

Virtual Private Cloud

User Guide(Kuala Lumpur Region)

Issue 01
Date 2022-10-31



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 Service Overview.....	1
1.1 What Is Virtual Private Cloud?.....	1
1.2 Application Scenarios.....	2
1.3 VPC Connectivity.....	2
1.4 VPC and Other Services.....	3
1.5 Basic Concepts.....	4
1.5.1 Subnet.....	4
1.5.2 Elastic IP.....	4
1.5.3 Route Table.....	5
1.5.4 Security Group.....	7
1.5.5 VPC Peering Connection.....	7
1.5.6 Network ACL.....	8
1.5.7 Virtual IP Address.....	8
1.5.8 Region and AZ.....	10
2 Getting Started.....	12
2.1 Typical Application Scenarios.....	12
2.2 Configuring a VPC for ECSs That Do Not Require Internet Access.....	12
2.2.1 Overview.....	12
2.2.2 Step 1: Create a VPC.....	14
2.2.3 Step 2: Create a Subnet for the VPC.....	19
2.2.4 Step 3: Create a Security Group.....	22
2.2.5 Step 4: Add a Security Group Rule.....	24
2.3 Configuring a VPC for ECSs That Access the Internet Using EIPs.....	27
2.3.1 Overview.....	32
2.3.2 Step 1: Create a VPC.....	34
2.3.3 Step 2: Create a Subnet for the VPC.....	39
2.3.4 Step 3: Assign an EIP and Bind It to an ECS.....	42
2.3.5 Step 4: Create a Security Group.....	45
2.3.6 Step 5: Add a Security Group Rule.....	46
3 VPC and Subnet.....	50
3.1 VPC and Subnet Planning Suggestions.....	50
3.2 VPC.....	53

3.2.1 Creating a VPC.....	53
3.2.2 Modifying a VPC.....	59
3.2.3 Managing VPC Tags.....	61
3.2.4 Obtaining a VPC ID.....	62
3.2.5 Viewing a VPC Topology.....	63
3.2.6 Exporting VPC List.....	63
3.2.7 Deleting a VPC.....	64
3.3 Subnet.....	64
3.3.1 Creating a Subnet for the VPC.....	64
3.3.2 Modifying a Subnet.....	67
3.3.3 Managing Subnet Tags.....	70
3.3.4 Viewing and Deleting Resources in a Subnet.....	71
3.3.5 Viewing IP Addresses in a Subnet.....	72
3.3.6 Exporting Subnet List.....	73
3.3.7 Deleting a Subnet.....	74
3.4 IPv4 and IPv6 Dual-Stack Network.....	74
4 Route Tables.....	78
4.1 Route Tables and Routes.....	78
4.2 Managing Route Tables.....	81
4.2.1 Creating a Custom Route Table.....	81
4.2.2 Associating a Route Table with a Subnet.....	82
4.2.3 Changing the Route Table Associated with a Subnet.....	83
4.2.4 Viewing the Route Table Associated with a Subnet.....	83
4.2.5 Viewing Route Table Information.....	84
4.2.6 Exporting Route Table Information.....	84
4.2.7 Deleting a Route Table.....	85
4.3 Managing Routes.....	85
4.3.1 Adding a Custom Route.....	85
4.3.2 Modifying a Route.....	87
4.3.3 Replicating a Route.....	88
4.3.4 Deleting a Route.....	89
4.4 Configuring an SNAT Server.....	90
5 Virtual IP Address.....	94
5.1 Virtual IP Address Overview.....	94
5.2 Assigning a Virtual IP Address.....	96
5.3 Binding a Virtual IP Address to an EIP or ECS.....	97
5.4 Binding a Virtual IP Address to an EIP.....	98
5.5 Releasing a Virtual IP Address.....	99
5.6 Disabling IP Forwarding on the Standby ECS.....	100
5.7 Disabling Source/Destination Check for an ECS NIC.....	101
6 Access Control.....	102

6.1 What Is Access Control?	102
6.2 Security Group	103
6.2.1 Security Groups and Security Group Rules	103
6.2.2 Default Security Group and Rules	105
6.2.3 Security Group Configuration Examples	106
6.2.4 Managing a Security Group	111
6.2.4.1 Creating a Security Group	111
6.2.4.2 Cloning a Security Group	113
6.2.4.3 Modifying a Security Group	114
6.2.4.4 Deleting a Security Group	114
6.2.5 Managing Security Group Rules	115
6.2.5.1 Adding a Security Group Rule	115
6.2.5.2 Fast-Adding Security Group Rules	119
6.2.5.3 Modifying a Security Group Rule	121
6.2.5.4 Replicating a Security Group Rule	122
6.2.5.5 Importing and Exporting Security Group Rules	122
6.2.5.6 Deleting a Security Group Rule	125
6.2.6 Managing Instances Associated with a Security Group	125
6.2.6.1 Adding an Instance to or Removing an Instance from a Security Group	125
6.2.6.2 Changing the Security Group of an ECS	127
6.3 Network ACL	127
6.3.1 Network ACL Overview	127
6.3.2 Network ACL Configuration Examples	131
6.3.3 Managing Network ACLs	133
6.3.3.1 Creating a Network ACL	134
6.3.3.2 Modifying a Network ACL	134
6.3.3.3 Enabling or Disabling a Network ACL	135
6.3.3.4 Viewing a Network ACL	135
6.3.3.5 Deleting a Network ACL	136
6.3.4 Management Network ACL Rules	136
6.3.4.1 Adding a Network ACL Rule	136
6.3.4.2 Modifying a Network ACL Rule	138
6.3.4.3 Changing the Sequence of a Network ACL Rule	140
6.3.4.4 Enabling or Disabling a Network ACL Rule	141
6.3.4.5 Exporting and Importing Network ACL Rules	141
6.3.4.6 Deleting a Network ACL Rule	142
6.3.5 Managing Subnets Associated with a Network ACL	142
6.3.5.1 Associating Subnets with a Network ACL	143
6.3.5.2 Disassociating Subnets from a Network ACL	143
7 VPC Peering Connection	145
7.1 VPC Peering Connection Overview	145
7.2 VPC Peering Connection Usage Examples	147

7.3 Creating a VPC Peering Connection with Another VPC in Your Account.....	157
7.4 Creating a VPC Peering Connection with a VPC in Another Account.....	162
7.5 Obtaining the Peer Project ID of a VPC Peering Connection.....	167
7.6 Modifying a VPC Peering Connection.....	168
7.7 Viewing VPC Peering Connections.....	168
7.8 Deleting a VPC Peering Connection.....	169
7.9 Modifying Routes Configured for a VPC Peering Connection.....	169
7.10 Viewing Routes Configured for a VPC Peering Connection.....	171
7.11 Deleting Routes Configured for a VPC Peering Connection.....	172
8 VPC Flow Log.....	175
8.1 VPC Flow Log Overview.....	175
8.2 Creating a VPC Flow Log.....	176
8.3 Viewing a VPC Flow Log.....	178
8.4 Enabling or Disabling VPC Flow Log.....	180
8.5 Deleting a VPC Flow Log.....	181
9 Elastic IP.....	182
9.1 Assigning an EIP and Binding It to an ECS.....	182
9.2 Unbinding an EIP from an ECS and Releasing the EIP.....	184
9.3 Modifying an EIP Bandwidth.....	185
9.4 Exporting EIP Information.....	186
9.5 Managing EIP Tags.....	186
10 Shared Bandwidth.....	188
10.1 Shared Bandwidth Overview.....	188
10.2 Assigning a Shared Bandwidth.....	188
10.3 Adding EIPs to a Shared Bandwidth.....	189
10.4 Removing EIPs from a Shared Bandwidth.....	190
10.5 Modifying a Shared Bandwidth.....	190
10.6 Deleting a Shared Bandwidth.....	191
11 Interconnecting with CTS.....	192
11.1 Supported VPC Operations.....	192
11.2 Viewing Traces.....	194
12 Monitoring.....	196
12.1 Supported Metrics.....	196
12.2 Viewing Metrics.....	198
12.3 Creating an Alarm Rule.....	199
13 FAQ.....	200
13.1 General Questions.....	200
13.1.1 What Is a Quota?.....	200
13.2 VPCs and Subnets.....	201
13.2.1 What Is Virtual Private Cloud?.....	201

13.2.2 Which CIDR Blocks Are Available for the VPC Service?.....	201
13.2.3 Can Subnets Communicate with Each Other?.....	202
13.2.4 What Subnet CIDR Blocks Are Available?.....	204
13.2.5 How Many Subnets Can I Create?.....	204
13.2.6 Why Can't I Delete My VPCs and Subnets?.....	204
13.3 EIPs.....	208
13.3.1 Can I Bind an EIP to Multiple ECSs?.....	208
13.3.2 How Do I Access an ECS with an EIP Bound from the Internet?.....	208
13.3.3 Can I Bind an EIP of an ECS to Another ECS?.....	209
13.3.4 Can I Bind an EIP to a Cloud Resource in Another Region?.....	209
13.3.5 Can I Change the Region of My EIP?.....	209
13.4 VPC Peering Connections.....	209
13.4.1 How Many VPC Peering Connections Can I Create in an Account?.....	209
13.4.2 Can a VPC Peering Connection Connect VPCs in Different Regions?.....	209
13.4.3 Why Did Communication Fail Between VPCs That Were Connected by a VPC Peering Connection?	210
13.5 Bandwidth.....	216
13.5.1 What Is the Bandwidth Size Range?.....	216
13.5.2 What Bandwidth Types Are Available?.....	216
13.5.3 What Is the Relationship Between Bandwidth and Upload/Download Rate?.....	217
13.6 Connectivity.....	217
13.6.1 Does a VPN Allow Communication Between Two VPCs?.....	217
13.6.2 Why Are Internet or Internal Domain Names in the Cloud Inaccessible Through Domain Names When My ECS Has Multiple NICs?.....	217
13.6.3 What Are the Priorities of the Custom Route and EIP If Both Are Configured for an ECS to Enable the ECS to Access the Internet?.....	217
13.7 Routing.....	218
13.7.1 Can a Route Table Span Multiple VPCs?.....	218
13.7.2 How Many Routes Can a Route Table Contain?.....	218
13.7.3 Are There Any Restrictions on Using a Route Table?.....	218
13.7.4 Do the Same Routing Priorities Apply to Direct Connect Connections and Custom Routes in the Same VPC?.....	218
13.7.5 Are There Different Routing Priorities of the VPN and Custom Routes in the Same VPC?.....	218
13.8 Security.....	218
13.8.1 Does a Modified Security Group Rule or a Network ACL Rule Take Effect Immediately for Existing Connections?.....	219
13.8.2 Why Can't I Delete a Security Group?.....	219
13.8.3 Can I Change the Security Group of an ECS?.....	220
13.8.4 How Do I Configure a Security Group for Multi-Channel Protocols?.....	220
A Change History.....	221

1 Service Overview

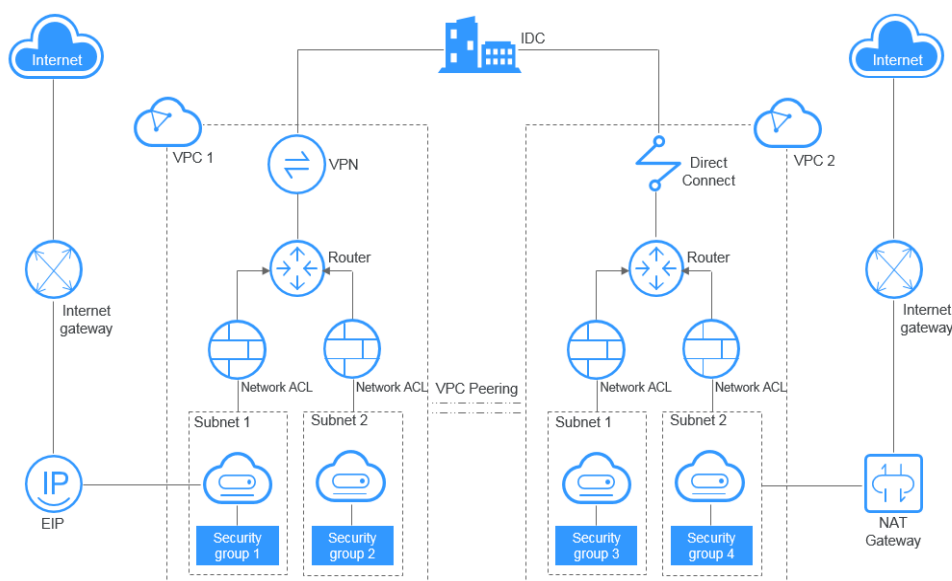
1.1 What Is Virtual Private Cloud?

VPC Overview

Virtual Private Cloud (VPC) enables you to provision logically isolated virtual networks for Elastic Cloud Servers (ECSs), improving cloud resource security and simplifying network deployment. You can configure and manage the virtual networks as required.

Within your own VPC, you can create security groups and VPNs, configure IP address ranges, specify bandwidth sizes, manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. You can also define rules to control communications between ECSs in the same security group or in different security groups.

Figure 1-1 VPC components



Accessing the VPC Service

You can access the VPC service through the management console or using HTTPS-based APIs.

- Management console

You can use the console to directly perform operations on VPC resources. To access the VPC service, log in to the management console and select **Virtual Private Cloud** from the console homepage.

- API

If you need to integrate a VPC into a third-party system for secondary development, you can use APIs to access the VPC service. For details, see the *Virtual Private Cloud API Reference*.

1.2 Application Scenarios

- Hosting web applications

You can host web applications and websites in a VPC and use the VPC as a regular network. With EIPs, you can connect ECSs running your web applications to the Internet. A VPN gateway is used to establish a VPN tunnel between the web applications and the service system on the cloud, ensuring high-speed communication between the website and the service system.

- Hosting services that demand high security

You can create a VPC and security groups to host multi-tier web applications in different security zones. You can associate web servers and database servers with different security groups and configure different access control rules for security groups. You can launch web servers in a publicly accessible subnet, and also run database servers in subnets that are not publicly accessible. In this way, you can ensure high security.

- Extending your corporate network into the cloud

You can establish a VPN connection between a VPC and a traditional data center to use the ECSs and block storage resources. Applications can be migrated to the cloud and additional web servers can be quickly deployed as needed when there is a spike in demand for computing resources. This way, less money has to be spent on IT and O&M and data is kept safer than in a traditional arrangement. A VPC can span multiple AZs, protecting from single points of failure and ensuring high availability for e-commerce systems.

1.3 VPC Connectivity

You can use EIPs, load balancers, NAT gateways, VPN connections, and Direct Connect connections to access the Internet if required.

- **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.

- **Use NAT Gateways 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 the ECSs. With NAT gateways, you do not need to assign an EIP to each ECS, which reduces management costs incurred by an excessive number of EIPs. A NAT gateway offers both the SNAT and DNAT functions. 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. SNAT supports up to 1 million concurrent connections and 30,000 new connections. 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.

- **Use ELB to Connect to 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.

- **Use VPN or Direct Connect to Extend Your On-premises Data Center into the Cloud over the Internet**

For customers with equipment rooms in their on-premises data centers, not all businesses of the customers will be migrated to the cloud because the customers want to reuse their legacy devices and require smooth business evolution. Then, you can use VPN or Direct Connect to interconnect your VPC and on-premises data center. A VPN connection routes traffic through the Internet, which allows you to use a private network with the price of the public network. A Direct Connect connection is a dedicated, private network connection that provides you with more efficient data transmission and more consistent network experience than Internet-based connections.

1.4 VPC and Other Services

- **ECS**

The VPC service provides an isolated virtual network for ECSs. You can configure and manage the network as required. There are multiple connectivity options for ECSs to access the Internet. You can also define rules for communication between ECSs in the same security group or in different security groups.

- **ELB**

ELB uses the EIPs and bandwidths associated with the VPC service.

- **Cloud Eye**

You can use Cloud Eye to monitor the status of your VPCs without adding plug-ins.

1.5 Basic Concepts

1.5.1 Subnet

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.

- After a subnet is created, its CIDR block cannot be modified. Subnets in the same VPC cannot overlap.

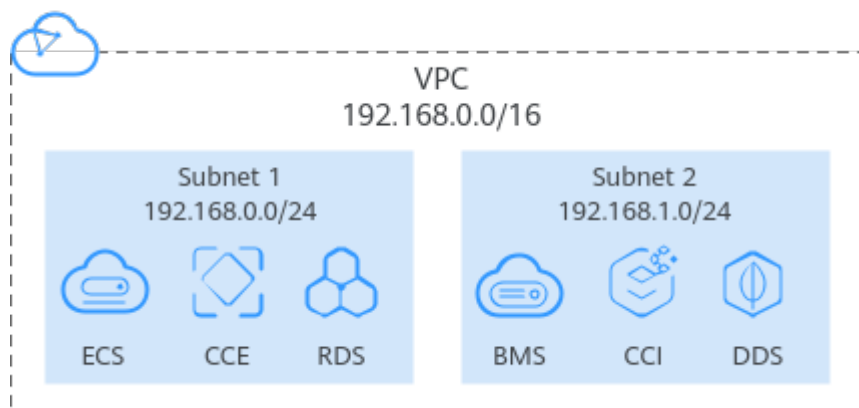
A subnet mask can be between the netmask of its VPC CIDR block and /28 netmask. If a VPC CIDR block is 10.0.0.0/16, its subnet mask can be between 16 and 28.

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 [What Is a Quota?](#)

Figure 1-2 Subnet

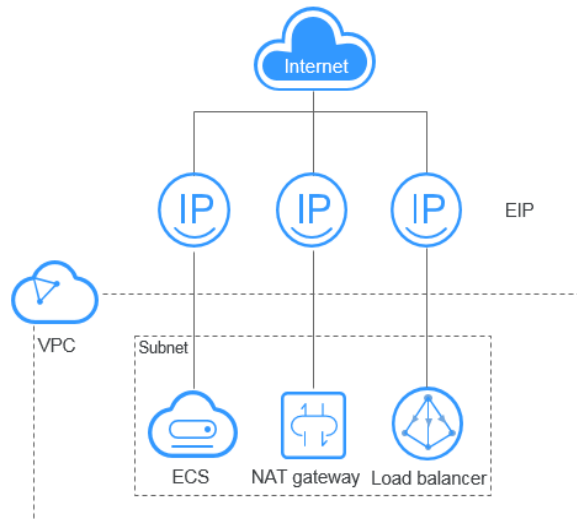


1.5.2 Elastic IP

The Elastic IP (EIP) service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. EIPs can be bound to or unbound from ECSs, BMSs, virtual IP addresses, NAT gateways, or load balancers.

Each EIP can be used by only one cloud resource at a time.

Figure 1-3 Accessing the Internet using an EIP



1.5.3 Route Table

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.

- 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

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.

 **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 1-1](#) 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 1-1 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
VPN gateway	Traffic intended for the destination is forwarded to a VPN gateway.	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

Next Hop Type	Description	Supported 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

 **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.

1.5.4 Security Group

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.

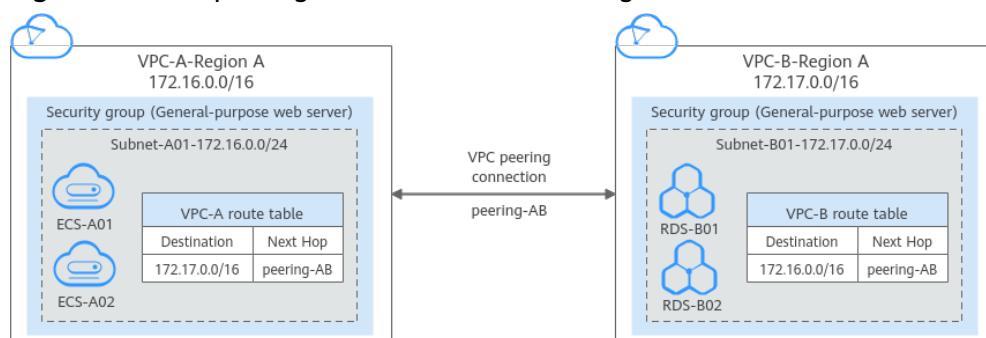
1.5.5 VPC Peering Connection

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 1-4 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.

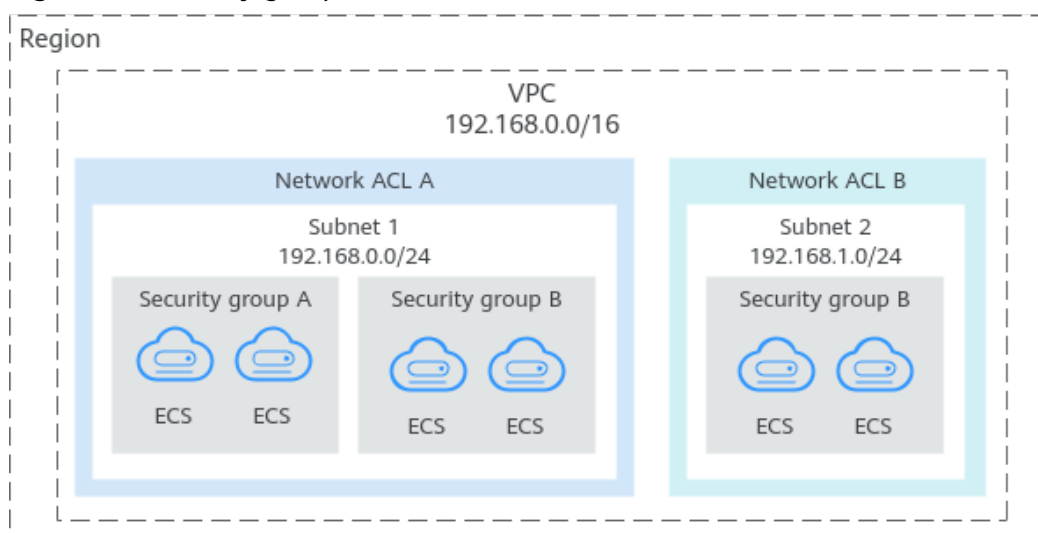
Figure 1-4 VPC peering connection network diagram



1.5.6 Network ACL

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 1-5 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.

1.5.7 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.

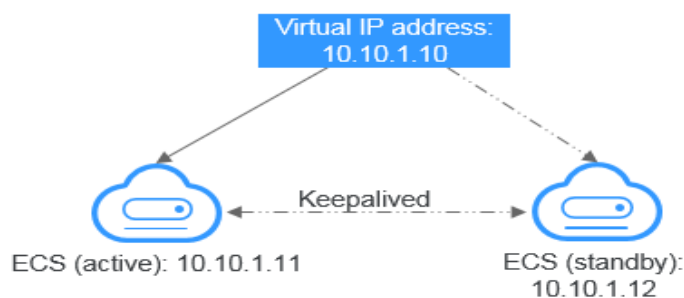
Networking

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 1-6 Networking diagram of the HA mode

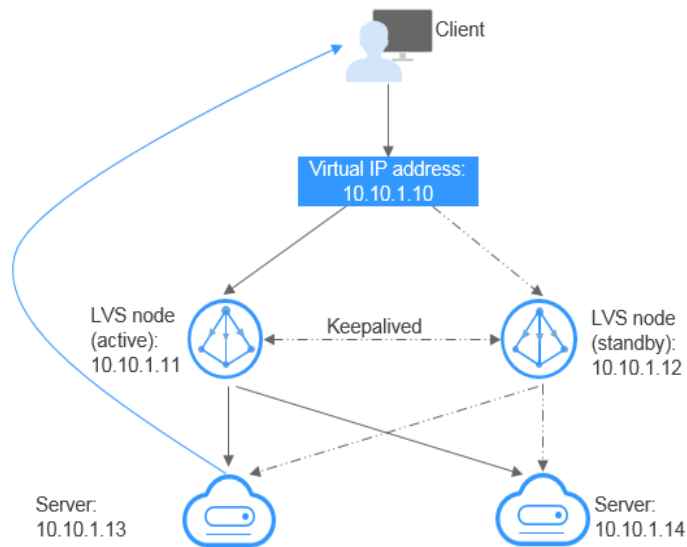


- As shown in the above figure, bind a virtual IP address to two ECSs in the same subnet.
- Configure Keepalived for the two ECSs to work in the active/standby pair. Follow industry standards for configuring Keepalived. The details are not included here.

- **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 1-7 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.

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 VPN for security and Direct Connect for stable connectivity. The VPC peering connection is needed so that the VPCs in the same region can communicate with each other.

1.5.8 Region and AZ

Concept

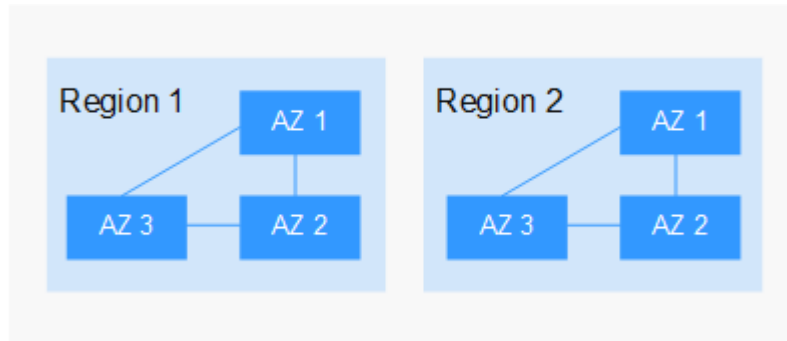
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.

- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-8 shows the relationship between regions and AZs.

Figure 1-8 Regions and AZs



Selecting a Region

Select a region closest to your target users for lower network latency and quick access.

Selecting an AZ

When deploying resources, consider your applications' requirements on disaster recovery (DR) and network latency.

- For high DR capability, deploy resources in different AZs within the same region.
- For lower network latency, deploy resources in the same AZ.

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

2 Getting Started

2.1 Typical Application Scenarios

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

- If any of your ECSs, for example, ECSs that function as the database of server nodes for website deployment, do not need to access the Internet, you can configure a VPC for the ECSs by following the instructions described in [Configuring a VPC for ECSs That Do Not Require Internet Access](#).
- If your ECSs need to access the Internet, you can configure EIPs for them. For example, the ECSs functioning as the service nodes for deploying a website need to be accessed by users over the Internet. Then, you can configure a VPC for these ECSs by following the instructions provided in [Configuring a VPC for ECSs That Access the Internet Using EIPs](#).
- When you need to access the IPv6 services on the Internet or provide services accessible from users using an IPv6 client, you need to enable the IPv6 function. After the IPv6 function is enabled, you can provide services for users using an IPv4 or IPv6 client.

2.2 Configuring a VPC for ECSs That Do Not Require Internet Access

2.2.1 Overview

If your ECSs do not require Internet access (for example, the ECSs functioning as the database nodes or server nodes for deploying a website), you can follow the procedure shown in [Figure 2-1](#) to configure a VPC for the ECSs.

Figure 2-1 Configuring the network

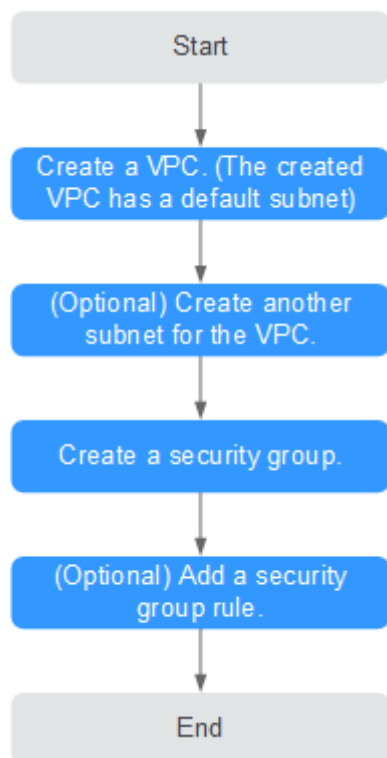


Table 2-1 describes the different tasks in the procedure for configuring the network.

Table 2-1 Configuration process description

Task	Description
Create a VPC.	This task is mandatory. After the VPC is created, you can create other required network resources in the VPC based on your service requirements.
Create another subnet for the VPC.	This task is optional. If the default subnet cannot meet your requirements, you can create one. The new subnet is used to assign IP addresses to NICs added to the ECS.
Create a security group.	This task is mandatory. You can create a security group and add ECSs in the VPC to the security group to improve ECS access security. After a security group is created, it has default rules.

Task	Description
Add a security group rule.	This task is optional. If the default rule meets your service requirements, you do not need to add rules to the security group.

2.2.2 Step 1: Create 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. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. Click **Create VPC**.
The **Create VPC** page is displayed.
4. 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.

Table 2-2 VPC parameter descriptions

Parameter	Description	Example Value
Region	Select the region nearest to you to ensure the lowest latency possible.	-
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 	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 <i>Enterprise Management User Guide</i>.</p>	default
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Retain the default settings.
Tag	The VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC.	<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 2-3 Subnet 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-01
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set IPv6 CIDR Block to Enable . 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.	-
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
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including Gateway and DNS Server Address .	Retain the default settings.
Gateway	The gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1

Parameter	Description	Example Value
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of five 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. Unit: Day or hour</p> <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
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses.</p> <p>If you do not specify this parameter, no additional NTP server IP addresses will be added.</p> <p>Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.</p>	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet.	<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>	N/A

Table 2-4 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 letters, digits, underscores (_), and hyphens (-). 	vpc_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	vpc-01

Table 2-5 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 letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

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

2.2.3 Step 2: Create 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
4. Click **Create Subnet**.
The **Create Subnet** page is displayed.
5. Set the parameters as prompted.

Table 2-6 Parameter descriptions

Parameter	Description	Example Value
VPC	The VPC for which you want to create a subnet.	-
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
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set IPv6 CIDR Block to Enable . 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.	-
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

Parameter	Description	Example Value
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of five DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If you do not specify this parameter, no additional NTP server IP addresses will be added.</p>	192.168.2.1
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. Unit: Day or hour</p> <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. You can add a maximum of 10 tags to each subnet.</p> <p>The tag key and value must meet the requirements listed in Table 2-7.</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 2-7 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 letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

6. Click **OK**.

Precautions

When a subnet is created, there are five reserved IP addresses, which 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.

2.2.4 Step 3: Create 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.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > 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.
 - In the upper right corner, click **Create Security Group**.
The **Create Security Group** page is displayed.
 - Configure the parameters as prompted.

Table 2-8 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


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

2.2.5 Step 4: Add 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.

Adding Rules to a Security Group

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.

4. 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.
5. On the **Inbound Rules** tab, click **Add Rule**.
The **Add Inbound Rule** dialog box is displayed.
6. Configure required parameters.
You can click + to add more inbound rules.

Table 2-9 Inbound rule parameter description

Parameter	Description	Example Value
Type	Source IP address version. You can select: <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
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
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Inbound rules control incoming traffic over specific ports to instances in the security group.	22, or 22-30
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. <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) 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
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

7. Click **OK**.
The inbound rule list is displayed.
8. On the **Outbound Rules** tab, click **Add Rule**.
The **Add Outbound Rule** dialog box is displayed.

9. Configure required parameters.
You can click + to add more outbound rules.

Table 2-10 Outbound rule parameter description

Parameter	Description	Example Value
Type	Destination IP address version. You can select: <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
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
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Outbound rules control outgoing traffic over specific ports from instances in the security group.	22, or 22-30
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. For example: <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	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

10. 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 2-11](#) shows the rule.

Table 2-11 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 2-2 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 2-3 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.

2.3 Configuring a VPC for ECSs That Access the Internet Using EIPs


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. Click **Create VPC**.
The **Create VPC** page is displayed.
4. 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.

Table 2-12 VPC parameter descriptions

Parameter	Description	Example Value
Region	Select the region nearest to you to ensure the lowest latency possible.	-
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
IPv4 CIDR Block	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). The following CIDR blocks are supported: <ul style="list-style-type: none"> • 10.0.0.0/8-24 • 172.16.0.0/12-24 • 192.168.0.0/16-24 	192.168.0.0/16
Enterprise Project	The enterprise project to which the VPC belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Retain the default settings.
Tag	The VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC.	<ul style="list-style-type: none"> • Key: vpc_key1 • Value: vpc-01

Parameter	Description	Example Value
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 2-13 Subnet parameter descriptions

Parameter	Description	Example Value
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>	192.168.0.0/24
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>	-
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.

Parameter	Description	Example Value
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
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of five 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. Unit: Day or hour</p> <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
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses.</p> <p>If you do not specify this parameter, no additional NTP server IP addresses will be added.</p> <p>Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.</p>	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet.	<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>	N/A

Table 2-14 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 letters, digits, underscores (_), and hyphens (-). 	vpc_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	vpc-01

Table 2-15 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 letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

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

2.3.1 Overview

If your ECSs need to access the Internet (for example, the ECSs functioning as the service nodes for deploying a website), you can follow the procedure shown in [Figure 2-4](#) to bind EIPs to the ECSs.

Figure 2-4 Configuring the network

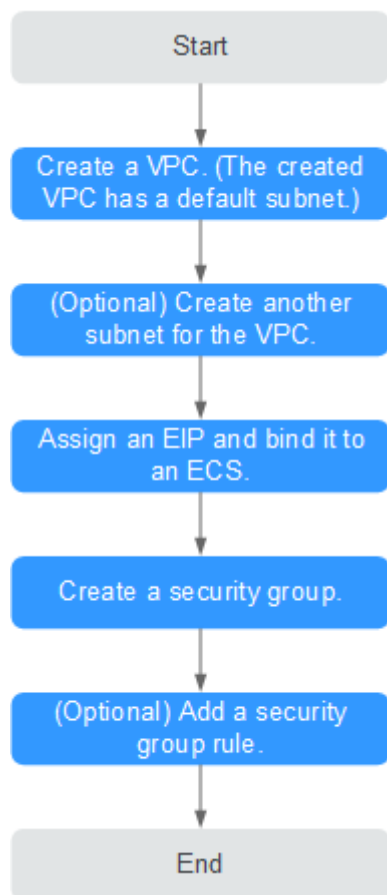


Table 2-16 describes the different tasks in the procedure for configuring the network.

Table 2-16 Configuration process description

Task	Description
Create a VPC.	This task is mandatory. A created VPC comes with a default subnet you specified. After the VPC is created, you can create other required network resources in the VPC based on your service requirements.
Create another subnet for the VPC.	This task is optional. If the default subnet cannot meet your requirements, you can create one. The new subnet is used to assign IP addresses to NICs added to the ECS.

Task	Description
Assign an EIP and bind it to an ECS.	This task is mandatory. You can assign an EIP and bind it to an ECS for Internet access.
Create a security group.	This task is mandatory. You can create a security group and add ECSs in the VPC to the security group to improve ECS access security. After a security group is created, it has default rules, which allow all outgoing data packets. ECSs in a security group can access each other without the need to add rules.
Add a security group rule.	This task is optional. If the default rule does not meet your service requirements, you can add security group rules.

2.3.2 Step 1: Create 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. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. Click **Create VPC**.
The **Create VPC** page is displayed.
4. 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.

Table 2-17 VPC parameter descriptions

Parameter	Description	Example Value
Region	Select the region nearest to you to ensure the lowest latency possible.	-

Parameter	Description	Example Value
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
IPv4 CIDR Block	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). The following CIDR blocks are supported: <ul style="list-style-type: none"> • 10.0.0.0/8-24 • 172.16.0.0/12-24 • 192.168.0.0/16-24 	192.168.0.0/16
Enterprise Project	The enterprise project to which the VPC belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Retain the default settings.
Tag	The VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC.	<ul style="list-style-type: none"> • Key: vpc_key1 • Value: vpc-01

Parameter	Description	Example Value
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 2-18 Subnet parameter descriptions

Parameter	Description	Example Value
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>	192.168.0.0/24
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>	-
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.

Parameter	Description	Example Value
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
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of five 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. Unit: Day or hour</p> <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
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses.</p> <p>If you do not specify this parameter, no additional NTP server IP addresses will be added.</p> <p>Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.</p>	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet.	<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>	N/A

Table 2-19 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 letters, digits, underscores (_), and hyphens (-). 	vpc_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	vpc-01

Table 2-20 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 letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

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

2.3.3 Step 2: Create 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
4. Click **Create Subnet**.
The **Create Subnet** page is displayed.
5. Set the parameters as prompted.

Table 2-21 Parameter descriptions

Parameter	Description	Example Value
VPC	The VPC for which you want to create a subnet.	-
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
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set IPv6 CIDR Block to Enable . 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.	-
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

Parameter	Description	Example Value
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of five DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If you do not specify this parameter, no additional NTP server IP addresses will be added.</p>	192.168.2.1
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. Unit: Day or hour</p> <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. You can add a maximum of 10 tags to each subnet.</p> <p>The tag key and value must meet the requirements listed in Table 2-22.</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 2-22 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 letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> Can contain a maximum of 43 characters. Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

- Click **OK**.

Precautions

When a subnet is created, there are five reserved IP addresses, which 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.

2.3.4 Step 3: Assign an EIP and Bind It to an ECS

Scenarios

You can assign an EIP and bind it to an ECS so that the ECS can access the Internet.

Assigning an EIP

- Log in to the management console.
- Click  in the upper left corner and choose **Network > Elastic IP**.
- On the displayed page, click **Assign EIP**.

4. Set the parameters as prompted.

Table 2-23 Parameter descriptions

Parameter	Description	Example Value
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.	N/A
EIP Type	Dynamic BGP: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
Billed By	The following bandwidth types are available: <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 and is suitable for scenarios with staggered traffic. 	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
EIP Name	The name of the EIP.	eip-test
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 2-24 .	<ul style="list-style-type: none"> Key: ipv4_key1 Value: 3005eip
Quantity	The number of EIPs you want to purchase.	1
Enterprise Project	The enterprise project that the EIP belongs to. An enterprise project lets you manage cloud resources and personnel by enterprise project. The default project is default . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default

Table 2-24 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 letters, digits, underscores (_), and hyphens (-). 	ipv4_key1
Value	<ul style="list-style-type: none"> Can contain a maximum of 43 characters. Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	3005eip

5. Click **Create Now**.
6. 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**.

2.3.5 Step 4: Create 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.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. In the upper right corner, click **Create Security Group**.
The **Create Security Group** page is displayed.
5. Configure the parameters as prompted.

Table 2-25 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 lets you manage cloud resources and personnel by enterprise project. 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 description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-


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

2.3.6 Step 5: Add 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.

Adding Rules to a Security Group

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.

4. 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.
5. On the **Inbound Rules** tab, click **Add Rule**.
The **Add Inbound Rule** dialog box is displayed.
6. Configure required parameters.
You can click + to add more inbound rules.

Table 2-26 Inbound rule parameter description

Parameter	Description	Example Value
Type	Source IP address version. You can select: <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
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
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Inbound rules control incoming traffic over specific ports to instances in the security group.	22, or 22-30
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. <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) 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
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

7. Click **OK**.
The inbound rule list is displayed.
8. On the **Outbound Rules** tab, click **Add Rule**.
The **Add Outbound Rule** dialog box is displayed.

9. Configure required parameters.
You can click + to add more outbound rules.

Table 2-27 Outbound rule parameter description

Parameter	Description	Example Value
Type	Destination IP address version. You can select: <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
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
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Outbound rules control outgoing traffic over specific ports from instances in the security group.	22, or 22-30
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. For example: <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	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

10. Click **OK**.
The outbound rule list is displayed and you can view your added rule.

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 2-28](#) shows the rule.

Table 2-28 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 2-5 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 2-6 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.

3 VPC and Subnet

3.1 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 by referring to [What Is a 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 3-1 lists the supported VPC CIDR blocks.

Table 3-1 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	$2^{16}-2=65534$

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.

- After a subnet is created, its CIDR block cannot be modified. Subnets in the same VPC cannot overlap.

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 [What Is a 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.

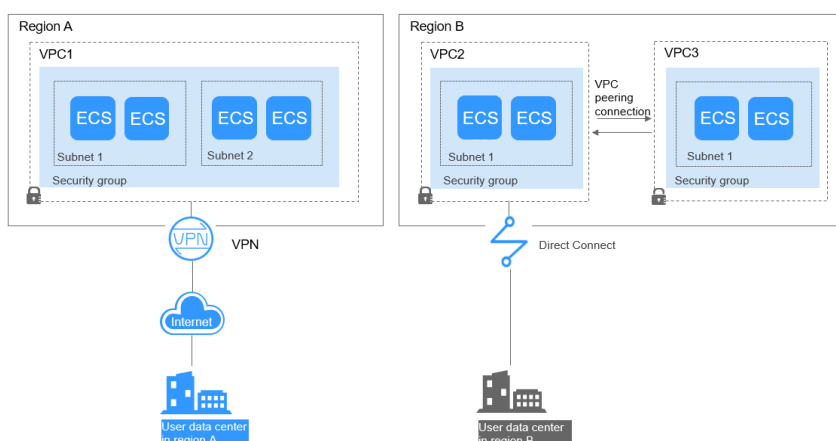
You cannot add two routes with the same destination to a VPC route table even if their next hop types are different, because the destination determines the route priority. According to the longest match routing rule, the destination with a higher matching degree is preferentially selected for packet 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 3-1](#), 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 3-1 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.

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.

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.

3.2 VPC

3.2.1 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. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. Click **Create VPC**.
The **Create VPC** page is displayed.
4. 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.

Table 3-2 VPC parameter descriptions

Parameter	Description	Example Value
Region	Select the region nearest to you to ensure the lowest latency possible.	-
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
IPv4 CIDR Block	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). The following CIDR blocks are supported: <ul style="list-style-type: none"> • 10.0.0.0/8-24 • 172.16.0.0/12-24 • 192.168.0.0/16-24 	192.168.0.0/16

Parameter	Description	Example Value
Enterprise Project	The enterprise project to which the VPC belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default
Advanced Settings	Click the drop-down arrow to set advanced VPC parameters, including tags.	Retain the default settings.
Tag	The VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC.	<ul style="list-style-type: none"> • Key: vpc_key1 • Value: vpc-01
Description	Supplementary information about the VPC. This parameter is optional. The VPC description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

Table 3-3 Subnet 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-01
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24

Parameter	Description	Example Value
IPv6 CIDR Block	Specifies whether to set IPv6 CIDR Block to Enable . 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.	-
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
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including Gateway and DNS Server Address .	Retain the default settings.
Gateway	The gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1
DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of five DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	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. Unit: Day or hour</p> <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
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses.</p> <p>If you do not specify this parameter, no additional NTP server IP addresses will be added.</p> <p>Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.</p>	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet.	<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>	N/A

Table 3-4 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 letters, digits, underscores (_), and hyphens (-). 	vpc_key1
Value	<ul style="list-style-type: none"> Can contain a maximum of 43 characters. Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	vpc-01

Table 3-5 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 letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> Can contain a maximum of 43 characters. Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

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


3.2.2 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](#)


Modifying the Name and Description of a VPC

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.

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

3. 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 choose **Network > 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. 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.

Figure 3-2 Modifying network address and subnet mask

Edit CIDR Block ×

VPC vpc-0809

CIDR Block · · · / ▼

- If a VPC has subnets, you only can change its subnet mask.

Figure 3-3 Modifying subnet mask

Edit CIDR Block

VPC vpc-0809

CIDR Block 192 · 168 · 0 · 0 / 16

- Click **OK**.

3.2.3 Managing VPC Tags

Scenarios

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

You can add a tag to a VPC when creating the VPC, or you can add a tag to a created VPC on the VPC details page. A maximum of 10 tags can be added to each VPC.


A tag consists of a key and value pair. [Table 3-6](#) lists the tag key and value requirements.

Table 3-6 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 letters, digits, underscores (_), and hyphens (-). 	vpc_key1
Value	<ul style="list-style-type: none"> Can contain a maximum of 43 characters. Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	vpc-01

Procedure


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

- Log in to the management console.
- Click  in the upper left corner and choose **Network > Virtual Private Cloud**.

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

3. In the search box above the VPC list, click anywhere in the search box.
Click the tag key and then the value as required. The system filters resources based on the tag you select.
Click anywhere in the search box to add the next 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 VPCs, the VPCs containing all specified tags will be displayed.

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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. 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.
4. 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**.


3.2.4 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.

3. On the **Virtual Private Cloud** page, locate the VPC and click its name.
The VPC details page is displayed.
4. In the **VPC Information** area, view the VPC ID.


Click  next to ID to copy the VPC ID.

3.2.5 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the VPC list, click the name of the VPC for which the topology is to be viewed.
The VPC details page is displayed.
4. 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.


3.2.6 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the VPC list, select one or more VPCs you want to export and click **Export** in the upper left corner.

The system will automatically export information about all of your VPCs as an Excel file to a local directory.

3.2.7 Deleting a VPC

Scenarios


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

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 **Network > 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?](#)

3.3 Subnet

3.3.1 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
4. Click **Create Subnet**.
The **Create Subnet** page is displayed.
5. Set the parameters as prompted.

Table 3-7 Parameter descriptions

Parameter	Description	Example Value
VPC	The VPC for which you want to create a subnet.	-
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
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set IPv6 CIDR Block to Enable . 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.	-
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

Parameter	Description	Example Value
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of five DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If you do not specify this parameter, no additional NTP server IP addresses will be added.</p>	192.168.2.1
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. Unit: Day or hour</p> <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. You can add a maximum of 10 tags to each subnet.</p> <p>The tag key and value must meet the requirements listed in Table 3-8.</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 3-8 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 letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

6. Click **OK**.

Precautions

When a subnet is created, there are five reserved IP addresses, which 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.

3.3.2 Modifying a Subnet

Scenarios

Modify the subnet name and DNS server address.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.


3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**. The **Subnets** page is displayed.
4. In the subnet list, locate the target subnet and click its name. The subnet details page is displayed.
5. On the **Summary** tab, click  on the right of the parameter to be modified and modify the parameter as prompted.

Table 3-9 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
DNS Server Address	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. DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers. If you want to use other public DNS servers for resolution, you can change the default DNS server addresses. A maximum of five DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	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. Unit: Day or hour</p> <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>	-
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If you do not specify this parameter, no additional NTP server IP addresses will be added.</p> <p>A maximum of four unique NTP server IP addresses can be configured. Multiple IP addresses must be separated by a comma (,). If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.</p>	192.168.2.1

Parameter	Description	Example Value
Description	Supplementary information about the subnet. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

6. Click **OK**.

3.3.3 Managing Subnet Tags

Scenarios

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

You can add a tag to a subnet when creating the subnet, or you can add a tag to a created subnet on the subnet details page. A maximum of 10 tags can be added to each subnet.


A tag consists of a key and value pair. [Table 3-10](#) lists the tag key and value requirements.

Table 3-10 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 letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	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 choose **Network > Virtual Private Cloud**.

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

3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. In the search box above the subnet list, click the search box.
Click the tag key and then the value as required. The system filters resources based on the tag you select.
Click anywhere in the search box to add the next 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 VPCs, the VPCs containing all specified tags will be displayed.

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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. In the subnet list, locate the target subnet and click its name.
5. 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**.

3.3.4 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, 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. Locate the target subnet and click its name.
The subnet details page is displayed.
5. 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.
6. Delete resources from the subnet.

Table 3-11 Viewing and deleting resources in a subnet

Resource	Reference
Load balancer	You can directly switch to load balancers from the subnet details page. <ol style="list-style-type: none">1. Click the load balancer quantity. The load balancer list is displayed.2. Locate the row that contains the load balancer and click Delete in the Operation column.

3.3.5 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, system interface, and DHCP.

- 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. Locate the target subnet and click its name.
The subnet details page is displayed.
5. 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.

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?](#)

3.3.6 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. In the subnet list, select one or more subnets you want to export and click **Export** in the upper left corner.

The system will automatically export information about all of your subnets as an Excel file to a local directory.

3.3.7 Deleting a Subnet

Scenarios


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

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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. 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.
5. 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?](#)

3.4 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 3-4](#) shows how an IPv4 and IPv6 dual-stack network works.

Figure 3-4 An IPv4 and IPv6 dual-stack network

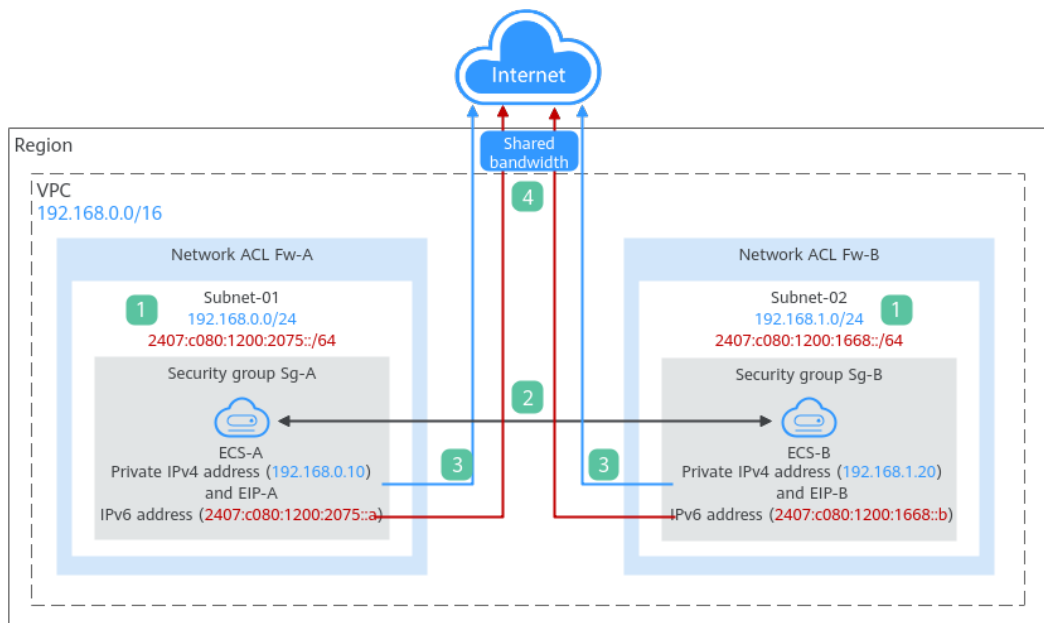


Table 3-12 Steps for deploying a dual-stack network

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 3-4 , 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 3-4, 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 3-4, 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>

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 3-13](#) describes how you can build and use an IPv6 network.

Table 3-13 Operation guide on IPv6 networks

Scenario	Description	Reference
Creating an IPv6 subnet	<p>Select Enable for IPv6 CIDR Block when creating a subnet. An IPv6 CIDR block will be automatically assigned to the subnet.</p> <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

Scenario	Description	Reference
Adding an IPv6 route to the VPC route table	<p>Add a route with Destination and Next Hop set to an IPv4 or IPv6 CIDR block.</p> <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

4 Route Tables

4.1 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.

- **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**

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.

 **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 4-1](#) 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 4-1 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
VPN gateway	Traffic intended for the destination is forwarded to a VPN gateway.	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

Next Hop Type	Description	Supported 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

 **NOTE**

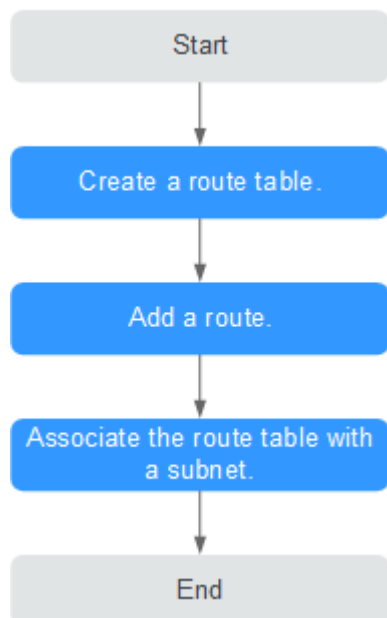
If you specify the destination when creating a resource, a system route is delivered. If you do not specify a destination when creating a resource, a custom route that can be modified or deleted is delivered.

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.

Custom Route Table Configuration Process

Figure 4-1 shows the process of creating and configuring a custom route table.

Figure 4-1 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](#).

- 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.

4.2 Managing Route Tables

4.2.1 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.

Procedure


- Log in to the management console.
- Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
- In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
- In the upper right corner, click **Create Route Table**. On the displayed page, configure parameters as prompted.

Table 4-2 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 >).	-

Parameter	Description	Example Value
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.	-

5. 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**.

4.2.2 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.


3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. In the route table list, locate the row that contains the target route table and click **Associate Subnet** in the **Operation** column.
5. Select the subnet to be associated.
6. Click **OK**.

4.2.3 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. Click the name of the target route table.
5. On the **Associated Subnets** tab page, click **Change Route Table** in the **Operation** column and select a new route table as prompted.
6. 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.

4.2.4 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. Locate the target subnet and click its name.
The subnet details page is displayed.

5. In the right of the subnet details page, view the route table associated with the subnet.
6. Click the name of the route table.
The route table details page is displayed. You can further view the route information.


4.2.5 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. 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.

4.2.6 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.

3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. In the route table list, select one or more route tables you want to export and click **Export** in the upper left corner.
The system will automatically export information about all of your route tables as an Excel file to a local directory.

4.2.7 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.
- 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 choose **Network > Virtual Private Cloud**. The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. 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.
5. Click **Yes**.

4.3 Managing Routes

4.3.1 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. In the route table list, click the name of the route table to which you want to add a route.
5. Click **Add Route** and set parameters as prompted.
You can click **+** to add more routes.

Table 4-3 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 or Direct Connect gateway.</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>	-

6. Click **OK**.

4.3.2 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. In the route table list, click the name of the target route table.
5. Locate the row that contains the route to be modified and click **Modify** in the **Operation** column.
6. Modify the route information in the displayed dialog box.

Table 4-4 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

Parameter	Description	Example Value
Next Hop Type	Mandatory Set the type of the next hop. NOTE 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 or Direct Connect gateway .	VPC peering connection
Next Hop	Mandatory Set the next hop. The resources in the drop-down list box are displayed based on the selected next hop type.	peer-AB
Description	Optional Enter the description of the route in the text box as required.	-

- Click **OK**.

4.3.3 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 4-5 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 4-5 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
VPN gateway	No	Yes
Direct Connect gateway	No	Yes

Next Hop Type	Can Be Replicated to Default Route Table	Can Be Replicated to Custom Route Table
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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. 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.
5. 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.
6. Click **OK**.

4.3.4 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 gateway

The following figure shows a route with **VPN gateway** as **Next Hop Type**. If you want to delete such a route, click the next hop hyperlink to delete the corresponding resource.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Route Tables**.
4. Locate the target route table and click its name.
The route table details page is displayed.
5. 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.
6. Confirm the information and click **Yes**.

4.4 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 **Network** 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. In the upper left corner of the page, click . In the service list, choose **Computing > Elastic Cloud Server**.
3. 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.
4. On the displayed ECS details page, click the **NICs** tab.
5. 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.

6. 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](#).
7. On the ECS console, use the remote login function to log in to the ECS where you plan to configure SNAT.
8. Run the following command and enter the password of user **root** to switch to user **root**:
9. 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 www.google.com

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

```
[root@localhost ~]# ping www.google.com
PING www.google.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
```

10. 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 **13**.
- If IP forwarding in Linux is disabled, go to **11** 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.

11. 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.

12. Run the following command to make the change take effect:

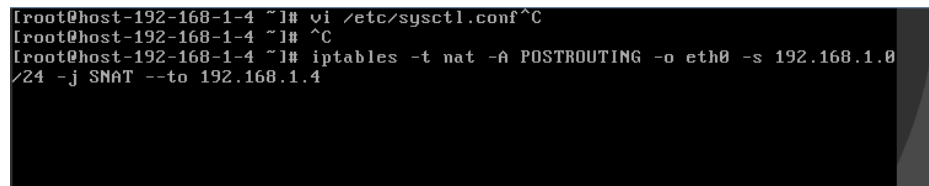
```
sysctl -p /etc/sysctl.conf
```

13. 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 4-2 Configuring SNAT



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 [13](#) 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
```

14. Check whether the configuration is successful. If information similar to [Figure 4-3](#) (for example, 192.168.1.0/24) is displayed, the configuration was successful.

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

Figure 4-3 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 ~]# _
```

15. 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.

5 Virtual IP Address

5.1 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.

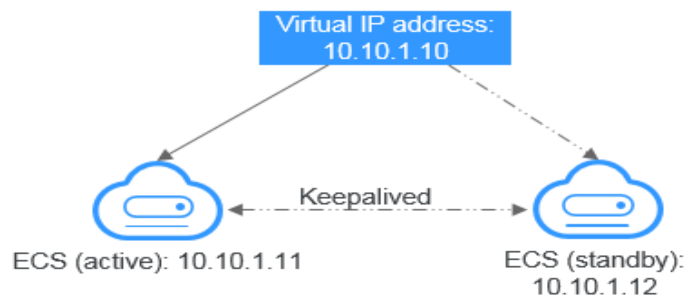
Networking

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**

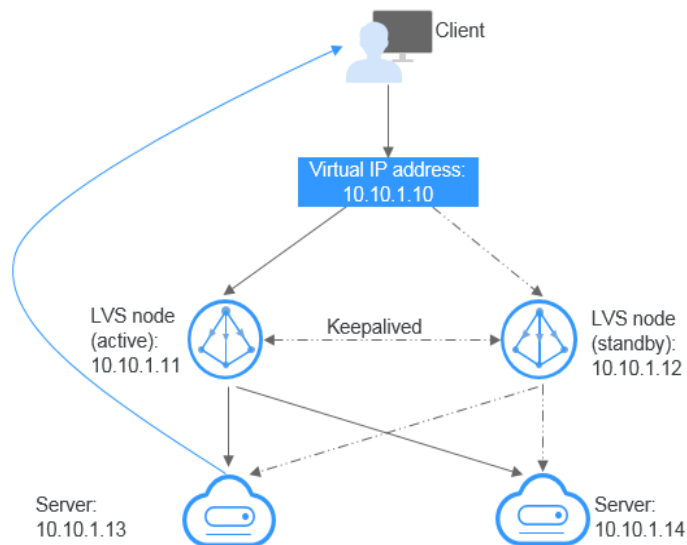
To improve service availability and eliminate single points of failure, you can deploy ECSs in the active/standby pair or deploy one active ECS and multiple standby ECSs. And then, you can bind the same virtual IP address to these ECSs. If the active ECS becomes faulty, a standby ECS takes over services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

Figure 5-1 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 5-2 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 VPN for security and Direct Connect for stable connectivity. The VPC peering connection is needed so that the 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](#).

5.2 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
4. In the subnet list, click the name of the subnet where a virtual IP address is to be assigned.
5. Click the **IP Addresses** tab and click **Assign Virtual IP Address**.

6. Select an IP address type. This parameter is available only in regions supporting IPv6.
 - IPv4
 - IPv6
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.

5.3 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
The **Subnets** page is displayed.
4. Click the name with a hyperlink of the subnet that the virtual IP address belongs to.
The subnet details page is displayed.
5. 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.
6. 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

- 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.
-

5.4 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 choose **Network > Elastic IP**.
The EIP list page is displayed.
3. Locate the row that contains the EIP to be bound to the virtual IP address, and click **Bind** in the **Operation** column.
4. In the **Bind EIP** dialog box, set **Instance Type** to **Virtual IP address**.
5. In the virtual IP address list, select the virtual IP address to be bound and click **OK**.

5.5 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 5-1](#).

Table 5-1 Releasing a virtual IP address that is being used by a resource

Prompts	Cause Analysis and Solution
This operation cannot be performed because the IP address is bound to an instance or an EIP. Unbind the IP address and try again.	This virtual IP address is being used by an EIP or an ECS. Release the virtual IP address.
This operation cannot be performed because the IP address is being used by a system component.	The virtual IP address is being used by an RDS DB instance. Delete the DB instance, which will also release its virtual IP address.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
4. Click the name of the subnet that the virtual IP address belongs to.
5. 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.
6. Confirm the information and click **Yes**.

5.6 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.

5.7 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. In the upper left corner of the page, click . In the service list, choose **Computing > Elastic Cloud Server**.
3. In the ECS list, click the ECS name.
4. On the displayed ECS details page, click the **NICs** tab.
5. Check that **Source/Destination Check** is disabled.

6 Access Control

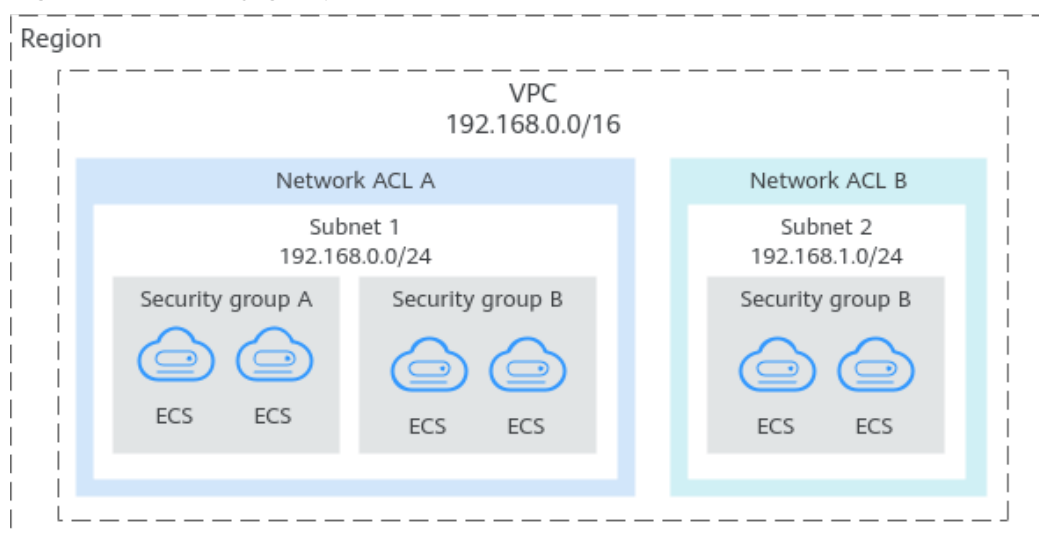
6.1 What Is Access Control?

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 6-1 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 6-1 Security groups and network ACLs



Differences Between Security Groups and Network ACLs

Table 6-1 describes detailed differences between security groups and network ACLs.

Table 6-1 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	If there are conflicting rules, they are combined and applied together.	If rules conflict, the rule with the highest priority will be applied.
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.

6.2 Security Group

6.2.1 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.

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.
 - **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 apply 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 Constraints

- By default, you can add up to 50 security group rules to a security group.
- By default, you can add an ECS or extension NIC to up to five security groups. In such a case, the rules of all the selected security groups are aggregated to take effect.
- A security group can have no more than 6,000 instances associated, or its performance will deteriorate.

6.2.2 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:

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 6-2 Default security group

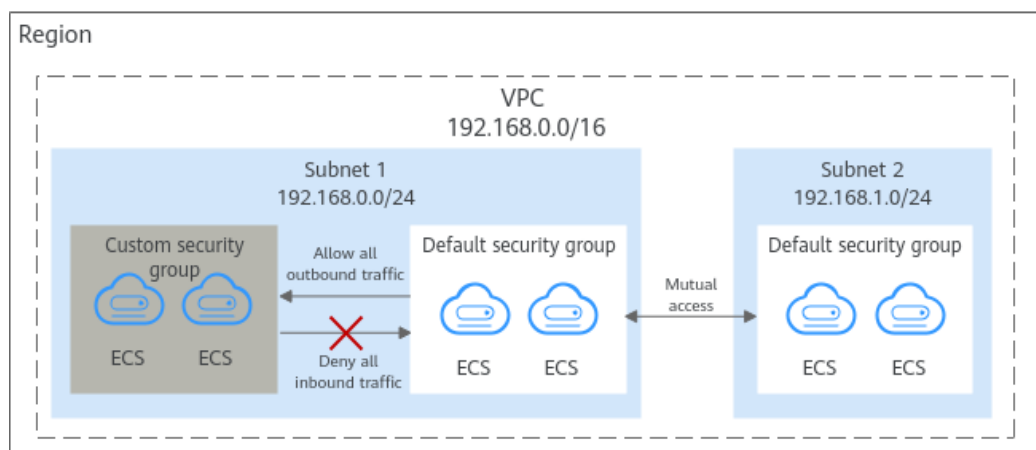


Table 6-2 describes the default rules for the default security group.

Table 6-2 Default security group rules

Direction	Protocol	Port/Range	Source/Destination	Description
Outbound	All	All	Destination: 0.0.0.0/0	Allows all outbound traffic.
Inbound	All	All	Source: the current security group (for example, sg-xxxxx)	Allows communications among ECSs within the security group and denies all inbound traffic (incoming data packets).
Inbound	TCP	22	Source: 0.0.0.0/0	Allows all IP addresses to access Linux ECSs over SSH.
Inbound	TCP	3389	Source: 0.0.0.0/0	Allows all IP addresses to access Windows ECSs over RDP.

6.2.3 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](#)

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 6-3](#).

Table 6-3 Default outbound rules in a security group

Direction	Protocol & Port	Destination	Description
Outbound	All	0.0.0.0/0	This rule allows the instances in the security group to access any IPv4 address over any port.
Outbound	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 6-4](#).
- To remotely log in to a Windows ECS using RDP, enable port 3389. For details, see [Table 6-5](#).

Table 6-4 Remotely logging in to a Linux ECS using SSH

Direction	Protocol & Port	Source
Inbound	TCP: 22	IP address: 0.0.0.0/0

Table 6-5 Remotely logging in to a Windows ECS using RDP

Direction	Protocol & Port	Source
Inbound	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 6-6](#).

Table 6-6 Remotely logging in to an ECS using a specified IP address

ECS Type	Direction	Protocol & Port	Source
Linux ECS	Inbound	TCP: 22	IP address: 192.168.0.0/24
Windows ECS	Inbound	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 6-7 Remotely connecting to an ECS from a local server to upload or download files

Direction	Protocol & Port	Source
Inbound	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 6-8 Setting up a website on an ECS to provide services externally

Direction	Protocol & Port	Source
Inbound	TCP: 80	IP address: 0.0.0.0/0
Inbound	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 6-9 Using ping command to verify network connectivity

Direction	Protocol & Port	Source
Inbound	ICMP: All	IP address: 0.0.0.0/0

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 6-10 Enabling communications between instances in different security groups

Direction	Protocol & Port	Source
Inbound	TCP: 3306	Security group: sg-A

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 6-11 Allowing external instances to access the database deployed on an ECS

Direction	Protocol & Port	Source	Description
Inbound	TCP: 3306	Security group: sg-A	This rule allows the ECSs in security group sg-A to access the MySQL database service.
Inbound	TCP: 1521	Security group: sg-B	This rule allows the ECSs in security group sg-B to access the Oracle database service.
Inbound	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	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.

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 6-13](#) 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 6-12 Allowing ECSs to access specific external websites

Direction	Protocol & Port	Destination	Description
Outbound	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.

Direction	Protocol & Port	Destination	Description
Outbound	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 6-13 Default outbound rules in a security group

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

6.2.4 Managing a Security Group

6.2.4.1 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.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. In the upper right corner, click **Create Security Group**.
The **Create Security Group** page is displayed.
5. Configure the parameters as prompted.

Table 6-14 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
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

Parameter	Description	Example Value
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

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

6.2.4.2 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.

The security group list is displayed.

4. Locate the row that contains the security group, click **More** in the **Operation** column, and click **Clone**.
5. Select the region and name of the new security group as prompted.
6. Click **OK**.


You can then switch to the required region to view the cloned security group in the security group list.

6.2.4.3 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. 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.
5. Modify the name and description of the security group as required.
6. Click **OK** to save the modification.

6.2.4.4 Deleting a Security Group

Scenarios

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


Notes and Constraints

- The default security group is named **default** and cannot be deleted.
- 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. Locate the row that contains the target security group, click **More** in the **Operation** column, and click **Delete**.
A confirmation dialog box is displayed.
5. Confirm the information and click **OK**.

6.2.5 Managing Security Group Rules

6.2.5.1 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.

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 6-15](#) shows the inbound rules.

Table 6-15 Inbound rules for communication between instances

Direction	Protocol & Port	Source/Destination
Inbound	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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. 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.
5. On the **Inbound Rules** tab, click **Add Rule**.
The **Add Inbound Rule** dialog box is displayed.
6. Configure required parameters.
You can click + to add more inbound rules.

Table 6-16 Inbound rule parameter description

Parameter	Description	Example Value
Type	Source IP address version. You can select: <ul style="list-style-type: none">• IPv4• IPv6	IPv4
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
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Inbound rules control incoming traffic over specific ports to instances in the security group.	22, or 22-30

Parameter	Description	Example Value
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
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

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

Table 6-17 Outbound rule parameter description

Parameter	Description	Example Value
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.</p>	22, or 22-30

Parameter	Description	Example Value
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

10. 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 6-18](#) shows the rule.

Table 6-18 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 6-3 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 6-4 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.

6.2.5.2 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.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. 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.
5. On the **Inbound Rules** tab, click **Fast-Add Rule**.
The **Fast-Add Inbound Rule** dialog box is displayed.
6. Configure required parameters.

Table 6-19 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
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

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

Table 6-20 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)
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"> 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
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

10. Click **OK**.

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

6.2.5.3 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

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list 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 **Modify** in the **Operation** column.
7. Modify the security group rule information as prompted and click **Confirm**.

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

6.2.5.5 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.

Procedure




1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. On the security group list, click the name of the target security group.
The security group details page is displayed.
5. Export and import security group rules.
 - Click  to export all rules of the current security group to an Excel file.
 - Click  to import security group rules from an Excel file into the current security group.

Table 6-21 describes the parameters in the template for importing rules.

Table 6-21 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

Parameter	Description	Example Value
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
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Inbound rules control incoming traffic over specific ports to instances in the security group. Outbound rules control outgoing traffic over specific ports from instances in the security group.	22, or 22-30
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. <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	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:	sg-test[96a8a93f-XXX-d7872990c314]
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 >).	-
Last Modified	The time when the security group was modified.	-

6.2.5.6 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.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list 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. 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.
7. Click **Yes**.

6.2.6 Managing Instances Associated with a Security Group

6.2.6.1 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.

Adding an Instance to a Security Group

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. 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.
5. Click the required instance type tab.
The following operations use **Servers** as an example.
6. Click the **Servers** tab and click **Add**.
The **Add Server** dialog box is displayed.
7. 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Security Groups**.
The security group list is displayed.
4. 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.
5. Click the required instance type tab.
The following operations use **Servers** as an example.
6. 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.
7. Confirm the information and click **Yes**.

6.2.6.2 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. Under **Computing**, 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 be aggregated to apply on 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.

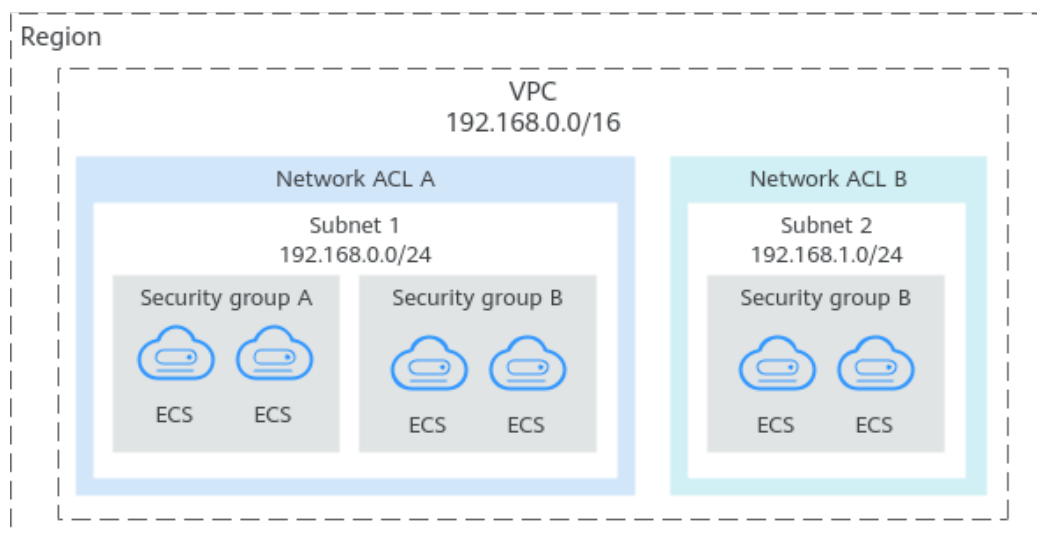
5. Click **OK**.

6.3 Network ACL

6.3.1 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 6-5 shows how a network ACL works.

Figure 6-5 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 apply 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 6-22](#) shows the default rules. You cannot modify or delete the default rules.

Table 6-22 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

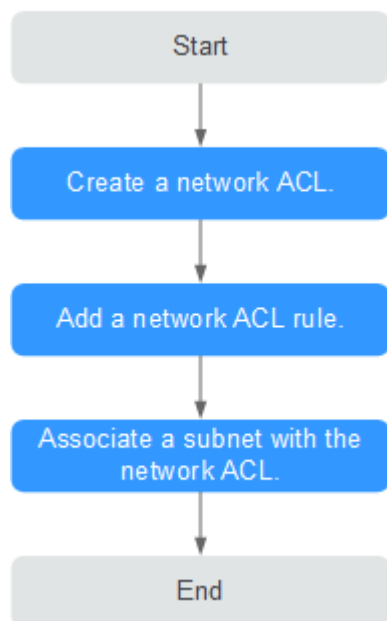
- Each network ACL rule has a priority value where a smaller value corresponds to a higher priority. Any time two rules conflict, the rule with the higher priority is the one that gets applied. The rule whose priority value is an asterisk (*) has the lowest priority.
- If multiple network ACL rules conflict, only the rule with the highest priority takes effect. If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule.

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 6-6](#) shows the procedure for configuring a network ACL.

Figure 6-6 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](#).
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 20 rules in one direction, or performance will deteriorate.

6.3.2 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 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 6-23](#) lists the inbound rules required.

Table 6-23 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 [Changing the Sequence of a Network ACL Rule](#).

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 6-24 lists the inbound and outbound rules required.

Table 6-24 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.

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	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 6-25 lists the inbound and outbound security group rules required.

Table 6-25 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.

6.3.3 Managing Network ACLs

6.3.3.1 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. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. In the right pane displayed, click **Create Network ACL**.
5. On the **Create Network ACL** page, configure parameters as prompted.

Table 6-26 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 (_), 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


6. Click **OK**.





6.3.3.2 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.

3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the displayed page, click  on the right of **Name** and edit the network ACL name.
6. Click  to save the new network ACL name.
7. Click  on the right of **Description** and edit the network ACL description.
8. Click  to save the new network ACL description.


6.3.3.3 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the row that contains the network ACL, click **More** in the **Operation** column, and click **Enable** or **Disable**.
5. Click **Yes** in the displayed dialog box.

6.3.3.4 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.


3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the displayed page, click the **Inbound Rules**, **Outbound Rules**, and **Associated Subnets** tabs one by one to view details about inbound rules, outbound rules, and subnet associations.

6.3.3.5 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the network ACL, click **More** in the **Operation** column, and click **Delete**.
5. Click **Yes**.

NOTE

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

6.3.4 Management Network ACL Rules

6.3.4.1 Adding a Network ACL Rule


Scenarios

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

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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.

3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. 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 6-27 Parameter descriptions

Parameter	Description	Example Value
Type	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
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

Parameter	Description	Example Value
Destination	<p>The destination to which the traffic is allowed. The destination can be an IP address or IP address range.</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
Destination Port Range	<p>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.</p> <p>You must specify this parameter if TCP or UDP is selected for Protocol.</p>	22, or 22-30
Description	<p>Supplementary information about the network ACL rule. This parameter is optional.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	N/A


6. Click **OK**.

6.3.4.2 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule and click **Modify** in the **Operation** column. In the displayed

dialog box, configure parameters as prompted. [Table 6-28](#) lists the parameters to be configured.

Table 6-28 Parameter descriptions

Parameter	Description	Example Value
Type	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
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

Parameter	Description	Example Value
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

6. Click **Confirm**.


6.3.4.3 Changing the Sequence of a Network ACL Rule

Scenarios

If you need a rule to take effect before or after a specific rule, you can insert that rule before or after the specific rule.

If multiple network ACL rules conflict, only the rule with the highest priority takes effect.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the target rule, click **More** in the **Operation** column, and select **Insert Rule Above** or **Insert Rule Below**.
6. In the displayed dialog box, configure required parameters and click **OK**.
The rule is inserted. The procedure for inserting an outbound rule is the same as that for inserting an inbound rule.

6.3.4.4 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule, and click **Enable** or **Disable** in the **Operation** column.
6. Click **Yes** in the displayed dialog box.
The rule is enabled or disabled. The procedure for enabling or disabling an outbound rule is the same as that for enabling or disabling an inbound rule.

6.3.4.5 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.

Exporting Network ACL Rules

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.

5. Click  to export the inbound and outbound network ACL rules. The exported rules are stored in an Excel file. You need to download the file to a local directory.

Importing Network ACL Rules


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. Click .
6. Select the Excel file containing the exported network ACL rules and click **Import** to import the rules.

6.3.4.6 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule and click **Delete** in the **Operation** column.
6. Click **Yes** in the displayed dialog box.

Deleting Multiple Network ACL Rules at a Time

You can also select multiple network ACL rules and click **Delete** above the network ACL rule list to delete multiple rules at a time.

6.3.5 Managing Subnets Associated with a Network ACL

6.3.5.1 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](#).

Procedure

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

6.3.5.2 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.

3. In the navigation pane on the left, choose **Access Control > Network ACLs**.
4. Locate the target network ACL and click its name to switch to the page showing details of that particular network ACL.
5. On the displayed page, click the **Associated Subnets** tab.
6. On the **Associated Subnets** page, locate the row that contains the target subnet and click **Disassociate** in the **Operation** column.
7. 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.

7 VPC Peering Connection

7.1 VPC Peering Connection Overview

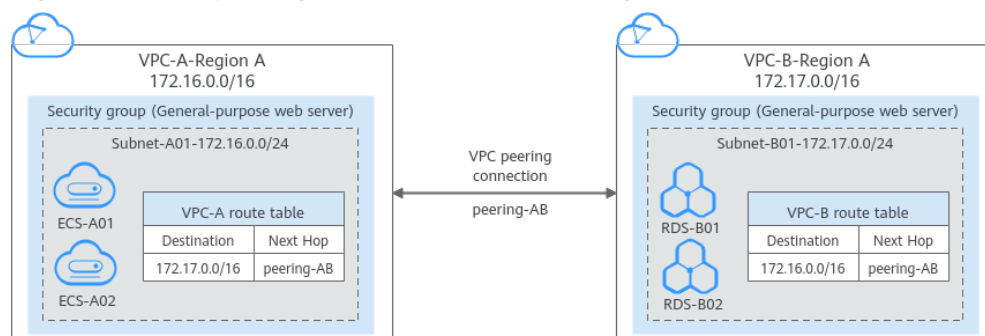
What Is a VPC Peering Connection?

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



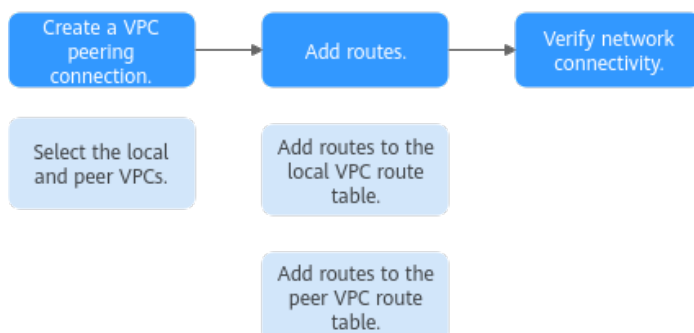
VPC Peering Connection Creation Process

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

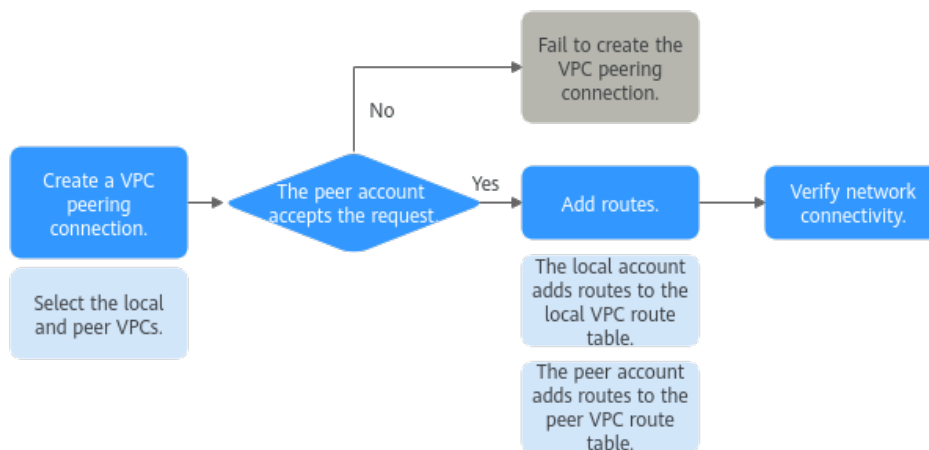


- If two VPCs are in different accounts, the process of creating a VPC peering connection is shown in [Figure 7-3](#).

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 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.

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. 	You can create VPC peering connections to connect specific subnets or ECSs from different VPCs. <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
			<ul style="list-style-type: none"> Peering ECSs in a Central VPC with ECSs in Two Other VPCs
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)

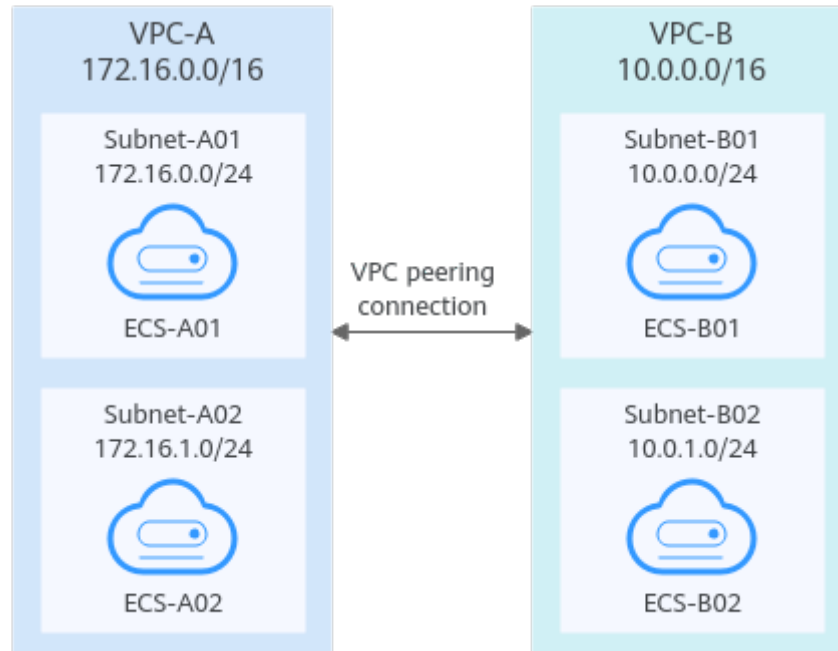


Table 7-2 Peering relationships (IPv4)

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)

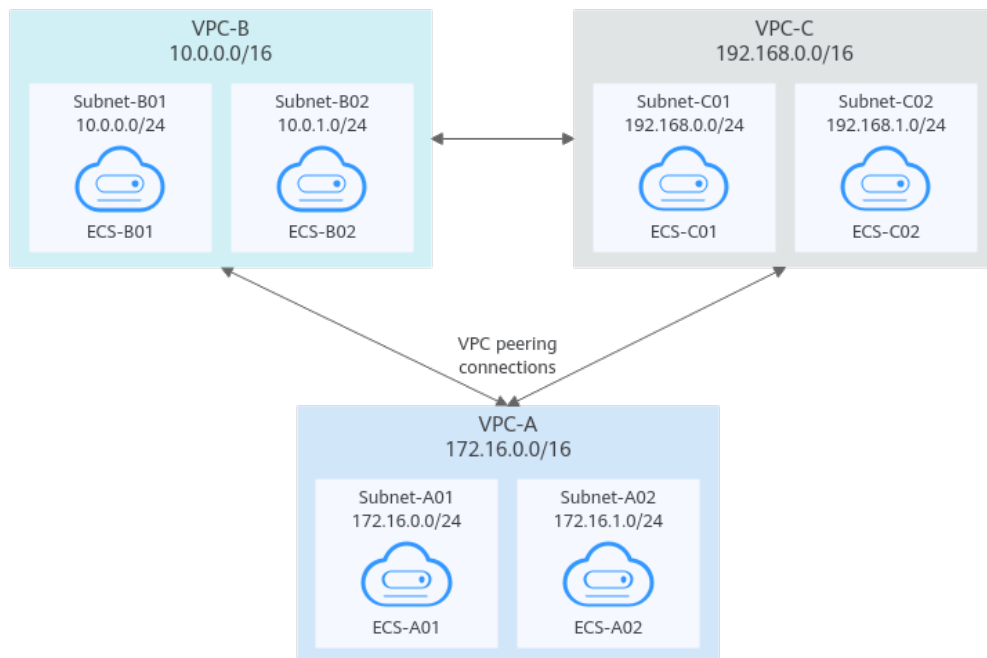


Table 7-4 Peering relationships (IPv4)

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
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)

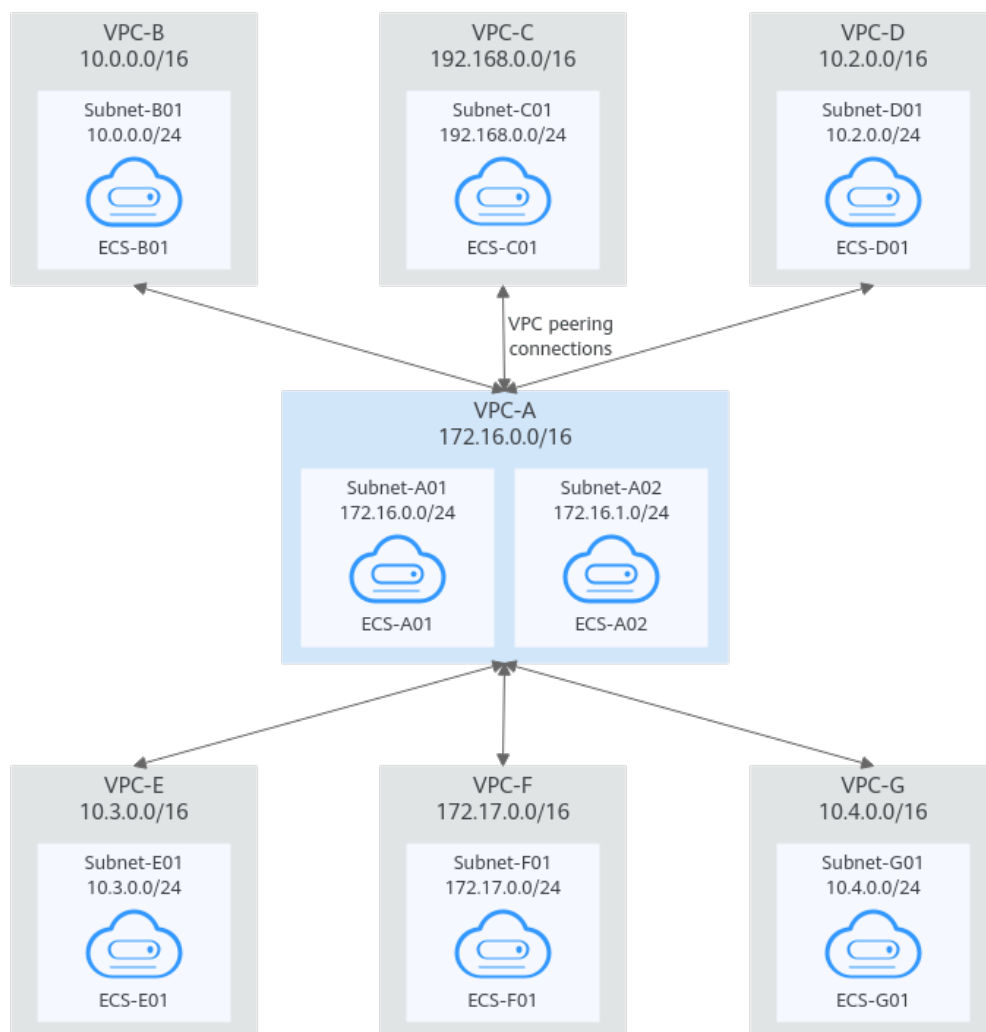


Table 7-6 Peering relationships (IPv4)

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)

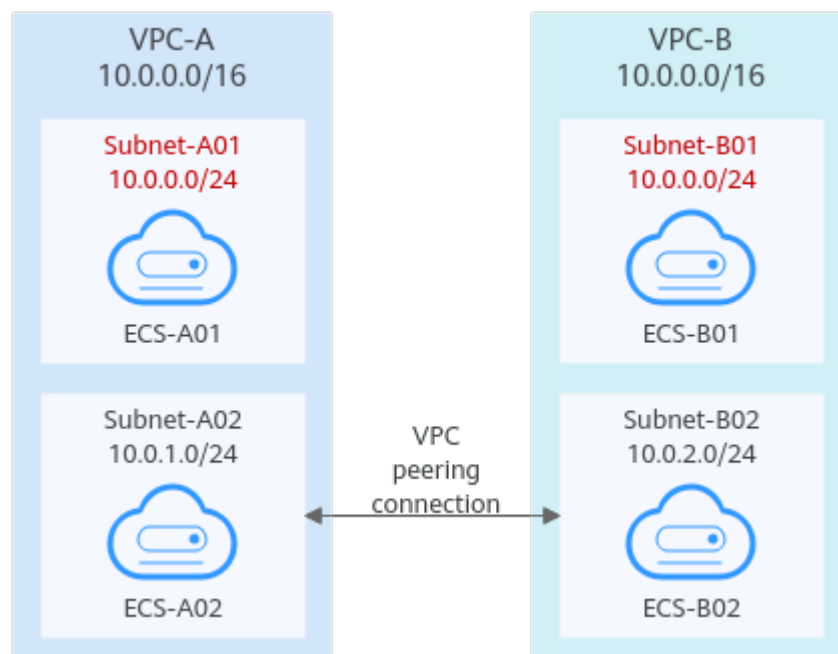


Table 7-8 Peering relationships (IPv4)

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)

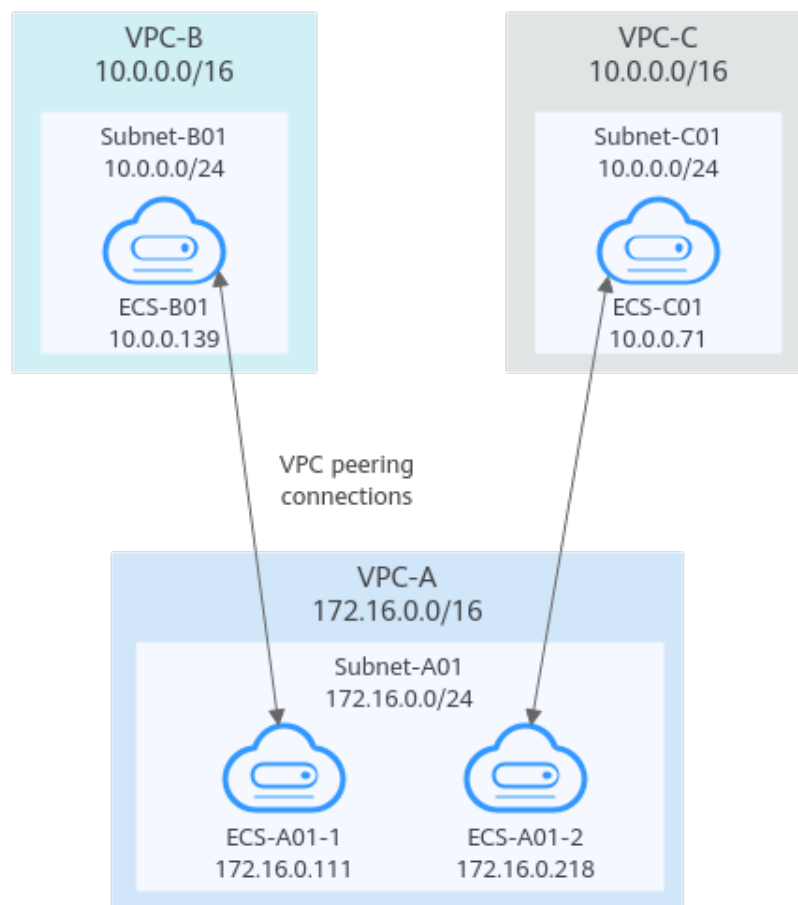


Table 7-10 Peering relationships (IPv4)

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)

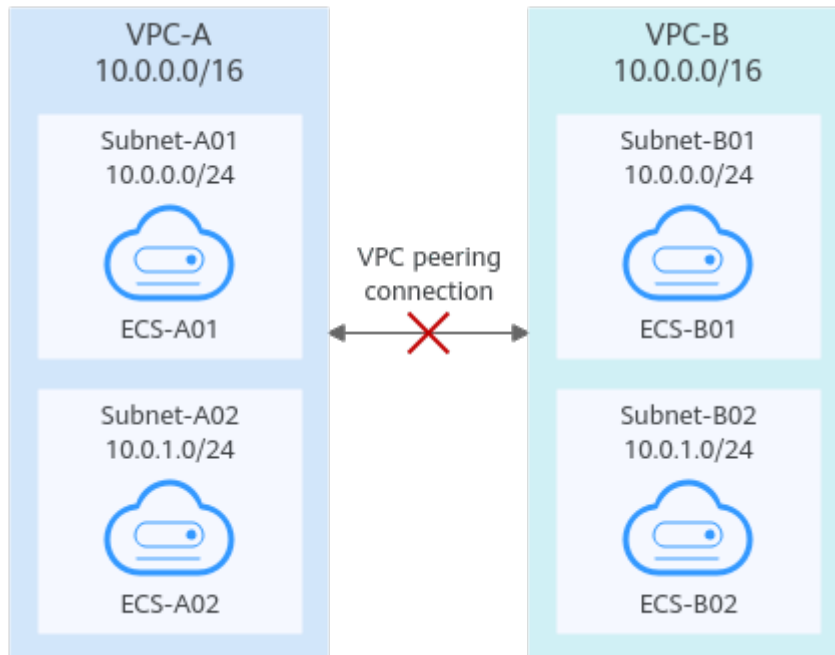


Table 7-12 VPC route table details

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.

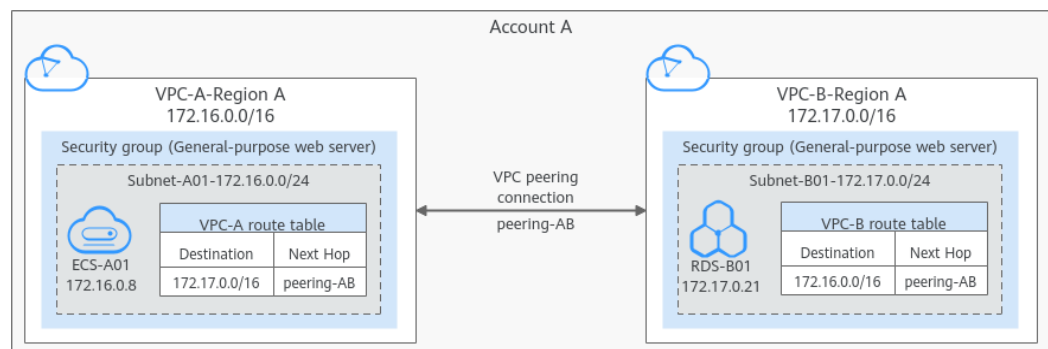
Procedure:

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



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 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. Log in to the management console.


2. Click  in the upper left corner and choose **Network > 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 right corner of the page, click **Create VPC Peering Connection**.
The **Create VPC Peering Connection** dialog box is displayed.
5. Configure the parameters as prompted.
For details, see [Table 7-13](#).

Table 7-13 Parameters for creating a VPC peering connection

Parameter	Description	Example Value
VPC Peering Connection 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 account • Select 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

Parameter	Description	Example Value
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
Description	Optional Enter the description of the VPC peering connection in the text box as required.	peering-AB connects VPC-A and VPC-B.

6. Click **OK**.
A dialog box for adding routes is displayed.
7. In the displayed dialog box, click **Add Now**. On the displayed **Local Routes** page, go to [Step 2: Add Routes for the VPC Peering Connection](#) to add a route.

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

Parameter	Description	Example Value
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:

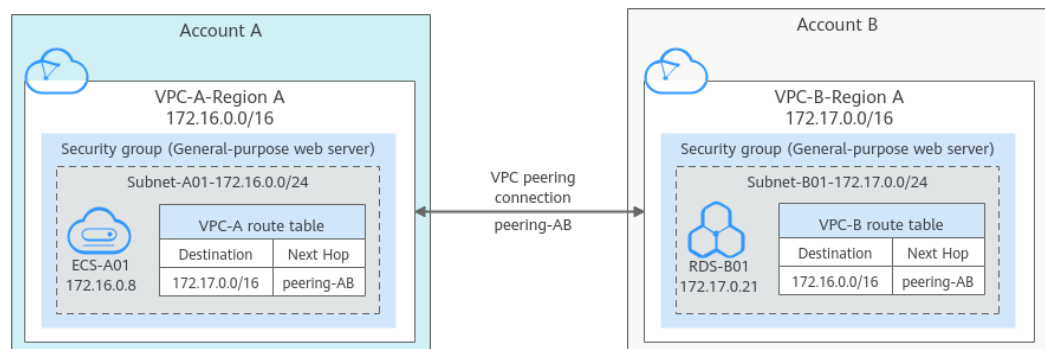
Step 1: Create a VPC Peering Connection

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 7-11 Networking diagram of a VPC peering connection between VPCs in different accounts



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 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. Log in to the management console.
2. Click  in the upper left corner and choose **Network > 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 right corner of the page, click **Create VPC Peering Connection**.
The **Create VPC Peering Connection** dialog box is displayed.
5. Configure the parameters as prompted.
For details, see [Table 7-16](#).

Table 7-16 Parameters for creating a VPC peering connection


Parameter	Description	Example Value
VPC Peering Connection 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 Another account.	Another account

Parameter	Description	Example Value
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.

6. 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](#).

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 **Network > Virtual Private Cloud**.

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

- In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
- In the upper part of the VPC peering connection list, locate the VPC peering connection request to be accepted.
- 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.
- 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.

- Add routes to the route table of the local VPC:
 - 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.
 - 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.
 - 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

Parameter	Description	Example Value
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.
3. In the project list, obtain the project ID.


7.6 Modifying a VPC Peering Connection

Scenarios

This section describes how to modify the name of a VPC peering connection.

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 choose **Network > 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 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.
5. 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 choose **Network > 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 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 choose **Network > 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 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.
5. 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 choose **Network > 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 VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
5. 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**.
6. 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
 - b. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
 - c. 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.
- d. 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 choose **Network > 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 VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
5. 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
 - b. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
 - c. 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.
 - d. 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 choose **Network > 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 VPC peering connection list, click the name of the target VPC peering connection.
The page showing the VPC peering connection details is displayed.
 5. 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**.
 6. 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
 - b. In the navigation pane on the left, choose **Virtual Private Cloud > VPC Peering Connections**.
The VPC peering connection list is displayed.
 - c. 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.
 - d. 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

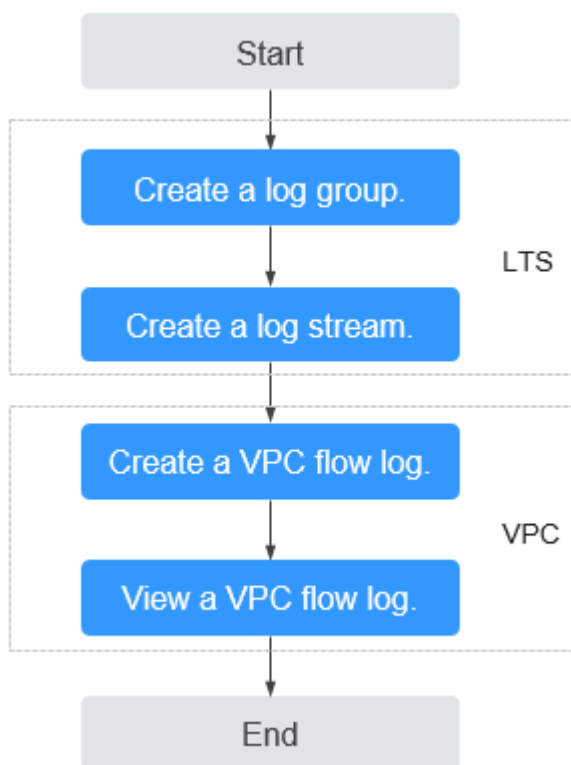
What Is a VPC Flow Log?

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



Notes and Constraints

- Currently, S6, C6, M6, and E3 ECSs support VPC flow logs.
- 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. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.

- The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **VPC Flow Logs**.
 4. 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.

5. 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **VPC Flow Logs**.
4. 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
action	The action associated with the traffic: <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

Field	Description	Example Value
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:</p> <p>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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **VPC Flow Logs**.
4. Locate the VPC flow log to be enabled or disabled, and click **Enable** or **Disable** in the **Operation** column.
5. 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 choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **VPC Flow Logs**.
4. Locate the row that contains the VPC flow log to be deleted and click **Delete** in the **Operation** column.
5. Click **Yes** in the displayed dialog box.

9 Elastic IP

9.1 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.

Assigning an EIP


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Elastic IP**.
3. On the displayed page, click **Assign EIP**.
4. Set the parameters as prompted.

Table 9-1 Parameter descriptions

Parameter	Description	Example Value
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.	N/A

Parameter	Description	Example Value
EIP Type	Dynamic BGP: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
Billed By	The following bandwidth types are available: <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 and is suitable for scenarios with staggered traffic. 	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
EIP Name	The name of the EIP.	eip-test
Bandwidth Name	The name of the bandwidth.	bandwidth
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
Quantity	The number of EIPs you want to purchase.	1
Enterprise Project	The enterprise project that the EIP belongs to. An enterprise project lets you manage cloud resources and personnel by enterprise project. The default project is default . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default

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 letters, digits, underscores (_), and hyphens (-).	Ipv4_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	3005eip

5. Click **Create Now**.
6. 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**.

9.2 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.


Procedure

Unbinding a single EIP


1. Log in to the management console.

2. Click  in the upper left corner and choose **Network > Elastic IP**.
3. On the displayed page, locate the row that contains the EIP, and click **Unbind**.
4. 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 choose **Network > Elastic IP**.
3. On the displayed page, locate the row that contains the target EIP, click **More** and then **Release** in the **Operation** column.
4. 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 choose **Network > Elastic IP**.
3. On the displayed page, select the EIPs to be unbound.
4. Click the **Unbind** button located above the EIP list.
5. 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 choose **Network > Elastic IP**.
3. On the displayed page, select the EIPs to be released.
4. Click the **Release** button located above the EIP list.
5. Click **Yes** in the displayed dialog box.

9.3 Modifying an EIP Bandwidth

Scenarios

Modify the EIP bandwidth name or size.

Procedure


1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Elastic IP**.
3. Locate the row that contains the target EIP in the EIP list, click **More** in the **Operation** column, and select **Modify Bandwidth**.
4. Modify the bandwidth parameters as prompted.
5. Click **Next**.
6. Click **Submit**.

9.4 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 choose **Network > Elastic IP**.
3. On the EIP list page, select one or more EIPs and click **Export** in the upper left corner.

The system will automatically export all EIPs to an Excel file and download the file to a local directory.

9.5 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 10 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 letters, digits, underscores (<code>_</code>), and hyphens (<code>-</code>).	Ipv4_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain letters, digits, underscores (<code>_</code>), periods (<code>.</code>), and hyphens (<code>-</code>).	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 choose **Network > Elastic IP**.
3. In the search box above the EIP list, click anywhere in the box to set filters.
Select the tag key and then the value as required. The system filters resources based on the tag you select.
Click anywhere in the search box 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 EIPs, the system will display only the EIPs that match all of the tags you specified.

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 choose **Network > Elastic IP**.
3. On the displayed page, locate the EIP whose tags you want to manage, and click the EIP name.
4. 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**.

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, BMSs, 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, increasing O&M workload. If all EIPs share the same bandwidth, VPCs and the region-level bandwidth can be managed in a unified manner, simplifying O&M statistics and network operations cost settlement.

- Lowered Bandwidth Costs
Region-level bandwidth sharing and multiplexing reduce bandwidth usage and O&M costs.
- Easy to Manage
Region-level bandwidth sharing and multiplexing simplify O&M statistics, management, and operations cost settlement.
- Flexible Operations
You can add 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.

10.2 Assigning a Shared Bandwidth

Scenarios

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 **Network > Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the upper right corner, click **Assign Shared Bandwidth**. On the displayed page, configure parameters as prompted.

Table 10-1 Parameter descriptions

Parameter	Description	Example Value
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
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. The maximum bandwidth can be 300 Mbit/s.	10
Name	The name of the shared bandwidth.	Bandwidth-001
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 . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default

5. Click **Create Now**.

10.3 Adding EIPs to a Shared Bandwidth


Scenarios

Add EIPs to a shared bandwidth and the EIPs can then share that bandwidth. You can add multiple EIPs to a shared bandwidth at the same time.

Notes and Constraints

- The type of EIPs must be the same as that of the shared bandwidth the EIPs to be added to.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > 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 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**.

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 **Network > 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 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. You can configure the EIP billing mode and bandwidth size.
6. Click **OK**.

10.5 Modifying a Shared Bandwidth

Scenarios

You can modify the name and size of a shared bandwidth as required.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > 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**.

10.6 Deleting a Shared Bandwidth


Scenarios

Delete a shared bandwidth when it is no longer required.

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 **Network > 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 delete, click **More** in the **Operation** column, and then click **Delete**.
5. In the displayed dialog box, click **Yes**.

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


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.

Procedure

1. Log in to the management console.
2. In the upper left corner of the page, click  to go to the service list. Under , click **Cloud Trace Service**.
3. In the navigation pane on the left, choose **Trace List**.
4. Specify filters as needed. The following filters are available:
 - **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.
5. Click arrow on the left of the required trace to expand its details.
6. 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. In the upper left corner of the page, click  to open the service list and choose **Management & Deployment > Cloud Eye**.
3. Click **Cloud Service Monitoring** on the left of the page, and choose **Elastic IP and Bandwidth**.
4. Locate the row that contains 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. In the upper left corner of the page, click  to open the service list and choose **Management & Deployment > Cloud Eye**.
3. In the left navigation pane on the left, choose **Alarm Management > Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters, or modify an existing alarm rule.
5. 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 FAQ

13.1 General Questions



13.1.1 What Is a Quota?

What Is a Quota?

A quota limits the quantity of a resource available to users, thereby preventing spikes in the usage of the resource. For example, a VPC quota limits the number of VPCs that can be created.

You can also request for an increased quota if your existing quota cannot meet your service requirements.

How Do I View My Quotas?

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 right corner of the page, click  .
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

1. Log in to the management console.
2. In the upper right corner of the page, choose **Resources > My Quotas**.
The **Service Quota** page is displayed.
3. Click **Increase Quota** in the upper right corner of the page.
4. On the **Create Service Ticket** page, configure parameters as required.

In the **Problem Description** area, fill in the content and reason for adjustment.

5. After all necessary parameters are configured, select **I have read and agree to the Ticket Service Protocol and Privacy Statement** and click **Submit**.

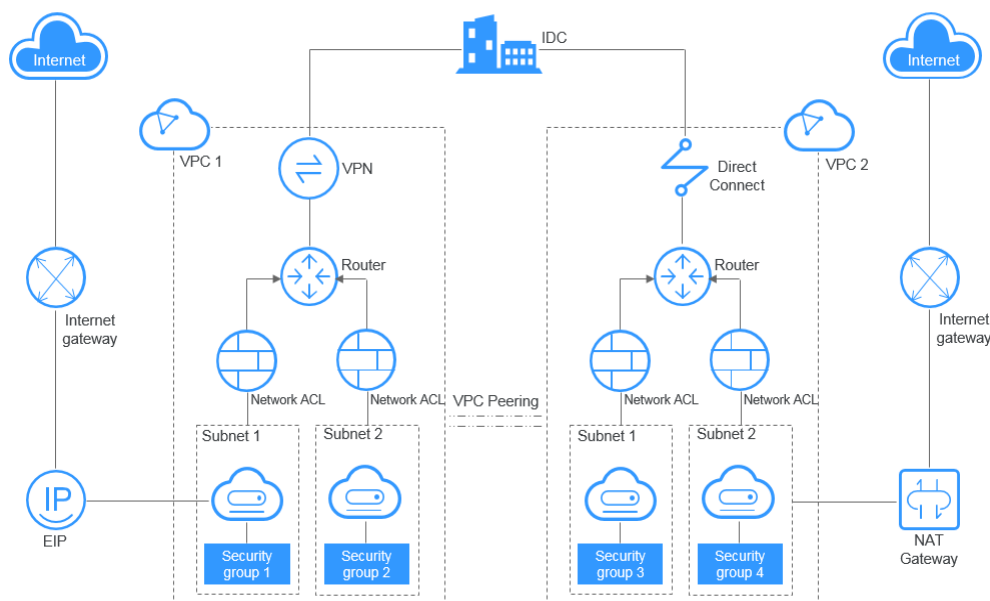
13.2 VPCs and Subnets

13.2.1 What Is Virtual Private Cloud?

Virtual Private Cloud (VPC) enables you to provision logically isolated virtual networks for Elastic Cloud Servers (ECSs), improving cloud resource security and simplifying network deployment. You can configure and manage the virtual networks as required.

Within your own VPC, you can create security groups and VPNs, configure IP address ranges, specify bandwidth sizes, manage the networks in the VPC, and make changes to these networks as needed, quickly and securely. You can also define rules to control communications between ECSs in the same security group or in different security groups.

Figure 13-1 Product Architecture



13.2.2 Which CIDR Blocks Are Available for the VPC Service?

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 13-1 lists the supported VPC CIDR blocks.

Table 13-1 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	$2^{16}-2=65534$

13.2.3 Can Subnets Communicate with Each Other?

- Different VPCs cannot communicate with each other, so subnets in different VPCs are isolated from each other.
- Subnets in the same VPC can communicate with each other by default. If network ACLs and security groups are used to protect network security, communications between subnets may be denied by these rules.
 - Network ACL: If you associate subnets with different network ACLs and do not add inbound and outbound allow rules, communications between these subnets would fail.
 - Security group: If you associate instances (such as ECSs) in a subnet with different security groups and do not add inbound and outbound allow rules, communications between these instances would fail.

If both network ACLs and security groups are configured, traffic preferentially matches the network ACL rules. For details, see [Table 13-2](#).

Figure 13-2 Communications between subnets in a VPC

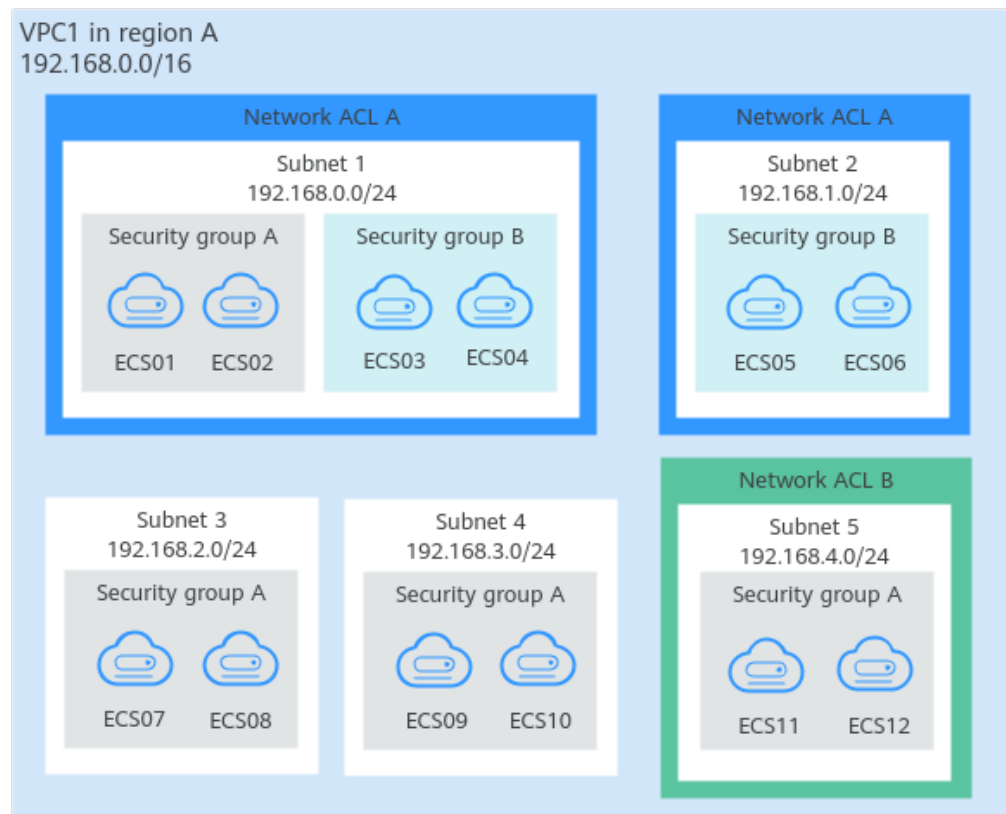


Table 13-2 Communication scenarios

Scenario	Access Control Configuration	Description
Between subnets	No network ACLs associated Instances associated with the same security group	<ul style="list-style-type: none"> Subnets 3 and 4 are not associated with a network ACL, so they can communicate with each other. ECS07, ECS08, ECS09, and ECS10 are associated with the same security group (security group A), so they can communicate with each other.
	Subnet associated with the same network ACL Instances associated with different security groups	<ul style="list-style-type: none"> Subnets 1 and 2 are associated with the same network ACL (network ACL A), so they can communicate with each other. ECS01 and ECS02 in subnet 1 are associated with security group A, and ECS05 and ECS06 in subnet 2 are associated with security group B. If security groups A and B have no allow rules, ECSs in the two security groups cannot communicate with each other. For example, ECS01 and ECS05 cannot communicate with each other.

Scenario	Access Control Configuration	Description
	Subnet associated with different network ACLs	Subnet 1 is associated with network ACL A, and subnet 5 is associated with network ACL B. If network ACLs A and B have no allow rules, subnet 1 and subnet 5 cannot communicate with each other. As a result, ECSs in subnets 1 and 5 are blocked from each other even they are in the same security group. For example, ECS01 and ECS 11 cannot communicate with each other.
Within a subnet	Instances associated with different security groups	ECS01 and ECS02 in subnet 1 are associated with security group A, and ECS03 and ECS04 are associated with security group B. If security groups A and B have no allow rules, ECSs in the two security groups cannot communicate with each other even they are in the same subnet (subnet 1). For example, ECS01 and ECS03 cannot communicate with each other.

13.2.4 What Subnet CIDR Blocks Are Available?

A subnet is an IP address range from a VPC. The VPC service supports CIDR blocks 10.0.0.0/8-24, 172.16.0.0/12-24, and 192.168.0.0/16-24.

Subnets must reside within your VPC, and the subnet masks used to define them can be between the netmask of its VPC CIDR block and /28 netmask.

13.2.5 How Many Subnets Can I Create?

Each account can have a maximum of 100 subnets. If the number of subnets cannot meet your service requirements, request a quota increase. For details, see [What Is a Quota?](#)

13.2.6 Why Can't I Delete My VPCs and Subnets?

If VPCs and subnets are being used by other resources, you need to delete these resources first based on the prompts on the console before deleting the VPCs and subnets. This following provides detailed deletion prompts and corresponding deletion guide.

- [Deleting Subnets](#)
- [Deleting VPCs](#)

Deleting Subnets

You can refer to [Table 13-3](#) to delete subnets.

Table 13-3 Deleting subnets

Prompts	Cause	Solution
You do not have permission to perform this operation.	Your account does not have permissions to delete subnets.	Contact the account administrator to grant permissions to your account and then delete the subnet.
Delete custom routes from the associated route table of the subnet and then delete the subnet.	The route table has custom routes with the following as the next hop type: <ul style="list-style-type: none"> • Server • Extension NIC • Virtual IP address • NAT gateway 	Delete the custom routes from the route table and then delete the subnet. <ol style="list-style-type: none"> 1. Viewing the Route Table Associated with a Subnet 2. Deleting a Route
Release any virtual IP addresses configured in the subnet and then delete the subnet.	The subnet has virtual IP addresses configured.	Release the virtual IP addresses from the subnet and then delete the subnet. Releasing a Virtual IP Address
Release any private IP addresses configured in the subnet and then delete the subnet.	The subnet has virtual IP addresses that are not used by any instance.	On the IP Addresses tab, release these private IP addresses that are not required and then delete the subnet. <ol style="list-style-type: none"> 1. Viewing IP Addresses in a Subnet 2. In the private IP address list, locate the IP address that is not being used and click Release in the Operation column. <p>NOTICE If you want to release an in-use private IP address, you need to delete the resource that uses the IP address first.</p>

Prompts	Cause	Solution
Delete the resource (ECS or load balancer) that is using the subnet and then delete the subnet.	The subnet is being used by an ECS or a load balancer.	Delete the ECS or load balancer and then delete the subnet. Viewing and Deleting Resources in a Subnet
Delete the load balancer that is using the subnet and then delete the subnet.	The subnet is being used by a load balancer.	Delete the load balancer and then delete the subnet. Viewing and Deleting Resources in a Subnet
Delete the NAT gateway that is using the subnet and then delete the subnet.	The subnet is being used by a NAT gateway.	Delete the NAT gateway and then delete the subnet. Viewing and Deleting Resources in a Subnet
Delete the resource that is using the subnet and then delete the subnet.	The subnet is being used by cloud resources.	On the IP Addresses tab, view the usage of the IP address, find the resource that is using the IP address, delete the resource, and delete the subnet. <ol style="list-style-type: none"> Viewing IP Addresses in a Subnet Locate resource based on the usage of the IP address. Delete the resource and then delete the subnet.

Deleting VPCs

Before deleting a VPC, ensure that all subnets in the VPC have been deleted. You can refer to [Table 13-4](#) to delete VPCs.

Table 13-4 Deleting VPCs

Prompts	Cause	Solution
You do not have permission to perform this operation.	Your account does not have permissions to delete VPCs.	Contact the account administrator to grant permissions to your account and then delete the VPC.
Delete the VPC endpoint service or the route configured for the service from the VPC route table and then delete the VPC.	The VPC route table has custom routes.	Delete the custom routes and then delete the VPC. 1. In the VPC list, locate the row that contains the VPC and click the number in the Route Tables column. The route table list is displayed. 2. Deleting a Route
	The VPC is being used by a VPC endpoint service.	Search for the VPC endpoint service on the VPC endpoint service console and delete it.
This VPC cannot be deleted because it has associated resources.	The VPC is being used by the following resources: <ul style="list-style-type: none"> Subnet VPC peering connection Custom route table 	Click the resource name hyperlink as prompted to delete the resource. <ul style="list-style-type: none"> Table 13-3 Deleting a VPC Peering Connection Deleting a Route Table
Delete the virtual gateway that is using the VPC and then delete the VPC.	The VPC is being used by a Direct Connect virtual gateway.	On the Direct Connect console, locate the virtual gateway and delete it.
Delete the VPN gateway that is using the VPC and then delete the VPC.	The VPC is being used by a VPN gateway.	On the VPN console, locate the VPN gateway and delete it.

Prompts	Cause	Solution
Delete all custom security groups in this region and then delete this last VPC.	In the current region, this is the last VPC and there are custom security groups. NOTICE You only need to delete the custom security groups. The default security group does not affect the deletion of VPCs.	Delete all custom security groups and then delete the VPC. Deleting a Security Group
Release all EIPs in this region and then delete this last VPC.	In the current region, this is the last VPC and there are EIPs.	Release all EIPs in this region and then delete this last VPC. Unbinding an EIP from an ECS and Releasing the EIP

13.3 EIPs

13.3.1 Can I Bind an EIP to Multiple ECSs?

Each EIP can be bound to only one ECS at a time.

Multiple ECSs cannot share the same EIP. An ECS and its bound EIP must be in the same region. If you want multiple ECSs in the same VPC to share an EIP, you have to use a NAT gateway. For more information, see *NAT Gateway User Guide*.

13.3.2 How Do I Access an ECS with an EIP Bound from the Internet?

Each ECS is automatically added to a security group after being created to ensure its security. The security group denies access traffic from the Internet by default (except TCP traffic from port 22 through SSH to a Linux ECS and TCP traffic from port 3389 through RDP to a Windows ECS). To allow external access to ECSs in the security group, add an inbound rule to the security group.

You can set **Protocol** to **TCP**, **UDP**, **ICMP**, or **All** as required on the page for creating a security group rule.

- If your ECS needs to be accessible over the Internet and you know the IP address used to access the ECS, set **Source** to the IP address range containing the IP address.
- If your ECS needs to be accessible over the Internet but you do not know the IP address used to access the ECS, retain the default setting 0.0.0.0/0 for **Source**, and then set allowed ports to improve network security.

The default source **0.0.0.0/0** indicates that all IP addresses can access ECSs in the security group.

- Allocate ECSs that have different Internet access requirements to different security groups.

13.3.3 Can I Bind an EIP of an ECS to Another ECS?

Yes.

You can unbind the EIP from the original ECS. For details, see section "Unbinding an EIP from an Instance" in the *Elastic IP User Guide*.

Then, bind the EIP to the target ECS. For details, see section "Assigning an EIP and Binding It to an ECS" in *Elastic IP User Guide*.

13.3.4 Can I Bind an EIP to a Cloud Resource in Another Region?

No. EIPs and their associated cloud resources must be in the same region.

13.3.5 Can I Change the Region of My EIP?

The region of an EIP cannot be changed.

If you assigned an EIP in region A but need an EIP in region B, you cannot directly change the region of the assigned EIP from A to B. Instead, you have to assign an EIP in region B.

13.4 VPC Peering Connections

13.4.1 How Many VPC Peering Connections Can I Create in an Account?

If you use a VPC peering connection to connect VPCs in the same region, you can log in to the management console to view your VPC peering connection quota. For details, see [What Is a Quota?](#)

- Number of VPC peering connections that you can create in each region between VPCs in the same account: subject to the actual quota
- Number of VPC peering connections that you can create in each region between VPCs in different accounts: Accepted VPC peering connections use the quotas of both accounts. To-be-accepted VPC peering connections only use the quotas of accounts that request the connections.

An account can create VPC peering connections with different accounts if the account has enough quota.

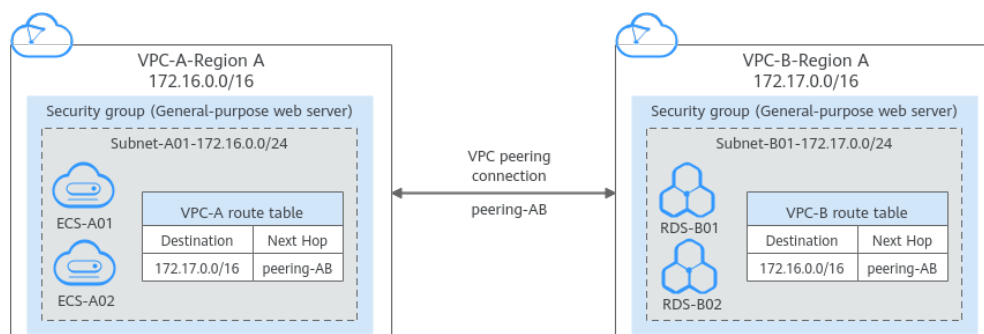
13.4.2 Can a VPC Peering Connection Connect VPCs in Different Regions?

A VPC peering connection only can connect VPCs in the same region.

Figure 13-3 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 13-3 VPC peering connection network diagram



13.4.3 Why Did Communication Fail Between VPCs That Were Connected by a VPC Peering Connection?

Symptom

After a VPC peering connection is created, the local and peer VPCs cannot communicate with each other.

Troubleshooting

The issues here are described in order of how likely they are to occur.

Table 13-5 Possible causes and solutions

No.	Possible Cause	Solution
1	<p>Overlapping CIDR blocks of local and peer VPCs</p> <ul style="list-style-type: none"> • All their subnet CIDR blocks overlap. • Some of their subnet CIDR blocks overlap. 	<p>Refer to Overlapping CIDR Blocks of Local and Peer VPCs.</p>

No.	Possible Cause	Solution
2	<p>Incorrect route configuration for the local and peer VPCs</p> <ul style="list-style-type: none">• No routes are added.• Incorrect routes are added.• Destinations of the routes overlap with that configured for Direct Connect or VPN connections.	Refer to Incorrect Route Configuration for Local and Peer VPCs .
3	<p>Incorrect network configuration</p> <ul style="list-style-type: none">• The security group rules of the ECSs that need to communicate deny inbound traffic from each other.• The firewall of the ECS NIC blocks traffic.• The network ACL rules of the subnets connected by the VPC peering connection deny inbound traffic.• Check the policy-based routing configuration of an ECS with multiple NICs.	Refer to Incorrect Network Configuration .
4	ECS network failure	Refer to ECS Network Failure .

Overlapping CIDR Blocks of Local and Peer VPCs

If the CIDR blocks of VPCs connected by a VPC peering connection overlap, the connection may not take effect due to route conflicts.

Table 13-6 Overlapping CIDR blocks of local and peer VPCs

Scenario	Description	Solution
<p>VPCs with overlapping CIDR blocks also include subnets that overlap.</p>	<p>As shown in Figure 13-4, the CIDR blocks of VPC-A and VPC-B overlap, and all their subnets overlap.</p> <ul style="list-style-type: none"> • Overlapping CIDR blocks of VPC-A and VPC-B: 10.0.0.0/16 • Overlapping CIDR blocks of Subnet-A01 in VPC-A and Subnet-B01 in VPC-B: 10.0.0.0/24 • Overlapping CIDR blocks of Subnet-A02 in VPC-A and Subnet-B02 in VPC-B: 10.0.1.0/24 	<p>VPC-A and VPC-B cannot be connected using a VPC peering connection. Replan the network.</p>
<p>Two VPCs have overlapping CIDR blocks but some of their subnets do not overlap.</p>	<p>As shown in Figure 13-5, the CIDR blocks of VPC-A and VPC-B overlap, and some of their subnets overlap.</p> <ul style="list-style-type: none"> • Overlapping CIDR blocks of VPC-A and VPC-B: 10.0.0.0/16 • Overlapping CIDR blocks of Subnet-A01 in VPC-A and Subnet-B01 in VPC-B: 10.0.0.0/24 • CIDR blocks of Subnet-A02 in VPC-A and Subnet-B02 in VPC-B do not overlap. 	<ul style="list-style-type: none"> • A VPC peering connection cannot connect the entire VPCs, VPC-A and VPC-B. • A connection can connect their subnets (Subnet-A02 and Subnet-B02) that do not overlap. For details, see Figure 13-6.

Figure 13-4 Networking diagram (IPv4)

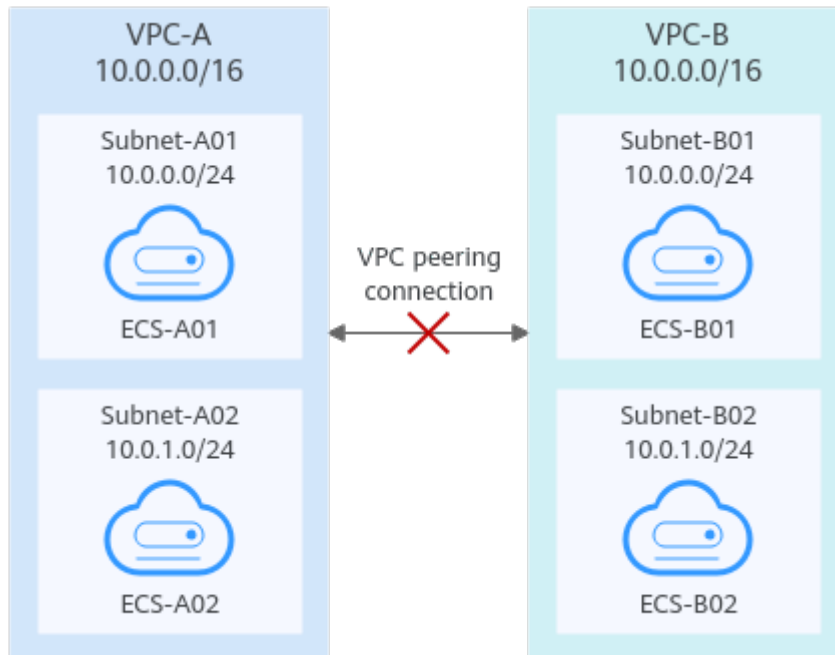
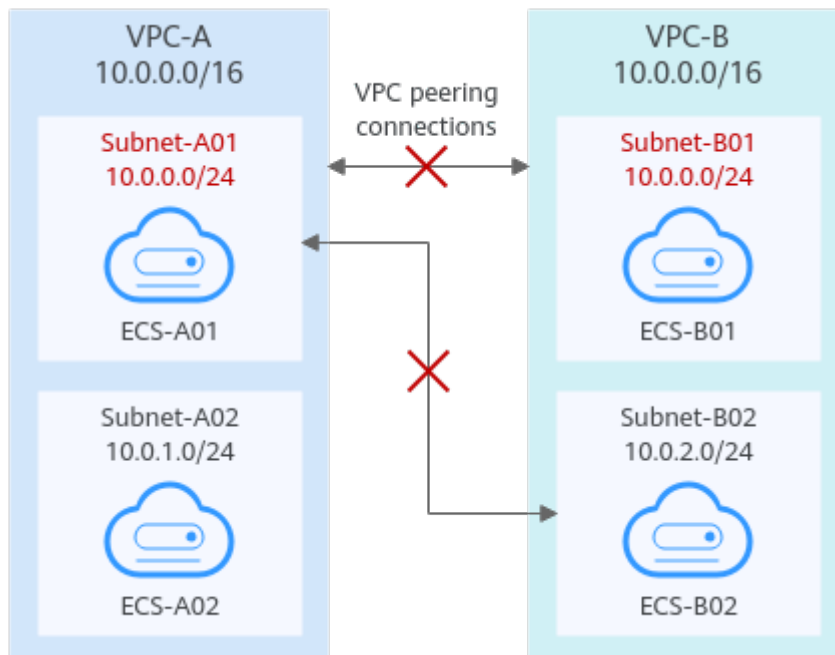


Figure 13-5 Networking diagram (IPv4)



If CIDR blocks of VPCs overlap and some of their subnets overlap, you can create a VPC peering connection between their subnets with non-overlapping CIDR blocks. [Figure 13-6](#) shows the networking diagram of connecting Subnet-A02 and Subnet-B02. [Table 13-7](#) describes the routes required.

Figure 13-6 Networking diagram (IPv4)

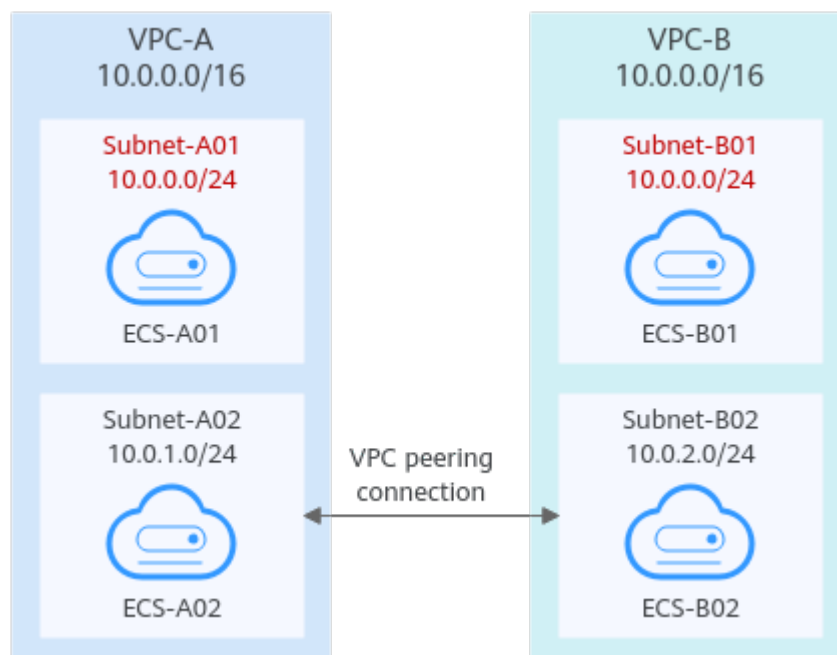


Table 13-7 Routes required for the VPC peering connection between Subnet-A02 and Subnet-B02

Route Table	Destination	Next Hop	Description
VPC-A route table	10.0.2.0/24	Peering-AB	Add a route with the CIDR block of Subnet-B02 as the destination and Peering-AB as the next hop.
VPC-B route table	10.0.1.0/24	Peering-AB	Add a route with the CIDR block of Subnet-A02 as the destination and Peering-AB as the next hop.

Incorrect Route Configuration for Local and Peer VPCs

Check the routes in the route tables of the local and peer VPCs by referring to [Viewing Routes Configured for a VPC Peering Connection](#). [Table 13-8](#) lists the items that you need to check.

Table 13-8 Route check items

Item	Solution
Check whether routes are added to the route tables of the local and peer VPCs.	If routes are not added, add routes by referring to: <ul style="list-style-type: none"> • Creating a VPC Peering Connection with Another VPC in Your Account

Item	Solution
<p>Check the destinations of routes added to the route tables of the local and peer VPCs.</p> <ul style="list-style-type: none"> • In the route table of the local VPC, check whether the route destination is the CIDR block, subnet CIDR block, or related private IP address of the peer VPC. • In the route table of the peer VPC, check whether the route destination is the CIDR block, subnet CIDR block, or related private IP address of the local VPC. 	<p>If the route destination is incorrect, change it by referring to Modifying Routes Configured for a VPC Peering Connection.</p>
<p>Destinations of the routes overlap with that configured for Direct Connect or VPN connections.</p>	<p>Check whether any of the VPCs connected by the VPC peering connection also has a VPN or Direct Connect connection connected. If they do, check the destinations of their routes.</p> <p>If the destinations of the routes overlap, the VPC peering connection does not take effect. In this case, replan the network connection.</p>

Incorrect Network Configuration

1. Check whether the security group rules of the ECSs that need to communicate with each other allow inbound traffic from each other.
 - If the ECSs are associated with the same security group, you do not need to check their rules.
 - If the ECSs are associated with different security groups, add an inbound rule to allow access from each other by referring to [Security Group Configuration Examples](#).
2. Check whether the firewall of the ECS NIC blocks traffic.
If the firewall blocks traffic, configure the firewall to allow inbound traffic.
3. Check whether network ACL rules of the subnets connected by the VPC peering connection deny inbound traffic.
If the network ACL rules deny inbound traffic, configure the rules to allow the traffic.
4. If an ECS has more than one NIC, check whether correct policy-based routing has been configured for the ECS and packets with different source IP addresses match their own routes from each NIC.
If an ECS has two NICs (eth0 and eth1):
 - IP address of eth0: 192.168.1.10; Subnet gateway: 192.168.1.1

- IP address of eth1: 192.168.2.10; Subnet gateway: 192.168.2.1

Command format:

- **ping -I** *IP address of eth0* *Subnet gateway address of eth0*
- **ping -I** *IP address of eth1* *Subnet gateway address of eth1*

Run the following commands:

- **ping -I 192.168.1.10 192.168.1.1**
- **ping -I 192.168.2.10 192.168.2.1**

If the network communication is normal, the routes of the NICs are correctly configured.

ECS Network Failure

1. Log in to the ECS.
2. Check whether the ECS NIC has an IP address assigned.
 - Linux ECS: Use the **ifconfig** or **ip address** command to view the IP address of the NIC.
 - Windows ECS: In the search box, enter **cmd** and press **Enter**. In the displayed command prompt, run the **ipconfig** command.If the ECS NIC has no IP address assigned, see
3. Check whether the subnet gateway of the ECS can be pinged.
 - a. In the ECS list, click the ECS name.
The ECS details page is displayed.
 - b. On the ECS details page, click the hyperlink of VPC.
The **Virtual Private Cloud** page is displayed.
 - c. In the VPC list, locate the target VPC and click the number in the **Subnets** column.
The **Subnets** page is displayed.
 - d. In the subnet list, click the subnet name.
The subnet details page is displayed.
 - e. Click the **IP Addresses** tab and view the gateway address of the subnet.
 - f. Check whether the gateway communication is normal:
ping *Subnet gateway address*
Example command: **ping 172.17.0.1**

13.5 Bandwidth

13.5.1 What Is the Bandwidth Size Range?

The bandwidth range is from 1 Mbit/s to 300 Mbit/s.

13.5.2 What Bandwidth Types Are Available?

There are dedicated bandwidths and shared bandwidths. A dedicated bandwidth can only be used by one EIP, but a shared bandwidth can be used by multiple EIPs.

13.5.3 What Is the Relationship Between Bandwidth and Upload/Download Rate?

The bandwidth is measured in bit/s, but the download rate is measured in byte/s.

1 byte = 8 bits, that is, download rate = bandwidth/8

Due to various issues such as computer performance, network device quality, resource usage, and network peak hours, if the bandwidth is 1 Mbit/s, the actual upload or download rate is generally lower than 125 kByte/s (1 Mbit/s = 1,000 Kbit/s, upload or download rate = 1,000/8 = 125 kByte/s).

13.6 Connectivity

13.6.1 Does a VPN Allow Communication Between Two VPCs?

If the two VPCs are in the same region, you can use a VPC peering connection to enable communication between them.

If the two VPCs are in different regions, you can use a VPN to enable communication between the VPCs. The CIDR blocks of the two VPCs are the local and remote subnets, respectively.

13.6.2 Why Are Internet or Internal Domain Names in the Cloud Inaccessible Through Domain Names When My ECS Has Multiple NICs?

When an ECS has more than one NIC, if different DNS server addresses are configured for the subnets used by the NICs, the ECS cannot access the Internet or domain names in the cloud.

You can resolve this issue by configuring the same DNS server address for the subnets used by the same ECS. You can perform the following steps to modify DNS server addresses of subnets in a VPC:

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
4. In the subnet list, locate the target subnet and click its name.
5. On the subnet details page, change the DNS server address of the subnet.
6. Click **OK**.

13.6.3 What Are the Priorities of the Custom Route and EIP If Both Are Configured for an ECS to Enable the ECS to Access the Internet?

The priority of an EIP is higher than that of a custom route in a VPC route table. For example:

The VPC route table of an ECS has a custom route with 0.0.0.0/0 as the destination and NAT gateway as the next hop.

If an ECS in the VPC has an EIP bound, the VPC route table will have a policy-based route with 0.0.0.0/0 as the destination, which has a higher priority than its custom route. In this case, traffic is forwarded to the EIP and cannot reach the NAT gateway.

13.7 Routing

13.7.1 Can a Route Table Span Multiple VPCs?

A route table cannot span multiple VPCs.

A route table contains a set of routes that are used to determine where network traffic from your subnets in a VPC is directed. A VPC has a default route table and can have multiple custom route tables.

Each subnet in a VPC must be associated with a route table. A subnet can only be associated with one route table at a time, but you can associate multiple subnets in a VPC with the same route table.

13.7.2 How Many Routes Can a Route Table Contain?

Each route table can contain a maximum of 200 routes by default, including routes added for Direct Connect and VPC peering connections.

13.7.3 Are There Any Restrictions on Using a Route Table?

- An ECS providing SNAT must have **Unbind IP from MAC** enabled.
- The destination of each route in a route table must be unique. The next hop must be a private IP address or a virtual IP address in the VPC. Otherwise, the route table will not take effect.
- If a virtual IP address is set to be the next hop in a route, EIPs bound with the virtual IP address in the VPC will become invalid.

13.7.4 Do the Same Routing Priorities Apply to Direct Connect Connections and Custom Routes in the Same VPC?

No. Direct Connect connections and custom routes are used in different scenarios, so the routing priorities are different.

13.7.5 Are There Different Routing Priorities of the VPN and Custom Routes in the Same VPC?

No. The routing priority of custom routes and that of VPNs are the same.

13.8 Security

13.8.1 Does a Modified Security Group Rule or a Network ACL Rule Take Effect Immediately for Existing Connections?

- 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.
- 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 apply 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.

13.8.2 Why Can't I Delete a Security Group?

- The default security group is named **default** and cannot be deleted.
- 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.
- A security group cannot be deleted if it is used as the source or destination of a rule in another security group.

You need to delete or modify the rule first and delete the security group.

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**.

13.8.3 Can I Change the Security Group of an ECS?

Yes. Log in to the ECS console, switch to the page showing ECS details, and change the security group of the ECS.

13.8.4 How Do I Configure a Security Group for Multi-Channel Protocols?

ECS Configuration

The TFTP daemon determines whether a configuration file specifies the port range. If you use a TFTP configuration file that allows the data channel ports to be configurable, it is a good practice to configure a small range of ports that are not listened on.

Security Group Configuration

You can configure port 69 and configure data channel ports used by TFTP for the security group. In RFC1350, the TFTP protocol specifies that ports available to data channels range from 0 to 65535. However, not all these ports are used by the TFTP daemon processes of different applications. You can configure a smaller range of ports for the TFTP daemon.

A Change History

Release Date	Description
2022-10-31	<p>This release incorporates the following changes:</p> <ul style="list-style-type: none">• Added Can I Bind an EIP of an ECS to Another ECS?• Added Can I Bind an EIP to a Cloud Resource in Another Region?• Added What Bandwidth Types Are Available?• Added What Is the Relationship Between Bandwidth and Upload/Download Rate?• Added Can a Route Table Span Multiple VPCs?
2022-06-07	<p>This release incorporates the following changes: Added IPv6 information to the following sections:</p> <ul style="list-style-type: none">• Creating a VPC• Creating a Subnet for the VPC• IPv4 and IPv6 Dual-Stack Network• Adding a Security Group Rule• Fast-Adding Security Group Rules• Importing and Exporting Security Group Rules• Adding a Network ACL Rule• Modifying a Network ACL Rule
2022-04-12	<p>This issue is the first official release.</p>