ALIBABA CLOUD

Alibaba Cloud

Virtual Private Cloud

Route tables

Document Version: 20201014

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

After you create a virtual private cloud (VPC), the system creates a system route table for the VPC and adds system routes to the route table. You can use the route table to manage network traffic transmitted over the VPC. You cannot create or delete system route entries. However, you can create custom route entries to route traffic from specific CIDR blocks to the specified destination.

Route tables

After you create a VPC, the system creates a system route table to manage routes of the VPC. By default, VSwitches in the VPC use this route table. You cannot create or delete the system route table of a VPC. However, you can disassociate a VSwitch from the system route table and then associate it with a custom route table to manage your network in a more flexible way. For more information, see Create a custom route table.

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

When you manage route tables, note that:

- Each VPC supports at most 10 route tables, including the system route table.
- Each VSwitch can be associated with only one route table. The routing policies of a VSwitch are managed by the route table that is associated with the VSwitch.
- After you create a VSwitch, it is associated with the system route table by default.
- If the VSwitch is associated with a custom route table and you want to associate the VSwitch with the system route table, you must disassociate the custom route table from the VSwitch first. Before you can associate the VSwitch with another route table, you must disassociate the current route table from the VSwitch.
- All regions support custom route tables, except the China (Beijing), China (Shenzhen), and China (Hangzhou) regions.
- Custom route tables do not support active or standby routes, or load-balancing routes.

System routes

After you create a VPC, the system automatically adds the following system routes to the route table:

- A route entry with a destination CIDR block of 100.64.0.0/10. This route is used for communication among cloud resources within the VPC.
- Route entries whose destination CIDR blocks are the same as the CIDR blocks of the VSwitches in the VPC. These routes are used for communication among cloud resources within VSwitches.

For example, if you create a VPC whose CIDR block is 192.168.0.0/16 and two VSwitches whose CIDR blocks are 192.168.1.0/24 and 192.168.0.0/24, three system routes are automatically added to the route table of the VPC. The following table describes the system routes.

Destination CIDR block	Next hop	Route entry type
100.64.0.0/10	-	System route
192.168.1.0/24	-	System route

Destination CIDR block	Next hop	Route entry type
192.168.0.0/24	-	System route

Custom routes

You can add custom routes to replace system routes or route traffic to a specific destination. You can specify the following next hop types when you create a custom route:

- ECS instance: Traffic destined for the destination CIDR block is routed to a specified Elastic Compute Service (ECS) instance in the VPC.

  You can select this type if you want to access the Internet or other applications through the applications deployed on the ECS instance.
- VPN gateway: Traffic destined for the destination CIDR block is routed to a specified VPN gateway.

  You can select this type if you want to connect a VPC to another VPC or an on-premises network through the VPN gateway.
- NAT gateway: Traffic destined for the destination CIDR block is routed to a specified NAT gateway.

  You can select this type if you want to connect a VPC to the Internet through the NAT gateway.
- VPC-facing router interface: Traffic destined for the destination CIDR block is routed to a specified VPC.

  You can select this type if you want to connect two VPCs through Express Connect.
- VBR-facing router interface: Traffic destined for the destination CIDR block is routed to a specified virtual border router (VBR).

  You can select this type if you want to connect a VPC to an on-premises network through Express Connect.
- Secondary ENI: Traffic destined for the destination CIDR block is routed to a specified secondary elastic network interface (ENI).
- IPv6 gateway: Traffic destined for the destination CIDR block is routed to a specified IPv6 gateway.

  You can select this type if you want to implement IPv6 communication through an IPv6 gateway.

IPv6 routes

If IPv6 is enabled for your VPC, the following route entries are automatically added to the system route table of the VPC:

- A custom route entry whose destination CIDR block is ::/0 and whose next hop is the IPv6 gateway. Cloud resources deployed in the VPC network use this route to access the Internet through IPv6 addresses.
- A system route entry whose destination CIDR block is the IPv6 CIDR block of a VSwitch. This route is used for communication within the VSwitch.

> **Note** If you create a custom route table and associate the custom route table with a VSwitch whose IPv6 CIDR block is enabled, you must add a custom route entry whose destination CIDR block is ::/0 and the next hop is the IPv6 gateway instance. For more information, see Add a custom route entry.

Routing rules

If multiple route entries match the destination CIDR block, the route entry with the largest suffix prevails and determines the next hop. This ensures that the traffic is routed to the most precise destination.

For example, the following table describes the route table of a VPC.

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` are system route entries. The route entries destined for `0.0.0.0/0` and `10.0.0.0/24` are custom route entries. Traffic destined for `0.0.0.0/0` is routed to the ECS instance `i-12345678`, and traffic destined for `10.0.0.0/24` is routed to the ECS instance `i-87654321`. Based on the preceding rule, traffic destined for `10.0.0.1` is routed to the ECS instance `i-87654321`, and traffic destined for `10.0.1.1` is routed to the ECS instance `i-12345678`.

Limits

Routing examples

You can add custom route entries to a route table to control inbound and outbound traffic transmitted over the VPC.

- Routes within a VPC

  A NAT gateway is deployed on an ECS instance (ECS 01) in a VPC, as shown in the following figure. To enable the cloud resources in the VPC to access the Internet through the ECS instance, you must add the following route entry to the route table:

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

- Connect two VPCs through Express Connect

  VPC 1 (172.16.0.0/12) is connected to VPC 2 (192.168.0.0/16) through Express Connect as shown in the following figure. After you create router interfaces, you must add the following route entry in both VPCs:

  - VPC 1

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	VPC-facing router interface	VPC2

  - VPC 2

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	VPC-facing router interface	VPC1

- Connect two VPCs through a VPN gateway

  VPC 1 (172.16.0.0/12) is connected to VPC 2 (10.0.0.0/8) through a VPN gateway as shown in the following figure. After you configure the VPN gateway, you must add the following route entry in both VPCs.

  - VPC 1

Destination CIDR block	Next hop type	Next hop
10.0.0.0/8	VPN gateways	VPN gateway 1

  - VPC 2

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	VPN gateways	VPN gateway 2

- Connect a VPC to an on-premises data center through Express Connect

  A VPC network is connected to an on-premises network through Express Connect as shown in the following figure. After you configure the leased line and VBR, you must add the following route entries:

  - VPC

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Router interfaces (general routing)	Router interface RI 1

- VBR

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	Leased lines	Router interface RI 3
172.16.0.0/12	VPCs	Router interface RI 2

- On-premises network

Destination CIDR block	Next hop type	Next hop
172.16.0.0/12	—	On-premises gateway device

- **Connect a VPC to an on-premises data center through a VPN gateway**

  A VPC (172.16.0.0/12) is connected to an on-premises data center (192.168.0.0/16) as shown in the following figure. After you configure the VPN gateway, you must add the following route entry to the VPC:

Destination CIDR block	Next hop type	Next hop
192.168.0.0/16	VPN gateways	The VPN gateway that you created

2.System route table management

2.1. Add a custom route entry

This topic describes how to add a custom route entry. After you create a Virtual Private Cloud (VPC) network, the system creates a default route table and adds system route entries to the route table for traffic management. You cannot create or delete system route entries. However, you can create custom route entries to route traffic from source CIDR blocks to specific destinations.

Context

Each entry in the route table is a route entry. A route entry, which specifies the destination for network traffic, consists of the destination CIDR block, next hop type, and next hop. Route entries are classified into system route entries and custom route entries. You can add custom route entries to both system and custom route tables.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**.
3. In the top navigation bar, select the region to which the route tables belong.
4. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
5. In the **Route Table Details** section, click the **Route Entry List** tab, and then click **Add Route Entry**.
6. On the **Add Route Entry** page, set the following parameters and click **OK**.

Parameter	Description
Name	The name of the route entry. The name must be 2 to 128 characters and can contain digits, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
Destination CIDR Block	The destination CIDR block to which you want to route traffic.

Parameter	Description
Next Hop Type	The type of the next hop. Valid values: ○ **ECS Instance**: Traffic destined for the specified CIDR block is routed to the Elastic Compute Service (ECS) instance you select. Select this type if you want to route traffic to an ECS instance for centralized traffic forwarding and management. For example, when an ECS instance is configured as the Internet-facing gateway to manage the traffic from other ECS instances to the Internet. ○ **VPN Gateway**: Traffic destined for the specified CIDR block is routed to the VPN gateway you select. ○ **NAT Gateway**: Traffic destined for the specified CIDR block is routed to the NAT gateway you select. ○ **Secondary ENI**: Traffic destined for the specified CIDR block is routed to the secondary elastic network interface (ENI) you select.
Resource Group	Select the resource group of the next hop. This option appears only when you set **Next Hop Type** to **ECS Instance** or **Secondary ENI**.
ECS Instance/VPN Gateway/NAT Gateway/Secondary ENI	Select the next-hop instance.

Related information

- CreateRouteEntry

2.2. Export route entries

This topic describes how to export route entries from a route table for backup.

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
6. In the **Route Table Details** area, click the **Route Entry List** tab, and then click **Export**. The route entries are exported as a *.csv* file. After you export the route entries, you can view them in your local computer.

2.3. Modify the basic information of a route table

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

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
6. In the **Route Table Details** area, click **Edit** after the **Name** field to modify the name of the route table. 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 route table. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://` .

2.4. Delete a custom route entry

This topic describes how to delete a custom route entry. You can delete custom route entries, but you cannot delete system route entries.

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
6. On the **Route Entry List** tab page, find the target route entry, and then click **Delete** in the **Actions** column.
7. In the **Delete Route Entry** dialog box, click **OK**.

3.Custom route table management

3.1. Create a custom route table

This topic describes how to create a custom route table. A route table consists of one or more route entries. Each route entry specifies the destination network to which traffic is routed. You can create a custom route table to manage the inbound and outbound network traffic of subnets in a Virtual Private Cloud (VPC) network.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**.
3. Select the region where you want to create a route table.

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

4. On the **Route Tables** page, click **Create Route Table**.
5. In the **Create Route Table** dialog box that appears, set the following parameters and click **OK**.

Parameter	Description
Resource Group	Select the resource group to which the route table belongs.
VPC	Select the VPC network to which the route table belongs. If a VPC network contains an Elastic Compute Service (ECS) instance that belongs to one of the following instance families, you cannot create a custom route table for the VPC network. ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4. To create a custom route table, you must upgrade or release ECS instances that do not support VPC advanced features. ○ For more information about how to upgrade an ECS instance, see Upgrade configurations of subscription instances and Change the instance type of a pay-as-you-go instance. ○ For more information about how to release an ECS instance, see Release an instance. **Note** If your VPC network contains ECS instances of the preceding instance families and uses a custom route table, you must upgrade or release the instance. Otherwise, the custom route table cannot work as expected. For more information, see Overview of VPC advanced features.

Parameter	Description
Name	Enter a name for the route table that you want to create. 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 Chinese character.
Description	Enter a description for the route table that you want to create. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.

After you create a custom route table, you can go to the **Route Tables** page to check the custom route table. The type of the route table is displayed as **Custom** in the **Route Table Type** column.

The following system route entries are automatically added to the custom route table:

- A route destined for the CIDR block 100.64.0.0/10. This route is used for communication among cloud resources over the VPC network.
- A route destined for the CIDR block of a VSwitch of the VPC network to which the route table belongs. This route is used for communication among resources attached to the VSwitch.

For example, you have created two VSwitches whose CIDR blocks are 192.168.1.0/24 and 192.168.0.0/24. These VSwitches are deployed in the VPC network whose CIDR block is 192.168.0.0/16. The custom route table that you have created for your VPC network includes the following route entries:

Destination CIDR block	Next hop	Type
100.64.0.0/10	-	System routes
192.168.1.0/24	-	System routes
192.168.0.0/24	-	System routes

3.2. Add a custom route entry

This topic describes how to add a custom route entry. After you create a Virtual Private Cloud (VPC) network, the system creates a default route table and adds system route entries to the route table for traffic management. You cannot create or delete system route entries. However, you can create custom route entries to route traffic from source CIDR blocks to specific destinations.

Context

Each entry in the route table is a route entry. A route entry, which specifies the destination for network traffic, consists of the destination CIDR block, next hop type, and next hop. Route entries are classified into system route entries and custom route entries. You can add custom

route entries to both system and custom route tables.

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**.
3. In the top navigation bar, select the region to which the route tables belong.
4. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
5. In the **Route Table Details** section, click the **Route Entry List** tab, and then click **Add Route Entry**.
6. On the **Add Route Entry** page, set the following parameters and click **OK**.

Parameter	Description
Name	The name of the route entry. The name must be 2 to 128 characters and can contain digits, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
Destination CIDR Block	The destination CIDR block to which you want to route traffic.
Next Hop Type	The type of the next hop. Valid values: ○ **ECS Instance**: Traffic destined for the specified CIDR block is routed to the Elastic Compute Service (ECS) instance you select. Select this type if you want to route traffic to an ECS instance for centralized traffic forwarding and management. For example, when an ECS instance is configured as the Internet-facing gateway to manage the traffic from other ECS instances to the Internet. ○ **VPN Gateway**: Traffic destined for the specified CIDR block is routed to the VPN gateway you select. ○ **NAT Gateway**: Traffic destined for the specified CIDR block is routed to the NAT gateway you select. ○ **Secondary ENI**: Traffic destined for the specified CIDR block is routed to the secondary elastic network interface (ENI) you select.
Resource Group	Select the resource group of the next hop. This option appears only when you set **Next Hop Type** to **ECS Instance** or **Secondary ENI**.
ECS Instance/VPN Gateway/NAT Gateway/Secondary ENI	Select the next-hop instance.

Related information

- CreateRouteEntry

3.3. Export route entries

This topic describes how to export route entries from a route table for backup.

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
6. In the **Route Table Details** area, click the **Route Entry List** tab, and then click **Export**. The route entries are exported as a *.csv* file. After you export the route entries, you can view them in your local computer.

3.4. Delete a custom route entry

This topic describes how to delete a custom route entry. You can delete custom route entries, but you cannot delete system route entries.

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
6. On the **Route Entry List** tab page, find the target route entry, and then click **Delete** in the **Actions** column.
7. In the **Delete Route Entry** dialog box, click **OK**.

3.5. Associate a route table with a VSwitch

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

Prerequisites

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

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

Procedure

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**.
3. In the top navigation bar, select the region to which the route tables belong.
4. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
5. On the **Route Table** page, click the **Associated VSwitch** tab and then click **Associate VSwitch**.
6. In the **Associate VSwitch** pane, select the target VSwitch and click **OK**.

3.6. 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 from a VSwitch, the VSwitch is automatically associated with the system route table.

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
6. In the **Route Table Details** area, click the **Associated VSwitches** tab, find the target VSwitch, and then click **Unbind** in the **Actions** column.
7. In the **Unbind Route Table** dialog box, click **OK**.

3.7. Modify the basic information of a route table

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

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
6. In the **Route Table Details** area, click **Edit** after the **Name** field to modify the name of the route table. 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 route table. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.

3.8. Delete a custom route table

This topic describes how to delete a custom route table.

Prerequisites

The custom route table to be deleted is not associated with a VSwitch. Otherwise, you must disassociate it from the VSwitch first. For more information, see Disassociate a custom route table from a VSwitch.

Procedure

1.
2.
3. In the left-side navigation pane, click **Route Tables**.
4. In the top navigation bar, select the region to which the route tables belong.
5. On the **Route Tables** page, find the target route table, and then click **Delete** in the **Actions** column.
6. In the **Delete Route Table** dialog box, click **OK**.

4.Add a subnet route to a custom route table

This topic describes how to add a subnet route to a custom route table. After you add a subnet route to a custom route table, you can associate the custom route table with a VSwitch to control the flow of traffic to and from the VSwitch.

Prerequisites

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

Limits

Before you add a subnet route to a route table, note the following limits:

- You can only create up to 10 route tables in each 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.
- Custom route tables are supported in all regions except China (Beijing), China (Shenzhen), and China (Hangzhou).

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. Select the region where you want to create a route table.

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

4. On the **Route Tables** page, click **Create Route Table**.
5. In the **Create Route Table** dialog box that appears, set the following parameters and click **OK**.

Parameter	Description
Resource Group	Select the resource group to which the route table belongs.

Parameter	Description
VPC	Select the VPC network to which the route table belongs. If a VPC network contains an Elastic Compute Service (ECS) instance that belongs to one of the following instance families, you cannot create a custom route table for the VPC network. ecs.c1, ecs.c2, ecs.c4, ecs.ce4, ecs.cm4, ecs.d1, ecs.e3, ecs.e4, ecs.ga1, ecs.gn4, ecs.gn5, ecs.i1, ecs.m1, ecs.m2, ecs.mn4, ecs.n1, ecs.n2, ecs.n4, ecs.s1, ecs.s2, ecs.s3, ecs.se1, ecs.sn1, ecs.sn2, ecs.t1, and ecs.xn4. To create a custom route table, you must upgrade or release ECS instances that do not support VPC advanced features. ○ For more information about how to upgrade an ECS instance, see Upgrade configurations of subscription instances and Change the instance type of a pay-as-you-go instance. ○ For more information about how to release an ECS instance, see Release an instance. Note If your VPC network contains ECS instances of the preceding instance families and uses a custom route table, you must upgrade or release the instance. Otherwise, the custom route table cannot work as expected. For more information, see Overview of VPC advanced features.
Name	Enter a name for the route table that you want to create. 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 Chinese character.
Description	Enter a description for the route table that you want to create. The description must be 2 to 256 characters in length and cannot start with `http://` or `https://`.

After you create a custom route table, you can go to the **Route Tables** page to check the custom route table. The type of the route table is displayed as **Custom** in the **Route Table Type** column.

The following system route entries are automatically added to the custom route table:

- A route destined for the CIDR block 100.64.0.0/10. This route is used for communication among cloud resources over the VPC network.
- A route destined for the CIDR block of a VSwitch of the VPC network to which the route table belongs. This route is used for communication among resources attached to the VSwitch.

For example, you have created two VSwitches whose CIDR blocks are 192.168.1.0/24 and 192.168.0.0/24. These VSwitches are deployed in the VPC network whose CIDR block is 192.168.0.0/16. The custom route table that you have created for your VPC network includes the following route entries:

Destination CIDR block	Next hop	Type
100.64.0.0/10	-	System routes
192.168.1.0/24	-	System routes
192.168.0.0/24	-	System routes

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

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

1. Log on to the VPC console.
2. In the left-side navigation pane, click **Route Tables**.
3. In the top navigation bar, select the region to which the route tables belong.
4. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
5. In the **Route Table Details** section, click the **Route Entry List** tab, and then click **Add Route Entry**.
6. On the **Add Route Entry** page, set the following parameters and click **OK**.

Parameter	Description
Name	The name of the route entry. The name must be 2 to 128 characters and can contain digits, underscores (_), and hyphens (-). The name must start with a letter or a Chinese character.
Destination CIDR Block	The destination CIDR block to which you want to route traffic.
Next Hop Type	The type of the next hop. Valid values: ○ **ECS Instance**: Traffic destined for the specified CIDR block is routed to the Elastic Compute Service (ECS) instance you select. Select this type if you want to route traffic to an ECS instance for centralized traffic forwarding and management. For example, when an ECS instance is configured as the Internet-facing gateway to manage the traffic from other ECS instances to the Internet. ○ **VPN Gateway**: Traffic destined for the specified CIDR block is routed to the VPN gateway you select. ○ **NAT Gateway**: Traffic destined for the specified CIDR block is routed to the NAT gateway you select. ○ **Secondary ENI**: Traffic destined for the specified CIDR block is routed to the secondary elastic network interface (ENI) you select.

Parameter	Description
Resource Group	Select the resource group of the next hop. This option appears only when you set **Next Hop Type** to **ECS Instance** or **Secondary ENI**.
ECS Instance/VPN Gateway/NAT Gateway/Secondary ENI	Select the next-hop instance.

Step 3: Associate the route table with a VSwitch

You can associate the route table with a VSwitch (subnet) to control the flow of traffic to and from the VSwitch. Each VSwitch can be associated with only one custom route table or system route table. To associate the 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. In the top navigation bar, select the region to which the route tables belong.
4. On the **Route Tables** page, find the route table and click **Manage** in the **Actions** column.
5. On the **Route Table** page, click the **Associated VSwitch** tab and then click **Associate VSwitch**.
6. In the **Associate VSwitch** pane, select the target VSwitch and click **OK**.