ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

VPCs and VSwitches

Document Version: 20200828

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 of VPCs and VSwitches

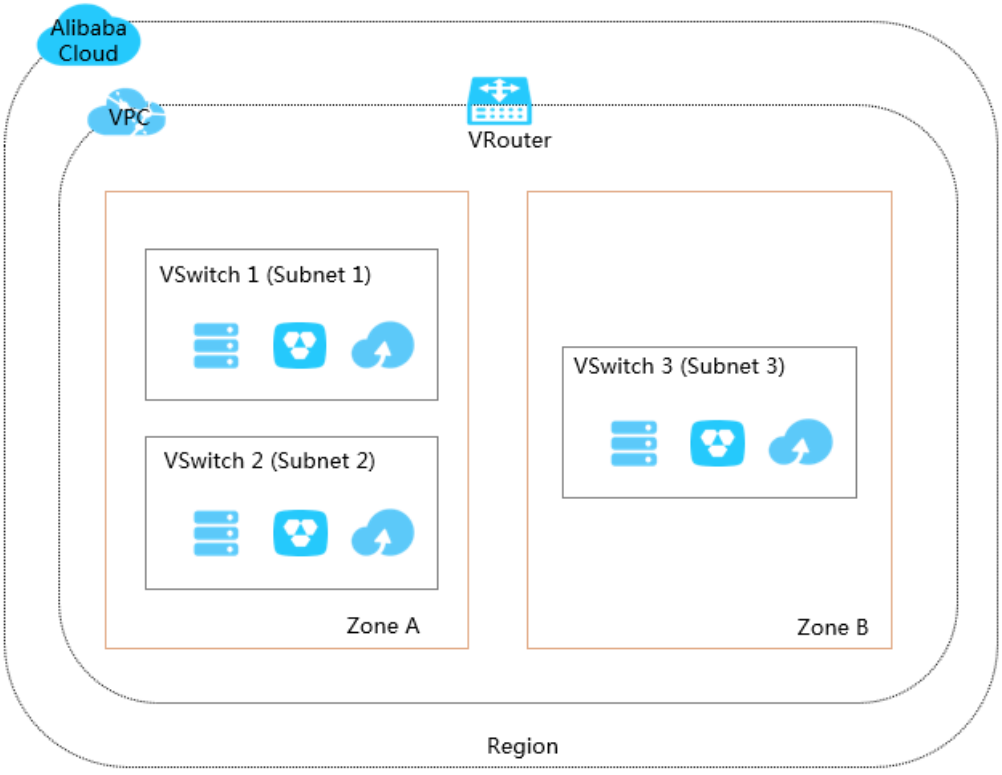
This topic provides an overview of VPCs and VSwitches. You must create a VPC and a VSwitch before you can use the cloud resources in the VPC. You can create more than one VSwitch to divide a VPC into multiple subnets. By default, the subnets in a VPC are interconnected over the intranet.

VPCs and VSwitches

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

> **Note** Cloud resources cannot be directly deployed in a VPC. They must be deployed in a VSwitch (subnet) of the VPC.

A VSwitch is a basic network device that is used to build a VPC and connect cloud resource instances. A VPC is a regional resource. It cannot be deployed across regions, but it contains all zones in the region to which it 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 as needed.

VPCs can operate in dual-stack mode, whereby VPC resources can communicate with each other 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 compares an IPv4 address and an IPv6 address.

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.
The IPv4 address protocol is enabled by default.	The IPv6 address protocol can be enabled manually.
The size of the VPC CIDR block is /56.	The size of the VPC CIDR block is /56.
The size of the VSwitch CIDR block range from /16 to /29.	The size of the VSwitch CIDR block must be /64.
You can select an IPv4 CIDR block.	You cannot select an IPv6 CIDR block. The system assigns 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.
ClassicLink is supported.	ClassicLink is 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, IPv4 and IPv6 addresses of VPCs only support intranet communication. Cloud resources 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, or a VPN Gateway. For more information, see Connect an on-premises data center to a VPC network.

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

- IPv4 Internet communication

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

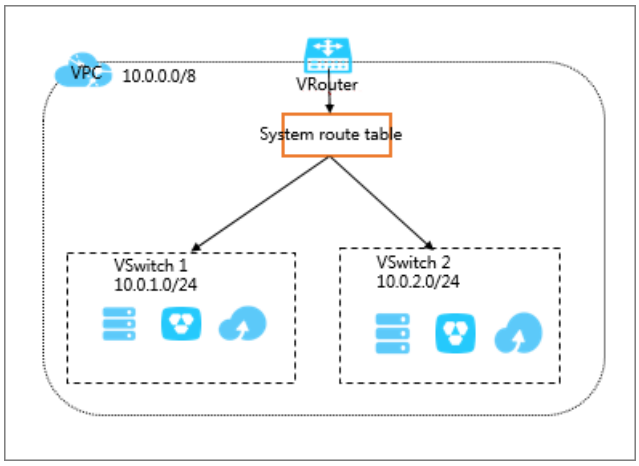
  For more information, see Associate an EIP with an ECS instance and Configure a NAT Gateway.

- IPv6 Internet communication

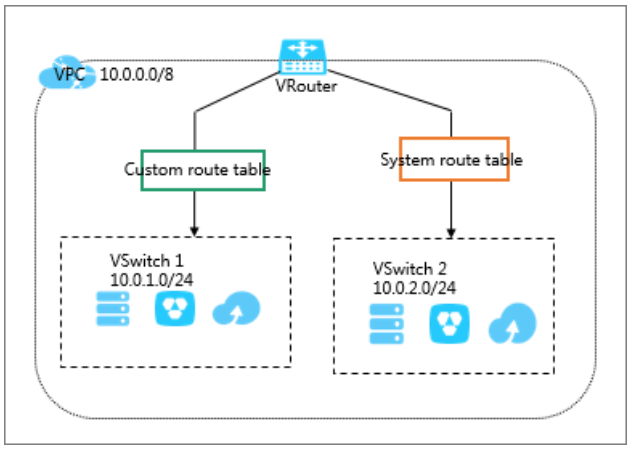
  You need to purchase an Internet bandwidth for the IPv6 address used for communication with the Internet. Then, you can configure an egress-only rule for the IPv6 address. This allows cloud resource instances in the VPC to access the Internet by only using the IPv6 address, but does not allow the IPv6 client to establish connections with these cloud resource instances.

Routes

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



You can create a custom route table in a VPC and then associate it with a VSwitch to control the subnet routing for more flexible network management. Each VSwitch can only be associated with one route table. For more information, see Create a custom route table.



Route tables use 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.

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:

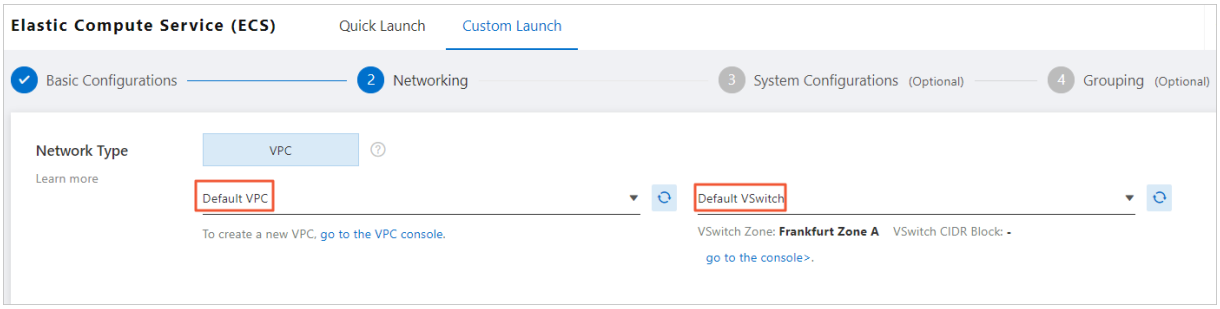
Default VPC network	Default VSwitch
You can create only one default VPC network in one region.	You can create only one default VSwitch for each zone in a VPC network.
The subnet mask for a default VPC network has 16 bits, such as 172.31.0.0/16, which provides up to 65,536 internal IP addresses.	The subnet 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.



3.VPC and subnets

3.1. Create a VPC

A virtual private cloud (VPC) is a private network dedicated for your use. 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 Apsara Stack resources in your VPC, such as Elastic Compute Service (ECS) instances, ApsaraDB for RDS (RDS) instances, and Server Load Balancer (SLB) instances.

Procedure

1. Log on to the VPC console.
2. In the top navigation bar, select a region to deploy your VPC.

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

3. On the **VPC** page, click **Create VPC**.
4. On the **Create VPC** page, configure the VPC and click **Submit**. The following table describes the parameters for creating a VPC.

Parameter	Description
VPC	
Region	The region where the VPC is to be deployed.
Name	Enter a name for the VPC. 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.
IPv4 CIDR Block	Select the primary IPv4 CIDR block for the VPC. The following setting methods are supported: ○ **Recommended CIDR Block**: Enter 192.168.0.0/16, 172.16.0.0/12, or 10.0.0.0/8. ○ **Custom CIDR Block**: Enter 192.168.0.0/16, 172.16.0.0/12, 10.0.0.0/8, or a subset of these CIDR blocks as the primary IPv4 CIDR block of the VPC. The subnet mask must be 8 to 24 bits in length. For example, enter 192.168.0.0/16. If you want to use a public CIDR block as the CIDR block of the VPC, submit a ticket. Notice 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.

Parameter	Description
Description	Enter a description for the VPC network. 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 letters, Chinese characters, digits, underscores (_), and hyphens (-). It must start with a letter or a Chinese character.
Zone	Select a zone to deploy the VSwitch. VSwitches within a VPC can communicate with each other across zones over the private network.
Zone Resources	Displays the types of cloud resources that you can create in the zone. The supported cloud resources vary, depending on the zone and the time when you want to create cloud resources. The buy page displays which cloud instances are available. Currently, you can check the availability of ECS, RDS, and SLB instances on the buy page.
IPv4 CIDR Block	Enter 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 this VSwitch resides in. For example, if the CIDR block of a VPC is 192.168.0.0/16, the CIDR block of a VSwitch in the VPC must be a segment from 192.168.0.0/17 to 192.168.0.0/29. ○ The first and the last three IP addresses in each VSwitch CIDR block are reserved by the system. 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, you must make sure that the CIDR blocks involved do not conflict with each other. **Notice** After you create a VSwitch, you cannot modify its CIDR block.
Number of Available Private IPs	Displays the number of available IP addresses.

Parameter	Description
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 basic information about a VPC network

This topic describes how to modify the name and description of a Virtual Network Cloud (VPC) network.

Prerequisites

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

Procedure

1. Log on to the VPC console.
2. In the top status bar, select the region where your VPC network 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 network and click **OK**. The name must be 2 to 128 characters in length and can contain digits, underscores (_), and hyphens (-). It must start with a letter or 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) network by adding a secondary IPv4 CIDR block to the VPC network.

Prerequisites

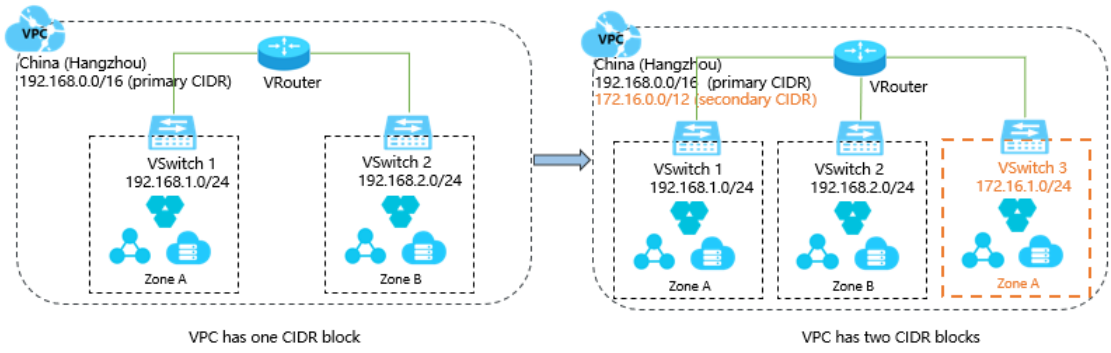
A VPC network is created. For more information, see Create a VPC.

Context

When you create a VPC network, you must specify the primary IPv4 CIDR block of the VPC network. After the VPC network is created, the primary IPv4 CIDR block of the VPC network cannot be modified. However, you can add a secondary IPv4 CIDR block to expand the VPC network. After you add the secondary IPv4 CIDR block, 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 can not be the same as or larger than those of other routes in the route table of the VPC network.

For example, you have added 172.16.0.0/16 to the VPC network as a secondary IPv4 CIDR block. The VPC route table already contains 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 the CIDR block 172.16.0.0/25 or a smaller one.



Note By default, you can add only one secondary IPv4 CIDR block to each VPC network. You can submit a ticket to increase the quota. After your application is approved, up to three secondary IPv4 CIDR blocks can be added to a 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 **VPC** page, find the VPC network that you want to manage, and click **Manage** in the **Actions** column.
4. On the VPC details page, click **CIDRs**tab, and click **Add IPv4 CIDR**.
5. In the **Add Secondary CIDR** dialog box, configure a secondary IPv4 CIDR block based on the following information, and click **OK**.

Parameter	Description
VPC	The VPC network 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. If you need to specify a public IP address range as the secondary IPv4 CIDR block of a VPC network, submit a ticket. You must follow these rules when you add a secondary IPv4 CIDR block: ○ The CIDR block cannot start with 0. The 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 network. For example, the primary IPv4 CIDR block of a VPC network 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. ■ CIDR block 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 VBR to CEN through the VPC or Express Connect console.

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 Cross-account authorization.

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

This topic describes how to create cloud resources in a VSwitch. You can deploy cloud resources in a VPC network only after you create these resources in a VSwitch (subnet) of the VPC network. You can 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 network where the VSwitch is deployed.
4. On the **VSwitches** page, find the target VSwitch, click **Purchase** in the **Actions** column, and select the cloud resource you want to create. You can create ECS instances, SLB instances, and RDS instances in a VSwitch.
5. On the cloud resource creation page, create a cloud resource.

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

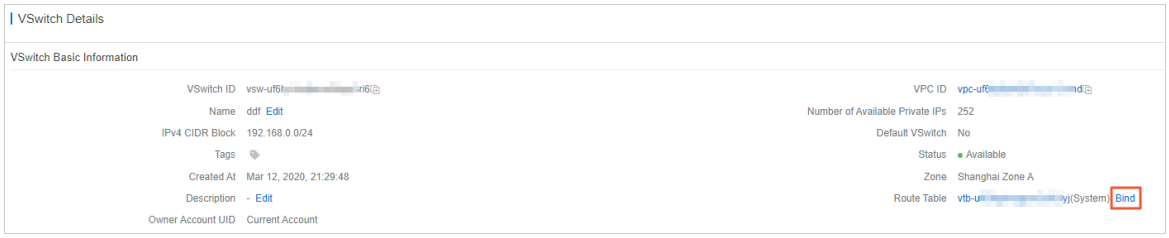
A custom route table is created. For more information, see Create a custom route table.

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.



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. After a VSwitch is deleted, cloud resources can no longer be deployed in the VSwitch.

Prerequisites

Before you can delete a VSwitch, the following conditions must be met:

- All cloud resources in the VSwitch, such as ECS, SLB, and RDS instances, are deleted.
- The resources associated with the VSwitch, such as SNAT entries and HAVIP, are deleted.

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 then click **Delete** in the **Actions** column.
6. In the **Delete VSwitch** dialog box, click **OK**.