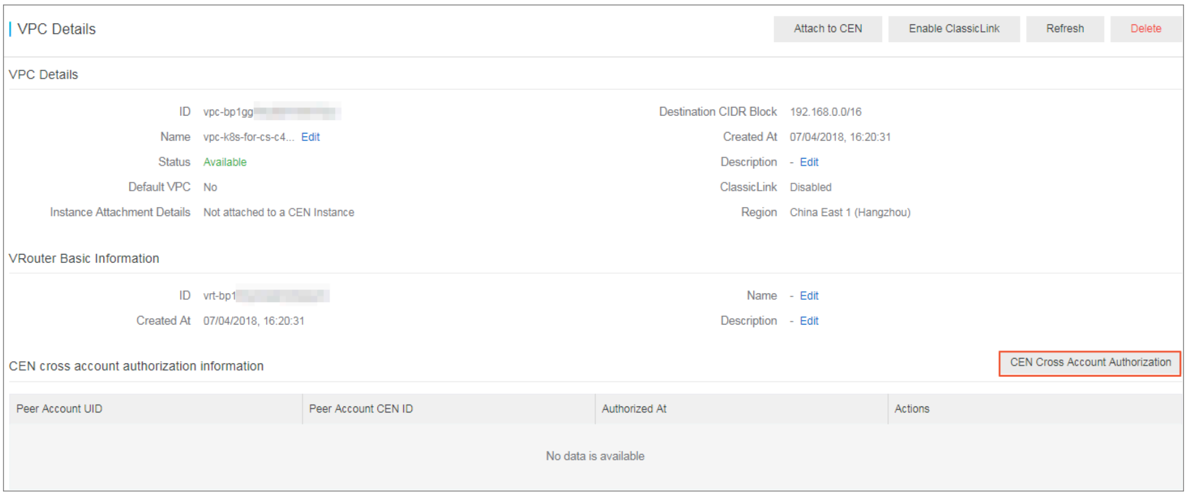
4. Select the target CEN instance and click OK.

Authorize a CEN instance under another account to attach the VPC

If you want to attach the VPC to a CEN instance under a different account, you need to authorize the CEN instance that is to attach it.

To authorize a CEN instance under a different account to attach your VPC, follow these steps:

1. Log on to the VPC console.
2. Select the target region and click the ID of the target VPC.
3. In the CEN cross account authorization information area, click CEN Cross Account Authorization.



VPC Details

ID	vpc-bp1gg[redacted]	Destination CIDR Block	192.168.0.0/16
Name	vpc-k8s-for-cs-c4... Edit	Created At	07/04/2018, 16:20:31
Status	Available	Description	- Edit
Default VPC	No	ClassicLink	Disabled
Instance Attachment Details	Not attached to a CEN Instance	Region	China East 1 (Hangzhou)

VRouter Basic Information

ID	vrt-bp1[redacted]	Name	- Edit
Created At	07/04/2018, 16:20:31	Description	- Edit

CEN cross account authorization information

Peer Account UID	Peer Account CEN ID	Authorized At	Actions
No data is available			

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

Delete a VPC

Before you delete a VPC, make sure that you have deleted all VSwitches in the VPC . Otherwise, the deletion operation will not take effect. After a VPC is deleted, its associated VRouters and route tables are also deleted.

To delete a VPC, follow these steps:

1. Log on to the VPC console and select the target region.
2. Locate the target VPC and click Delete.
3. In the displayed dialog box, click OK.

Related API actions

CreateVpc

DeleteVpc

DescribeVpcAttribute

DescribeVpcs

1.4 Manage VSwitches

This topic describes how to manage VSwitches, covering how to create and delete a VSwitch and how to create a cloud a cloud resource in a VSwitch.

After creating a VPC, you can further 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.

Create a VSwitch

To create a VSwitch, follow these steps:

1. Log on to the *VPC console*.
2. Select the region of the VPC to which the VSwitch will belong.

3. In the left-side navigation pane, click VSwitches.
4. Click Create VSwitch and then click OK. Descriptions about the configuration items are provided in the following table.

> Note:
> Currently, only the China (Hohhot) region supports enabling IPv6. After IPv6 is enabled, the system creates an IPv6 Gateway.

Configuration	Description
Resource Group	Optional. Select a resource group to which the VSwitch to be created belongs.
VPC	Select a VPC to which the VSwitch to be created belongs.
IPv4 CIDR Block	The IPv4 CIDR block of the selected VPC.
IPv6 CIDR Block	The IPv6 CIDR block of the selected VPC. Note: If an IPv6 CIDR block is not enabled for the VPC you selected, click Enable IPv6 CIDR Block. After the IPv6 CIDR block is enabled, the system automatically creates an IPv6 Gateway of the Free Version specification for the VPC.
Name	Enter a name for the VSwitch to be created. The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_), and hyphens (-). The name must start with a letter.
Zone	The zone of the VSwitch to be created. VSwitches that belong to the same VPC, but different zones, can communicate with each other through the intranet.

Configuration	Description
IPv4 CIDR Block	The IPv4 CIDR block of the VSwitch. - The IPv4 CIDR block of the VSwitch can be the same as the CIDR block of the VPC that the VSwitch belongs. It can also be a subnet 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 can be 192.168.0.0/16, or any CIDR block between 192.168.0.0/17 and 192.168.0.0/29. Note: If the CIDR block of the VSwitch is the same as the CIDR block of the VPC, you can only create one VSwitch. - The subnet mask of the VSwitch CIDR block can be 16 to 29 bits, which means the VSwitch can provide 8 to 65536 IP addresses. - The first IP address and the last three IP addresses in the VSwitch CIDR block are reserved. For example, if the VSwitch CIDR block is 192.168.1.0/24, the IP addresses 192.168.1.0, 192.168.1.253, 192.168.1.254, and 192.168.1.255 are reserved. - If the VSwitch needs to communicate with other VSwitches of other VPCs or on-premises data centers, you need to make sure that the CIDR blocks involved do not conflict with each other. Notice: You cannot modify the CIDR block of the VSwitch after the VSwitch is created.
Number of Available Private IPs	The number of available IPv4 addresses provided by the VSwitch.

Configuration	Description
IPv6 CIDR Block	The IPv6 CIDR block of the VSwitch. The mask of the IPv6 CIDR block of the VSwitch is set to /64 by default. You can enter 0 to 255 to customize the last eight bits of the IPv6 CIDR block. For example, if the IPv6 CIDR block of the selected VPC is 2001:db8::/64, you can enter 255 (ff in hexadeciaml notation). Then, the IPv6 CIDR block of the VSwitch is 2001:db8:ff::/64.
Description	Optional. Enter a description for the VSwitch. The description must be 2 to 256 characters in length and can contain letters, numbers, and special characters. The description cannot start with http:// or https://.

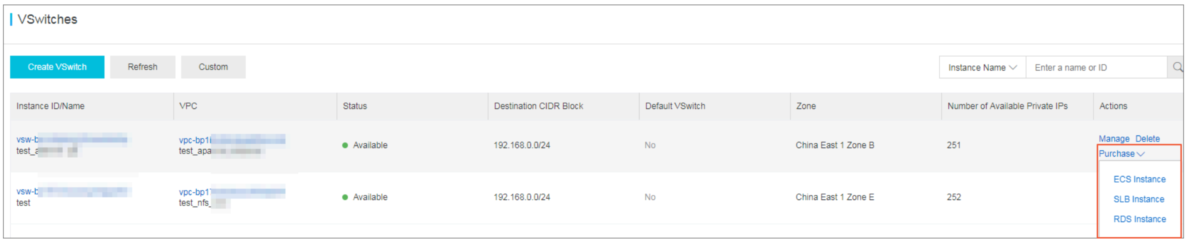
Create cloud resources in a VSwitch

To create cloud resources in a VSwitch, follow 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 resource to create.

Note:

Currently, you can create the following cloud resources in a VSwitch: ECS instances, SLB instances, and RDS instances.



Instance ID/Name	VPC	Status	Destination CIDR Block	Default VSwitch	Zone	Number of Available Private IPs	Actions
vsw-b[redacted] test_a[redacted]	vpc-bp1i[redacted] test_apa[redacted]	● Available	192.168.0.0/24	No	China East 1 Zone B	251	Manage Delete Purchase
vsw-b[redacted] test	vpc-bp1[redacted] test_nfs_[redacted]	● Available	192.168.0.0/24	No	China East 1 Zone E	252	

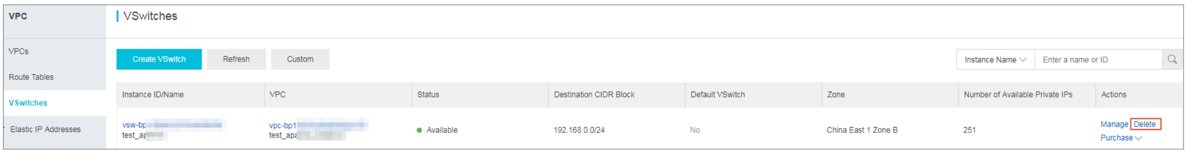
Delete a VSwitch

Before deleting a VSwitch, make sure the following conditions are met:

- You have deleted all cloud resources in the VSwitch (such as ECS, SLB, and RDS instances).
- If the VSwitch has been configured with SNAT entries, HAVIP, or any other configuration, make sure that you have deleted these associated resources.

To delete a VSwitch, follow 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.



Instance ID/Name	VPC	Status	Destination CIDR Block	Default VSwitch	Zone	Number of Available Private IPs	Actions
vsw-bp[redacted] test_ap[redacted]	vpc-bp1[redacted] test_apa[redacted]	● Available	192.168.0.0/24	No	China East 1 Zone B	251	Manage Delete Purchase

5. In the displayed dialog box, click OK.

Related APIs

CreateVSwitch

DescribeVSwitches

DeleteVSwitch

DescribeVSwitchAttributes

2 Routes

2.1 Route overview

After a VPC is created, the system automatically creates a default route table and adds system routes to it to manage traffic. You cannot create or delete system routes. However, you can create custom routes to route traffic to the destination CIDR block.

Route tables

After a VPC is created, the system creates a default route table to control routes of the VPC and all VSwitches in the VPC use the route table by default. You cannot create or delete the default route table. However, you can create a custom route table and attach it to the VSwitch to control the routes of the subnet.

A route entry specifies the destination of the traffic and consists of the destination CIDR block, the next hop type, and the next hop. Route entries include system route entries and custom route entries.

Note the following when managing route tables:

- Each VPC can contain up to ten route tables. This number includes the system route table.
- Each VSwitch can be attached to only one route table. The routes of a VSwitch (subnet) are managed by the associated route table.
- After a VSwitch is created, it is automatically attached to the system route table.
- To change a custom route table attached to a VSwitch to a system route table, detach the custom route table from the VSwitch. To attach the VSwitch to another route table, detach the current route table from the VSwitch and then attach the VSwitch to the target custom route table.
- Currently, all regions except China (Beijing), China (Shenzhen), and China (Hangzhou) support custom route tables.
- Cutom route tables do not support active/standby routes and load balancing routes .

System routes

After a VPC is created, the system automatically adds the following system routes to the route table:

- The route entry whose destination CIDR block is 100.64.0.0/10. It is used for cloud product communication within the VPC.
- The route entry whose destination CIDR block is the CIDR block of the VSwitch. It is used for cloud product communication within the VSwitch.

Custom routes

You can add custom route entries to replace system route entries or route traffic to a specified destination. You can specify the following next hop types when creating a custom route entry:

- ECS instance: Route the traffic pointing to the destination CIDR block to an ECS instance in the VPC.

  Select this type when you want to access the Internet or other applications through the application deployed on the ECS instance.
- VPN Gateway: Route the traffic pointing to the destination CIDR block to a VPN Gateway.

  Select this type when you want to connect to another VPC or an on-premises data center through VPN Gateway.
- Router Interface (To VPC): Route the traffic pointing to the destination CIDR block to a VPC.

  Select this type when you want to connect two VPCs through router interfaces of Express Connect.
- Router Interface (To VBR): Route the traffic pointing to the destination CIDR block to a VBR.

  Select this type when you want to connect a VPC to a local data center through Express Connect (physical access).
- Secondary ENI: Route the traffic pointing to the destination CIDR block to a secondary ENI.

IPv6 routes

If your VPC has enabled IPv6, the following route entries will be automatically added to the system route table of the VPC:

- The custom route entry (whose destination CIDR block is ::/0 and whose next hop is the IPv6 Gateway) is used for communicating with the Internet within a VPC through IPv6 addresses.
- The system route entry (whose destination CIDR block is the IPv6 CIDR block of the VSwitch) is used for communication within aVSwitch.

> Note:
> If you have created a custom route table and attached it to a VSwitch with IPv6 CIDR block enabled, you must maunally add a custom route entry whose the destination CIDR block is ::/0 and the next hop is the IPv6 Gateway instance.

Routing rules

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

The route table of a VPC is as follows:

Destination CIDR block	Next hop type	Next hop	Route entry 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

The route entries destined for `100.64.0.0/10` and `192.168.0.0/24` CIDR blocks are system route entries. The route entries destined for the `0.0.0.0/0` and `10.0.0.0/24` CIDR blocks 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`, and traffic destined for `10.0.1.1` will be routed to the ECS instance `i-12345678`.

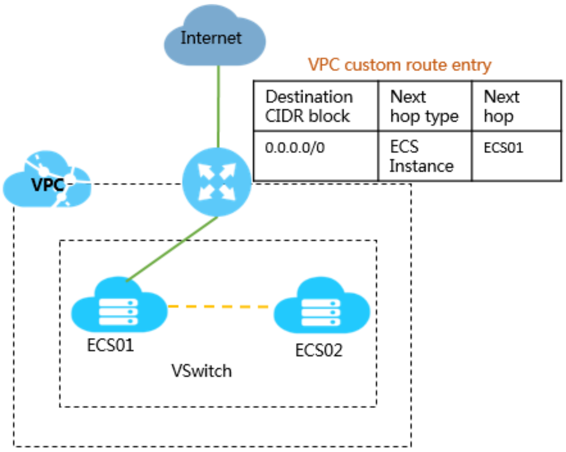
Routing examples

You can add custom route entries to the route table to control traffic.

- Routing within a VPC

  As shown in the following figure, a self-built NAT Gateway is deployed on an ECS instance (ECS01) in a VPC. To enable cloud resources in the VPC to access the Internet through this ECS instance, add the following route entry to the route table :

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



VPC custom route entry

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

- Connect VPCs (Express Connect)

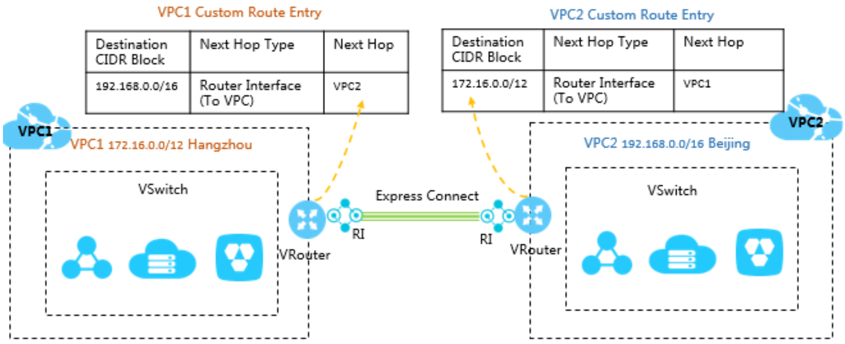
  As shown in the following figure, when using Express Connect to connect VPC 1 (172.16.0.0/12) and VPC 2 (192.168.0.0/16), you must add the following route entries in the VPCs after creating route interfaces:

  - Route entry added to VPC1

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface (To VPC)	VPC2

  - Route entry added to VPC2

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	Router interface (To VPC)	VPC1



VPC1 Custom Route Entry

Destination CIDR Block	Next Hop Type	Next Hop
192.168.0.0/16	Router Interface (To VPC)	VPC2

VPC2 Custom Route Entry

Destination CIDR Block	Next Hop Type	Next Hop
172.16.0.0/12	Router Interface (To VPC)	VPC1

- Connect VPCs

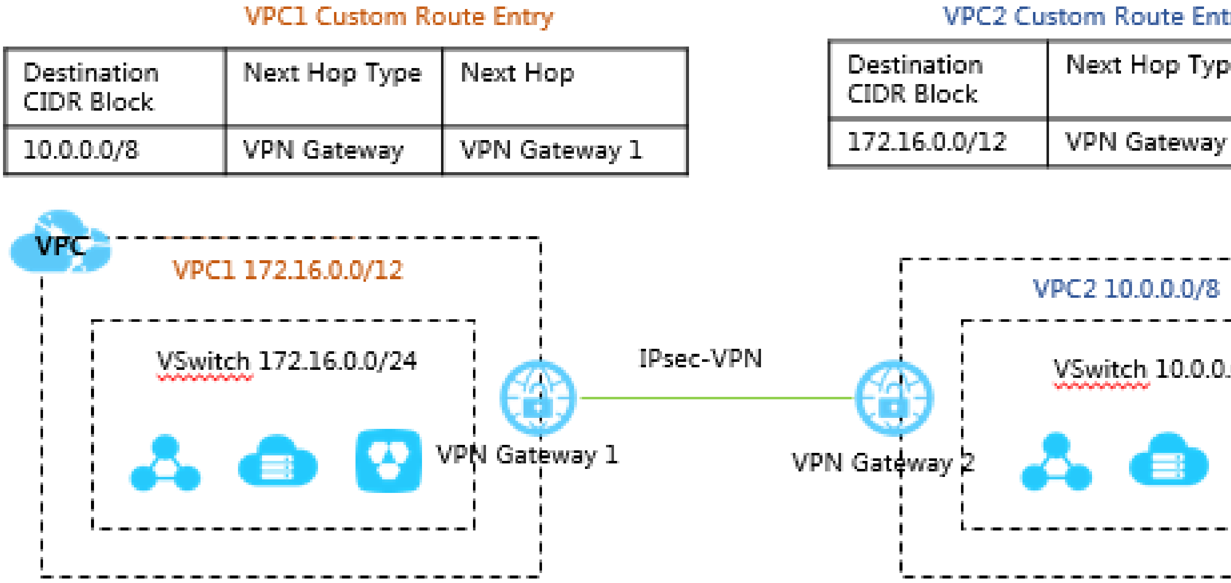
  As shown in the following figure, when using VPN Gateway to connect VPC 1 (172.16.0.0/12) and VPC 2 (10.0.0.0/8), you must add the following route entries in the VPCs after configuring VPN Gateway:

  - Route entry added to VPC 1

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

  - Route entry added to VPC 2

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



VPC1 Custom Route Entry

Destination CIDR Block	Next Hop Type	Next Hop
10.0.0.0/8	VPN Gateway	VPN Gateway 1

VPC2 Custom Route Ent

Destination CIDR Block	Next Hop Typ
172.16.0.0/12	VPN Gateway

- Connect a VPC to a local data center (Express Connect)

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

  - Route entry added to VPC

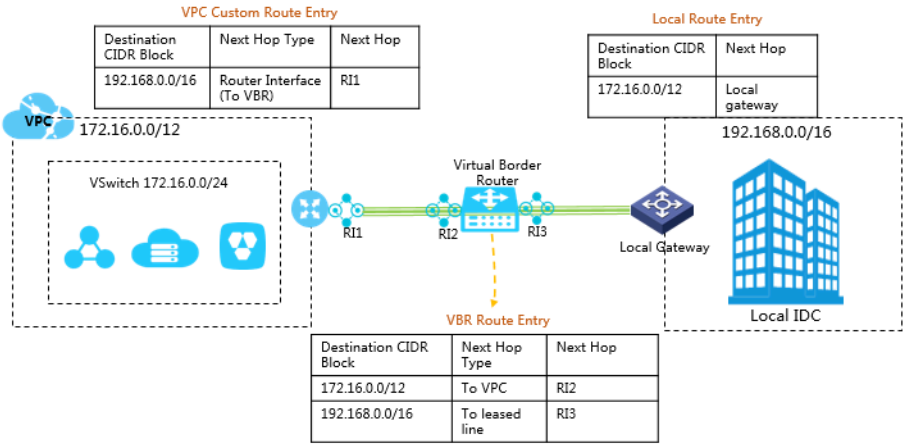
Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interface (To VBR /General Routing)	Router interface (RI 1)

  - Route entry added to 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)

  - Route entry added to the local network

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



VPC Custom Route Entry

Destination CIDR Block	Next Hop Type	Next Hop
192.168.0.0/16	Router Interface (To VBR)	RI1

Local Route Entry

Destination CIDR Block	Next Hop
172.16.0.0/12	Local gateway

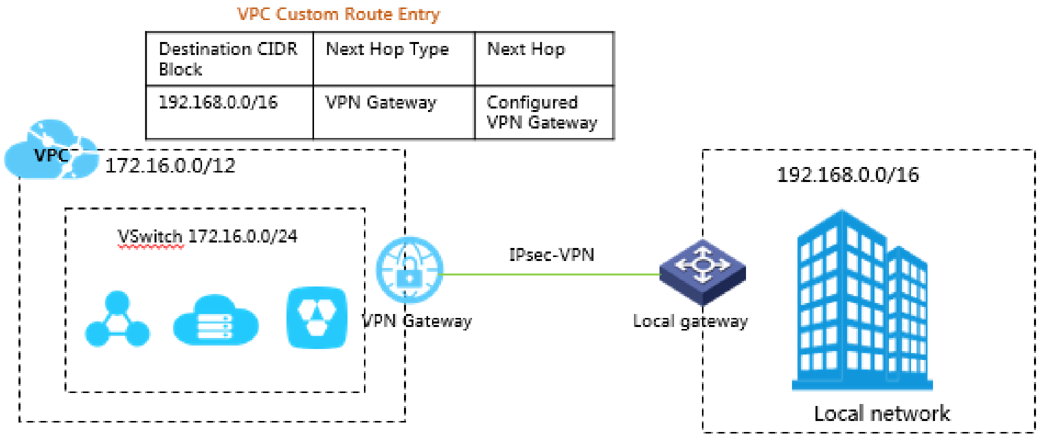
VBR Route Entry

Destination CIDR Block	Next Hop Type	Next Hop
172.16.0.0/12	To VPC	RI2
192.168.0.0/16	To leased line	RI3

- Connect a VPC to a local data center (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 route entry to the VPC:

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	VPN Gateway	The created VPN Gateway



VPC Custom Route Entry

Destination CIDR Block	Next Hop Type	Next Hop
192.168.0.0/16	VPN Gateway	Configured VPN Gateway

2.2 Manage custom route tables

This topic describes how to manage custom route tables. Specifically, this topic explains how you can create and edit custom route tables and how you can associate them with or detach them from a VSwitch.

Create a custom route table

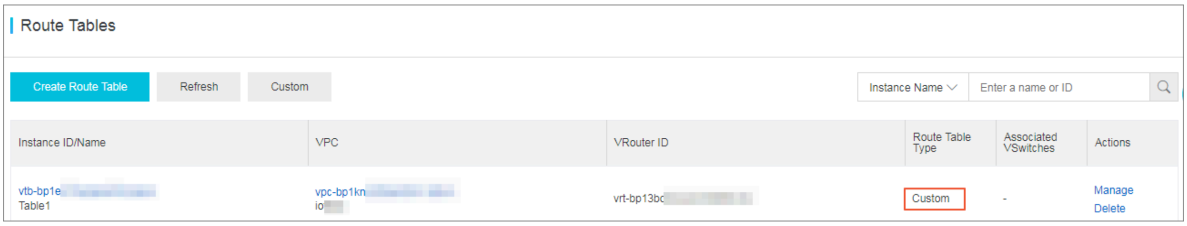
To create a custom route table, follow these steps:

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

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



Instance ID/Name	VPC	VRouter ID	Route Table Type	Associated VSwitches	Actions
vtb-bp1e[redacted] Table1	vpc-bp1kn[redacted] io[redacted]	vrt-bp13bc[redacted]	Custom	-	Manage Delete

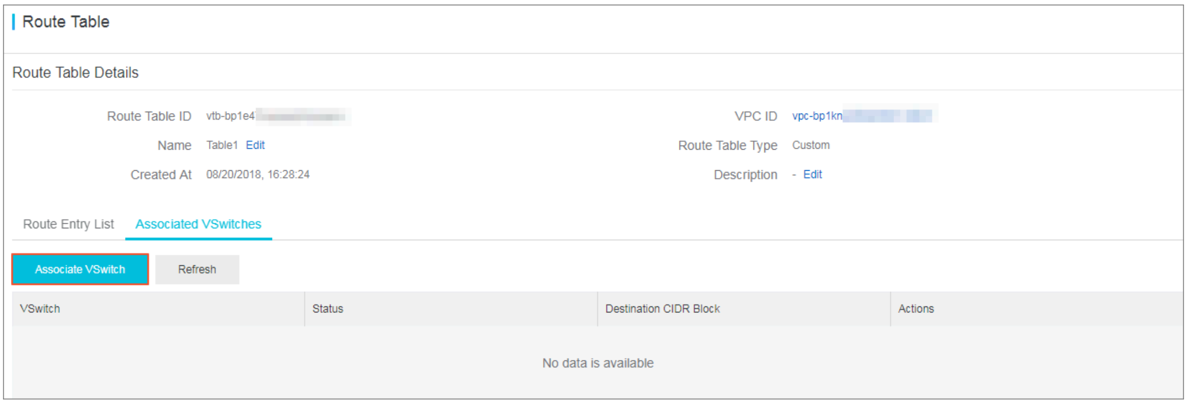
Associate a custom route table with a VSwitch

You can associate a custom route table with a VSwitch to control routing of the VSwitch subnet. A VSwitch can only be associated with one route table, including the system route table.

To associate a custom route table with a VSwitch, follow 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.



Route Table

Route Table Details

Route Table ID vtb-bp1e4[redacted]

Name Table1 Edit

Created At 08/20/2018, 16:28:24

VPC ID vpc-bp1kn[redacted]

Route Table Type Custom

Description - Edit

Route Entry List | Associated VSwitches

VSwitch	Status	Destination CIDR Block	Actions
No data is available			

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

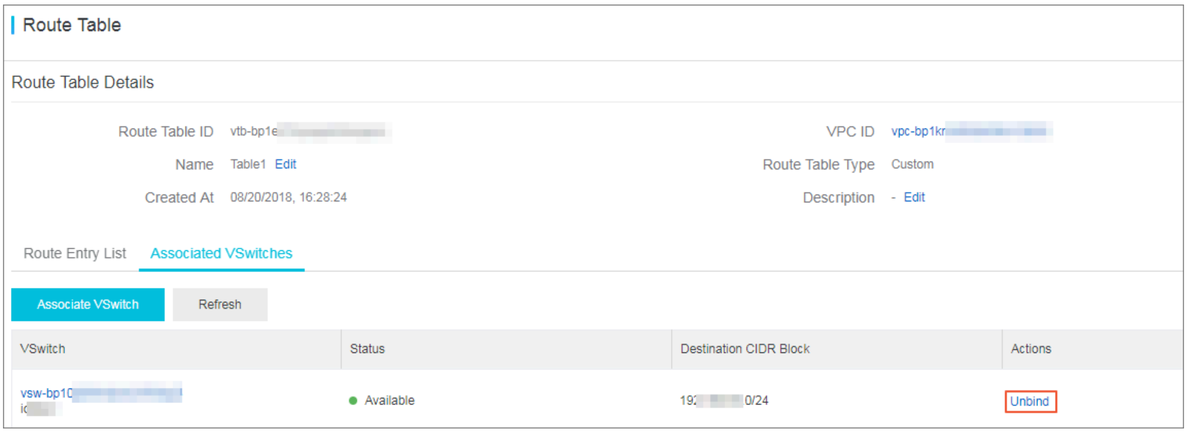
   For more information, see *#unique_27/unique_27_Connect_42_section_k5r_n5y_rdb*.

Detach a custom route table from a VSwitch

You can detach a custom route table from a VSwitch. After a customer route table is detached, the VSwitch automatically uses the default route table if you do not associate it with another custom route table.

To detach a custom route table from a VSwitch, follow 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.



Route Table

Route Table Details

Route Table ID vtb-bp1e[redacted]

Name Table1 Edit

Created At 08/20/2018, 16:28:24

VPC ID vpc-bp1kr[redacted]

Route Table Type Custom

Description - Edit

Route Entry List | Associated VSwitches

VSwitch	Status	Destination CIDR Block	Actions
vsw-bp10[redacted] i[redacted]	● Available	19[redacted]0/24	Unbind

Edit the custom route table

To modify the name and description of a custom route table, follow 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

#unique_27/unique_27_Connect_42_section_k5r_n5y_rdb

2.3 Add a custom route entry

After a VPC is created, the system automatically creates a default route table and adds system routes to the route table to manage traffic. You cannot create or delete system routes, but you can create custom routes to direct traffic to specified destination CIDR blocks.

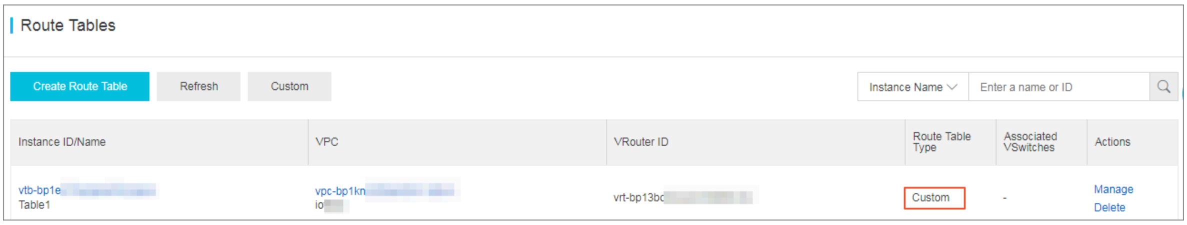
Context

Each item in a route table is a *route entry*. A route entry specifies the destination of the traffic and consists of the destination CIDR block, next hop type, and next hop. Route entries include system routes and custom routes.

You can add custom routes to a system route table or a custom route table.

Procedure

1. Log on to the *VPC Console*.
2. Select the region to which the target VPC belongs.
3. In the left-side navigation pane, select Route Tables.
4. Click the ID of the target route table, and then click the Route Entry List tab page.



Instance ID/Name	VPC	VRouter ID	Route Table Type	Associated VSwitches	Actions
vtb-bp1e[redacted] Table1	vpc-bp1kn[redacted] io[redacted]	vrt-bp13bc[redacted]	Custom	-	Manage Delete

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 destination CIDR block. · IPv4 CIDR Block: Traffic is forwarded to an IPv4 address. · IPv6 CIDR Block: Traffic is forwarded to an IPv6 address.

Configuration	Description
Next Hop Type and Next Hop	Select the next hop type: · ECS Instance: Direct the traffic pointing to the destination CIDR block to the selected ECS instance. Select this type when you want to direct the specifed traffic to an ECS instance to uniformly forward and manage the traffic. For example, configure an ECS instance as an Internet gateway to manage the access of other ECS instances to the Internet. · VPN Gateway: Direct the traffic pointing to the destination CIDR block to the selected VPN Gateway. · NAT Gateway: Direct the traffic pointing to the destination CIDR block to the selected NAT Gateway. · Secondary NetworkInterface: Direct the traffic pointing to the destination CIDR block to the selected secondary ENI. · Router Interface (To VPC): Direct the traffic pointing to the destination CIDR block to the selected VPC. Select this type when you want to use Express Connect to connect VPCs. · Router Interface (To VBR): Direct the traffic pointing to the destination CIDR block to the router interface associated with the VBR. Select this type when you want to use Express Connect to connect a VPC to an on-premises data center. In this mode, you also need to select the route type: - General Routing: Select any associated router interface. - Active/Standby Routing: You can use only two instances as the next hops, one that is designated as active, the other as standby. The active route is weighted at 100, and the standby route at 0. When the active route is declared as unhealthy, the standby route replaces the active route. - Load Balancing Routing: You need to use two to four router interfaces as the next hops and the peer routers of the next hops must be VBRs. Valid values of the router interface weight are from 1 to 255, and the default router interface weight is 100. The weight of

2.4 Add a subnet route to a route table

You can create a custom route table in a VPC and add subnet routes to the created custom route table. Then, you can associate the route table with a VSwitch to control the traffic to and from the VSwitch, enabling flexible network management.

Prerequisites

A VPC and a VSwitch are created. For more information, see *Manage a VPC*.

Limits

Note the following limits before you add subnet routes to a route table:

- You can create up to ten route tables in a VPC, including system route tables.
- Each VSwitch can be associated with only one route table.
- Active/standby routes and load balancing routes are not supported by custom route tables.

Step 1: Create a custom route table

To create a custom route table, follow these steps:

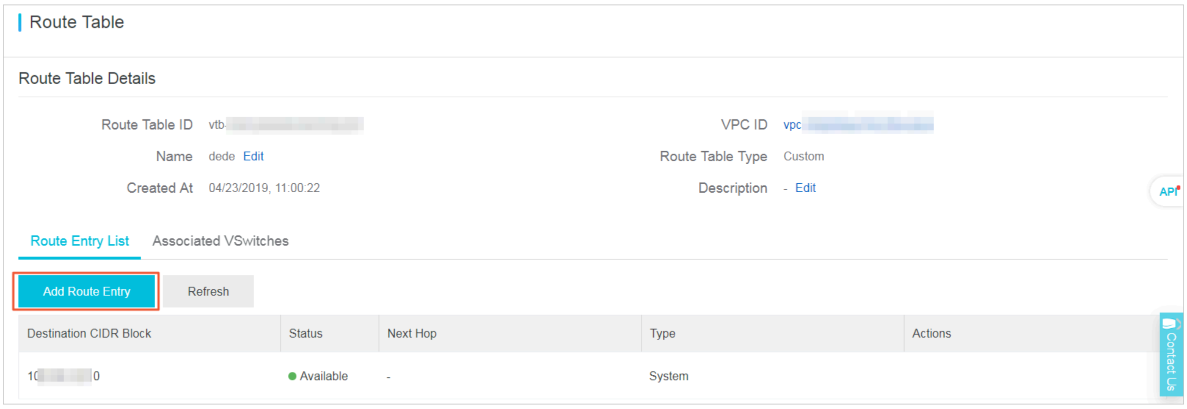
1. Log on to the *VPC console*.
2. In the left-side navigation pane, click Route Tables.
3. Click Create Route Table.
4. Configure the route table according to the following information, and then click OK.

Configuration	Description
Name	Enter a name for the route table to be created. The name must be 2 to 128 characters in length and can contain letters, numbers, Chinese characters, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
VPC	Select a VPC to which the route table to be created belongs.
Description	Enter a description for the route table to be created. The description must be 2 to 256 characters in length and cannot start with `http ://` or `https ://`.

Step 2: Add a subnet route to the custom route table

To add a subnet route entry to the created custom route table, follow these steps:

1. Log on to the *VPC console*.
2. Select the region of the VPC to which the created route table belongs.
3. In the left-side navigation pane, click Route Tables.
4. Find the target route table, click the route table ID, and then click the Route Entry List tab.



Route Table

Route Table Details

Route Table ID vtb[redacted]

VPC ID vpc[redacted]

Name dede Edit

Route Table Type Custom

Created At 04/23/2019, 11:00:22

Description - Edit

Destination CIDR Block	Status	Next Hop	Type	Actions
10[redacted]0	● Available	-	System	

5. Click Add Route Entry.
6. In the displayed dialog box, configure the subnet route entry according to the following information, and then click OK.

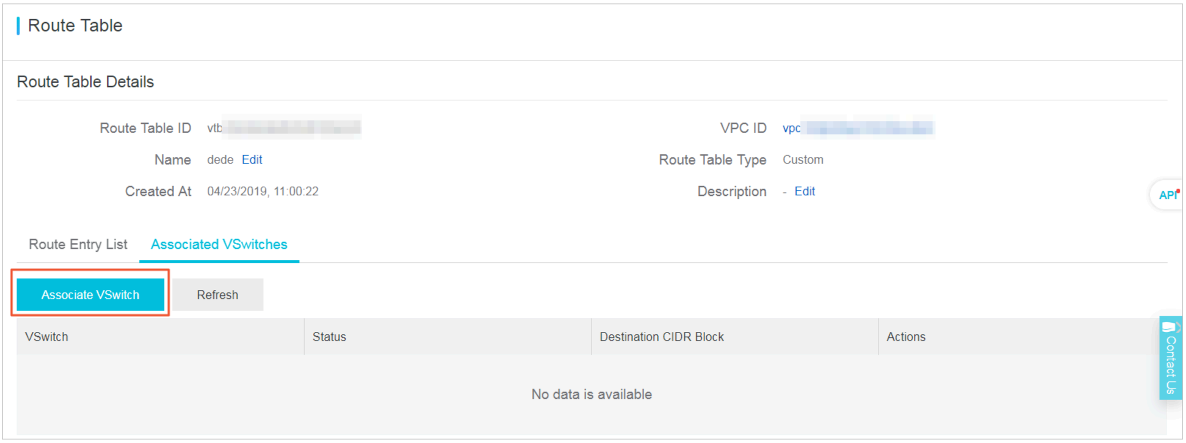
Configuration	Description
Destination CIDR Block	Specify the destination CIDR block of the traffic. · IPv4 CIDR Block: Forwards IPv4 traffic. · IPv6 CIDR Block: Forwards IPv6 traffic.

Configuration	Description
Next Hop Type and Next Hop	Select the type of the next hop. ・ ECS Instance: Directs the traffic from the destination CIDR block to a specified ECS instance. This type of next hop is suitable for when you need to direct specific traffic to an ECS instance for centralized traffic forwarding and management (for example, set an ECS instance as an Internet gateway to manage access of other ECS instances to the Internet). ・ VPN Gateway: Directs the traffic from the destination CIDR block to a specified VPN Gateway. ・ NAT Gateway: Directs the traffic from the destination CIDR block to a specified NAT Gateway. ・ Secondary NetworkInterface: Directs the traffic from the destination CIDR block to a specified secondary Elastic Network Interface (ENI). ・ Router Interface (To VPC): Directs the traffic from the destination CIDR block to a specified VPC. This type of next hop is suitable for when you connect two VPCs by using Express Connect. ・ Router Interface (To VBR): Directs the traffic from the destination CIDR block to a router interface that is associated with the Virtual Border Router (VBR). This type of next hop is suitable for when you connect your on-premises data center to a VPC by using Express Connect. If you select Router Interface (To VBR), you need to select a routing method. - General Routing: Select a router interface that is associated with the VBR. - Active/Standby Routing: Active/standby routing only supports up to two router interfaces for the next hop. The active router interface has a weight of 100, and the standby router interface has a weight of 0. If the active router interface fails health checks, the system switches to the standby router interface. - Load Balancing Routing: You can select two to four

Step 3: Associate the route table with a VSwitch

You can associate the created route table with a VSwitch (subnet) to control the traffic to and from this VSwitch. A VSwitch can be associated with only one route table, including system route tables. To associate the created custom route table with a VSwitch, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click Route Tables.
3. Select the region of the target custom route table.
4. Find the route table and click the route table ID.
5. Click the Associated VSwitches tab. Then, click Associate VSwitch.



Route Table

Route Table Details

Route Table ID vtb[redacted]

Name dede Edit

Created At 04/23/2019, 11:00:22

VPC ID vpc[redacted]

Route Table Type Custom

Description - Edit

VSwitch	Status	Destination CIDR Block	Actions
No data is available			

6. In the displayed dialog box, select the target VSwitch. Then, click OK.

3 Network connection

3.1 Network connection overview

Alibaba Cloud provides rich solutions for connecting a VPC to the Internet, other VPCs, or on-premises data centers.

Connect to the Internet

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

Product	Features	Benefits
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 traffic balancing.	Internet access for multiple ECS instances is supported. (Note that EIP does not provide this support.)

Product	Features	Benefits
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 the Internet to the backend ECS instances. Note: ECS instances without a public IP address cannot access the Internet (SNAT) through Server Load Balancer.	In DNAT, Server Load Balancer supports forwarding an Internet request to multiple ECS instances. Server Load Balancer can increase your service capability and enhance overall 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 and functions that you can use to connect a VPC to another VPC.

Product	Features	Benefits
VPN Gateway	VPN Gateway allows you to create an IPsec-VPN connection to build an encrypted communication between two VPCs.	· Low cost, secure, and simple configuration. (The quality of the network depends on your Internet connection.) · IPsec-VPN supports IKEv1 and IKEv2 protocols. Devices that support these two protocols can connect to Alibaba Cloud VPN Gateway. Supported devices: Huawei, H3C, SANGFOR, Cisco ASA, Juniper, SonicWall, Nokia, IBM, and Ixia.

Product	Features	Benefits
Cloud Enterprise Network (CEN)	CEN allows you to connect VPCs in different regions and under different accounts to build an interconnected network. For more information, see *Tutorial overview*.	· Simple configuration, and automatic route learning and distribution. · Low latency and fast speed. · The networks (VPCs/VBRs) attached to a CEN instance are connected to each other. · The network connection in the same region is free of charge.

Connect a VPC to an on-premises data center

The following table lists the products and functions that you can use to connect a VPC to an on-premises data center.

Product	Features	Benefits
Express Connect	Express Connect allows you to connect a VPC to an on-premises data center. For more information, see *Connect an on-premises IDC to a VPC through a physical connection*.	· Based on the backbone network, low latency. · Leased line access features higher security and reliability, faster speed, and lower latency.

Product	Features	Benefits
VPN Gateway	- VPN Gateway allows you to create an IPsec-VPN connection between a VPC to an on-premises data center. - Connect multiple on-premises data centers The VPN-Hub function of VPN Gateway allows you to connect multiple on-premises data centers to the VPC. The connected data centers can communicate with the VPC , but also can communicate with each other. - 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. Devices that support these two protocols can connect to Alibaba Cloud VPN Gateway . Supported devices: Huawei , H3C, SANGFOR, Cisco ASA , Juniper, SonicWall, Nokia, IBM, and Ixia. - SSL-VPN connections support connecting a VPC from a remote computer using the Linux, Windows, and MacOS.

Product	Features	Benefits
CEN	· Connect to an on-premises data center CEN allows you to attach the VBR associated with an on-premises data center to a CEN instance to build an interconnected network. · Connect multiple VPCs with on-premises data centers CEN allows you to attach multiple networks (VPC/VBR) to a CEN instance. All the attached networks are connected with each other.	· 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. · The network connection in the same region is free of charge.

Product	Features	Benefits
Smart Access Gateway(SAG)	- Smart Access Gateway allows you to connect on-premises branches to the Alibaba Cloud to build a hybrid cloud for large organizations. - Connect local branches.	- SAG features highly automated configuration 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 authentication is implemented during the Internet transmission.

3.2 Connect a VPC to the Internet

You can use Elastic IP Address (EIP) or NAT Gateway to allow cloud resources in a VPC to access the Internet.

Overview

By default, cloud resources in a VPC cannot access the Internet or be accessed from the Internet. You can configure a public IP address or a NAT Gateway so that the VPC can communicate with the Internet.

In addition, VPC provides Internet Shared Bandwidth and Data Transfer Plan to help you save Internet cost. For more information, see *How to save the Internet cost?*

EIP

An Elastic IP Address (EIP) is a public IP address resource that you can purchase and possess independently. An EIP is a type of NAT IP address. It is located on the Internet gateway of Alibaba Cloud, and is mapped to the attached resource, then the resource can communicate with the Internet through the EIP.

Currently, you can attach an EIP to an ECS instance of the VPC network, an ENI, an intranet SLB instance of the VPC network, or a NAT Gateway. For more information, see *EIP user guide*.

The benefits of EIP are as follows:

- Independently purchased and possessed

  You can purchase an EIP as an independent resource instead of purchasing it together with other computing or storage resources.
- Flexible attaching

  You can attach an EIP to a resource that needs to access the Internet and detach and release the EIP when it is unneccessary to avoid additional cost.
- Configurable network capability

  You can adjust the bandwidth of an EIP as needed. The bandwidth change takes effect immediately.

NAT Gateway

NAT Gateway is an enterprise-class VPC Internet gateway that provides NAT proxy services (SNAT and DNAT), the forwarding capacity of up to 10 Gbps, and cross-zone disaster recovery.

With NAT Gateway, multiple ECS instances of the VPC network can access the Internet through one public IP address. For more information, see *NAT Gateway user guide*.

The benefits of NAT Gateway are as follows:

- Flexible and easy-to-use

  As an enterprise-class Internet gateway for VPC, NAT Gateway provides SNAT and DNAT functions, which means you can directly configure SNAT and DNAT rules without setting up a NAT Gateway by yourself.

- High availability

  The NAT gateway is a virtual network hardware which is based on the self-developed distributed gateway of Alibaba Cloud and virtualized by SDN technology . With the forwarding capacity of up to 10 Gbps, NAT Gateway supports large-scale Internet applications.
- Pay-AS-You-Go billing

  You can change the gateway specification as well as the specifications and number of EIPs at any time to meet changing service requirements.

3.3 Connect VPCs

You can use CEN and Express Connect to connect different VPCs.

Overview

To meet various demands of different application scenarios, Alibaba Cloud provides several products for connecting VPCs. You can use CEN or Express Connect to connect VPCs. We recommend that you use CEN because it is easy to configure and automatically distributes and learns routes.

- *CEN*

  You can use Cloud Enterprise Network (CEN) to build an intranet connection between multiple VPCs or between a VPC and a local data center. CEN provides automatic route distribution and learning, which ensures rapid network convergence and enhances the quality and security of cross-network communication.
- *Express Connect*

  You can use Express Connect to build an intranet connection between two VPCs.

Scenarios

Scenario	Product	Method
Connect VPCs in the same region and under the same account	*CEN*	*Connect VPCs in the same region and under the same account*
	Express Connect	*Interconnect two VPCs under the same account*

Scenario	Product	Method
Connect VPCs in the same region but under different accounts	*CEN*	*Connect VPCs in the same region but under different accounts*
	Express Connect	*Interconnect two VPCs under different accounts*
Connect VPCs in different regions but under the same account	*CEN*	*Connect VPCs in different regions but under the same account*
	Express Connect	*Interconnect two VPCs under the same account*
Connect VPCs in different regions and under different accounts	*CEN*	*Connect VPCs in different regions and under different accounts*
	Express Connect	*Interconnect two VPCs under different accounts*

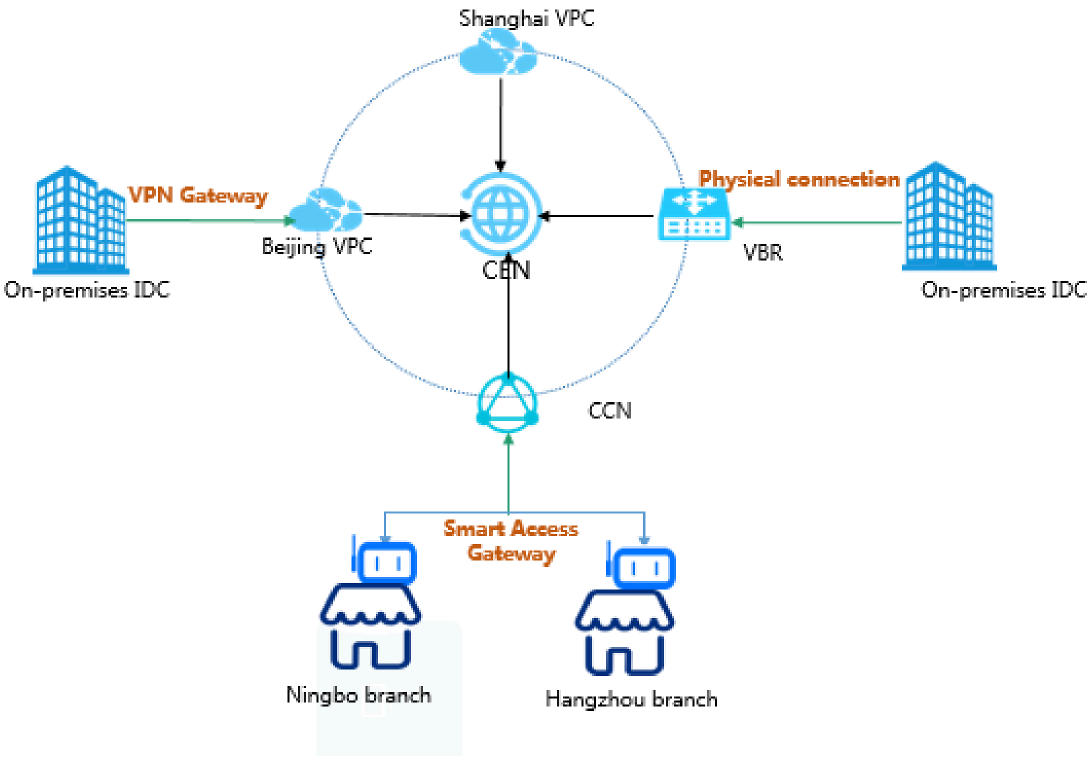
3.4 Connect a VPC to an on-premises data center

You can connect an on-premises data center to a VPC by using VPN Gateway, a physical connection of Express Connect, or Smart Access Gateway to build a hybrid cloud.

Overview

You can establish intranet communication between a local data center and Alibaba Cloud to build a hybrid cloud. Then you can seamlessly expand your local IT infrastructure to Alibaba Cloud to cope with service fluctuation and improve application stability by right of the mass computing, storage, network, and CDN resources of Alibaba Cloud.

You can use VPN Gateway, a physical connection of Express Connect and Smart Access Gateway to connect a local data center to a VPC. In addition, you can interconnect global networks by using CEN.



Solutions

Solution	Description
VPN Gateway	You can use IPsec-VPN to connect a local data center to a VPC. VPN Gateway contains two different gateway instances which form active/standby hot backup. The traffic is automatically distributed to the standby node when the active node fails. The VPN Gateway is based on Internet communication , so its network latency and availability are decided by the Internet. If you do not have a particularly high demand for network latency, we recommend that you use VPN Gateway. For more information, see *Create a site-to-site connection through IPsec-VPN*.

Solution	Description
Physical connection	You can use a leased line of your service provider to establish a physical connection between your on-premises IDC and an Alibaba Cloud access point. Physical connection features good network quality and large bandwidth. Therefore, if your priority is good network quality, we recommend that you select physical connection. For more information, see *Connect a local data center to a VPC through a physical connection*.
Redundant physical connections	You can use redundant physical connections to connect your on-premises data center to a VPC. Redundant physical connections provide high-quality and high-reliability intranet communication between your local data center and Alibaba Cloud. Alibaba Cloud supports up to four physical connections to achieve Equal-CostMultipathRouting (ECMP). For more information, see *Create redundant physical connections*.
Smart Access Gateway	Smart Access Gateway (SAG) is an all-in-one solution for connecting local branches of an enterprise to the Alibaba Cloud. With Smart Access Gateway, enterprises can access Alibaba Cloud through the Internet using a fully encrypted connection, which is more intelligent, more reliable, and more secure. Smart Access Gateway is an easy-to-configure and low-cost service. If you want to connect multiple local branches of an enterprise to the cloud, we recommend that you select Smart Access Gateway. For more information, see *Connect local branches to Alibaba Cloud through Smart Access Gateway*.
BGP active/standby links	Function by using both a physical connection and CEN, allowing you to connect an on-premises data center to VPCs in different regions through active/standby links. For more information, see *Connect a local data center to Alibaba Cloud by using BGP active/standby links*.
Physical connection + Smart Access Gateway	A solution using Smart Access Gateway as the backup link of the existing physical connection to build a reliable and high-availability hybrid cloud. For more information, see *Tutorial for configuring Smart Access Gateway as the backup of a physical connection*.

3.5 ClassicLink

3.5.1 ClassicLink overview

VPC provides the ClassicLink function so that ECS instances of the classic network can communicate cloud resources in a VPC network through the intranet.

Background

The basic implementation for the connection of classic networks with VPCs is the same as that of two classic networks. Therefore, when connecting a classic network to a VPC, the intranet latency and bandwidth limits remain unchanged. Moreover, operations, such as downtime migration, hot migration, stopping, starting, restarting , and system disk replacement will not change the link of a previously established ClassicLink.

The classic network and VPC network 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 IP addresses properly to avoid IP address conflicts.

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

Limits

Note the following before you use 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, and the VPC must be under the same account and belong to the same region.

  For cross-account connection such as ones connecting an ECS instance under account A to a VPC under account B, you can transfer the ECS instance 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. 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 of a classic network to a VPC network.

Network type of the initiator	Region/ account	Network type of the acceptor/intranet communication	
		Classic network	VPC network
Classic network	Same region Same account	Add a same-account authorization rule in the security group.	Build a ClassicLink connection.

	Same region Different accounts	Add a cross-account authorization rule in the security group.	· Solution A: 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 Different accounts	· 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	

	Different regions Same account	1. Migrate the receiver ECS instance of the classic network to the VPC 2. Connect the VPCs	
	Different regions Different accounts		

Example scenario

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

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

  After a ClassicLink connection is successfully established, ECS instances in the classic network can access other cloud resources in the connected VPC (such as other ECS, RDS, or SLB instances). An real example may be that an ECS instance in the classic network is connected to a VPC of which the IP address range is 10.0.0.0/8, and the VPC has a VSwitch of which the IP address range is 10.111.1.0/24. If you have deployed cloud resources (such as ECS and RDS instances) 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 ECS instances in the classic network connected to the VPC and cannot access ECS instances or any other cloud resources in classic networks that are not connected to the VPC.

3.5.2 Establish a ClassicLink connection

You can establish a ClassicLink connection so that the ECS instance of the classic network can access resources deployed in a VPC network.

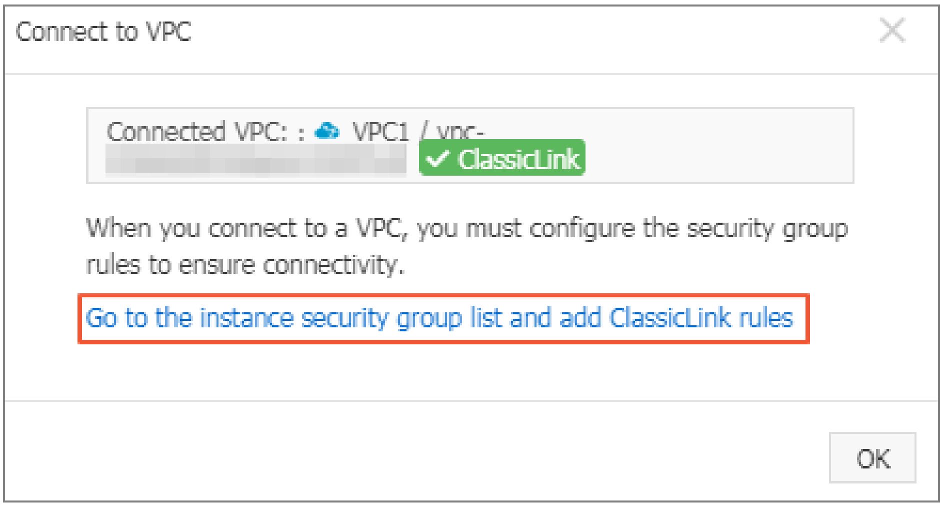
Prerequisites

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. Log on to the ECS console.
5. In the left-side navigation pane, click Instances.
6. Select a region, and then locate the target ECS instance of the classic network.
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 link for configuring security groups.



Connect to VPC

Connected VPC: : VPC1 / vpc-[redacted] ✓ ClassicLink

When you connect to a VPC, you must configure the security group rules to ensure connectivity.

Go to the instance security group list and add ClassicLink rules

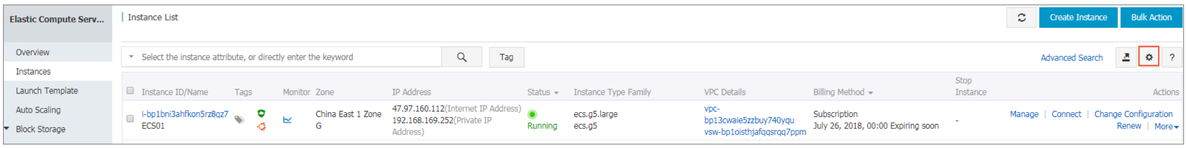
9. Click Add ClassicLink Rules and configure the security rule according to the following information. Then, click OK.

Configuration	Description
Classic Security Group	Displays the classic network security group.
Select VPC Security Group	Select the security group of the VPC.
Mode	Select one of the following modes: · Classic <=> VPC: The connected resources can access each other (recommended). · Classic => VPC: Authorize the ECS instance of the classic network to access cloud resources in the connected VPC. · Classic <= VPC: Authorize the cloud resources in the VPC to access the ECS instance of the connected classic network.

Configuration	Description
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 in the upper-right corner. In the displayed dialog box, click Connection Status and then click OK.

Figure 3-1: Column Filter



Elastic Compute Serv...
- Overview
- Instances
- Launch Template
- Auto Scaling
- Block Storage

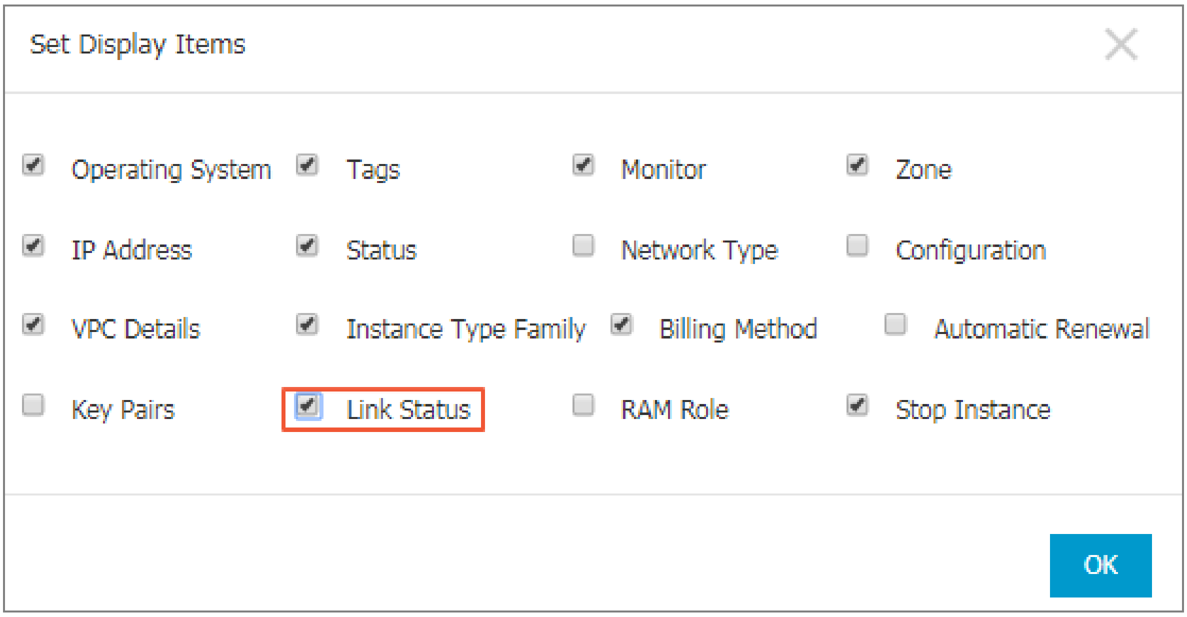
Instance List

Create Instance
Bulk Action
Select the instance attribute, or directly enter the keyword
Tag
Advanced Search
?

Instance ID/Name	Tags	Monitor	Zone	IP Address	Status	Instance Type Family	VPC Details	Billing Method	Stop Instance	Actions

i-bp1bni3ahfkon5rz8qz7
ECS01
			China East 1 Zone G	47.97.160.112(Internet IP Address)
				192.168.169.252(Private IP Address)
					Running	ecs.g5.large
						ecs.g5
							vpc-bp13cwaie5zzbuy740yqu
							vsw-bp1oisthjafqqsrqq7ppm
								Subscription
								July 26, 2018, 00:00 Expiring soon
									-	Manage | Connect | Change Configuration
										Renew | More

Figure 3-2: Connection Status



Set Display Items

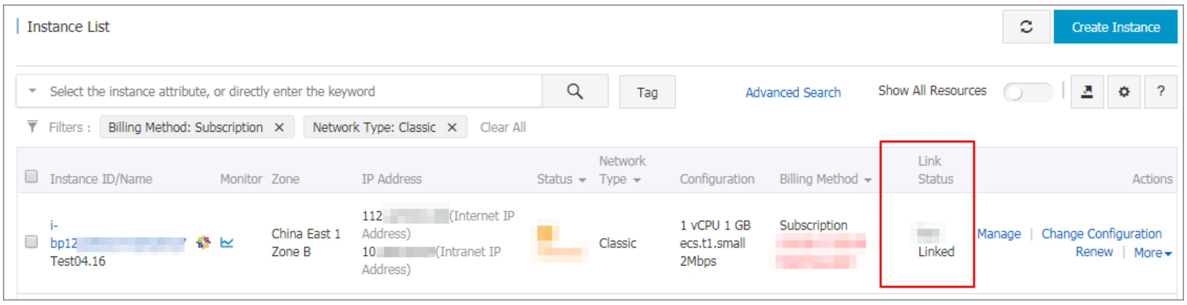
☑ Operating System ☑ Tags ☑ Monitor ☑ Zone

☑ IP Address ☑ Status □ Network Type □ Configuration

☑ VPC Details ☑ Instance Type Family ☑ Billing Method □ Automatic Renewal

□ Key Pairs ☑ Link Status □ RAM Role ☑ Stop Instance

Figure 3-3: Connected to a VPC



Instance List

Create Instance
Select the instance attribute, or directly enter the keyword
Tag
Advanced Search
Show All Resources
?

Filters : Billing Method: Subscription × Network Type: Classic × Clear All

Instance ID/Name	Monitor	Zone	IP Address	Status	Network Type	Configuration	Billing Method	Link Status	Actions
i-bp12[redacted] Test04.16		China East 1 Zone B	112[redacted](Internet IP Address) 10[redacted](Intranet IP Address)	[redacted]	Classic	1 vCPU 1 GB ecs.t1.small 2Mbps	Subscription [redacted]	[redacted] Linked	Manage | Change Configuration Renew | More

3.5.3 Cancel a ClassicLink connection

You can cancel the ClassicLink connection between ECS instances when the connection is no longer needed.

Procedure

1. Log on to the ECS console.

2. In the left-side navigation pane, click Instances.
3. Select the region to which the instance belongs, and then locate the target instance.
4. Choose More > Network and Security Group > Disconnect from VPC.
5. In the displayed dialog box, click OK.

3.5.4 Disable ClassicLink

After canceling 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. In the displayed dialog box, click OK.

4 Access control

4.1 Overview

Currently, VPC does not provide an independent access control policy. Therefore, you need to rely on the access control functions of target cloud products in VPC to achieve your desired results. For example, when using ECS instances, you can use security groups to achieve access control over your instances, and when using SLB and RCS instances, you can achieve access control by using whitelists."

ECS security group

A security group is a virtual firewall capable of status detection packet inspection. In general, security groups are used to configure 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, or you can customize the rule as needed. However, you cannot delete the default security group.

RDS whitelist

You can use the whitelist function provided by ApsaraDB for RDS for access control . Doing so enables you to specify IP addresses that are allowed to access the RDS instance while also denying access from other IP addresses. When using RDS in a VPC , you can 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

You can use the whitelist function provided by SLB for Server Load Balancer listeners , so that only IP addresses in the whitelist can access the listeners. We recommend doing so for applications that only allow access from certain IP addresses.

4.2 Cases for configuring ECS security groups

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

This topic lists some common security group configurations for ECS instances of the VPC network.

Case 1: Intranet communication

The following are two types of communication methods between ECS instances of the VPC network:

- By default, ECS instances in the same security group of the same VPC can communicate with each other.
- ECS instances in different VPCs cannot communicate with each other. To achieve communication between two ECS instances in different VPCs, use Express Connect, VPN Gateway, or CEN to connect them. When doing so, make sure the security group rules allow access between the target ECS instances, as shown in the following table.

Security group rules	Rule direct	Autho ion policy	Protocol type and port range	Authoriz 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	

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
	Inbound	Allow	Custom TCP Custom	Address field access	

Case 2: Deny the access of specific IP addresses or ports

You can configure security groups to deny the access of specific IP addresses or ports to an ECS instance.

Security group rules	Rule direction	Authorization policy	Protocol type and port range	Authorization type	Authorization object
Deny the 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 the 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 the remote access of a specific IP address

If you have configured a NAT Gateway or EIP for an 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 direct	Autho ion policy	Protocol type and port range	Authoriza ion 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 an 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 direct	Autho ion policy	Protocol type and port range	Authoriza ion 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

5 Flow logs

This topic describes the flow logs function in Alibaba Cloud Virtual Private Cloud (VPC). The flow logs function allows you to monitor the IP traffic going to and coming from Elastic Network Interfaces (ENI) in your VPC. By using the flow logs, you can check the access control list (ACL) rules, monitor network traffic, and troubleshoot networking problems.

Note:

The flow log function is available only in the China (Hohhot), Malaysia, Indonesia (Jakarta), UK (London), and Indonesia (Jakarta) regions.

Introduction to flow logs

You can use the flow log function to monitor the IP traffic information for an ENI , a VSwitch or a VPC. If you create a flow log for a VSwitch or a VPC, all the Elastic Network Interfaces, including the newly created Elastic Network Interfaces, are monitored.

Flow log data is stored in Log Service, where you can view and analyze IP traffic information. Currently, the flow log function is available free of charge. However, corresponding storage and indexing fees associated with the use of Log Service are billed. For more information, see *Billing method*.

The traffic information monitored by the flow log function is recorded as flow log records. Each record captures the network flow for a specific 5-tuple in a specific monitoring time period (approximately 10 minutes). During the monitoring time period, Log Service aggregates data, which takes about 5 minutes, and then publishes the generated flow log records.

The following table describes the fields recorded in flow log records.

Field	Description
version	The version of the flow log.
vswitch-id	The ID of the VSwitch to which the ENI belongs.
vm-id	The ID of the ECS instance to which the ENI is attached.
vpc-id	The ID of the VPC to which the ENI belongs.
account-id	The ID of the account.

Field	Description
eni-id	The ID of the ENI.
srcaddr	The source address.
srcport	The source port.
dstaddr	The destination IP address.
dstport	The destination port of traffic.
protocol	The IANA protocol number of traffic. For more information, see *Assigned Internet Protocol Numbers*.
direction	The direction of traffic. Supported values include: · in: traffic goes to the ENI · out: traffic goes from the ENI
packets	The number of packets monitored in the specified time period.
bytes	The number of bytes monitored in the specified time period.
start	The start time of the monitoring time period.
end	The end time of the monitoring time period.
log-status	The logging status of the flow log: Supported values include: · OK: Data is normally recorded. · NODATA: There is no traffic recorded going to or coming from the ENI during the monitoring time period. · SKIPDATA: Some flow log records were skipped during the monitoring time period.
action	Actions associated with the traffic. Supported values include: · ACCEPT: Traffic that security groups allow to be recorded · REJECT: Traffic that security groups do not allow to be recorded

Create a flow log

Note:

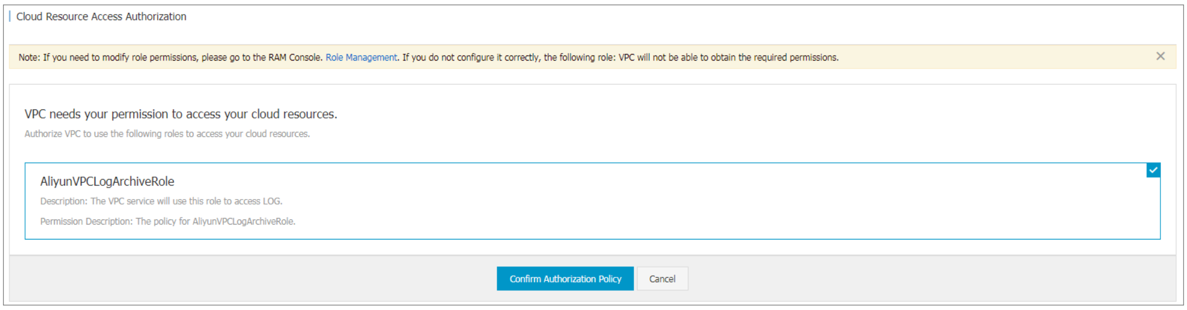
Before creating a flow log, make sure that Log Service is activated.

After you have activated Log Service, you can create flow logs. To do so, follow these steps:

1. Log on to the *VPC console*.

2. In the left-side navigation pane, click FlowLog.
3. If it is the first time that you activate the flow logs function, click Confirm Authorization Policy to authorize VPC to write data to your specified LogStore.

> Note:
> Authorization is required only when the primary account uses the flow log function for the first time.



Cloud Resource Access Authorization

Note: If you need to modify role permissions, please go to the RAM Console. Role Management. If you do not configure it correctly, the following role: VPC will not be able to obtain the required permissions.

VPC needs your permission to access your cloud resources.

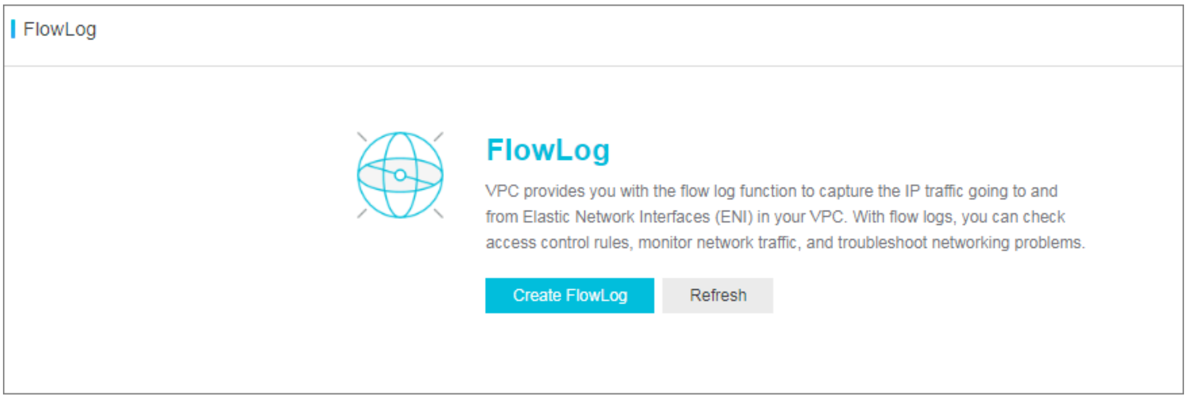
Authorize VPC to use the following roles to access your cloud resources.

☑ AliyunVPCLogArchiveRole

Description: The VPC service will use this role to access LOG.

Permission Description: The policy for AliyunVPCLogArchiveRole.

4. Select the region in which to monitor flow logs and then click Create Flow Log.



FlowLog

FlowLog

VPC provides you with the flow log function to capture the IP traffic going to and from Elastic Network Interfaces (ENI) in your VPC. With flow logs, you can check access control rules, monitor network traffic, and troubleshoot networking problems.

5. On the Create Flow Log page, configure the flow log according to the following information and then click OK.

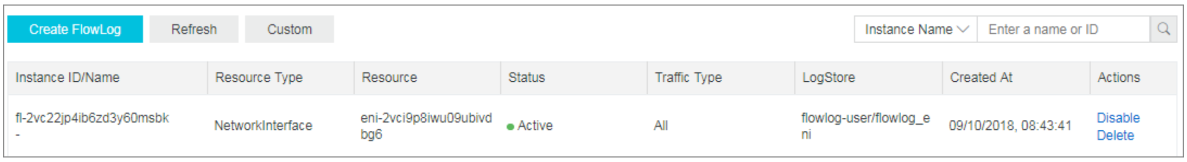
Configuration	Description
Name	Enter a name for the flow log.
Resource Type	Select the resource where a flow log is created: · `ENI` : Monitor IP traffic for the selected ENI. · `VSwitch` : Monitor IP traffic for all ENIs in the selected VSwitch. · `VPC` : Monitor IP traffic for all ENIs in the selected VPC.

Configuration	Description
Traffic Type	Select the type of traffic to be monitored: · `All` : All traffic is monitored. · `Allow` : Only monitor traffic that is allowed by the security group rules. · `Drop` : Only monitor traffic that is not allowed by the security group rules.
LogStore	Select the LogStore in which to store the monitored traffic information.
Turn on FlowLog Analysis Report Function	If this option is selected, the LogSearch/Analytics (index) function is automatically enabled and a dashboard is created for the selected LogStore, so that you can perform SQL and visualized analysis of the collected data. The indexing function of Log Service incurs fees. However, the dashboard is provided free of charge. For more information, see *Log Service Billing*. Note: This option is available only when the report function of the selected LogStore is not enabled.
Description	Enter a description for the flow log.

View logs

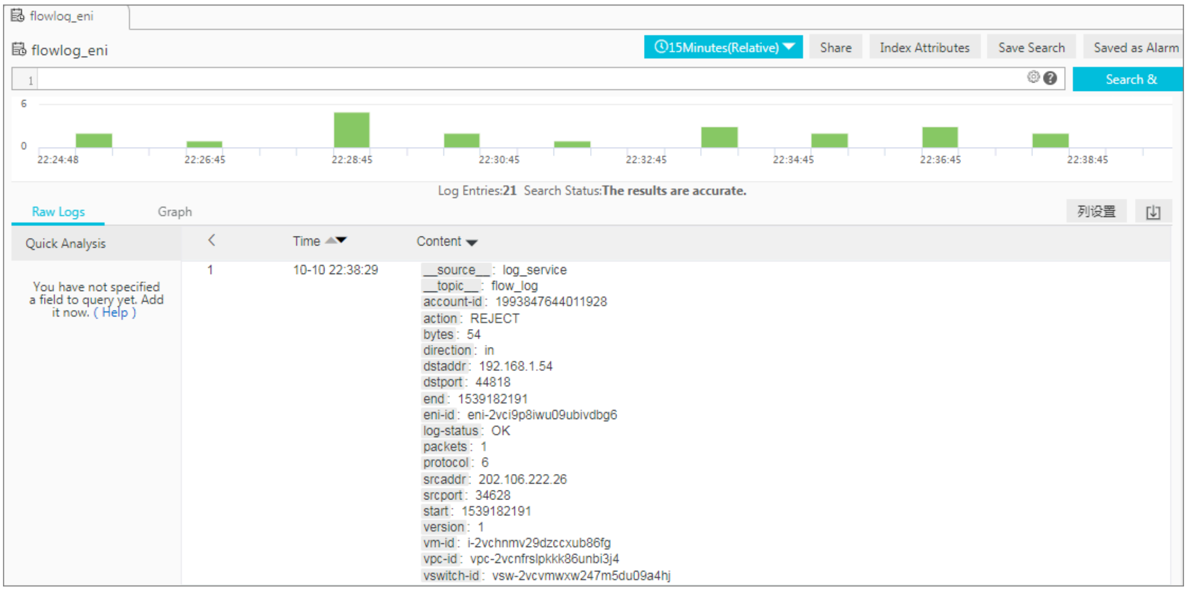
To view the monitored traffic information, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click Flow Log.
3. Select the target region, and then click the LogStore link of the flow log.



Instance ID/Name	Resource Type	Resource	Status	Traffic Type	LogStore	Created At	Actions
fl-2vc22jp4ib6zd3y60msbk -	NetworkInterface	eni-2vci9p8iwu09ubivdbg6	● Active	All	flowlog-user/flowlog_eni	09/10/2018, 08:43:41	Disable Delete

4. On the Log Service console, click Search.



Log Entries:21 Search Status:**The results are accurate.**

You have not specified a field to query yet. Add it now. (Help)

```
1    10-10 22:38:29    __source__: log_service
                       __topic__: flow_log
                       account-id: 1993847644011928
                       action: REJECT
                       bytes: 54
                       direction: in
                       dstaddr: 192.168.1.54
                       dstport: 44818
                       end: 1539182191
                       eni-id: eni-2vci9p8iwu09ubivdbg6
                       log-status: OK
                       packets: 1
                       protocol: 6
                       srcaddr: 202.106.222.26
                       srcport: 34628
                       start: 1539182191
                       version: 1
                       vm-id: i-2vchnmv29dzccxub86fg
                       vpc-id: vpc-2vcnfrslpkkk86unbi3j4
                       vswitch-id: vsw-2vcvmwxw247m5du09a4hj
```

Disable a flow log

You can disable a flow log when you no longer need to monitor the corresponding traffic information.

To disable a flow log, follow these steps:

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click Flow Log.
3. Select the target region, find the target flow log, and then click Disable.

Limits

Before you activate the flow log function, note the following:

- The object where a flow log is created can only be ENI.
- Only the following resource types support the creation of flow logs: VPC, VSwitch, and ENI.
- The maximum number of flow log instances that can be created in each region is 10. If you need to create more flow log instances, open a ticket.

6 Manage quotas

You can query the number of remaining resources in your quota through the VPC console. If the remaining quota number is insufficient for your requirements, you can open a ticket to apply for an increase to your quota.

Procedure

1. Log on to the *VPC console*.
2. In the left-side navigation pane, click Quota Management.
3. On the Quota Management page, click the VPC tab page to view the quota usage of VPCs under your account.
4. To increase your resource quota, click Apply in the Actions column. Then, enter the following information.
    - Quantity for Application: the number of resources you require. You must enter a number that is larger than the current quota. For more information about the resource limits of VPC, see *Limits*.
    - Reason for Application: your reason for applying for an increase to your quota. We recommend that you include details about your specific scenario.
    - Mobile/Landline Phone Number: the mobile or landline phone number of the person to contact.
    - Email: the email address of the person to contact.
5. Click OK.

    The system then determines whether the quota application is reasonable.

    - If the system determines the request is unreasonable, the application enters the Rejected state.
    - If the application is reasonable, the application status enters the Approved state and the quota is automatically upgraded to the specified quota number.

    To view the history of quota applications, click Application History in the Application History.