

Virtual Private Cloud

User Guide

Issue 1
Date 2023-12-22



Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

Contents

1 VPC and Subnet	1
1.1 VPC and Subnet Planning Suggestions	1
1.2 VPC	5
1.2.1 Creating a VPC	5
1.2.2 Adding a Secondary IPv4 CIDR Block to a VPC	12
1.2.3 Modifying a VPC	14
1.2.4 Managing VPC Tags	15
1.2.5 Obtaining a VPC ID	17
1.2.6 Viewing a VPC Topology	18
1.2.7 Exporting VPC List	18
1.2.8 Deleting a Secondary IPv4 CIDR Block from a VPC	19
1.2.9 Deleting a VPC	19
1.3 Subnet	20
1.3.1 Creating a Subnet for the VPC	20
1.3.2 Modifying a Subnet	25
1.3.3 Managing Subnet Tags	27
1.3.4 Viewing and Deleting Resources in a Subnet	29
1.3.5 Viewing IP Addresses in a Subnet	32
1.3.6 Exporting Subnet List	33
1.3.7 Deleting a Subnet	33
1.4 IPv4 and IPv6 Dual-Stack Network	34
2 Route Tables	40
2.1 Route Tables and Routes	40
2.2 Managing Route Tables	44
2.2.1 Creating a Custom Route Table	44
2.2.2 Associating a Route Table with a Subnet	45
2.2.3 Changing the Route Table Associated with a Subnet	46
2.2.4 Viewing the Route Table Associated with a Subnet	47
2.2.5 Viewing Route Table Information	47
2.2.6 Exporting Route Table Information	48
2.2.7 Deleting a Route Table	48
2.3 Managing Routes	49
2.3.1 Adding a Custom Route	49

2.3.2 Modifying a Route.....	50
2.3.3 Replicating a Route.....	52
2.3.4 Deleting a Route.....	53
2.4 Configuring an SNAT Server.....	54
3 Virtual IP Address.....	57
3.1 Virtual IP Address Overview.....	57
3.2 Assigning a Virtual IP Address.....	59
3.3 Binding a Virtual IP Address to an EIP or ECS.....	60
3.4 Binding a Virtual IP Address to an EIP.....	67
3.5 Unbinding a Virtual IP Address from an Instance.....	67
3.6 Unbinding a Virtual IP Address from an EIP.....	68
3.7 Releasing a Virtual IP Address.....	68
3.8 Disabling IP Forwarding on the Standby ECS.....	70
3.9 Disabling Source/Destination Check for an ECS NIC.....	71
4 Elastic Network Interface and Supplementary Network Interface.....	72
4.1 Elastic Network Interface.....	72
4.1.1 Elastic Network Interface Overview.....	72
4.1.2 Creating a Network Interface.....	73
4.1.3 Viewing Basic Information About a Network Interface.....	74
4.1.4 Attaching a Network Interface to an Instance.....	74
4.1.5 Binding a Network Interface to an EIP.....	75
4.1.6 Binding a Network Interface to a Virtual IP Address.....	75
4.1.7 Detaching a Network Interface from an Instance or Unbinding an EIP from a Network Interface....	76
4.1.8 Changing Security Groups That Are Associated with a Network Interface.....	77
4.1.9 Deleting a Network Interface.....	78
4.2 Supplementary Network Interfaces.....	78
4.2.1 Supplementary Network Interface Overview.....	79
4.2.2 Creating a Supplementary Network Interface.....	80
4.2.3 Viewing Basic Information About a Supplementary Network Interface.....	83
4.2.4 Binding or Unbinding a Supplementary Network Interface to or from an EIP.....	84
4.2.5 Changing Security Groups That Are Associated with a Supplementary Network Interface.....	85
4.2.6 Deleting a Supplementary Network Interface.....	86
5 Access Control.....	87
5.1 What Is Access Control?.....	87
5.2 Security Group.....	89
5.2.1 Security Groups and Security Group Rules.....	89
5.2.2 Default Security Group and Rules.....	98
5.2.3 Security Group Configuration Examples.....	100
5.2.4 Common Ports Used by ECSs.....	105
5.2.5 Managing a Security Group.....	107
5.2.5.1 Creating a Security Group.....	108

5.2.5.2 Cloning a Security Group.....	109
5.2.5.3 Modifying a Security Group.....	110
5.2.5.4 Deleting a Security Group.....	111
5.2.6 Managing Security Group Rules.....	112
5.2.6.1 Adding a Security Group Rule.....	112
5.2.6.2 Fast-Adding Security Group Rules.....	118
5.2.6.3 Allowing Common Ports with A Few Clicks.....	122
5.2.6.4 Modifying a Security Group Rule.....	123
5.2.6.5 Replicating a Security Group Rule.....	124
5.2.6.6 Importing and Exporting Security Group Rules.....	125
5.2.6.7 Deleting a Security Group Rule.....	128
5.2.7 Managing Instances Associated with a Security Group.....	129
5.2.7.1 Adding an Instance to or Removing an Instance from a Security Group.....	129
5.2.7.2 Changing the Security Group of an ECS.....	130
5.3 Network ACL.....	131
5.3.1 Network ACL Overview.....	131
5.3.2 Network ACL Configuration Examples.....	135
5.3.3 Managing Network ACLs.....	138
5.3.3.1 Creating a Network ACL.....	138
5.3.3.2 Modifying a Network ACL.....	139
5.3.3.3 Enabling or Disabling a Network ACL.....	139
5.3.3.4 Viewing a Network ACL.....	140
5.3.3.5 Deleting a Network ACL.....	141
5.3.4 Management Network ACL Rules.....	141
5.3.4.1 Adding a Network ACL Rule (Default Effective Sequence).....	141
5.3.4.2 Adding a Network ACL Rule (Custom Effective Sequence).....	144
5.3.4.3 Modifying a Network ACL Rule.....	144
5.3.4.4 Enabling or Disabling a Network ACL Rule.....	146
5.3.4.5 Exporting and Importing Network ACL Rules.....	147
5.3.4.6 Deleting a Network ACL Rule.....	148
5.3.5 Managing Subnets Associated with a Network ACL.....	148
5.3.5.1 Associating Subnets with a Network ACL.....	148
5.3.5.2 Disassociating Subnets from a Network ACL.....	149
6 IP Address Group.....	151
6.1 IP Address Group Overview.....	151
6.2 Managing an IP Address Group.....	151
6.2.1 Creating an IP Address Group.....	152
6.2.2 Associating an IP Address Group with Resources.....	153
6.2.3 Modifying an IP Address Group.....	154
6.3 Managing IP Addresses in an IP Address Group.....	155
6.3.1 Adding IP Addresses to an IP Address Group.....	155
6.3.2 Modifying IP Addresses in an IP Address Group.....	156

6.3.3 Deleting IP Addresses from an IP Address Group.....	157
7 VPC Peering Connection.....	159
7.1 VPC Peering Connection Overview.....	159
7.2 VPC Peering Connection Usage Examples.....	161
7.3 Creating a VPC Peering Connection with Another VPC in Your Account.....	171
7.4 Creating a VPC Peering Connection with a VPC in Another Account.....	176
7.5 Obtaining the Peer Project ID of a VPC Peering Connection.....	183
7.6 Modifying a VPC Peering Connection.....	184
7.7 Viewing VPC Peering Connections.....	184
7.8 Deleting a VPC Peering Connection.....	185
7.9 Modifying Routes Configured for a VPC Peering Connection.....	186
7.10 Viewing Routes Configured for a VPC Peering Connection.....	187
7.11 Deleting Routes Configured for a VPC Peering Connection.....	189
8 VPC Flow Log.....	191
8.1 VPC Flow Log Overview.....	191
8.2 Creating a VPC Flow Log.....	192
8.3 Viewing a VPC Flow Log.....	194
8.4 Enabling or Disabling VPC Flow Log.....	197
8.5 Deleting a VPC Flow Log.....	197
9 Elastic IP.....	199
9.1 EIP Overview.....	199
9.2 Assigning an EIP and Binding It to an ECS.....	200
9.3 Unbinding an EIP from an ECS and Releasing the EIP.....	205
9.4 Modifying an EIP Bandwidth.....	206
9.5 Exporting EIP Information.....	207
9.6 Managing EIP Tags.....	207
9.7 IPv6 EIP	209
10 Shared Bandwidth.....	215
10.1 Shared Bandwidth Overview.....	215
10.2 Assigning a Shared Bandwidth.....	216
10.3 Adding EIPs to a Shared Bandwidth.....	218
10.4 Removing EIPs from a Shared Bandwidth.....	218
10.5 Modifying a Shared Bandwidth.....	219
10.6 Deleting a Shared Bandwidth.....	220
11 Interconnecting with CTS.....	222
11.1 Supported VPC Operations.....	222
11.2 Viewing Traces.....	225
12 Monitoring.....	227
12.1 Supported Metrics.....	227
12.2 Viewing Metrics.....	229

12.3 Creating an Alarm Rule.....	230
13 Permissions Management.....	231
13.1 Creating a User and Granting VPC Permissions.....	231
13.2 VPC Custom Policies.....	232
A Change History.....	235

1 VPC and Subnet

1.1 VPC and Subnet Planning Suggestions

Before creating your VPCs, determine how many VPCs, the number of subnets, and what IP address ranges or connectivity options you will need.

- [How Do I Determine How Many VPCs I Need?](#)
- [How Do I Plan Subnets?](#)
- [How Do I Plan Routing Policies?](#)
- [How Do I Connect to an On-Premises Data Center?](#)
- [How Do I Access the Internet?](#)

How Do I Determine How Many VPCs I Need?

VPCs are region-specific. By default, networks in VPCs in different regions or even in the same region are not connected.

- One VPC
If your services do not require network isolation, a single VPC should be enough.
- Multiple VPCs

If you have multiple service systems in a region and each service system requires an isolated network, you can create a separate VPC for each service system.

NOTE

By default, you can create a maximum of five VPCs in each region. If this cannot meet your service requirements, request a quota increase. For details, see [How Do I Apply for a Higher Quota?](#)

The following table lists the private CIDR blocks that you can specify when creating a VPC. Consider the following when selecting a VPC CIDR block:

- Number of IP addresses: Reserve sufficient IP addresses in case of business growth.
- IP address range: Avoid IP address conflicts if you need to connect a VPC to an on-premises data center or connect two VPCs.

Table 1-1 lists the supported VPC CIDR blocks.

Table 1-1 VPC CIDR blocks

VPC CIDR Block	IP Address Range	Maximum Number of IP Addresses
10.0.0.0/8-24	10.0.0.0-10.255.255.255	$2^{24}-2=16777214$
172.16.0.0/12-24	172.16.0.0-172.31.255.255	$2^{20}-2=1048574$
192.168.0.0/16-24	192.168.0.0-192.168.255.255	$2^{16}-2=65534$

NOTICE

Table 1-1 describes the primary IPv4 CIDR blocks available for a VPC. After a VPC is created, its primary CIDR block cannot be modified. If the primary CIDR block is insufficient, you can [add a secondary IPv4 CIDR block for the VPC](#).

How Do I Plan Subnets?

A subnet is a unique CIDR block with a range of IP addresses in a VPC. All resources in a VPC must be deployed on subnets.

- By default, all instances in different subnets of the same VPC can communicate with each other and the subnets can be located in different AZs. If you have a VPC with two subnets in it and they are located in different AZs, they can communicate with each other by default.
- After a subnet is created, its CIDR block cannot be modified. Subnets in the same VPC cannot overlap.

When you create a VPC, a default subnet will be created together. If you need more subnets, see [Creating a Subnet for the VPC](#).

A subnet mask can be between the netmask of its VPC CIDR block and /28 netmask. If a VPC CIDR block is 10.0.0.0/16, its subnet mask can be between 16 and 28.

For example, if the CIDR block of VPC-A is 10.0.0.0/16, you can specify 10.0.0.0/24 for subnet A01, 10.0.1.0/24 for subnet A02, and 10.0.2.0/24 for subnet A03.

NOTE

By default, you can create a maximum of 100 subnets in each region. If this cannot meet your service requirements, request a quota increase by referring to [How Do I Apply for a Higher Quota?](#)

When planning subnets, consider the following:

- You create different subnets for different modules in a VPC. For example, in VPC-A, you can create subnet A01 for web services, subnet A02 for

management services, and subnet A03 for data services. You can leverage network ACLs to control access to each subnet.

- If your VPC needs to communicate with an on-premises data center through VPN or Direct Connect, ensure that the VPC subnet and the CIDR block used for communication in the data center do not overlap.

How Do I Plan Routing Policies?

When you create a VPC, the system automatically generates a default route table for the VPC. If you create a subnet in the VPC, the subnet automatically associates with the default route table. A route table contains a set of routes that are used to determine where network traffic from your subnets in a VPC is directed. The default route table ensures that subnets in a VPC can communicate with each other.

If you do not want to use the default route table, you can now create a custom route table and associate it with the subnets. The custom route table associated with a subnet affects only the outbound traffic. The default route table controls the inbound traffic.

You can add routes to default and custom route tables and configure the destination, next hop type, and next hop in the routes to determine where network traffic is directed. Routes are classified into system routes and custom routes.

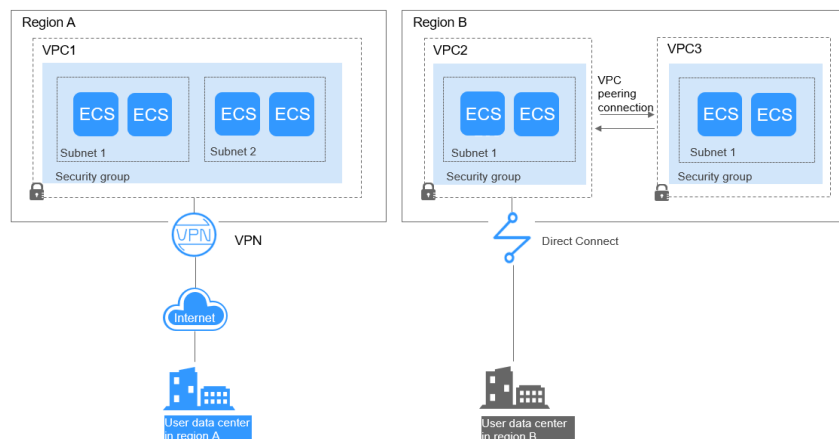
- System routes: Routes that are automatically added by the system and cannot be modified or deleted. System routes allow instances in a VPC to communicate with each other.
- Custom routes: Routes that can be modified and deleted. The destination of a custom route cannot overlap with that of a system route.

You cannot add two routes with the same destination to a VPC route table even if their next hop types are different, because the destination determines the route priority. According to the longest match routing rule, the destination with a higher matching degree is preferentially selected for packet forwarding.

How Do I Connect to an On-Premises Data Center?

If you require interconnection between a VPC and an on-premises data center, ensure that the VPC does not have an overlapping IP address range with the on-premises data center to be connected.

As shown in [Figure 1-1](#), you have VPC 1 in region A and VPC 2 and VPC 3 in region B. To connect to an on-premises data center, they can use a VPN, as VPC 1 does in Region A; or a Direct Connect connection, as VPC 2 does in Region B. VPC 2 connects to the data center through a Direct Connect connection, but to connect to another VPC in that region, like VPC 3, a VPC peering connection must be established.

Figure 1-1 Connections to on-premises data centers

When planning CIDR blocks for VPC 1, VPC 2, and VPC 3:

- The CIDR block of VPC 1 cannot overlap with the CIDR block of the on-premises data center in Region A.
- The CIDR block of VPC 2 cannot overlap with the CIDR block of the on-premises data center in Region B.
- The CIDR blocks of VPC 2 and VPC 3 cannot overlap.

How Do I Access the Internet?

Use EIPs to enable a small number of ECSs to access the Internet.

When only a few ECSs need to access the Internet, you can bind the EIPs to the ECSs. This will provide them with Internet access. You can also dynamically unbind the EIPs from the ECSs and bind them to NAT gateways and load balancers instead, which will also provide Internet access. The process is not complicated.

For more information about EIP, see [EIP Overview](#).

Use a NAT gateway to enable a large number of ECSs to access the Internet.

When a large number of ECSs need to access the Internet, the public cloud provides NAT gateways for your ECSs. With NAT gateways, you do not need to assign an EIP to each ECS. NAT gateways reduce costs as you do not need so many EIPs. NAT gateways offer both source network address translation (SNAT) and destination network address translation (DNAT). SNAT allows multiple ECSs in the same VPC to share one or more EIPs to access the Internet. SNAT prevents the EIPs of ECSs from being exposed to the Internet. DNAT can implement port-level data forwarding. It maps EIP ports to ECS ports so that the ECSs in a VPC can share the same EIP and bandwidth to provide Internet-accessible services.

For more information, see [NAT Gateway User Guide](#).

Use ELB to access the Internet if there are a large number of concurrent requests.

In high-concurrency scenarios, such as e-commerce, you can use load balancers provided by the ELB service to evenly distribute incoming traffic across multiple ECSs, allowing a large number of users to concurrently access your business system or application. ELB is deployed in the cluster mode. It provides fault

tolerance for your applications by automatically balancing traffic across multiple AZs. You can also take advantage of deep integration with Auto Scaling (AS), which enables automatic scaling based on service traffic and ensures service stability and reliability.

For more information, see [Elastic Load Balance User Guide](#).

Helpful Links

- [Application Scenarios](#)

1.2 VPC

1.2.1 Creating a VPC

Scenarios

A VPC provides an isolated virtual network for ECSs. You can configure and manage the network as required.

You can create a VPC by following the procedure provided in this section. Then, create subnets, security groups, and assign EIPs by following the procedure provided in subsequent sections based on your actual network requirements.

Procedure

1. Go to the [Create VPC](#) page.
2. On the **Create VPC** page, set parameters as prompted.
A default subnet will be created together with a VPC and you can also click **Add Subnet** to create more subnets for the VPC.

Figure 1-2 Creating a VPC and subnet

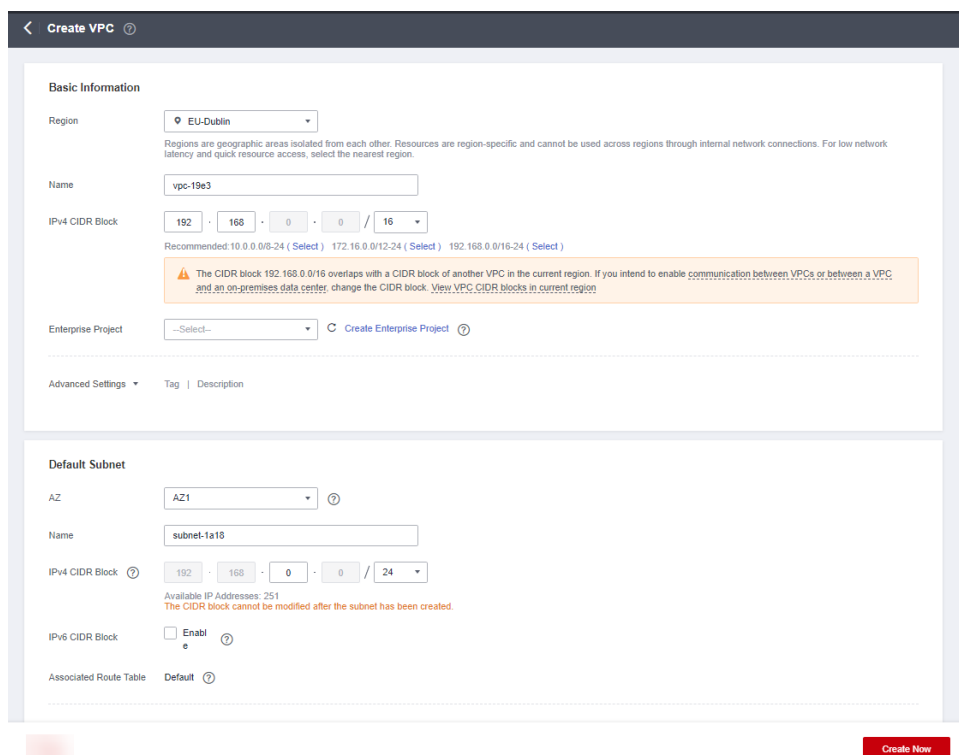


Table 1-2 VPC parameter descriptions

Parameter	Description	Example Value
Region	Select the region nearest to you to ensure the lowest latency possible.	EU-Dublin
Name	The VPC name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	VPC-test

Parameter	Description	Example Value
IPv4 CIDR Block	<p>The CIDR block of the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets in the VPC).</p> <p>The following CIDR blocks are supported:</p> <ul style="list-style-type: none">• 10.0.0.0/8-24• 172.16.0.0/12-24• 192.168.0.0/16-24 <p>This parameter will be CIDR Block in regions where IPv4/IPv6 dual stack is not supported, and IPv4 CIDR Block if IPv4/IPv6 dual stack is supported.</p>	192.168.0.0/16
Enterprise Project	<p>The enterprise project to which the VPC belongs.</p> <p>An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default.</p> <p>For details about creating and managing enterprise projects, see the Enterprise Management User Guide.</p>	default
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Retain the default settings.
Tag	<p>The VPC tag, which consists of a key and value pair.</p> <p>Each cloud resource can have a maximum of 20 tags.</p>	<ul style="list-style-type: none">• Key: vpc_key1• Value: vpc-01
Description	<p>Supplementary information about the VPC. This parameter is optional.</p> <p>The VPC description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	N/A

Table 1-3 Subnet parameter descriptions

Parameter	Description	Example Value
AZ	<p>An AZ is a geographic location with independent power supply and network facilities in a region. AZs are physically isolated, and AZs in the same VPC are interconnected through an internal network. For details, see Region and AZ.</p> <p>Note the following when you select an AZ:</p> <ul style="list-style-type: none">• A VPC can have subnets that are in different AZs. For example, a VPC can have subnet A in AZ 1, and subnet B in AZ 3.• A cloud resource and its subnet can be in different AZs. For example, a cloud server in AZ 1 can use a subnet in AZ 3. If AZ 3 becomes faulty, cloud servers in AZ 1 can still use the subnet in AZ 3, and your services are not interrupted.	AZ1
Name	<p>The subnet name.</p> <p>The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.</p>	subnet-01
IPv4 CIDR Block	<p>The CIDR block for the subnet. This value must be within the VPC CIDR block.</p> <p>This parameter is displayed only in regions where IPv4/IPv6 dual stack is supported.</p>	192.168.0.0/24

Parameter	Description	Example Value
IPv6 CIDR Block	<p>Specifies whether to set IPv6 CIDR Block to Enable.</p> <p>After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.</p> <p>This parameter is displayed only in regions where IPv4/IPv6 dual stack is supported.</p>	-
Associated Route Table	<p>The default route table to which the subnet will be associated. You can change the route table to a custom route table on the Subnets page.</p>	Default
Advanced Settings	<p>Click the drop-down arrow to set advanced settings for the subnet, including Gateway and DNS Server Address.</p>	Retain the default settings.
Gateway	<p>The gateway address of the subnet.</p> <p>This IP address is used to communicate with other subnets.</p>	192.168.0.1

Parameter	Description	Example Value
DNS Server Address	<p>Huawei Cloud private DNS server addresses are entered by default. This allows ECSs in a VPC to communicate with each other and also access other cloud services using private domain names without exposing their IP addresses to the Internet.</p> <p>You can change the default DNS server addresses if needed. This may interrupt your access to cloud services.</p> <p>You can also click Reset on the right to restore the DNS server addresses to the default value.</p> <p>A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x
DHCP Lease Time	<p>The period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client.</p> <ul style="list-style-type: none">• Limited: Set the DHCP lease time. The unit can be day or hour.• Unlimited: The DHCP lease time does not expire. <p>After you change the DHCP lease time on the console, the change is applied automatically when the DHCP lease of an instance (such as ECS) is renewed. You can wait for the system to renew the lease or manually renew the lease. Renewing lease will not change the IP address used by the instance. If you want the new lease time to take effect immediately, manually renew the lease or restart the ECS.</p>	-

Parameter	Description	Example Value
Tag	The subnet tag, which consists of a key and value pair. Each cloud resource can have a maximum of 20 tags.	<ul style="list-style-type: none"> • Key: subnet_key1 • Value: subnet-01
Description	Supplementary information about the subnet. This parameter is optional. The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

Table 1-4 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each VPC and can be the same for different VPCs. • Can contain a maximum of 36 characters. • Can contain only the following character types: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters, including hyphens (-) and underscores (_) 	vpc_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain only the following character types: <ul style="list-style-type: none"> - Uppercase letters - Lowercase letters - Digits - Special characters, including periods (.), hyphens (-) and underscores (_) 	vpc-01

Table 1-5 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each subnet.• Can contain a maximum of 36 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	subnet_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	subnet-01

3. Confirm the current configuration and click **Create Now**.

1.2.2 Adding a Secondary IPv4 CIDR Block to a VPC

Scenarios

When you create a VPC, you specify a primary IPv4 CIDR block for the VPC, which cannot be changed. To extend the IP address range of your VPC, you can add a secondary CIDR block to the VPC.

NOTE

If the [secondary IPv4 CIDR block](#) function is available in a region, the CIDR block of a VPC in this region cannot be modified through the console. You can call an API to modify VPC CIDR block. For details, see section "Updating VPC Information" in the *Virtual Private Cloud API Reference*.

Notes and Constraints

- You can allocate a subnet from either a primary or a secondary CIDR block of a VPC. A subnet cannot use both the primary and the secondary CIDR blocks. Subnets in the same VPC can communicate with each other by default, even if some subnets are allocated from the primary CIDR block and some are from the secondary CIDR block of a VPC.

- If a subnet in a secondary CIDR block of your VPC is the same as or overlaps with the destination of an existing route in the VPC route table, the existing route does not take effect.

If you create a subnet in a secondary CIDR block of your VPC, a route (the destination is the subnet CIDR block and the next hop is **Local**) is automatically added to your VPC route table. This route allows communications within the VPC and has a higher priority than any other routes in the VPC route table. For example, if a VPC route table has a route with the VPC peering connection as the next hop and 100.20.0.0/24 as the destination, and a route for the subnet in the secondary CIDR block has a destination of 100.20.0.0/16, 100.20.0.0/16 and 100.20.0.0/24 overlaps and traffic will be forwarded through the route of the subnet.

- The allowed secondary CIDR block size is between a /28 netmask and /3 netmask.
- [Table 1-6](#) lists the secondary CIDR blocks that are not supported.

Table 1-6 Restricted secondary CIDR blocks

Type	CIDR Block (Not Supported)
Primary CIDR blocks and existing CIDR blocks	<ul style="list-style-type: none">• 10.0.0.0/8• 172.16.0.0/12• 192.168.0.0/16
Reserved system CIDR blocks	<ul style="list-style-type: none">• 100.64.0.0/10• 214.0.0.0/7• 198.18.0.0/15• 169.254.0.0/16
Reserved public CIDR blocks	<ul style="list-style-type: none">• 0.0.0.0/8• 127.0.0.0/8• 240.0.0.0/4• 255.255.255.255/32

Procedure


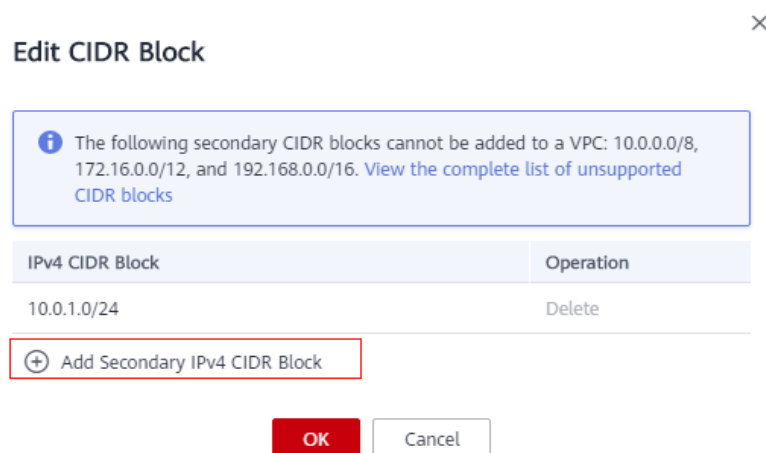
1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the VPC list, locate the row that contains the VPC and click **Edit CIDR Block** in the **Operation** column.
The **Edit CIDR Block** dialog box is displayed.
4. Click **Add Secondary IPv4 CIDR Block**.

Figure 1-3 Add Secondary IPv4 CIDR Block

5. Enter the secondary CIDR block and click **OK**.

1.2.3 Modifying a VPC

Scenarios



You can modify the following information about a VPC:

- [Modifying the Name and Description of a VPC](#)
- [Modifying the CIDR Block of a VPC](#)


NOTICE



If the [secondary IPv4 CIDR block](#) function is available in a region, the CIDR block of a VPC in this region cannot be modified through the console. You can call an API to modify VPC CIDR block. For details, see section "Updating VPC Information" in the *Virtual Private Cloud API Reference*.

Modifying the Name and Description of a VPC



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. Modify the name and description of a VPC using either of the following methods:
 - Method 1:
 - i. In the VPC list, click  on the right of the VPC name.
 - ii. Enter the VPC name and click **OK**.
 - Method 2:

- i. In the VPC list, click the VPC name with a hyperlink.
The **Summary** page is displayed.
- ii. Click  on the right of the VPC name or description, enter the information, and click .

Modifying the CIDR Block of a VPC

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the VPC list, locate the row that contains the VPC and click **Edit CIDR Block** in the **Operation** column.
The **Edit CIDR Block** dialog box is displayed.
5. Modify the VPC CIDR block as prompted.

NOTICE

A VPC CIDR block must be from 10.0.0.0/8-24, 172.16.0.0/12-24, or 192.168.0.0/16-24.

- If a VPC has no subnets, you can change both its network address and subnet mask.
- If a VPC has subnets, you only can change its subnet mask.

6. Click **OK**.

1.2.4 Managing VPC Tags

Scenarios

You can add tags to VPCs to help you identify and organize them.

You can add tags when creating a VPC or add tags to existing VPCs.

Each cloud resource can have a maximum of 20 tags.



A tag consists of a key and value pair. [Table 1-7](#) lists the tag key and value requirements.

Table 1-7 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each VPC and can be the same for different VPCs.• Can contain a maximum of 36 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	vpc_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including periods (.), hyphens (-) and underscores (_)	vpc-01

Procedure

Search for VPCs by tag key and value on the page showing the VPC list.



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the upper right corner of the VPC list, click **Search by Tag**.
5. In the displayed area, enter the tag key and value of the VPC you are looking for.

Both the tag key and value must be specified. The system automatically displays the VPCs you are looking for if both the tag key and value are matched.

6. Click + to add more tag keys and values.
You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for VPCs, the VPCs containing all specified tags will be displayed.
7. Click **Search**.

The system displays the VPCs you are looking for based on the entered tag keys and values.

Add, delete, edit, and view tags on the Tags tab of a VPC.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. On the **Virtual Private Cloud** page, locate the VPC whose tags are to be managed and click the VPC name.

The page showing details about the particular VPC is displayed.

5. Click the **Tags** tab and perform desired operations on tags.

- View tags.

On the **Tags** tab, you can view details about tags added to the current VPC, including the number of tags and the key and value of each tag.

- Add a tag.

Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.

- Edit a tag.

Locate the row that contains the tag you want to edit and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, change the tag value and click **OK**.

- Delete a tag.

Locate the row that contains the tag you want to delete, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.



1.2.5 Obtaining a VPC ID

Scenarios

This section describes how to view and obtain a VPC ID.

If you create a VPC peering connection between two VPCs in different accounts, you need to obtain the project ID of the region that the peer VPC resides. You can recommend this section to the user of the peer VPC to obtain the project ID.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. On the **Virtual Private Cloud** page, locate the VPC and click its name.

The VPC details page is displayed.

5. In the **VPC Information** area, view the VPC ID.


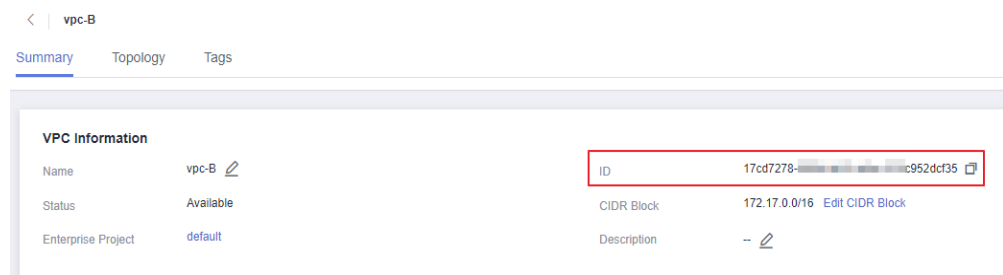
Click  next to ID to copy the VPC ID.

Figure 1-4 VPC ID





1.2.6 Viewing a VPC Topology

Scenarios

This section describes how to view the topology of a VPC. The topology displays the subnets in a VPC and the ECSs in the subnets.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. In the VPC list, click the name of the VPC for which the topology is to be viewed.

The VPC details page is displayed.

5. Click the **Topology** tab to view the VPC topology.

The topology displays the subnets in the VPC and the ECSs in the subnets.

You can also perform the following operations on subnets and ECSs in the topology:

- Modify or delete a subnet.
- Add an ECS to a subnet, bind an EIP to the ECS, and change the security group of the ECS.




1.2.7 Exporting VPC List

Scenarios

Information about all VPCs under your account can be exported as an Excel file to a local directory.

This file records the names, ID, status, CIDR blocks, and the number of subnets of your VPCs.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the upper right corner of the VPC list, click .
The system will automatically export information about all VPCs under your account in the current region as an Excel file to a local directory.


1.2.8 Deleting a Secondary IPv4 CIDR Block from a VPC

Scenarios

If a secondary CIDR block of a VPC is no longer required, you can delete it.

- A secondary IPv4 CIDR block of a VPC can be deleted, but the primary CIDR block cannot be deleted.
- If you want to delete a secondary CIDR block that contains subnets, you need to delete the subnets first.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the VPC list, locate the row that contains the VPC and click **Edit CIDR Block** in the **Operation** column.
The **Edit CIDR Block** dialog box is displayed.
4. Locate the row that contains the secondary CIDR block to be deleted and click **Delete** in the **Operation** column.
5. Click **OK**.

1.2.9 Deleting a VPC

Scenarios

If you no longer need a VPC, you can delete it.

NOTICE


VPCs are free of charge.

Notes and Constraints

If you want to delete a VPC that has subnets, custom routes, or other resources, you need to delete these resources as prompted on the console first and then delete the VPC.

You can refer to [Why Can't I Delete My VPCs and Subnets?](#)

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. On the **Virtual Private Cloud** page, locate the row that contains the VPC to be deleted and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
4. Confirm the information and click **Yes**.

NOTICE

If a VPC cannot be deleted, a message will be displayed on the console. Delete the resources that are in the VPC by referring to [Why Can't I Delete My VPCs and Subnets?](#)

1.3 Subnet



1.3.1 Creating a Subnet for the VPC

Scenarios

A VPC comes with a default subnet. If the default subnet cannot meet your requirements, you can create one.

A subnet is configured with DHCP by default. When an ECS in this subnet starts, the ECS automatically obtains an IP address using DHCP.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.

5. Click **Create Subnet**.
The **Create Subnet** page is displayed.
6. Set the parameters as prompted.

Table 1-8 Parameter descriptions

Parameter	Description	Example Value
VPC	The VPC for which you want to create a subnet.	-
AZ	<p>An AZ is a geographic location with independent power supply and network facilities in a region. AZs are physically isolated, and AZs in the same VPC are interconnected through an internal network. For details, see Region and AZ.</p> <p>Note the following when you select an AZ:</p> <ul style="list-style-type: none">• Subnets in a VPC can be in different AZs. For example, a VPC can have a subnet in AZ 1, and another subnet in AZ 3.• A cloud resource can be in a different AZ from its subnet. For example, a cloud server in AZ 1 can be in a subnet in AZ 3. If AZ 3 becomes faulty, cloud servers in AZ 1 can still use the subnet in AZ 3, and your services are not interrupted.	AZ1
Name	<p>The subnet name.</p> <p>The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.</p>	Subnet
IPv4 CIDR Block	<p>The CIDR block for the subnet. This value must be within the VPC CIDR block.</p> <p>This parameter is displayed only in regions where IPv4/IPv6 dual stack is supported.</p>	192.168.0.0/24

Parameter	Description	Example Value
IPv6 CIDR Block	<p>Specifies whether to set IPv6 CIDR Block to Enable.</p> <p>This parameter is displayed only in regions where IPv4/IPv6 dual stack is supported.</p> <p>If you select this option, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.</p>	-
Associated Route Table	The default route table to which the subnet will be associated. You can change the route table to a custom route table on the Subnets page.	Default
Gateway	The gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1
DNS Server Address	<p>Huawei Cloud private DNS server addresses are entered by default. This allows ECSs in a VPC to communicate with each other and also access other cloud services using private domain names without exposing their IP addresses to the Internet.</p> <p>You can change the default DNS server addresses if needed. This may interrupt your access to cloud services.</p> <p>You can also click Reset on the right to restore the DNS server addresses to the default value.</p> <p>A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x

Parameter	Description	Example Value
DHCP Lease Time	<p>The period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client.</p> <ul style="list-style-type: none">● Limited: Set the DHCP lease time. The unit can be day or hour.● Unlimited: The DHCP lease time does not expire. <p>If the time period is changed, the new lease time takes effect when the instance (such as an ECS) in the subnet is renewed next time. You can wait for the instance to be renewed automatically or manually modify the lease time. If you want the new lease time to take effect immediately, manually renew the lease or restart the ECS.</p>	-
Tag	<p>The subnet tag, which consists of a key and value pair.</p> <p>Each cloud resource can have a maximum of 20 tags.</p> <p>The tag key and value must meet the requirements listed in Table 1-9.</p>	<ul style="list-style-type: none">● Key: subnet_key1● Value: subnet-01
Description	<p>Supplementary information about the subnet. This parameter is optional.</p> <p>The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-

Table 1-9 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each subnet.• Can contain a maximum of 36 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	subnet_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	subnet-01

7. Click **OK**.

Precautions

After a subnet is created, some reserved IP addresses cannot be used. For example, in a subnet with CIDR block 192.168.0.0/24, the following IP addresses are reserved:

- 192.168.0.0: Network ID. This address is the beginning of the private IP address range and will not be assigned to any instance.
- 192.168.0.1: Gateway address.
- 192.168.0.253: Reserved for the system interface. This IP address is used by the VPC for external communication.
- 192.168.0.254: DHCP service address.
- 192.168.0.255: Network broadcast address.

If you configured the default settings under **Advanced Settings** during subnet creation, the reserved IP addresses may be different from the default ones, but there will still be five of them. The specific addresses depend on your subnet settings.

1.3.2 Modifying a Subnet

Scenarios

Modify the subnet name, NTP server address, and DNS server address.

Notes and Constraints

After a subnet is created, its AZ cannot be changed.

Procedure




1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. In the subnet list, locate the target subnet and click its name.
The subnet details page is displayed.
6. On the **Summary** tab, click  on the right of the parameter to be modified and modify the parameter as prompted.

Table 1-10 Parameter descriptions

Parameter	Description	Example Value
Name	The subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet

Parameter	Description	Example Value
DNS Server Address	<p>By default, two DNS server addresses are configured. You can change them as required. A maximum of two DNS server addresses are supported. Use commas (,) to separate every two addresses.</p> <p>Huawei Cloud private DNS server addresses are entered by default. This allows ECSs in a VPC to communicate with each other and also access other cloud services using private domain names without exposing their IP addresses to the Internet.</p> <p>You can change the default DNS server addresses if needed. This may interrupt your access to cloud services.</p> <p>You can also click Reset on the right to restore the DNS server addresses to the default value.</p> <p>A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x

Parameter	Description	Example Value
DHCP Lease Time	<p>The period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client.</p> <ul style="list-style-type: none">● Limited: Set the DHCP lease time. The unit can be day or hour.● Unlimited: The DHCP lease time does not expire. <p>If the time period is changed, the new lease time takes effect when the instance (such as an ECS) in the subnet is renewed next time. You can wait for the instance to be renewed automatically or manually modify the lease time. If you want the new lease time to take effect immediately, manually renew the lease or restart the ECS.</p>	-
Description	<p>Supplementary information about the subnet. This parameter is optional.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-

7. Click **OK**.

1.3.3 Managing Subnet Tags

Scenarios

You can add tags to subnets to help you identify and organize them.

You can add tags when creating a subnet or add tags to existing subnets.

Each cloud resource can have a maximum of 20 tags.



A tag consists of a key and value pair. [Table 1-11](#) lists the tag key and value requirements.

Table 1-11 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each subnet.• Can contain a maximum of 36 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	subnet_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	subnet-01

Procedure

Search for subnets by tag key and value on the page showing the subnet list.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. In the upper right corner of the subnet list, click **Search by Tag**.
6. Enter the tag key of the subnet to be queried.
Both the tag key and value must be specified. The system automatically displays the subnets you are looking for if both the tag key and value are matched.
7. Click **+** to add another tag key and value.


You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for subnets, the subnets containing all specified tags will be displayed.


8. Click **Search**.

The system displays the subnets you are looking for based on the entered tag keys and values.

Add, delete, edit, and view tags on the Tags tab of a subnet.

1. Log in to the management console.

2. Click  in the upper left corner and select the desired region and project.

3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.

The **Subnets** page is displayed.

5. In the subnet list, locate the target subnet and click its name.

6. On the subnet details page, click the **Tags** tab and perform desired operations on tags.

– View tags.

On the **Tags** tab, you can view details about tags added to the current subnet, including the number of tags and the key and value of each tag.

– Add a tag.

Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.

– Edit a tag.

Locate the row that contains the tag you want to edit and click **Edit** in the **Operation** column. In the **Edit Tag** dialog box, change the tag value and click **OK**.

– Delete a tag.

Locate the row that contains the tag you want to delete, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

1.3.4 Viewing and Deleting Resources in a Subnet

Scenarios

VPC subnets have private IP addresses used by cloud resources. This section describes how to view resources that are using private IP addresses of subnets. If these resources are no longer required, you can delete them.

You can view resources, including ECSs, BMSs, network interfaces, load balancers, and NAT gateways.

NOTICE

After you delete all resources in a subnet by referring to this section, the message "Delete the resource that is using the subnet and then delete the subnet." is displayed when you delete the subnet, you can refer to [Viewing IP Addresses in a Subnet](#).

Procedure



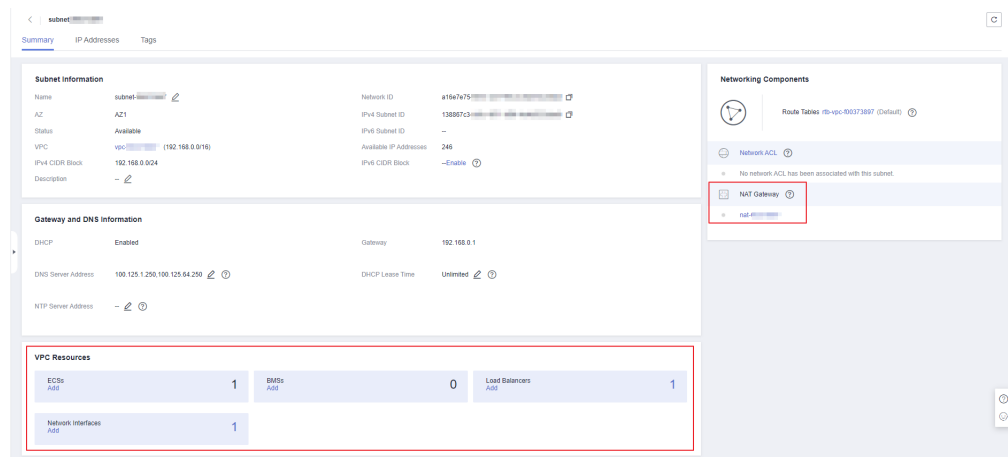

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. Locate the target subnet and click its name.
The subnet details page is displayed.
6. On the **Summary** page, view the resources in the subnet.
 - a. In the **VPC Resources** area, view the quantities of resources, such as ECSs, BMSs, network interfaces, and load balancers, in the subnet. Click the resource quantity with a hyperlink to view the resources in the subnet.
 - b. In the **Networking Components** area on the right of the page, view the NAT gateways in the subnet.

Figure 1-5 Viewing resources in a subnet

7. Delete resources from the subnet.

Table 1-12 Viewing and deleting resources in a subnet

Resource	Reference
ECS	<p>Currently, you cannot directly switch to ECSs from the subnet details page. You need to search for the target ECS in the ECS list and delete it.</p> <ol style="list-style-type: none">In the ECS list, click the ECS name. The ECS details page is displayed.In the NICs area, view the name of the subnet associated with the ECS.Confirm the information and delete the ECS.
BMS	<p>Currently, you cannot directly switch to BMSs from the subnet details page. You need to search for the target BMS in the BMS list and delete it.</p> <ol style="list-style-type: none">In the BMS list, click the BMS name. The BMS details page is displayed.In the NICs tab, view the subnet associated with the BMS.Confirm the information and release the BMS.
Load balancer	<p>You can directly switch to load balancers from the subnet details page.</p> <ol style="list-style-type: none">Click the load balancer quantity. The load balancer list is displayed.Locate the row that contains the load balancer and click Delete in the Operation column. For details, see Deleting a Load Balancer.
Network interface	<p>You can directly switch to network interfaces from the subnet details page.</p> <ol style="list-style-type: none">Click the network interface quantity. The Network Interfaces page is displayed.Locate the row that contains the network interface and choose More > Delete in the Operation column. For details, see Deleting a Network Interface.
NAT gateway	<p>You can directly switch to NAT gateways from the subnet details page.</p> <ol style="list-style-type: none">Click the NAT gateway name in the Networking Components area. The NAT gateway details page is displayed.Click  to return to the NAT gateway list.Locate the row that contains the NAT gateway and click Delete in the Operation column.<ul style="list-style-type: none">Deleting a Public NAT Gateway

1.3.5 Viewing IP Addresses in a Subnet

Scenarios

A subnet is an IP address range in a VPC. This section describes how to view the used IP addresses in a subnet.

- Virtual IP addresses
- Private IP addresses
 - Used by the subnet itself, such as the gateway, DHCP, and system interface.
 - Used by cloud resources, such as ECSs, load balancers, and RDS instances.

Notes and Constraints

- A subnet cannot be deleted if its IP addresses are used by cloud resources.
- A subnet can be deleted if its IP addresses are used by itself.

Procedure



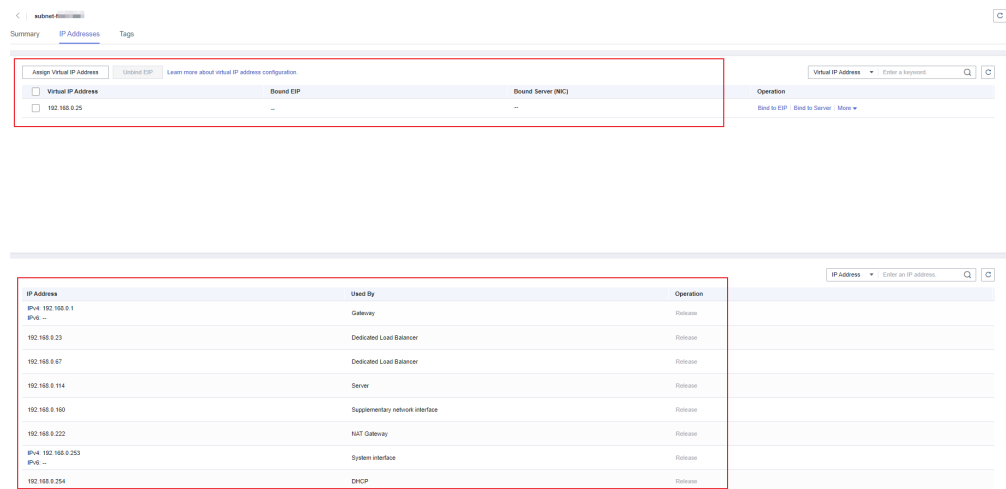
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. Locate the target subnet and click its name.
The subnet details page is displayed.
6. Click the **IP Addresses** tab to view the IP addresses in the subnet.
 - a. In the virtual IP address list, you can view the virtual IP addresses assigned from the subnet.
 - b. In the private IP address list in the lower part of the page, you can view the private IP addresses and the resources that use the IP addresses of the subnet.

Figure 1-6 Viewing IP addresses in a subnet

Follow-up Operations




If you want to view and delete the resources in a subnet, refer to [Why Can't I Delete My VPCs and Subnets?](#)

1.3.6 Exporting Subnet List

Scenarios

Information about all subnets under your account can be exported as an Excel file to a local directory. This file records the name, ID, VPC, CIDR block, and associated route table of each subnet.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. In the upper right corner of the subnet list, click .
The system will automatically export information about all subnets under your account in the current region as an Excel file to a local directory.

1.3.7 Deleting a Subnet

Scenarios

If your subnet is no longer required, you can delete it:

NOTICE



Subnets are free of charge.

Notes and Constraints

If you want to delete a subnet that has custom routes, virtual IP addresses, or other resources (ECSs, load balancers, or NAT gateways), you need to delete these resources as prompted on the console first and then delete the subnet.

You can refer to [Why Can't I Delete My VPCs and Subnets?](#)

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. In the subnet list, locate the row that contains the subnet you want to delete and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
6. Click **Yes**.

NOTICE

If a VPC cannot be deleted, a message will be displayed on the console. Delete the resources that are in the VPC by referring to [Why Can't I Delete My VPCs and Subnets?](#)

1.4 IPv4 and IPv6 Dual-Stack Network

What Is an IPv4 and IPv6 Dual-Stack Network?

An IPv4 and IPv6 dual-stack network allows your resources, such as ECSs, to use both IPv4 and IPv6 addresses for private and public network communications. [Figure 1-7](#) shows how an IPv4 and IPv6 dual-stack network works.

Figure 1-7 An IPv4 and IPv6 dual-stack network

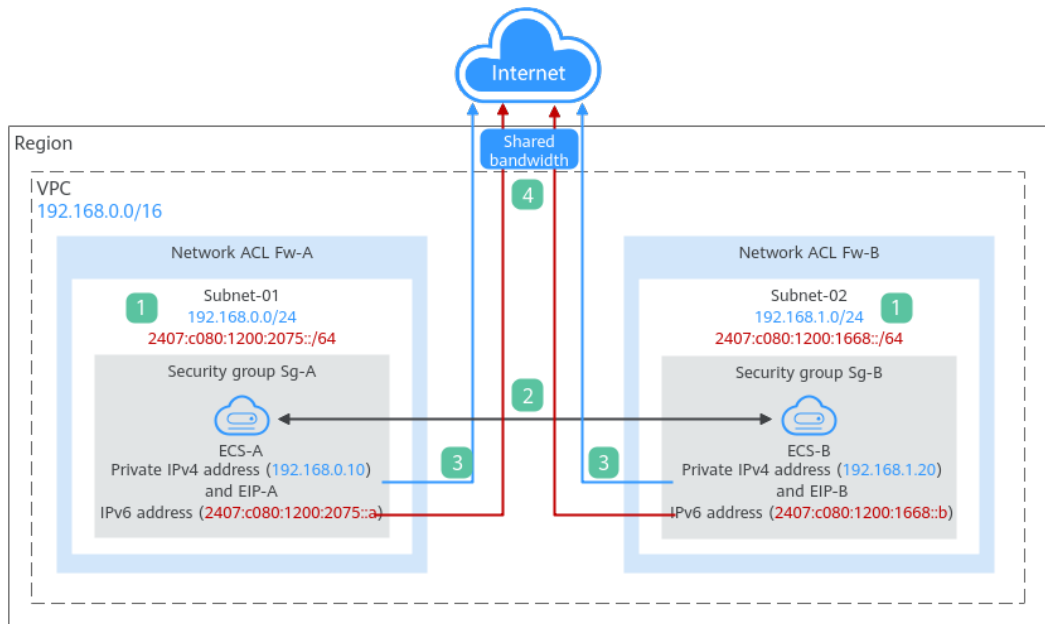


Table 1-13 Steps for deploying a dual-stack network

Step	Description
1	If you enable IPv6 when adding a VPC subnet, an IPv6 CIDR block is automatically assigned to the subnet. You cannot customize the IPv6 CIDR block.
2	Subnets in the same VPC can communicate with each other by default. Network ACLs protect subnets, and security groups protect the instances in it. <ol style="list-style-type: none"> Subnets in different network ACLs are isolated from each other. To connect these subnets, you need to add inbound and outbound rules to allow traffic in and out of the subnets. Security groups are isolated from each other. If two instances are associated with different security groups, you need to add inbound and outbound rules to allow the instances to communicate with each other. As shown in Figure 1-7 , if allow rules are configured for network ACLs Fw-A and Fw-B and security groups Sg-A and Sg-B , ECS-A and ECS-B can communicate with each other: <ul style="list-style-type: none"> Using private IPv4 addresses (192.168.0.10 and 192.168.1.20). Using IPv6 addresses (2407:c080:1200:2075::a and 2407:c080:1200:1668::b).
3	To enable instances to communicate with the Internet using IPv4 addresses, you need to buy an EIP and bind it to the instance. An EIP can be bound to only one instance. <p>As shown in Figure 1-7, you can bind EIP-A to ECS-A and EIP-B to ECS-B so that ECS-A and ECS-B can communicate with the Internet.</p>

Step	Description
4	<p>To enable instances to communicate with the Internet using an IPv6 address, you need to add the IPv6 address to a shared bandwidth. You can add multiple IPv6 addresses to a shared bandwidth.</p> <p>As shown in Figure 1-7, you can add the IPv6 addresses of ECS-A and ECS-B to a shared bandwidth so that ECS-A and ECS-B can communicate with the Internet.</p>

Notes and Constraints

- The IPv4/IPv6 dual-stack function is free for now, but will be billed at a later date (price yet to be determined).
- Only certain ECS specifications support IPv6 networks and can use IPv4/IPv6 dual-stack networks. You need to select such ECSs in supported regions.
To check which ECSs support IPv6:
 - On the ECS console: Click **Buy ECS**. On the displayed page, view the ECS specifications.
If there is the **IPv6** parameter with the value of **Yes**, the ECS specifications support IPv6.

IPv4 and IPv6 Dual-Stack Application Scenarios

If your ECS supports IPv6, you can build an IPv4 and IPv6 dual-stack network. [Table 1-14](#) shows where IPv4 and IPv6 dual-stack networks can be used.

Table 1-14 Application scenarios of IPv4 and IPv6 dual-stack networks

Application Scenario	Scenario	Subnet	ECS
Private communication using IPv6 addresses	Your applications deployed on ECSs need to communicate with other systems (such as databases) through private networks using IPv6 addresses.	<ul style="list-style-type: none"> IPv4 CIDR block IPv6 CIDR block 	<ul style="list-style-type: none"> Private IPv4 address: used for private communication IPv6 address: used for private communication.

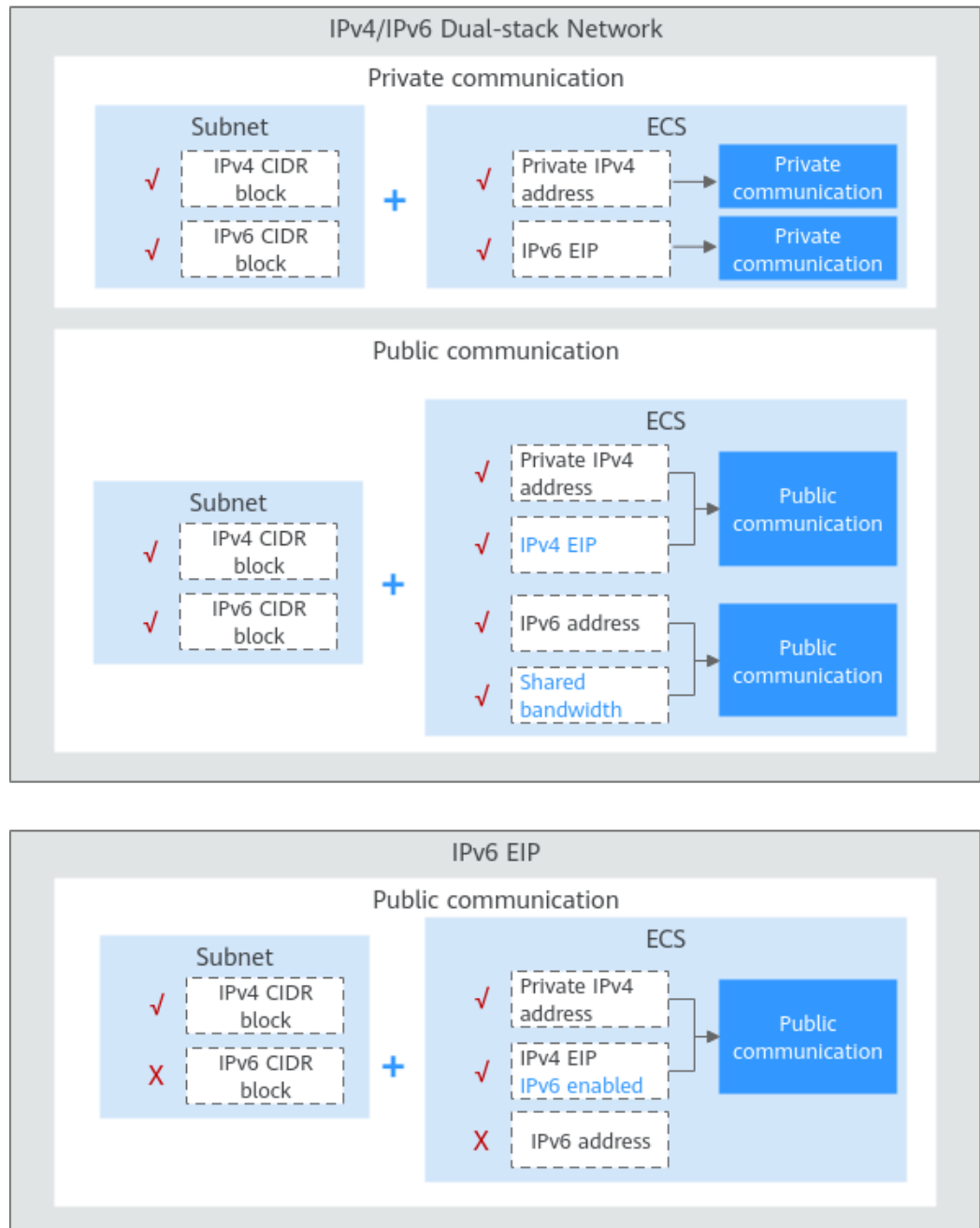
Application Scenario	Scenario	Subnet	ECS
Public communication using IPv6 addresses	Your applications deployed on ECSs need to provide services accessible from the Internet using IPv6 addresses.	<ul style="list-style-type: none"> IPv4 CIDR block IPv6 CIDR block 	<ul style="list-style-type: none"> Private IPv4 address + IPv4 EIP: used for public network communication IPv6 address + shared bandwidth: used for public network communication
	Your applications deployed on ECSs need to both provide services accessible from the Internet and analyze the access request data using IPv6 addresses.		

If your ECS flavor does not support IPv6 addresses, you can enable the IPv6 EIP function to allow communications using IPv6 addresses. For details, see [Table 1-15](#).

Table 1-15 Application scenarios of IPv6 EIPs

Application Scenario	Description	Subnet	ECS
Public communication using IPv6 addresses	Your applications deployed on ECSs need to provide services accessible from the Internet using IPv6 addresses.	IPv4 CIDR block	<ul style="list-style-type: none"> Private IPv4 address IPv4 EIP (with IPv6 function enabled): used for public communication using IPv4 and IPv6 EIPs

Figure 1-8 Application scenarios of IPv6 networks



Operation Guide on IPv6 Networks

Operations on an IPv6 network are similar to those on an IPv4 network. Only some functions are configured in a different way. [Table 1-16](#) describes how you can build and use an IPv6 network.

Table 1-16 Operation guide on IPv6 networks

Scenario	Description	Reference
Creating an IPv6 subnet	Select Enable for IPv6 CIDR Block when creating a subnet. An IPv6 CIDR block will be automatically assigned to the subnet. <ul style="list-style-type: none">You cannot customize an IPv6 CIDR block.IPv6 cannot be disabled after the subnet is created.You can enable IPv6 for existing subnets.	Creating a Subnet for the VPC
Viewing in-use IPv6 addresses	In the subnet list, click the subnet name. On the displayed page, view in-use IPv4 and IPv6 addresses on the IP Addresses tab.	Viewing IP Addresses in a Subnet
Adding a security group rule (IPv6)	Add a security group rule with Type set to IPv6 and Source or Destination set to an IPv6 address or IPv6 CIDR block.	Adding a Security Group Rule
Adding a network ACL rule (IPv6)	Add a network ACL rule with Type set to IPv6 and Source or Destination set to an IPv6 address or IPv6 CIDR block.	Adding a Network ACL Rule (Default Effective Sequence)
Adding an IPv6 route to the VPC route table	Add a route with Destination and Next Hop set to an IPv4 or IPv6 CIDR block. <ul style="list-style-type: none">If the destination is an IPv6 CIDR block, the next hop can only be an IP address in the same VPC as the IPv6 CIDR block.If the destination is an IPv6 CIDR block, the next hop type can only be ECS, extension NIC, or virtual IP address. They must also have IPv6 addresses.	Adding a Custom Route
Assigning a virtual IPv6 address	If IPv6 is enabled for a VPC subnet, you can set IP Address Type to IPv6 when assigning for a virtual IP address.	Assigning a Virtual IP Address

2 Route Tables

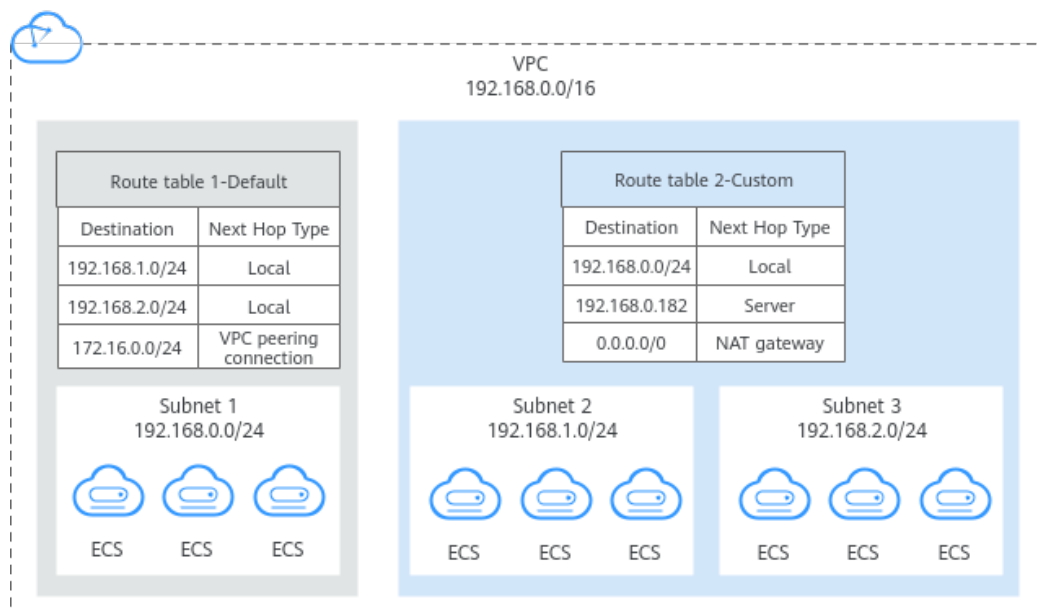
2.1 Route Tables and Routes

Route Tables

A route table contains a set of routes that are used to determine where network traffic from your subnets in a VPC is directed. Each subnet must be associated with a route table. A subnet can only be associated with one route table, but you can associate multiple subnets with the same route table.

Both IPv4 and IPv6 routes are supported.

Figure 2-1 Route tables



- **Default route table:** When you create a VPC, the system automatically generates a default route table for the VPC. If you create a subnet in the VPC, the subnet automatically associates with the default route table. The default route table ensures that subnets in a VPC can communicate with each other.

- You can add routes to, delete routes from, and modify routes in the default route table, but cannot delete the table.
- When you create a VPC endpoint, VPN or Direct Connect connection, the default route table automatically delivers a route that cannot be deleted or modified.
- Custom route table: If you do not want to use the default route table, you can create a custom route table and associate it with the subnet. Custom route tables can be deleted if they are no longer required.

The custom route table associated with a subnet affects only the outbound traffic. The default route table of a subnet controls the inbound traffic.

NOTE

To use a custom route table, you need to submit a service ticket. You need to click **Increase quota** on the **Create Route Table** page or choose **More > Service Tickets > Create Service Ticket** in the upper right corner of the page. For more information, see [Submitting a Service Ticket](#).

Route

You can add routes to default and custom route tables and configure the destination, next hop type, and next hop in the routes to determine where network traffic is directed. Routes are classified into system routes and custom routes.

- System routes: These routes are automatically added by the system and cannot be modified or deleted.

After a route table is created, the system automatically adds the following system routes to the route table, so that instances in a VPC can communicate with each other.

- Routes whose destination is 100.64.0.0/10 or 198.19.128.0/20.
- Routes whose destination is a subnet CIDR block.

If you enable IPv6 when creating a subnet, the system automatically assigns an IPv6 CIDR block to the subnet. Then, you can view IPv6 routes in its route table. Example destinations of subnet CIDR blocks are as follows:

- IPv4: 192.168.2.0/24
- IPv6: 2407:c080:802:be7::/64

NOTE

In addition to the preceding system routes, the system automatically adds a route whose destination is 127.0.0.0/8. This is the local loopback address.

- Custom routes: These are routes that you can add, modify, and delete. The destination of a custom route cannot overlap with that of a system route.

You can add a custom route and configure the destination, next hop type, and next hop in the route to determine where network traffic is directed. [Table 2-1](#) lists the supported types of next hops.

You cannot add two routes with the same destination to a VPC route table even if their next hop types are different. The route priority depends on the

destination. According to the longest match routing rule, the destination with a higher matching degree is preferentially selected for packet forwarding.

Table 2-1 Next hop type

Next Hop Type	Description	Supported Route Table
Server	Traffic intended for the destination is forwarded to an ECS in the VPC.	<ul style="list-style-type: none">• Default route table• Custom route table
Extension NIC	Traffic intended for the destination is forwarded to the extension NIC of an ECS in the VPC.	<ul style="list-style-type: none">• Default route table• Custom route table
BMS user-defined network	Traffic intended for the destination is forwarded to a BMS user-defined network.	<ul style="list-style-type: none">• Custom route table
Direct Connect gateway	Traffic intended for the destination is forwarded to a Direct Connect gateway.	Custom route table
NAT gateway	Traffic intended for the destination is forwarded to a NAT gateway.	<ul style="list-style-type: none">• Default route table• Custom route table
VPC peering connection	Traffic intended for the destination is forwarded to a VPC peering connection.	<ul style="list-style-type: none">• Default route table• Custom route table
Virtual IP address	Traffic intended for the destination is forwarded to a virtual IP address and then sent to active and standby ECSs to which the virtual IP address is bound.	<ul style="list-style-type: none">• Default route table• Custom route table
VPC endpoint	Traffic intended for the destination is forwarded to a VPC endpoint.	<ul style="list-style-type: none">• Default route table• Custom route table
Cloud container	Traffic intended for the destination is forwarded to a cloud container.	<ul style="list-style-type: none">• Default route table• Custom route table

Next Hop Type	Description	Supported Route Table
Enterprise router	Traffic intended for the destination is forwarded to an enterprise router.	<ul style="list-style-type: none">• Default route table• Custom route table
Cloud firewall	Traffic intended for the destination is forwarded to a cloud firewall.	<ul style="list-style-type: none">• Default route table• Custom route table

NOTE

If you specify the destination when creating a resource, a system route is delivered. If you do not specify a destination when creating a resource, a custom route that can be modified or deleted is delivered.

For example, when you create a NAT gateway, the system automatically delivers a custom route without a specific destination (0.0.0.0/0 is used by default). In this case, you can change the destination. However, when you create a VPN gateway, you need to specify the remote subnet, that is, the destination of a route. In this case, the system delivers this system route. Do not modify the route destination on the **Route Tables** page. If you do, the destination will be inconsistent with the configured remote subnet. To modify the route destination, go to the specific resource page and modify the remote subnet, then the route destination will be changed accordingly.

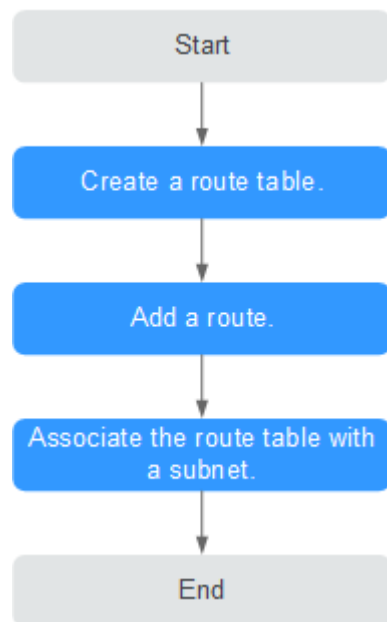
Notes and Constraints

When you create a VPC, the system automatically generates a default route table for the VPC. You can also create a custom route table.

- A VPC can be associated with a maximum of five route tables, including the default route table and four custom route tables.
- All route tables in a VPC can have a maximum of 1,000 routes, excluding system routes.
- In a VPC route table, the route priority is as follows:
 - Local route: A route that is automatically added by the system for communication within a VPC. It has a higher priority than a custom route.
 - Custom route: A route added by a user or routes that are delivered during instance creation. It uses the longest prefix match rule to find a destination for packet forwarding.

Custom Route Table Configuration Process

[Figure 2-2](#) shows the process of creating and configuring a custom route table.

Figure 2-2 Route table configuration process

1. For details about how to create a custom route table, see [Creating a Custom Route Table](#).
2. For details about how to add a custom route, see [Adding a Custom Route](#).
3. For details about how to associate a subnet with a route table, see [Associating a Route Table with a Subnet](#). After the association, the routes in the route table control the routing for the subnet.

2.2 Managing Route Tables

2.2.1 Creating a Custom Route Table

Scenarios

A VPC automatically comes with a default route table. If your default route table cannot meet your service requirements, you can create a custom route table.

Notes and Constraints

By default, you do not have a quota for creating custom route tables. To create custom route tables, you need to apply for a quota increase first. For details, see [How Do I Apply for a Higher Quota?](#)

Procedure

1. Go to the [route table list page](#).
2. In the upper right corner, click **Create Route Table**. On the displayed page, configure parameters as prompted.

Table 2-2 Parameter descriptions

Parameter	Description	Example Value
Name	The name of the route table. This parameter is mandatory. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	rtb-001
VPC	The VPC that the route table belongs to. This parameter is mandatory.	vpc-001
Description	Supplementary information about the route table. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-
Route Settings	The route information. This parameter is optional. You can add a route when creating the route table or after the route table is created. For details, see Adding a Custom Route . You can click + to add more routes.	-

3. Click **OK**.

A message is displayed. You can determine whether to associate the route table with subnets immediately as prompted. If you want to associate immediately, perform the following operations:

- a. Click **Associate Subnet**. The route table details page is displayed.
- b. Click **Associate Subnet** and select the target subnets to be associated.
- c. Click **OK**.

2.2.2 Associating a Route Table with a Subnet

Scenarios

After a subnet is created, the system associates the subnet with the default route table of its VPC. If you want to use specific routes for a subnet, you can associate the subnet with a custom route table.

The custom route table associated with a subnet affects only the outbound traffic. The default route table determines the inbound traffic.



NOTICE

After a route table is associated with a subnet, the routes in the route table control the routing for the subnet and apply to all cloud resources in the subnet.

Notes and Constraints

- A subnet must have a route table associated and can only be associated with one route table.
- A route table can be associated with multiple subnets.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. In the route table list, locate the row that contains the target route table and click **Associate Subnet** in the **Operation** column.
6. Select the subnet to be associated.
7. Click **OK**.

2.2.3 Changing the Route Table Associated with a Subnet

Scenarios

You can change the route table for a subnet. If the route table for a subnet is changed, routes in the new route table will apply to all cloud resources in the subnet.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. Click the name of the target route table.
6. On the **Associated Subnets** tab page, click **Change Route Table** in the **Operation** column and select a new route table as prompted.

7. Click **OK**.



After the route table for a subnet is changed, routes in the new route table will apply to all cloud resources in the subnet.

2.2.4 Viewing the Route Table Associated with a Subnet

Scenarios

This section describes how to view the route table associated with a subnet.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. Locate the target subnet and click its name.
The subnet details page is displayed.
6. In the right of the subnet details page, view the route table associated with the subnet.
7. Click the name of the route table.
The route table details page is displayed. You can further view the route information.



2.2.5 Viewing Route Table Information

Scenarios

This section describes how to view detailed information about a route table, including:

- Basic information, such as name, type (default or custom), and ID of the route table
- Routes, such as destination, next hop, and route type (system or custom)
- Associated subnets

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.




4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. Click the name of the target route table.
The route table details page is displayed.
 - a. On the **Summary** tab page, view the basic information and routes of the route table.
 - b. On the **Associated Subnets** tab page, view the subnets associated with the route table.

2.2.6 Exporting Route Table Information

Scenarios

Information about all route tables under your account can be exported as an Excel file to a local directory. This file records the name, ID, VPC, type, and number of associated subnets of the route tables.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. On the displayed page, click  in the upper right of the route table list.
The system will automatically export information about all route tables under your account in the current region as an Excel file to a local directory.

2.2.7 Deleting a Route Table



Scenarios

This section describes how to delete a custom route table.

Notes and Constraints

- The default route table cannot be deleted.
However, deleting a VPC will also delete its default route table. Both default and custom route tables are free of charge.
- A custom route table with a subnet associated cannot be deleted directly.
If you want to delete such a route table, you can associate the subnet with another route table first by referring to [Changing the Route Table Associated with a Subnet](#).

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**. The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. Locate the row that contains the route table you want to delete and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
6. Confirm the information and click **OK**.

2.3 Managing Routes

2.3.1 Adding a Custom Route

Scenarios

Each route table contains a default system route, which indicates that ECSs in a VPC can communicate with each other. You can also add custom routes as required to forward the traffic destined for the destination to the specified next hop.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. In the route table list, click the name of the route table to which you want to add a route.
6. Click **Add Route** and set parameters as prompted.
You can click + to add more routes.

Table 2-3 Parameter descriptions

Parameter	Description	Example Value
Destination	<p>Mandatory</p> <p>Enter the destination of the route. You can enter a single IP address or an IP address range in CIDR notation.</p> <p>NOTICE</p> <ul style="list-style-type: none"> The destination of each route in a route table must be unique. If an IP address group contains an IP address range in the format of <i>Start IP address-End IP address</i>, the IP address group is not supported. For example, an IP address group cannot contain 192.168.0.1-192.168.0.62. You need to change 192.168.0.1-192.168.0.62 to 192.168.0.0/26. 	IPv4: 192.168.0.0/16
Next Hop Type	<p>Mandatory</p> <p>Set the type of the next hop.</p> <p>NOTE</p> <p>When you add or modify a custom route in a default route table, the next hop type of the route cannot be set to VPN gateway, Direct Connect gateway, or Cloud connection.</p>	VPC peering connection
Next Hop	<p>Mandatory</p> <p>Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.</p>	peer-AB
Description	<p>Optional</p> <p>Enter the description of the route in the text box as required.</p>	-

7. Click **OK**.

2.3.2 Modifying a Route

Scenarios

This section describes how to modify a custom route in a route table.

Notes and Constraints

- System routes cannot be modified.
- When you create a VPC endpoint, VPN or Direct Connect connection, the default route table automatically delivers a route that cannot be deleted or modified.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. In the route table list, click the name of the target route table.
6. Locate the row that contains the route to be modified and click **Modify** in the **Operation** column.
7. Modify the route information in the displayed dialog box.

Table 2-4 Parameter descriptions

Parameter	Description	Example Value
Destination	<p>Mandatory</p> <p>Enter the destination of the route. You can enter a single IP address or an IP address range in CIDR notation.</p> <p>NOTICE</p> <ul style="list-style-type: none">• The destination of each route in a route table must be unique.• If an IP address group contains an IP address range in the format of <i>Start IP address-End IP address</i>, the IP address group is not supported. For example, an IP address group cannot contain 192.168.0.1-192.168.0.62. You need to change 192.168.0.1-192.168.0.62 to 192.168.0.0/26.	IPv4: 192.168.0.0/16
Next Hop Type	<p>Mandatory</p> <p>Set the type of the next hop.</p> <p>NOTE</p> <p>When you add or modify a custom route in a default route table, the next hop type of the route cannot be set to VPN gateway, Direct Connect gateway, or Cloud connection.</p>	VPC peering connection
Next Hop	<p>Mandatory</p> <p>Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.</p>	peer-AB
Description	<p>Optional</p> <p>Enter the description of the route in the text box as required.</p>	-

8. Click **OK**.

2.3.3 Replicating a Route

Scenarios

This section describes how to replicate routes among all route tables of a VPC. VPC route tables include the default and custom route tables.

Notes and Constraints

Table 2-5 shows whether routes of different types can be replicated to default or custom route tables.

For example, if the next hop type of a route is a server, this route can be replicated to both default or custom route tables.

If the next hop type of a route is a Direct Connect gateway, the route cannot be replicated to the default route table, but can be replicated to a custom route table.



Table 2-5 Route replication

Next Hop Type	Can Be Replicated to Default Route Table	Can Be Replicated to Custom Route Table
Local	No	No
Server	Yes	Yes
Extension NIC	Yes	Yes
BMS user-defined network	No	Yes
VPN gateway	No	Yes
Direct Connect gateway	No	Yes
Cloud connection	No	Yes
Supplementary network interface	Yes	Yes
NAT gateway	Yes	Yes
VPC peering connection	Yes	Yes
Virtual IP address	Yes	Yes

NOTE

- If the Direct Connect service is enabled by call or email, the routes delivered to the default route table cannot be replicated to a custom route table.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. In the route table list, locate the row that contains the route table you want to replicate routes from and click **Replicate Route** in the **Operation** column.
6. Select the target route table that you want to replicate route to and the routes to be replicated as prompted.
The listed routes are those that do not exist in the target route table. You can select one or more routes to replicate to the target route table.
7. Click **OK**.

2.3.4 Deleting a Route



Scenarios

This section describes how to delete a custom route from a route table.

Notes and Constraints

- System routes cannot be deleted.
- The routes automatically delivered by VPN or Direct Connect to the default route table cannot be deleted. The next hop types of such routes are:
 - VPN gateway
 - Direct Connect gatewayTo delete these routes, you need to delete the associated network instances first.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
5. Locate the target route table and click its name.
The route table details page is displayed.
6. In the route list, locate the row that contains the route to be deleted and click **Delete** in the **Operation** column.

- A confirmation dialog box is displayed.
7. Confirm the information and click **Yes**.

2.4 Configuring an SNAT Server

Scenarios

Together with VPC route tables, you can configure SNAT on an ECS to enable other ECSs that have no EIPs bound in the same VPC to access the Internet through this ECS.

The configured SNAT takes effect for all subnets in a VPC.

Prerequisites

- You have an ECS where SNAT is to be configured.
- The ECS where SNAT is to be configured runs Linux.
- The ECS where SNAT is to be configured has only one network interface card (NIC).



Differences Between SNAT ECSs and NAT Gateways

The NAT Gateway service provides network address translation (NAT) for servers, such as ECSs, BMSs and Workspace desktops, in a VPC or servers from an on-premises data center that connects to a VPC through Direct Connect or VPN. A NAT gateway allows these servers to share an EIP to access the Internet or provide services accessible from the Internet.

The NAT Gateway service is easier to configure and use than SNAT. This service can be flexibly deployed across subnets and AZs and has different NAT gateway specifications. You can click **NAT Gateway** under **Networking** on the management console to try this service.

For details, see the *NAT Gateway User Guide*.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click . In the service list, choose **Compute > Elastic Cloud Server**.
4. On the displayed page, locate the target ECS in the ECS list and click the ECS name to switch to the page showing ECS details.
5. On the displayed ECS details page, click the **NICs** tab.
6. In the displayed area showing the NIC IP address details, disable **Source/Destination Check**.

By default, the source/destination check is enabled. When this check is enabled, the system checks whether source IP addresses contained in the packets sent by ECSs are correct. If the IP addresses are incorrect, the system does not allow the ECSs to send the packets. This mechanism prevents packet

spoofing, thereby improving system security. If the SNAT function is used, the SNAT server needs to forward packets. This mechanism prevents the packet sender from receiving returned packets. Therefore, you need to disable the source/destination check for SNAT servers.

7. Bind an EIP.
 - Bind an EIP to the private IP address of the ECS. For details, see [Assigning an EIP and Binding It to an ECS](#).
 - Bind an EIP to the virtual IP address of the ECS. For details, see [Binding a Virtual IP Address to an EIP or ECS](#).
8. On the ECS console, use the remote login function to log in to the ECS where you plan to configure SNAT.
9. Run the following command and enter the password of user **root** to switch to user **root**:
su - root
10. Run the following command to check whether the ECS can successfully connect to the Internet:

 **NOTE**

Before running the command, you must disable the response iptables rule on the ECS where SNAT is configured and configure security group rules.

ping support.huawei.com

The ECS can access the Internet if the following information is displayed:

```
[root@localhost ~]# ping support.huawei.com
PING support.huawei.com (xxx.xxx.xxx.xxx) 56(84) bytes of data:
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=51 time=9.34 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=51 time=9.11 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=51 time=8.99 ms
```

11. Run the following command to check whether IP forwarding of the Linux OS is enabled:

cat /proc/sys/net/ipv4/ip_forward

In the command output, **1** indicates that IP forwarding is enabled, and **0** indicates that IP forwarding is disabled. The default value is **0**.

- If IP forwarding in Linux is enabled, go to step [14](#).
- If IP forwarding in Linux is disabled, go to [12](#) to enable IP forwarding in Linux.

Many OSs support packet routing. Before forwarding packets, OSs change source IP addresses in the packets to OS IP addresses. Therefore, the forwarded packets contain the IP address of the public sender so that the response packets can be sent back along the same path to the initial packet sender. This method is called SNAT. The OSs need to keep track of the packets where IP addresses have been changed to ensure that the destination IP addresses in the packets can be rewritten and that packets can be forwarded to the initial packet sender. To achieve these purposes, you need to enable the IP forwarding function and configure SNAT rules.

12. Use the vi editor to open the **/etc/sysctl.conf** file, change the value of **net.ipv4.ip_forward** to **1**, and enter **:wq** to save the change and exit.
13. Run the following command to make the change take effect:

sysctl -p /etc/sysctl.conf

14. Configure the SNAT function.

Run the following command to enable all ECSs on the network (for example, 192.168.1.0/24) to access the Internet using the SNAT function:

```
iptables -t nat -A POSTROUTING -o eth0 -s subnet -j SNAT --to nat-instance-ip
```

Figure 2-3 Configuring SNAT

```
[root@host-192-168-1-4 ~]# vi /etc/sysctl.conf^C
[root@host-192-168-1-4 ~]# ^C
[root@host-192-168-1-4 ~]# iptables -t nat -A POSTROUTING -o eth0 -s 192.168.1.0/24 -j SNAT --to 192.168.1.4
```

NOTE

To ensure that the rule will not be lost after the restart, write the rule into the `/etc/rc.local` file.

1. Switch to the `/etc/sysctl.conf` file:

```
vi /etc/rc.local
```

2. Perform [14](#) to configure SNAT.
3. Save the configuration and exit:

```
:wq
```

4. Add the execution permissions for the `rc.local` file:

```
# chmod +x /etc/rc.local
```

15. Check whether the configuration is successful. If information similar to [Figure 2-4](#) (for example, 192.168.1.0/24) is displayed, the configuration was successful.

```
iptables -t nat --list
```

Figure 2-4 Verifying configuration

```
[root@host-192-168-1-4 ~]# iptables -t nat --list
Chain PREROUTING (policy ACCEPT)
target    prot opt source                destination

Chain POSTROUTING (policy ACCEPT)
target    prot opt source                destination
SNAT      all  --  192.168.1.0/24        anywhere             to:192.168.1.4
SNAT      all  --  192.168.1.0/24        anywhere             to:192.168.1.4

Chain OUTPUT (policy ACCEPT)
target    prot opt source                destination
[root@host-192-168-1-4 ~]# _
```

16. Add a route. For details, see section [Adding a Custom Route](#).

Set the destination to `0.0.0.0/0`, and the next hop to the private or virtual IP address of the ECS where SNAT is deployed. For example, the next hop is `192.168.1.4`.

After these operations are complete, if the network communication still fails, check your security group and network ACL configuration to see whether required traffic is allowed.

3 Virtual IP Address

3.1 Virtual IP Address Overview

What Is a Virtual IP Address?

A virtual IP address can be shared among multiple ECSs. An ECS can have a private and a virtual IP address, which allows your users to access the ECS through either IP address.

You can use either IP address to enable layer 2 and layer 3 communications in a VPC, access a different VPC using peering connections, and access cloud servers through EIPs, Direct Connect connections, and VPN connections.

You can bind a virtual IP address to ECSs deployed in the active/standby pair, and then bind an EIP to the virtual IP address. Virtual IP addresses can work together with Keepalived to ensure high availability and disaster recovery. If the active ECS is faulty, the standby ECS automatically takes over services from the active one.

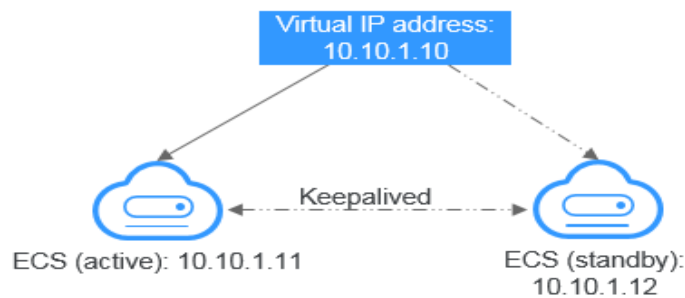
Networking

Virtual IP addresses are used for high availability and can work together with Keepalived to make active/standby ECS switchover possible. This way if one ECS goes down for some reason, the other one can take over and services continue uninterrupted. ECSs can be configured for HA or as load balancing clusters.

- **Networking mode 1: HA**

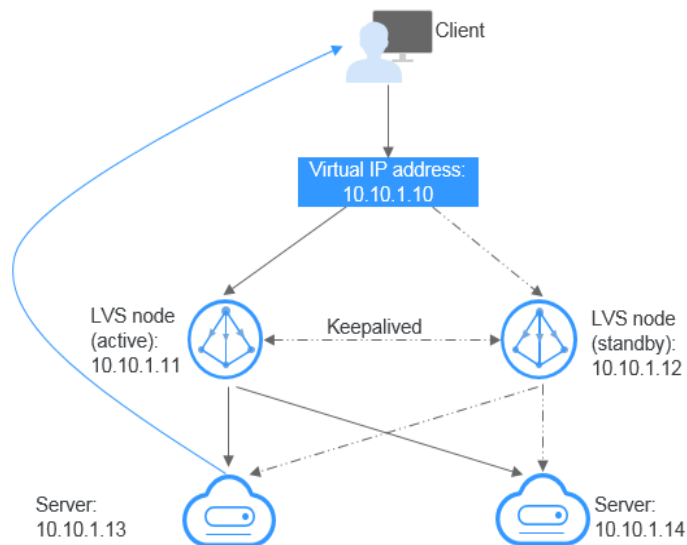
To improve service availability and eliminate single points of failure, you can deploy ECSs in the active/standby pair or deploy one active ECS and multiple standby ECSs. And then, you can bind the same virtual IP address to these ECSs. If the active ECS becomes faulty, a standby ECS takes over services from the active ECS and services continue uninterrupted.

Figure 3-1 Networking diagram of the HA mode



- As shown in the above figure, bind a virtual IP address to two ECSs in the same subnet.
- Configure Keepalived for the two ECSs to work in the active/standby pair. Follow industry standards for configuring Keepalived. The details are not included here.
- **Networking mode 2: HA load balancing cluster**
If you want to build a high-availability load balancing cluster, use Keepalived and configure LVS nodes as direct routers.

Figure 3-2 HA load balancing cluster



- Bind a single virtual IP address to two ECSs.
- Configure the two ECSs as LVS nodes working as direct routers and use Keepalived to configure the nodes in the active/standby pair. The two ECSs will evenly forward requests to different backend servers.
- Configure two more ECSs as backend servers.
- Disable the source/destination check for the two backend servers.
- Check whether the source/destination check is disabled on the active and standby LVS ECSs. For details, see [Disabling Source/Destination Check for an ECS NIC](#).

If you bind an ECS to a virtual IP address on the management console, the source/destination check is automatically disabled. If you bind an ECS to a virtual IP address by calling APIs, you need to manually disable the source/destination check.

Follow industry standards for configuring Keepalived. The details are not included here.

Application Scenarios

- Accessing the virtual IP address through an EIP

If your application has high availability requirements and needs to provide services through the Internet, it is recommended that you bind an EIP to a virtual IP address.

- Using a VPN, Direct Connect, or VPC peering connection to access a virtual IP address

To ensure high availability and access to the Internet, use a VPN for security and Direct Connect for a stable connection. A VPC peering connection is needed so that two VPCs in the same region can communicate with each other.

Notes and Constraints



- Virtual IP addresses are not recommended when multiple NICs in the same subnet are configured on an ECS. Using the virtual IP addresses may cause route conflicts on the ECS, which would lead to communication failures.
- A virtual IP address from a subnet can only be bound to cloud servers from the same subnet.
- If a virtual IP address is used in an active/standby scenario, disable IP forwarding on the standby ECS. For details, see [Disabling IP Forwarding on the Standby ECS](#).
- Virtual IP addresses and extension network interfaces cannot be used to directly access Huawei Cloud services, such as DNS. You can use VPCEP to access these services. For details, see [Buying a VPC Endpoint](#).

3.2 Assigning a Virtual IP Address

Scenarios

If an ECS requires a virtual IP address or if a virtual IP address needs to be reserved, you can assign a virtual IP address from the subnet.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
5. In the subnet list, click the name of the subnet where a virtual IP address is to be assigned.
6. Click the **IP Addresses** tab and click **Assign Virtual IP Address**.
7. Select a virtual IP address assignment mode.
 - **Automatic**: The system assigns an IP address automatically.
 - **Manual**: You can specify an IP address.
8. Select **Manual** and enter a virtual IP address.
9. Click **OK**.

You can then query the assigned virtual IP address in the IP address list.

3.3 Binding a Virtual IP Address to an EIP or ECS

Scenarios

You can use a virtual IP address and an EIP together.

If you bind a virtual IP address to ECSs that work in active/standby pairs and bind an EIP to the virtual IP address, you can access the ECSs over the Internet.



Notes and Constraints

- A virtual IP address can only be bound to one EIP.
- Do not bind more than eight virtual IP addresses to an ECS.
- A virtual IP address can be bound to a maximum of 10 ECSs.

NOTE

If a virtual IP address is bound to an ECS, the virtual IP address is also associated with the security group of the ECS. A virtual IP address can be associated with up to 10 security groups.

Binding a Virtual IP Address to an EIP or ECS on the Console

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. Click the name with a hyperlink of the subnet that the virtual IP address belongs to.
The subnet details page is displayed.
6. On the **IP Addresses** tab, bind an EIP to the virtual IP address:
 - a. Locate the row that contains the virtual IP address and click **Bind to EIP** in the **Operation** column.

- The **Bind to EIP** dialog box is displayed.
- b. Select an EIP and click **OK**.
In the virtual IP address list, you can view that the virtual IP address has an EIP bound.
7. On the **IP Addresses** tab, bind an instance to the virtual IP address:
- a. Locate the row that contains the virtual IP address and click **Bind to Server** in the **Operation** column.
The **Bind to Server** dialog box is displayed.
 - b. Select an ECS and click **OK**.
In the virtual IP address list, you can view that the virtual IP address has an ECS bound.

NOTICE

- After a virtual IP address is bound to an ECS NIC, you need to manually configure the virtual IP address on the ECS. For details, see [Configuring a Virtual IP Address for an ECS](#).
- If an ECS has multiple NICs, bind the virtual IP address to the primary NIC.
- An ECS NIC can have multiple virtual IP addresses bound.

Configuring a Virtual IP Address for an ECS

Manually configure the virtual IP address bound to an ECS.

The following OSs are used as examples here. For other OSs, see the help documents on their official websites.

- Linux: CentOS 7.2 64bit and Ubuntu 22.04 server 64bit
- Windows: Windows Server

Linux (CentOS 7.2 64bit is used as an example.)

1. Obtain the NIC that the virtual IP address is to be bound and the connection of the NIC:

nmcli connection

Information similar to the following is displayed:

```
[root@ecs-paas-ops-1 ~]# nmcli connection
NAME                UUID                                  TYPE      DEVICE
Wired connection 1  5e72ec5a-6165-3bd6-a34b-ce43981acb27  ethernet  eth0
docker0             cd351a91-c5eb-4b69-83eb-df092a2ccf6b  bridge    docker0
```

The command output in this example is described as follows:

- **eth0** in the **DEVICE** column indicates the NIC that the virtual IP address is to be bound.
 - **Wired connection 1** in the **NAME** column indicates the connection of the NIC.
2. Add the virtual IP address for the connection:
nmcli connection modify "Connection name of the NIC" +ipv4.addresses Virtual IP address

Configure the parameters as follows:

- *Connection name of the NIC*: The connection name of the NIC obtained in **1**. In this example, the connection name is **Wired connection 1**.
- *Virtual IP address*: Enter the virtual IP address to be added. If you add multiple virtual IP addresses at a time, separate every two with a comma (,).

Example commands:

- Adding a single virtual IP address: **nmcli connection modify "Wired connection 1" +ipv4.addresses 172.16.0.125**
- Adding multiple virtual IP addresses: **nmcli connection modify "Wired connection 1" +ipv4.addresses 172.16.0.125,172.16.0.126**

3. Make the configuration in **2** take effect:

```
nmcli connection up "Connection name of the NIC"
```

In this example, run the following command:

```
nmcli connection up "Wired connection 1"
```

Information similar to the following is displayed:

```
[root@ecs ~]# nmcli connection up "Wired connection 1"
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/6)
```

4. Check whether the virtual IP address has been bound:

```
ip a
```

Information similar to the following is displayed. In the command output, the virtual IP address 172.16.0.125 is bound to NIC eth0.

```
[root@ecs ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether fa:16:3e:e5:d5:cd brd ff:ff:ff:ff:ff:ff
    inet 172.16.0.247/24 brd 172.16.0.255 scope global noprefixroute dynamic eth0
        valid_lft 86398sec preferred_lft 86398sec
    inet 172.16.0.125/32 brd 172.16.0.125 scope global noprefixroute eth0
        valid_lft forever preferred_lft forever
    inet6 2001:db8:a583:62c:7dd3:a13a:4031:d6fb/128 scope global tentative noprefixroute dynamic
        valid_lft 86400sec preferred_lft 86400sec
    inet6 fe80::5371:9bf9:b652:e35b/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

NOTE

To delete an added virtual IP address, perform the following steps:

1. Delete the virtual IP address from the connection of the NIC:

```
nmcli connection modify "Connection name of the NIC" -ipv4.addresses Virtual IP address
```

To delete multiple virtual IP addresses at a time, separate every two with a comma (,). Example commands are as follows:

- Deleting a single virtual IP address: **nmcli connection modify "Wired connection 1" -ipv4.addresses 172.16.0.125**
- Deleting multiple virtual IP addresses: **nmcli connection modify "Wired connection 1" -ipv4.addresses 172.16.0.125,172.16.0.126**

2. Make the deletion take effect by referring to **3**.

Linux (Ubuntu 22.04 server 64bit is used as an example.)

If an ECS runs Ubuntu 22 or Ubuntu 20, perform the following operations:

1. Obtain the NIC that the virtual IP address is to be bound:

ifconfig

Information similar to the following is displayed. In this example, the NIC bound to the virtual IP address is **eth0**.

```
root@ecs-X-ubuntu:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 172.16.0.210 netmask 255.255.255.0 broadcast 172.16.0.255
    inet6 fe80::f816:3eff:fe01:f1c3 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:01:f1:c3 txqueuelen 1000 (Ethernet)
    RX packets 43915 bytes 63606486 (63.6 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3364 bytes 455617 (455.6 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
...
```

2. Switch to the **/etc/netplan** directory:

```
cd /etc/netplan
```

3. Add a virtual IP address to the NIC.

- a. Open the configuration file **01-netcfg.yaml**:

```
vim 01-netcfg.yaml
```

- b. Press **i** to enter the editing mode.
- c. In the NIC configuration area, add a virtual IP address.

In this example, add a virtual IP address for **eth0**:

```
addresses:
```

```
- 172.16.0.26/32
```

The file content is as follows:

```
network:
  version: 2
  renderer: NetworkManager
  ethernets:
    eth0:
      dhcp4: true
      addresses:
        - 172.16.0.26/32
    eth1:
      dhcp4: true
    eth2:
      dhcp4: true
    eth3:
      dhcp4: true
    eth4:
      dhcp4: true
```

- d. Press **Esc**, enter **:wq!**, save the configuration, and exit.

4. Make the configuration in **3** take effect:

```
netplan apply
```

5. Check whether the virtual IP address has been bound:

ip a

Information similar to the following is displayed. In the command output, the virtual IP address 172.16.0.26 is bound to NIC eth0.

```
root@ecs-X-ubuntu:/etc/netplan# ip a
...
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default
qlen 1000
    link/ether fa:16:3e:01:f1:c3 brd ff:ff:ff:ff:ff:ff
    altname enp0s3
    altname ens3
inet 172.16.0.26/32 scope global noprefixroute eth0
    valid_lft forever preferred_lft forever
```

```
inet 172.16.0.210/24 brd 172.16.0.255 scope global dynamic noprefixroute eth0
valid_lft 107999971sec preferred_lft 107999971sec
inet6 fe80::f816:3eff:fe01:f1c3/64 scope link
valid_lft forever preferred_lft forever
```

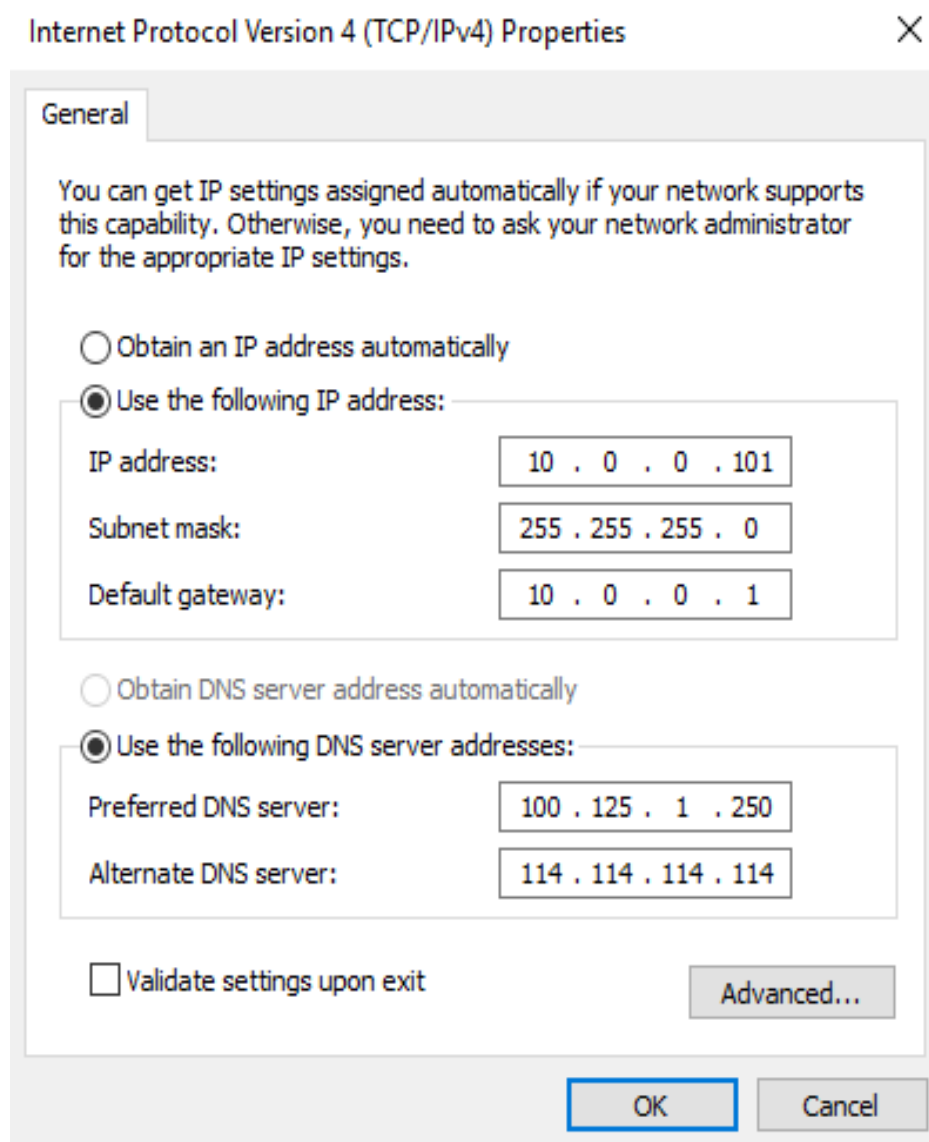
 **NOTE**

To delete an added virtual IP address, perform the following steps:

1. Open the configuration file **01-netcfg.yaml** and delete the virtual IP address of the corresponding NIC by referring to [3](#).
2. Make the deletion take effect by referring to [4](#).

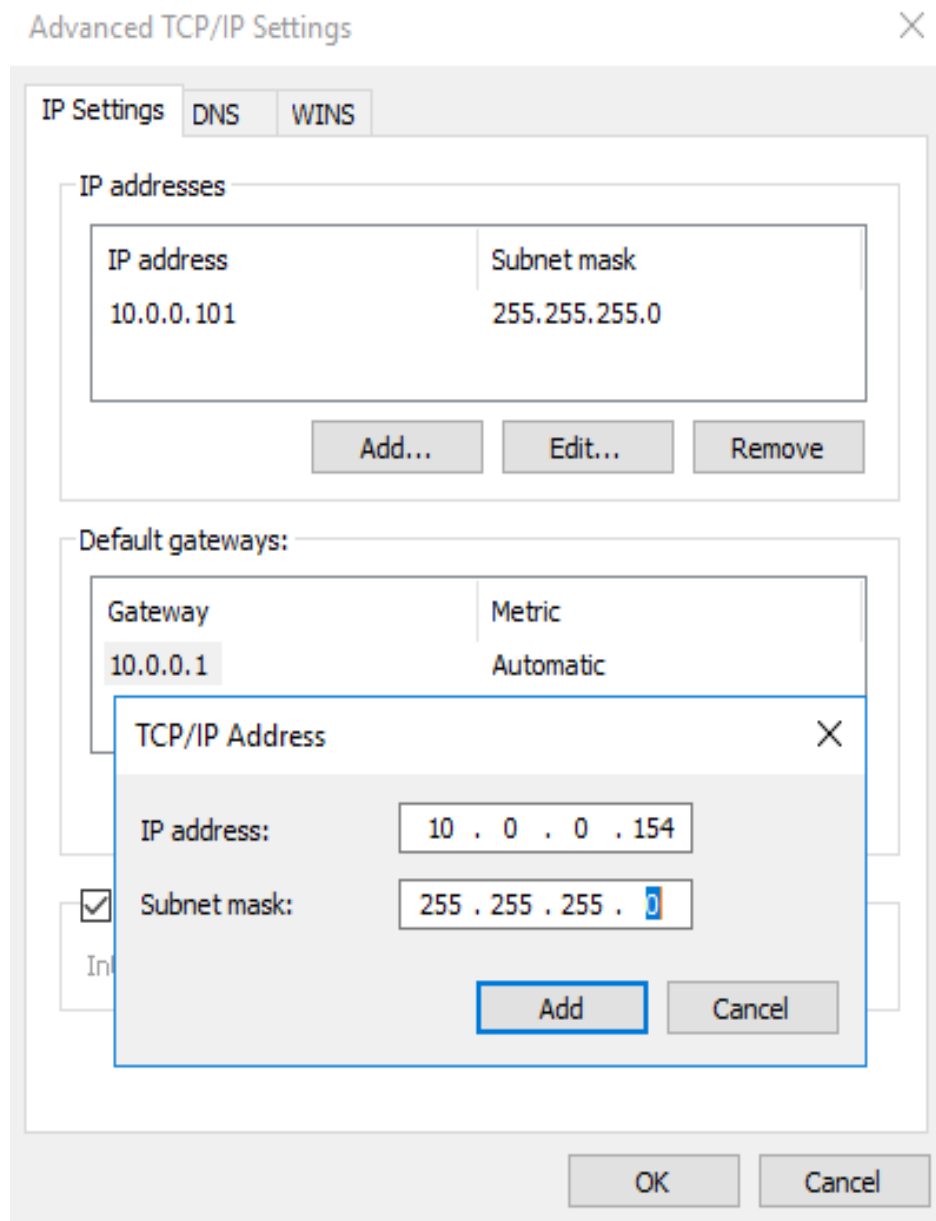
Windows OS (Windows Server is used as an example here.)

1. In **Control Panel**, click **Network and Sharing Center**, and click the corresponding local connection.
2. On the displayed page, click **Properties**.
3. On the **Network** tab page, select **Internet Protocol Version 4 (TCP/IPv4)**.
4. Click **Properties**.
5. Select **Use the following IP address** and set **IP address** to the private IP address of the ECS, for example, 10.0.0.101.

Figure 3-3 Configuring private IP address

6. Click **Advanced**.
7. On the **IP Settings** tab, click **Add** in the **IP addresses** area. Add the virtual IP address, for example, 10.0.0.154.

Figure 3-4 Configuring virtual IP address



8. Click **OK**.
9. In the **Start** menu, open the Windows command line window and run the following command to check whether the virtual IP address has been configured:

ipconfig /all

In the command output, **IPv4 Address** is the virtual IP address 10.0.0.154, indicating that the virtual IP address of the ECS NIC has been correctly configured.

Helpful Links

- [Why Can't the Virtual IP Address Be Pinged After It Is Bound to an ECS NIC?](#)

- [What Are the Differences Between EIP, Private IP Address, and Virtual IP Address?](#)
- [Unbinding a Virtual IP Address from an EIP](#)

3.4 Binding a Virtual IP Address to an EIP



Scenarios

This section describes how to bind a virtual IP address to an EIP.

Prerequisites

- You have configured the ECS networking based on [Networking](#) and ensure that the ECS has been bound with a virtual IP address.
- You have assigned an EIP.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
The EIP list page is displayed.
4. Locate the row that contains the EIP to be bound to the virtual IP address, and click **Bind** in the **Operation** column.
5. In the **Bind EIP** dialog box, set **Instance Type** to **Virtual IP address**.
6. In the virtual IP address list, select the virtual IP address to be bound and click **OK**.

3.5 Unbinding a Virtual IP Address from an Instance

Scenarios

This section describes how to unbind a virtual IP address from an ECS.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud** > **Subnets**.
The **Subnets** page is displayed.
5. Click the name of the subnet that the virtual IP address belongs to.
The **Summary** page is displayed.



6. Click the **IP Addresses** tab.
The virtual IP address list is displayed.
7. Locate the row that contains the virtual IP address, click **More** in the **Operation** column, and select **Unbind from Instance**.
The **Bound Instance** dialog box is displayed.
8. Unbind the virtual IP address from the instance.
 - a. Select the type of the instance bound to the virtual IP address.
 - b. Locate the row that contains the instance and click **Unbind** in the **Operation** column.
A confirmation dialog box is displayed.
 - c. Confirm the information and click **Yes**.

3.6 Unbinding a Virtual IP Address from an EIP

Scenarios

This section describes how to unbind a virtual IP address from an EIP.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
5. Click the name of the subnet that the virtual IP address belongs to.
The **Summary** page is displayed.
6. Click the **IP Addresses** tab.
The virtual IP address list is displayed.
7. Locate the row that contains the virtual IP address, click **More** in the **Operation** column, and select **Unbind from EIP**.
A confirmation dialog box is displayed.
8. Confirm the information and click **Yes**.

3.7 Releasing a Virtual IP Address

Scenarios

If you no longer need a virtual IP address or a reserved virtual IP address, you can release it to avoid wasting resources.

Notes and Constraints

If you want to release a virtual IP address that is being used by a resource, refer to [Table 3-1](#).

Table 3-1 Releasing a virtual IP address that is being used by a resource

Prompts	Cause Analysis and Solution
<p>Scenario 1: Virtual IP address cannot be released:</p> <p>This operation cannot be performed because the IP address is bound to an instance or an EIP. Unbind the IP address and try again.</p>	<p>This virtual IP address is being used by cloud resources such as an EIP or an ECS.</p> <p>Unbind the virtual IP address from the cloud resources first.</p> <ul style="list-style-type: none"> EIP: Unbinding a Virtual IP Address from an EIP ECS: Unbinding a Virtual IP Address from an Instance <p>Release the virtual IP address.</p>
<p>Scenario 2: Virtual IP address cannot be released:</p> <p>This operation cannot be performed because the IP address is being used by a system component.</p>	<p>The virtual IP address is being used by an instance. Delete the instance, which will also release the virtual IP address.</p> <p>Search for the instance based on the instance information displayed on the virtual IP address console and delete the instance.</p> <ul style="list-style-type: none"> RDS instance CCE instance API gateway

Figure 3-5 Scenario 1: Virtual IP address cannot be released

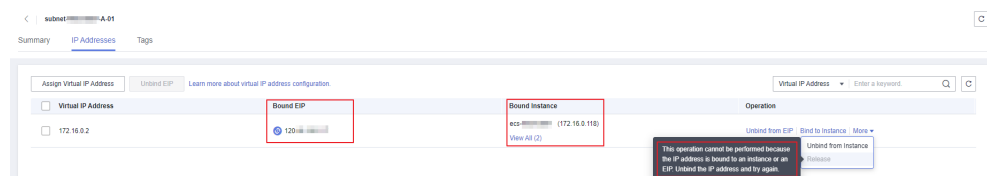
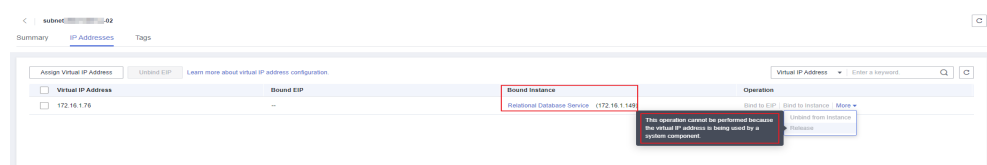




Figure 3-6 Scenario 2: Virtual IP address cannot be released



Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.

3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
5. Click the name of the subnet that the virtual IP address belongs to.
6. Click the **IP Addresses** tab, locate the row that contains the virtual IP address to be released, click **More** in the **Operation** column, and select **Release**.
A confirmation dialog box is displayed.
7. Confirm the information and click **Yes**.

3.8 Disabling IP Forwarding on the Standby ECS

Scenarios

If a virtual IP address is used in an active/standby scenario, disable IP forwarding on the standby ECS.

Linux

1. Log in to the ECS.
2. Run the following command to switch to user **root**:
su root
3. Check whether IP forwarding is enabled:
cat /proc/sys/net/ipv4/ip_forward
In the command output, **1** indicates it is enabled, and **0** indicates it is disabled. The default value is **0**.
 - If **1** is displayed, go to **4**.
 - If **0** is displayed, no further action is required.
4. Use either of the following methods to modify the configuration file:
 - Method 1: Use the vi editor to open the **/etc/sysctl.conf** file, change the value of **net.ipv4.ip_forward** to **0**, and enter **:wq** to save the change and exit.
 - Method 2: Use the **sed** command. An example command is as follows:
sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf
5. Make the modification take effect:
sysctl -p /etc/sysctl.conf

Windows

1. Log in to the ECS.
2. Open **Command Prompt** and run the following command:
ipconfig/all
In the command output, if the value of **IP Routing Enabled** is **No**, the IP forwarding function is disabled.



3. Press **Windows** and **R** keys together to open the **Run** box, and enter **regedit** to open the **Registry Editor**.
4. Set the value of **IPEnableRouter** under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters** to **0**.
 - If the value is set to **0**, IP forwarding will be disabled.
 - If the value is set to **1**, IP forwarding will be enabled.

3.9 Disabling Source/Destination Check for an ECS NIC

Scenarios

If a virtual IP address is used in an HA load balancing cluster, you need to disable source/destination check for ECS NICs.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click . In the service list, choose **Compute > Elastic Cloud Server**.
4. In the ECS list, click the ECS name.
5. On the displayed ECS details page, click the **NICs** tab.
6. Check that **Source/Destination Check** is disabled.

4 Elastic Network Interface and Supplementary Network Interface

4.1 Elastic Network Interface

4.1.1 Elastic Network Interface Overview

An elastic network interface (referred to as a network interface in this documentation) is a virtual network card. You can create and configure network interfaces and attach them to your instances (ECSs and BMSs) to obtain flexible and highly available network configurations.

Network Interface Types

- A primary network interface is created together with an instance by default, and cannot be detached from the instance.
- An extended network interface is created on the **Network Interfaces** console, and can be attached to or detached from an instance.

Application Scenarios

- Flexible migration
You can detach a network interface from an instance and then attach it to another instance. The network interface retains its private IP address, EIP, and security group rules. In this way, service traffic on the faulty instance can be quickly migrated to the standby instance, implementing quick service recovery.
- Traffic management
You can attach multiple network interfaces that belong to different subnets in a VPC to the same instance, and configure the network interfaces to carry the private network traffic, public network traffic, and management network traffic of the instance. You can configure access control policies and routing policies for each subnet, and configure security group rules for each network interface to isolate networks and service traffic.

4.1.2 Creating a Network Interface

Scenarios

A primary network interface is created together with an instance by default. You can perform the following operations to create extended network interfaces on the **Network Interfaces** console.

Notes and Constraints

An extended network interface created on the console can only be attached to an instance from the same VPC, but they can be associated with different security groups.

 **NOTE**

If you create an extended network interface using an API, the interface can be attached to an instance from a different VPC.

Procedure

1. Go to the [network interface list page](#).
2. Click **Create Network Interface**.
3. Configure parameters for the network interface, as shown in [Table 4-1](#).

Table 4-1 Parameter descriptions

Parameter	Parameter Description	Example Value
Name	(Mandatory) Specifies the network interface name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	networkInterface-891e
VPC	(Mandatory) Select the VPC to which the network interface belongs.	vpc-001
Subnet	(Mandatory) Select the subnet that the network interface belongs to.	subnet-001
Private IP Address	Select whether to automatically assign a private IP address.	-
Security Group	Select the security group that the network interface belongs to.	sg-001


4. Click **OK**.

4.1.3 Viewing Basic Information About a Network Interface

Scenarios

You can view basic information about your network interface on the management console, including the name, ID, type, VPC, attached instance, and associated security groups.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. On the **Network Interfaces** page, click the name of the target network interface.

Other Operations

On the network interface details page, you can also modify the following information:


- You can edit the network interface name, change IP addresses, and attach the network interface to or detach it from the instance.
- Instance-dependent Deletion
 - **Instance-dependent Deletion** is disabled by default. The network interface will not be deleted if it is detached from the instance or if the instance is deleted. You can attach the network interface to another instance.
 - If **Instance-dependent Deletion** has been enabled, the network interface will be deleted after it is detached from the instance.

4.1.4 Attaching a Network Interface to an Instance

Scenarios

You can attach a network interface to an ECS or a BMS to achieve flexible and high-availability network configurations.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.

4. In the network interface list, locate the row that contains the target network interface, click **Attach Instance** in the **Operation** column, and select the instance to be attached.
5. Click **OK**.

4.1.5 Binding a Network Interface to an EIP


Scenarios

You can bind an EIP to a network interface to achieve more flexible and scalable networks.

Each network interface has a private IP address. After the network interface is bound to an EIP, the network interface has both a private IP address and a public IP address. The binding between a network interface and an EIP will not change even after the network interface is detached from an instance. After a network interface is migrated from one instance to another, its private IP address and EIP will be migrated together at the same time.

An instance can have multiple network interfaces attached. If each network interface has an EIP bound, the instance will have multiple EIPs and can provide flexible access services.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. In the network interface list, locate the row that contains the target network interface, click **Bind EIP** in the **Operation** column, and select the EIP to be bound.
5. Click **OK**.

4.1.6 Binding a Network Interface to a Virtual IP Address


Scenarios

You can bind a network interface to a virtual IP address so that you can access the instance attached to the network interface using the virtual IP address.

Only a network interface with an instance attached can be bound to a virtual IP address.

For more information about virtual IP addresses, see [Virtual IP Address Overview](#).

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. In the network interface list, locate the row that contains the target network interface, and choose **More > Bind Virtual IP Address** in the **Operation** column.
The **IP Addresses** page will be displayed.
5. Locate the row that contains the target virtual IP address and click **Bind to Server** in the **Operation** column.
6. Select the server and NIC, and click **OK**.

4.1.7 Detaching a Network Interface from an Instance or Unbinding an EIP from a Network Interface

Scenarios

This section describes how to detach a network interface from an instance or unbind a network interface from an EIP.


Notes and Constraints

- If **Instance-dependent Deletion** is enabled for a network interface, the network interface will be deleted if it is detached from its instance.
 - Deleting a network interface will also delete any supplementary network interfaces and VLAN sub-interfaces attached to it.
 - Deleting a network interface will also unbind its EIP.
- If **Instance-dependent Deletion** is disabled for a network interface, the network interface will not be deleted if it is detached from its instance.
If a network interface has an EIP bound, detaching the network interface from its instance will also unbind the EIP from the network interface.

NOTE

After an EIP is unbound from a network interface, if you do not release the EIP, the EIP will continue to be billed, but you can still bind it to other cloud resources.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.

4. In the network interface list, locate the row that contains the target network interface, and click **Detach Instance** or **Unbind EIP** in the **Operation** column.
5. Click **Yes**.
If you no longer need an EIP, you can release the EIP after unbinding it.


4.1.8 Changing Security Groups That Are Associated with a Network Interface

Scenarios


You can change the security groups that are associated with a network interface on either the network interface list page or the network interface details page.

Procedure

Changing the security group associated with a network interface on the network interface list page

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. In the network interface list, locate the row that contains the target network interface, and choose **More > Change Security Group** in the **Operation** column.
5. On the **Change Security Group** page, select the security groups to be associated and click **OK**.

Changing the security group associated with a network interface on the network interface details page

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. Click the name of the target network interface.
5. Click the **Associated Security Groups** tab. Then, click **Change Security Group**.
6. On the **Change Security Group** page, select the security groups to be associated and click **OK**.

Other Operations

On the network interface details page, click the **Associated Security Groups** tab, and then click **Manage Rule**. For details about how to configure security group rules, see [Adding a Security Group Rule](#).

4.1.9 Deleting a Network Interface


Scenarios

This section describes how to delete a network interface.

Notes and Constraints

- A primary network interface is created together with an instance by default, and cannot be detached from the instance. If you want to delete a primary network interface, you need to delete its instance first, which will also delete the primary network interface.
- If you want to delete an extended network interface that is attached to an instance, [detach the interface from the instance](#) first.
- Deleting a network interface will also delete its supplementary network interfaces.
- Deleting a network interface will also unbind its EIP. You can choose to release the EIP if needed.
If you do not release the EIP, the EIP will continue to be billed, but you can still bind it to other cloud resources.
- If a network interface has resources associated, deleting the interface will also delete any rules for associated resources that reference it.
For example, if the next hop of a custom route in a VPC route table is a network interface, deleting the network interface will also delete the route.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. Locate the row that contains the network interface, click **More** in the **Operation** column, and click **Delete**.
A confirmation dialog box is displayed.
5. Confirm the information and click **OK**.

4.2 Supplementary Network Interfaces

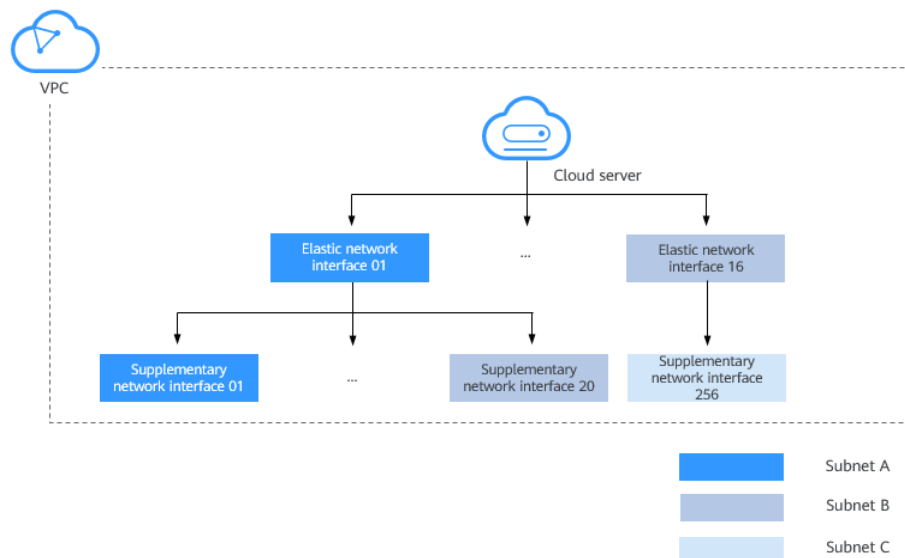
4.2.1 Supplementary Network Interface Overview

Supplementary network interfaces are a supplement to elastic network interfaces. If the number of elastic network interfaces that can be attached to your ECS cannot meet your requirements, you can use supplementary network interfaces, which can be attached to VLAN subinterfaces of elastic network interfaces.

Application Scenarios

Supplementary network interfaces are attached to VLAN subinterfaces of elastic network interfaces. [Figure 4-1](#) shows the networking diagram.

Figure 4-1 Supplementary network interface networking diagram



The number of elastic network interfaces that can be attached to each ECS is limited. If this limit cannot meet your requirements, you can attach supplementary network interfaces to elastic network interfaces.

- You can attach supplementary network interfaces that belong to different subnets in the same VPC to an ECS. Each supplementary network interface has its private IP address and EIP for private or Internet communication.
- You can security group rules for supplementary network interfaces for network isolation.

Notes and Constraints

- A maximum of 256 supplementary network interfaces can be attached to an ECS of certain flavors. The number of supplementary network interfaces that can be attached to an ECS varies by ECS flavor.
- An ECS cannot use Cloud-Init through the private IP addresses of its supplementary network interfaces.
- A supplementary network interface cannot have a virtual IP address bound.
- The flow logs of supplementary network interfaces cannot be collected separately. Their flow logs are generated together with their network interfaces.

4.2.2 Creating a Supplementary Network Interface

Scenarios

The number of elastic network interfaces that can be attached to each ECS is limited. If this limit cannot meet your requirements, you can use supplementary network interfaces.

Notes and Constraints

- Supplementary network interfaces and its elastic network interface must be in the same VPC but can belong to different subnets and security groups.
- Before using a supplementary network interface, you need to create a VLAN sub-interface on its ECS NIC and configure routes. For details, see [Configuring a Supplementary Network Interface](#).

Creating a Supplementary Network Interface

1. Go to the [supplementary network interface list page](#).
2. In the upper right corner of the page, click **Create Supplementary Network Interface**.
3. Configure the parameters based on [Table 4-2](#).

Table 4-2 Parameter descriptions

Parameter	Description	Example Value
Network Interface	Elastic network interface that the supplementary network interface to be attached to. Select an elastic network interface from the drop-down list.	--(172.16.0.145)
VPC	VPC that the supplementary network interface belongs to. You do not need to set this parameter.	vpc-A
Subnet	Select the subnet for the supplementary network interface.	subnet-A01
Description	(Optional) Enter the description of the supplementary network interface in the text box as required. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-
Quantity	Number of supplementary network interfaces to be created. The value ranges from 1 to 20.	1

Parameter	Description	Example Value
Private IP Address	Whether to assign a private IPv4 address to the supplementary network interface. This parameter cannot be deselected in the current version.	-
IPv4 Address	Select a virtual IP address assignment mode. <ul style="list-style-type: none">• Automatically assign IP address: The system assigns an IP address automatically.• Manually specify IP address: The system assigns an IP address that you specify. If you select Manually specify IP address, enter a private IPv4 address.	Automatically assign IP address
Security Group	Select the security group that the supplementary network interface belongs to.	sg-001

4. Click **OK**.

NOTICE

After a supplementary network interface is created, you need to create a VLAN sub-interface on the ECS NIC and configure routes. For details, see [Configuring a Supplementary Network Interface](#).

Configuring a Supplementary Network Interface

After a supplementary network interface is created, you need to create a VLAN sub-interface and configure a private IP address and default routes for the interface.

You need to obtain the information about the supplementary network interface, as shown in [Table 4-3](#).

Table 4-3 Supplementary network interface information

Information	How to Obtain	Description
VLAN	Management console	Obtain the value from the supplementary network interface list. For details, see Viewing Basic Information About a Supplementary Network Interface .
MAC address		
Private IP address		
Gateway		Obtain the value from the details page of the subnet that the supplementary network interface belongs to.

The following describes how to create a VLAN sub-interface on eth0 of an ECS (CentOS 8.2 is used as an example. For details about other OSs, see the OS documentation).

In this example:

- VLAN: 2110
- Private IP address: 192.168.0.2/24
- Gateway: 192.168.0.1
- MAC address: fa:16:3e:a1:b2:**

Procedure

1. Log in to the ECS.
2. Create a VLAN sub-interface for eth0.
ip link add link eth0 name eth0.2110 type vlan id 2110
3. Create a namespace **ns2110**.
ip netns add ns2110
4. Add the VLAN sub-interface **eth0.2110** to the namespace **ns2110**.
ip link set eth0.2110 netns ns2110
5. Change the MAC address of the VLAN sub-interface to **fa:16:3e:a1:b2:****.
ip netns exec ns2110 ifconfig eth0.2110 hw ether fa:16:3e:a1:b2:**
6. Enable the VLAN sub-interface.
ip netns exec ns2110 ifconfig eth0.2110 up
7. Configure the private IP address **192.168.0.2/24** for the VLAN sub-interface.
ip netns exec ns2110 ip addr add 192.168.0.2/24 dev eth0.2110
8. Configure the default route for the VLAN sub-interface. 192.168.0.1 is the gateway of the subnet that the supplementary network interface works.
ip netns exec ns2110 ip route add default via 192.168.0.1

Verification

1. Access other private IP addresses in the same VPC from the namespace to check whether the configuration on the supplementary network interface takes effect.

```
ip netns exec ns2110 ping a.b.c.d
```

Figure 4-2 Success example

```
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data:
64 bytes from 10.0.0.1: icmp_seq=1 ttl=63 time=0.275 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=63 time=0.351 ms
```

Figure 4-3 Failure example


```
--- 10.0.0.1 ping statistics ---
11 packets transmitted, 0 received, 100% packet loss, time 10004ms
```

4.2.3 Viewing Basic Information About a Supplementary Network Interface

Scenarios

You can view basic information about your supplementary network interface on the management console, including its ID, network interface, VLAN ID, VPC, subnet, private IP address, EIP, MAC address, and security groups.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. On the **Network Interfaces** page, click **Supplementary Network Interfaces** tab.
5. Click the private IP address of the supplementary network interface whose details you want to view.
 - On the **Summary** tab, you can view its ID, network interface, VLAN ID, VPC, subnet, private IP address, EIP, and MAC address.
 - On the **Associated Security Groups** tab, you can view its associated security groups and their rules.

Other Operations

On the supplementary network interface details page, you can also modify the following information:

- On the **Summary** tab, you can modify the description of the interface and change its bound EIP.

- On the **Associated Security Groups** tab, you can change the associated security groups of the interface. For details, see [Changing Security Groups That Are Associated with a Supplementary Network Interface](#).

4.2.4 Binding or Unbinding a Supplementary Network Interface to or from an EIP

Scenarios


You can bind a supplementary network interface to an EIP.

A supplementary network interface has a private IP address. You can also bind an EIP to the interface. The binding between a supplementary network interface and an EIP does not change when the network interface of the supplementary network interface is detached from an ECS and then attached to another ECS. The supplementary network interface still has its private IP address and EIP.


A network interface can have multiple supplementary network interfaces attached. If each supplementary network interface has an EIP, the ECS with the network interface attached can have multiple EIPs for flexible Internet access.

If you do not need an EIP or want to delete a supplementary network interface, you can unbind the EIP from the interface.

Binding a Supplementary Network Interface to an EIP

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. On the **Network Interfaces** page, click **Supplementary Network Interfaces** tab.
5. Locate the row that contains the supplementary network interface, click **Bind EIP** in the **Operation** column, and select the EIP to be bound.
6. Click **OK**.

Unbinding a Supplementary Network Interface from an EIP

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. On the **Network Interfaces** page, click **Supplementary Network Interfaces** tab.
5. Locate the row that contains the supplementary network interface and click **Unbind EIP** in the **Operation** column.

6. Click **Yes**.

4.2.5 Changing Security Groups That Are Associated with a Supplementary Network Interface

Scenarios


After a supplementary network interface is created, you can change its security group.

You can change the security group of a supplementary network interface:


- On the page of the supplementary network interface list.
- On the details page of a supplementary network interface.

Procedure

Changing the security group associated with a supplementary network interface on the supplementary network interface list page

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. On the **Network Interfaces** page, click the **Supplementary Network Interfaces** tab.
5. Locate the row that contains the supplementary network interface and click **Change Security Group** in the **Operation** column.
6. On the **Change Security Group** page, select the security group to be associated.
7. Click **OK**.

Changing the security group associated with a supplementary network interface on the supplementary network interface details page

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. On the **Network Interfaces** page, click the **Supplementary Network Interfaces** tab.
5. Click the private IP address of the supplementary network interface whose security group is to be changed.
6. Click the **Associated Security Groups** tab. Then, click **Change Security Group**.

7. On the **Change Security Group** page, select the security group to be associated.
8. Click **OK**.

4.2.6 Deleting a Supplementary Network Interface


Scenarios

If you want to delete a supplementary network interface with an EIP bound, you have to first unbind the EIP from the interface.

Notes and Constraints

- Deleting a supplementary network interface will also detach it from its network interface.
- Deleting a supplementary network interface will also unbind its EIP. You can choose to release the EIP if needed.
If you do not release the EIP, the EIP will continue to be billed, but you can still bind it to other cloud resources.
- If a supplementary network interface has resources associated, deleting the interface will also delete any rules for associated resources that reference it.
For example, if the next hop of a custom route in a VPC route table is a supplementary network interface, deleting the interface will also delete the route.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Network Interfaces**.
4. On the **Network Interfaces** page, click **Supplementary Network Interfaces** tab.
5. Locate the row that contains the supplementary network interface and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
6. Confirm the information and click **OK**.
Deleting a supplementary network interface will also delete the VLAN sub-interfaces configured on the ECS.

5 Access Control

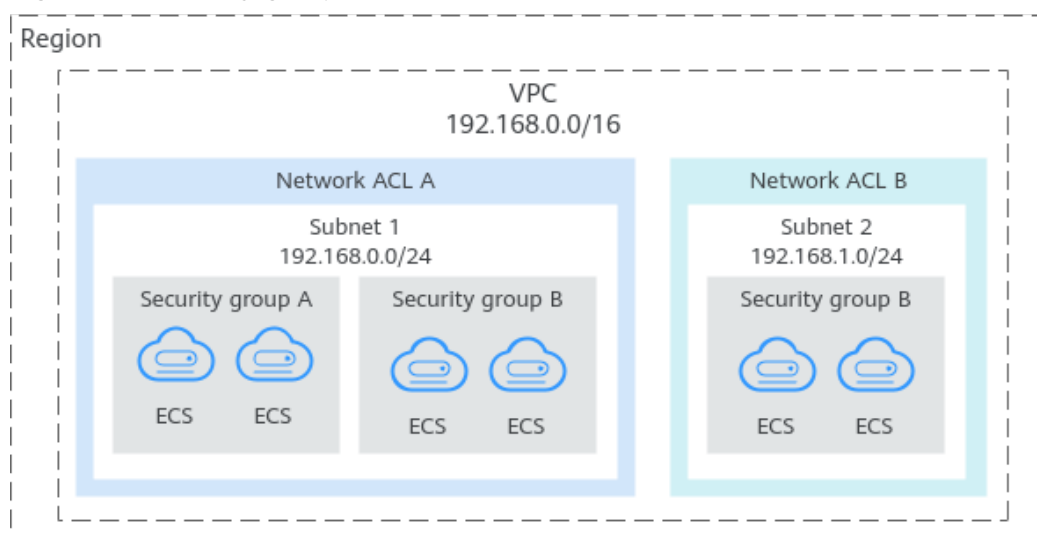
5.1 What Is Access Control?

A VPC is your private network on the cloud. You can configure security groups and network ACL rules to ensure the security of instances, such as ECSs, databases, and containers, running in a VPC.

- A security group protects the instances in it.
- A network ACL protects associated subnets and all the resources in the subnets.

Figure 5-1 shows how security groups and network ACLs are used. Security groups A and B protect the network security of ECSs. Network ACLs A and B add an additional layer of defense to subnets 1 and 2.

Figure 5-1 Security groups and network ACLs



Differences Between Security Groups and Network ACLs

Table 5-1 describes detailed differences between security groups and network ACLs.

Table 5-1 Differences between security groups and network ACLs

Item	Security Group	Network ACL
Protection Scope	Protects instances in a security group, such as ECSs, databases, and containers.	Protects subnets and all the instances in the subnets.
Mandatory	Mandatory. Instance must be added to at least one security group.	Optional. You can determine whether to associate a subnet with a network ACL based on service requirements.
Rules	Does not support Allow or Deny rules.	Supports both Allow and Deny rules.
Matching Order	<p>If an instance is associated with multiple security groups that have multiple rules:</p> <ol style="list-style-type: none">1. Rules are first matched based on the sequence each security group is associated with an instance. Security groups with lower sequence numbers have higher priorities.2. Rules are then matched by priority in that security group. Rules with lower values have higher priorities than those with higher values.3. Deny rules take precedence over allow rules if the rules have the same priority.	<p>A subnet can only have one network ACL. If there are multiple rules, the rules are processed based on their priorities. A smaller value indicates a higher priority.</p>

Item	Security Group	Network ACL
Usage	<ul style="list-style-type: none">• When creating an instance, for example, an ECS, you must select a security group. If no security group is selected, the ECS will be associated with the default security group.• After creating an instance, you can:<ul style="list-style-type: none">– Add or remove the instance to or from the security group on the security group console.– Associate or disassociate a security group with or from the instance on the instance console.	Selecting a network ACL is not allowed when you create a subnet. You must create a network ACL, add inbound and outbound rules, associate subnets with it, and enable network ACL. The network ACL then protects the associated subnets and instances in the subnets.
Packets	Packet filtering based on the 3-tuple (protocol, port, and source/destination) is supported.	Packet filtering based on the 5-tuple (protocol, source port, destination port, and source/destination) is supported.

5.2 Security Group

5.2.1 Security Groups and Security Group Rules

Security Groups

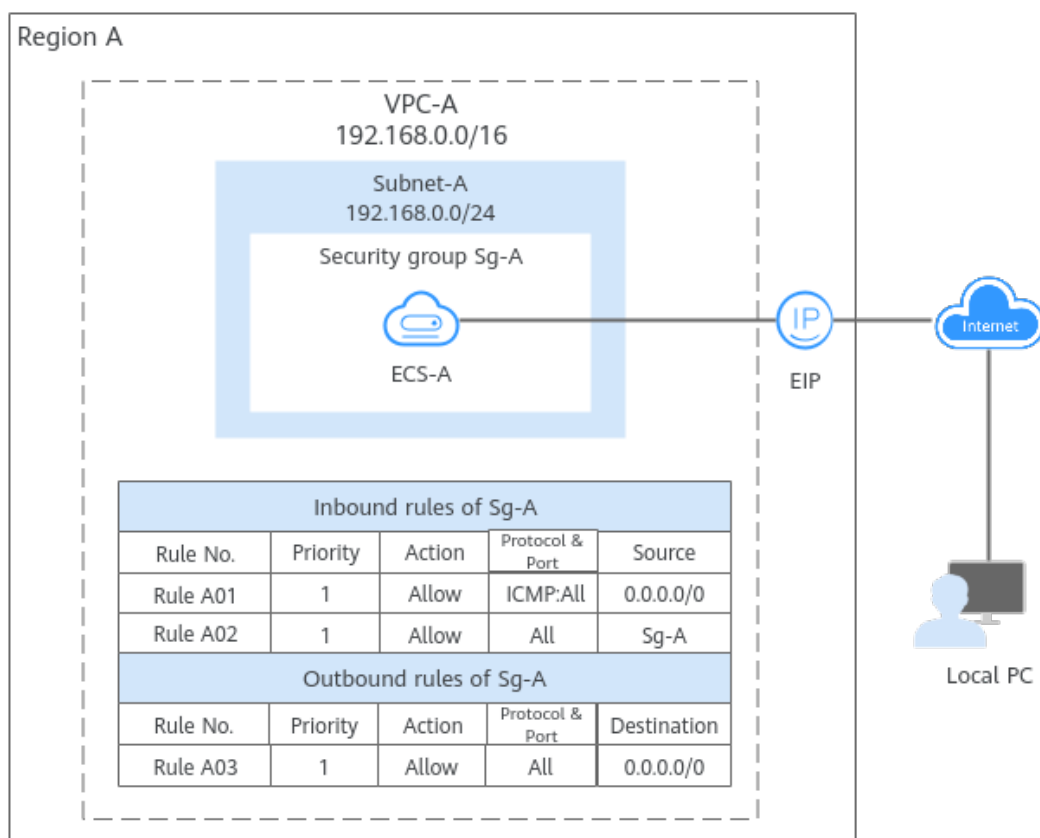
A security group is a collection of access control rules for cloud resources, such as cloud servers, containers, and databases, that have the same security protection requirements and that are mutually trusted. After a security group is created, you can configure access rules that will apply to all cloud resources added to this security group.

When creating an instance (for example, an ECS), you must associate it with a security group. If there are no security groups yet, a **default security group** will be automatically created and associated with the instance. You can also create a security group based on service requirements and associate it with the instance. A cloud resource can be associated with multiple security groups, and traffic to and from the cloud resource is matched by priority in a descending order.

Each security group can have both inbound and outbound rules. You need to specify the source, port, and protocol for each inbound rule and specify the destination, port, and protocol for each outbound rule to control the inbound and outbound traffic to and from the instances in the security group. As shown in [Figure 5-2](#), you have a VPC (**VPC-A**) with a subnet (**Subnet-A**) in region A. An ECS (**ECS-A**) is running in **Subnet-A** and associated with security group **Sg-A**.

- Security group **Sg-A** has a custom inbound rule to allow ICMP traffic to **ECS-A** from your PC over all ports. However, the security group does not contain rules that allow SSH traffic to **ECS-A** so you cannot remotely log in to **ECS-A** from your PC.
- If **ECS-A** needs to access the Internet through an EIP, the outbound rule of **Sg-A** must allow all traffic from **ECS-A** to the Internet.

Figure 5-2 Security group architecture



NOTE

You can use security groups free of charge.

Security Group Rules

- A security group has inbound and outbound rules to control traffic that's allowed to reach or leave the instances associated with the security group.
 - Inbound rules: control traffic to the instances in a security group.
 - Outbound rules: control traffic from the instances in a security group for accessing external networks.
- You can specify protocol, port, source or destination for a security group rule. The following describes key information about a security group.
 - **Action: Allow or Deny.** If the protocol, port, source or destination of the traffic matches a security group rule, traffic will be allowed or denied.
 - **Priority:** The value ranges from 1 to 100. A smaller value indicates a higher priority. Security group rules are matched by priority and then by

action. Deny rules take precedence over allow rules. For more information, see [How Traffic Matches Security Group Rules](#).

- **Type:** IPv4 or IPv6.
- **Protocol & Port:** network protocol type and port range.
 - Network protocol: The protocol can be TCP, UDP, ICMP, or GRE.
 - Port range: The value ranges from 1 to 65535.
- **Source or Destination:** source address of traffic in the inbound direction or destination address of traffic in the outbound direction.

How Security Groups Work

- Security groups are stateful. If you send a request from your instance and the outbound traffic is allowed, the response traffic for that request is allowed to flow in regardless of inbound security group rules. Similarly, if inbound traffic is allowed, responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.
- Security groups use connection tracking to track traffic to and from instances. If an inbound rule is modified, the modified rule immediately takes effect for the existing traffic. Changes to outbound security group rules do not affect existing persistent connections and take effect only for new connections.

If you add, modify, or delete a security group rule, or add or remove an instance to or from a security group, the inbound connections of all instances in the security group will be automatically cleared.

 - The existing inbound persistent connections will be disconnected. All the new connections will match the new rules.
 - The existing outbound persistent connections will not be disconnected, and the original rule will still be applied. All the new connections will match the new rules.

NOTICE

After a persistent connection is disconnected, new connections will not be established immediately until the timeout period of connection tracking expires. For example, after an ICMP persistent connection is disconnected, a new connection will be established and a new rule will be applied when the timeout period (30s) expires.

- The timeout period of connection tracking varies by protocol. The timeout period of a TCP connection in the established state is 600s, and that of an ICMP connection is 30s. For other protocols, if packets are received in both inbound and outbound directions, the connection tracking timeout period is 180s. If packets are received only in one direction, the connection tracking timeout period is 30s.
 - The timeout period of TCP connections varies by connection status. The timeout period of a TCP connection in the established state is 600s, and that of a TCP connection in the FIN-WAIT state is 30s.
-

- Security group rules are like a whitelist. If there are no rules that allow or deny some traffic, the security group denies all traffic to or from the instances in the security group.
 - Inbound rules: If the source of a request matches the source specified in a rule with **Action** set to **Allow**, the request is allowed. For this reason, you do not need to configure a deny rule in the inbound direction.

The rules in [Table 5-2](#) ensure that instances in a security group can communicate with each other. Do not delete or modify these rules.
 - Outbound rules: The rules in [Table 5-2](#) allow all traffic to leave the instances in the security group so that the instances can access any external IP address. If you delete these rules, the instances in the security group cannot access external networks.

Table 5-2 Security group rules

Direction	Action	Type	Protocol & Port	Source/Destination
Inbound	Allow	IPv4	All	Source: current security group
Inbound	Allow	IPv6	All	Source: current security group
Outbound	Allow	IPv4	All	Destination: 0.0.0.0/0
Outbound	Allow	IPv6	All	Destination: ::/0

How Traffic Matches Security Group Rules

An instance can have multiple security groups associated, and a security group can contain multiple security group rules. Security group rules are matched by priority and then by action. Deny rules take precedence over allow rules. The following takes inbound traffic as an example to match security group rules:

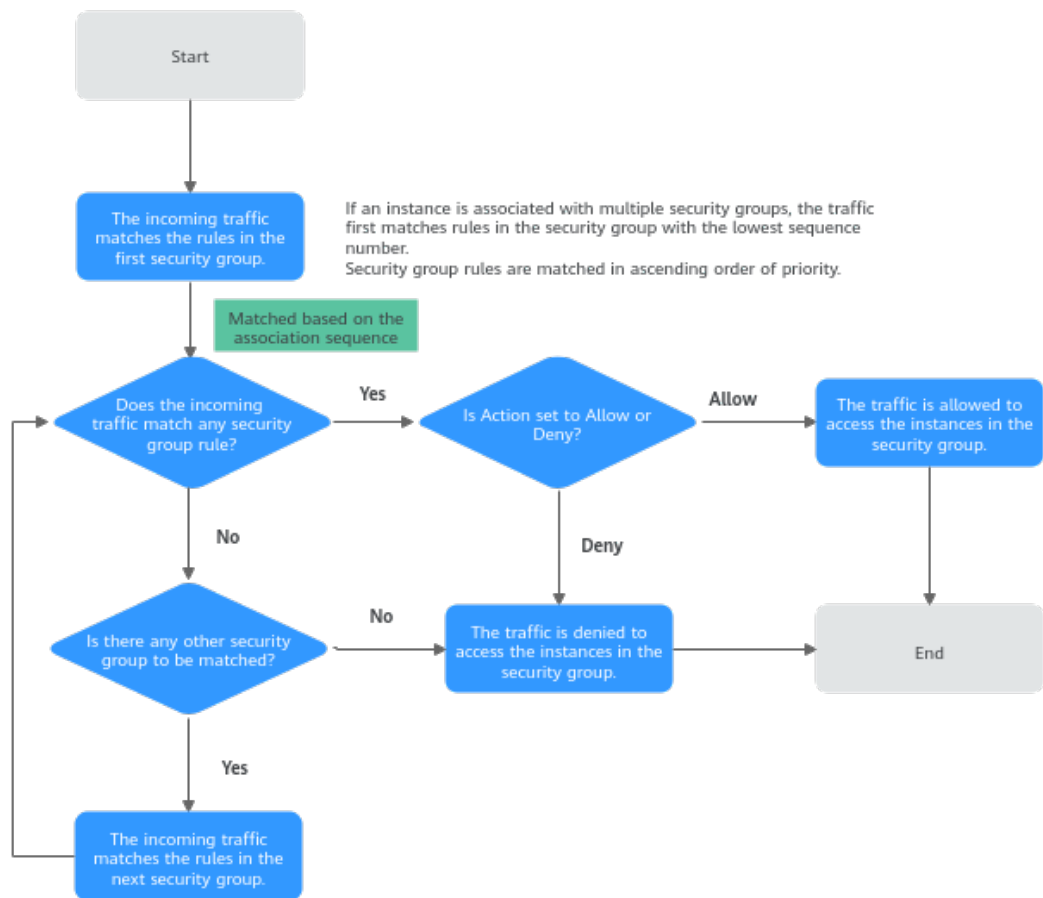
1. First, traffic is matched based on the sequence number of security groups. You can adjust the security group sequence. A smaller security group sequence number indicates a higher priority.

If the sequence number of security group A is 1 and that of security group B is 2, the priority of security group A is higher than that of security group B. Traffic preferentially matches the inbound rules of security group A.
2. Second, traffic is matched based on the priorities and actions of security group rules.
 - a. Security group rules are matched by priority first. A smaller value indicates a higher priority.

If the priority of security group rule A is 1 and that of security group rule B is 2, the priority of security group rule A is higher than that of security group rule B. Therefore, traffic preferentially matches security group rule A.
 - b. Deny rules take precedence over allow rules of the same priority.

3. Traffic matches all inbound rules of a security group based on the protocol, ports and source.
 - If the traffic matches a rule:
 - With **Action of Allow**, the traffic is allowed to access the instances in the security group.
 - With **Action of Deny**, the traffic is denied to access the instances in the security group.
 - If the traffic does not match any rule, the traffic is denied to access the instances in the security group.

Figure 5-3 Security group matching sequence



How Security Groups Are Used

You can allow given IP addresses to access instances in a security group, or allow access from another security group to enable instances in different security groups to communicate with each other. You can add security group rules to flexibly control the traffic in and out of a network to ensure network security. The following provides some security group configuration examples.

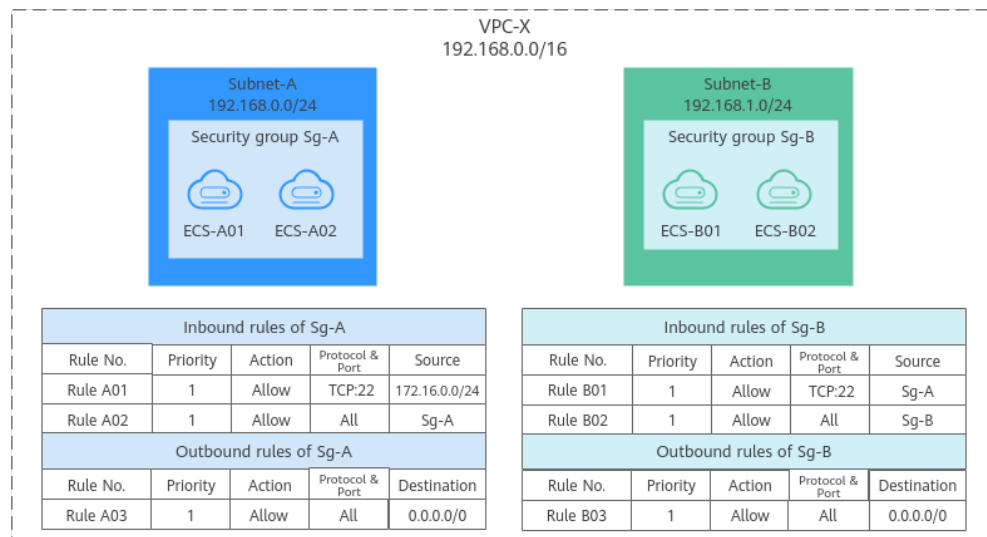
Allowing Traffic from Given IP Addresses or a Security Group

As shown in [Figure 5-4](#), there are two subnets (**Subnet-A** and **Subnet-B**) in **VPC-X**. ECSs in **Subnet-A** are associated with **Sg-A** because these ECSs are used to run

the same services and have the same network communication requirements. Similarly, ECSs in **Subnet-B** are associated with security group **Sg-B**.

- The inbound rule A01 of **Sg-A** allows traffic from IP addresses in **172.16.0.0/24** to access SSH port 22 of the ECSs in **Sg-A** for remotely logging in to these ECSs.
- The inbound rule A02 of **Sg-A** allows the ECSs in this security group to communicate with each other using any protocol and port.
- The inbound rule B01 of **Sg-B** allows the ECSs in **Sg-A** to access SSH port 22 of the ECSs in **Sg-B** for remotely logging in to the ECSs in **Subnet-B**.
- The inbound rule B02 of **Sg-B** allows the ECSs in this security group to communicate with each other using any protocol and port.
- The outbound rules of both security groups allow all traffic from the ECSs in the security groups.

Figure 5-4 Security group examples (allowing traffic from given IP addresses and security groups)



NOTE

[Security Group Configuration Examples](#) lists more security group rule configuration examples.

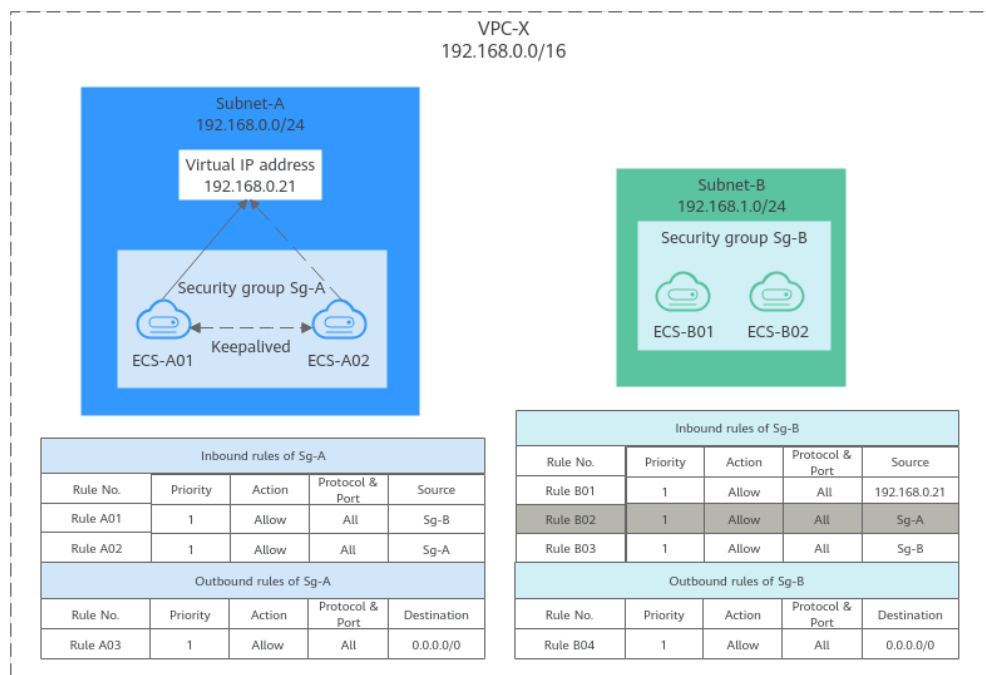
Allowing Traffic from a Virtual IP Address

As shown in [Figure 5-5](#), you use virtual IP address **192.168.0.21** to connect the ECSs in **Subnet-A** and **Subnet-B**. If you set the source of an inbound rule to the security group associated with the ECSs, the ECSs in the two security groups cannot communicate with each other, because they are connected by a virtual IP address.

In [Figure 5-5](#), **VPC-X** has two subnets: **Subnet-A** and **Subnet-B**. ECSs in **Subnet-A** are associated with security group **Sg-A**, and ECSs in **Subnet-B** are associated with security group **Sg-B**. **ECS-A01** and **ECS-A02** work in active/standby mode, forming a Keepalived HA cluster. The ECSs use virtual IP address **192.168.0.21** to communicate with external networks.

- Inbound rule A01 of **Sg-A** allows ECSs in **Sg-B** to access ECSs in **Sg-A** using any protocol over any port.
- **Sg-B** has the following inbound rules:
 - Rule B02: Allows ECSs in **Sg-A** to use private IP addresses to access ECSs in **Sg-B**. However, in this networking, ECSs in **Sg-A** are supposed to communicate with ECSs in **Sg-B** through virtual IP address **192.168.0.21**. However, rule B02 does not allow traffic from this virtual IP address.
 - Rule B01: Allows traffic from virtual IP address **192.168.0.21** to ECSs in **Sg-B** using any protocol over port. In this networking, you can also set the source to **192.168.0.0/24**, the CIDR block of **Subnet-A**.

Figure 5-5 Security group examples (allowing traffic from a virtual IP address)



Inbound rules of Sg-A				
Rule No.	Priority	Action	Protocol & Port	Source
Rule A01	1	Allow	All	Sg-B
Rule A02	1	Allow	All	Sg-A

Outbound rules of Sg-A				
Rule No.	Priority	Action	Protocol & Port	Destination
Rule A03	1	Allow	All	0.0.0.0/0

Inbound rules of Sg-B				
Rule No.	Priority	Action	Protocol & Port	Source
Rule B01	1	Allow	All	192.168.0.21
Rule B02	1	Allow	All	Sg-A
Rule B03	1	Allow	All	Sg-B

Outbound rules of Sg-B				
Rule No.	Priority	Action	Protocol & Port	Destination
Rule B04	1	Allow	All	0.0.0.0/0

NOTE

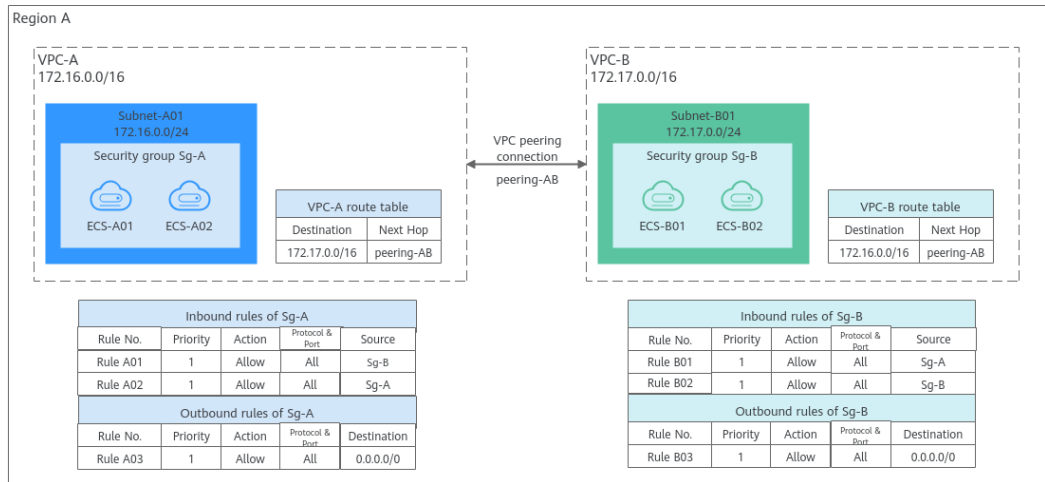
[Security Group Configuration Examples](#) lists more security group rule configuration examples.

Allowing Communications Between Instances in Two VPCs Connected by a VPC Peering Connection

In [Figure 5-6](#), VPC-A and VPC-B in region A are connected by VPC peering connection **peering-AB**. After routes are configured for the VPC peering connection, **Subnet-A** and **Subnet-B** can communicate with each other. However, the ECSs in the two subnets are associated with different security groups. To allow ECSs in **Sg-A** and **Sg-B** to communicate with each other, you can add the following rules:

- Rule A01 with **Source** to **Sg-B** to allow ECSs in **Sg-B** to access ECSs in **Sg-A**.
- Rule B01 with **Source** to **Sg-A** to allow ECSs in **Sg-A** to access ECSs in **Sg-B**.

Figure 5-6 Security group examples (allowing communications between ECSs in two VPCs connected by a VPC peering connection)



NOTE

[Security Group Configuration Examples](#) lists more security group rule configuration examples.

Security Group Configuration Process

Figure 5-7 Process of using a security group

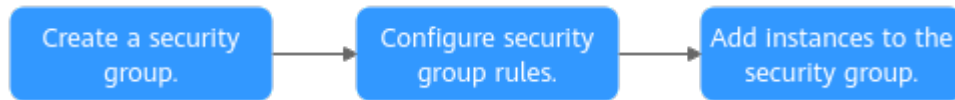


Table 5-3 Security group configuration process description

No.	Step	Description	Reference
1	Create a security group.	When creating a security group, you can select a template, such General-purpose web server or All ports open .	Creating a Security Group
2	Configure security group rules.	After a security group is created, if its rules cannot meet your service requirements, you can add new rules to the security group or modify original rules.	Adding a Security Group Rule Fast-Adding Security Group Rules

No.	Step	Description	Reference
3	Add instances to the security group.	When you create an instance, the system automatically adds the instance to a security group for protection. If one security group cannot meet your requirements, you can add an instance to multiple security groups.	Adding an Instance to or Removing an Instance from a Security Group

Security Group Constraints

- For better network performance, you are advised to associate an instance with no more than five security groups.
- A security group can have no more than 6,000 instances associated, or its performance will deteriorate.
- For inbound security group rules, the sum of the rules with **Source** set to **Security group**, the rules with **Source** set to **IP address group**, and the rules with inconsecutive ports, cannot exceed 128. Outbound rules also have this restriction.
 - When **Source** is set to **Security group**, you can select the current security group or a different security group.
 - An example of inconsecutive ports is 22,25,27.

Recommendations

- Instances in a security group deny all external access requests by default, but you can add rules to allow specific requests.
- When adding a security group rule, grant the minimum permissions possible. For example, if remote login to an ECS over port 22 is allowed, only allow specific IP addresses to log in to the ECS. Do not use 0.0.0.0/0 (all IP addresses).
- Keep your configurations simple. There should be a different reason for each security group. If you use the same security group for all your different instances, the rules in the security group will likely be redundant and complex. It will make it much harder to maintain and manage.
- You can add instances to different security groups based on their functions. For example, if you want to provide website services accessible from the Internet, you can add the web servers to a security group configured for that specific purpose and only allow external access over specific ports, such as 80 and 443. By default, other external access requests are denied. Do not run internal services, such as MySQL or Redis, on web servers that provide services accessible from the Internet. Deploy internal services on servers that do not need to connect to the Internet and associate these servers with security groups specifically configured for that purpose.
- If you have multiple IP addresses with the same security requirements, you can add them to an IP address group and select this IP address group when you configure a rule, to help you manage them in a more simple way. When

an IP address changes, you only need to change the IP address in the IP address group. Then, the rules in the IP address group change accordingly. You do not need to modify the rules in the security group one by one. This simplifies security group management and improves efficiency. For details, see [Using IP Address Groups to Reduce the Number of Security Group Rules](#).

- Do not directly modify security group rules for active services. Before you modify security group rules used by a service, you can clone the security group and modify the security group rules in the test environment to ensure that the modified rules work. For details, see [Cloning a Security Group](#).
- After you add instances to or modify rules of a security group, the security group rules are applied automatically. There is no need to restart the instances.

If a security group rule does not take effect after being configured, see [Why Are My Security Group Rules Not Applied?](#)

5.2.2 Default Security Group and Rules

If no security groups have been created yet, a default security group is automatically created for you, and the instance will be associated with it when you are creating the instance. Note the following when using the default security group:

- The name of the default security group is **default**. It is recommended that you do not change the name of the default security group in order to distinguish it from any security groups that you may create.
- You cannot delete the default security group, but you can modify its rules or add rules to it.
- The default security group denies all external requests. To allow access to an instance associated with this security group, you can add rules to allow access over given ports by referring to [Remotely Logging In to an ECS from a Local Server](#).
- If your service has different security requirements on instances for different purposes, you can create security groups and associate these instances with different security groups based on their purposes.

NOTE

Security groups are free of charge.

Default Security Group Rules

Note the following when using default security group rules:

- Inbound rules control incoming traffic to instances in the default security group. The instances can only communicate with each other but cannot be accessed from external networks.
- Outbound rules allow all traffic from the instances in the default security group to external networks.

Figure 5-8 Default security group

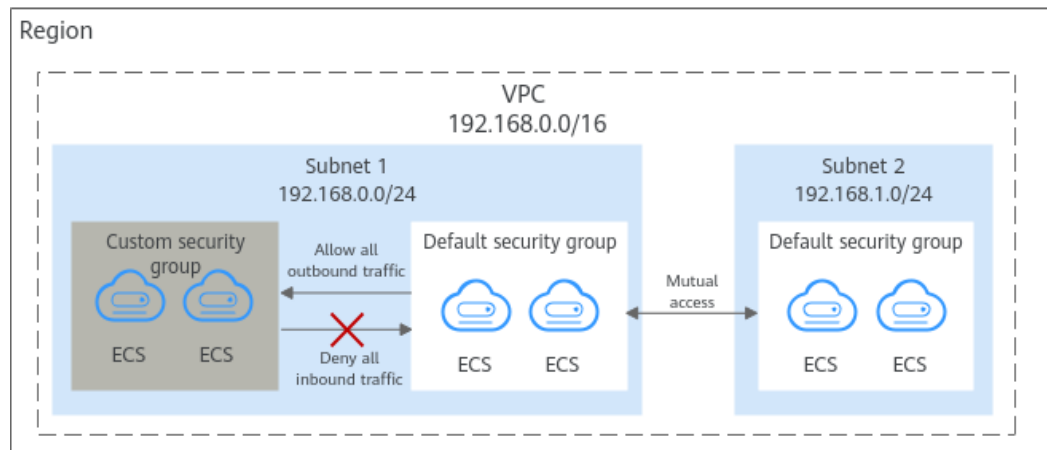


Table 5-4 describes the default rules for the default security group.

Table 5-4 Rules in the default security group

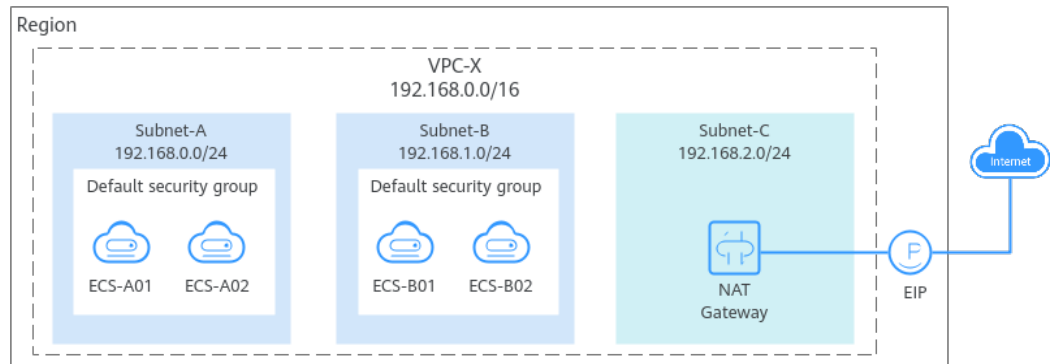
Direction	Action	Type	Protocol & Port	Source/Destination	Description
Inbound	Allow	IPv4	All	Source: default security group (default)	This rule allows IPv4 instances in the security group to communicate with each other using any protocol over any port.
Inbound	Allow	IPv6	All	Source: Default security group (default)	This rule allows IPv6 instances in the security group to communicate with each other using any protocol over any port.
Outbound	Allow	IPv4	All	Destination: 0.0.0.0/0	This rule allows all traffic from the instances in the security group to any IPv4 address over any port.
Outbound	Allow	IPv6	All	Destination: :/0	This rule allows all traffic from the instances in the security group to any IPv6 address over any port.

A Default Security Group Example

As shown in **Figure 5-9**, VPC-X has three subnets: **Subnet-A**, **Subnet-B**, and **Subnet-C**. ECSs in **Subnet-A** and **Subnet-B** have been associated with the default security group. The default security group allows the instances in the security group to communicate with each other and denies all external requests. So, the four ECSs (**ECS-A01**, **ECS-A02**, **ECS-B01**, and **ECS-B02**) can communicate with each other, but they cannot receive traffic from the NAT gateway.

To allow traffic from the NAT gateway, you need to add rules to the default security group or create a security group and associate it with the instances.

Figure 5-9 Use cases



5.2.3 Security Group Configuration Examples

When you create instances, such as cloud servers, containers, and databases, in a VPC subnet, you can use the default security group or create a security group. You can add inbound and outbound rules to the default or your security group to control traffic from and to the instances in the security group. Here are some common security group configuration examples:

- [Remotely Logging In to an ECS from a Local Server](#)
- [Remotely Connecting to an ECS from a Local Server to Upload or Download FTP Files](#)
- [Setting Up a Website on an ECS to Provide Services Externally](#)
- [Using ping Command to Verify Network Connectivity](#)
- [Enabling Communications Between Instances in Different Security Groups](#)
- [Allowing External Instances to Access the Database Deployed on an ECS](#)
- [Allowing ECSs to Access Specific External Websites](#)

NOTICE

If your security group rules are not applied, [submit a service ticket](#).

Precautions

Note the following before configuring security group rules:

- Instances associated with different security groups are isolated from each other by default.
- Generally, a security group denies all external requests by default. You need to add inbound rules to allow specific traffic to the instances in the security group.
- By default, outbound security group rules allow all requests from the instances in the security group to access external resources.

If outbound rules are deleted, the instances in the security group cannot communicate with external resources. To allow outbound traffic, you need to add outbound rules by referring to [Table 5-5](#).

Table 5-5 Default outbound rules in a security group

Direction	Priority	Action	Type	Protocol & Port	Destination	Description
Outbound	1	Allow	IPv4	All	0.0.0.0/0	This rule allows the instances in the security group to access any IPv4 address over any port.
Outbound	1	Allow	IPv6	All	::/0	This rule allows the instances in the security group to access any IPv6 address over any port.

Remotely Logging In to an ECS from a Local Server

A security group denies all external requests by default. To remotely log in to an ECS in a security group from a local server, add an inbound rule based on the OS running on the ECS.

- To remotely log in to a Linux ECS using SSH, enable port 22. For details, see [Table 5-6](#).
- To remotely log in to a Windows ECS using RDP, enable port 3389. For details, see [Table 5-7](#).

Table 5-6 Remotely logging in to a Linux ECS using SSH

Direction	Priority	Action	Type	Protocol & Port	Source
Inbound	1	Allow	IPv4	TCP: 22	IP address: 0.0.0.0/0

Table 5-7 Remotely logging in to a Windows ECS using RDP

Direction	Priority	Action	Type	Protocol & Port	Source
Inbound	1	Allow	IPv4	TCP: 3389	IP address: 0.0.0.0/0

NOTICE

If the source is set to 0.0.0.0/0, any IP address can be used to remotely log in to the ECS. To ensure security, set the source to a specific IP address based on service requirements. For details about the configuration example, see [Table 5-8](#).

Table 5-8 Remotely logging in to an ECS using a specified IP address

ECS Type	Direction	Priority	Action	Type	Protocol & Port	Source
Linux ECS	Inbound	1	Allow	IPv4	TCP: 22	IP address: 192.168.0.0/24
Windows ECS	Inbound	1	Allow	IPv4	TCP: 3389	IP address: 10.10.0.0/24

Remotely Connecting to an ECS from a Local Server to Upload or Download FTP Files

By default, a security group denies all external requests. If you need to remotely connect to an ECS from a local server to upload or download files, you need to enable FTP ports 20 and 21.

Table 5-9 Remotely connecting to an ECS from a local server to upload or download files

Direction	Priority	Action	Type	Protocol & Port	Source
Inbound	1	Allow	IPv4	TCP: 20-21	IP address: 0.0.0.0/0

NOTICE

You must first install the FTP server program on the ECSs and check whether ports 20 and 21 are working properly.

Setting Up a Website on an ECS to Provide Services Externally

A security group denies all external requests by default. If you have set up a website on an ECS that can be accessed externally, you need to add an inbound rule to the ECS security group to allow access over specific ports, such as HTTP (80) and HTTPS (443).

Table 5-10 Setting up a website on an ECS to provide services externally

Direction	Priority	Action	Type	Protocol & Port	Source
Inbound	1	Allow	IPv4	TCP: 80	IP address: 0.0.0.0/0
Inbound	1	Allow	IPv4	TCP: 443	IP address: 0.0.0.0/0

Using ping Command to Verify Network Connectivity

Ping works by sending an Internet Control Message Protocol (ICMP) Echo Request. To ping an ECS from your PC to verify the network connectivity, you need to add an inbound rule to the security group of the ECS to allow ICMP traffic.

Table 5-11 Using ping command to verify network connectivity

Direction	Priority	Action	Type	Protocol & Port	Source
Inbound	1	Allow	IPv4	ICMP: All	IP address: 0.0.0.0/0
Inbound	1	Allow	IPv6	ICMP: All	IP address: ::/0

Enabling Communications Between Instances in Different Security Groups

Instances in the same VPC but associated with different security groups cannot communicate with each other. If you want ECSs in security group **sg-A** to access MySQL databases in security group **sg-B**, you need to add an inbound rule to security group **sg-B** to allow access from ECSs in security group **sg-A**.

Table 5-12 Enabling communications between instances in different security groups

Direction	Priority	Action	Type	Protocol & Port	Source
Inbound	1	Allow	IPv4	TCP: 3306	Security group: sg-A

NOTICE

As shown in [How Security Groups Are Used](#), if you want to use virtual IP address **192.168.0.21** to connect the ECSs in **Subnet-A** and **Subnet-B**, you need to set the source of an inbound rule to virtual IP address **192.168.0.21**.

Allowing External Instances to Access the Database Deployed on an ECS

A security group denies all external requests by default. If you have deployed a database on an ECS and want the database to be accessed from external instances

on a private network, you need to add an inbound rule to the security group of the ECS to allow access over corresponding ports. Here are some common ports for databases:

- MySQL: port 3306
- Oracle: port 1521
- MS SQL: port 1433
- PostgreSQL: port 5432
- Redis: port 6379

Table 5-13 Allowing external instances to access the database deployed on an ECS

Direction	Priority	Action	Type	Protocol & Port	Source	Description
Inbound	1	Allow	IPv4	TCP: 3306	Security group: sg-A	This rule allows the ECSs in security group sg-A to access the MySQL database service.
Inbound	1	Allow	IPv4	TCP: 1521	Security group: sg-B	This rule allows the ECSs in security group sg-B to access the Oracle database service.
Inbound	1	Allow	IPv4	TCP: 1433	IP address: 172.16.3.21/32	This rule allows the ECS whose private IP address is 172.16.3.21 to access the MS SQL database service.
Inbound	1	Allow	IPv4	TCP: 5432	IP address: 192.168.0.0/24	This rule allows ECSs whose private IP addresses are in the 192.168.0.0/24 network to access the PostgreSQL database service.
Inbound	1	Allow	IPv4	TCP: 6379	IP address group: ipGroup-A	This rule allows ECSs whose private IP addresses are in IP address group ipGroup-A to access the Redis database service.

NOTICE

In this example, the source is for reference only. Set the source address based on your requirements.

Allowing ECSs to Access Specific External Websites

By default, a security group allows all outbound traffic. [Table 5-15](#) lists the default rules. If you want to allow ECSs to access specific websites, configure the security group as follows:

1. Add outbound rules to allow traffic over specific ports to specific IP addresses.

Table 5-14 Allowing ECSs to access specific external websites

Direction	Priority	Action	Type	Protocol & Port	Destination	Description
Outbound	1	Allow	IPv4	TCP: 80	IP address: 132.15.XX.XX	This rule allows ECSs in the security group to access the external website at http://132.15.XX.XX:80.
Outbound	1	Allow	IPv4	TCP: 443	IP address: 145.117.XX.XX	This rule allows ECSs in the security group to access the external website at https://145.117.XX.XX:443.

2. Delete the original outbound rules that allow all traffic.

Table 5-15 Default outbound rules in a security group

Direction	Priority	Action	Type	Protocol & Port	Destination	Description
Outbound	1	Allow	IPv4	All	0.0.0.0/0	This rule allows the instances in the security group to access any IPv4 address over any port.
Outbound	1	Allow	IPv6	All	::/0	This rule allows the instances in the security group to access any IPv6 address over any port.

5.2.4 Common Ports Used by ECSs

When adding a security group rule, you must specify a port or port range for communications. Traffic is then allowed or denied if traffic matches this rule.

Suppose a client requests to remotely log in to an ECS using SSH. When the request reaches the security group, the IP address and port of the client will be checked. If the IP address and the port match the allow rules in the security group, the request is allowed.

Table 5-16 lists some high-risk ports that are blocked by default. Even if you have added a security group rule to allow access over these ports, traffic over these ports in restricted regions is still denied. In this case, do not use these high-risk ports for your services.

Table 5-16 High-risk ports

Protocol	Port
TCP	42, 135, 137, 138, 139, 444, 445, 593, 1025, 1068, 1433, 1434, 3127, 3128, 3129, 3130, 4444, 4789, 5554, 5800, 5900, 8998, 9995, and 9996
UDP	135~139 1026 1027 1028 1068 1433 1434 4789 5554 9995 9996

Common Ports

Table 5-17 lists the common ports used by ECSs. You can configure security group rules to allow traffic to and from specified ECS ports. For details, see [Adding a Security Group Rule](#). For more information about requirements for Windows, see [Service overview and network port requirements for Windows](#).

Table 5-17 Common ports used by ECSs

Port	Protocol	Description
21	FTP	Used by FTP services for uploading and downloading files. For configuration examples, see Remotely Connecting to an ECS from a Local Server to Upload or Download FTP Files .
22	SSH	Used to remotely connect to Linux ECSs. For configuration examples, see Remotely Logging In to an ECS from a Local Server .
23	Telnet	Used to remotely log in to ECSs.
25	SMTP	Used to send emails. For security purposes, TCP port 25 is disabled in the outbound direction by default. For details about how to open the port, see Why Is Outbound Access Through TCP Port 25 Restricted?
80	HTTP	Used to access websites over HTTP. For configuration examples, see Setting Up a Website on an ECS to Provide Services Externally .

Port	Protocol	Description
110	POP3	Used to receive emails using Post Office Protocol version 3 (POP3).
143	IMAP	Used to receive emails using Internet Message Access Protocol (IMAP).
443	HTTPS	Used to access websites over HTTPS. For configuration examples, see Setting Up a Website on an ECS to Provide Services Externally .
1433	SQL Server	A TCP port of the SQL Server for providing services. For configuration examples, see Allowing External Instances to Access the Database Deployed on an ECS .
1434	SQL Server	A UDP port of the SQL Server for returning the TCP/IP port number used by the SQL Server. For configuration examples, see Allowing External Instances to Access the Database Deployed on an ECS .
1521	Oracle	Used for Oracle database communications. This port must be enabled on the ECSs where Oracle SQL Server is deployed. For configuration examples, see Allowing External Instances to Access the Database Deployed on an ECS .
3306	MySQL	Used by MySQL databases to provide services. For configuration examples, see Allowing External Instances to Access the Database Deployed on an ECS .
3389	Windows Server Remote Desktop Services	Used to connect to Windows ECSs. For configuration examples, see Remotely Logging In to an ECS from a Local Server . For details about how to log in to a Windows ECS, see .
8080	Proxy	Used by the WWW proxy service for web browsing, like port 80. If you use port 8080, you need to add :8080 after the IP address when you visit a website or use a proxy server. If Apache Tomcat is installed, its default service port is 8080.
137, 138, and 139	NetBIOS	Used for Windows files, printer sharing, and Samba. <ul style="list-style-type: none">• Ports 137 and 138: UDP ports that are used when files are transferred using Network Neighborhood (My Network Places).• Port 139: Connections from this port try to access the NetBIOS/SMB service.

5.2.5 Managing a Security Group

5.2.5.1 Creating a Security Group

Scenarios

A security group consists of inbound and outbound rules. You can add security group rules to allow or deny the traffic to reach and leave the instances (such as ECSs) in the security group.

When creating an instance (for example, an ECS), you must associate it with a security group. If no security group has been created yet, a **default security group** will be created and associated with the instance. You can also create a security group and add inbound and outbound rules to allow specific traffic. For more information about security groups and rules, see [Security Groups and Security Group Rules](#).

Procedure

1. Go to the [security group list page](#).
2. In the upper right corner, click **Create Security Group**.
The **Create Security Group** page is displayed.
3. Configure the parameters as prompted.

Table 5-18 Parameter description

Parameter	Description	Example Value
Name	<p>Mandatory</p> <p>Enter the security group name.</p> <p>The security group name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.</p> <p>NOTE</p> <p>You can change the security group name after a security group is created. It is recommended that you give each security group a different name.</p>	sg-AB
Enterprise Project	<p>Mandatory</p> <p>When creating a security group, you can add the security group to an enabled enterprise project.</p> <p>An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default.</p> <p>For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i>.</p>	default

Parameter	Description	Example Value
Template	<p>Mandatory</p> <p>A template comes with default security group rules, helping you quickly create security groups. The following templates are provided:</p> <ul style="list-style-type: none">• Custom: This template allows you to create security groups with custom security group rules.• General-purpose web server (default value): The security group that you create using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389.• All ports open: The security group that you create using this template includes default rules that allow inbound traffic on any port. Note that allowing inbound traffic on any port poses security risks.	General-purpose web server
Description	<p>Optional</p> <p>Supplementary information about the security group.</p> <p>The security group description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	N/A

4. Confirm the inbound and outbound rules of the template and click **OK**.

Related Operations

- After a security group is created, if its rules cannot meet your service requirements, you can add new rules to the security group or modify original rules. For details, see [Adding a Security Group Rule](#).
- Each ECS must be associated with at least one security group. You can add an ECS to multiple security groups based on service requirements. For details, see [Adding an Instance to or Removing an Instance from a Security Group](#).

5.2.5.2 Cloning a Security Group

Scenarios

You can clone a security group from the same or a different region to another to quickly apply the security group rules to ECSs in that region.



You can clone a security group in the following scenarios:

- For example, you have security group **sg-A** in region A. If ECSs in region B require the same security group rules as those configured for security group **sg-A**, you can clone security group **sg-A** to region B, freeing you from creating a new security group in region B.
- If you need new security group rules, you can clone the original security group as a backup.
- Before you modify security group rules used by a service, you can clone the security group and modify the security group rules in the test environment to ensure that the modified rules work.

Notes and Constraints

- You can clone a security group from the same or a different region.
 - If you want to clone a security group from the same region, you can clone all rules in the security group.
 - If you want to clone a security group from a different region, the system will clone only rules whose source and destination are IP addresses and rules whose source and destination is the current security group.
- Only security group rules are cloned, but not the instances associated with the security group.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
5. Locate the row that contains the security group, click **More** in the **Operation** column, and click **Clone**.
6. Select the region and name of the new security group as prompted.
7. Click **OK**.
You can then switch to the required region to view the cloned security group in the security group list.


5.2.5.3 Modifying a Security Group

Scenarios

After a security group is created, you can change its name and description.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.

3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
5. Locate the row that contains the security group, click **More** in the **Operation** column, and click **Modify**.
The **Modify Security Group** dialog box is displayed.
6. Modify the name and description of the security group as required.
7. Click **OK** to save the modification.

5.2.5.4 Deleting a Security Group

Scenarios

If your security group is no longer required, you can delete it.

NOTE

Both default and custom security groups are free.

Notes and Constraints

- The default security group is named **default** and cannot be deleted.

Figure 5-10 Default security group





- If you want to delete a security group that is associated with instances, such as cloud servers, containers, and databases, you need to remove the instances from the security group first. For details, see [Adding an Instance to or Removing an Instance from a Security Group](#).
- A security group cannot be deleted if it is used as the source or destination of a rule in another security group.

Delete or **modify** the rule and delete the security group again.

For example, if the source of a rule in security group **sg-B** is set to **sg-A**, you need to delete or modify the rule in **sg-B** before deleting **sg-A**.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

- The **Virtual Private Cloud** page is displayed.
- In the navigation pane on the left, choose **Access Control > Security Groups**. The security group list is displayed.
 - Locate the row that contains the target security group, click **More** in the **Operation** column, and click **Delete**. A confirmation dialog box is displayed.
 - Confirm the information and click **Yes**.

5.2.6 Managing Security Group Rules

5.2.6.1 Adding a Security Group Rule

Scenarios

A security group consists of inbound and outbound rules. You can add security group rules to allow or deny the traffic to reach and leave the instances (such as ECSs) in the security group.

Security group rules allow or deny network traffic from specific sources over specific protocols or specific ports.

Precautions

- Before configuring security group rules, you need to plan access policies for instances in the security group. For details about common security group rules, see [Security Group Configuration Examples](#).
- Add as fewer rules as possible. [Security Group Constraints](#) lists the constraints on the number of rules in a security group.
- After allowing traffic over a port in a security group rule, ensure that the port used by the instance is opened. For details, see [Verifying Security Group Rules](#).
- By default, instances in the same security group can communicate with each other. If instances in the same security group cannot communicate with each other, possible causes are as follows:
 - The inbound rules for communications between these instances are deleted. [Table 5-19](#) shows the inbound rules.



Table 5-19 Inbound rules for communication between instances

Direction	Priority	Action	Type	Protocol & Port	Source/Destination
Inbound	1	Allow	IPv4	All	Source: current security group (Sg-A)
Inbound	1	Allow	IPv6	All	Source: current security group (Sg-A)

- Different VPCs cannot communicate with each other. The instances belong to the same security group but different VPCs.

You can use [VPC peering connections](#) to connect VPCs in different regions.

Adding Rules to a Security Group

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

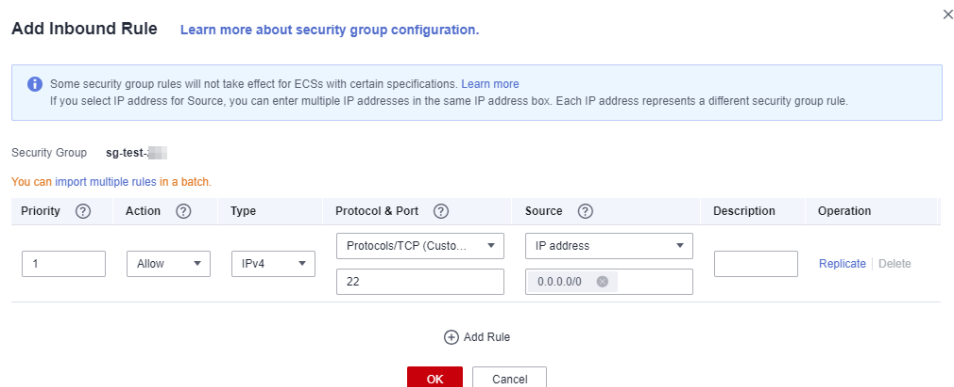
The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
5. Locate the row that contains the target security group, and click **Manage Rule** in the **Operation** column.

The page for configuring security group rules is displayed.

6. On the **Inbound Rules** tab, click **Add Rule**.
The **Add Inbound Rule** dialog box is displayed.
7. Configure required parameters.
You can click **+** to add more inbound rules.

Figure 5-11 Add Inbound Rule



Add Inbound Rule [Learn more about security group configuration.](#) ×

i Some security group rules will not take effect for ECSs with certain specifications. [Learn more](#)
If you select IP address for Source, you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule.

Security Group **sg-test**

You can import multiple rules in a batch.

Priority	Action	Type	Protocol & Port	Source	Description	Operation
1	Allow	IPv4	Protocols/TCP (Custo... 22	IP address 0.0.0.0/0		Replicate Delete

+ Add Rule

OK Cancel

Table 5-20 Inbound rule parameter description

Parameter	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default value is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1

Parameter	Description	Example Value
Action	<p>Allow or Deny</p> <ul style="list-style-type: none"> If the Action is set to Allow, access from the source is allowed to ECSs in the security group over specified ports. If the Action is set to Deny, access from the source is denied to ECSs in the security group over specified ports. <p>Security group rules are matched by priority and then by action. Deny rules take precedence over allow rules. For more information, see How Traffic Matches Security Group Rules.</p>	Allow
Type	<p>Source IP address version. You can select:</p> <ul style="list-style-type: none"> IPv4 IPv6 	IPv4
Protocol & Port	<p>The network protocol used to match traffic in a security group rule. The value can be All, TCP, UDP, GRE, and ICMP.</p>	TCP
	<p>Destination port used to match traffic in a security group rule. The value can be from 1 to 65535.</p> <p>Inbound rules control incoming traffic over specific ports to instances in the security group.</p> <p>Specify one of the following:</p> <ul style="list-style-type: none"> Individual port: Enter a port, such as 22. Consecutive ports: Enter a port range, such as 22-30. All ports: Leave it empty or enter 1-65535. 	22, or 22-30
Source	<p>Source of the security group rule. The value can be an IP address or a security group to allow access from IP addresses or instances in the security group.</p> <ul style="list-style-type: none"> IP address: <ul style="list-style-type: none"> Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) <p>If the source is a security group, this rule will apply to all instances associated with the selected security group.</p>	0.0.0.0/0

Parameter	Description	Example Value
Description	Supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

8. Click **OK**.
The inbound rule list is displayed.
9. On the **Outbound Rules** tab, click **Add Rule**.
The **Add Outbound Rule** dialog box is displayed.
10. Configure required parameters.
You can click **+** to add more outbound rules.

Figure 5-12 Add Outbound Rule

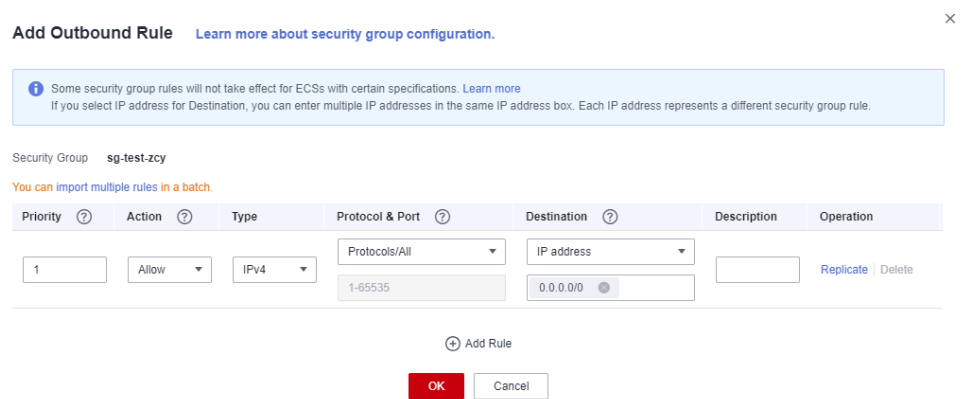


Table 5-21 Outbound rule parameter description

Parameter	Description	Example Value
Priority	The security group rule priority. The priority value ranges from 1 to 100. The default value is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1

Parameter	Description	Example Value
Action	<p>Allow or Deny</p> <ul style="list-style-type: none"> If the Action is set to Allow, access from ECSs in the security group is allowed to the destination over specified ports. If the Action is set to Deny, access from ECSs in the security group is denied to the destination over specified ports. <p>Security group rules are matched by priority and then by action. Deny rules take precedence over allow rules. For more information, see How Traffic Matches Security Group Rules.</p>	Allow
Type	<p>Destination IP address version. You can select:</p> <ul style="list-style-type: none"> IPv4 IPv6 	IPv4
Protocol & Port	<p>The network protocol used to match traffic in a security group rule. The value can be All, TCP, UDP, GRE, and ICMP.</p>	TCP
	<p>Destination port used to match traffic in a security group rule. The value can be from 1 to 65535.</p> <p>Outbound rules control outgoing traffic over specific ports from instances in the security group. Specify one of the following:</p> <ul style="list-style-type: none"> Individual port: Enter a port, such as 22. Consecutive ports: Enter a port range, such as 22-30. All ports: Leave it empty or enter 1-65535. 	22, or 22-30
Destination	<p>Destination of the security group rule. The value can be an IP address or a security group to allow access to IP addresses or instances in the security group. For example:</p> <ul style="list-style-type: none"> IP address: <ul style="list-style-type: none"> Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) 	0.0.0.0/0
Description	<p>Supplementary information about the security group rule. This parameter is optional.</p> <p>The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	N/A

11. Click **OK**.
The outbound rule list is displayed.

Verifying Security Group Rules

After allowing traffic over a port in a security group rule, you need to ensure that the port used by the instance is also opened.

For example, if you have deployed a website on an ECS and want users to access your website through HTTP (80), you need to add an inbound rule to the ECS security group to allow access over the port. [Table 5-22](#) shows the rule.

Table 5-22 Security group rule

Direction	Protocol & Port	Source
Inbound	TCP: 80	IP address: 0.0.0.0/0

After adding the security group rule, perform the following operations to check whether the ECS port is opened and whether the rule is applied:

1. Log in to the ECS and check whether the ECS port is opened.
 - **Checking the port of a Linux server**
Run the following command to check whether TCP port 80 is being listened on:

```
netstat -an | grep 80
```

If the following figure is displayed, TCP port 80 is enabled.

Figure 5-13 Command output for the Linux ECS

```
tcp        0      0 0.0.0.0:80          0.0.0.0:*          LISTEN
```

- **Checking the port of a Windows server**
 - i. Choose **Start > Run**. Type **cmd** to open the Command Prompt.
 - ii. Run the following command to check whether TCP port 80 is being listened on:

```
netstat -an | findstr 80
```

If the following figure is displayed, TCP port 80 is enabled.

Figure 5-14 Command output for the Windows ECS

```
TCP        0.0.0.0:80          0.0.0.0:0          LISTENING
```

2. Enter **http://ECS EIP** in the address box of the browser and press **Enter**.
If the requested page can be accessed, the security group rule has taken effect.

5.2.6.2 Fast-Adding Security Group Rules

Scenarios

The fast-adding rule function of security groups allows you to quickly add rules with common ports and protocols for remote login, ping tests, common web services, and database services.

For details about common ports used by cloud servers, see [Common Ports Used by ECSs](#).

Procedure



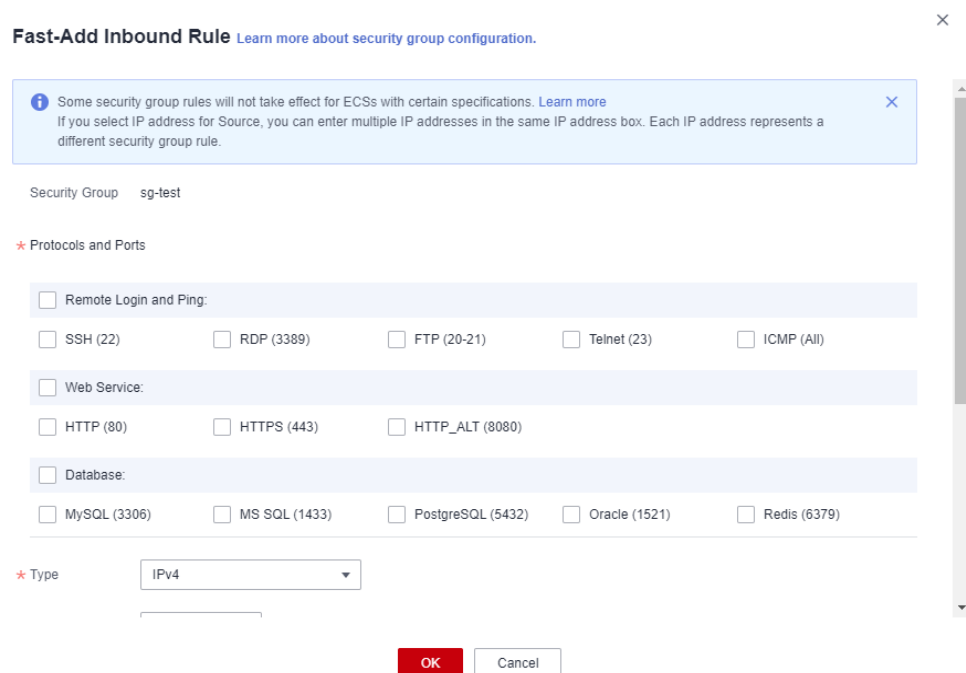
1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
The security group list is displayed.
5. Locate the row that contains the target security group and click **Manage Rule** in the **Operation** column.
The page for configuring security group rules is displayed.
6. On the **Inbound Rules** tab, click **Fast-Add Rule**.
The **Fast-Add Inbound Rule** dialog box is displayed.
7. Configure required parameters.

Figure 5-15 Fast-Add Inbound Rule



Fast-Add Inbound Rule [Learn more about security group configuration.](#)

Security Group sg-test

*** Protocols and Ports**

Remote Login and Ping:

SSH (22) RDP (3389) FTP (20-21) Telnet (23) ICMP (All)

Web Service:

HTTP (80) HTTPS (443) HTTP_ALT (8080)

Database:

MySQL (3306) MS SQL (1433) PostgreSQL (5432) Oracle (1521) Redis (6379)

*** Type** IPv4

OK **Cancel**

Table 5-23 Inbound rule parameter description

Parameter	Description	Example Value
Protocols and Ports	Common protocols and ports are provided for: <ul style="list-style-type: none">• Remote login and ping• Web services• Databases	SSH (22)
Type	Source IP address version. You can select: <ul style="list-style-type: none">• IPv4• IPv6	IPv4
Source	Source of the security group rule. The value can be an IP address or a security group to allow access from IP addresses or instances in the security group. You can specify: <ul style="list-style-type: none">• Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6)• IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6)• All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6)• Security group: sg-abc If the source is a security group, this rule will apply to all instances associated with the selected security group.	0.0.0.0/0
Action	Allow or Deny <ul style="list-style-type: none">• If the Action is set to Allow, access from the source is allowed to ECSs in the security group over specified ports.• If the Action is set to Deny, access from the source is denied to ECSs in the security group over specified ports. Security group rules are matched by priority and then by action. Deny rules take precedence over allow rules. For more information, see How Traffic Matches Security Group Rules .	Allow
Priority	Security group rule priority. The priority value is from 1 to 100. The default value is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1

Parameter	Description	Example Value
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

8. Click **OK**.
The inbound rule list is displayed and you can view your added rule.
9. On the **Outbound Rules** tab, click **Fast-Add Rule**.
The **Fast-Add Outbound Rule** dialog box is displayed.
10. Configure required parameters.

Figure 5-16 Fast-Add Outbound Rule

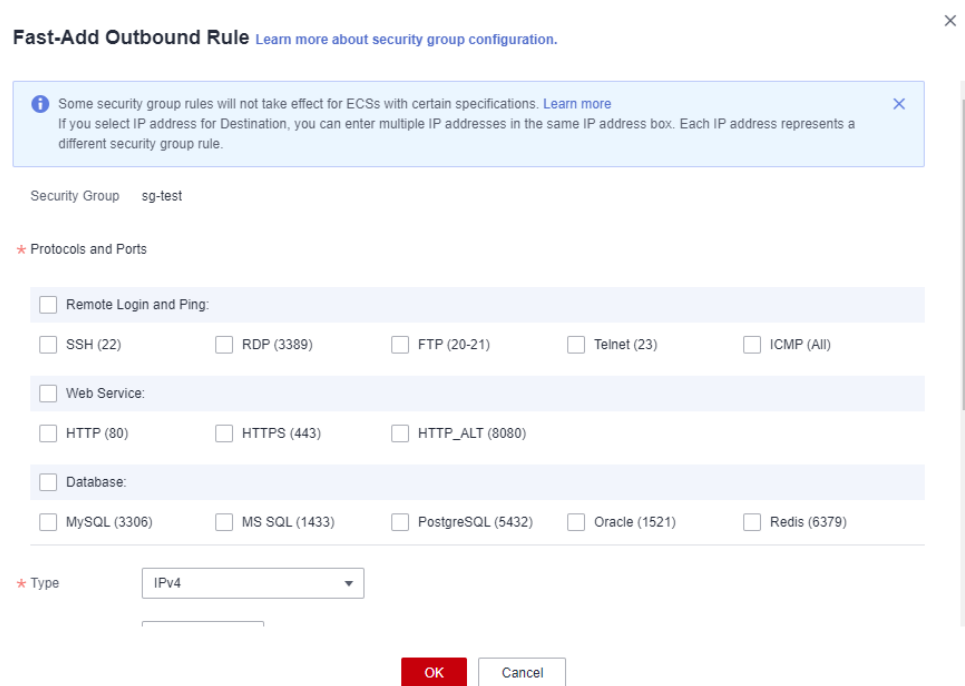


Table 5-24 Outbound rule parameter description

Parameter	Description	Example Value
Protocols and Ports	Common protocols and ports are provided for: <ul style="list-style-type: none"> • Remote login and ping • Web services • Databases 	SSH (22)

Parameter	Description	Example Value
Type	Source IP address version. You can select: <ul style="list-style-type: none"> IPv4 IPv6 	IPv4
Destination	Destination of the security group rule. The value can be an IP address or a security group to allow access to IP addresses or instances in the security group. You can specify: <ul style="list-style-type: none"> xxx.xxx.xxx.xxx/32 (IPv4 address) xxx.xxx.xxx.0/24 (IPv4 address range) 0.0.0.0/0 (all IPv4 addresses) sg-abc (security group) Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6) IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) Security group: sg-abc 	0.0.0.0/0
Priority	Security group rule priority. The priority value is from 1 to 100. The default value is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Allow or Deny <ul style="list-style-type: none"> If the Action is set to Allow, access from ECSs in the security group is allowed to the destination over specified ports. If the Action is set to Deny, access from ECSs in the security group is denied to the destination over specified ports. Security group rules are matched by priority and then by action. Deny rules take precedence over allow rules. For more information, see How Traffic Matches Security Group Rules .	Allow
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

11. Click **OK**.

The outbound rule list is displayed and you can view your added rule.

5.2.6.3 Allowing Common Ports with A Few Clicks

Scenarios

You can configure a security group to allow common ports with a few clicks. This function is suitable for the following scenarios:



- Remotely log in to ECSs.
- Use the ping command to test ECS connectivity.
- ECSs functioning as web servers provide website access services.

Table 5-25 describes the common ports that can be opened with a few clicks.

Table 5-25 Common ports

Direction	Protocol & Port & Type	Source/ Destination	Description
Inbound	TCP: 22 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 22 (SSH) for remotely logging in to Linux ECSs.
	TCP: 3389 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 3389 (RDP) for remotely logging in to Windows ECSs.
	TCP: 80 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 80 (HTTP) for visiting websites.
	TCP: 443 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 443 (HTTPS) for visiting websites.
	TCP: 20-21 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over ports 20 and 21 (FTP) for uploading or downloading files.
	ICMP: All (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over any port for using the ping command to test ECS connectivity.
Outbound	All (IPv4) All (IPv6)	0.0.0.0/0 ::/0	Allows access from ECSs in the security group to any IP address over any port.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
5. In the security group list, click the name of the security group.
The security group details page is displayed.
6. Click the **Inbound Rules** or **Outbound Rules** tab, and then click **Allow Common Ports**.
The **Allow Common Ports** page is displayed.
7. Click **OK**.
After the operation is complete, you can view the added rules in the security group rule list.

5.2.6.4 Modifying a Security Group Rule

Scenarios

You can modify the port, protocol, and IP address of your security group rules as required to ensure the security of your instances.

Notes and Constraints

Note that modifying a security group rule may interrupt your services or cause network security risks.



Security group rules are like a whitelist. If there are no rules that allow or deny some traffic, the security group denies all traffic to or from the instances in the security group

- The inbound rules in [Table 5-26](#) ensure that instances in the security group can communicate with each other. Do not modify these rules.
- The outbound rules in [Table 5-26](#) allow instances in the security group to access external networks. If you modify these rules, the instances in the security group cannot access external networks.

Table 5-26 Security group rules

Direction	Action	Type	Protocol & Port	Source/Destination
Inbound	Allow	IPv4	All	Source: current security group
Inbound	Allow	IPv6	All	Source: current security group
Outbound	Allow	IPv4	All	Destination: 0.0.0.0/0
Outbound	Allow	IPv6	All	Destination: ::/0

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
5. In the security group list, click the name of the security group.
The security group details page is displayed.
6. Click the **Inbound Rules** or **Outbound Rules** tab as required.
The security group rule list is displayed.
7. Locate the row that contains the rule and click **Modify** in the **Operation** column.
8. Modify the security group rule information as prompted and click **Confirm**.

5.2.6.5 Replicating a Security Group Rule

Scenarios

You can replicate an existing security group rule and modify it to quickly generate a new rule.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.

4. In the security group list, click the name of the security group.
The security group details page is displayed.
5. Click the **Inbound Rules** or **Outbound Rules** tab as required.
The security group rule list is displayed.
6. Locate the row that contains the rule and click **Replicate** in the **Operation** column.
The **Replicate Inbound Rule** dialog box is displayed.
7. Modify the security group rule information as prompted and click **OK**.

5.2.6.6 Importing and Exporting Security Group Rules

Scenarios

You can configure security group rules in an Excel file and import the rules to the security group. You can also export security group rules to an Excel file.



You can import and export security group rules in the following scenarios:

- If you want to back up security group rules locally, you can export the rules to an Excel file.
- If you want to quickly create or restore security group rules, you can import your security group rule file to the security group.
- If you want to quickly apply the rules of one security group to another, you can export and import existing rules.
- If you want to modify multiple rules of the current security group at a time, you can export and import existing rules.

Notes and Constraints

- The security group rules to be imported must be configured based on the template. Do not add parameters or change existing parameters. Otherwise, the import will fail.
- If a security group rule to be imported is the same as an existing one, the security group rule cannot be imported. You can delete the rule and try again.
- If you want to import rules of the security group in one region to another under one account, only rules with both **Source** and **Destination** set to **IP address** can be applied.
- If you want to import rules of the security group in one account to the security group in another account, only rules with both **Source** and **Destination** set to **IP address** can be applied.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **Access Control > Security Groups**. The security group list is displayed.
5. On the security group list, click the name of the target security group. The security group details page is displayed.
6. Export and import security group rules.
 - Click **Export Rule** to export all rules of the current security group to an Excel file.
 - Click **Import Rule** to import security group rules from an Excel file into the current security group.

Table 5-27 describes the parameters in the template for importing rules.

Table 5-27 Template parameters

Parameter	Description	Example Value
Direction	The direction in which the security group rule takes effect. <ul style="list-style-type: none">• Inbound: Inbound rules control incoming traffic to instances in the security group.• Outbound: Outbound rules control outgoing traffic from instances in the security group.	Inbound
Priority	The priority value ranges from 1 to 100. The default value is 1 and has the highest priority. The security group rule with a smaller value has a higher priority.	1
Action	Allow or Deny <ul style="list-style-type: none">• If the Action is set to Allow, access from the source is allowed to ECSs in the security group over specified ports.• If the Action is set to Deny, access from the source is denied to ECSs in the security group over specified ports. Security group rules are matched by priority and then by action. Deny rules take precedence over allow rules. For more information, see How Traffic Matches Security Group Rules .	Allow
Protocol & Port	The network protocol used to match traffic in a security group rule. The value can be All , TCP , UDP , GRE , and ICMP .	TCP

Parameter	Description	Example Value
	<p>Destination port used to match traffic in a security group rule. The value can be from 1 to 65535.</p> <p>Inbound rules control incoming traffic over specific ports to instances in the security group.</p> <p>Outbound rules control outgoing traffic over specific ports from instances in the security group.</p> <p>Specify one of the following:</p> <ul style="list-style-type: none"> • Individual port: Enter a port, such as 22. • Consecutive ports: Enter a port range, such as 22-30. • All ports: Leave it empty or enter 1-65535. 	22, or 22-30
Type	<p>Source IP address version. You can select:</p> <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
Source	<p>Source of the security group rule. The value can be an IP address or a security group to allow access from IP addresses or instances in the security group.</p> <ul style="list-style-type: none"> • IP address: <ul style="list-style-type: none"> - Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) - All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) - IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) 	sg-test[96a8a93f-XXX-d7872990c314]
Destination	<p>Destination of the security group rule. The value can be an IP address or a security group to allow access to IP addresses or instances in the security group. For example:</p>	sg-test[96a8a93f-XXX-d7872990c314]
Description	<p>Supplementary information about the security group rule. This parameter is optional.</p> <p>The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-
Last Modified	<p>The time when the security group was modified.</p>	-

5.2.6.7 Deleting a Security Group Rule

Scenarios

If you no longer need a security group rule to control the traffic to and from the instances in a security group, you can delete it.

Notes and Constraints

Note that deleting a security group rule may interrupt your services or cause network security risks.



Security group rules are like a whitelist. If there are no rules that allow or deny some traffic, the security group denies all traffic to or from the instances in the security group.

- The inbound rules in [Table 5-28](#) ensure that instances in the security group can communicate with each other. Do not delete these rules.
- The outbound rules in [Table 5-28](#) allow all traffic from the instances in the security groups to external networks. If you delete these rules, the instances in the security group cannot access external networks.

Table 5-28 Security group rules

Direction	Action	Type	Protocol & Port	Source/Destination
Inbound	Allow	IPv4	All	Source: current security group
Inbound	Allow	IPv6	All	Source: current security group
Outbound	Allow	IPv4	All	Destination: 0.0.0.0/0
Outbound	Allow	IPv6	All	Destination: ::/0

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
5. In the security group list, click the name of the security group.
The security group details page is displayed.
6. Click the **Inbound Rules** or **Outbound Rules** tab as required.
The security group rule list is displayed.

7. In the security group rule list:
 - To delete a single security group rule, locate the row that contains the rule and click **Delete** in the **Operation** column.
 - To delete multiple security group rules, select multiple security group rules and click **Delete** in the upper left corner of the rule list.
8. Click **Yes**.

5.2.7 Managing Instances Associated with a Security Group

5.2.7.1 Adding an Instance to or Removing an Instance from a Security Group

Scenarios



When you create an instance, the system automatically adds the instance to a security group for protection.

- If one security group cannot meet your requirements, you can add an instance to multiple security groups.
- An instance must be added to at least one security group. If you want to change the security group for an instance, you can add the instance to a new security group and then remove the instance from the original security group.

You can add servers, extension NICs, and supplementary network interfaces to a security group by referring to the following operations:



- [Adding an Instance to a Security Group](#)
- [Removing an Instance from a Security Group](#)

Adding an Instance to a Security Group

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
The security group list is displayed.
5. In the security group list, locate the row that contains the security group and click **Manage Instances** in the **Operation** column.
The **Associated Instances** tab is displayed.
6. Click the required instance type tab.
The following operations use **Servers** as an example.
7. Click the **Servers** tab and click **Add**.
The **Add Server** dialog box is displayed.
8. In the server list, select one or more servers and click OK to add them to the current security group.

Removing an Instance from a Security Group

An instance must be added to at least one security group. If you want to remove an instance from a security group, the instance must be associated with at least two security groups now.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
5. In the security group list, locate the row that contains the security group and click **Manage Instances** in the **Operation** column.
The **Associated Instances** tab is displayed.
6. Click the required instance type tab.
The following operations use **Servers** as an example.
7. Click the **Servers** tab, select one or more servers, and click **Remove** in the upper left corner of the server list.
A confirmation dialog box is displayed.
8. Confirm the information and click **Yes**.


5.2.7.2 Changing the Security Group of an ECS

Scenarios

When creating an ECS, you must associate it with a security group. If no security group has been created yet, a **default security group** will be created and associated with the ECS. If the default security group cannot meet your service requirements, you can change the security group associated with the ECS.

You can also associate an ECS with a custom security group. If the custom security group cannot meet your requirements, you can change the custom security group.

Procedure

1. Log in to the management console.
2. Click . Under **Compute**, click **Elastic Cloud Server**.
3. In the ECS list, locate the row that contains the target ECS. Click **More** in the **Operation** column and select **Manage Network > Change Security Group**.
The **Change Security Group** dialog box is displayed.
4. Select the target NIC and security groups.
You can select multiple security groups. In such a case, the rules of all the selected security groups will apply to the ECS.
To create a security group, click **Create Security Group**.

NOTE

Using multiple security groups may deteriorate ECS network performance. You are suggested to select no more than five security groups.

5. Click **OK**.

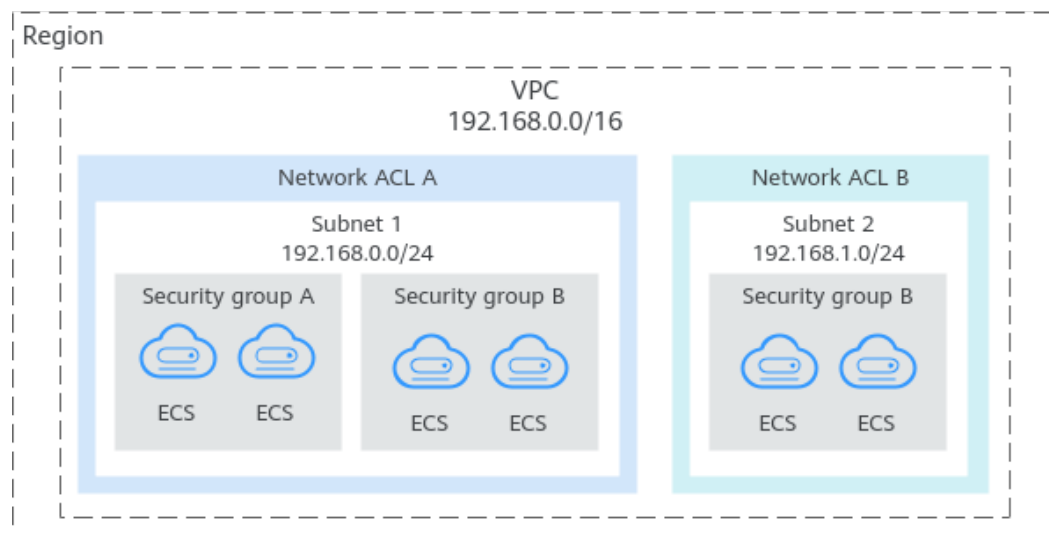
5.3 Network ACL

5.3.1 Network ACL Overview

A network ACL is an optional layer of security for your subnets. After you associate one or more subnets with a network ACL, you can control traffic in and out of the subnets.

[Figure 5-17](#) shows how a network ACL works.

Figure 5-17 Security groups and network ACLs



Similar to security groups, network ACLs control access to subnets and add an additional layer of defense to your subnets. Security groups only have the "allow" rules, but network ACLs have both "allow" and "deny" rules. You can use network ACLs together with security groups to implement comprehensive and fine-grained access control.

[What Is Access Control?](#) summarizes the basic differences between security groups and network ACLs.

Network ACL Basics

- Your VPC does not come with a network ACL, but you can create a network ACL and associate it with a VPC subnet if required. By default, each network ACL denies all inbound traffic to and outbound traffic from the associated subnet until you add rules.
- You can associate a network ACL with multiple subnets. However, a subnet can only be associated with one network ACL at a time.

- Each newly created network ACL is in the **Inactive** state until you associate subnets with it.
- Network ACLs are stateful. If the network ACL rule allows outbound traffic and you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound network ACL rules. Similarly, if inbound traffic is allowed, responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.
- Network ACLs use connection tracking to track traffic to and from instances. Changes to inbound and outbound rules do not take effect immediately for the existing traffic.

If you add, modify, or delete a network ACL rule, or associate or disassociate a subnet with or from a network ACL, all the inbound and outbound persistent connections will not be disconnected. New rules will only be applied for the new connections.

NOTICE

After a persistent connection is disconnected, new connections will not be established immediately until the timeout period of connection tracking expires. For example, after an ICMP persistent connection is disconnected, a new connection will be established and a new rule will be applied when the timeout period (30s) expires.

- The timeout period of connection tracking varies by protocol. The timeout period of a TCP connection in the established state is 600s, and that of an ICMP connection is 30s. For other protocols, if packets are received in both inbound and outbound directions, the connection tracking timeout period is 180s. If packets are received only in one direction, the connection tracking timeout period is 30s.
- The timeout period of TCP connections varies by connection status. The timeout period of a TCP connection in the established state is 600s, and that of a TCP connection in the FIN-WAIT state is 30s.

Default Network ACL Rules

By default, each network ACL has preset rules that allow the following packets:

- Packets whose source and destination are in the same subnet.
- Broadcast packets with the destination 255.255.255.255/32, which is used to configure host startup information.
- Multicast packets with the destination 224.0.0.0/24, which is used by routing protocols.
- Metadata packets with the destination 169.254.169.254/32 and TCP port number 80, which is used to obtain metadata.
- Packets from CIDR blocks that are reserved for public services (for example, packets with the destination 100.125.0.0/16).
- A network ACL denies all traffic in and out of a subnet excepting the preceding packets. [Table 5-29](#) shows the default rules. You cannot modify or delete the default rules.

Table 5-29 Default network ACL rules

Direction	Priority	Action	Protocol	Source	Destination	Description
Inbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all inbound traffic.
Outbound	*	Deny	All	0.0.0.0/0	0.0.0.0/0	Denies all outbound traffic.

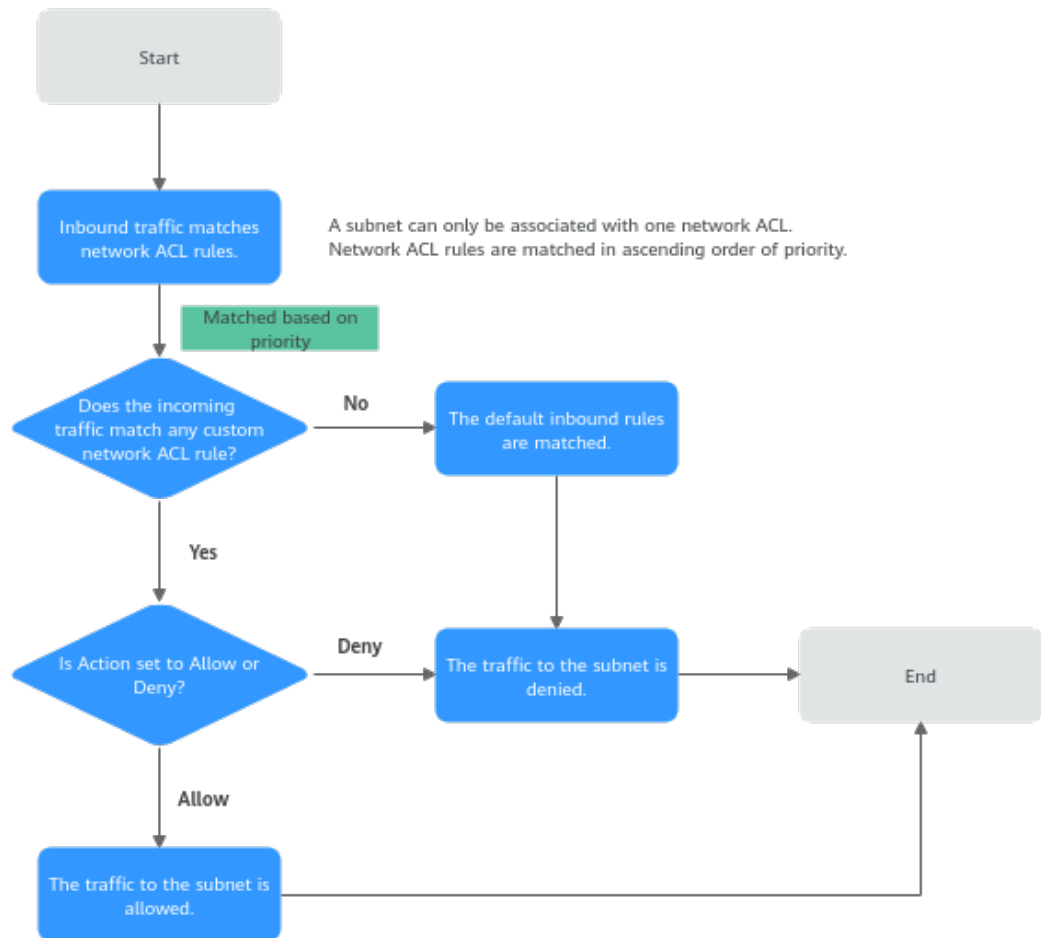
How Traffic Matches Network ACL Rules

A subnet can be bound to only one network ACL rule. When multiple rules exist, traffic is matched based on the rule priority. A smaller value indicates a higher priority. The default value is *, which has the lowest priority.

The following takes inbound traffic as an example to match security group rules.

- If traffic matches a rule:
 - With **Action** set to **Deny**, the traffic is denied to flow into the subnet.
 - With **Action** set to **Allow**, the traffic is allowed to flow into the subnet.
- If the traffic does not match any rule, the default rule applies and the traffic is denied to flow into the subnet.

Figure 5-18 Network ACL matching sequence



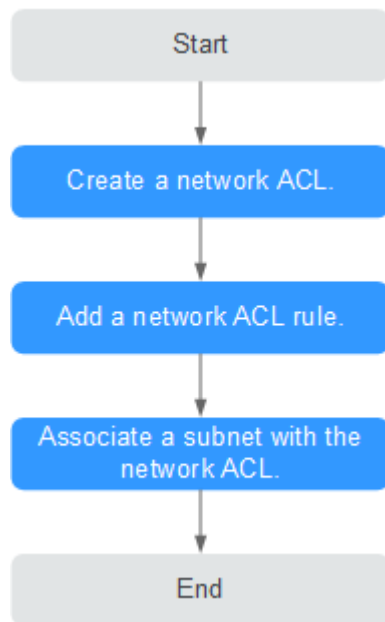
Application Scenarios

- If the application layer needs to provide services for users, traffic must be allowed to reach the application layer from all IP addresses. However, you also need to prevent illegal access from malicious users.
Solution: You can add network ACL rules to deny access from suspect IP addresses.
- How can I isolate ports with identified vulnerabilities? For example, how do I isolate port 445 that can be exploited by WannaCry worm?
Solution: You can add network ACL rules to deny access traffic from a specific port and protocol, for example, TCP port 445.
- No defense is required for the communication within a subnet, but access control is required for communication between subnets.
Solution: You can add network ACL rules to control traffic between subnets.
- For frequently accessed applications, a security rule sequence may need to be adjusted to improve performance.
Solution: A network ACL allows you to adjust the rule sequence so that frequently used rules are applied before other rules.

Configuration Procedure

Figure 5-19 shows the procedure for configuring a network ACL.

Figure 5-19 network ACL configuration procedure



1. Create a network ACL by following the steps described in [Creating a Network ACL](#).
2. Add network ACL rules by following the steps described in [Adding a Network ACL Rule \(Default Effective Sequence\)](#).
3. Associate subnets with the network ACL by following the steps described in [Associating Subnets with a Network ACL](#). After subnets are associated with the network ACL, the subnets will be protected by the configured network ACL rules.

Notes and Constraints

- By default, each account can have up to 200 network ACLs in a region.
- A network ACL can contain no more than 100 rules in one direction, or performance will deteriorate.
- A network ACL can have up to 124 rules to be associated with IP address groups in one direction.

5.3.2 Network ACL Configuration Examples

This section provides examples for configuring network ACLs.

- [Denying Access from a Specific Port](#)
- [Allowing Access from Specific Ports and Protocols](#)
- [Denying Access from a Specific IP Address](#)

Denying Access from a Specific Port

You might want to block TCP port 445 to protect against the WannaCry ransomware attacks. You can add a network ACL rule to deny all incoming traffic from TCP port 445.

Network ACL Configuration

Table 5-30 lists the inbound rules required.

Table 5-30 Network ACL rules

Direction	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range	Description
Inbound	Deny	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	445	Denies inbound traffic from any IP address through TCP port 445.
Inbound	Allow	All	0.0.0.0/0	1-65535	0.0.0.0/0	All	Allows all inbound traffic.

NOTE

- By default, a network ACL denies all inbound traffic. You can add a rule to allow all inbound traffic if necessary.
- If you want a deny rule to be matched first, insert the deny rule above the allow rule. For details, see [Adding a Network ACL Rule \(Custom Effective Sequence\)](#).

Allowing Access from Specific Ports and Protocols

In this example, an ECS in a subnet is used as the web server, and you need to allow inbound traffic from HTTP port 80 and HTTPS port 443 and allow all outbound traffic. You need to configure both the network ACL rules and security group rules to allow the traffic.

Network ACL Configuration

Table 5-31 lists the inbound and outbound rules required.

Table 5-31 Network ACL rules

Direction	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range	Description
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	80	Allows inbound HTTP traffic from any IP address to ECSs in the subnet through port 80.
Inbound	Allow	TCP	0.0.0.0/0	1-65535	0.0.0.0/0	443	Allows inbound HTTPS traffic from any IP address to ECSs in the subnet through port 443.
Outbound	Allow	All	0.0.0.0/0	All	0.0.0.0/0	All	Allows all outbound traffic from the subnet.

Security group configuration

Table 5-32 lists the inbound and outbound security group rules required.

Table 5-32 Security group rules

Direction	Protocol / Application	Port	Source/ Destination	Description
Inbound	TCP	80	Source: 0.0.0.0/0	Allows inbound HTTP traffic from any IP address to ECSs associated with the security group through port 80.
Inbound	TCP	443	Source: 0.0.0.0/0	Allows inbound HTTPS traffic from any IP address to ECSs associated with the security group through port 443.
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic from the security group.

A network ACL adds an additional layer of security. Even if the security group rules allow more traffic than that actually required, the network ACL rules allow only access from HTTP port 80 and HTTPS port 443 and deny other inbound traffic.

Denying Access from a Specific IP Address

In this example, you can add a network ACL rule to deny the access from some abnormal IP addresses, for example, 192.168.1.102.

Network ACL Configuration

[Table 5-33](#) lists the inbound rules required.

Table 5-33 Network ACL rules

Direction	Action	Protocol	Source	Source Port Range	Destination	Destination Port Range	Description
Inbound	Deny	TCP	192.168.1.102/32	1-65535	0.0.0.0/0	All	Denies access from 192.168.1.102.
Inbound	Allow	All	0.0.0.0/0	1-65535	0.0.0.0/0	All	Allows all inbound traffic.

NOTE

- By default, a network ACL denies all inbound traffic. You can add a rule to allow all inbound traffic if necessary.
- If you want a deny rule to be matched first, insert the deny rule above the allow rule. For details, see [Adding a Network ACL Rule \(Custom Effective Sequence\)](#).

5.3.3 Managing Network ACLs

5.3.3.1 Creating a Network ACL

Scenarios

You can create a custom network ACL. By default, a newly created network ACL is disabled and has no inbound or outbound rules, or any subnets associated.

Procedure

1. Go to the [network ACL list page](#).
2. In the right pane displayed, click **Create Network ACL**.
3. On the **Create Network ACL** page, configure parameters as prompted.

Table 5-34 Parameter descriptions

Parameter	Description	Example Value
Name	The network ACL name. This parameter is mandatory. The name contains a maximum of 64 characters, which may consist of letters, digits, underscores (_), periods (.), and hyphens (-). The name cannot contain spaces.	fw-92d3
Description	Supplementary information about the network ACL. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A



4. Click **OK**.

5.3.3.2 Modifying a Network ACL

Scenarios

Modify the name and description of a network ACL.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control** > **Network ACLs**.
The network ACL list is displayed.
5. In the network ACL list, locate the target network ACL and click its name.
The network ACL summary page is displayed.
6. On the **Summary** tab, modify the name and description as needed.



5.3.3.3 Enabling or Disabling a Network ACL

Scenarios

After a network ACL is created, you may need to enable it based on network security requirements. You can also disable an enabled network ACL if needed. Before enabling a network ACL, ensure that subnets have been associated with the network ACL and that inbound and outbound rules have been added to the network ACL.

When a network ACL is disabled, custom rules will become invalid while default rules still take effect. Disabling a network ACL may interrupt network traffic. For information about the default network ACL rules, see [Default Network ACL Rules](#).

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
The network ACL list is displayed.
5. In the network ACL list, enable or disable the target network ACL.
 - Enabling a network ACL
 - i. Locate the target network ACL and choose **More > Enable** in the **Operation** column.
A confirmation dialog box is displayed.
 - ii. Confirm the information and click **Yes**.
 - Disabling a network ACL
 - i. Locate the target network ACL and choose **More > Disable** in the **Operation** column.
A confirmation dialog box is displayed.
 - ii. Confirm the information and click **Yes**.

5.3.3.4 Viewing a Network ACL

Scenarios

View details about a network ACL.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
The network ACL list is displayed.
5. In the network ACL list, locate the target network ACL and click its name.
The network ACL summary page is displayed.



6. On the **Summary** tab, you can view the following information:
 - Basic information: name, ID, status, and description.
 - Inbound and outbound rules: rule priority, status, protocol, source, source port, destination, and destination port.
 - Associated subnets: the subnets associated with the network ACL. A network ACL can be associated with multiple subnets.

5.3.3.5 Deleting a Network ACL

Scenarios

Delete a network ACL when it is no longer required.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
The network ACL list is displayed.
5. In the network ACL list, locate the target network ACL and choose **More > Delete** in the **Operation** column.
A confirmation dialog box is displayed.
6. Confirm the information and click **OK**.

NOTE

Deleting a network ACL will also disassociate its associated subnets and delete the network ACL rules.

5.3.4 Management Network ACL Rules

5.3.4.1 Adding a Network ACL Rule (Default Effective Sequence)

Scenarios

You can add inbound and outbound rules to a network ACL to control the traffic in and out of a subnet.

When you perform the following operations to add a rule, the system generates a priority based on the sequence when the rule is added. You cannot specify a priority.

For example, there are two custom inbound rules (rule A and rule B) and one default rule. The priority of rule A is 1 and that of rule B is 2. The default rule has the lowest priority. If rule C is added, the system sets its priority to 3, which has lower priority than rules A and B and higher priority than the default rule.

If the default priorities do not meet your requirements, you can customize the priorities by referring to [Adding a Network ACL Rule \(Custom Effective Sequence\)](#).

Notes and Constraints

A network ACL can contain no more than 20 rules in one direction, or performance will deteriorate.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
5. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
6. On the **Inbound Rules** or **Outbound Rules** tab, click **Add Rule** to add an inbound or outbound rule.
 - Click **+** to add more rules.
 - Locate the row that contains the network ACL rule and click **Replicate** in the **Operation** column to replicate an existing rule.

Table 5-35 Parameter descriptions

Parameter	Description	Example Value
Priority	Priority of a network ACL rule. A smaller priority value represents a higher priority. Each network ACL includes a default rule whose priority value is an asterisk (*). Default rules have the lowest priority.	3
Status	Status of a network ACL. When you add a rule to it, its default status is Enabled .	Enabled
Type	This parameter is available only after the IPv6 function is enabled. The network ACL type. This parameter is mandatory. You can select a value from the drop-down list. Currently, only IPv4 and IPv6 are supported.	IPv4
Action	The action in the network ACL. This parameter is mandatory. You can select a value from the drop-down list. Currently, the value can be Allow or Deny .	Allow

Parameter	Description	Example Value
Protocol	The protocol supported by the network ACL. This parameter is mandatory. You can select a protocol from the drop-down list. You can select TCP , UDP , ICMP , or All .	TCP
Source	The source from which the traffic is allowed. The source can be an IP address or IP address range. <ul style="list-style-type: none">IP address:<ul style="list-style-type: none">Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6)All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6)IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6)	0.0.0.0/0
Source Port Range	The source port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, 1-100 .	22, or 22-30
Destination	The destination to which the traffic is allowed. The destination can be an IP address or IP address range. <ul style="list-style-type: none">IP address:<ul style="list-style-type: none">Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6)All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6)IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6)	0.0.0.0/0
Destination Port Range	The destination port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, 1-100 . You must specify this parameter if TCP or UDP is selected for Protocol .	22, or 22-30
Description	Supplementary information about the network ACL rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.



5.3.4.2 Adding a Network ACL Rule (Custom Effective Sequence)

Scenarios

If you want a new rule to have a higher or lower priority than a specific rule, you can insert the new rule above or below the specific rule.

For example, there are two custom inbound rules (rule A and rule B) and one default rule. The priority of rule A is 1 and that of rule B is 2. The default rule has the lowest priority. If you want rule C to be applied earlier than rule B, you can insert rule C above rule B. After rule C is added, the priority of rule C is 2, and that of rule B is 3.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
The network ACL list is displayed.
5. In the network ACL list, locate the target network ACL and click its name.
The network ACL summary page is displayed.
6. Click the **Inbound Rules** or **Outbound Rules** tab and insert a rule.
 - Locate the target rule and choose **More > Insert Rule Above** in the **Operation** column. The new rule is applied earlier than the current rule.
 - Locate the target rule and choose **More > Insert Rule Below** in the **Operation** column. The new rule is applied later than the current rule.

5.3.4.3 Modifying a Network ACL Rule

Scenarios

Modify an inbound or outbound network ACL rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **Access Control > Network ACLs**. The network ACL list is displayed.
5. In the network ACL list, locate the target network ACL and click its name. The network ACL summary page is displayed.
6. Click the **Inbound Rules** or **Outbound Rules** tab, locate the target rule, click **Modify** in the **Operation** column, and modify parameters as needed.

[Table 5-36](#) lists the parameters to be configured.

Table 5-36 Parameter descriptions

Parameter	Description	Example Value
Priority	Priority of a network ACL rule. A smaller priority value represents a higher priority. Each network ACL includes a default rule whose priority value is an asterisk (*). Default rules have the lowest priority.	3
Status	Status of a network ACL. When you add a rule to it, its default status is Enabled .	Enabled
Type	This parameter is available only after the IPv6 function is enabled. The network ACL type. This parameter is mandatory. You can select a value from the drop-down list. Currently, only IPv4 and IPv6 are supported.	IPv4
Action	The action in the network ACL. This parameter is mandatory. You can select a value from the drop-down list. Currently, the value can be Allow or Deny .	Allow
Protocol	The protocol supported by the network ACL. This parameter is mandatory. You can select a protocol from the drop-down list. You can select TCP , UDP , ICMP , or All .	TCP
Source	The source from which the traffic is allowed. The source can be an IP address or IP address range. <ul style="list-style-type: none"> • IP address: <ul style="list-style-type: none"> - Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) - All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) - IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) 	0.0.0.0/0

Parameter	Description	Example Value
Source Port Range	The source port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, 1-100 .	22, or 22-30
Destination	The destination to which the traffic is allowed. The destination can be an IP address or IP address range. <ul style="list-style-type: none"> IP address: <ul style="list-style-type: none"> Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/128 (IPv6) All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6) IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6) 	0.0.0.0/0
Destination Port Range	The destination port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, 1-100 . You must specify this parameter if TCP or UDP is selected for Protocol .	22, or 22-30
Description	Supplementary information about the network ACL rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A



7. Click **Confirm**.

5.3.4.4 Enabling or Disabling a Network ACL Rule

Scenarios

Enable or disable an inbound or outbound rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Virtual Private Cloud**.

- The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
The network ACL list is displayed.
 5. In the network ACL list, locate the target network ACL and click its name.
The network ACL summary page is displayed.
 6. Click the **Inbound Rules** or **Outbound Rules** tab as required.
The network ACL rule list is displayed.
 7. In the rule list, perform the following operations to enable or disable a rule:
 - Enabling a network ACL rule
 - i. Locate the target network ACL rule and choose **More > Enable** in the **Operation** column.
A confirmation dialog box is displayed.
 - ii. Confirm the information and click **Yes**.
 - Disabling a network ACL rule
 - i. Locate the target network ACL rule and choose **More > Disable** in the **Operation** column.
A confirmation dialog box is displayed.
 - ii. Confirm the information and click **Yes**.

5.3.4.5 Exporting and Importing Network ACL Rules



Scenarios

You can export inbound and outbound rules of a specific network ACL as an Excel file and then import these rules for another network ACL. Importing and exporting rules across regions are supported.

Notes and Constraints

- For optimal performance, import no more than 40 network ACL rules at a time.
- Importing rules will not delete existing rules.
- Importing duplicate rules will fail.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
The network ACL list is displayed.
5. In the network ACL list, locate the target network ACL and click its name.



- The network ACL summary page is displayed.
6. Export or import network ACL rules.
 - Click **Export Rule** to export the network ACL rules to an Excel file.
 - Click **Import Rule** to import the network ACL rules from an Excel file into the current network ACL.

5.3.4.6 Deleting a Network ACL Rule

Scenarios

Delete an inbound or outbound rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
The network ACL list is displayed.
5. In the network ACL list, locate the target network ACL and click its name.
The network ACL summary page is displayed.
6. Click the **Inbound Rules** or **Outbound Rules** tab as required.
The network ACL rule list is displayed.
7. In the rule list, perform the following operations to delete a rule:
 - To delete a single rule, locate the target rule and click **Delete** in the **Operation** column.
 - To delete multiple rules, select the rules and click **Delete** in the upper left corner.
8. In the displayed dialog box, confirm the information and click **Yes**.

5.3.5 Managing Subnets Associated with a Network ACL

5.3.5.1 Associating Subnets with a Network ACL

Scenarios



You can associate a network ACL with a subnet to protect resources in the subnet.

Notes and Constraints

- You can associate a network ACL with multiple subnets. However, a subnet can only be associated with one network ACL at a time.
- After a network ACL is associated with a subnet, the default network ACL rules deny all traffic to and from the subnet until you add custom rules to

allow traffic. For details, see [Adding a Network ACL Rule \(Default Effective Sequence\)](#).

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
5. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
6. On the displayed page, click the **Associated Subnets** tab.
7. On the **Associated Subnets** tab, click **Associate**.
8. On the displayed page, select the subnets to be associated with the network ACL, and click **OK**.

NOTE



A subnet with a network ACL associated will not be displayed on the page for you to select. If you want to associate such a subnet with another network ACL, you must first disassociate the subnet from the original network ACL. One-click subnet association and disassociation are not supported currently. A subnet can only be associated with one network ACL.

5.3.5.2 Disassociating Subnets from a Network ACL

Scenarios

You can disassociate a subnet from its network ACL based on your network requirements.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > Network ACLs**.
5. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
6. On the displayed page, click the **Associated Subnets** tab.
7. On the **Associated Subnets** page, locate the row that contains the target subnet and click **Disassociate** in the **Operation** column.

8. Click **Yes** in the displayed dialog box.

Disassociating subnets from a network ACL

Select multiple subnets and click **Disassociate** above the subnet list to disassociate the subnets from the network ACL at a time.

6 IP Address Group

6.1 IP Address Group Overview

An IP address group is a collection of IP addresses that can use the same security group rules or network ACL rules. You can use an IP address group to manage IP addresses that have the same security requirements or whose security requirements change frequently.

You can create an IP address group and add IP addresses that need to be managed in a unified manner to the group. Then, you can select this IP address group when configuring a security group rule. The rule will take effect for all IP addresses in the IP address group.

Notes and Constraints

- Security group rules that are associated with an IP address group do not take effect for certain ECSs.
 - General computing (S1, C1, and C2 ECSs)
 - Memory-optimized (M1 ECSs)
 - High-performance computing (H1 ECSs)
 - Disk-intensive (D1 ECSs)
 - GPU-accelerated (G1 and G2 ECSs)
 - Large-memory (E1, E2, and ET2 ECSs)
- If a network ACL rule uses an IP address group:
 - Either the source or the destination of an inbound rule can use the IP address group.
 - Either the source or the destination of an outbound rule can use the IP address group.

For example, if the source of an inbound rule network ACL is set to an IP address group, the rule destination can only be an IP address.

6.2 Managing an IP Address Group

6.2.1 Creating an IP Address Group

Scenarios

This section describes how to create an IP address group. An IP address group is a collection of IP addresses that can be associated with security groups and network ACLs to simplify IP address configuration and management.

Procedure

1. Go to the [Create IP Address Group](#) page.
2. Configure the parameters as prompted.

For details, see [Table 6-1](#).

Table 6-1 Parameters for creating an IP address group

Parameter	Description	Example Value
Region	Mandatory Select the region nearest to you to ensure the lowest latency possible. An IP address group can be associated only with resources in the same region.	Region A
Name	Mandatory Enter the name of the IP address group. The name: <ul style="list-style-type: none">• Can contain 1 to 64 characters.• Can contain letters, digits, underscores (_), hyphens (-), and periods (.). You can customize the name of an IP address group that is uniquely identified by its ID.	ipGroup-A
IP Address Version	Mandatory Select the type of IP addresses that can be added to an IP address group. <ul style="list-style-type: none">• IPv4• IPv6	IPv4

Parameter	Description	Example Value
IP Addresses	Optional Enter an IP address or IP address range on each line, and press Enter . You can enter: <ul style="list-style-type: none">• An IPv4 address range, for example, 192.168.0.0/16• A single IPv4 address, for example, 192.168.10.10/32• An IPv6 address range, for example, 2001:db8:a583:6e::/64• A single IPv6 address, for example, 2001:db8:a583:6e::5c/128	192.168.0.0/16 192.168.10.10/32
Description	Optional Enter the description of the IP address group in the text box as required.	-

3. Click **Create Now**.

The IP address group list is displayed. The status of the created IP address group is **Normal**.

NOTICE

An IP address group takes effect only after it is associated with corresponding resources. For details, see [Associating an IP Address Group with Resources](#).

6.2.2 Associating an IP Address Group with Resources

Scenarios

This section describes how to associate an IP address group with a resource.

An IP address group can be associated with security groups and network ACLs.

Prerequisites

- You have created an IP address group has been created. For details, see [Creating an IP Address Group](#).
- You have added IP addresses to the IP address group. For details, see [Adding IP Addresses to an IP Address Group](#).

Procedure

You need to associate an IP address group with resources. For details, see [Table 6-2](#).

Table 6-2 Associating an IP address group with resources

Resource	Description	Reference
Security group	The Source or Destination of a security group rule can be set to IP address group .	Adding a Security Group Rule <ul style="list-style-type: none">• Inbound rule: Set Source to an IP address group.• Outbound rule: Set Destination to an IP address group.
Network ACL	The Source or Destination of a network ACL is set to IP address group .	Adding a Network ACL Rule (Default Effective Sequence) <ul style="list-style-type: none">• Inbound rule: Set Source or Destination to an IP address group. Either the source or the destination can use the IP address group.• Outbound rule: Set Source or Destination to an IP address group. Either the source or the destination can use the IP address group.

6.2.3 Modifying an IP Address Group



Scenarios

This section describes how to modify an IP address group.

NOTE

After an IP address group is modified, the source of its associated security group rules and network ACL rules will also change.

Modifying an IP Address Group

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Access Control > IP Address Groups**.
5. On the displayed page, click **Modify** in the **Operation** column to modify the name, IP address, and description of the IP address group.

6.3 Managing IP Addresses in an IP Address Group

6.3.1 Adding IP Addresses to an IP Address Group

Scenarios

This section describes how to add IP addresses to an IP address group.

Notes and Constraints

If an IP address group has resources associated, adding IP addresses to the group may affect your network communications.

If an IP address group is associated with security groups and network ACLs, the rules associated with the IP address groups will change.

Procedure



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **IP Address Groups**.
The IP address group list is displayed.
5. In the IP address group list, click the hyperlink of the IP address group name.
The basic information page of the IP address group is displayed.
6. In the upper left corner of the IP address list, click **Add**.
The **Add IP Address** dialog box is displayed.
7. Add IP addresses to the IP address group as prompted.

Table 6-3 IP address group parameters

Parameter	Description	Example Value
Name	The name of the IP address group.	ipGroup-A

Parameter	Description	Example Value
IP Address Version	IP address version supported by an IP address group. You can select an IP address version when you create an IP address group. IP address version cannot be modified after the IP address group is created. The supported versions are as follows: <ul style="list-style-type: none">• IPv4• IPv6	IPv4
IP Addresses	Mandatory Enter an IP address or IP address range on each line, and press Enter . You can enter: <ul style="list-style-type: none">• An IPv4 address range, for example, 192.168.0.0/16• A single IPv4 address, for example, 192.168.10.10/32• An IPv6 address range, for example, 2001:db8:a583:6e::/64• A single IPv6 address, for example, 2001:db8:a583:6e::5c/128	192.168.0.0/16 192.168.10.10/32

6.3.2 Modifying IP Addresses in an IP Address Group

Scenarios



This section describes how to modify IP addresses, IP address ranges, and their descriptions in an IP address group.

Notes and Constraints

If an IP address group has resources associated, modifying IP addresses in an IP address group may affect your network communications.

If an IP address group is associated with security groups and network ACLs, the rules associated with the IP address groups will change.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **IP Address Groups**.
The IP address group list is displayed.
5. In the IP address group list, click the hyperlink of the IP address group name.
The basic information page of the IP address group is displayed.
6. In the upper left corner of the IP address list, click **Modify**.
The **Modify IP Address** dialog box is displayed.
7. Modify the information as prompted.
For details, see [Table 6-4](#).

Table 6-4 Parameters for modifying IP addresses

Parameter	Description	Example Value
Name	The name of the IP address group.	ipGroup-A
IP Address Version	IP address version supported by an IP address group. You can select an IP address version when you create an IP address group. IP address version cannot be modified after the IP address group is created. The supported versions are as follows: <ul style="list-style-type: none"> ● IPv4 ● IPv6 	IPv4
IP Addresses	Mandatory Enter an IP address or IP address range on each line, and press Enter . You can enter: <ul style="list-style-type: none"> ● An IPv4 address range, for example, 192.168.0.0/16 ● A single IPv4 address, for example, 192.168.10.10/32 ● An IPv6 address range, for example, 2001:db8:a583:6e::/64 ● A single IPv6 address, for example, 2001:db8:a583:6e::5c/128 	192.168.0.0/16 192.168.10.10/32

8. Click **OK**.
The IP address list is displayed and you can view that the IP address was modified.

6.3.3 Deleting IP Addresses from an IP Address Group

Scenarios



This section describes how to delete IP addresses from an IP address group.

Notes and Constraints

If an IP address group has resources associated, deleting IP addresses from the group may affect your network communications.

If an IP address group is associated with security groups and network ACLs, the rules associated with the IP address groups will change.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **IP Address Groups**.
The IP address group list is displayed.
5. In the IP address group list, click the hyperlink of the IP address group name.
The basic information page of the IP address group is displayed.
6. Delete IP addresses:
 - Delete a single IP address.
 - i. In the IP address list, locate the row that contains the IP address and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
 - ii. Confirm the information and click **OK**.
 - Delete IP addresses in batches.
 - i. In the IP address list, select the IP addresses to be deleted.
 - ii. Click the **Delete** button located above the IP address list.
A confirmation dialog box is displayed.
 - iii. Confirm the information and click **OK**.

7 VPC Peering Connection

7.1 VPC Peering Connection Overview

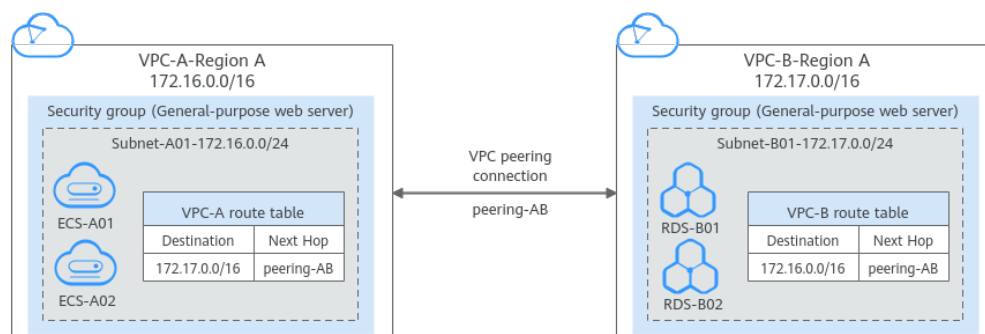
What Is a VPC Peering Connection?

A VPC peering connection is a networking connection that connects two VPCs for them to communicate using private IP addresses. The VPCs to be peered can be in the same account or different accounts, but must be in the same region.

Figure 7-1 shows an application scenario of VPC peering connections.

- There are two VPCs (VPC-A and VPC-B) in region A that are not connected.
- Service servers (ECS-A01 and ECS-A02) are in VPC-A, and database servers (RDS-B01 and RDS-B02) are in VPC-B. The service servers and database servers cannot communicate with each other.
- You need to create a VPC peering connection (peering-AB) between VPC-A and VPC-B so the service servers and database servers can communicate with each other.

Figure 7-1 VPC peering connection network diagram



NOTICE

Currently, VPC peering connections are free of charge.

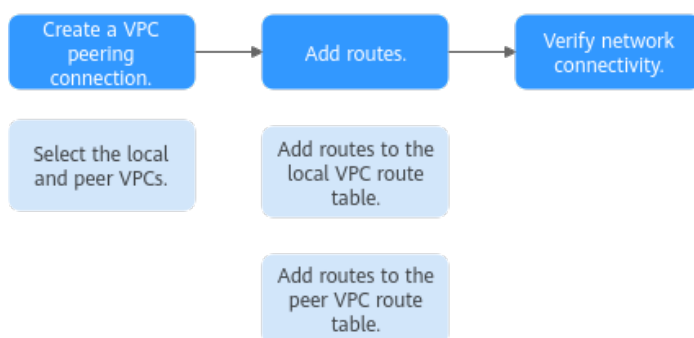
VPC Peering Connection Creation Process

A VPC peering connection can only connect VPCs in the same region.

- If two VPCs are in the same account, the process of creating a VPC peering connection is shown in [Figure 7-2](#).

For details about how to create a VPC peering connection, see [Creating a VPC Peering Connection with Another VPC in Your Account](#).

Figure 7-2 Process of creating a VPC peering connection between VPCs in the same account

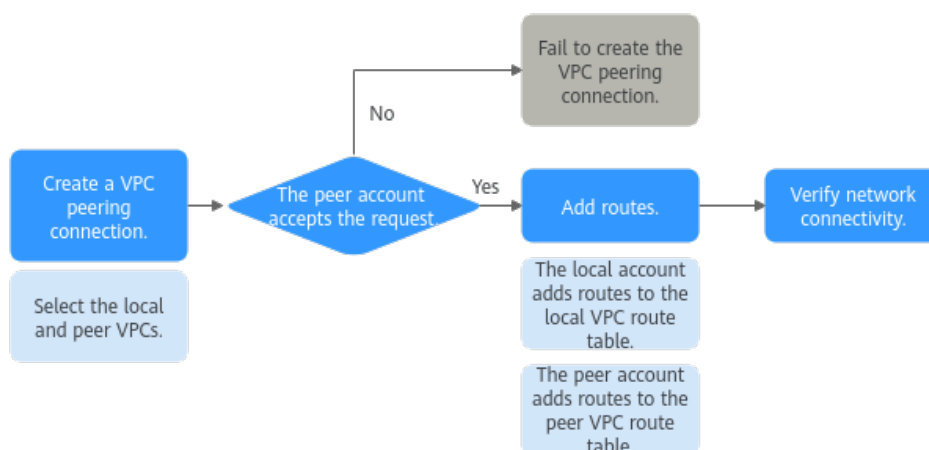


- If two VPCs are in different accounts, the process of creating a VPC peering connection is shown in [Figure 7-3](#).

For details about how to create a VPC peering connection, see [Creating a VPC Peering Connection with a VPC in Another Account](#).

If account A initiates a request to create a VPC peering connection with a VPC in account B, the VPC peering connection takes effect only after account B accepts the request.

Figure 7-3 Process of creating a VPC peering connection between VPCs in different accounts



Notes and Constraints

- A VPC peering connection can only connect VPCs in the same region.
 - If you only need few ECSs in different regions to communicate with each other, you can [assign and bind EIPs to the ECSs](#).

- If the local and peer VPCs have overlapping CIDR blocks, the VPC peering connection may not take effect.
- By default, if VPC A is peered with VPC B that has EIPs, VPC A cannot use EIPs in VPC B to access the Internet. To enable this, you can use the NAT Gateway service or configure an SNAT server. For details, see [Enabling Internet Connectivity for an ECS Without an EIP](#).

7.2 VPC Peering Connection Usage Examples

A VPC peering connection is a networking connection between two VPCs in the same region and enables them to communicate. [Table 7-1](#) lists different scenarios of using VPC peering connections.

Table 7-1 VPC peering connection usage examples

Location	CIDR Block	Description	Usage Example
VPCs in the same region	<ul style="list-style-type: none"> • VPC CIDR blocks do not overlap. • Subnet CIDR blocks of VPCs do not overlap. 	You can create VPC peering connections to connect entire CIDR blocks of VPCs. Then, all resources in the VPCs can communicate with each other.	<ul style="list-style-type: none"> • Peering Two or More VPCs • Peering One Central VPC with Multiple VPCs
VPCs in the same region	<ul style="list-style-type: none"> • VPC CIDR blocks overlap. • Some subnet CIDR blocks overlap. 	<p>You can create VPC peering connections to connect specific subnets or ECSs from different VPCs.</p> <ul style="list-style-type: none"> • To connect specific subnets from two VPCs, the subnet CIDR blocks cannot overlap. • To connect specific ECSs from two VPCs, each ECS must have a unique private IP address. 	<ul style="list-style-type: none"> • Peering Two VPCs with Overlapping CIDR Blocks • Peering ECSs in a Central VPC with ECSs in Two Other VPCs

Location	CIDR Block	Description	Usage Example
VPCs in the same region	<ul style="list-style-type: none"> VPC CIDR blocks overlap. All subnet CIDR blocks overlap. 	VPC peering connections are not usable.	<ul style="list-style-type: none"> Invalid VPC Peering Connections

Peering Two or More VPCs

- Two VPCs peered together: [Figure 7-4](#) shows the networking diagram of a VPC peering connection that connects VPC-A and VPC-B.

Figure 7-4 Networking diagram (IPv4)

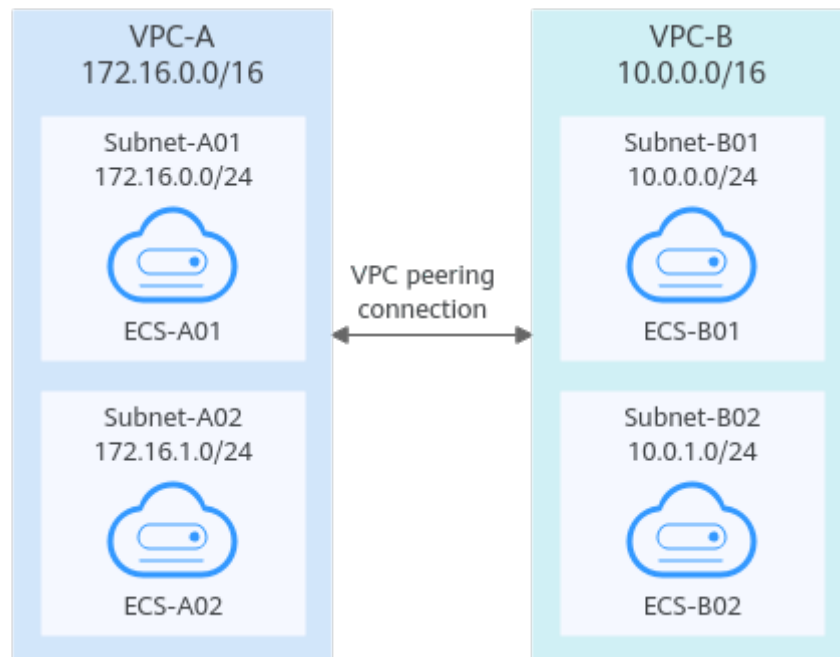


Table 7-2 Peering relationships (IPv4)

Peering Relationship	Peering Connection Name	Local VPC	Peer VPC
VPC-A is peered with VPC-B.	Peering-AB	VPC-A	VPC-B

Table 7-3 VPC route tables (IPv4)

Route Table	Destination	Next Hop	Route Type	Description
rtb-VPC-A	10.0.0.0/16	Peering-AB	Custom	Add a route with the CIDR block of VPC-B as the destination and Peering-AB as the next hop.
rtb-VPC-B	172.16.0.0/16	Peering-AB	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AB as the next hop.

- Multiple VPCs peered together: **Figure 7-5** shows the networking diagram of VPC peering connections that connect VPC-A, VPC-B, and VPC-C.

Figure 7-5 Networking diagram (IPv4)

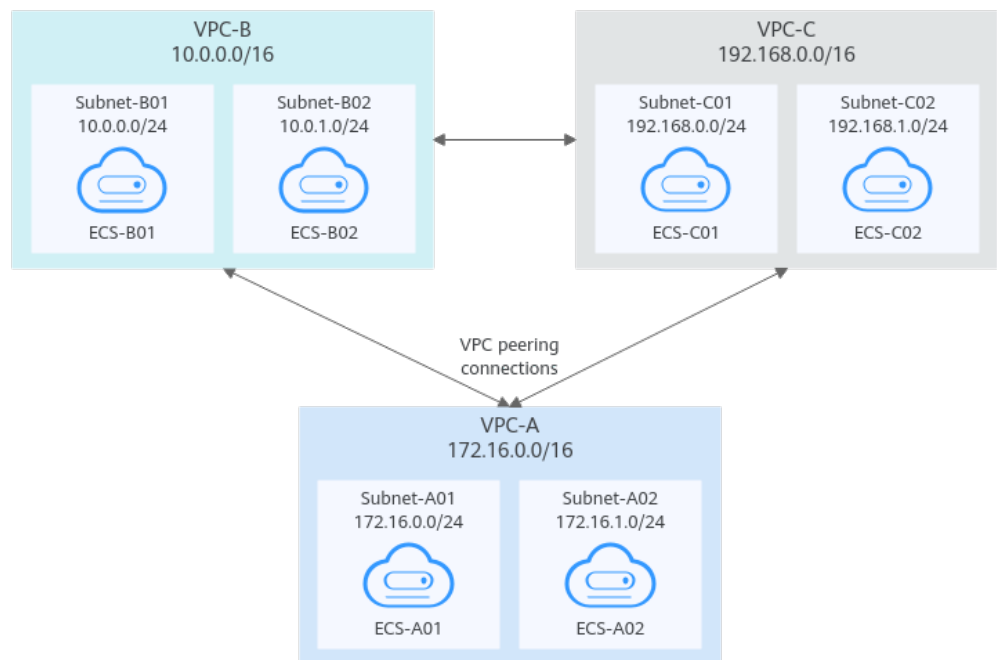


Table 7-4 Peering relationships (IPv4)

Peering Relationship	Peering Connection Name	Local VPC	Peer VPC
VPC-A is peered with VPC-B.	Peering-AB	VPC-A	VPC-B
VPC-A is peered with VPC-C.	Peering-AC	VPC-A	VPC-C

Peering Relationship	Peering Connection Name	Local VPC	Peer VPC
VPC-B is peered with VPC-C.	Peering-BC	VPC-B	VPC-C

Table 7-5 VPC route tables (IPv4)

Route Table	Destination	Next Hop	Route Type	Description
rtb-VPC-A	10.0.0.0/16	Peering-AB	Custom	Add a route with the CIDR block of VPC-B as the destination and Peering-AB as the next hop.
	192.168.0.0/16	Peering-AC	Custom	Add a route with the CIDR block of VPC-C as the destination and Peering-AC as the next hop.
rtb-VPC-B	172.16.0.0/16	Peering-AB	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AB as the next hop.
	192.168.0.0/16	Peering-BC	Custom	Add a route with the CIDR block of VPC-C as the destination and Peering-BC as the next hop.
rtb-VPC-C	172.16.0.0/16	Peering-AC	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AC as the next hop.
	10.0.0.0/16	Peering-BC	Custom	Add a route with the CIDR block of VPC-B as the destination and Peering-BC as the next hop.

Peering One Central VPC with Multiple VPCs

Figure 7-6 shows the networking diagram of VPC peering connections that connect VPC-B, VPC-C, VPC-D, VPC-E, VPC-F, VPC-G, and central VPC-A.

Figure 7-6 Networking diagram (IPv4)

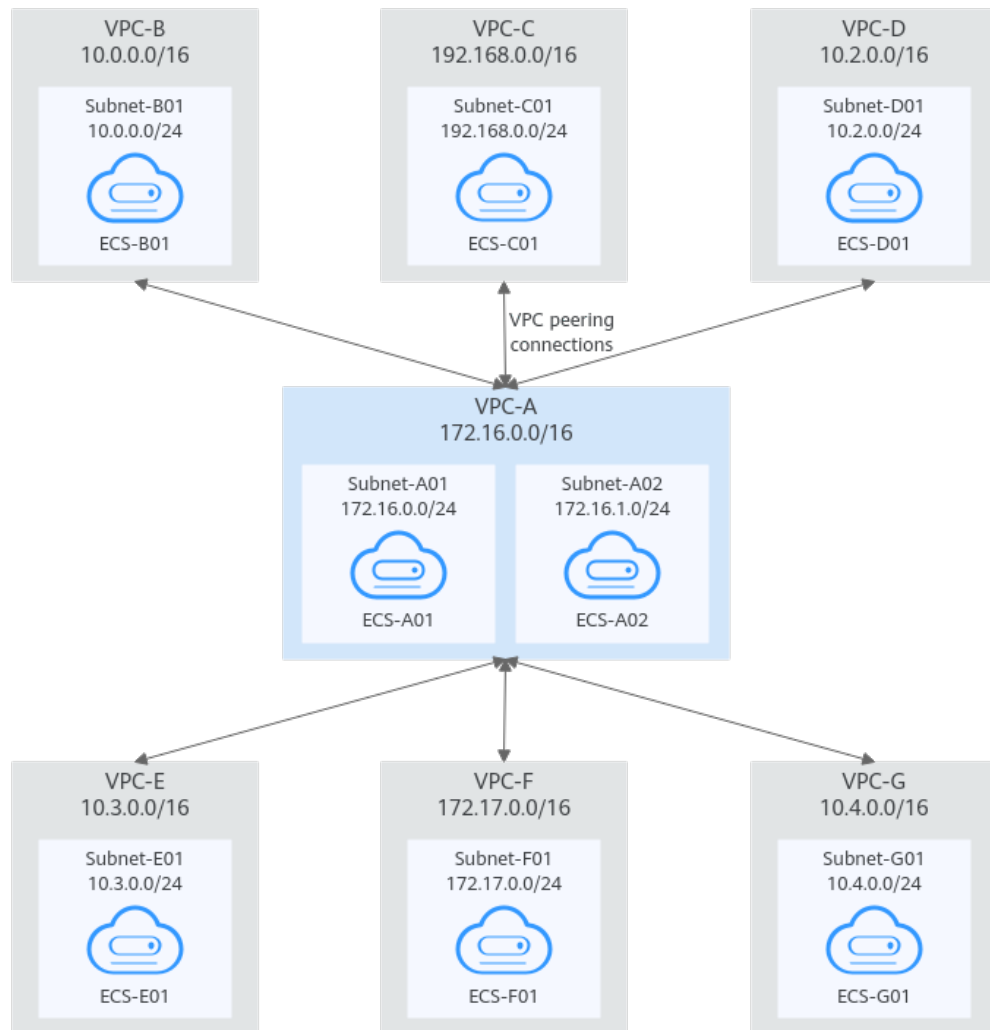


Table 7-6 Peering relationships (IPv4)

Peering Relationship	Peering Connection Name	Local VPC	Peer VPC
VPC-A is peered with VPC-B.	Peering-AB	VPC-A	VPC-B
VPC-A is peered with VPC-C.	Peering-AC	VPC-A	VPC-C
VPC-A is peered with VPC-D.	Peering-AD	VPC-A	VPC-D
VPC-A is peered with VPC-E.	Peering-AE	VPC-A	VPC-E
VPC-A is peered with VPC-F.	Peering-AF	VPC-A	VPC-F

Peering Relationship	Peering Connection Name	Local VPC	Peer VPC
VPC-A is peered with VPC-G.	Peering-AG	VPC-A	VPC-G

Table 7-7 VPC route table details (IPv4)

Route Table	Destination	Next Hop	Route Type	Description
rtb-VPC-A	10.0.0.0/16	Peering-AB	Custom	Add a route with the CIDR block of VPC-B as the destination and Peering-AB as the next hop.
	192.168.0.0/16	Peering-AC	Custom	Add a route with the CIDR block of VPC-C as the destination and Peering-AC as the next hop.
	10.2.0.0/16	Peering-AD	Custom	Add a route with the CIDR block of VPC-D as the destination and Peering-AD as the next hop.
	10.3.0.0/16	Peering-AE	Custom	Add a route with the CIDR block of VPC-E as the destination and Peering-AE as the next hop.
	172.17.0.0/16	Peering-AF	Custom	Add a route with the CIDR block of VPC-F as the destination and Peering-AF as the next hop.
	10.4.0.0/16	Peering-AG	Custom	Add a route with the CIDR block of VPC-G as the destination and Peering-AG as the next hop.
rtb-VPC-B	172.16.0.0/16	Peering-AB	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AB as the next hop.
rtb-VPC-C	172.16.0.0/16	Peering-AC	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AC as the next hop.
rtb-VPC-D	172.16.0.0/16	Peering-AD	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AD as the next hop.
rtb-VPC-E	172.16.0.0/16	Peering-AE	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AE as the next hop.

Route Table	Destination	Next Hop	Route Type	Description
rtb-VPC-F	172.16.0.0/16	Peering-AF	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AF as the next hop.
rtb-VPC-G	172.16.0.0/16	Peering-AG	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AG as the next hop.

Peering Two VPCs with Overlapping CIDR Blocks

As shown in [Figure 7-7](#), VPC-A and VPC-B have overlapping CIDR blocks, and their Subnet-A01 and Subnet-B01 also have overlapping CIDR blocks. In this case, a VPC peering connection can connect their Subnet-A02 and Subnet-B02 that do not overlap with each other.

Figure 7-7 Networking diagram (IPv4)

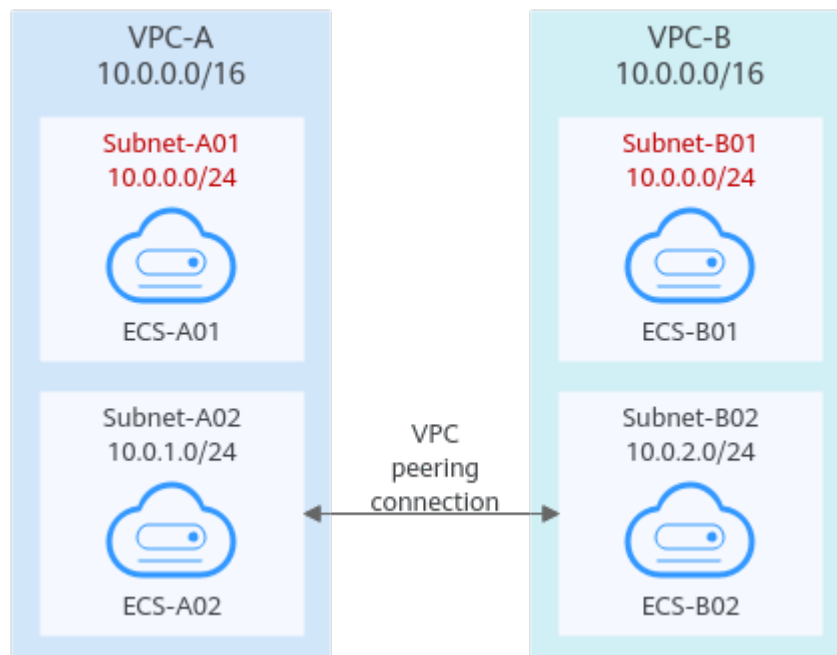


Table 7-8 Peering relationships (IPv4)

Peering Relationship	Peering Connection Name	Local VPC	Peer VPC
VPC-A is peered with VPC-B.	Peering-AB	VPC-A	VPC-B

Table 7-9 VPC route table details (IPv4)

Route Table	Destination	Next Hop	Route Type	Description
rtb-VPC-A	10.0.2.0/24	Peering-AB	Custom	Add a route with the CIDR block of Subnet-B02 as the destination and Peering-AB as the next hop.
rtb-VPC-B	10.0.1.0/24	Peering-AB	Custom	Add a route with the CIDR block of Subnet-A02 as the destination and Peering-AB as the next hop.

Peering ECSs in a Central VPC with ECSs in Two Other VPCs

As shown in [Figure 7-8](#), VPC-B and VPC-C have overlapping CIDR blocks, and their Subnet-B01 and Subnet-C01 have overlapping CIDR blocks. You can only create a VPC peering connection between ECSs.

- Use VPC peering connection Peering-AB to connect ECSs in Subnet-B01 and Subnet-A01.
- Use VPC peering connection Peering-AC to connect ECSs in Subnet-C01 and Subnet-A01.

Figure 7-8 Networking diagram (IPv4)

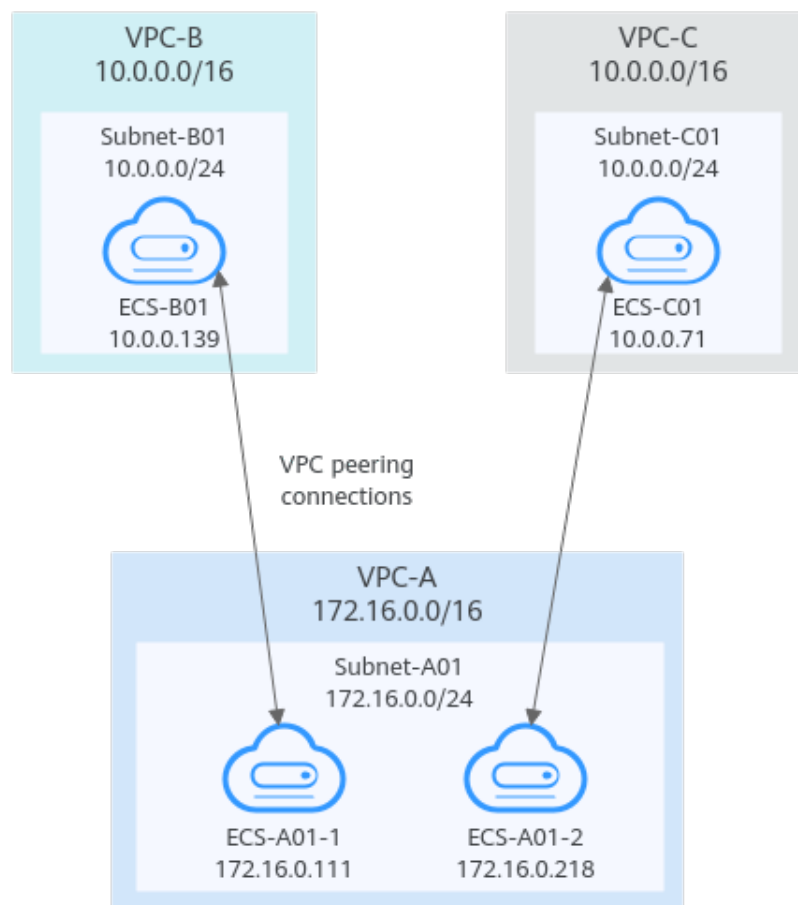


Table 7-10 Peering relationships (IPv4)

Peering Relationship	Peering Connection Name	Local VPC	Peer VPC
ECS-A01-1 in VPC-A is peered with ECS-B01 in VPC-B.	Peering-AB	VPC-A	VPC-B
ECS-A01-2 in VPC-A is peered with ECS-C01 in VPC-C.	Peering-AC	VPC-A	VPC-C

Table 7-11 VPC route table details (IPv4)

Route Table	Destination	Next Hop	Route Type	Description
rtb-VPC-A	10.0.0.13/32	Peering-AB	Custom	Add a route with the private IP address of ECS-B01 as the destination and Peering-AB as the next hop.
	10.0.0.71/32	Peering-AC	Custom	Add a route with the private IP address of ECS-C01 as the destination and Peering-AC as the next hop.
rtb-VPC-B	172.16.0.111/32	Peering-AB	Custom	Add a route with the private IP address of ECS-A01-1 as the destination and Peering-AB as the next hop.
rtb-VPC-C	172.16.0.218/32	Peering-AC	Custom	Add a route with the private IP address of ECS-A01-2 as the destination and Peering-AC as the next hop.

Invalid VPC Peering Connections

If VPCs with the same CIDR block also include subnets that overlap, VPC peering connections are not usable. VPC-A and VPC-B have the same CIDR block and their subnets have the same CIDR block. If a VPC peering connection is created between VPC-A and VPC-B, traffic cannot be routed between them because there are routes with the same destination.

In the rtb-VPC-A route table, the custom route for routing traffic from VPC-A to VPC-B and the local route have overlapping destinations. The local route has a higher priority and traffic will be forwarded within VPC-A and cannot reach VPC-B.

Figure 7-9 Networking diagram (IPv4)

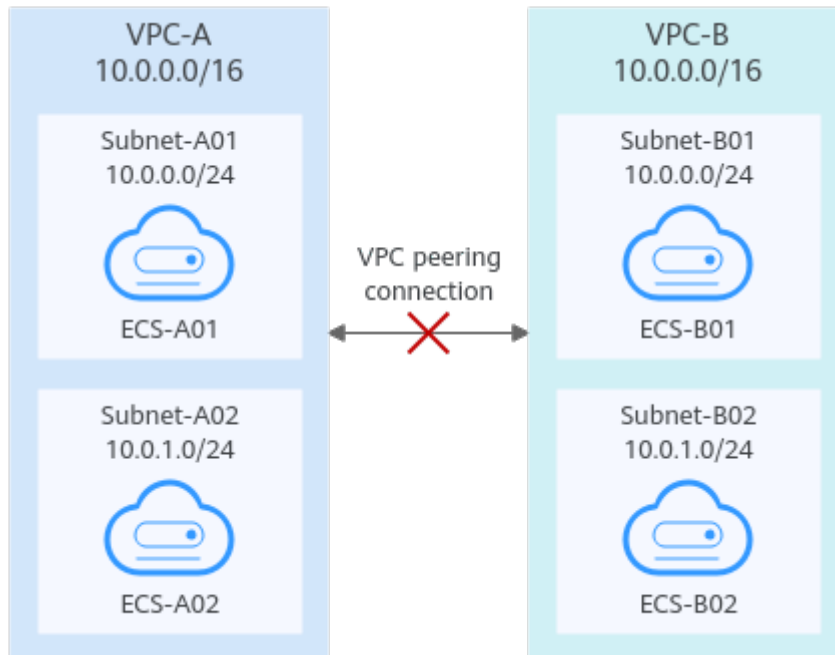


Table 7-12 VPC route table details

Route Table	Destination	Next Hop	Route Type	Description
rtb-VPC-A	10.0.0.0/24	Local	System	Local routes are automatically added for communications within a VPC.
	10.0.1.0/24	Local	System	
	10.0.0.0/16 (VPC-B)	Peering-AB	Custom	Add a route with the CIDR block of VPC-B as the destination and Peering-AB as the next hop.
rtb-VPC-B	10.0.0.0/24	Local	System	Local routes are automatically added for communications within a VPC.
	10.0.1.0/24	Local	System	
	10.0.0.0/16 (VPC-A)	Peering-AB	Custom	Add a route with the CIDR block of VPC-A as the destination and Peering-AB as the next hop.

7.3 Creating a VPC Peering Connection with Another VPC in Your Account

Scenarios

If two VPCs from the same region cannot communicate with each other, you can use a VPC peering connection. This section describes how to create a VPC peering connection between two VPCs in the same account.

This following describes how to create a VPC peering connection between VPC-A and VPC-B in account A to enable communications between ECS-A01 and RDS-B01.

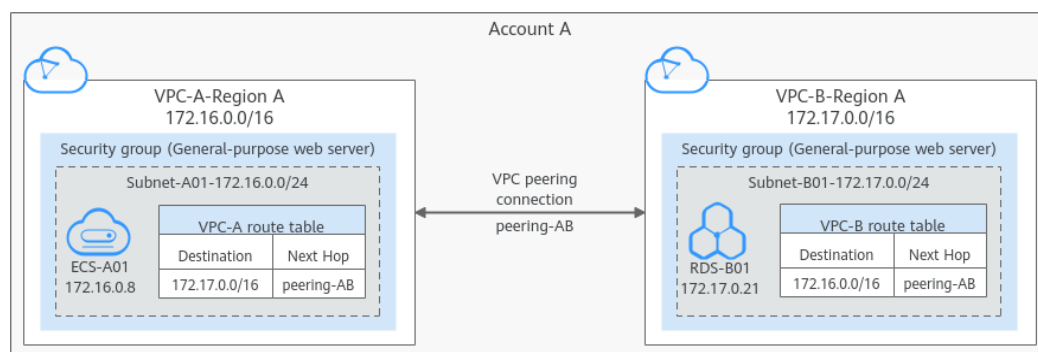
Procedure:

Step 1: Create a VPC Peering Connection

Step 2: Add Routes for the VPC Peering Connection

Step 3: Verify Network Connectivity

Figure 7-10 Networking diagram of a VPC peering connection between VPCs in the same account



NOTICE

Currently, VPC peering connections are free of charge.

Notes and Constraints

- Only one VPC peering connection can be created between two VPCs at the same time.
- A VPC peering connection can only connect VPCs in the same region.
 - If you only need few ECSs in different regions to communicate with each other, you can [assign and bind EIPs to the ECSs](#).
- If the local and peer VPCs have overlapping CIDR blocks, the VPC peering connection may not take effect.

Prerequisites

You have two VPCs from the same account in the same region. If you want to create one, see [Creating a VPC](#).

Step 1: Create a VPC Peering Connection

1. Go to the [VPC peering connection list page](#).
2. In the upper right corner of the page, click **Create VPC Peering Connection**. The **Create VPC Peering Connection** dialog box is displayed.
3. Configure the parameters as prompted.
For details, see [Table 7-13](#).

Figure 7-11 Create VPC Peering Connection

Create VPC Peering Connection

Local VPC Settings

* Name

* Local VPC

Local VPC CIDR Block 172.16.0.0/16

Peer VPC Settings

* Account My account Another account

* Peer Project

* Peer VPC

Peer VPC CIDR Block 172.17.0.0/16

Table 7-13 Parameters for creating a VPC peering connection

Parameter	Description	Example Value
Name	Mandatory Enter a name for the VPC peering connection. The name can contain a maximum of 64 characters, including letters, digits, hyphens (-), and underscores (_).	peering-AB
Local VPC	Mandatory VPC at one end of the VPC peering connection. You can select one from the drop-down list.	VPC-A
Local VPC CIDR Block	CIDR block of the selected local VPC	172.16.0.0/16
Account	Mandatory <ul style="list-style-type: none">Options: My account and Another accountSelect My account.	My account
Peer Project	The system fills in the corresponding project by default because My account is set to Account . For example, if VPC-A and VPC-B are in account A and region A, the system fills in the correspond project of account A in region A by default.	ab-cdef-1
Peer VPC	This parameter is mandatory if Account is set to My account . VPC at the other end of the VPC peering connection. You can select one from the drop-down list.	VPC-B
Peer VPC CIDR Block	CIDR block of the selected peer VPC If the local and peer VPCs have overlapping CIDR blocks, the VPC peering connection may not take effect. For details, see VPC Peering Connection Usage Examples .	172.17.0.0/16

Parameter	Description	Example Value
Description	Optional Enter the description of the VPC peering connection in the text box as required.	peering-AB connects VPC-A and VPC-B.

4. Click **OK**.
A dialog box for adding routes is displayed.
5. Click **Add Route** or **Add Later**.
 - a. If you click **Add Route**, the **Local Routes** page is displayed. Then, go to [Step 2: Add Routes for the VPC Peering Connection](#).
 - b. If you click **Add Later**, the VPC peering connection list is displayed.

Step 2: Add Routes for the VPC Peering Connection

To enable communications between VPCs connected by a VPC peering connection, you need to add forward and return routes to the route tables of the VPCs. For details, see [VPC Peering Connection Usage Examples](#).

1. Add routes to the route table of the local VPC:
 - a. On the **Local Routes** tab of the VPC peering connection, click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the local VPC is displayed.
 - b. Click **Add Route**.
[Table 7-14](#) describes the route parameters.

Table 7-14 Parameter description

Parameter	Description	Example Value
Destination	The peer VPC CIDR block, subnet CIDR block, or ECS IP address. For details, see VPC Peering Connection Usage Examples .	VPC-B CIDR block: 172.17.0.0/16
Next Hop Type	The next hop type. Select VPC peering connection .	VPC peering connection
Next Hop	The next hop address. Select the name of the current VPC peering connection.	peering-AB
Description	Supplementary information about the route. This parameter is optional. The route description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

- c. Click **OK**.
You can view the route in the route list.
2. Add routes to the route table of the peer VPC:
 - a. On the **Peer Routes** tab of the VPC peering connection, click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the peer VPC is displayed.
 - b. Click **Add Route**.
Table 7-15 describes the route parameters.

Table 7-15 Parameter description

Parameter	Description	Example Value
Destination	The local VPC CIDR block, subnet CIDR block, or ECS IP address. For details, see VPC Peering Connection Usage Examples .	VPC-A CIDR block: 172.16.0.0/16
Next Hop Type	The next hop type. Select VPC peering connection .	VPC peering connection
Next Hop	The next hop address. Select the name of the current VPC peering connection.	peering-AB
Description	Supplementary information about the route. This parameter is optional. The route description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

- c. Click **OK**.
You can view the route in the route list.

Step 3: Verify Network Connectivity

After you add routes for the VPC peering connection, verify the communication between the local and peer VPCs.

1. Log in to ECS-A01 in the local VPC.
2. Check whether ECS-A01 can communicate with RDS-B01.

ping *IP address of RDS-B01*

Example command:

ping 172.17.0.21

If information similar to the following is displayed, ECS-A01 and RDS-B01 can communicate with each other, and the VPC peering connection between VPC-A and VPC-B is successfully created.

```
[root@ecs-A02 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
```

```
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

NOTICE

- In this example, ECS-A01 and RDS-B01 are in the same security group. If the instances in different security groups, you need to add inbound rules to allow access from the peer security group. For details, see [Enabling Communications Between Instances in Different Security Groups](#).
- If VPCs connected by a VPC peering connection cannot communicate with each other, refer to [Why Did Communication Fail Between VPCs That Were Connected by a VPC Peering Connection?](#)

7.4 Creating a VPC Peering Connection with a VPC in Another Account

Scenarios

If two VPCs from the same region cannot communicate with each other, you can use a VPC peering connection. This section describes how to create a VPC peering connection between two VPCs in different accounts.

This following describes how to create a VPC peering connection between VPC-A in account A and VPC-B in account B to enable communications between ECS-A01 and RDS-B01.

Procedure:

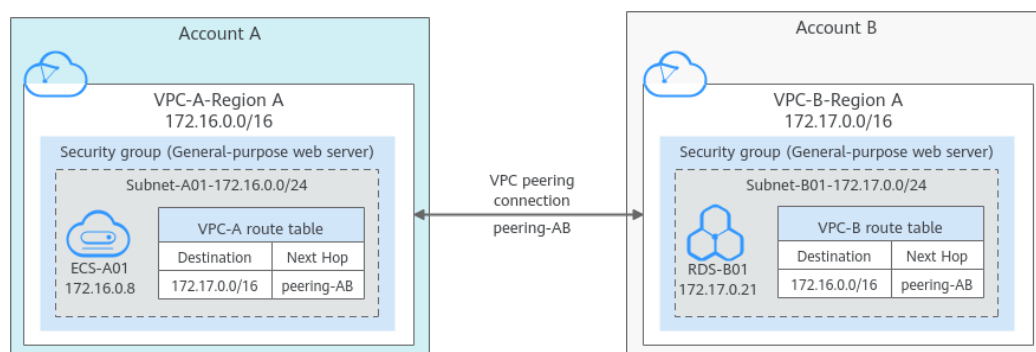
Step 1: Create a VPC Peering Connection

Step 2: Peer Account Accepts the VPC Peering Connection Request

Step 3: Add Routes for the VPC Peering Connection

Step 4: Verify Network Connectivity

Figure 7-12 Networking diagram of a VPC peering connection between VPCs in different accounts



NOTICE

Currently, VPC peering connections are free of charge.

Notes and Constraints

- Only one VPC peering connection can be created between two VPCs at the same time.
- A VPC peering connection can only connect VPCs in the same region.
 - If you only need few ECSs in different regions to communicate with each other, you can [assign and bind EIPs to the ECSs](#).
- If the local and peer VPCs have overlapping CIDR blocks, the VPC peering connection may not take effect.
- For a VPC peering connection between VPCs in different accounts:
 - If account A initiates a request to create a VPC peering connection with a VPC in account B, the VPC peering connection takes effect only after account B accepts the request.
 - To ensure network security, do not accept VPC peering connections from unknown accounts.

Prerequisites

You have two VPCs in the same region, but they are from different accounts. If you want to create one, see [Creating a VPC](#).

Step 1: Create a VPC Peering Connection

1. Go to the [VPC peering connection list page](#).
2. In the upper right corner of the page, click **Create VPC Peering Connection**. The **Create VPC Peering Connection** dialog box is displayed.
3. Configure the parameters as prompted.
For details, see [Table 7-16](#).

Figure 7-13 Create VPC Peering Connection

✕

i A VPC peering connection allows two VPCs to communicate with each other if they are in the same region.
If you need two VPCs in different regions to communicate with each other, use [Cloud Connect](#).

Create VPC Peering Connection

Local VPC Settings

★ Name

★ Local VPC ↕ ↻

Local VPC CIDR Block 172.16.0.0/16

Peer VPC Settings

★ Account My account Another account ?

The VPC peering connection will be activated only after the peer account accepts the connection request.

★ Peer Project ID ?

★ Peer VPC ID

Description

OK
Cancel

Table 7-16 Parameters for creating a VPC peering connection

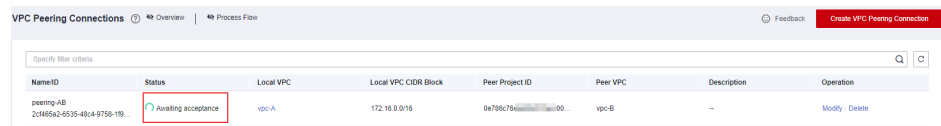
Parameter	Description	Example Value
Name	Mandatory Enter a name for the VPC peering connection. The name can contain a maximum of 64 characters, including letters, digits, hyphens (-), and underscores (_).	peering-AB
Local VPC	Mandatory VPC at one end of the VPC peering connection. You can select one from the drop-down list.	VPC-A

Parameter	Description	Example Value
Local VPC CIDR Block	CIDR block of the selected local VPC	172.16.0.0/16
Account	Mandatory <ul style="list-style-type: none">Options: My account and Another accountSelect Another account.	Another account
Peer Project ID	This parameter is mandatory because Account is set to Another account . The project ID of the region that the peer VPC resides. For details about how to obtain the project ID, see Obtaining the Peer Project ID of a VPC Peering Connection .	Project ID of VPC-B in region A: 067cf8aecf3XXX08322f13b
Peer VPC ID	This parameter is mandatory because Account is set to Another account . ID of the VPC at the other end of the VPC peering connection. For details about how to obtain the ID, see Obtaining a VPC ID .	VPC-B ID: 17cd7278-XXX-530c952dcf35
Description	Optional Enter the description of the VPC peering connection in the text box as required. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	peering-AB connects VPC-A and VPC-B.

4. Click **OK**.

- If the message "Invalid VPC ID and project ID." is displayed, check whether the project ID and VPC ID are correct.
 - Peer Project ID: The value must be the project ID of the region where the peer VPC resides.
 - The local and peer VPCs must be in the same region.
- If the status of the created VPC peering connection is **Awaiting acceptance**, go to [Step 2: Peer Account Accepts the VPC Peering Connection Request](#).

Figure 7-14 Awaiting acceptance



The screenshot shows the 'VPC Peering Connections' page with a table containing one entry. The 'Status' column for this entry is highlighted with a red box and contains the text 'Awaiting acceptance'.

NameID	Status	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Description	Operation
peering-AB 2046542-6535-4804-8758-195...	Awaiting acceptance	vpc-A	172.16.0.0/16	04786c7b...	vpc-B	--	Modify Delete

Step 2: Peer Account Accepts the VPC Peering Connection Request

After you create a VPC peering connection with a VPC in another account, you need to contact the peer account to accept the VPC peering connection request. In this example, account A notifies account B to accept the request. Account B needs to:


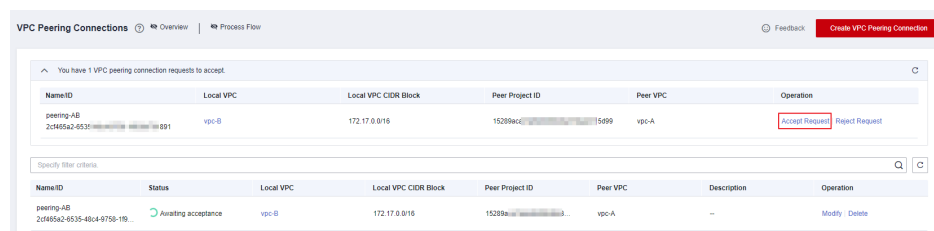
1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
4. In the upper part of the VPC peering connection list, locate the VPC peering connection request to be accepted.

Figure 7-15 Accept Request



The screenshot shows the 'VPC Peering Connections' page with a table containing one entry. The 'Operation' column for this entry has two buttons: 'Accept Request' (highlighted with a red box) and 'Reject Request'.

NameID	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Operation
peering-AB 2046542-6535-4804-8758-195...	vpc-B	172.17.0.0/16	15289ac...	vpc-A	Accept Request Reject Request

5. Locate the row that contains the target VPC peering connection and click **Accept Request** in the **Operation** column.
After the status of the VPC peering connection changes to **Accepted**, the VPC peering connection is created.
6. Go to [Step 3: Add Routes for the VPC Peering Connection](#).

Step 3: Add Routes for the VPC Peering Connection

To enable communications between VPCs connected by a VPC peering connection, you need to add forward and return routes to the route tables of the VPCs. For details, see [VPC Peering Connection Usage Examples](#).

Both accounts need to add a route to the route table of their VPC. In this example, account A adds a route to the route table of VPC-A, and account B adds a route to the route table of VPC-B.

1. Add routes to the route table of the local VPC:
 - a. In the VPC peering connection list of the local account, click the name of the target VPC peering connection.

- The **Basic Information** tab of the VPC peering connection is displayed.
- b. On the **Local Routes** tab of the VPC peering connection, click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the local VPC is displayed.
 - c. Click **Add Route**.
Table 7-17 describes the route parameters.

Table 7-17 Parameter description

Parameter	Description	Example Value
Destination	The peer VPC CIDR block, subnet CIDR block, or ECS IP address. For details, see VPC Peering Connection Usage Examples .	VPC-B CIDR block: 172.17.0.0/16
Next Hop Type	The next hop type. Select VPC peering connection .	VPC peering connection
Next Hop	The next hop address. Select the name of the current VPC peering connection.	peering-AB
Description	Supplementary information about the route. This parameter is optional. The route description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

- d. Click **OK**.
You can view the route in the route list.
2. Add routes to the route table of the peer VPC:
 - a. In the VPC peering connection list of the peer account, click the name of the target VPC peering connection.
The **Basic Information** tab of the VPC peering connection is displayed.
 - b. On the **Local Routes** tab of the VPC peering connection, click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the peer VPC is displayed.
 - c. Click **Add Route**.
Table 7-18 describes the route parameters.

Table 7-18 Parameter description

Parameter	Description	Example Value
Destination	The local VPC CIDR block, subnet CIDR block, or ECS IP address. For details, see VPC Peering Connection Usage Examples .	VPC-A CIDR block: 172.16.0.0/16
Next Hop Type	The next hop type. Select VPC peering connection .	VPC peering connection
Next Hop	The next hop address. Select the name of the current VPC peering connection.	peering-AB
Description	Supplementary information about the route. This parameter is optional. The route description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

- d. Click **OK**.

You can view the route in the route list.

Step 4: Verify Network Connectivity

After you add routes for the VPC peering connection, verify the communication between the local and peer VPCs.

1. Log in to ECS-A01 in the local VPC.
2. Check whether ECS-A01 can communicate with RDS-B01.

ping *IP address of RDS-B01*

Example command:

ping 172.17.0.21

If information similar to the following is displayed, ECS-A01 and RDS-B01 can communicate with each other, and the VPC peering connection between VPC-A and VPC-B is successfully created.

```
[root@ecs-A02 ~]# ping 172.17.0.21
PING 172.17.0.21 (172.17.0.21) 56(84) bytes of data.
64 bytes from 172.17.0.21: icmp_seq=1 ttl=64 time=0.849 ms
64 bytes from 172.17.0.21: icmp_seq=2 ttl=64 time=0.455 ms
64 bytes from 172.17.0.21: icmp_seq=3 ttl=64 time=0.385 ms
64 bytes from 172.17.0.21: icmp_seq=4 ttl=64 time=0.372 ms
...
--- 172.17.0.21 ping statistics ---
```

NOTICE

- In this example, ECS-A01 and RDS-B01 are in the same security group. If the instances in different security groups, you need to add inbound rules to allow access from the peer security group. For details, see [Enabling Communications Between Instances in Different Security Groups](#).
- If VPCs connected by a VPC peering connection cannot communicate with each other, refer to [Why Did Communication Fail Between VPCs That Were Connected by a VPC Peering Connection?](#)

7.5 Obtaining the Peer Project ID of a VPC Peering Connection

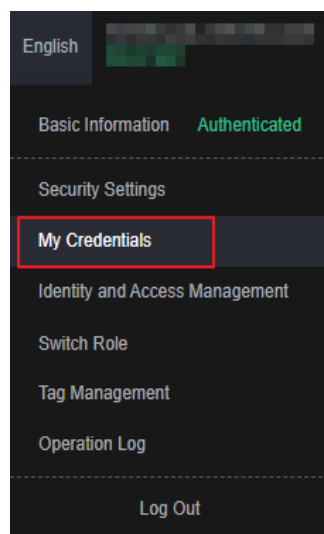
Scenarios

If you create a VPC peering connection between two VPCs in different accounts, you can refer to this section to obtain the project ID of the region that the peer VPC resides.

Procedure

1. Log in to the management console.
The owner of the peer account logs in to the management console.
2. In the upper right corner of the page, select **My Credentials** from the username drop-down list.
The **My Credentials** page is displayed.

Figure 7-16 My Credentials



3. In the project list, obtain the project ID.
Locate the region of the peer VPC and obtain the project ID corresponding to the region.

Figure 7-17 Project ID

Projects

Project ID	Project Name	Region
067	13b	4
92f	4d5	9
152	5d99	3
857	5ad	-1
59f	8ba5	4



7.6 Modifying a VPC Peering Connection

Scenarios

This section describes how to modify the basic information about a VPC peering connection, including its name and description.

Either owner of a VPC in a peering connection can modify the VPC peering connection in any state.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
5. In the VPC peering connection list, locate the row that contains the target VPC peering connection and click **Modify** in the **Operation** column.
The **Modify VPC Peering Connection** dialog box is displayed.
6. Modify the VPC peering connection information and click **OK**.



7.7 Viewing VPC Peering Connections

Scenarios

This section describes how to view basic information about a VPC peering connection, including the connection name, status, and information about the local and peer VPCs.

If a VPC peering connection is created between two VPCs in different accounts, both the local and peer accounts can view information about the VPC peering connection.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
5. In the VPC peering connection list, click the name of the target VPC peering connection.
On the displayed page, view details about the VPC peering connection.

7.8 Deleting a VPC Peering Connection

Scenarios



This section describes how to delete a VPC peering connection.

Either owner of a VPC in a peering connection can delete the VPC peering connection in any state.

Notes and Constraints

The owner of either VPC in a peering connection can delete the VPC peering connection at any time. Deleting a VPC peering connection will also delete all information about this connection, including the routes in the local and peer VPC route tables added for the connection.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
5. In the VPC peering connection list, locate the row that contains the target VPC peering connection and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
6. Click **Yes**.

7.9 Modifying Routes Configured for a VPC Peering Connection



Scenarios

This section describes how to modify the routes added for a VPC peering connection in the route tables of the local and peer VPCs.

- [Modifying Routes of a VPC Peering Connection Between VPCs in the Same Account](#)
- [Modifying Routes of a VPC Peering Connection Between VPCs in Different Accounts](#)

You can follow the instructions provided in this section to modify routes based on your requirements.



Modifying Routes of a VPC Peering Connection Between VPCs in the Same Account

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
5. In the VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
6. Modify the route added to the route table of the local VPC:
 - a. Click the **Local Routes** tab and then click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the local VPC is displayed.
 - b. Locate the row that contains the route to be modified and click **Modify** in the **Operation** column.
The **Modify Route** dialog box is displayed.
 - c. Modify the route and click **OK**.
7. Modify the route added to the route table of the peer VPC:
 - a. Click the **Peer Routes** tab and then click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the peer VPC is displayed.
 - b. Locate the row that contains the route to be modified and click **Modify** in the **Operation** column.

- The **Modify Route** dialog box is displayed.
- c. Modify the route and click **OK**.

Modifying Routes of a VPC Peering Connection Between VPCs in Different Accounts

Only the account owner of a VPC can modify the routes added for the connection.

1. Log in to the management console using the account of the local VPC and modify the route of the local VPC:
 - a. Click  in the upper left corner and select the desired region and project.
 - b. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
 - c. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
 - d. In the VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
 - e. Modify the route added to the route table of the local VPC:
 - i. Click the **Local Routes** tab and then click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the local VPC is displayed.
 - ii. Locate the row that contains the route to be modified and click **Modify** in the **Operation** column.
The **Modify Route** dialog box is displayed.
 - iii. Modify the route and click **OK**.
2. Log in to the management console using the account of the peer VPC and modify the route of the peer VPC by referring to [1](#).

7.10 Viewing Routes Configured for a VPC Peering Connection



Scenarios

This section describes how to view the routes added to the route tables of local and peer VPCs of a VPC peering connection.

- [Viewing Routes of a VPC Peering Connection Between VPCs in the Same Account](#)
- [Viewing Routes of a VPC Peering Connection Between VPCs in Different Accounts](#)



If two VPCs cannot communicate through a VPC peering connection, you can check the routes added for the local and peer VPCs by following the instructions provided in this section.

Viewing Routes of a VPC Peering Connection Between VPCs in the Same Account

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
5. In the VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
6. View the routes added for the VPC peering connection:
 - a. Click the **Local Routes** tab to view the local route added for the VPC peering connection.
 - b. Click the **Peer Routes** tab to view the peer route added for the VPC peering connection.

Viewing Routes of a VPC Peering Connection Between VPCs in Different Accounts

Only the account owner of a VPC in a VPC peering connection can view the routes added for the connection.

1. Log in to the management console using the account of the local VPC and view the route of the local VPC:
 - a. Click  in the upper left corner and select the desired region and project.
 - b. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
 - c. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
 - d. In the VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
 - e. Click the **Local Routes** tab to view the local route added for the VPC peering connection.

2. Log in to the management console using the account of the peer VPC and view the route of the peer VPC by referring to 1.



7.11 Deleting Routes Configured for a VPC Peering Connection

Scenarios

This section describes how to delete routes from the route tables of the local and peer VPCs connected by a VPC peering connection.

- [Deleting Routes of a VPC Peering Connection Between VPCs in the Same Account](#)
- [Deleting Routes of a VPC Peering Connection Between VPCs in Different Accounts](#)



Deleting Routes of a VPC Peering Connection Between VPCs in the Same Account

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
5. In the VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
6. Delete the route added to the route table of the local VPC:
 - a. Click the **Local Routes** tab and then click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the local VPC is displayed.
 - b. Locate the row that contains the route to be deleted and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
 - c. Click **Yes**.
7. Delete the route added to the route table of the peer VPC:
 - a. Click the **Peer Routes** tab and then click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the peer VPC is displayed.
 - b. Locate the row that contains the route to be deleted and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.

- c. Click **Yes**.

Deleting Routes of a VPC Peering Connection Between VPCs in Different Accounts

Only the account owner of a VPC in a VPC peering connection can delete the routes added for the connection.

1. Log in to the management console using the account of the local VPC and delete the route of the local VPC:
 - a. Click  in the upper left corner and select the desired region and project.
 - b. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
 - c. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
 - d. In the VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
 - e. Delete the route added to the route table of the local VPC:
 - i. Click the **Local Routes** tab and then click the **Route Tables** hyperlink.
The **Summary** tab of the default route table for the local VPC is displayed.
 - ii. Locate the row that contains the route to be deleted and click **Delete** in the **Operation** column.
A confirmation dialog box is displayed.
 - iii. Click **Yes**.
2. Log in to the management console using the account of the peer VPC and delete the route of the peer VPC by referring to [1](#).

8 VPC Flow Log

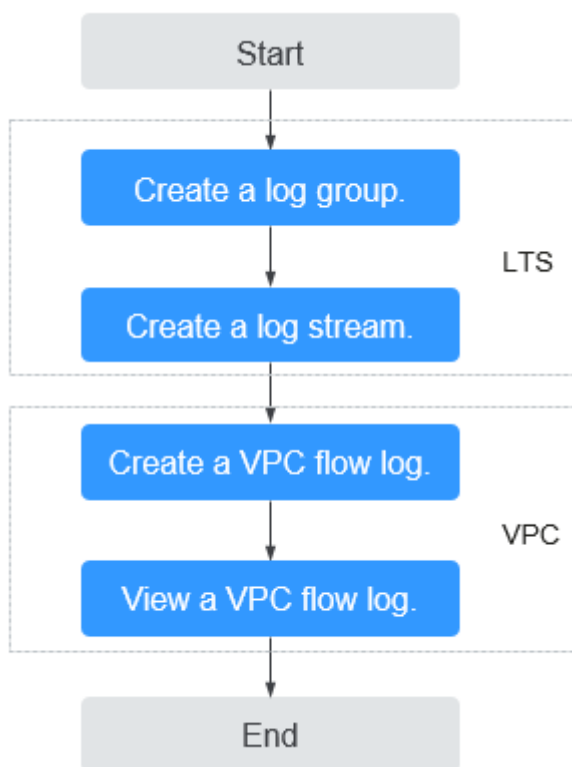
8.1 VPC Flow Log Overview

What Is a VPC Flow Log?

A VPC flow log records information about the traffic going to and from a VPC. VPC flow logs help you monitor network traffic, analyze network attacks, and determine whether security group and network ACL rules require modification.

VPC flow logs must be used together with the Log Tank Service (LTS). Before you create a VPC flow log, you need to create a log group and a log stream in LTS.

Figure 8-1 shows the process for configuring VPC flow logs.

Figure 8-1 Configuring VPC flow logs

The VPC flow log function itself is free of charge, but you may be charged for other resources used. For example, the storage of VPC flow log records will be charged. For details, see *Log Tank Service User Guide*.

Notes and Constraints

- Currently, S2, M2, Hc2, D2, Pi1, S3, C3, M3, H3, Ir3, I3, S6, E3, C3ne, M3ne, G5, P2v, C6, M6, Pi1, and H3 ECSs support VPC flow logs.
For details about ECS types, see [ECS Types](#).
- Each account can have up to 10 VPC flow logs in a region.

8.2 Creating a VPC Flow Log

Scenarios

A VPC flow log records information about the traffic going to and from a VPC.

Prerequisites

Ensure that the following operations have been performed on the LTS console:

- Create a log group.
- Create a log stream.

For more information about the LTS service, see the *Log Tank Service User Guide*.

Procedure

1. Go to the [VPC flow log list page](#).
2. In the upper right corner, click **Create VPC Flow Log**. On the displayed page, configure parameters as prompted.

Table 8-1 Parameter descriptions

Parameter	Description	Example Value
Name	The VPC flow log name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	flowlog-495d
Resource Type	The type of resources whose traffic is to be logged. You can select NIC , Subnet , or VPC .	NIC
Resource	The specific NIC whose traffic is to be logged. NOTE We recommend that you select an ECS that is in the running state. If an ECS in the stopped state is selected, restart the ECS after creating the VPC flow log for accurately recording the information about the traffic going to and from the ECS NIC.	N/A
Filter	<ul style="list-style-type: none">● All traffic: specifies that both accepted and rejected traffic of the specified resource will be logged.● Accepted traffic: specifies that only accepted traffic of the specified resource will be logged. Accepted traffic refers to the traffic permitted by the security group or network ACL.● Rejected traffic: specifies that only rejected traffic of the specified resource will be logged. Rejected traffic refers to the traffic denied by the network ACL.	All
Log Group	The log group created in LTS.	lts-group-abc
Log Stream	The log stream created in LTS.	lts-topic-abc
Description	Supplementary information about the VPC flow log. This parameter is optional. The VPC flow log description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

 NOTE

Only two flow logs, each with a different filter, can be created for a single resource under the same log group and log stream. Each VPC flow log must be unique.

3. Click **OK**.

8.3 Viewing a VPC Flow Log

Scenarios



View information about your flow log record.

The capture window is approximately 10 minutes, which indicates that a flow log record will be generated every 10 minutes. After creating a VPC flow log, you need to wait about 10 minutes before you can view the flow log record.

 NOTE

If an ECS is in the stopped state, its flow log records will not be displayed.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **VPC Flow Logs**.
5. Locate the target VPC flow log and click **View Log Record** in the **Operation** column to view information about the flow log record in LTS.

The flow log record is in the following format:

```
<version> <project-id> <interface-id> <srcaddr> <dstaddr> <srcport> <dstport> <protocol> <packets>  
<bytes> <start> <end> <action> <log-status>
```

Example 1: The following is an example of a flow log record in which data was recorded during the capture window:

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd 192.168.0.154  
192.168.3.25 38929 53 17 1 96 1548752136 1548752736 ACCEPT OK
```

Value **1** indicates the VPC flow log version. Traffic with a size of 96 bytes to NIC **1d515d18-1b36-47dc-a983-bd6512aed4bd** during the past 10 minutes (from 16:55:36 to 17:05:36 on January 29, 2019) was allowed. A data packet was transmitted over the UDP protocol from source IP address **192.168.0.154** and port **38929** to destination IP address **192.168.3.25** and port **53**.

Example 2: The following is an example of a flow log record in which no data was recorded during the capture window:

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - - - -  
1431280876 1431280934 - NODATA
```

Example 3: The following is an example of a flow log record in which data was skipped during the capture window:

```
1 5f67944957444bd6bb4fe3b367de8f3d 1d515d18-1b36-47dc-a983-bd6512aed4bd - - - - -
1431280876 1431280934 - SKIPDATA
```

Table 8-2 describes the fields of a flow log record.

Table 8-2 Log field description

Field	Description	Example Value
version	The VPC flow log version.	1
project-id	The project ID.	5f67944957444bd6bb4fe3b367de8f3d
interface-id	The ID of the NIC for which the traffic is recorded.	1d515d18-1b36-47dc-a983-bd6512aed4bd
srcaddr	The source IP address.	192.168.0.154
dstaddr	The destination IP address.	192.168.3.25
srcport	The source port.	38929
dstport	The destination port.	53
protocol	The Internet Assigned Numbers Authority (IANA) protocol number of the traffic. For details, see Assigned Internet Protocol Numbers .	17
packets	The number of packets transferred during the capture window.	1
bytes	The number of bytes transferred during the capture window.	96
start	The time, in Unix seconds, of the start of the capture window.	1548752136
end	The time, in Unix seconds, of the end of the capture window.	1548752736

Field	Description	Example Value
action	<p>The action associated with the traffic:</p> <ul style="list-style-type: none"> ● ACCEPT: The recorded traffic was allowed by the security groups or network ACLs. ● REJECT: The recorded traffic was denied by the security groups or network ACLs. 	ACCEPT
log-status	<p>The logging status of the VPC flow log:</p> <ul style="list-style-type: none"> ● OK: Data is logging normally to the chosen destinations. ● NODATA: There was no traffic of the Filter setting to or from the NIC during the capture window. ● SKIPDATA: Some flow log records were skipped during the capture window. This may be caused by an internal capacity constraint or an internal error. <p>Example: When Filter is set to Accepted traffic, if there is accepted traffic, the value of log-status is OK. If there is no accepted traffic, the value of log-status is NODATA regardless of whether there is rejected traffic. If some accepted traffic is abnormally skipped, the value of log-status is SKIPDATA.</p>	OK

You can enter a keyword on the log stream details page on the LTS console to search for flow log records.

8.4 Enabling or Disabling VPC Flow Log



Scenarios

After a VPC flow log is created, the VPC flow log is automatically enabled. If you do not need to record flow log data, you can disable the corresponding VPC flow log. A disabled VPC flow log can be enabled again.

Notes and Constraints

- After a VPC flow log is enabled, the system starts to collect flow logs in the next log collection period.
- After a VPC flow log is disabled, the system stops collecting flow logs in the next log collection period. Generated flow logs will still be reported.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **VPC Flow Logs**.
5. Locate the VPC flow log to be enabled or disabled, and click **Enable** or **Disable** in the **Operation** column.
6. Click **Yes**.

8.5 Deleting a VPC Flow Log



Scenarios

Delete a VPC flow log that is not required. Deleting a VPC flow log will not delete the existing flow log records in LTS.

NOTE

If a NIC that uses a VPC flow log is deleted, the flow log will be automatically deleted. However, the flow log records are not deleted.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking > Virtual Private Cloud**.

The **Virtual Private Cloud** page is displayed.

4. In the navigation pane on the left, choose **VPC Flow Logs**.
5. Locate the row that contains the VPC flow log to be deleted and click **Delete** in the **Operation** column.
6. Click **Yes** in the displayed dialog box.

9 Elastic IP

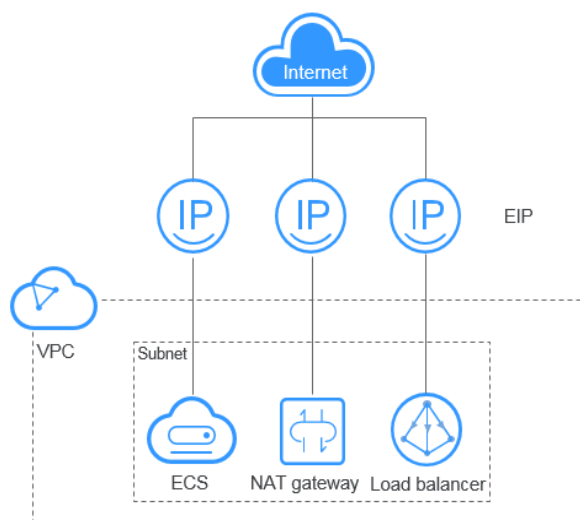
9.1 EIP Overview

EIP

The Elastic IP (EIP) service enables you to use static public IP addresses and scalable bandwidths to connect your cloud resources to the Internet. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, NAT gateways, or load balancers. Various billing modes are provided to meet diverse service requirements.

Each EIP can be bound to only one cloud resource and they must be in the same region.

Figure 9-1 Accessing the Internet using an EIP



EIP Quotas

If you want to know the number of EIPs that can be assigned in a region, see [How Do I View My Quotas?](#)

If you want to increase your quota, see [How Do I Apply for a Higher Quota?](#)

- Your request for a larger quota will only be approved if your account has valid orders and you are continuously using cloud resources. If you have released resources immediately after subscribing to them multiple times, your request for quota increase will be declined.
- If you have increased the EIP quota but you have not used the quota for a long time, Huawei Cloud will reduce the quota to the default value.

Advantages

- Flexibility
An EIP can be flexibly associated with or disassociated from the ECS, BMS, NAT gateway, load balancer, or virtual IP address. The bandwidth can be adjusted according to service changes.
- Shared bandwidth
EIPs can use shared bandwidth to lower bandwidth costs.
- Immediate use
EIP binding, unbinding, and bandwidth adjustments take effect immediately.

Notes and Constraints

- If the used EIP bandwidth exceeds the purchased size or is attacked (usually by a DDoS attack), the EIP will be blocked but can still be bound or unbound.
- EIPs cannot be transferred across accounts. That is, an EIP of account A cannot be transferred to account B.

9.2 Assigning an EIP and Binding It to an ECS


Scenarios

You can assign an EIP and bind it to an ECS so that the ECS can access the Internet.

Notes and Constraints

- Each EIP can only be bound to one cloud resource and they must be in the same region.
- If an EIP is frozen due to account arrears or security reasons, it cannot be bound or unbound.

Assigning an EIP

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.


3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. On the displayed page, click **Buy EIP**.
5. Set the parameters as prompted.

Table 9-1 Parameter descriptions

Parameter	Description	Example Value
Billing Mode	The following billing modes are available: <ul style="list-style-type: none">• Yearly/Monthly• Pay-per-use	Pay-per-use
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you. The region selected for the EIP is its geographical location.	-
EIP Type	<ul style="list-style-type: none">• Dynamic BGP: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP

Parameter	Description	Example Value
Billed By	<p>This parameter is available only when you set Billing Mode to Pay-per-use.</p> <ul style="list-style-type: none"> • Bandwidth: You specify a maximum bandwidth and pay for the amount of time you use the bandwidth. This is suitable for scenarios with heavy or stable traffic. • Traffic: You specify a maximum bandwidth and pay for the total traffic you use. This is suitable for scenarios with light or sharply fluctuating traffic. • Shared Bandwidth: The bandwidth can be shared by multiple EIPs. This is suitable for scenarios with staggered traffic. 	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
DDoS Protection	<p>Cloud Native Anti-DDoS Basic</p> <p>Cloud Native Anti-DDoS Basic provides up to 5 Gbit/s of DDoS mitigation capacity. If the attack to an EIP exceeds 5 Gbit/s, the EIP will be blocked.</p>	-
EIP Name	The EIP name.	eip-test
Enterprise Project	<p>The enterprise project that the EIP belongs to.</p> <p>An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default.</p> <p>For details about creating and managing enterprise projects, see the Enterprise Management User Guide.</p>	default
Advanced Settings	Click the drop-down arrow to configure parameters, including the bandwidth name and tag.	-
Bandwidth Name	The name of the bandwidth.	bandwidth

Parameter	Description	Example Value
Tag	The EIP tags. Each tag contains a key and value pair. The tag key and value must meet the requirements listed in Table 9-2 .	<ul style="list-style-type: none">• Key: lpv4_key1• Value: 3005eip
Monitoring	Used to monitor the EIP and enabled by default. You can use the management console or APIs provided by Cloud Eye to query the metrics and alarms generated for the EIP and bandwidth.	-
Required Duration	The duration for which the purchased EIP will use. The duration must be specified if the Billing Mode is set to Yearly/Monthly .	1 month
Quantity	The number of EIPs you want to purchase. The quantity must be specified if the Billing Mode is set to Pay-per-use .	1
Quantity	The number of EIPs you want to assign.	1

Table 9-2 EIP tag requirements

Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each EIP.• Can contain a maximum of 36 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	lpv4_key1

Parameter	Requirement	Example Value
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	3005eip

 NOTE

- If you are buying an EIP billed on a pay-per-use basis and you want to use a shared bandwidth, you can only select an existing shared bandwidth from the **Bandwidth Name** drop-down list. If there are no shared bandwidths to select, purchase a shared bandwidth first.
 - A dedicated bandwidth cannot be changed to a shared bandwidth and vice versa. However, you can purchase a shared bandwidth for pay-per-use EIPs.
 - After an EIP is added to a shared bandwidth, the EIP will use the shared bandwidth.
 - After an EIP is removed from the shared bandwidth, the EIP will use the dedicated bandwidth.
6. Click **Next**.
 7. Click **Submit**.

Binding an EIP

1. On the **EIPs** page, locate the row that contains the target EIP, and click **Bind**.
2. Select the instance that you want to bind the EIP to.
3. Click **OK**.

Helpful Links

- [How Do I Assign or Retrieve a Specific EIP?](#)
- [How Do I Access an ECS with an EIP Bound from the Internet?](#)
- [Can I Bind an EIP of an ECS to Another ECS?](#)
- [How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?](#)
- [Why Can't My ECS Access the Internet Even After an EIP Is Bound?](#)

9.3 Unbinding an EIP from an ECS and Releasing the EIP

Scenarios



If you no longer need an EIP, unbind it from the ECS and release the EIP to avoid wasting network resources.

Notes and Constraints



- Only EIPs with no instance bound can be released. If you want to release an EIP with an instance bound, you need to unbind EIP from the instance first.
- You cannot buy an EIP that has been released if it is currently in use by another user.
- If an EIP is frozen due to account arrears or security reasons, it cannot be bound or unbound.

Procedure



Unbinding a single EIP

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. On the displayed page, locate the row that contains the EIP, and click **Unbind**.
5. Click **Yes** in the displayed dialog box.



Releasing a single EIP

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. On the displayed page, locate the row that contains the target EIP, click **More** and then **Release** in the **Operation** column.
5. Click **Yes** in the displayed dialog box.

Unbinding multiple EIPs at once

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. On the displayed page, select the EIPs to be unbound.
5. Click the **Unbind** button located above the EIP list.
6. Click **Yes** in the displayed dialog box.

Releasing multiple EIPs at once

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. On the displayed page, select the EIPs to be released.
5. Click the **Release** button located above the EIP list.
6. Click **Yes** in the displayed dialog box.



9.4 Modifying an EIP Bandwidth

Scenarios

No matter which billing mode is used, if your EIP is not added to a shared bandwidth, it uses a dedicated bandwidth. A dedicated bandwidth can control how much data can be transferred using a single EIP.

This section describes how to increase or decrease the bandwidth size. Changing bandwidth size does not change the EIPs.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. Locate the target EIP, click **More** in the **Operation** column, and select **Modify Bandwidth**.
 - If it is a pay-per-use EIP, the **Modify Bandwidth** page is displayed.
 - If it is a yearly/monthly EIP, select either of the following method to increase or decrease the bandwidth and click **Continue**.
 - Increase bandwidth
 - Decrease bandwidth
5. Modify the bandwidth parameters as prompted.
6. Click **Next**.
7. Click **Submit**.

Helpful Links




- [How Do I Change the EIP Billing Option from Bandwidth to Traffic or from Traffic to Bandwidth?](#)
- [Can I Increase My Bandwidth Billed on Yearly/Monthly Basis and Then Decrease It?](#)

9.5 Exporting EIP Information

Scenarios

The information of all EIPs under your account can be exported in an Excel file to a local directory. The file records the ID, status, type, bandwidth name, and bandwidth size of EIPs.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. On the displayed page, click  in the upper right corner of the EIP list.
The system will automatically export all EIPs in the current region of your account to an Excel file and download the file to a local directory.

9.6 Managing EIP Tags

Scenarios

Tags can be added to EIPs to facilitate EIP identification and administration. You can add a tag to an EIP when assigning the EIP. Alternatively, you can add a tag to an assigned EIP on the EIP details page. A maximum of 20 tags can be added to each EIP.

A tag consists of a key and value pair. [Table 9-3](#) lists the tag key and value requirements.



Table 9-3 EIP tag requirements

Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each EIP.• Can contain a maximum of 36 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	Ipv4_key1

Parameter	Requirement	Example Value
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain only the following character types:<ul style="list-style-type: none">- Uppercase letters- Lowercase letters- Digits- Special characters, including hyphens (-) and underscores (_)	3005eip

Procedure



Searching for EIPs by tag key and value on the page showing the EIP list

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. Click the search box above the EIP list.
5. Select the tag key and value of the EIP.

You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for EIPs, the system will display only the EIPs that contain all of the tags you specified.
6. Click **OK**.

The system displays the EIPs you are looking for based on the entered tag keys and values.

Adding, deleting, editing, and viewing tags on the Tags tab of an EIP

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Networking** > **Elastic IP**.
4. On the displayed page, locate the EIP whose tags you want to manage and click the EIP name.
5. On the page showing EIP details, click the **Tags** tab and perform desired operations on tags.
 - View tags.

On the **Tags** tab, you can view details about tags added to the current EIP, including the number of tags and the key and value of each tag.
 - Add a tag.

Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.
 - Edit a tag.

Locate the row that contains the tag you want to edit, and click **Edit** in the **Operation** column. Enter the new tag value, and click **OK**.

The tag key cannot be modified.

- Delete a tag.

Locate the row that contains the tag you want to delete, and click **Delete** in the **Operation** column. In the displayed dialog box, click **Yes**.

9.7 IPv6 EIP

Overview

Both IPv4 and IPv6 EIPs are available. You can assign an IPv6 EIP or map an existing IPv4 EIP to an IPv6 EIP.

After the IPv6 EIP function is enabled, you will obtain both an IPv4 EIP and its corresponding IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

Application Scenarios of IPv4/IPv6 Dual Stack

If your ECS supports IPv6, you can use the IPv4/IPv6 dual stack. [Table 9-4](#) shows the example application scenarios.

Table 9-4 Application scenarios of IPv4/IPv6 dual stack

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Private IPv4 communication	Your applications on ECSs need to communicate with other systems (such as databases) through private networks using IPv4 addresses.	<ul style="list-style-type: none">No EIPs have been bound to the ECSs.	IPv4 CIDR Block	Private IPv4 address: used for private IPv4 communication.

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv4 communication	Your applications on ECSs need to communicate with other systems (such as databases) through public IPv4 addresses.	<ul style="list-style-type: none"> EIPs have been bound to the ECSs. 	IPv4 CIDR Block	<ul style="list-style-type: none"> Private IPv4 address: used for private IPv4 communication. Public IPv4 address: used for public IPv4 communication.

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Private IPv6 communication	Your applications on ECSs need to communicate with other systems (such as databases) through private IPv6 addresses.	<ul style="list-style-type: none"> • IPv6 has been enabled for the VPC subnet. • The network has been configured for the ECSs as follows: <ul style="list-style-type: none"> – Flavor: Any ECS flavor that supports the IPv6 network. For details, see section "x86 ECS Specifications and Types" in the Elastic Cloud Server User Guide. – VPC and Subnet: IPv6-enabled subnet and VPC. – Self-assigned IPv6 address: Selected. – Shared Bandwidth: Selected Do not configure. 	<ul style="list-style-type: none"> • IPv4 CIDR Block • IPv6 CIDR block 	<ul style="list-style-type: none"> • Private IPv4 address + IPv4 EIP: Bind an IPv4 EIP to the instance to allow public IPv4 communication. • Private IPv4 address: Do not bind any IPv4 EIP to the instance and use only the private IPv4 address to allow private IPv4 communication. • IPv6 address: Do not configure shared bandwidth for the IPv6 address to allow private IPv6 communication.

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv6 communication	An IPv6 network is required for the ECS to access the IPv6 service on the Internet.	<ul style="list-style-type: none"> IPv6 has been enabled for the VPC subnet. The network has been configured for the ECSs as follows: <ul style="list-style-type: none"> VPC and Subnet: IPv6-enabled subnet and VPC. Self-assigned IPv6 address: Selected. Shared Bandwidth: Selected a shared bandwidth. <p>NOTE For details, see Setting Up an IPv6 Network.</p>	<ul style="list-style-type: none"> IPv4 CIDR Block IPv6 CIDR block 	<ul style="list-style-type: none"> Private IPv4 address + IPv4 EIP: Bind an IPv4 EIP to the instance to allow public IPv4 communication. Private IPv4 address: Do not bind any IPv4 EIP to the instance and use only the private IPv4 address to allow private IPv4 communication. IPv6 address + shared bandwidth: Allow both private IPv6 communication and public IPv6 communication.

For details, see [IPv4 and IPv6 Dual-Stack Network](#).

Application Scenarios of IPv6 EIP

If you want an ECS to provide IPv6 services but the ECS does not support IPv6 networks or you do not want to build an IPv6 network, you can use IPv6 EIP to

quickly address your requirements. For details about application scenarios and resource planning, see [Table 9-5](#).

Table 9-5 Application scenarios and resource planning of an IPv6 EIP network (with IPv6 EIP enabled)

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv6 communication	You want to allow an ECS to provide IPv6 services for clients on the Internet without setting up an IPv6 network.	<ul style="list-style-type: none">An EIP has been bound to the ECS.IPv6 EIP has been enabled.	IPv4 CIDR Block	<ul style="list-style-type: none">Private IPv4 address: used for private IPv4 communication.IPv4 EIP (with IPv6 EIP enabled): used for public network communication through IPv4 and IPv6 addresses.

Enabling IPv6 (Assigning IPv6 EIPs)

- Method 1:
Select the **IPv6 EIP** option when you assign an EIP by referring to [Assigning an EIP and Binding It to an ECS](#) so that you can obtain both an IPv4 and an IPv6 EIP.
External IPv6 addresses can access cloud resources through this IPv6 EIP.
- Method 2:
If you want an IPv6 EIP in addition to an existing IPv4 EIP, locate the row that contains the target IPv4 EIP, click **More** in the **Operation** column, and select **Enable IPv6 EIP**. Then, a corresponding IPv6 EIP will be assigned.
After the IPv6 EIP is enabled, you will obtain both an IPv4 EIP and an IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

NOTE

There is no adverse impact on the cloud resources bound with existing IPv4 EIPs.

Configuring Security Groups

After IPv6 EIP is enabled, add inbound and outbound security group rules to allow packets to and from the IP address range **198.19.0.0/16**. [Table 9-6](#) shows the security group rules. IPv6 EIP uses NAT64 to convert the source IP address in the inbound direction to an IPv4 address in the IP address range 198.19.0.0/16. The source port can be a random one, the destination IP address is the private IPv4 address of your local server, and the destination port remains unchanged.

For details, see [Virtual Private Cloud User Guide](#).

Table 9-6 Security group rules

Direction	Protocol	Source or Destination
Inbound	All	Source: 198.19.0.0/16
Outbound	All	Destination: 198.19.0.0/16

Disabling IPv6 EIP

If you do not need the IPv6 EIP, locate the row that contains its corresponding IPv4 EIP, click **More** in the **Operation** column, and select **Disable IPv6 EIP**. Then, the IPv6 EIP will be released. You will only have the IPv4 EIP.

10 Shared Bandwidth

10.1 Shared Bandwidth Overview

A shared bandwidth can be shared by multiple EIPs and controls the data transfer rate on these EIPs in a centralized manner. All ECSs and load balancers that have EIPs bound in the same region can share a bandwidth.

NOTE

- A shared bandwidth cannot control how much data can be transferred using a single EIP. Data transfer rate on EIPs cannot be customized.

When you host a large number of applications on the cloud, if each EIP uses a bandwidth, a lot of bandwidths are required, which significantly increases bandwidth costs. If all EIPs share the same bandwidth, you can lower bandwidth costs and easily perform system O&M.

- Lowered Bandwidth Costs
Region-level bandwidth sharing and multiplexing reduce bandwidth usage and O&M costs.
- Flexible Operations
You can add pay-per-use EIPs (except for **5_gray** EIPs of dedicated load balancers) to or remove them from a shared bandwidth regardless of the type of instances that they are bound to.
- Flexible Billing Modes
The yearly/monthly and pay-per-use billing modes are provided.

You can use a shared bandwidth in either of the following ways:

- Assign a shared bandwidth and add your pay-per-use EIPs to the bandwidth.
 - [Assigning a Shared Bandwidth](#)
 - [Adding EIPs to a Shared Bandwidth](#)
- Assign a shared bandwidth, set **Billed By** to **Shared Bandwidth** and select the shared bandwidth when you assign EIPs.
 - [Assigning a Shared Bandwidth](#)

- [Assigning an EIP and Binding It to an ECS](#)

Notes and Constraints

- If a yearly/monthly shared bandwidth is deleted upon expiration, EIPs sharing the bandwidth will be removed from the bandwidth and be billed based on the mode before they are added to the shared bandwidth.
- A shared bandwidth can only be used by resources from its same account.

NOTE

- A dedicated bandwidth cannot be changed to a shared bandwidth and vice versa. However, you can purchase a shared bandwidth for pay-per-use EIPs.
 - Add an EIP to a shared bandwidth and then the EIP will use the shared bandwidth.
 - Remove the EIP from the shared bandwidth and then the EIP will use the dedicated bandwidth.
- If you want to submit a service ticket, refer to [Submitting a Service Ticket](#).

10.2 Assigning a Shared Bandwidth

Scenarios

When you host a large number of applications on the cloud, if each EIP uses dedicated bandwidth, a lot of bandwidths are required, which incurs high costs. If all EIPs share the same bandwidth, your network operation costs will be lowered and your system O&M as well as resource statistics will be simplified.

Assign a shared bandwidth for use with EIPs.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the upper right corner, click **Buy Shared Bandwidth**. On the displayed page, configure parameters as prompted.

Table 10-1 Parameter descriptions

Parameter	Description	Example Value
Billing Mode	A shared bandwidth can be billed on a yearly/monthly or pay-per-use basis. <ul style="list-style-type: none">• Yearly/Monthly: You pay for the bandwidth by year or month before using it. No other charges apply during the validity period of the bandwidth.• Pay-per-use: You pay for the bandwidth based on the amount of time you use the bandwidth.	Yearly/Monthly
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	N/A
Bandwidth Type	Select a type of the shared bandwidth based on your EIP type. <ul style="list-style-type: none">• Standard: Dynamic BGP and premium BGP EIPs can be added to a shared bandwidth of this type. NOTE In the CN-Hong Kong region, only dynamic BGP EIPs can be added to standard shared bandwidths.	Standard
Billed By	The billing method for the shared bandwidth. You can specify a shared bandwidth to be billed by bandwidth.	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	10
Enterprise Project	The enterprise project that the EIP belongs to. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default .	default
Name	The name of the shared bandwidth.	Bandwidth-001
Required Duration	The duration for which the purchased EIP will use. The duration must be specified if the Billing Mode is set to Yearly/Monthly .	2 months

5. Click **Create Now**.

10.3 Adding EIPs to a Shared Bandwidth


Scenarios

You can add multiple EIPs to a shared bandwidth at the same time.

Notes and Constraints

- Currently, yearly/monthly EIPs cannot be added to a shared bandwidth.
- If it is a premium shared bandwidth, you can add premium BGP EIPs and IPv6 NICs to it.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the shared bandwidth list, locate the target shared bandwidth that you want to add EIPs to. In the **Operation** column, choose **Add Public IP Address**, and select the EIPs to be added.

NOTE

- After an EIP is added to a shared bandwidth, the dedicated bandwidth used by the EIP will become invalid and the EIP will start to use the shared bandwidth. The EIP's dedicated bandwidth will be deleted and will no longer be billed.
5. Click **OK**.

Helpful Links


[What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth? Can a Dedicated Bandwidth Be Changed to a Shared Bandwidth or the Other Way Around?](#)

10.4 Removing EIPs from a Shared Bandwidth

Scenarios

Remove EIPs that are no longer required from a shared bandwidth if needed.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Elastic IP**.

3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the shared bandwidth list, locate the target shared bandwidth from which EIPs are to be removed, choose **More > Remove Public IP Address** in the **Operation** column, and select the EIPs to be removed in the displayed dialog box.
5. Set the EIP bandwidth after the EIP is removed.
6. Click **OK**.

10.5 Modifying a Shared Bandwidth


Scenarios

You can modify the name and size of a shared bandwidth as required.

- If a shared bandwidth is billed on a pay-per-use basis, the modification will take effect immediately. For details, see [Modifying a Shared Bandwidth \(Pay-per-Use\)](#).
- If a shared bandwidth is billed on a yearly/monthly basis:
 - **You can increase the bandwidth.** The increased bandwidth size will take effect immediately and the price difference will be billed accordingly.
 - **You can decrease the bandwidth.** The decreased bandwidth size will take effect in the first billing cycle after a successful renewal.


If you want to change the billing mode of a shared bandwidth, see [How Do I Change My EIP Billing Mode from Pay-per-Use to Yearly/Monthly?](#)

Modifying a Shared Bandwidth (Pay-per-Use)

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the shared bandwidth you want to modify, click **Modify Bandwidth** in the **Operation** column, and modify the bandwidth settings.
5. Click **Next**.
6. Click **Submit**.


The modification takes effect immediately.

Increasing a Shared Bandwidth (Yearly/Monthly)

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the target shared bandwidth, and click **Modify Bandwidth** in the **Operation** column.

5. Select **Increase bandwidth** and click **Continue**.
6. In the **New Configuration** area on the **Modify Bandwidth** page, change the bandwidth name and size.
7. Click **Next**.
8. Confirm the information and click **Pay Now**.
After you complete the payment, the increased bandwidth will take effect immediately.

Decreasing a Shared Bandwidth (Yearly/Monthly)

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the target shared bandwidth, and click **Modify Bandwidth** in the **Operation** column.
5. Select **Decrease bandwidth** and click **Continue**.
6. In the **New Configuration** area on the **Modify Bandwidth** page, change the bandwidth name and size.
7. Click **Next**.
8. Confirm the information and click **Pay Now**.
After you complete the payment, the decreased bandwidth will take effect in the first billing cycle after the current subscription ends.

10.6 Deleting a Shared Bandwidth

Scenarios

Delete a shared bandwidth when it is no longer required.


Notes and Constraints

- A yearly/monthly shared bandwidth cannot be directly deleted. It can only be unsubscribed.
- If you want to delete a shared bandwidth with EIPs added, you have to remove the EIPs from the shared bandwidth first.

Prerequisites

Before deleting a shared bandwidth, remove all the EIPs associated with it. For details, see [Removing EIPs from a Shared Bandwidth](#).

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Networking > Elastic IP**.

3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the pay-per-use shared bandwidth you want to delete, click **More** in the **Operation** column, and then click **Delete**.
5. In the displayed dialog box, click **OK**.

11 Interconnecting with CTS

11.1 Supported VPC Operations

With CTS, you can record operations performed on the VPC service for further query, audit, and backtracking purposes.

Table 11-1 lists the VPC operations that can be recorded by CTS.

Table 11-1 VPC operations that can be recorded by CTS

Operation	Resource Type	Trace
Modifying a bandwidth	Bandwidth	modifyBandwidth
Assigning an EIP	EIP	createEip
Releasing an EIP	EIP	deleteEip
Binding an EIP	EIP	bindEip
Unbinding an EIP	EIP	unbindEip
Assigning a private IP address	Private IP address	createPrivateIp
Deleting a private IP address	Private IP address	deletePrivateIp
Creating a security group	security_groups	createSecurity-group
Updating a security group	security_groups	updateSecurity-group
Deleting a security group	security_groups	deleteSecurity-group
Creating a security group rule	security-group-rules	createSecurity-group-rule

Operation	Resource Type	Trace
Updating a security group rule	security-group-rules	updateSecurity-group-rule
Deleting a security group rule	security-group-rules	deleteSecurity-group-rule
Creating a subnet	Subnet	createSubnet
Deleting a subnet	Subnet	deleteSubnet
Modifying a subnet	Subnet	modifySubnet
Creating a VPC	VPC	createVpc
Deleting a VPC	VPC	deleteVpc
Modifying a VPC	VPC	modifyVpc
Creating a VPN	VPN	createVpn
Deleting a VPN	VPN	deleteVpn
Modifying a VPN	VPN	modifyVpn
Creating a router	routers	createRouter
Updating a router	routers	updateRouter
Adding an interface to a router	routers	addRouterInterface
Deleting an interface from a router	routers	removeRouterInterface
Creating a port	ports	createPort
Updating a port	ports	updatePort
Deleting a port	ports	deletePort
Creating a network	networks	createNetwork
Updating a network	networks	updateNetwork
Deleting a network	networks	deleteNetwork
Batch creating or deleting subnet tags	tag	batchUpdateTags
Batch creating or deleting VPC tags	tag	batchUpdateVpcTags
Creating a route table	routetables	createRouteTable
Updating a route table	routetables	updateRouteTable
Deleting a route table	routetables	deleteRouteTable

Operation	Resource Type	Trace
Creating a VPC peering connection	vpc-peering	createVpcPeerings
Updating a VPC peering connection	vpc-peering	updateVpcPeerings
Deleting a VPC peering connection	vpc-peering	deleteVpcPeerings
Creating a network ACL group	firewall-groups	createFirewallGroup
Updating a network ACL group	firewall-groups	updateFirewallGroup
Deleting a network ACL group	firewall-groups	deleteFirewallGroup
Creating a network ACL policy	firewall-policies	createFirewallPolicy
Updating a network ACL policy	firewall-policies	updateFirewallPolicy
Deleting a network ACL policy	firewall-policies	deleteFirewallPolicy
Inserting a network ACL rule	firewall-policies	insertFirewallPolicyRule
Removing a network ACL rule	firewall-policies	removeFirewallPolicyRule
Creating a network ACL rule	firewall-rules	createFirewallRule
Updating a network ACL rule	firewall-rules	updateFirewallRule
Deleting a network ACL rule	firewall-rules	deleteFirewallRule
Creating an IP address group	address_group	createAddress_group
Updating an IP address group	address_group	updateAddress_group
Forcibly deleting an IP address group	address_group	force_deleteAddress_group
Deleting an IP address group	address_group	deleteAddress_group
Creating a flow log	flowlogs	createFlowLog

Operation	Resource Type	Trace
Updating a flow log	flowlogs	updateFlowLog
Deleting a flow log	flowlogs	deleteFlowLog

11.2 Viewing Traces

Scenarios



After CTS is enabled, CTS starts recording operations on cloud resources. The CTS management console stores the last seven days of operation records.

This section describes how to query or export the last seven days of operation records on the management console.

NOTICE

CTS only retains traces for seven days. To store traces for a longer time, configure your tracker to transfer traces to OBS buckets. For details, see [Configuring a Tracker](#).

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click  to go to the service list. Under **Management & Deployment**, click **Cloud Trace Service**.
4. In the navigation pane on the left, choose **Trace List**.
5. Specify filters as needed. The following filters are available:
 - **Trace Type**: Set it to **Management** or **Data**.
 - **Trace Source, Resource Type, and Search By**
Select filters from the drop-down list.
If you select **Trace name** for **Search By**, select a trace name.
If you select **Resource ID** for **Search By**, select or enter a resource ID.
If you select **Resource name** for **Search By**, select or enter a resource name.
 - **Operator**: Select a specific operator (a user other than an account).
 - **Trace Status**: Select **All trace statuses**, **Normal**, **Warning**, or **Incident**.
 - **Search time range**: In the upper right corner, choose **Last 1 hour**, **Last 1 day**, or **Last 1 week**, or specify a custom time range.
6. Click arrow on the left of the required trace to expand its details.
7. Locate the required trace and click **View Trace** in the **Operation** column.

A dialog box is displayed, showing the trace content.

12 Monitoring

12.1 Supported Metrics

Description

This section describes the namespace, list, and measurement dimensions of EIP and bandwidth metrics that you can check on Cloud Eye. You can use APIs or the Cloud Eye console to query the metrics of the monitored metrics and alarms generated for EIPs and bandwidths.

Namespace

SYS.VPC

Monitoring Metrics

Table 12-1 EIP and bandwidth metrics

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic (Previously called "Upstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic (Previously called "Downstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth in the unit of percent. Outbound bandwidth usage = Outbound bandwidth/ Purchased bandwidth	0% to 100%	Bandwidth or EIP	1 minute
upstream	Outbound Traffic	Network traffic going out of the cloud platform in a minute (Previously called "Upstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute
downstream	Inbound Traffic	Network traffic going into the cloud platform in a minute (Previously called "Downstream Traffic") Unit: byte	≥ 0 bytes	Bandwidth or EIP	1 minute

Dimensions

Key	Value
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

If a monitored object has multiple dimensions, all dimensions are mandatory when you use APIs to query the metrics.

- Query a monitoring metric:
dim.0=bandwidth_id,530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id,3773b058-5b4f-4366-9035-9bbd9964714a
- Query monitoring metrics in batches:
"dimensions": [
 {
 "name": "bandwidth_id",
 "value": "530cd6b0-86d7-4818-837f-935f6a27414d"
 }
 {
 "name": "publicip_id",
 "value": "3773b058-5b4f-4366-9035-9bbd9964714a"
 }
],



12.2 Viewing Metrics

Scenarios

You can view the bandwidth and EIP usage.

You can view the inbound bandwidth, outbound bandwidth, inbound bandwidth usage, outbound bandwidth usage, inbound traffic, and outbound traffic in a specified period.

Procedure (Cloud Eye Console)

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click  to open the service list and choose **Management & Deployment > Cloud Eye**.
4. Click **Cloud Service Monitoring** on the left of the page, and choose **Elastic IP and Bandwidth**.



5. Locate the target bandwidth or EIP and click **View Metric** in the **Operation** column to check the bandwidth or EIP monitoring information.

12.3 Creating an Alarm Rule

Scenarios

You can configure alarm rules to customize the monitored objects and notification policies. You can learn your resource statuses at any time.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper left corner of the page, click  to open the service list and choose **Management & Deployment > Cloud Eye**.
4. In the left navigation pane on the left, choose **Alarm Management > Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters, or modify an existing alarm rule.
6. After the parameters are set, click **Create**.

After the alarm rule is created, the system automatically notifies you if an alarm is triggered for the VPC service.

NOTE

For more information about alarm rules, see [Cloud Eye User Guide](#).

13 Permissions Management

13.1 Creating a User and Granting VPC Permissions

This section describes how to use IAM to implement fine-grained permissions control for your VPC resources. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing VPC resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a cloud account or cloud service to perform efficient O&M on your VPC resources.

If your cloud account meets your permissions requirements, you can skip this section.

[Figure 13-1](#) shows the process flow for granting permissions.

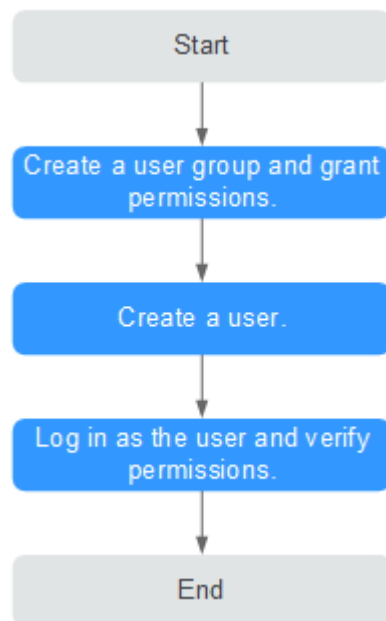
Prerequisites

Learn about the permissions (see [Permissions](#)) supported by VPC and choose policies or roles according to your requirements.

To grant permissions for other services, learn about all [system-defined permissions](#) supported by IAM.

Process Flow

Figure 13-1 Process for granting VPC permissions



1. On the IAM console, **create a user group and grant it permissions**.
Create a user group on the IAM console and assign the **VPCReadOnlyAccess** permissions to the group.
2. **Create an IAM user and add it to the created user group**.
Create a user on the IAM console and add the user to the group created in 1.
3. **Log in as the IAM user** and verify permissions.
In the authorized region, perform the following operations:
 - Choose **Service List > Virtual Private Cloud**. Then click **Create VPC** on the VPC console. If a message appears indicating that you have insufficient permissions to perform the operation, the **VPCReadOnlyAccess** policy is in effect.
 - Choose another service from **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **VPCReadOnlyAccess** policy is in effect.

13.2 VPC Custom Policies

Custom policies can be created to supplement the system-defined policies of VPC. For the actions supported for custom policies, see [Permissions Policies and Supported Actions](#).

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For operation details, see [Creating a Custom Policy](#). The following section contains examples of common VPC custom policies.

Example Custom Policies

- Example 1: Allowing users to create and view VPCs

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "vpc:vpcs:create",
        "vpc:vpcs:list"
      ]
    }
  ]
}
```

- Example 2: Denying VPC deletion

A deny policy must be used in conjunction with other policies to take effect. If the permissions assigned to a user contain both Allow and Deny actions, the Deny actions take precedence over the Allow actions.

The following method can be used if you need to assign permissions of the **VPC FullAccess** policy to a user but also forbid the user from deleting VPCs. Create a custom policy for denying VPC deletion, and assign both policies to the group the user belongs to. Then the user can perform all operations on VPC except deleting VPCs. The following is an example deny policy:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": [
        "vpc:vpcs:delete"
      ]
    }
  ]
}
```

- Example 3: Defining permissions for multiple services in a policy

A custom policy can contain the actions of multiple services that are of the global or project-level type. The following is an example policy containing actions of multiple services:

```
{
  "Version": "1.1",
  "Statement": [
    {
      "Action": [
        "vpc:vpcs:create",
        "vpc:vpcs:update"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "ecs:servers:delete"
      ],
      "Effect": "Allow"
    }
  ]
}
```


A Change History

Release Date	Description
2023-12-22	This release incorporates the following changes: Added VPC Flow Log .
2023-12-01	This release incorporates the following changes: <ul style="list-style-type: none">• Added Allowing Common Ports with A Few Clicks.• Added descriptions about priority, action, and IPv6 in Security Group.
2023-03-29	This release incorporates the following changes: <ul style="list-style-type: none">• Added IPv6 EIP and Elastic Network Interface and Supplementary Network Interface.• Added screenshots in Creating a VPC, Modifying a VPC, Adding a Security Group Rule, and Fast-Adding Security Group Rules.
2022-09-30	This issue is the first official release.