ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud
VPCs and VSwitches

Document Version: 20210202

Alibaba Cloud

Legal disclaimer

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

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

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

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

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

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

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

Document conventions

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

Table of Contents

1.Overview

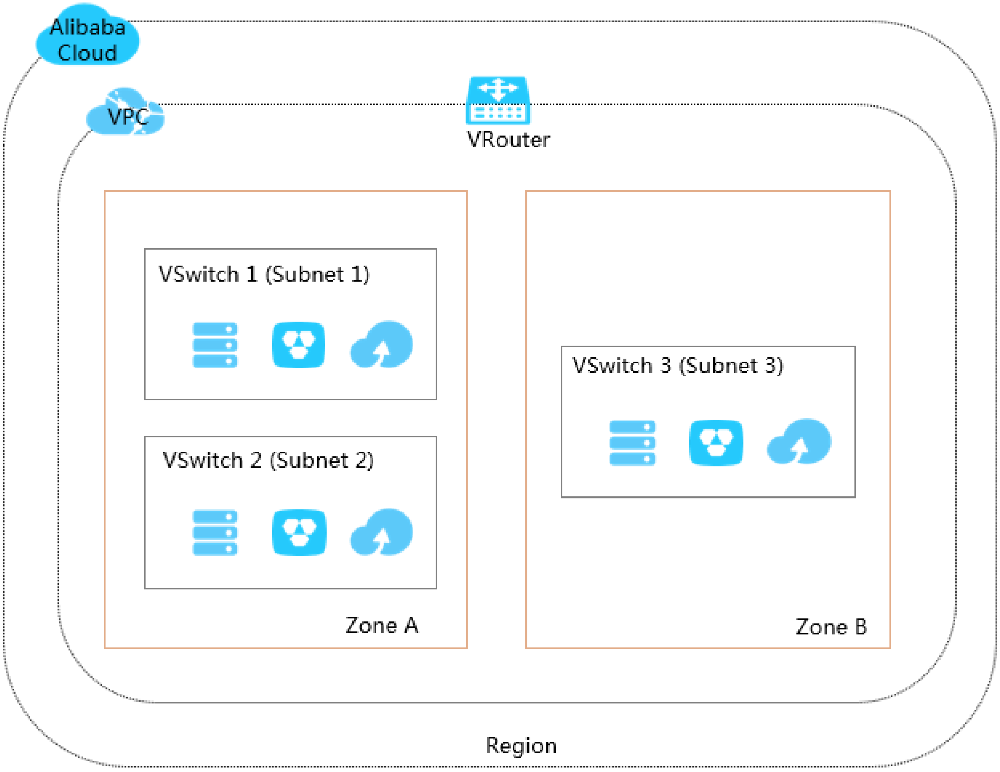
To get started with Virtual Private Cloud, you must create at least one Virtual Private Cloud (VPC) and one or more VSwitches. You can create more than one VSwitch to divide a VPC into multiple subnets. By default, the subnets in a VPC network can communicate with each other over the private network.

VPCs and VSwitches

A VPC is a virtual private network in which you can deploy your cloud resources.

> **Note** cannot be directly deployed in a VPC, but can be connected to a VSwitch in the VPC and deployed in the subnet that is specified by the VSwitch.

A VSwitch is a basic network device that is used to build a VPC network and connect cloud resource instances. A VPC is a region-specific resource. A VPC cannot be deployed across regions. However, A VPC contains all zones in the region to which the VPC belongs. You can create one or more VSwitches in a zone to divide the zone into subnets.



CIDR blocks and IP addresses

VPCs support both IPv4 and IPv6 addressing protocols. By default, VPCs use the IPv4 addressing protocol. However, you can enable the IPv6 addressing protocol based on your business requirements.

VPCs can communicate in dual-stack mode. Cloud resources in a VPC network can communicate by using IPv4 and IPv6 addresses. IPv4 and IPv6 addresses are independent of each other. Therefore, you must configure routing and security groups in your VPC network for IPv4 and IPv6 addresses.

The following table summarizes the differences between IPv4 and IPv6 addresses in a VPC network.

IPv4 VPC	IPv6 VPC
32 bits, 4 groups. Each group consists of up to 3 decimal digits.	128 bits, 8 groups. Each group consists of 4 hexadecimal digits.
By default, IPv4 addressing protocol is enabled for all VPCs.	IPv6 addressing protocol is optional for a VPC network.
The classless inter-domain routing (CIDR) block size for a VPC network can be from /8 to /24.	The size of CIDR block for a VPC network is /56.
The size of CIDR block for a VSwitch can be from /16 to /29.	The size of CIDR block for a VSwitch is /64.
You can select an IPv4 CIDR block for your VPC network.	You cannot select an IPv6 CIDR block. The system automatically assigns an IPv6 CIDR block to your VPC from the IPv6 address pool.
Supported by all instance types.	Not supported on specific instance types. For more information, see Instance families.
ClassicLink connections are supported.	ClassicLink connections are not supported.
Elastic IPv4 addresses are supported.	Elastic IPv6 addresses are not supported.
VPN gateways and NAT gateways are supported.	VPN gateways and NAT gateways are not supported.

By default, the IPv4 and IPv6 addresses provided for VPCs can only be used to communicate within the private network. Cloud resources under different VSwitches in a VPC can only communicate with each other over a private network. To connect a VPC to another VPC or a data center, you can configure Smart Access Gateway (SAG), Express Connect, or VPN Gateway. For more information, see Connect an on-premises data center to a VPC network.

To enable cloud resources in a VPC network to access the Internet, you need to configure the following settings:

- IPv4 communication

  You can configure a NAT gateway or associate elastic IP addresses (EIPs) with Elastic Compute Service (ECS) instances in a VPC. This way, these ECS instances can access the Internet by using IPv4 addresses.

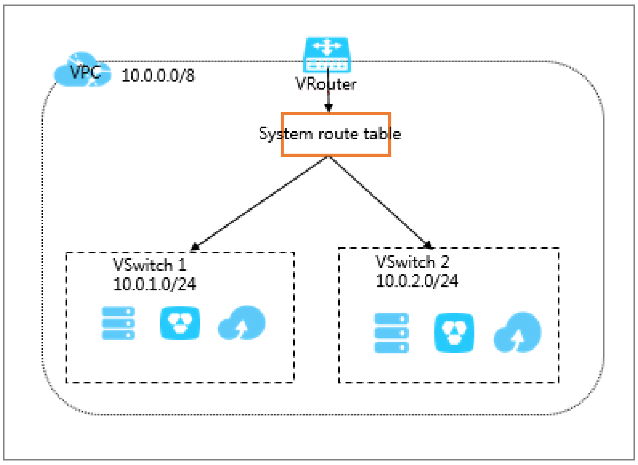
  For more information, see Associate an EIP with an ECS instance and Enable ECS instances to access the Internet through SNAT.

- IPv6 communication

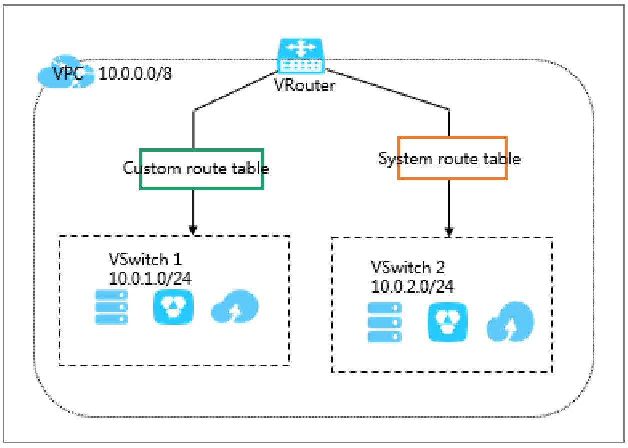
  To enable cloud resources in a VPC network to access the Internet by using IPv6 addresses, you must purchase Internet bandwidth plans for IPv6 addresses. You can configure an egress-only rule for an IPv6 address. This allows cloud resource instances in the VPC network to access the Internet by only using the IPv6 address. IPv6 clients are not allowed to establish connections with these cloud resource instances.

Routes

Alibaba Cloud automatically creates a default route table and adds system route entries to the default route table after you create a VPC network. Each VPC network has only one system route table. This route table is automatically generated when you create a VPC. You cannot create or delete system route tables.



You can create and associate custom route tables with VSwitches to control how each VSwitch routes traffic. A VSwitch can only be associated with one route table at a time. For more information, see Create a custom route table.



If one destination address matches more than one route entry in a route table, the system selects an entry by implementing the longest prefix match algorithm. 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 traffic to a specified IP address. For more information, see Add a custom route entry.

2.Create a default Virtual Private Cloud (VPC) network and VSwitch

You can use default VPC networks and VSwitches when you create Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and ApsaraDB for RDS instances. If you have not created a default VPC network or VSwitch, they are automatically created after you create an ECS, SLB, or ApsaraDB for RDS instance.

Default VPC networks and VSwitches

You can create only one default VPC network in one region and one default VSwitch for each zone in a VPC network. The following table lists the descriptions of default VPC networks and VSwitches:

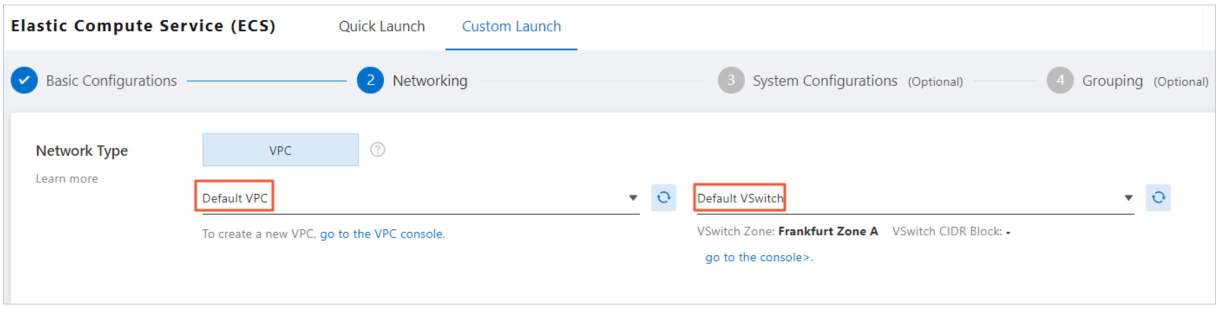
Default VPC network	Default VSwitch
You can create only one default VPC network in one region.	You can create only one default VSwitch for each zone in a VPC network.
The subnet mask for a default VPC network has 16 bits, such as 172.31.0.0/16, which provides up to 65,536 internal IP addresses.	The subnet mask for a default VSwitch has 20 bits, such as 172.16.0.0/20, which provides up to 4,096 internal IP addresses.
Default VPC networks do not consume the VPC quota allocated by Alibaba Cloud.	Default VSwitches do not consume the VSwitch quota in a VPC network.
Default VPC networks are created by Alibaba Cloud. Manually created VPC networks are not default VPC networks.	Default VSwitches are created by Alibaba Cloud. Manually created VSwitches are not default VSwitches.
The operations and specification limits of default VPC networks are the same as those of manually created VPC networks.	The operations and specifications of default VSwitches are the same as those of manually created VSwitches.

Create cloud resources for default VPC networks and VSwitches

You can use default VPC networks and VSwitches when you create ECS, SLB, and ApsaraDB for RDS instances. For more information, see:

- Create ECS instances
- Create SLB instances
- Create ApsaraDB for RDS instances

Note If you want to use default VPC networks and VSwitches when you create ECS instances, make sure that you have not created any VPC network in the region where you want to deploy the ECS instance.



Network Type: VPC

Learn more

Default VPC

To create a new VPC, go to the VPC console.

Default VSwitch

VSwitch Zone: **Frankfurt Zone A** VSwitch CIDR Block: **-**

go to the console>.

3.VPC and subnets

3.1. Create a VPC

This topic describes how to create a virtual private cloud (VPC). A VPC functions as a private network deployed in the cloud You have full control over your VPC. For example, you can specify Classless Inter-domain Routing (CIDR) blocks, configure route tables, and set network gateways for your VPC. You can deploy Alibaba Cloud resources in your own VPC, such as Elastic Compute Service (ECS) instances, ApsaraDB for RDS instances, and Server Load Balancer (SLB) instances.

Prerequisites

Before you create a VPC, you must have network subnetting prepared. For information, see Plan and design a VPC.

Procedure

1. Log on to the VPC console.
2. In the top navigation bar, select the region where you want to deploy the VPC.

   > ? **Note** The VPC must be in the same region as the cloud resources that you want to deploy.

3. On the **VPC** page, click **Create VPC**.
4. On the **Create VPC** page, set the following parameters and click **OK**.

Parameter	Description
VPC	
Region	The region where the VPC to be deployed.
Name	Enter a name for the VPC that you want to create. The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter.

Parameter	Description
IPv4 CIDR Block	Select the primary IPv4 CIDR block for the VPC. The following setting methods are supported: ○ **Default CIDR Block**: You can use one of the following standard IPv4 CIDR blocks: 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8. ○ **Custom CIDR Block**: You can use 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, and their subnets as the primary IPv4 CIDR blocks of your VPC. The CIDR block mask must be 8 to 24 bits in length. For example, enter 192.168.0.0/16. To use a public CIDR block as the primary CIDR block of the VPC,submit a ticket. ? **Note** After you create a VPC, you cannot change its primary IPv4 CIDR block. However, you can add a secondary IPv4 CIDR block to the VPC. For more information, see Add a secondary IPv4 CIDR block.
Description	The description of the VPC. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://` .
VSwitch	
Name	Enter a name for the VSwitch. The name must be 2 to 128 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter.
Zone	Select a zone for the VSwitch. In a VPC, VSwitches in different zones can communicate with each other.
Zone Resource	Displays the cloud instances that can be created in the specified zone. The supported cloud resources vary based on the zone and the time when you create cloud resources. The buy page displays whether the cloud instances are available. Only ECS, RDS, and SLB instances can be queried on the buy page.

Parameter	Description
IPv4 CIDR Block	Specify an IPv4 CIDR block for the VSwitch. Note the following limits when you specify an IPv4 CIDR block: ○ The CIDR block of a VSwitch must be a subset of the CIDR block of the VPC to which the VSwitch belongs. 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 any CIDR block from 192.168.0.0/17 to 192.168.0.0/29. ○ The first and 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 a VSwitch needs to communicate with the VSwitches in other VPCs or on-premises data centers, make sure that the CIDR blocks involved do not overlap with each other. **Note** After you create a VSwitch, you cannot modify the CIDR block.
Number of Available Private IPs	Displays the number of available IP addresses.
Description	Enter a description for the VSwitch. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://` .

Related information

- CreateVpc

3.2. Modify the name and description of a VPC

This topic describes how to modify the name and description of a virtual private cloud (VPC).

Procedure

1. Log on to the VPC console.
2. In the top navigation bar, select the region where your VPC is deployed.
3. On the **VPCs** page, find the target VPC network and click **Manage** in the **Actions** column.
4. In the **VPC Details** section, click **Edit** next to **Name**. In the dialog box that appears, enter a new name for the VPC and click **OK**.The name must be 2 to 128 characters in length and can contain letters, Chinese characters, digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.

5. Click **Edit** next to **Description**. In the dialog box that appears, enter a new description, and click **OK**.The description must be 2 to 256 characters in length and cannot start with `http://` or `https://` .

Related information

- ModifyVpcAttribute

3.3. Add a secondary IPv4 CIDR block

This topic describes how to expand a virtual private cloud (VPC) by adding a secondary IPv4 CIDR block to the VPC.

Prerequisites

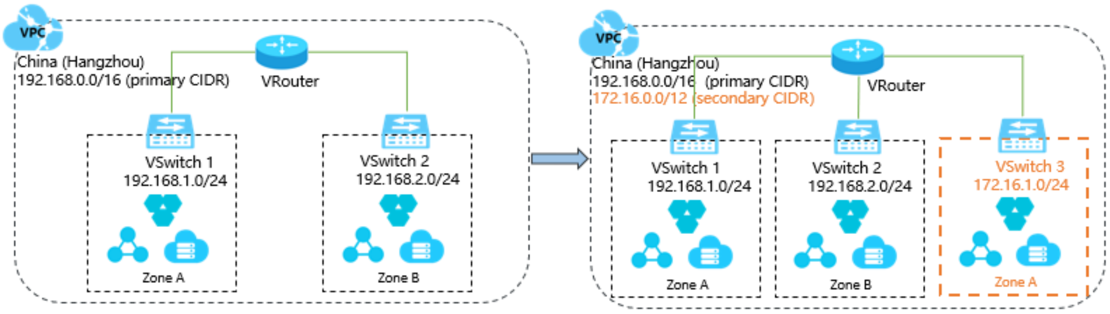
A VPC is created. For more information, see Create a VPC.

Context

When you create the VPC, the IPv4 CIDR block you specified is the primary CIDR block. After the VPC is created, the primary IPv4 CIDR block of the VPC cannot be modified. However, you can add a secondary IPv4 CIDR block to expand the VPC. After you add the secondary IPv4 CIDR block, both the primary and secondary IPv4 CIDR blocks are in effect. You can create a VSwitch with the primary CIDR block or secondary CIDR block. However, each VSwitch belongs to only one VPC CIDR block.

The system automatically adds a VSwitch route to the VPC route table when you create a VSwitch with the primary or secondary CIDR block. The destination CIDR block of a VSwitch route is the CIDR block with which the VSwitch is created. The CIDR block range cannot be the same as or larger than those of other routes in the route table of the VPC.

For example, you have added 172.16.0.0/16 to the VPC as a secondary IPv4 CIDR block. The VPC route table already contains Cloud Enterprise Network (CEN) routes (overlapping routing is enabled), and the destination CIDR block is 172.16.0.0/24. In this case, you cannot create a VSwitch with a CIDR block that is the same or larger than the CIDR block 172.16.0.0/24. However, you can create a VSwitch with 172.16.0.0/25 or a smaller CIDR block.



VPC has one CIDR block

VPC has two CIDR blocks

> ? **Note** You can add only one secondary IPv4 CIDR block to a VPC and you cannot increase the quota.

Procedure

1. Log on to the VPC console.
2. In the top navigation bar, select the region where the VPC is deployed.
3. On the **VPC** page, find the VPC that you want to manage, and click **Manage** in the **Actions** column.
4. On the **VPC details** page, click **CIDRs**, and then click **Add IPv4 CIDR**.
5. In the **Add Secondary CIDR** dialog box, configure the secondary IPv4 CIDR block based on the following parameters and click **OK**.

Parameter	Description
VPC	The VPC to which you want to add the secondary IPv4 CIDR block.
Secondary CIDR	Select a method to configure the secondary IPv4 CIDR block: ○ **Default CIDR Block**: You can specify one of the following standard IPv4 CIDR blocks as the secondary IPv4 CIDR block: 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8. ○ **Custom CIDR Block**: You can specify one of the following standard IPv4 CIDR blocks and their subnets as the secondary IPv4 CIDR block: 192.168.0.0/16, 172.16.0.0/12, and 10.0.0.0/8. To use a public CIDR block as the secondary IPv4 CIDR block,submit a ticket. When you add a secondary IPv4 CIDR block, note the following rules: ○ The CIDR block cannot start with 0. The subnet mask must be 8 to 24 bits in length. ○ The secondary CIDR block cannot overlap with the primary CIDR block or other secondary CIDR blocks of the VPC. For example, if the primary IPv4 CIDR block of a VPC is 192.168.0.0/16, you cannot specify the following CIDR blocks as secondary IPv4 CIDR blocks: ■ A larger CIDR block that overlaps with 192.168.0.0/16, such as 192.168.0.0/8. ■ 192.168.0.0/16. ■ A smaller CIDR block that overlaps with 192.168.0.0/16, such as 192.168.0.0/24.

What's next

Create a VSwitch

Related information

- AssociateVpcCidrBlock

3.4. Delete a secondary IPv4 CIDR block

This topic describes how to delete a secondary IPv4 CIDR block of a Virtual Private Cloud (VPC) network. You cannot delete the primary IPv4 CIDR block of a VPC network.

Prerequisites

You have deleted the VSwitch that is created with the secondary IPv4 CIDR block. For more information, see Delete a VSwitch.

Procedure

1. Log on to the VPC console.
2. On the top of the page, select the region where your VPC network is deployed.
3. On the **VPCs** page, find the VPC network that you want to manage, and click **Manage** in the **Actions** column.
4. On the VPC Details page, click the **CIDRs** tab.
5. Find the secondary IPv4 CIDR block that you want to delete, and click **Delete** in the **Actions** column.
6. In the message that appears, click **OK**.

Related information

- UnassociateVpcCidrBlock

3.5. Attach a VPC network to a CEN instance

This topic describes how to attach a Virtual Private Cloud (VPC) network to a Cloud Enterprise Network (CEN) instance. You can use a CEN instance to establish a private connection between two VPC networks, or between a VPC network and an on-premises data center to interconnect global cloud resources. You can attach a VPC network to a CEN instance under the same account, or attach a VPC network to a CEN instance under another account after authorization.

Attach a VPC network to a CEN instance under the same account

You can attach a VPC network to a CEN instance under the same account. In this way, the VPC can communicate with other VPC networks or on-premises data centers attached to the CEN instance. For more information, see Attach a VPC or a VBR to a CEN instance.

Attach a VPC network to a CEN instance across accounts

You can attach a VPC network to a CEN instance under another account after authorization. In this way, the VPC network can communicate with the instances attached to the CEN. For more information, see Acquire permissions from another Alibaba Cloud account.

3.6. Delete a VPC network

This topic describes how to delete a Virtual Private Cloud (VPC) network. After you delete a VPC network, the VRouters and route tables associated with this VPC network are also deleted.

Prerequisites

Before you delete a VPC network, make sure that the following requirements are met:

- No VSwitch exists in the VPC network. If the VPC network contains a VSwitch, you must delete the

VSwitch before you delete the VPC network. For more information, see Delete a VSwitch.

- No IPv6 gateway is associated with the VPC network. If the VPC network is associated with an IPv6 gateway, you must delete the IPv6 gateway before you delete the VPC network.

Procedure

1. Log on to the VPC console.
2. On the top of the page, select the region where your VPC network is deployed.
3. On the **VPCs** page, find the VPC that you want to manage, and click **Delete** in the **Actions** column.
4. In the **Delete VPC** message, click **OK**.

4.VSwitch management

4.1. Create a VSwitch

A VSwitch is a basic network device in a Virtual Private Cloud (VPC) network and is used to connect cloud resources.

Context

After you create a VPC network, you can create VSwitches to divide the VPC network into one or more subnets. VSwitches within the same VPC network can communicate with each other. Cloud resources must be deployed within the CIDR blocks of VSwitches. You can deploy applications in zones that are managed by different VSwitches to improve service availability.

? **Note** VSwitches do not support multicast or broadcast.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VSwitches**.
3. In the top navigation bar, select the region where you want to deploy the VSwitch.
4. On the **VSwitches** page, click **Create VSwitch**.
5. In the **Create VSwitch** pane, set the following parameters and click **OK**.

? **Note** IPv6 CIDR blocks are supported in the following regions: China (Shenzhen), China (Beijing), China (Hohhot), China (Shanghai), and China (Hong Kong). After you enable the IPv6 CIDR block feature, the system automatically creates an IPv6 gateway.

Parameter	Description
VPC	Select the VPC network to which the VSwitch belongs.
CIDR	Displays the IPv4 CIDR block of the VPC network. If the VPC network has a secondary IPv4 CIDR block, you can select the primary or secondary CIDR block for the VSwitch based on your business requirements.
IPv6 CIDR Block	Displays the IPv6 CIDR block of the VPC network. ? **Note** If the IPv6 CIDR block feature is not enabled for the VPC network, click **Enable IPv6 CIDR Block**. After the IPv6 CIDR block feature is enabled, the system automatically creates an IPv6 gateway that is free of charge.

Parameter	Description
Name	Enter a name for the VSwitch. The name must be 2 to 128 characters in length, and can contain digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.
Zone	Select a zone for the VSwitch. In a VPC network, VSwitches in different zones can communicate with each other.
IPv4 CIDR Block	Specify an IPv4 CIDR block for the VSwitch. Note the following limits when you specify an IPv4 CIDR block: ○ The CIDR block of the VSwitch must be a subset of the CIDR block of the VPC network. For example, if the CIDR block of the VPC network is 192.168.0.0/16, the CIDR block of the VSwitch can range from 192.168.0.0/17 to 192.168.0.0/29. ○ The first and last three IP addresses of each VSwitch are reserved. For example, if the CIDR block of a VSwitch 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 is required to communicate with VSwitches in other VPC networks or with on-premises data centers, make sure that the CIDR block of the VSwitch does not overlap with the destination CIDR blocks. ○ The CIDR block of a VSwitch cannot be the same as or larger than the destination CIDR block of a route in the route table of the VPC network to which the VSwitch belongs. For example, if a Cloud Enterprise Network (CEN) route (overlapping routing enabled) with a destination CIDR block of 172.16.0.0/24 is already added to the route table of the VPC network, the CIDR block of the VSwitch must fall within 172.16.0.0/24. You can use 172.16.0.0/25 or a smaller CIDR block as the CIDR block of the VSwitch. ○ CIDR blocks of VSwitches in the same VPC network cannot overlap with each other. If a CIDR block overlaps with another one, you must modify the CIDR block. **Notice** After you create a VSwitch, you cannot modify its CIDR block.
Number of Available Private IPs	Displays the number of available IPv4 addresses of the VSwitch.

Parameter	Description
IPv6 CIDR Block	Specify an IPv6 CIDR block for the VSwitch. By default, the mask for the IPv6 CIDR block of a VSwitch is /64. You can enter a number from 0 to 255 to define the last 8 bits of the IPv6 CIDR block. For example, if the IPv6 CIDR block of the VPC network is 2xx1:db8::/64, you can enter ff (the hexadecimal string of 255) for the IPv6 CIDR block of the VSwitch. The IPv6 CIDR block of the VSwitch is 2xx1:db8:ff::/64.
Description	Enter a description for the VSwitch. The description must be 2 to 256 characters in length, and cannot start with `http://` or `https://` .

Related information

- CreateVSwitch

4.2. Create cloud resources in a vSwitch

You cannot directly deploy cloud resources in a virtual private cloud (VPC). You can deploy cloud resources only in a vSwitch that belongs to a VPC. This topic describes how to create cloud resources in a vSwitch.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **vSwitches**.
3. Select the region of the VPC to which the vSwitch belongs.
4. On the **vSwitches** page, find the vSwitch, click **Create** in the **Actions** column, and select the cloud resource that you want to create.You can create Elastic Compute Service (ECS) instances, ApsaraDB RDS instances, and Server Load Balancer (SLB) instances in a vSwitch.
5. On the page that appears, set the parameters.

4.3. Associate a VSwitch with a custom route table

This topic describes how to associate a VSwitch with a custom route table. After you associate a VSwitch with a custom route table, you can use the custom route table to control how the VSwitch routes network traffic. Each VSwitch can be associated with only one custom route table or system route table. After the VSwitch is associated with a custom route table, the system route table is automatically disassociated.

Prerequisites

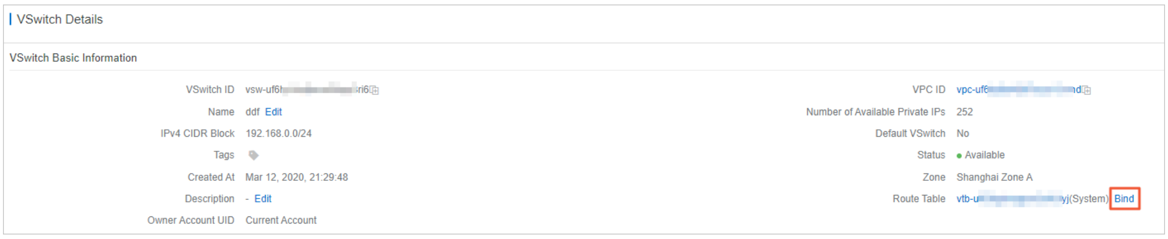
A custom route table is created. For more information, see Create a custom route table.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **vSwitches**.
3. On the top navigation bar, select the region where the VSwitch is deployed.

   > **Note** Custom route tables are supported in all regions except the China (Beijing), China (Shenzhen), and China (Hangzhou) regions.

4. On the **VSwitches** page, find the target VSwitch and click **Manage** in the **Actions** column.
5. In the **VSwitch Basic Information** section, click **Bind** next to the **Route Table** field.



VSwitch Details

VSwitch Basic Information

VSwitch ID vsw-uf6[redacted]ri6

Name ddf Edit

IPv4 CIDR Block 192.168.0.0/24

Tags

Created At Mar 12, 2020, 21:29:48

Description - Edit

Owner Account UID Current Account

VPC ID vpc-uf6[redacted]nd

Number of Available Private IPs 252

Default VSwitch No

Status ● Available

Zone Shanghai Zone A

Route Table vtb-u[redacted]yj(System) Bind

6. In the **Associate Route Table** pane, select the target route table and click **OK**.

4.4. Disassociate a custom route table from a VSwitch

This topic describes how to disassociate a custom route table from a VSwitch. After you disassociate a custom route table, the VSwitch is automatically associated with the system route table.

Procedure

1.
2.
3. In the left-side navigation pane, click **vSwitches**.
4. Select the region of the VPC to which the vSwitch belongs.
5. On the **VSwitches** page, find the target VSwitch, and click **Manage** in the **Actions** column.
6. In the **VSwitch Basic Information** section, click **Unbind** next to the **Route Tables** field.
7. In the **Unbind Route Table** dialog box, click **OK**.

4.5. Associate a network ACL

This topic describes how to associate VSwitches with network ACLs to control access from or to ECS instances in the VSwitches.

Prerequisites

You have created a network ACL. For more information, see Create a network ACL.

Context

Network access control list (ACL) is a feature to implement access control in VPC. You can customize rules for a network ACL and associate VSwitches with the network ACL to control access from or to ECS instances in the VSwitches. You can associate a network ACL with VSwitches when the network ACL and VSwitches belong to a VPC. Each VSwitch can be associated with only one network ACL at a time.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VSwitches**.
3. In the top navigation bar, select a region.
4. On the **VSwitches** page, click **Manage** in the **Actions** column corresponding to the target VSwitch.
5. On the **VSwitch Details** page that appears, find the VSwitch Basic Information section. Click **Bind** next to **Network ACL**.
6. In the **Bind Network ACL** dialog box that appears, select the target network ACL. Click **OK**.

Related information

- AssociateNetworkAcl

4.6. Change a network ACL

This topic describes how to change a network ACL that is associated with VSwitches. After the ACL is changed, the new ACL takes effect immediately and controls access to or from ECS instances in the VSwitches.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VSwitches**.
3. In the top navigation bar, select a region.
4. On the **VSwitches** page, click **Manage** in the **Actions** column corresponding to the target VSwitch.
5. On the **VSwitch Details** page that appears, find the VSwitch Basic Information section. Click **Change** next to **Network ACL**.
6. In the **Bind Network ACL** dialog box that appears, select the target network ACL. Click **OK**.

4.7. Disassociate a network ACL

This topic describes how to disassociate a network ACL from VSwitches. After the VSwitches are disassociated, access to or from the ECS instances is not controlled based on the specified rules of the network ACL.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **VSwitches**.
3. In the top navigation bar, select a region.
4. On the **VSwitches** page, click **Manage** in the **Actions** column corresponding to the target

VSwitch.

5. On the **VSwitch Details** page that appears, find the VSwitch Basic Information section. Click **Unbind** next to **Network ACL**.
6. In the **Unbind Network ACL** message that appears, click **OK**.

Related information

- UnassociateNetworkAcl

4.8. Modify the basic information of a VSwitch

This topic describes how to modify the the name and description of a VSwitch.

Procedure

1.
2.
3. In the left-side navigation pane, click **vSwitches**.
4. Select the region of the VPC to which the vSwitch belongs.
5. On the **VSwitches** page, find the target VSwitch, click **Manage** in the **Actions** column.
6. In the **VSwitch Basic Information** area, click **Edit** after the **Name** field to modify the name of the VSwitch. The name must be 2 to 128 characters in length and can contain letters, numbers, underscores (_) and hyphens (-). It must start with a letter.
7. Click **Edit** after the **Description** field to modify the description of the VSwitch. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://` .

4.9. Delete a VSwitch

This topic describes how to delete a VSwitch that you no longer need. Cloud resources cannot be connected to deleted VSwitches.

Prerequisites

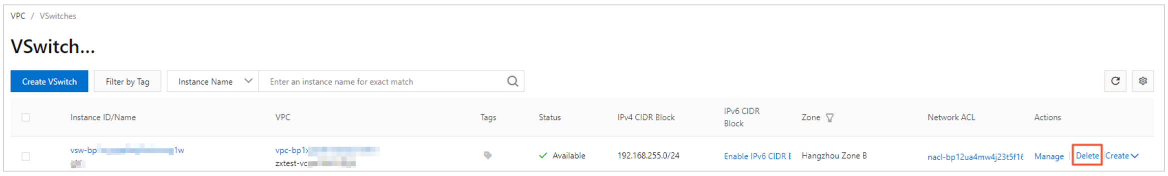
Before you delete a VSwitch, make sure that the following conditions are met:

- You have deleted all of your cloud resources that are created under the VSwitch, such as Elastic Compute Service (ECS) instances, Server Load Balancer (SLB) instances, and ApsaraDB for RDS (RDS) instances.
- You have deleted or disabled all resources and actions associated with this VSwitch, such as high-availability virtual IP addresses (HAVIPs) and source network address translation (SNAT) entries.

Procedure

1.
2.
3. In the left-side navigation pane, click **vSwitches**.
4. Select the region of the VPC to which the vSwitch belongs.

5. On the **VSwitches** page, find the VSwitch that you want to manage and click **Delete** in the **Actions** column.



VPC / VSwitches

VSwitch...

□	Instance ID/Name	VPC	Tags	Status	IPv4 CIDR Block	IPv6 CIDR Block	Zone	Network ACL	Actions
□	vsw-bp[redacted]1w [redacted]	vpc-bp1[redacted] zxtest-vc[redacted]		✓ Available	192.168.255.0/24	Enable IPv6 CIDR E	Hangzhou Zone B	nacl-bp12ua4mw4j23t5f1€	Manage | Delete | Create

6. In the **Delete VSwitch** message, click **OK**.

5.VPC FAQ

This topic provides answers to the commonly asked questions about Virtual Private Cloud (VPC).

What is CIDR?

Classless Inter-Domain Routing is a method for allocating IP addresses and for IP routing. Compared with the previous classful network addressing architecture, CIDR is more efficient in allocating IP addresses. For example, the IP addresses that range from 125.203.96.0 to 125.203.127.255 can be written in the CIDR format:

125.203.0110 0000.0000 0000 to 125.203.0111 1111.1111 1111, or 125.203.96.0/19.

When you create a VPC or VSwitch, you must specify its IP address range in the CIDR format.

What is the difference between a VPC and a classic network?

The differences between a VPC and a classic network are:

- Services that use the classic network are deployed in the public network infrastructure of Alibaba Cloud, and planned and managed by Alibaba Cloud. Classic networks are suitable for users who require networks that are easy to use.
- VPCs are private networks deployed on Alibaba Cloud. VPCs are logically isolated from each other. You can specify a custom topology and IP addresses for a VPC. VPCs are suitable for users who have high network security requirements and network management capabilities.

Does VPC support VPN?

Yes. For more information, see VPN gateways.

How do I specify the CIDR block for a VPC?

You can specify 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, and their subnets as the private CIDR block of the VPC. The subnet mask must be 8 to 24 bits in length.

For more information, see Create a VPC.

How do I specify the CIDR block for a VSwitch?

When you specify the CIDR block for a VSwitch, note that:

- The CIDR block of the VSwitch must fall within the range of the CIDR block of the VPC to which the VSwitch belongs.
- The subnet mask of the VSwitch must be 16 to 29 bits in length.
- The CIDR block of the VSwitch cannot be the same as or a subset of the CIDR block of an existing VSwitch.
- The CIDR block of the VSwitch cannot be the same as the destination CIDR block of any route entry in the VPC.
- The CIDR block of the VSwitch cannot contain the destination CIDR block of any route entry in the VPC, but can be a subnet of a destination CIDR block.

For more information, see Create a VSwitch.

In the same VPC, can an ECS instance deployed in the primary CIDR block communicate with an ECS instance deployed in the secondary CIDR block?

Communication can be established if both ECS instances are added to the same security group. For more information about how to add an ECS instance to a security group, see Add an ECS instance to a security group.

In the same VPC, can I disable the communication between an ECS instance deployed in the primary CIDR block and an ECS instance deployed in the secondary CIDR block?

You can disable the communication by using one of the following methods:

- Configure an access control list (ACL). For more information, see Create a network ACL.

- Configure security group rules. For more information, see Add security group rules.

After I add a secondary CIDR block to a VPC, does the Cloud Enterprise Network (CEN) instance automatically add a route?

If the VPC is associated with a CEN instance, after you add a secondary CIDR block to the VPC, the CEN instance automatically adds a route that specifies the secondary CIDR block as the destination CIDR block to the route table of the CEN instance.

If a VPC has the ClassicLink feature enabled, can an ECS instance deployed in a classic network communicate with an ECS instance deployed in the secondary CIDR block?

No, because the secondary CIDR block does not support the ClassicLink feature.

What is a customer CIDR block?

By default, a VPC uses 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, 100.64.0.0/10, and the CIDR block of the VPC for private network communication. An ECS instance or elastic network interface (ENI) can access the Internet in the following scenarios: The ECS instance is assigned a public IP address, the ECS instance or ENI is assigned an elastic IP address (EIP), or DNAT rules are applied to the ECS instance or ENI. In the preceding cases, when the ECS instance or ENI accesses CIDR blocks other than the preceding ones, the requests are forwarded to the Internet through the public IP address.

If you want the requests to be forwarded based on the route table of a private network (for example, a VPC or a hybrid cloud built with VPN, Express Connect, or CEN), you must set the destination as the customer CIDR block of the VPC to which the ECS instance or ENI belongs. After you set a customer CIDR block for the VPC, the requests that target the customer CIDR block are forwarded based on the route table instead of the public IP address.

For example, ECS 1 is assigned a public IP address. Therefore, when ECS 1 accesses the Alibaba Cloud International site (106.11.62.xx), requests are forwarded through the public IP address. If you want the requests to be forwarded to ECS 2, and then forwarded to the Internet through the IP address of ECS 2. You can set 106.11.62.0/24 as the customer CIDR block of the VPC to which ECS 1 belongs.

How do I configure a customer CIDR block?

You can configure the customer CIDR block when you create a VPC or for an existing VPC. However, the operations are different:

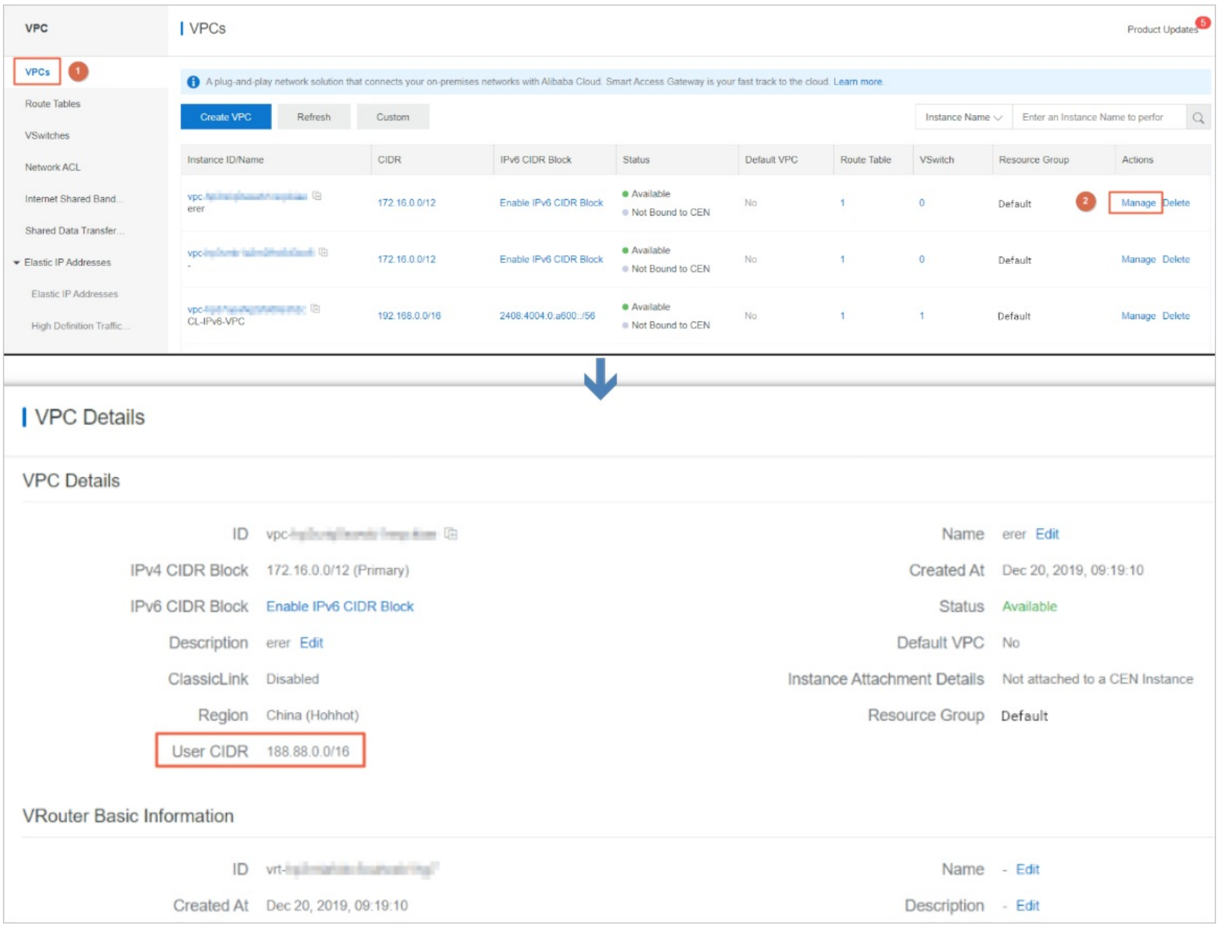
- Configure the customer CIDR block when you create a VPC

  You can only call the CreateVpc operation to configure the customer CIDR block. For more information, see CreateVpc.

- Configure the customer CIDR block for an existing VPC

  To configure the customer CIDR block for an existing VPC,submit a ticket.

After you configure the CIDR block, you can view it on the details page of the VPC.



VPC
VPCs
1
Route Tables
VSwitches
Network ACL
Internet Shared Band...
Shared Data Transfer...
Elastic IP Addresses
Elastic IP Addresses
High Definition Traffic...
VPCs
Product Updates
5
A plug-and-play network solution that connects your on-premises networks with Alibaba Cloud. Smart Access Gateway is your fast track to the cloud. Learn more
Create VPC
Refresh
Custom
Instance Name
Enter an Instance Name to perfor
2

Instance ID/Name	CIDR	IPv6 CIDR Block	Status	Default VPC	Route Table	VSwitch	Resource Group	Actions
vpc-[redacted] erer	172.16.0.0/12	Enable IPv6 CIDR Block	● Available ● Not Bound to CEN	No	1	0	Default	Manage Delete
vpc-[redacted] -	172.16.0.0/12	Enable IPv6 CIDR Block	● Available ● Not Bound to CEN	No	1	0	Default	Manage Delete
vpc-[redacted] CL-IPv6-VPC	192.168.0.0/16	2408:4004:0:a600::/56	● Available ● Not Bound to CEN	No	1	1	Default	Manage Delete

VPC Details

VPC Details

ID	vpc-[redacted]	Name	erer Edit
IPv4 CIDR Block	172.16.0.0/12 (Primary)	Created At	Dec 20, 2019, 09:19:10
IPv6 CIDR Block	Enable IPv6 CIDR Block	Status	Available
Description	erer Edit	Default VPC	No
ClassicLink	Disabled	Instance Attachment Details	Not attached to a CEN Instance
Region	China (Hohhot)	Resource Group	Default
User CIDR	188.88.0.0/16		

VRouter Basic Information

ID	vrt-[redacted]	Name	- Edit
Created At	Dec 20, 2019, 09:19:10	Description	- Edit

Can a VPC have multiple VRouters?

No. Each VPC can have only one VRouter. However, each router can have multiple route tables.

How many custom route entries can I create in a route table?

By default, you can create up to 48 custom route entries in a route table.

You can go to the Quota Management page and request a quota increase. For more information, see Manage service quotas.

How many VSwitches can I create in a VPC?

By default, you can create at most 24 VSwitches in a VPC.

You can go to the Quota Management page and request a quota increase. For more information, see Manage service quotas.

How many private IP addresses can be used for cloud services in each VPC?

Each VPC can use at most 60,000 private IP addresses for cloud services. The quota cannot be increased.

For example, if an ECS instance is assigned only one private IP address, the ECS instance uses one IP address. If an ECS instance is associated with multiple NICs or the NICs are assigned multiple IP addresses, the number of IP addresses used by the ECS instance is the sum of the IP addresses assigned to the NICs that are associated with the ECS instance.

In the same VPC, can ECS instances that belong to different VSwitches communicate with each other?

Yes. In the same VPC, regardless of whether the ECS instances belong to the same VSwitch, the ECS instances can communicate with each other if allowed by security group rules and network ACLs.

Can different VPCs communicate with each other over the private network?

Yes. Different VPCs are logically isolated from each other. However, different VPCs can communicate with each other through Express Connect, VPN Gateway, and CEN. For more information, see Connect VPCs.

Do VPCs support leased lines?

You can connect a VPC to an on-premises data center through leased lines. For more information, see Create a dedicated physical connection.

Can VPCs access Internet services?

Yes. You can allow VPCs to access Internet services by using one of the following methods:

- Assign public IP addresses to the cloud resources in the VPC
- Associate EIPs with the cloud resources in the VPC
- Configure NAT gateways

For more information, see Select a product to gain access to the Internet.

Can the Internet access the cloud resources in a VPC?

Yes. You can allow the Internet to access the cloud resources in the VPC by using one of the following methods:

- Assign public IP addresses to the cloud resources in the VPC
- Associate EIPs with the cloud resources in the VPC
- Configure NAT gateways
- Configure Server Load Balancer (SLB) instances

For more information, see Select a product to gain access to the Internet.

Can a VPC communicate with a classic network?

Yes. You can establish the communication by using one of the following methods:

- Assign a public IP address to an ECS instance in the VPC. This allows the ECS instance to communicate with the cloud resources in the classic network over the Internet. For more information, see Select a product to gain access to the Internet.
- Use the ClassicLink feature to establish low-latency and high-speed connections between ECS instances in a VPC and a classic network. For more information, see Overview.