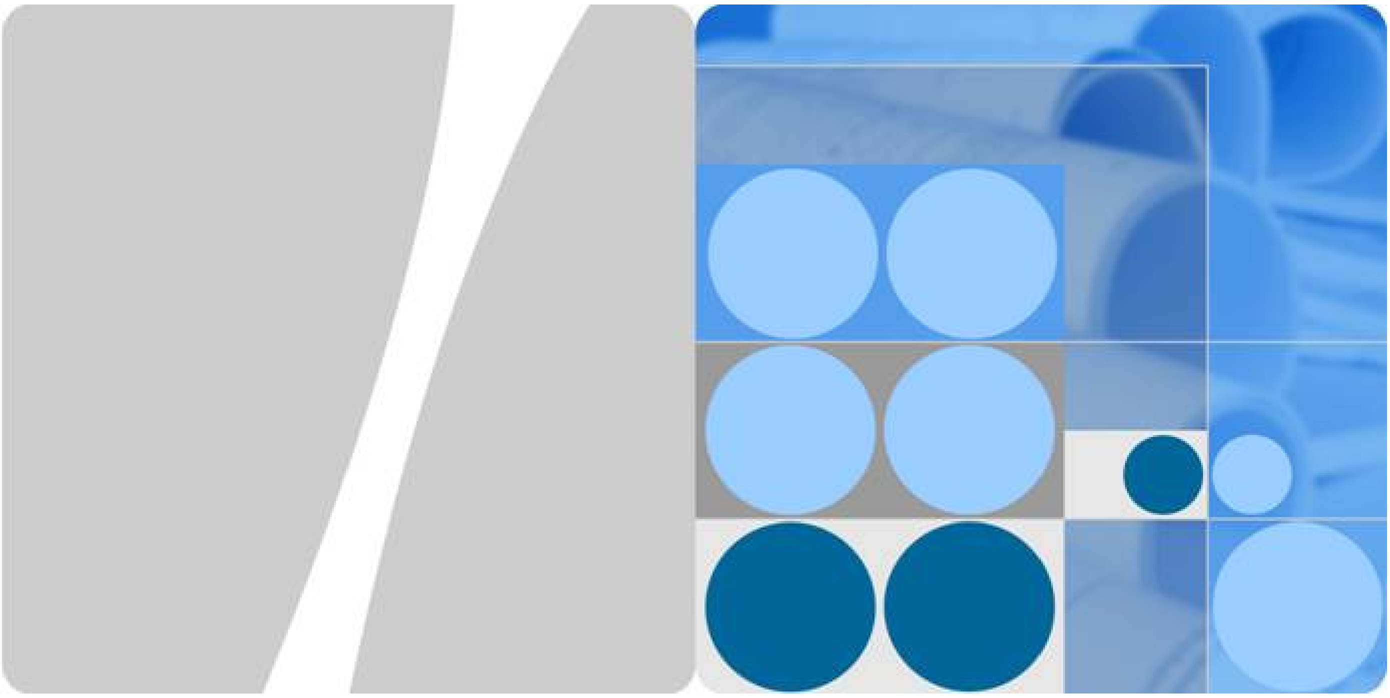


Virtual Private Cloud

User Guide

Date **2021-06-18**

Contents

1 Service Overview

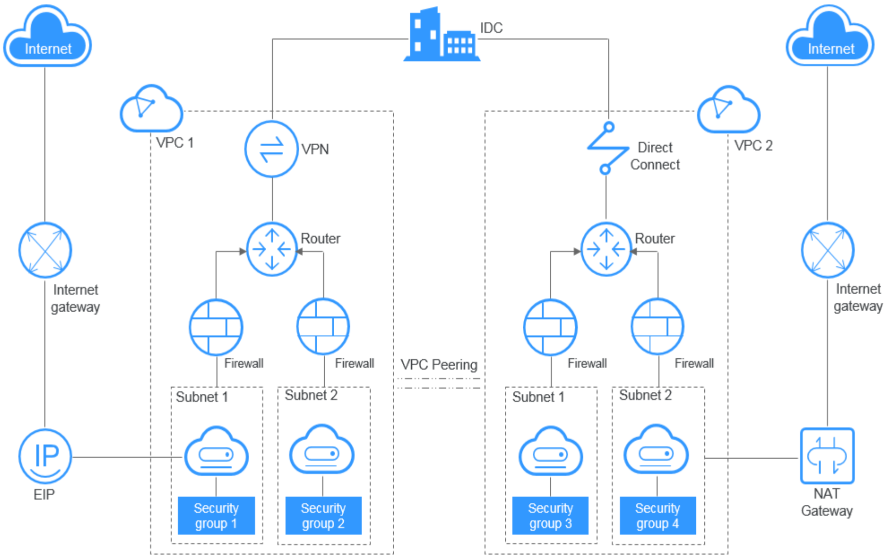
1.1 What Is Virtual Private Cloud?

Overview

The Virtual Private Cloud (VPC) service enables you to provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs), improving cloud resource security and simplifying network deployment.

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 for communication between ECSs in the same security group or in different security groups.

Figure 1-1 VPC components



Advantages

- Flexible configuration

  You can create VPCs, add subnets, specify IP address ranges, and configure route tables. You can configure the same VPC for ECSs that are in different availability zones (AZs).

- Secure and reliable

  Each VPC is logically isolated from other VPCs using the tunneling technology. By default, different VPCs cannot communicate with each other. Firewalls are provided to protect subnets, and security groups are provided to protect ECSs. The firewalls and security groups add additional layers of security to your VPC, making your network secure.

- Interconnectivity

  By default, instances in a VPC cannot access the Internet. You can leverage elastic IP addresses (EIPs), Elastic Load Balancing (ELB), NAT gateways, Virtual Private Network (VPN), and Direct Connect to enable access to or from the Internet.

  By default, instances in two VPCs cannot communicate with each other. You can create a VPC peering connection to enable the instances in the two VPCs in the same region to communicate with each other using private IP addresses.

  Multiple connectivity options are provided to meet diverse service requirements for the cloud, enabling you to deploy enterprise applications with ease and lower enterprise IT operation and maintenance (O&M) costs.

- High-speed access

  Dynamic Border Gateway Protocol (BGP) is used to provide access to various carrier networks. For example, up to 21 dynamic BGP connections are established to multiple carriers. The dynamic BGP connections enable real-time failover based on preset routing protocols, ensuring high network stability, low network latency, and smooth access to services on the cloud.

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 the VPC service provided by the cloud system 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 system 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 User Permissions

The cloud system provides two types of user permissions by default: user management and resource management. User management refers to the management of users, user groups, and user group rights. Resource management refers to the control operations that can be performed by users on cloud service resources.

For further details, see **Permissions**.

1.6 Basic Concepts

1.6.1 Subnet

A subnet is a unique CIDR block with a range of IP addresses in your VPC. All resources in a VPC must be deployed on subnets. Once a subnet has been created, its CIDR block cannot be modified.

By default, ECSs in all subnets of the same VPC can communicate with one another, but ECSs in different VPCs cannot.

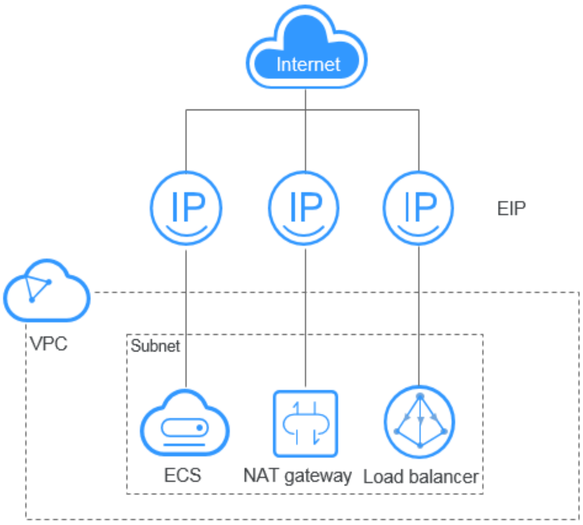
To enable ECSs in different VPCs but in the same region to communicate with one another, you can create a VPC peering connection. For details, see **VPC Peering Connection**.

1.6.2 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 1-2 Accessing the Internet using an EIP



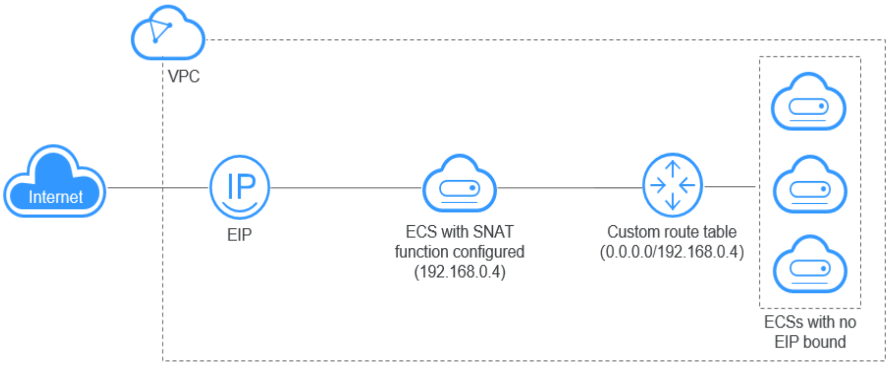
1.6.3 Route Table

A route table contains a set of rules that determine where network traffic is directed. You can add routes to a route table to enable other ECSs in a VPC to access the Internet through the ECS that has a bound EIP.

You can use a route table configured in standalone mode or active/standby mode.

- **Figure 1-3** shows the route table configured in standalone mode.

Figure 1-3 Route table configured in standalone mode

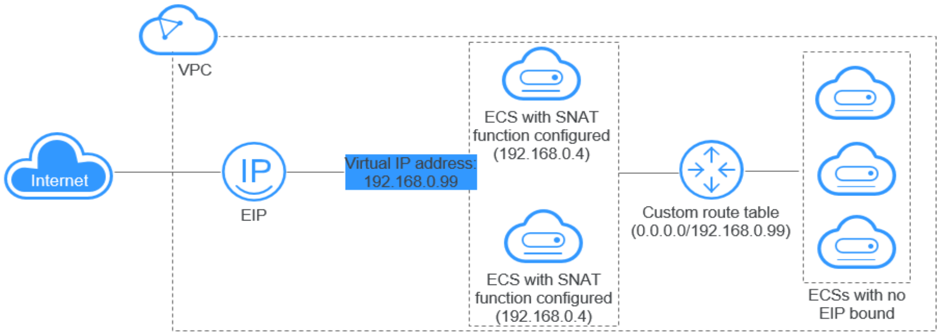

VPC
Internet
EIP
ECS with SNAT function configured (192.168.0.4)
Custom route table (0.0.0.0/192.168.0.4)
ECSs with no EIP bound

In standalone mode, ECSs in a VPC that do not have EIPs bound access the Internet through an ECS that has an EIP bound and has the SNAT function configured.

You can create a route table for the VPC used by ECSs that do not have EIPs bound to enable these ECSs to access the Internet. The next hop in the route table is the private IP address of the ECS that has an EIP bound (the private IP address of the SNAT server).

- **Figure 1-4** shows the route table configured in active/standby mode.

Figure 1-4 Route table configured in active/standby mode


VPC
Internet
EIP
Virtual IP address: 192.168.0.99
ECS with SNAT function configured (192.168.0.4)
ECS with SNAT function configured (192.168.0.4)
Custom route table (0.0.0.0/192.168.0.99)
ECSs with no EIP bound

In active/standby mode, ECSs in a VPC that do not have EIPs bound access the Internet through two ECSs that have EIPs bound and have the SNAT function configured.

In active/standby mode, you can add a route table for the VPC used by ECSs that do not have EIPs bound, to enable these ECSs to access the Internet. The next hop in the route table is the virtual IP address of the two ECSs that have EIPs bound.

In both the standalone and active/standby modes, the ECSs that have EIPs bound must have the SNAT function. For details about the SNAT function, see **SNAT**. For details about how to configure an ECS as the SNAT server, see **Configuring an SNAT Server**.

NOTICE

- Before using the route table function, you need to deploy the SNAT server. For details, see section **Configuring an SNAT Server**.
- The ECS providing SNAT function can have only one NIC.
- The ECS providing SNAT function must have the source/destination check function disabled.

1.6.4 SNAT

In addition to services provided by the system, some ECSs need to access the Internet to obtain information or download software. You can bind EIPs to virtual NICs (ports) of ECSs to enable the ECSs to access the Internet. However, assigning a public IP address to each ECS consumes already-limited IPv4 addresses, incurs additional costs, and may increase the attack surface for a virtual environment. Therefore, SNAT is introduced to enable multiple ECSs to share one public IP address.

On a public cloud, a public IP address can be assigned to an ECS that serves as the SNAT router or gateway for other ECSs from the same subnet or VPC.

For details about how to configure SNAT, see **Configuring an SNAT Server**.

1.6.5 Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted within a VPC. After you create a security group, you can create different access rules for the security group, and the rules will apply to any ECS that the security group contains.

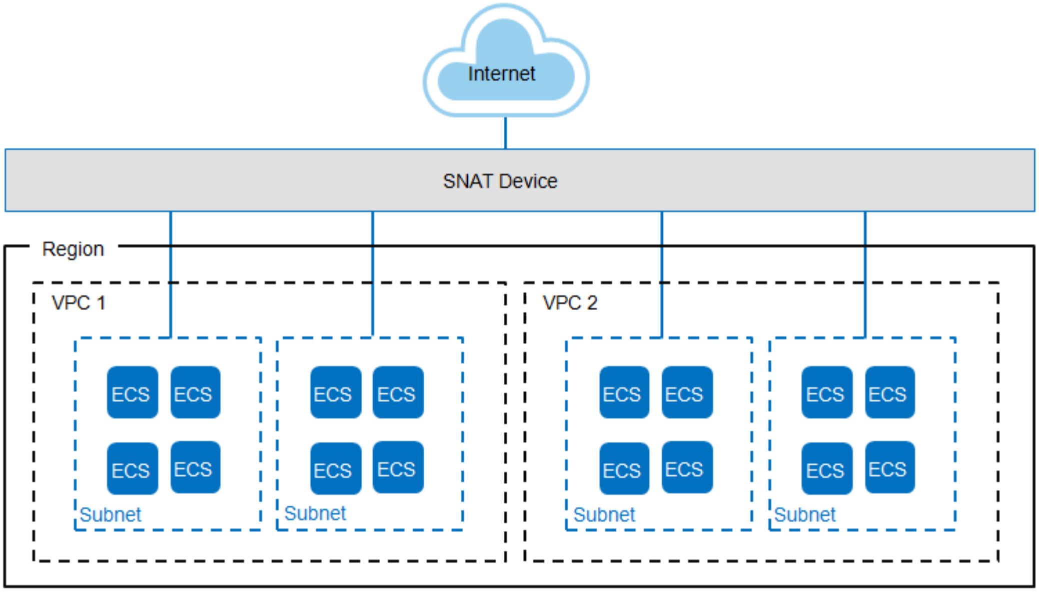
Your account automatically comes with a default security group. The default security group allows all outbound traffic, denies all inbound traffic, and allows all traffic between ECSs in the group. Your ECSs in this security group can communicate with each other already without adding additional rules.

1.6.6 Shared SNAT

The VPC service provides free SNAT function, which allows ECSs to use a limited number of public IP addresses to gain one-way access to the Internet for operations, such as updating software. However, Internet users cannot directly access the ECSs.

Figure 1-5 shows how shared SNAT works. The SNAT device forwards traffic from ECSs to the Internet and the response traffic from the Internet to the ECSs. When forwarding ECS traffic to the Internet, the SNAT device converts the source IP addresses (ECS private IP addresses) in the data packets into the public IP addresses set on the SNAT device. When processing the response packets from the Internet to the ECSs, the SNAT device changes the public IP addresses in the response data packets to the private IP addresses of the ECSs.

Figure 1-5 SNAT function



- To enable shared SNAT using the API, set **enable_snat** to **true** by following the instructions provided in **Neutron** > **Routers** > **Update router** in the *Native OpenStack API Reference*.
- To enable shared SNAT on the management console:
  a. Log in to the management console.
  b. On the console homepage, under **Network**, click **Virtual Private Cloud**.
  c. On the **Virtual Private Cloud** page, locate the VPC for which shared SNAT is to be enabled, and click **Modify**.
  d. In the displayed dialog box, enable **Shared SNAT**.
  e. Click **OK**.

After being configured for a VPC, shared SNAT takes effect for the whole VPC. If EIPs are bound to ECSs in a VPC for which shared SNAT is configured, Internet traffic is preferentially forwarded using the EIPs. If you want to prevent an ECS from connecting to the Internet, you can configure an outbound rule for the security group associated with the ECS.

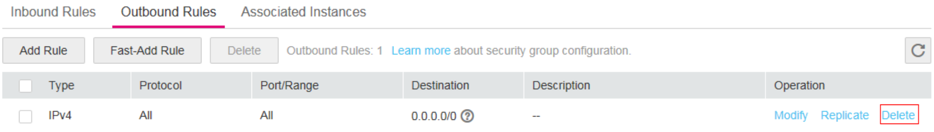
For example:

To prevent an ECS from connecting to the Internet but allow the ECS to access 192.168.10.0/24, configure the following rule for the security group associated with the ECS:

1. Delete the default outbound rule that allows all outgoing data packets from the security group.

   After this rule is deleted, ECSs associated with this security group are not allowed to access any network, including the internal networks in the VPC of the ECSs.

Figure 1-6 Deleting the default outbound rule from the security group


Inbound Rules Outbound Rules Associated Instances

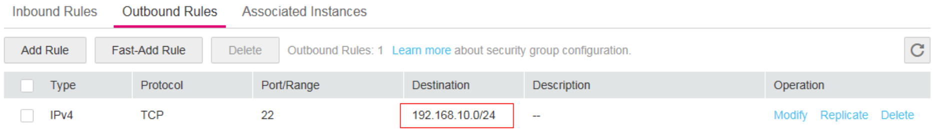
Add Rule Fast-Add Rule Delete Outbound Rules: 1 Learn more about security group configuration.

□ Type	Protocol	Port/Range	Destination	Description	Operation
□ IPv4	All	All	0.0.0.0/0 ⓘ	--	Modify Replicate Delete

2. Add the required outbound rule.

   The following shows the added outbound rule that allows the ECS to access the 192.168.10.0/24 CIDR block.

Figure 1-7 Adding an outbound rule for the security group


Inbound Rules Outbound Rules Associated Instances

Add Rule Fast-Add Rule Delete Outbound Rules: 1 Learn more about security group configuration.

□ Type	Protocol	Port/Range	Destination	Description	Operation
□ IPv4	TCP	22	192.168.10.0/24	--	Modify Replicate Delete

The differences between shared SNAT and custom routes are as follows:

- Shared SNAT provides the SNAT function for a specified VPC through an API or the management console and enables all ECSs in the VPC to gain one-way access to the Internet.
- A custom route enables ECSs to access the Internet through an SNAT server that has an EIP bound. The ECSs' access requests are routed to the SNAT server based on the route table.
- Shared SNAT takes effect for the whole VPC by default, while a custom route takes effect for the VPC or subnet for which routes have been configured.
- A custom route has a higher priority than a shared SNAT.

1.6.7 VPC Peering Connection

A VPC peering connection is a network connection between two VPCs in one region that enables you to route traffic between them using private IP addresses. ECSs in either VPC can communicate with each other just as if they were in the same region. You can create a VPC peering connection between your own VPCs, or between your VPC and another account's VPC within the same region. However, you cannot create a VPC peering connection between VPCs in different regions.

For details, see **VPC Peering Connection**.

1.6.8 Firewall

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

1.6.9 Virtual IP Address

A virtual IP address can be shared among multiple ECSs. An ECS can have both private and virtual IP addresses, and you can access the ECS through either IP address. A virtual IP address has the same network access capabilities as a private IP address, including layer 2 and layer 3 communication in VPCs, access between VPCs using VPC peering connections, as well as access through EIPs, VPN connections, and Direct Connect connections.

A virtual IP address can be bound to multiple ECSs deployed in active/standby mode. You can bind an EIP to the virtual IP address. When the EIP is accessed from the Internet, the virtual IP address has made it possible to either the active or standby ECS, making ECSs highly fault tolerant.

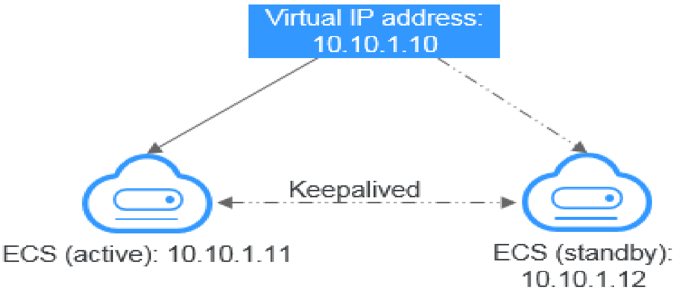
Networking

Virtual IP addresses are used for high availability as they 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

  If you want to improve service availability and avoid single points of failure, you can deploy ECSs in the active/standby mode or deploy one active ECS and multiple standby ECSs. In this arrangement, the ECSs all use the same virtual IP address. If the active ECS becomes faulty, a standby ECS takes over services from the active ECS and services continue uninterrupted.

  Figure 1-8 Networking diagram of the HA mode

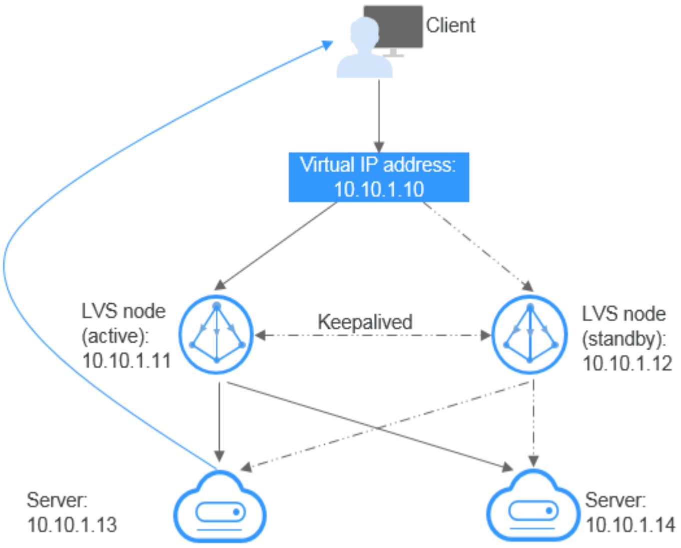
  

  - In this configuration, a single virtual IP address is bound to two ECSs in the same subnet.
  - Keepalived is then used to configure the two ECSs to work in the active/standby mode. Follow industry standards for configuring Keepalived. The details are not included here.

- **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 1-9 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 mode. 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 a VPN for security and Direct Connect for a stable connection. The VPC peering connection is needed so that the VPCs in the same region can communicate with each other.

1.6.10 Region and AZ

Concept

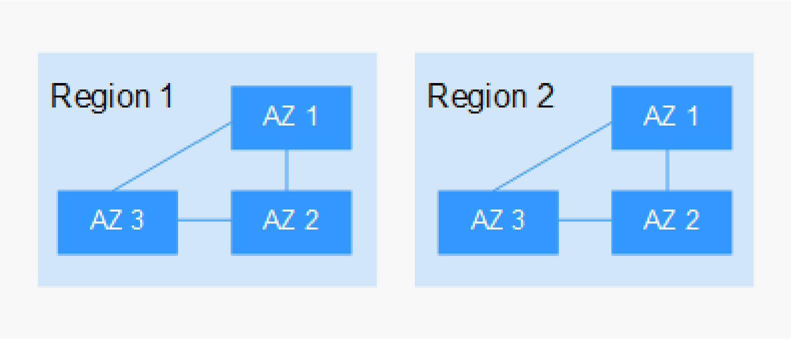
A region and availability zone (AZ) identify the location of a data center. You can create resources in a specific region and AZ.

- 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 1-10 shows the relationship between regions and AZs.

Figure 1-10 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**.

1.7 Document Usage Instructions

Instructions for using this document are as follows:

- To facilitate your operations, the management console may provide more than one way for you to perform a task or an operation. This document describes only the main way.
- You can click ✏ next to some parameter values to quickly edit the values. This document does not describe this function.

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 or need to access the Internet using a specific IP address with limited bandwidth on the default network segment, 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**.

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 or need to access the Internet using a specified IP address with limited bandwidth on default CIDR block 100.64.0.0/11 (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

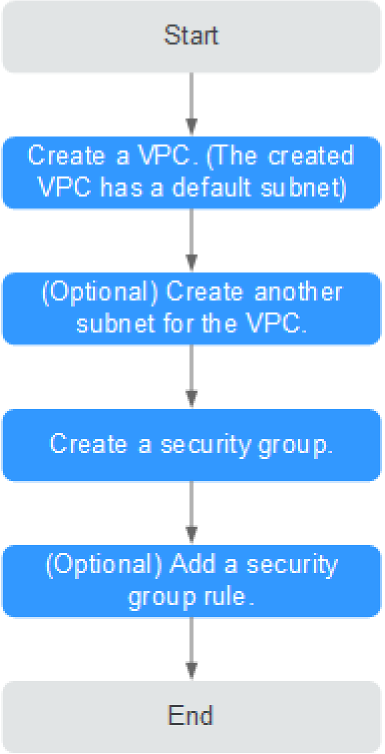

Start
Create a VPC. (The created VPC has a default subnet)
(Optional) Create another subnet for the VPC.
Create a security group.
(Optional) Add a security group rule.
End

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 a default rule, which allows all outgoing data packets. ECSs in a security group can access each other without the need to add 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.

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 select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. Click **Create VPC**.
5. 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

Category	Parameter	Description	Example Value
Basic Information	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.	eu-de

Category	Parameter	Description	Example Value
Basic Information	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-001
Basic Information	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: 10.0.0.0/8-24 172.16.0.0/12-24 192.168.0.0/16-24	192.168.0.0/16
Basic Information	Tag	The VPC tag, which consists of a key and value pair. You can add a maximum of 20 tags to each VPC. The tag key and value must meet the requirements listed in **Table 2-3**.	● Key: vpc_key1 ● Value: vpc-01
Default 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
Default Subnet	CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
Default Subnet	Advanced Settings	Two options are available, **Default** and **Custom**. You can set **Advanced Settings** to **Custom** to configure advanced subnet parameters.	Default
Default Subnet	Gateway	The gateway address of the subnet.	192.168.0.1

Category	Parameter	Description	Example Value
Default Subnet	DNS Server Address	By default, two DNS server addresses are configured. You can change them as required. A maximum of five DNS server addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
Default Subnet	NTP Server Address	The IP address of the NTP server. This parameter is optional. 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 this parameter is left empty, no IP address of the NTP server is added. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	192.168.2.1
Default Subnet	Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 20 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-4**.	● Key: subnet_key1 ● Value: subnet-01

Table 2-3 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for the same VPC and can be the same for different VPCs. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc-01

Table 2-4 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each subnet. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet_key1

Parameter	Requirements	Example Value
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet-01

6. Click **Create Now**.

2.2.3 Step 2: Create a Subnet for the VPC

Scenarios

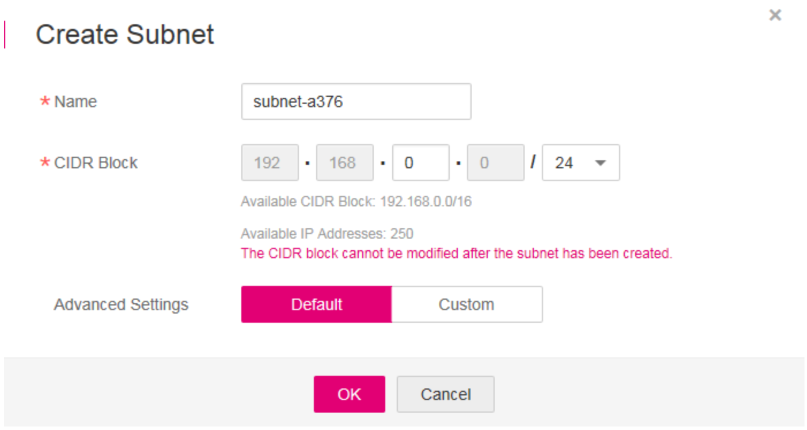
A VPC comes with a default subnet. If the default subnet cannot meet your requirements, you can create one.

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC for which a subnet is to be created and click the VPC name.
6. On the displayed **Subnets** tab, click **Create Subnet**.
7. Set the parameters as prompted.

Figure 2-2 Create Subnet



Create Subnet

* Name: subnet-a376

* CIDR Block: 192 . 168 . 0 . 0 / 24

Available CIDR Block: 192.168.0.0/16

Available IP Addresses: 250

The CIDR block cannot be modified after the subnet has been created.

Advanced Settings: Default | Custom

Table 2-5 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
CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
Advanced Settings	Two options are available, **Default** and **Custom**. You can set **Advanced Settings** to **Custom** to configure advanced subnet parameters.	Default
Gateway	The gateway address of the subnet.	192.168.0.1
DNS Server Address	By default, two DNS server addresses are configured. You can change them if necessary. A maximum of five DNS server addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
NTP Server Address	The IP address of the NTP server. This parameter is optional. 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 this parameter is left empty, no IP address of the NTP server is added. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 20 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-6**.	● Key: subnet_key1 ● Value: subnet-01

Table 2-6 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each subnet. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet-01

8. 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

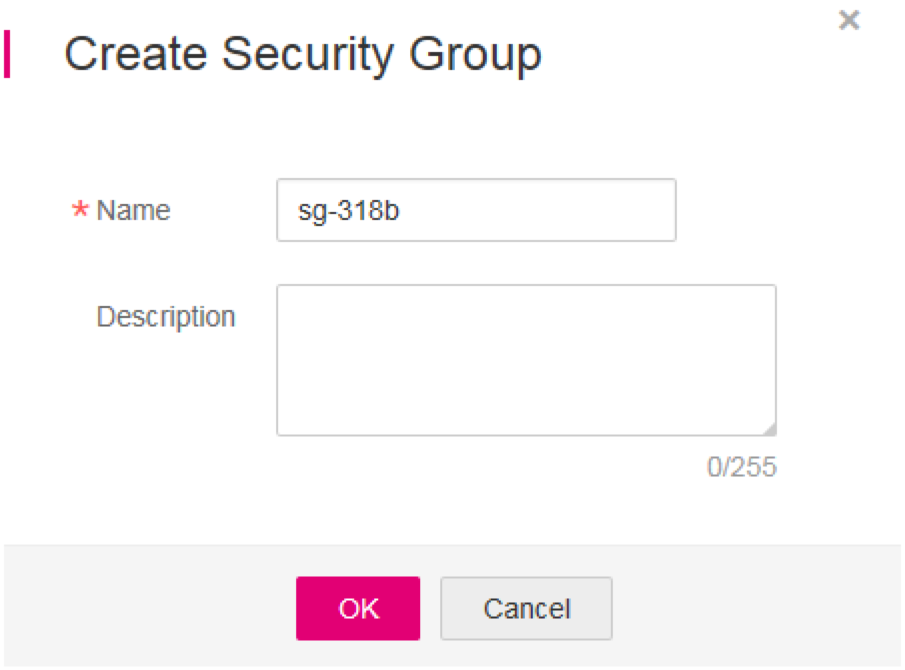
Scenarios

To improve ECS access security, you can create security groups, define security group rules, and add ECSs in a VPC to different security groups. We recommend that you allocate ECSs that have different Internet access policies to different security groups.

Procedure

1. Log in to the management console.
2. Click ⊙ in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click **Create Security Group**.
6. In the **Create Security Group** area, set the parameters as prompted. **Table 2-7** lists the parameters to be configured.

Figure 2-3 Create Security Group



Create Security Group

* Name: sg-318b

Description:

0/255

Table 2-7 Parameter description

Parameter	Description	Example Value
Name	The security group name. This parameter is mandatory. 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. **NOTE** 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.	sg-318b
Description	Supplementary information about the security group. This parameter is optional. The security group description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.

2.2.5 Step 4: Add a Security Group Rule

Scenarios

After you create a security group, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After you add ECSs to the security group, they are protected by the rules of the group.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

For details about the default security group rules, see **Default Security Groups and Security Group Rules**. For details about security group rule configuration examples, see **Security Group Configuration Examples**.

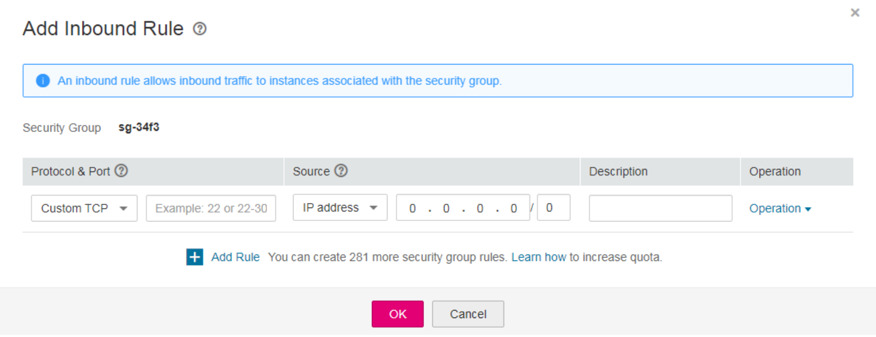
Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.

6. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   You can click **+** to add more inbound rules.

Figure 2-4 Add Inbound Rule



Add Inbound Rule

An inbound rule allows inbound traffic to instances associated with the security group.

Security Group sg-34f3

Protocol & Port		Source			Description	Operation
Custom TCP	Example: 22 or 22-30	IP address	0 . 0 . 0 . 0	0		Operation

Add Rule You can create 281 more security group rules. Learn how to increase quota.

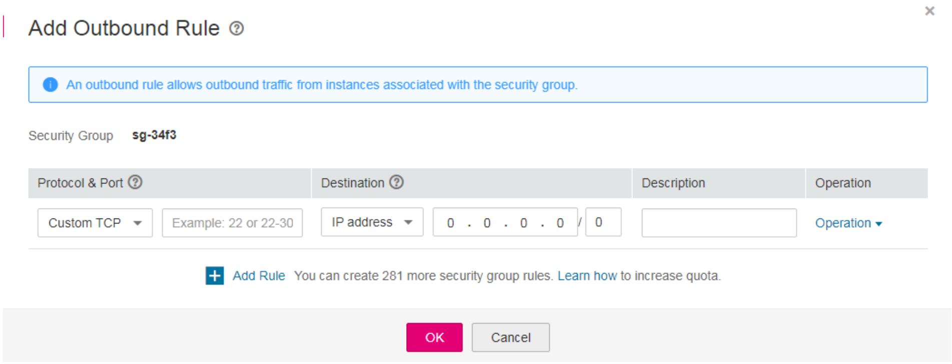
Table 2-8 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: The network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: The port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30
Source	The source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses) ● sg-abc (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. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

   You can click **+** to add more outbound rules.

Figure 2-5 Add Outbound Rule



Add Outbound Rule

An outbound rule allows outbound traffic from instances associated with the security group.

Security Group sg-34f3

Protocol & Port		Destination			Description	Operation
Custom TCP	Example: 22 or 22-30	IP address	0 . 0 . 0 . 0	0		Operation

You can create 281 more security group rules. Learn how to increase quota.

Table 2-9 Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: The network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: The port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Destination	The destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses) ● sg-abc (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

8. Click **OK**.

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

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 2-6** to bind EIPs to the ECSs.

Figure 2-6 Configuring the network

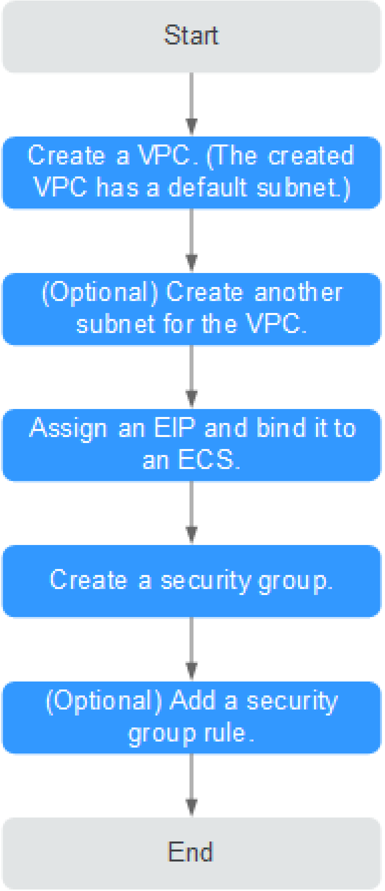

Start
Create a VPC. (The created VPC has a default subnet.)
(Optional) Create another subnet for the VPC.
Assign an EIP and bind it to an ECS.
Create a security group.
(Optional) Add a security group rule.
End

Table 2-10 describes the different tasks in the procedure for configuring the network.

Table 2-10 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.

Task	Description
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.
Assign an EIP and bind it to an ECS.	This task is mandatory. You can assign an EIP and bind it to an ECS so that the ECS can access the Internet.
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 a default rule, which allows 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.

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 select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. Click **Create VPC**.
5. 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 2-11 VPC parameter descriptions

Category	Parameter	Description	Example Value
Basic Information	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.	eu-de
Basic Information	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-001
Basic Information	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: 10.0.0.0/8-24 172.16.0.0/12-24 192.168.0.0/16-24	192.168.0.0/16
Basic Information	Tag	The VPC tag, which consists of a key and value pair. You can add a maximum of 20 tags to each VPC. The tag key and value must meet the requirements listed in **Table 2-12**.	- Key: vpc_key1 - Value: vpc-01
Default 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

Category	Parameter	Description	Example Value
Default Subnet	CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
Default Subnet	Advanced Settings	Two options are available, **Default** and **Custom**. You can set **Advanced Settings** to **Custom** to configure advanced subnet parameters.	Default
Default Subnet	Gateway	The gateway address of the subnet.	192.168.0.1
Default Subnet	DNS Server Address	By default, two DNS server addresses are configured. You can change them as required. A maximum of five DNS server addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
Default Subnet	NTP Server Address	The IP address of the NTP server. This parameter is optional. 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 this parameter is left empty, no IP address of the NTP server is added. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	192.168.2.1
Default Subnet	Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 20 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-13**.	● Key: subnet_key1 ● Value: subnet-01

Table 2-12 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	- Cannot be left blank. - Must be unique for the same VPC and can be the same for different VPCs. - Can contain a maximum of 36 characters. - Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc_key1
Value	- Can contain a maximum of 43 characters. - Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc-01

Table 2-13 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	- Cannot be left blank. - Must be unique for each subnet. - Can contain a maximum of 36 characters. - Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet_key1

Parameter	Requirements	Example Value
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet-01

6. Click **Create Now**.

2.3.3 Step 2: Create a Subnet for the VPC

Scenarios

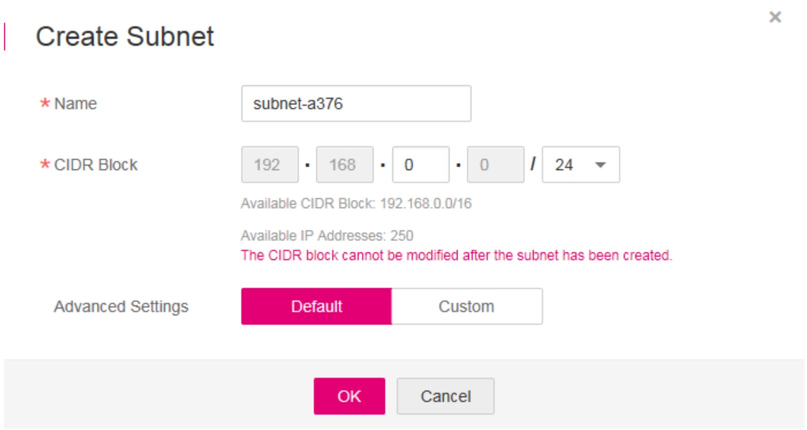
A VPC comes with a default subnet. If the default subnet cannot meet your requirements, you can create one.

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

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC for which a subnet is to be created and click the VPC name.
6. On the displayed **Subnets** tab, click **Create Subnet**.
7. Set the parameters as prompted.

Figure 2-7 Create Subnet



Create Subnet

* Name: subnet-a376

* CIDR Block: 192 . 168 . 0 . 0 / 24

Available CIDR Block: 192.168.0.0/16

Available IP Addresses: 250

The CIDR block cannot be modified after the subnet has been created.

Advanced Settings: Default

Table 2-14 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
CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
Advanced Settings	Two options are available, **Default** and **Custom**. You can set **Advanced Settings** to **Custom** to configure advanced subnet parameters.	Default
Gateway	The gateway address of the subnet.	192.168.0.1
DNS Server Address	By default, two DNS server addresses are configured. You can change them if necessary. A maximum of five DNS server addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
NTP Server Address	The IP address of the NTP server. This parameter is optional. 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 this parameter is left empty, no IP address of the NTP server is added. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 20 tags to each subnet. The tag key and value must meet the requirements listed in **Table 2-15**.	● Key: subnet_key1 ● Value: subnet-01

Table 2-15 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each subnet. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet-01

8. 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

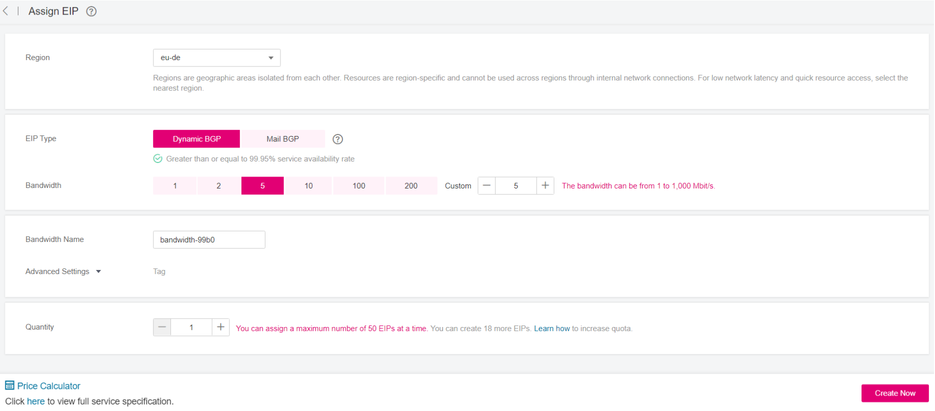
Scenarios

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

Assigning an EIP

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. On the displayed page, click **Assign EIP**.
5. Set the parameters as prompted.

Figure 2-8 Assign EIP



Assign EIP

Region: eu-de

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

EIP Type: Dynamic BGP

Greater than or equal to 99.95% service availability rate

Bandwidth: 5

Custom: 5

The bandwidth can be from 1 to 1,000 Mbit/s.

Bandwidth Name: bandwidth-99b0

Quantity: 1

You can assign a maximum number of 50 EIPs at a time. You can create 18 more EIPs. Learn how to increase quota.

Click here to view full service specification.

Table 2-16 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.	eu-de

Parameter	Description	Example Value
Type	● **Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails. ● **Mail BGP**: EIPs with port 25, 465, or 587 enabled are used. The selected EIP type cannot be changed after the EIP is assigned.	Dynamic BGP
Bandwidth	The bandwidth size in Mbit/s.	100
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 2-17**.	● Key: Ipv4_key1 ● Value: 192.168.12.10
Quantity	The number of EIPs you want to purchase.	1

Table 2-17 EIP tag requirements

Parameter	Requirement	Example Value
Key	● Cannot be left blank. ● Must be unique for each EIP. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	Ipv4_key1

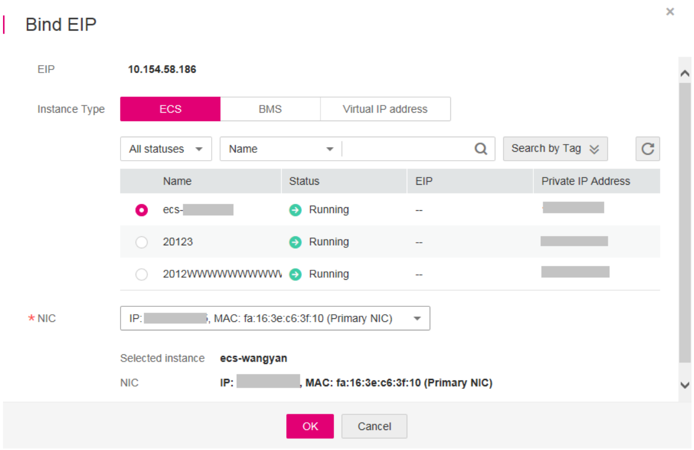
Parameter	Requirement	Example Value
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	192.168.12.10

6. Click **Assign Now**.
7. Click **Submit**.

Binding an EIP

1. On the **EIPs** page, locate the row that contains the target EIP, and click **Bind**.
2. Select the instance to which you want to bind the EIP.

Figure 2-9 Bind EIP



Bind EIP

EIP 10.154.58.186

Instance Type: ECS | BMS | Virtual IP address

All statuses ▾ | Name ▾ | Search by Tag

	Name	Status	EIP	Private IP Address
●	ecs-[redacted]	Running	--	[redacted]
○	20123	Running	--	[redacted]
○	2012WWWWWWWWWW\	Running	--	[redacted]

* NIC: IP: [redacted], MAC: fa:16:3e:c6:3f:10 (Primary NIC) ▾

Selected instance: **ecs-wangyan**

NIC: **IP: [redacted], MAC: fa:16:3e:c6:3f:10 (Primary NIC)**

OK | Cancel

3. Click **OK**.

An IPv6 client on the Internet can access the ECS that has an EIP bound in a VPC. For details about the implementation and constraints, see **How Does an IPv6 Client on the Internet Access the ECS That Has an EIP Bound in a VPC?**

2.3.5 Step 4: Create a Security Group

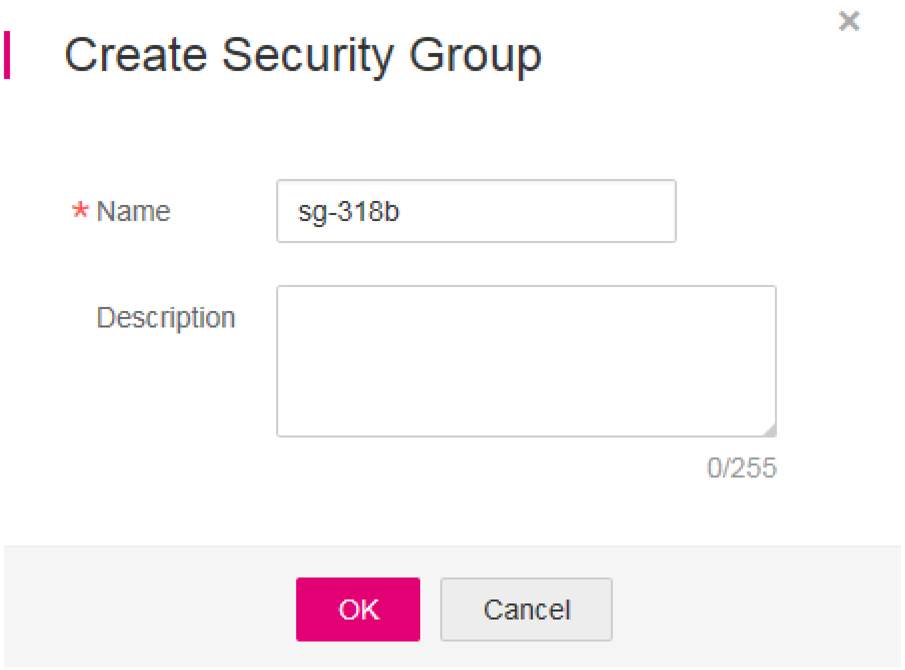
Scenarios

To improve ECS access security, you can create security groups, define security group rules, and add ECSs in a VPC to different security groups. We recommend that you allocate ECSs that have different Internet access policies to different security groups.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click **Create Security Group**.
6. In the **Create Security Group** area, set the parameters as prompted. **Table 2-18** lists the parameters to be configured.

Figure 2-10 Create Security Group



Create Security Group

* Name: sg-318b

Description:

0/255

Table 2-18 Parameter description

Parameter	Description	Example Value
Name	The security group name. This parameter is mandatory. 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. **NOTE** 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.	sg-318b

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

7. Click **OK**.

2.3.6 Step 5: Add a Security Group Rule

Scenarios

After you create a security group, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After you add ECSs to the security group, they are protected by the rules of the group.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

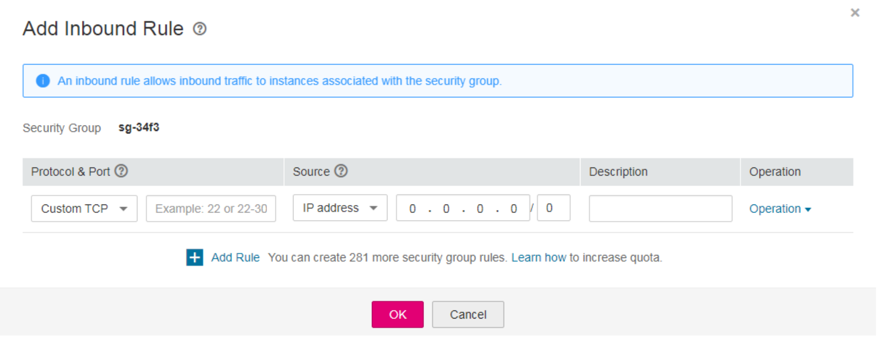
For details about the default security group rules, see **Default Security Groups and Security Group Rules**. For details about security group rule configuration examples, see **Security Group Configuration Examples**.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
6. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   You can click **+** to add more inbound rules.

Figure 2-11 Add Inbound Rule



Add Inbound Rule

An inbound rule allows inbound traffic to instances associated with the security group.

Security Group sg-34f3

Protocol & Port		Source		Description	Operation
Custom TCP	Example: 22 or 22-30	IP address	0 . 0 . 0 . 0 / 0		Operation

Add Rule You can create 281 more security group rules. Learn how to increase quota.

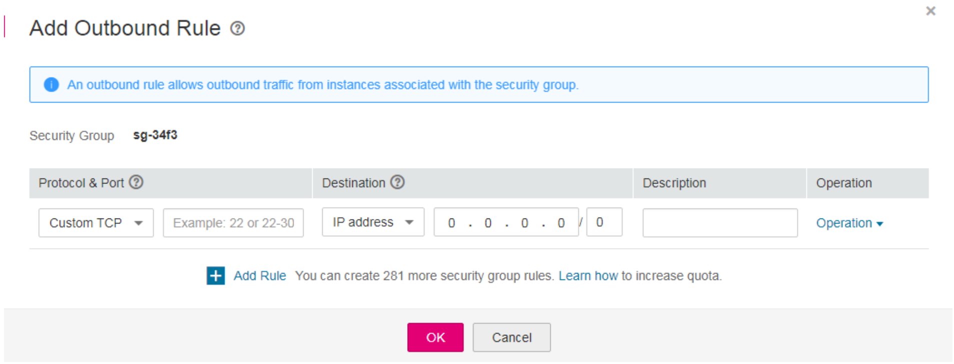
Table 2-19 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: The network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: The port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30
Source	The source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses) ● sg-abc (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. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

   You can click **+** to add more outbound rules.

Figure 2-12 Add Outbound Rule



Add Outbound Rule

An outbound rule allows outbound traffic from instances associated with the security group.

Security Group sg-34f3

Protocol & Port		Destination		Description	Operation
Custom TCP	Example: 22 or 22-30	IP address	0 . 0 . 0 . 0 / 0		Operation

Add Rule You can create 281 more security group rules. Learn how to increase quota.

Table 2-20 Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: The network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: The port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Destination	The destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses) ● sg-abc (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

8. Click **OK**.

3 VPC and Subnet

3.1 VPC

3.1.1 Creating a VPC

Scenarios

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

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 select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. Click **Create VPC**.
5. 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 3-1 VPC parameter descriptions

Category	Parameter	Description	Example Value
Basic Information	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.	eu-de
Basic Information	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-001
Basic Information	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: 10.0.0.0/8-24 172.16.0.0/12-24 192.168.0.0/16-24	192.168.0.0/16
Basic Information	Tag	The VPC tag, which consists of a key and value pair. You can add a maximum of 20 tags to each VPC. The tag key and value must meet the requirements listed in **Table 3-2**.	● Key: vpc_key1 ● Value: vpc-01
Default 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

Category	Parameter	Description	Example Value
Default Subnet	CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
Default Subnet	Advanced Settings	Two options are available, **Default** and **Custom**. You can set **Advanced Settings** to **Custom** to configure advanced subnet parameters.	Default
Default Subnet	Gateway	The gateway address of the subnet.	192.168.0.1
Default Subnet	DNS Server Address	By default, two DNS server addresses are configured. You can change them as required. A maximum of five DNS server addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
Default Subnet	NTP Server Address	The IP address of the NTP server. This parameter is optional. 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 this parameter is left empty, no IP address of the NTP server is added. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	192.168.2.1
Default Subnet	Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 20 tags to each subnet. The tag key and value must meet the requirements listed in **Table 3-3**.	● Key: subnet_key1 ● Value: subnet-01

Table 3-2 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for the same VPC and can be the same for different VPCs. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc-01

Table 3-3 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each subnet. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet_key1

Parameter	Requirements	Example Value
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet-01

6. Click **Create Now**.

3.1.2 Modifying a VPC

Scenarios

Change the VPC name and CIDR block.

If the VPC CIDR block conflicts with the CIDR block of a VPN created in the VPC, you can modify its CIDR block.

Notes and Constraints

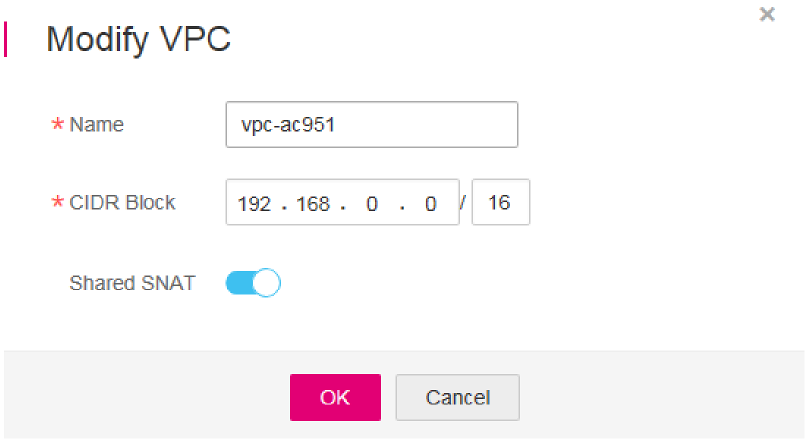
When modifying the VPC CIDR block:

- The VPC CIDR block to be modified must be in the supported CIDR blocks: 10.0.0.0 – 10.255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 – 192.168.255.255
- If the VPC has subnets, the VPC CIDR block to be modified must contain all subnet CIDR blocks.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the row that contains the VPC to be modified and click **Modify** in the **Operation** column.
6. In the displayed dialog box, modify parameters as prompted. You can change the VPC name, shared SNAT setting, and VPC CIDR block. **Figure 3-1** shows the screenshot.

Figure 3-1 Modify VPC



* Name: vpc-ac951

* CIDR Block: 192 . 168 . 0 . 0 / 16

Shared SNAT: On

7. Click **OK**.

3.1.3 Deleting a VPC

Scenarios

You can delete a VPC if the VPC is no longer required.

You can delete a VPC only if there are no resources in the VPC. If there are resources in the VPC, you must delete those resources before you can delete the VPC.

A VPC cannot be deleted if it contains subnets, Direct Connect connections, custom routes, VPC peering connections, or VPNs. To delete the VPC, you must first delete or disable the following resources.

- Subnets. For details, see section **Deleting a Subnet**.
- VPNs. For details, see *Virtual Private Network User Guide*.
- Direct Connect connections. For details, see the *Direct Connect User Guide*.
- Custom routes. For details, see section **Deleting a Route**.
- VPC peering connections. For details, see section **Deleting a VPC Peering Connection**.

Notes and Constraints

If there are any EIPs or security groups, the last VPC cannot be deleted.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the row that contains the VPC to be deleted and click **Delete** in the **Operation** column.

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

3.1.4 Managing VPC Tags

Scenarios

A VPC tag identifies a VPC. Tags can be added to VPCs to facilitate VPC identification and management. 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 20 tags can be added to each VPC.

A tag consists of a key and value pair. **Table 3-4** lists the tag key and value requirements.

Table 3-4 VPC tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for the same VPC and can be the same for different VPCs. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	vpc-01

Procedure

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

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.

5. In the upper right corner of the VPC list, click **Search by Tag**.
6. In the displayed area, enter the tag key and value of the VPC you are looking for.

   Both the tag key and value must be specified. The system automatically displays the VPCs you are looking for if both the tag key and value are matched.
7. Click **+** to add another tag key and value.

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

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

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

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. 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.
6. 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. Enter the new tag key and 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**.

3.1.5 Exporting VPC Information

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, IP address ranges of VPCs, and the number of subnets.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. In the upper right corner of the VPC list, click ↗.

   The system will automatically export information about all VPCs under your account in the current region. They will be exported in Excel format.

3.2 Subnet

3.2.1 Creating a Subnet for the VPC

Scenarios

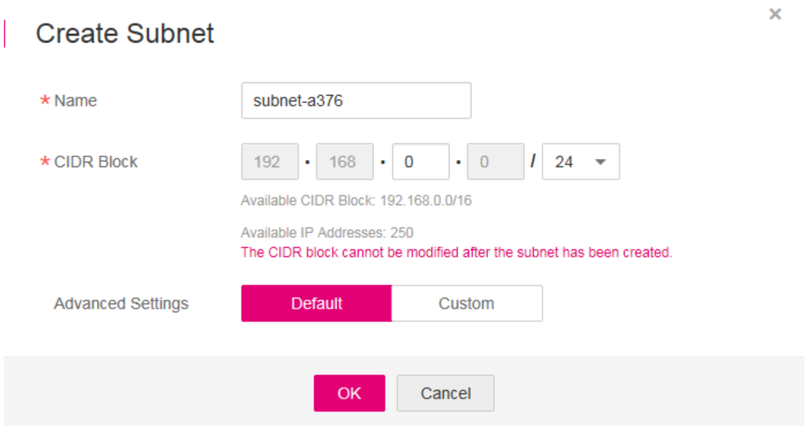
A VPC comes with a default subnet. If the default subnet cannot meet your requirements, you can create one.

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC for which a subnet is to be created and click the VPC name.
6. On the displayed **Subnets** tab, click **Create Subnet**.
7. Set the parameters as prompted.

Figure 3-2 Create Subnet



Create Subnet

* Name: subnet-a376

* CIDR Block: 192 . 168 . 0 . 0 / 24

Available CIDR Block: 192.168.0.0/16

Available IP Addresses: 250

The CIDR block cannot be modified after the subnet has been created.

Advanced Settings: Default | Custom

Table 3-5 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
CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
Advanced Settings	Two options are available, **Default** and **Custom**. You can set **Advanced Settings** to **Custom** to configure advanced subnet parameters.	Default
Gateway	The gateway address of the subnet.	192.168.0.1
DNS Server Address	By default, two DNS server addresses are configured. You can change them if necessary. A maximum of five DNS server addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
NTP Server Address	The IP address of the NTP server. This parameter is optional. 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 this parameter is left empty, no IP address of the NTP server is added. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 20 tags to each subnet. The tag key and value must meet the requirements listed in **Table 3-6**.	● Key: subnet_key1 ● Value: subnet-01

Table 3-6 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each subnet. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet-01

8. 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.

3.2.2 Modifying a Subnet

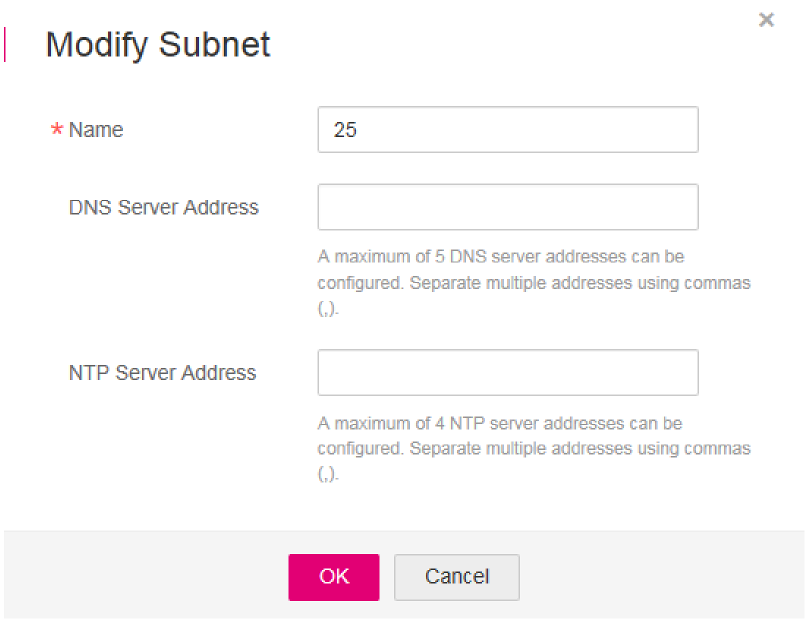
Scenarios

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC for which a subnet is to be modified and click the VPC name.
6. In the subnet list, locate the target subnet and click **Modify**. Modify the parameters as prompted.

Figure 3-3 Modify Subnet



Modify Subnet

* Name: 25

DNS Server Address:

A maximum of 5 DNS server addresses can be configured. Separate multiple addresses using commas (,).

NTP Server Address:

A maximum of 4 NTP server addresses can be configured. Separate multiple addresses using commas (,).

Table 3-7 Parameter descriptions

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

Parameter	Description	Example Value
DNS Server Address	By default, two DNS server addresses are configured. You can change them as required. A maximum of five DNS server addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
NTP Server Address	The IP address of the NTP server. This parameter is optional. 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 this parameter is left empty, no IP address of the NTP server is added. A maximum of four IP addresses can be configured. Multiple IP addresses must be separated using commas (,). **NOTE** ● 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.	192.168.2.1

7. Click **OK**.

3.2.3 Deleting a Subnet

Scenarios

You can delete a subnet to release network resources if the subnet is no longer required.

Prerequisites

You can delete a subnet only if there are no resources in the subnet. If there are resources in the subnet, you must delete those resources before you can delete the subnet.

You can view all resources of your account on the console homepage and check the resources that are in the subnet you want to delete.

The resources may include:

- ECS
- BMS
- CCE cluster
- RDS instance
- MRS cluster
- DCS instance
- Load balancer
- VPN
- Private IP address
- Custom route
- NAT gateway

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC from which a subnet is to be deleted and click the VPC name.
6. On the **Subnets** page, locate the target subnet and click **Delete**.
7. Click **Yes** in the displayed dialog box.

3.2.4 Managing Subnet Tags

Scenarios

A subnet tag identifies a subnet. Tags can be added to subnets to facilitate subnet identification and administration. 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 20 tags can be added to each subnet.

A tag consists of a key and value pair. **Table 3-8** lists the tag key and value requirements.

Table 3-8 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	● Cannot be left blank. ● Must be unique for each subnet. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	subnet-01

Procedure

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

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC containing the target subnet and click the VPC name.
6. In the upper right corner of the subnet list, click **Search by Tag**.
7. Enter the tag key of the subnet to be queried.

   Both the tag key and value must be specified. The system automatically displays the subnets you are looking for if both the tag key and value are matched.
8. Click **+** to add another tag key and value.

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

9. Click **Search**.

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

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

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC containing the target subnet and click the VPC name.
6. Click the name of the target subnet.
7. 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. Enter the new tag key and 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**.

4 Security

4.1 Security Group

4.1.1 Security Group Overview

Security Group

A security group is a collection of access control rules for ECSs that have the same security protection requirements and are mutually trusted within a VPC. After you create a security group, you can create different access rules for the security group, and the rules will apply to any ECS that the security group contains.

Your account automatically comes with a default security group. The default security group allows all outbound traffic, denies all inbound traffic, and allows all traffic between ECSs in the group. Your ECSs in this security group can communicate with each other already without adding additional rules. You can directly use the default security group. For details, see **Default Security Groups and Security Group Rules**.

You can also create custom security groups to meet your specific service requirements. For details, see **Creating a Security Group**.

Security Group Basics

- You can associate instances, such as servers and extension NICs, with one or more security groups.

  You can change the security groups that are associated with instances, such as servers or extension NICs. By default, when you create an instance, it is associated with the default security group of its VPC unless you specify another security group.
- You need to add security group rules to allow instances in the same security group to communicate with each other.
- 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 that they contain and security group rules are applied based on the connection status of the traffic to determine whether to allow or deny traffic. If you add, modify, or delete a security group rule, or create or delete an instance in the security group, the connection tracking of all instances in the security group will be automatically cleared. In this case, the inbound or outbound traffic of the instance will be considered as new connections, which need to match the inbound or outbound security group rules to ensure that the rules take effect immediately and the security of incoming traffic.

In addition, if the inbound or outbound traffic of an instance has no packets for a long time, the traffic will be considered as new connections after the connection tracking times out, and the connections need to match the outbound and inbound rules. The timeout period of connection tracking varies according to the protocol. The timeout period of a TCP connection in the established state is 600s, and the timeout period of an ICMP connection is 30s. For other protocols, if packets are received in both directions, the connection tracking timeout period is 180s. If one or more packets are received in one direction but no packet is received in the other direction, the connection tracking timeout period is 30s. For protocols other than TCP, UDP, and ICMP, only the IP address and protocol number are tracked.

NOTE

If two ECSs are in the same security group but in different VPCs, the ECSs cannot communicate with each other. To enable communications between the ECSs, use a VPC peering connection to connect the two VPCs.

Security Group Rules

After you create a security group, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After you add ECSs to the security group, they are protected by the rules of the group.

Each security group has **default rules**. You can also customize security group rules. For details, see **Adding a Security Group Rule**.

Security Group Constraints

- By default, you can create a maximum of 100 security groups in your cloud account.
- By default, you can add up to 50 security group rules to a security group.
- By default, you can add an ECS or an extension NIC to a maximum of five security groups. In such a case, the rules of all the selected security groups are aggregated to take effect.
- When creating a private network load balancer, you need to select a desired security group. Do not delete the default security group rules or ensure that the following requirements are met:
  - Outbound rules: only allow data packets to the selected security group or only data packets from the peer load balancer.
  - Inbound rules: only allow data packets from the selected security group or only data packets from the peer load balancer.

4.1.2 Default Security Groups and Security Group Rules

Your account automatically comes with a default security group. The default security group allows all outbound traffic, denies all inbound traffic, and allows all traffic between ECSs in the group. Your ECSs in this security group can communicate with each other already without adding additional rules.

Figure 4-1 shows the default security group.

Figure 4-1 Default security group

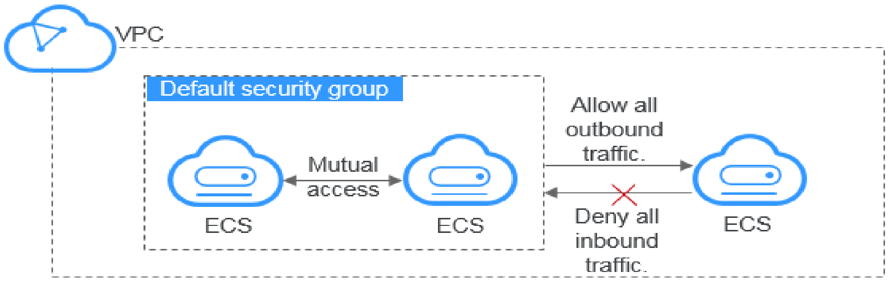


Table 4-1 describes the default rules for the default security group.

Table 4-1 Rules in the default security group

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 communication among ECSs within the security group and denies all inbound traffic (incoming data packets).

4.1.3 Security Group Configuration Examples

Common security group configurations are presented here. The examples in this section allow all outgoing data packets by default. This section will only describe how to configure inbound rules.

- **Allowing External Access to a Specified Port**
- **Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network**
- **Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group**

- **Remotely Connecting to Linux ECSs Using SSH**
- **Remotely Connecting to Windows ECSs Using RDP**
- **Enabling Communication Between ECSs**
- **Hosting a Website on ECSs**
- **Enabling an ECS to Function as a DNS Server**
- **Uploading or Downloading Files Using FTP**

You can use the default security group or create a security group in advance. For details, see sections **Creating a Security Group** and **Adding a Security Group Rule**.

Allowing External Access to a Specified Port

- Example scenario:

  After services are deployed, you can add security group rules to allow external access to a specified port (for example, 1100).

- Security group rule:

Direction	Protocol	Port	Source
Inbound	TCP	1100	0.0.0.0/0

Enabling ECSs in Different Security Groups to Communicate with Each Other Through an Internal Network

- Example scenario:

  Resources on an ECS in a security group need to be copied to an ECS associated with another security group. The two ECSs are in the same VPC. We recommend that you enable private network communication between the ECSs and then copy the resources.

- Security group configuration:

  Within a given VPC, ECSs in the same security group can communicate with one another by default. However, ECSs in different security groups cannot communicate with each other by default. To enable these ECSs to communicate with each other, you need to add certain security group rules.

  You can add an inbound rule to the security groups containing the ECSs to allow access from ECSs in the other security group. The required rule is as follows.

Direction	Protocol/Application	Port	Source
Inbound	Used for communication through an internal network	Port or port range	ID of another security group

Enabling Specified IP Addresses to Remotely Access ECSs in a Security Group

- Example scenario:

  To prevent ECSs from being attacked, you can change the port number for remote login and configure security group rules that allow only specified IP addresses to remotely access the ECSs.

- Security group configuration:

  To allow IP address **192.168.20.2** to remotely access Linux ECSs in a security group over the SSH protocol (port 22), you can configure the following security group rule.

Direction	Protocol	Port	Source
Inbound	SSH	22	IPv4 CIDR block or ID of another security group For example, 192.168.20.2/32

Remotely Connecting to Linux ECSs Using SSH

- Example scenario:

  After creating Linux ECSs, you can add a security group rule to enable remote SSH access to the ECSs.

- Security group rule:

Direction	Protocol	Port	Source
Inbound	SSH	22	0.0.0.0/0

Remotely Connecting to Windows ECSs Using RDP

- Example scenario:

  After creating Windows ECSs, you can add a security group rule to enable remote RDP access to the ECSs.

- Security group rule:

Direction	Protocol	Port	Source
Inbound	RDP	3389	0.0.0.0/0

Enabling Communication Between ECSs

- Example scenario:

  After creating ECSs, you need to add a security group rule so that you can run the **ping** command to test communication between the ECSs.

- Security group rule:

Direction	Protocol	Port	Source
Inbound	ICMP	All	0.0.0.0/0

Hosting a Website on ECSs

- Example scenario:

  If you deploy a website on your ECSs and require that your website be accessed over HTTP or HTTPS, you can add rules to the security group used by the ECSs that function as the web servers.

- Security group rule:

Direction	Protocol	Port	Source
Inbound	HTTP	80	0.0.0.0/0
Inbound	HTTPS	443	0.0.0.0/0

Enabling an ECS to Function as a DNS Server

- Example scenario:

  If you need to use an ECS as a DNS server, you must allow TCP and UDP access from port 53 to the DNS server. You can add the following rules to the security group associated with the ECS.

- Security group rules:

Direction	Protocol	Port	Source
Inbound	TCP	53	0.0.0.0/0
Inbound	UDP	53	0.0.0.0/0

Uploading or Downloading Files Using FTP

- Example scenario:

  If you want to use File Transfer Protocol (FTP) to upload files to or download files from ECSs, you need to add a security group rule.

  NOTE

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

- Security group rule:

Direction	Protocol	Port	Source
Inbound	TCP	20-21	0.0.0.0/0

4.1.4 Creating a Security Group

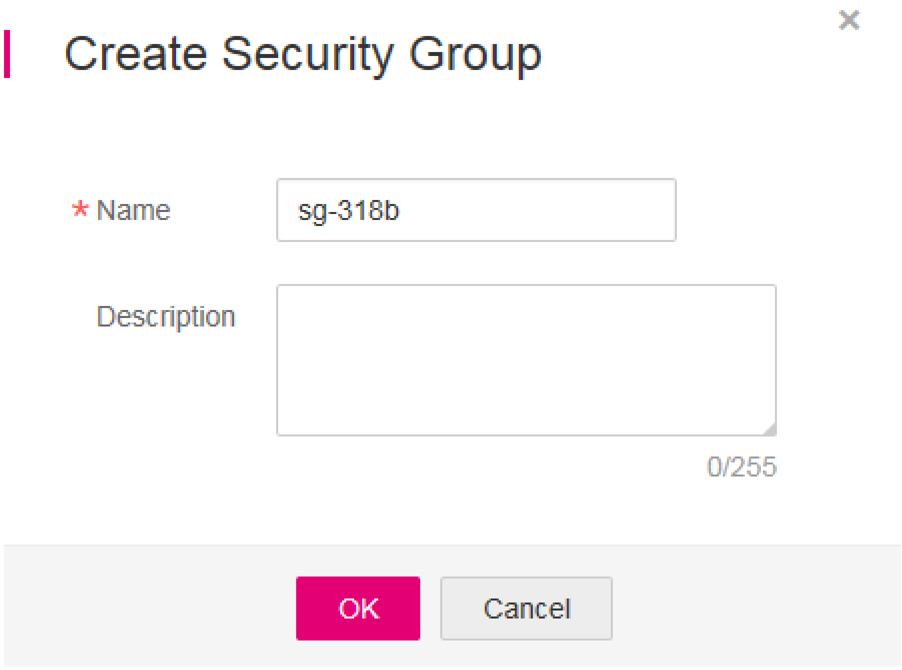
Scenarios

To improve ECS access security, you can create security groups, define security group rules, and add ECSs in a VPC to different security groups. We recommend that you allocate ECSs that have different Internet access policies to different security groups.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click **Create Security Group**.
6. In the **Create Security Group** area, set the parameters as prompted. **Table 4-2** lists the parameters to be configured.

Figure 4-2 Create Security Group



Create Security Group

* Name: sg-318b

Description:

0/255

Table 4-2 Parameter description

Parameter	Description	Example Value
Name	The security group name. This parameter is mandatory. 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. **NOTE** 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.	sg-318b
Description	Supplementary information about the security group. This parameter is optional. The security group description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.

4.1.5 Adding a Security Group Rule

Scenarios

After you create a security group, you can add rules to the security group. A rule applies either to inbound traffic or outbound traffic. After you add ECSs to the security group, they are protected by the rules of the group.

- Inbound rules control incoming traffic to ECSs associated with the security group.
- Outbound rules control outgoing traffic from ECSs associated with the security group.

For details about the default security group rules, see **Default Security Groups and Security Group Rules**. For details about security group rule configuration examples, see **Security Group Configuration Examples**.

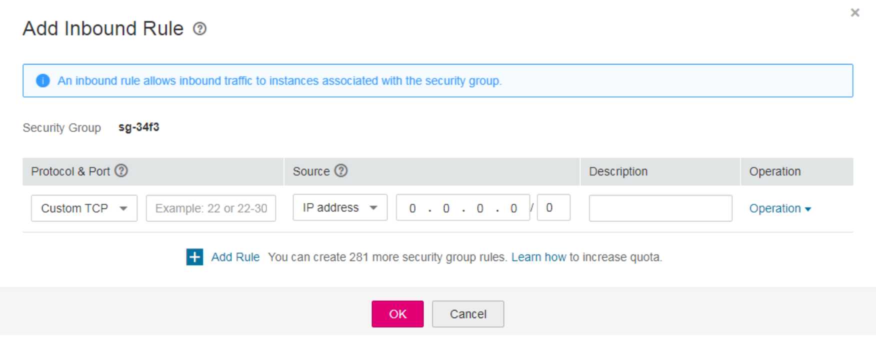
Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.

6. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   You can click **+** to add more inbound rules.

Figure 4-3 Add Inbound Rule



Add Inbound Rule

An inbound rule allows inbound traffic to instances associated with the security group.

Security Group **sg-34f3**

Protocol & Port		Source		Description	Operation
Custom TCP	Example: 22 or 22-30	IP address	0 . 0 . 0 . 0 / 0		Operation

Add Rule You can create 281 more security group rules. Learn how to increase quota.

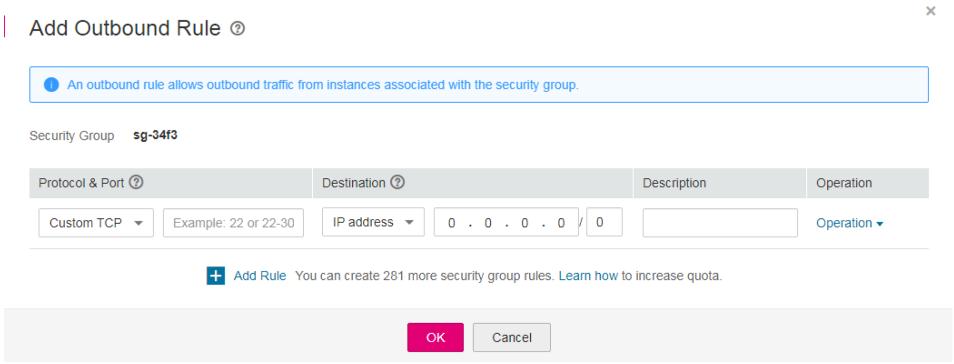
Table 4-3 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: The network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: The port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30
Source	The source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses) ● sg-abc (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. On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

   You can click **+** to add more outbound rules.

Figure 4-4 Add Outbound Rule



Add Outbound Rule

An outbound rule allows outbound traffic from instances associated with the security group.

Security Group sg-34f3

Protocol & Port		Destination		Description	Operation
Custom TCP	Example: 22 or 22-30	IP address	0 . 0 . 0 . 0 / 0		Operation

Add Rule You can create 281 more security group rules. Learn how to increase quota.

Table 4-4 Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	**Protocol**: The network protocol. Currently, the value can be **All**, **TCP**, **UDP**, **ICMP**, **GRE**, or others.	TCP
	Port: The port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30
Destination	The destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: ● xxx.xxx.xxx.xxx/32 (IPv4 address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses) ● sg-abc (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

8. Click **OK**.

4.1.6 Fast-Adding Security Group Rules

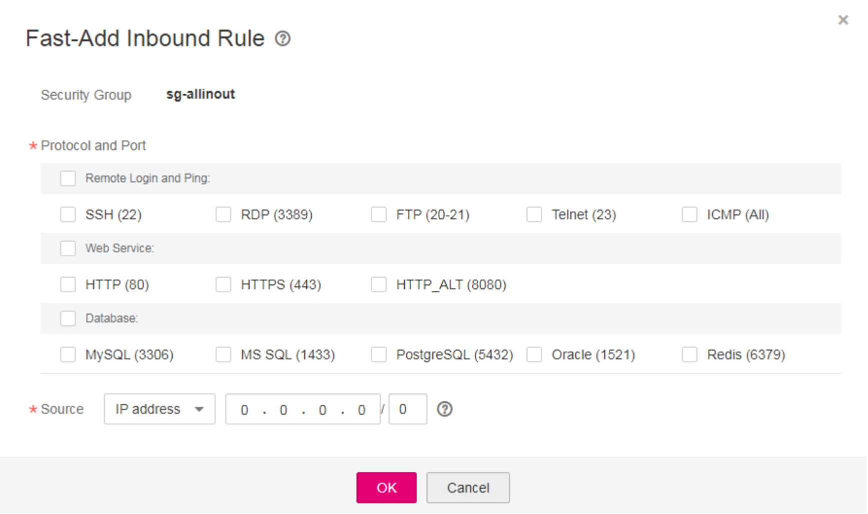
Scenarios

You can add multiple security group rules with different protocols and ports at the same time.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
6. On the **Inbound Rules** tab, click **Fast-Add Rule**. In the displayed dialog box, select the protocols and ports you wish to add all at once.

Figure 4-5 Fast-Add Inbound Rule



Fast-Add Inbound Rule ⓘ

Security Group sg-allinout

* Protocol and Port

□ Remote Login and Ping:

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

□ Web Service:

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

□ Database:

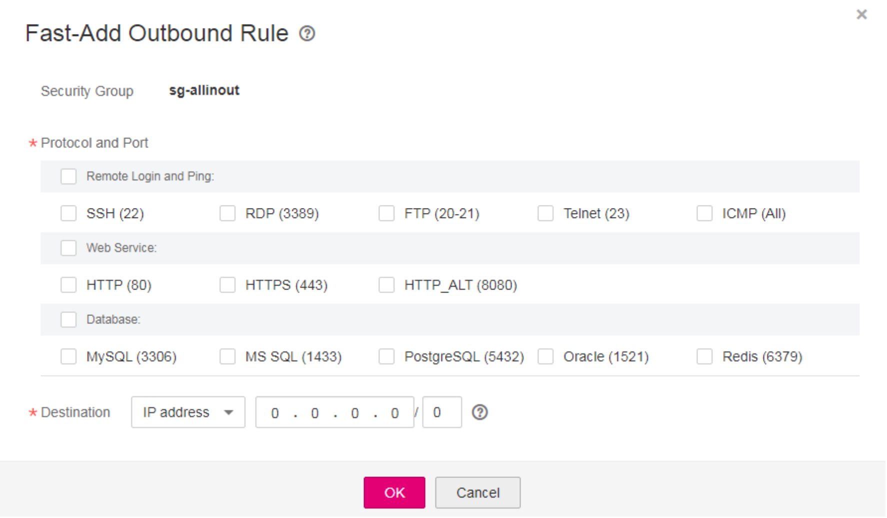
□ MySQL (3306) □ MS SQL (1433) □ PostgreSQL (5432) □ Oracle (1521) □ Redis (6379)

* Source IP address 0 . 0 . 0 . 0 / 0 ⓘ

OK Cancel

7. On the **Outbound Rules** tab, click **Fast-Add Rule**. In the displayed dialog box, select required protocols and ports to add multiple rules at a time.

Figure 4-6 Fast-Add Outbound Rule



Fast-Add Outbound Rule ⓘ

Security Group sg-allinout

* Protocol and Port

□ Remote Login and Ping:

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

□ Web Service:

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

□ Database:

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

* Destination IP address 0 . 0 . 0 . 0 / 0 ⓘ

OK Cancel

8. Click **OK**.

4.1.7 Replicating a Security Group Rule

Scenarios

Replicate an existing security group rule to generate a new rule. When replicating a security group rule, you can make changes so that it is not a perfect copy.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click the security group name.
6. On the displayed page, locate the row that contains the security group rule to be replicated, and click **Replicate** in the **Operation** column.

   You can also modify the security group rule as required to quickly generate a new rule.
7. Click **OK**.

4.1.8 Modifying a Security Group Rule

Scenarios

You can modify the port, protocol, and IP address of a security group rule to meet your specific requirements.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click the security group name.
6. On the displayed page, locate the row that contains the security group rule to be modified, and click **Modify** in the **Operation** column.
7. Modify the rule and click **Confirm**.

4.1.9 Deleting a Security Group Rule

Scenarios

If the source of an inbound security group rule or destination of an outbound security group rule needs to be changed, you need to first delete the security group rule and add a new one.

NOTE

Security group rules use whitelists. Deleting a security group rule may result in ECS access failures.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click the security group name.
6. If you do not need a security group rule, locate the row that contains the target rule, and click **Delete**.
7. Click **Yes** in the displayed dialog box.

Deleting multiple security group rules at once

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

4.1.10 Importing and Exporting Security Group Rules

Scenarios

If you want to quickly apply the rules of one security group to another, or if you want to modify multiple rules of the current security group at once, you can import or export existing rules.

Security group rules are imported or exported to an Excel file.

Notes and Constraints

When modifying exported security group rules, you can only modify existing fields in the exported file based on the template and cannot add new fields or modify the field names. Otherwise, the file will fail to be imported.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click the security group name.
6. On the displayed page, 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.

4.1.11 Deleting a Security Group

Scenarios

You can delete a security group to release resources if the security group is no longer required.

Notes and Constraints

- The default security group cannot be deleted.
- If a security group is associated with resources other than servers and extension NICs, the security group cannot be deleted.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the row that contains the target security group, click **More** in the **Operation** column, and click **Delete**.
6. Click **Yes** in the displayed dialog box.

4.1.12 Adding Instances to and Removing Them from a Security Group

Scenarios

After a security group is created, you can add instances, including servers and extension NICs, to the security group to protect the instances. If the instances are not required, you can also remove them from the security group.

You can add multiple instances to or remove them from a security group.

Adding Instances to a Security Group

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click **Associate Instance** in the **Operation** column.
6. On the **Servers** tab, click **Add** and add one or more servers to the current security group.

7. On the **Extension NICs** tab, click **Add** and add one or more extension NICs to the current security group.
8. Click **OK**.

Removing Instances from a Security Group

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click **Associate Instance** in the **Operation** column.
6. On the **Servers** tab, locate the target server and click **Remove** in the **Operation** column to remove the server from current security group.
7. On the **Extension NICs** tab, locate the target extension NIC and click **Remove** in the **Operation** column to remove the NIC from the current security group.
8. Click **Yes**.

Removing multiple instances from a security group

Select multiple servers and click **Remove** above the server list to remove the selected servers from the current security group all at once.

Select multiple extension NICs and click **Remove** above the extension NIC list to remove the selected extension NICs from the current security group all at once.

4.1.13 Modifying a Security Group

Scenarios

Modify the name and description of a created security group.

Procedure

Method 1

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, locate the target security group and choose **Modify** in the **Operation** column.
6. Modify the name and description of the security group as required.
7. Click **OK**.

Method 2

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

3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
5. On the **Security Groups** page, click the security group name.
6. On the displayed page, click ✎ on the right of **Name** and edit the security group name.
7. Click **√** to save the security group name.
8. Click ✎ on the right of **Description** and edit the security group description.
9. Click **√** to save the security group description.

4.1.14 Viewing the Security Group of an ECS

Scenarios

View inbound and outbound rules of a security group used by an ECS.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the target ECS.
5. Click the **Security Groups** tab and view information about the security group used by the ECS.

4.1.15 Changing the Security Group of an ECS

Scenarios

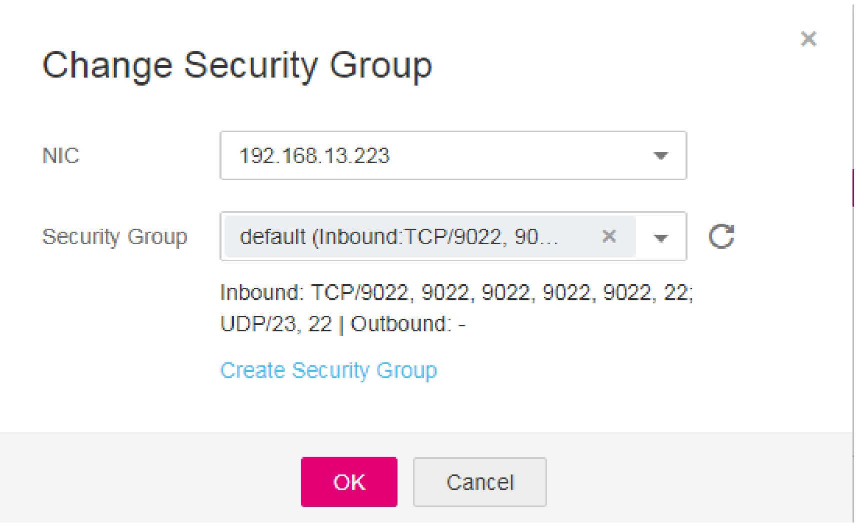
Change the security group associated with an ECS NIC.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select your region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. Locate the row containing the target ECS. Click **More** in the **Operation** column and select **Change Security Group**.

   The **Change Security Group** dialog box is displayed.

Figure 4-7 Change Security Group



Change Security Group

NIC: 192.168.13.223

Security Group: default (Inbound:TCP/9022, 90...

Inbound: TCP/9022, 9022, 9022, 9022, 9022, 22; UDP/23, 22 | Outbound: -

5. Select the target NIC and security groups as prompted.

   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.

6. Click **OK**.

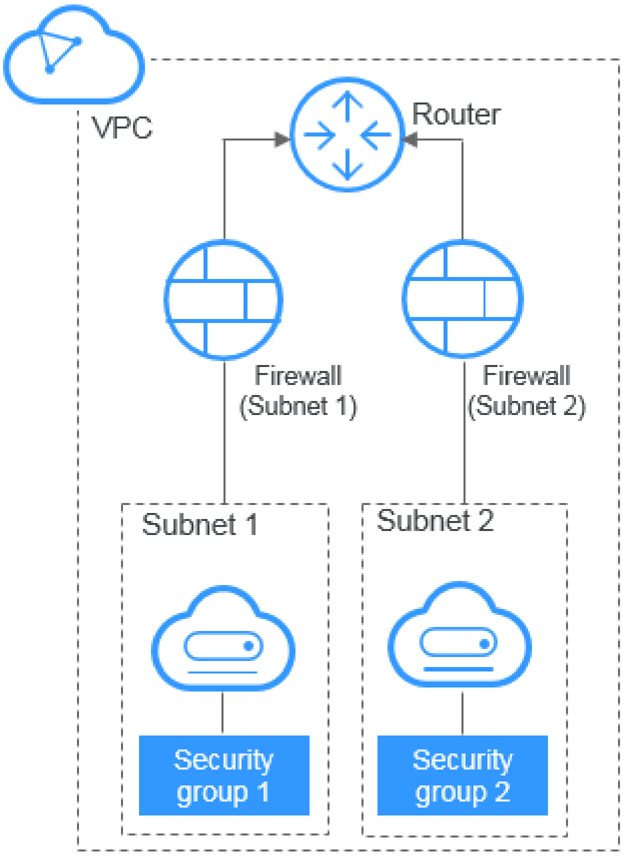
4.2 Firewall

4.2.1 Firewall Overview

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

Figure 4-8 shows how a firewall works.

Figure 4-8 Security groups and firewalls



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

Differences Between Security Groups and Firewalls summarizes the basic differences between security groups and firewalls.

Firewall Basics

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

Default Firewall Rules

By default, each firewall 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 firewall denies all traffic in and out of a subnet excepting the preceding ones. **Table 4-5** shows the default firewall rules. You cannot modify or delete the default rules.

Table 4-5 Default firewall 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.

Rule Priorities

- Each firewall 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 firewall 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 firewall 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 firewall rules to deny access traffic from a specific port and protocol, for example, TCP port 445.
- No defense is required for the east-west traffic between subnets, but access control is required for north-south traffic.

  Solution: You can add firewall rules to protect north-south traffic.

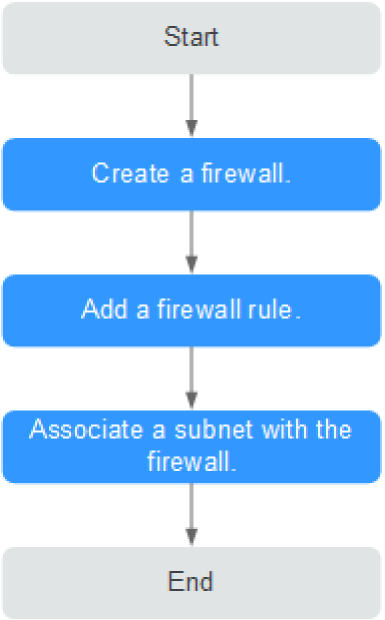
- For frequently accessed applications, a security rule sequence may need to be adjusted to improve performance.

  Solution: A firewall allows you to adjust the rule sequence so that frequently used rules are applied before other rules.

Configuration Procedure

Figure 4-9 shows the procedure for configuring a firewall.

Figure 4-9 Firewall configuration procedure



1. Create a firewall by following the steps described in **Creating a Firewall**.
2. Add firewall rules by following the steps described in **Adding a Firewall Rule**.
3. Associate subnets with the firewall by following the steps described in **Associating Subnets with a Firewall**. After subnets are associated with the firewall, the subnets will be protected by the configured firewall rules.

4.2.2 Firewall Configuration Examples

This section provides examples for configuring firewalls.

- **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 445 to protect against the WannaCry ransomware attacks. You can add a firewall rule to deny all incoming traffic from TCP port 445.

Firewall Configuration

Table 4-6 lists the inbound rule required.

Table 4-6 Firewall 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 firewall denies all inbound traffic. You need 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 Firewall 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 regardless of the port. You need to configure both the firewall rules and security group rules to allow the traffic.

Firewall Configuration

Table 4-7 lists the inbound rule required.

Table 4-7 Firewall 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 4-8 lists the inbound and outbound security group rules required.

Table 4-8 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 firewall adds an additional layer of security. Even if the security group rules allow more traffic than that actually required, the firewall rules allow only access from HTTP port 80 and HTTPS port 443 and deny other inbound traffic.

4.2.3 Creating a Firewall

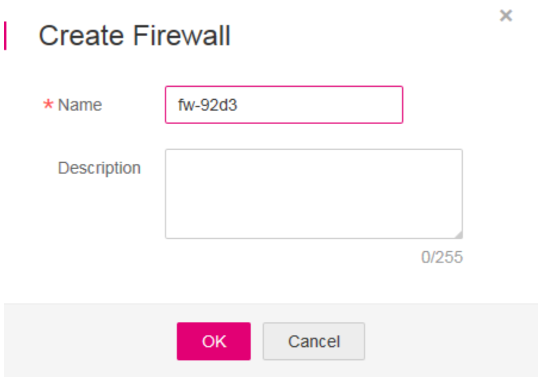
Scenarios

You can create a custom firewall, but any newly created firewall will be disabled by default. It will not have any inbound or outbound rules, or have any subnets associated. Each user can create up to 200 firewalls by default.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. In the right pane displayed, click **Create Firewall**.
6. In the displayed dialog box, enter firewall information as prompted. **Table 4-9** lists the parameters to be configured.

Figure 4-10 Create Firewall



Create Firewall

* Name: fw-92d3

Description:

Table 4-9 Parameter descriptions

Parameter	Description	Example Value
Name	The firewall 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 firewall. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.

4.2.4 Adding a Firewall Rule

Scenarios

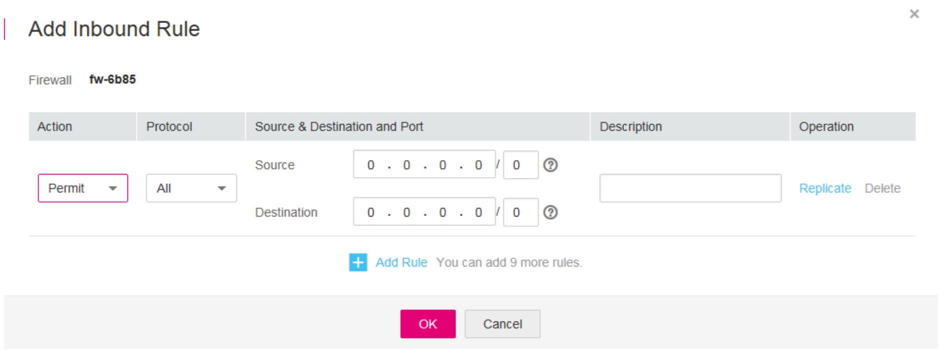
Add an inbound or outbound rule based on your network security requirements.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall and click its name to switch to the page showing details of that particular firewall.
6. On the **Inbound Rules** or **Outbound Rules** tab, click **Add Rule** to add an inbound or outbound rule.

   You can click **+** to add more rules.

Figure 4-11 Add Inbound Rule



Add Inbound Rule

Firewall **fw-6b85**

Action	Protocol	Source & Destination and Port	Description	Operation
Permit	All	Source 0 . 0 . 0 . 0 / 0 Destination 0 . 0 . 0 . 0 / 0		Replicate Delete

Add Rule You can add 9 more rules.

OK Cancel

Table 4-10 Parameter descriptions

Parameter	Description	Example Value
Action	The action in the firewall. 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 firewall. This parameter is mandatory. You can select a value from the drop-down list. The value can be **TCP**, **UDP**, **All**, or **ICMP**. If **ICMP** or **All** is selected, you do not need to specify port information.	TCP

Parameter	Description	Example Value
Source	The source from which the traffic is allowed. The source can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic from all IP addresses is allowed. For example: ● xxx.xxx.xxx.xxx/32 (IP address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses)	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**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30
Destination	The destination to which the traffic is allowed. The destination can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed. For example: ● xxx.xxx.xxx.xxx/32 (IP address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses)	0.0.0.0/0
Destination Port Range	The destination port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30
Description	Supplementary information about the firewall rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **OK**.

4.2.5 Associating Subnets with a Firewall

Scenarios

On the page showing firewall details, associate desired subnets with a firewall. After a firewall is associated with a subnet, the firewall denies all traffic to and from the subnet until you add rules to allow traffic.

Procedure

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

NOTE

Subnets that have already been associated with firewalls will not be displayed on the page for you to select. One-click subnet association and disassociation are not currently supported. Furthermore, a subnet can only be associated with one firewall. If you want to reassociate a subnet that has already been associated with another firewall, you must first disassociate the subnet from the original firewall.

4.2.6 Disassociating a Subnet from a Firewall

Scenarios

Disassociate a subnet from a firewall when necessary.

Procedure

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

Disassociating subnets from a firewall

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

4.2.7 Changing the Sequence of a Firewall 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 firewall 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 select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall and click its name to switch to the page showing details of that particular firewall.
6. 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**.
7. 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.

4.2.8 Modifying a Firewall Rule

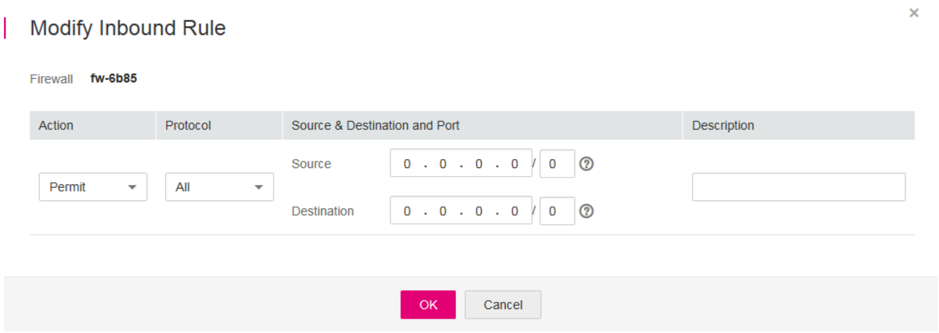
Scenarios

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall and click its name to switch to the page showing details of that particular firewall.
6. 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 4-11** lists the parameters to be configured.

Figure 4-12 Modify Rule



Modify Inbound Rule

Firewall fw-6b85

Action	Protocol	Source & Destination and Port	Description
Permit	All	Source 0 . 0 . 0 . 0 / 0 Destination 0 . 0 . 0 . 0 / 0	

Table 4-11 Parameter descriptions

Parameter	Description	Example Value
Action	The action in the firewall. 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 firewall. This parameter is mandatory. You can select a value from the drop-down list. The value can be **TCP**, **UDP**, **All**, or **ICMP**. If **ICMP** or **All** is selected, you do not need to specify port information.	TCP
Source	The source from which the traffic is allowed. The source can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic from all IP addresses is allowed. For example: ● xxx.xxx.xxx.xxx/32 (IP address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses)	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**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30

Parameter	Description	Example Value
Destination	The destination to which the traffic is allowed. The destination can be an IP address or IP address range. The default value is **0.0.0.0/0**, which indicates that traffic to all IP addresses is allowed. For example: ● xxx.xxx.xxx.xxx/32 (IP address) ● xxx.xxx.xxx.0/24 (IP address range) ● 0.0.0.0/0 (all IP addresses)	0.0.0.0/0
Destination Port Range	The destination port number or port number range. The value ranges from 1 to 65535. For a port number range, enter two port numbers connected by a hyphen (-). For example, **1-100**. You must specify this parameter if **TCP** or **UDP** is selected for **Protocol**.	22, or 22-30
Description	Supplementary information about the firewall rule. This parameter is optional. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

7. Click **Confirm**.

4.2.9 Enabling or Disabling a Firewall Rule

Scenarios

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall and click its name to switch to the page showing details of that particular firewall.
6. 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.

7. 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.

4.2.10 Deleting a Firewall Rule

Scenarios

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall and click its name to switch to the page showing details of that particular firewall.
6. On the **Inbound Rules** or **Outbound Rules** tab, locate the row that contains the target rule and click **Delete** in the **Operation** column.
7. Click **Yes** in the displayed dialog box.

Deleting multiple firewall rules at a time

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

4.2.11 Viewing a Firewall

Scenarios

View details about a firewall.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall and click its name to switch to the page showing details of that particular firewall.
6. 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.

4.2.12 Modifying a Firewall

Scenarios

Modify the name and description of a firewall.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall and click its name to switch to the page showing details of that particular firewall.
6. On the displayed page, click ✏ on the right of **Name** and edit the firewall name.
7. Click √ to save the new firewall name.
8. Click ✏ on the right of Description and edit the firewall description.
9. Click √ to save the new firewall description.

4.2.13 Enabling or Disabling a Firewall

Scenarios

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

When a firewall is disabled, custom rules will become invalid. Disabling a firewall may interrupt network traffic. For information about the default firewall rules, see **Default Firewall Rules**.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the row that contains the target firewall in the right pane, click **More** in the **Operation** column, and click **Enable** or **Disable**.
6. Click **Yes** in the displayed dialog box.

4.2.14 Deleting a Firewall

Scenarios

Delete a firewall when it is no longer required.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Access Control** > **Firewalls**.
5. Locate the target firewall in the right pane, click **More** in the **Operation** column, and click **Delete**.
6. Click **Yes**.

   NOTE

   After a firewall is deleted, associated subnets are disassociated and added rules are deleted from the firewall.

4.3 Differences Between Security Groups and Firewalls

You can configure security groups and firewall to increase the security of ECSs in your VPC.

- Security groups operate at the ECS level.
- Firewalls operate at the subnet level.

For details, see **Figure 4-13**.

Figure 4-13 Security groups and firewalls

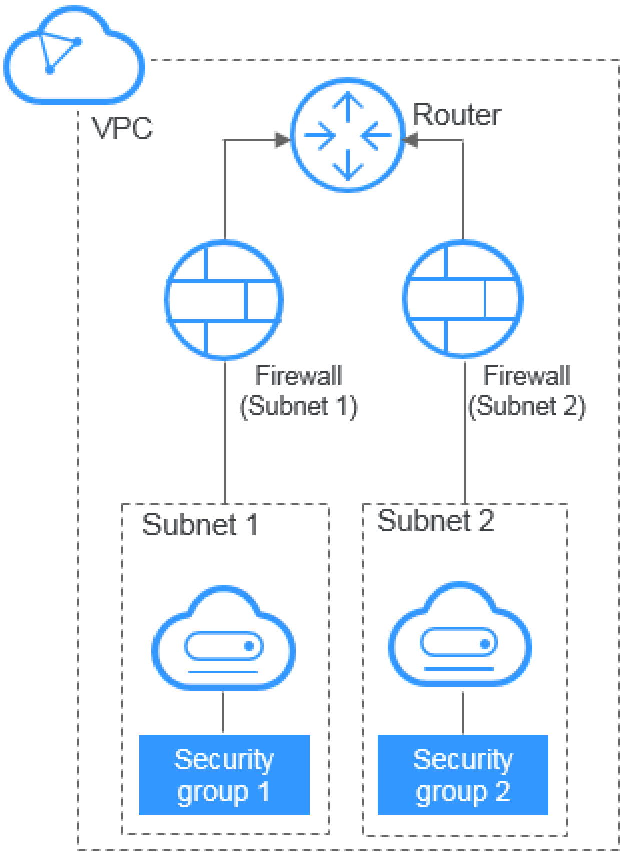


Table 4-12 describes the differences between security groups and firewalls.

Table 4-12 Differences between security groups and firewalls

Category	Security Group	Firewall
Targets	Operates at the ECS level.	Operates at the subnet level.
Rules	Only supports **Allow** rules.	Supports **Allow** and **Deny** rules.
Priority	If security group rules conflict, the overlapping elements of these rules take effect.	If rules conflict, the rule with the highest priority takes effect.
Usage	Automatically applies to ECSs in the security group that is selected during ECS creation. You must select a security group when creating ECSs.	Applies to all ECSs in the subnets associated with the firewall. Selecting a firewall is not allowed during subnet creation. You must create a firewall, associate subnets with it, add inbound and outbound rules, and enable firewall. The firewall then takes effect for the associated subnets and ECSs in the subnets.

Category	Security Group	Firewall
Packets	Only packet filtering based on the 3-tuple (protocol, port, and peer IP address) is supported.	Only packet filtering based on the 5-tuple (protocol, source port, destination port, source IP address, and destination IP address) is supported.

5 EIP

5.1 Assigning an EIP and Binding It to an ECS

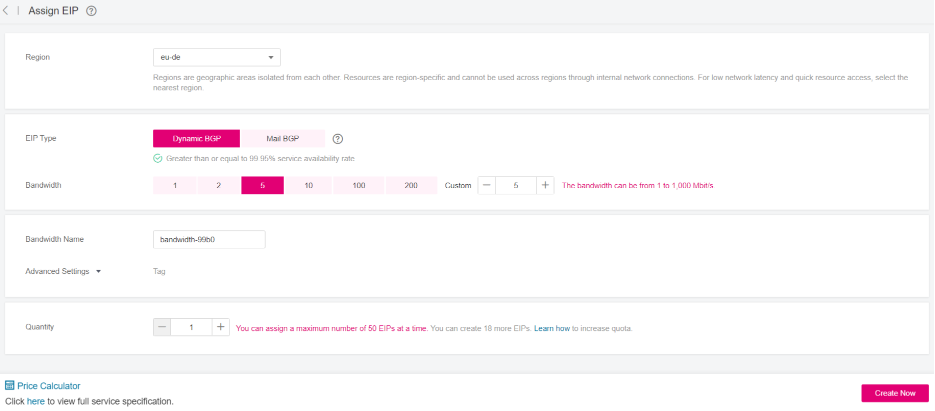
Scenarios

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 select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. On the displayed page, click **Assign EIP**.
5. Set the parameters as prompted.

Figure 5-1 Assign EIP



Assign EIP

Region: eu-de

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

EIP Type: Dynamic BGP

Greater than or equal to 99.95% service availability rate

Bandwidth: 5

The bandwidth can be from 1 to 1,000 Mbit/s.

Bandwidth Name: bandwidth-99b0

Quantity: 1

You can assign a maximum number of 50 EIPs at a time. You can create 18 more EIPs. Learn how to increase quota.

Click here to view full service specification.

Table 5-1 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.	eu-de
Type	● **Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails. ● **Mail BGP**: EIPs with port 25, 465, or 587 enabled are used. The selected EIP type cannot be changed after the EIP is assigned.	Dynamic BGP
Bandwidth	The bandwidth size in Mbit/s.	100
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 5-2**.	● Key: Ipv4_key1 ● Value: 192.168.12.10
Quantity	The number of EIPs you want to purchase.	1

Table 5-2 EIP tag requirements

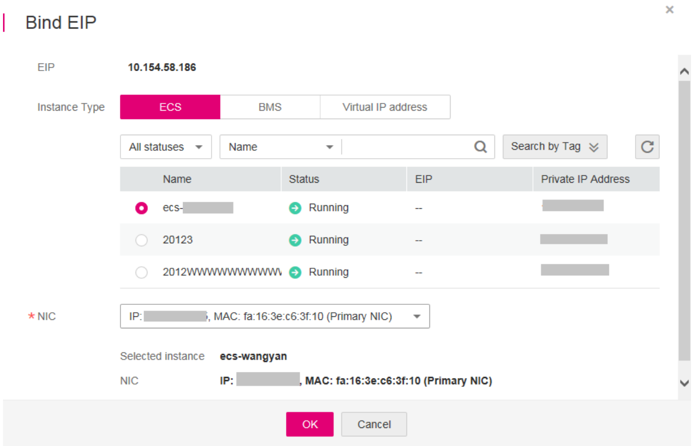
Parameter	Requirement	Example Value
Key	● Cannot be left blank. ● Must be unique for each EIP. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	Ipv4_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	192.168.12.10

6. Click **Assign Now**.
7. Click **Submit**.

Binding an EIP

1. On the **EIPs** page, locate the row that contains the target EIP, and click **Bind**.
2. Select the instance to which you want to bind the EIP.

Figure 5-2 Bind EIP



Bind EIP

EIP 10.154.58.186

Instance Type: ECS | BMS | Virtual IP address

	Name	Status	EIP	Private IP Address
●	ecs-[redacted]	Running	--	[redacted]
○	20123	Running	--	[redacted]
○	2012WWWWWWWWWW\	Running	--	[redacted]

* NIC: IP: [redacted], MAC: fa:16:3e:c6:3f:10 (Primary NIC)

Selected instance: **ecs-wangyan**

NIC: **IP: [redacted], MAC: fa:16:3e:c6:3f:10 (Primary NIC)**

3. Click **OK**.

An IPv6 client on the Internet can access the ECS that has an EIP bound in a VPC. For details about the implementation and constraints, see **How Does an IPv6 Client on the Internet Access the ECS That Has an EIP Bound in a VPC?**

Follow-Up Procedure

After an ECS with an EIP bound is created, the system generates a domain name in the format of **ecs-*xx-xx-xx-xx*.compute.*xxx*.com** for the EIP by default. *xx-xx-xx-xx* indicates the EIP, and xxx indicates the domain name of the cloud service provider. You can use the domain name to access the ECS.

You can use any of the following commands to obtain the domain name of an EIP:

- ping -a *EIP*
- nslookup [-qt=ptr] *EIP*
- dig -x *EIP*

5.2 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

- EIPs assigned and bound to load balancers in the ELB service are displayed in the EIP list of the VPC service, but you cannot unbind these EIPs from the load balancers.
- You can only release unbound EIPs.

Procedure

Unbinding a single EIP

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. On the displayed page, locate the row that contains the target EIP, and click **Unbind**.
5. Click **Yes** in the displayed dialog box.

Releasing a single EIP

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

3. On the console homepage, under **Network**, click **Elastic IP**.
4. On the displayed page, locate the row that contains the target EIP, click **More** and then **Release** in the **Operation** column.
5. Click **Yes** in the displayed dialog box.

Unbinding multiple EIPs at once

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. On the displayed page, select the EIPs to be unbound.
5. Click the **Unbind** button located above the EIP list.
6. Click **Yes** in the displayed dialog box.

Releasing multiple EIPs at once

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. On the displayed page, select the EIPs to be released.
5. Click the **Release** button located above the EIP list.
6. Click **Yes** in the displayed dialog box.

5.3 Managing EIP Tags

Scenarios

Tags can be added to EIPs to facilitate EIP identification and administration. You can add a tag to an EIP when assigning the EIP. Alternatively, you can add a tag to an assigned EIP on the EIP details page. A maximum of 20 tags can be added to each EIP.

A tag consists of a key and value pair. **Table 5-3** lists the tag key and value requirements.

Table 5-3 EIP tag requirements

Parameter	Requirement	Example Value
Key	● Cannot be left blank. ● Must be unique for each EIP. ● Can contain a maximum of 36 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	Ipv4_key1
Value	● Can contain a maximum of 43 characters. ● Can contain only the following character types: – Uppercase letters – Lowercase letters – Digits – Special characters, including hyphens (-) and underscores (_)	192.168.12.10

Procedure

Searching for EIPs by tag key and value on the page showing the EIP list

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. In the upper right corner of the EIP list, click **Search by Tag**.
5. In the displayed area, enter the tag key and value of the EIP you are looking for.

   You must specify both the tag key and value. The system will display the EIPs that contain the tag you specified.
6. Click **+** to add another tag key and value.

   You can add multiple tag keys and values to refine your search results. If you add more than one tag to search for EIPs, the system will display only the EIPs that contain all of the tags you specified.
7. Click **Search**.

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

Adding, deleting, editing, and viewing tags on the Tags tab of an EIP

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. On the displayed page, locate the EIP whose tags you want to manage, and click the EIP name.
5. On the page showing EIP details, click the **Tags** tab and perform desired operations on tags.
   - View tags.

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

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

     Locate the row that contains the tag you want to edit, and click **Edit** in the **Operation** column. Enter the new tag key and 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**.

5.4 Modifying an EIP Bandwidth

Scenarios

Modify the EIP bandwidth name or size.

NOTE

This section describes how to modify the dedicated bandwidth or shared bandwidth of an EIP. For details about how to modify a shared bandwidth, see **Modifying a Shared Bandwidth**.

Procedure

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

6 Shared Bandwidth

6.1 Shared Bandwidth Overview

Shared bandwidth allows multiple EIPs to share the same bandwidth. All ECSs, BMSs, and load balancers that have EIPs bound in the same region can share a bandwidth.

When you host a large number of applications on the cloud, if each EIP uses an independent 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.

- Easy to Manage

  Region-level bandwidth sharing and multiplexing simplify O&M statistics, management, and operations cost settlement.
- Flexible Operations

  You can add EIPs to a shared bandwidth or remove them from a shared bandwidth regardless of the instances to which they are bound.

6.2 Assigning a Shared Bandwidth

Scenarios

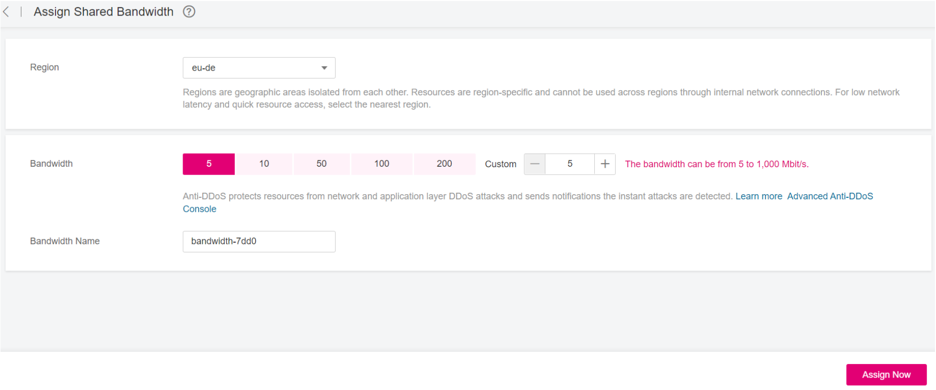
Assign a shared bandwidth for use with EIPs.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.

5. In the upper right corner, click **Assign Shared Bandwidth**. On the displayed page, configure parameters as prompted.

Figure 6-1 Assigning Shared Bandwidth



Region: eu-de

Regions are geographic areas isolated from each other. Resources are region-specific and cannot be used across regions through internal network connections. For low network latency and quick resource access, select the nearest region.

Bandwidth: 5

The bandwidth can be from 5 to 1,000 Mbit/s.

Anti-DDoS protects resources from network and application layer DDoS attacks and sends notifications the instant attacks are detected.

Bandwidth Name: bandwidth-7dd0

Table 6-1 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.	eu-de
Bandwidth	The bandwidth size in Mbit/s. The value ranges from starting with 5 Mbit/s. The maximum bandwidth can be 300 Mbit/s.	10
Bandwidth Name	The name of the shared bandwidth.	Bandwidth-001

6. Click **Create Now**.

6.3 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.

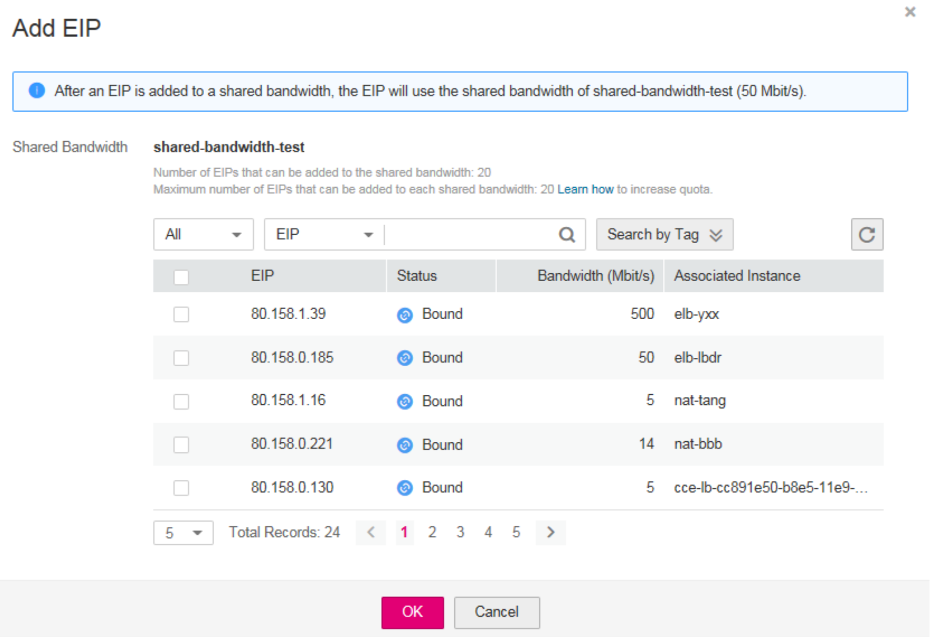
Notes and Constraints

- After an EIP is added to a shared bandwidth, the original bandwidth used by the EIP will become invalid and the EIP will start to use the shared bandwidth.
- The EIP's original dedicated bandwidth will be deleted.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. In the shared bandwidth list, locate the row that contains the shared bandwidth to which you want to add EIPs. In the **Operation** column, choose **More** > **Add EIP**, and select the EIPs to be added.

Figure 6-2 Add EIP



Add EIP

After an EIP is added to a shared bandwidth, the EIP will use the shared bandwidth of shared-bandwidth-test (50 Mbit/s).

Shared Bandwidth **shared-bandwidth-test**

Number of EIPs that can be added to the shared bandwidth: 20
Maximum number of EIPs that can be added to each shared bandwidth: 20 Learn how to increase quota.

All ▾ EIP ▾ Search by Tag

□	EIP	Status	Bandwidth (Mbit/s)	Associated Instance
□	80.158.1.39	Bound	500	elb-yxx
□	80.158.0.185	Bound	50	elb-lbdr
□	80.158.1.16	Bound	5	nat-tang
□	80.158.0.221	Bound	14	nat-bbb
□	80.158.0.130	Bound	5	cce-lb-cc891e50-b8e5-11e9-...

5 ▾ Total Records: 24 < 1 2 3 4 5 >

OK Cancel

6. Click **OK**.

6.4 Removing EIPs from a Shared Bandwidth

Scenarios

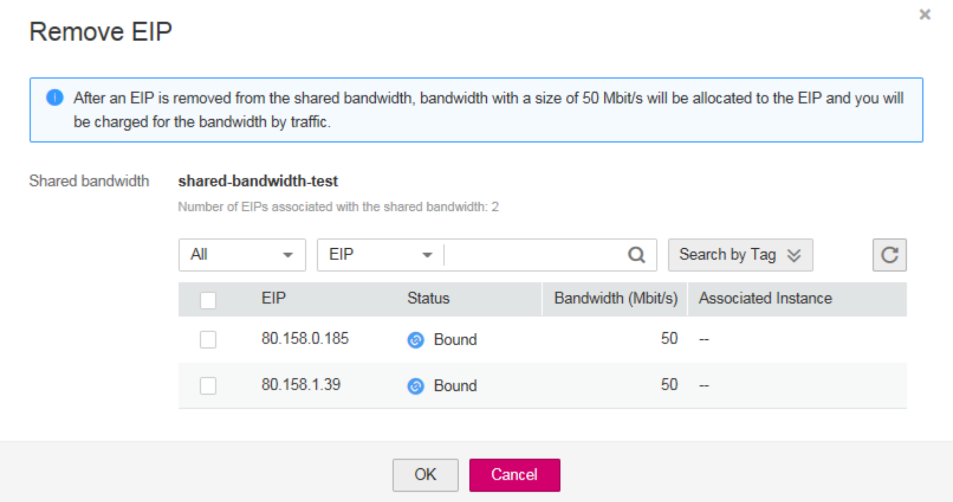
Remove EIPs that are no longer required from a shared bandwidth if needed.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.

5. In the shared bandwidth list, locate the row that contains the bandwidth from which EIPs are to be removed, choose **More** > **Remove EIP** in the **Operation** column, and select the EIPs to be removed in the displayed dialog box.

Figure 6-3 Remove EIP



Remove EIP

After an EIP is removed from the shared bandwidth, bandwidth with a size of 50 Mbit/s will be allocated to the EIP and you will be charged for the bandwidth by traffic.

Shared bandwidth: **shared-bandwidth-test**

Number of EIPs associated with the shared bandwidth: 2

☐	EIP	Status	Bandwidth (Mbit/s)	Associated Instance
☐	80.158.0.185	Bound	50	--
☐	80.158.1.39	Bound	50	--

6. Click **OK**.

6.5 Modifying a Shared Bandwidth

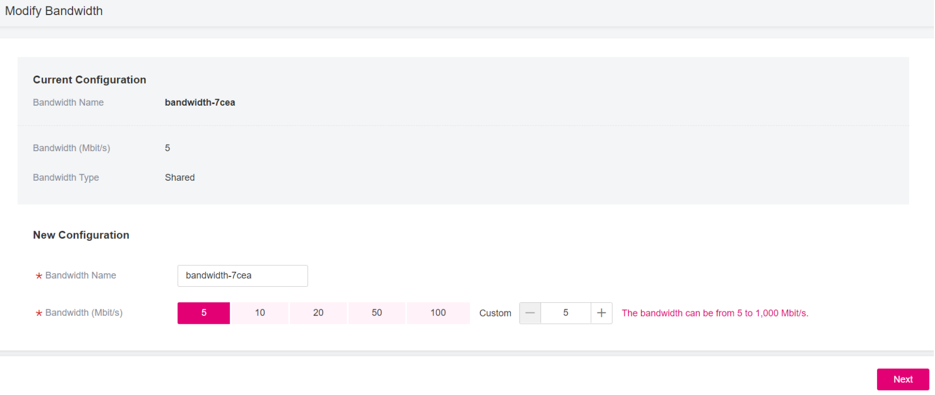
Scenarios

You can modify the name and size of a shared bandwidth, which takes effect immediately.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. 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.

Figure 6-4 Modify Bandwidth



Modify Bandwidth

Current Configuration

Bandwidth Name	bandwidth-7cea
Bandwidth (Mbit/s)	5
Bandwidth Type	Shared

New Configuration

* Bandwidth Name: bandwidth-7cea

* Bandwidth (Mbit/s): 5 | 10 | 20 | 50 | 100 | Custom − 5 + The bandwidth can be from 5 to 1,000 Mbit/s.

6. Click **Next**.
7. Click **Submit**.

6.6 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 select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. 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**.
6. In the displayed dialog box, click **Yes**.

7 Route Table

7.1 Route Table Overview

A custom route is a user-defined routing rule added to a VPC.

The route enables ECSs in a VPC that do not have EIPs bound to access the Internet.

7.2 Configuring an SNAT Server

Scenarios

To use the route table function provided by the VPC service, you need to configure SNAT on an ECS to enable other ECSs that do not have EIPs bound in a 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 the Linux OS.
- The ECS where SNAT is to be configured has only one network interface card (NIC).

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Computing**, click **Elastic Cloud Server**.
4. On the displayed page, locate the target ECS in the ECS list and click the ECS name to switch to the page showing ECS details.
5. On the displayed ECS details page, click the **NICs** tab.

6. Click the NIC IP address. In the displayed area showing the NIC details, disable the source/destination check function.

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

7. Bind an EIP.
   - Bind an EIP with the private IP address of the ECS. For details, see **Assigning an EIP and Binding It to an ECS**.
   - Bind an EIP with the virtual IP address of the ECS. For details, see **Binding a Virtual IP Address to an EIP or ECS**.

8. On the ECS console, use the remote login function to log in to the ECS where you plan to configure SNAT.

9. Run the following command and enter the password of user **root** to switch to user **root**:

   su - root

10. Run the following command to check whether the ECS can successfully connect to the Internet:

    NOTE

    Before running the command, you must disable the response iptables rule on the ECS where SNAT is configured and enable the 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.a.shifen.com (xxx.xxx.xxx.xxx) 56(84) bytes of data.
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=1 ttl=51 time=9.34 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=2 ttl=51 time=9.11 ms
64 bytes from xxx.xxx.xxx.xxx: icmp_seq=3 ttl=51 time=8.99 ms
```

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

    cat /proc/sys/net/ipv4/ip_forward

    In the command output, **1** indicates it is enabled, and **0** indicates it is disabled. The default value is **0**.
    - If IP forwarding in Linux is enabled, go to step **14**.
    - If IP forwarding in Linux is disabled, perform step **12** to enable IP forwarding in Linux.

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

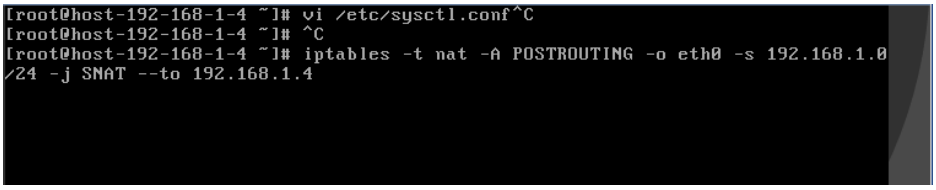
12. Use the vi editor to open the **/etc/sysctl.conf** file, change the value of **net.ipv4.ip_forward** to **1**, and enter **:wq** to save the change and exit.
13. Run the following command to make the change take effect:

    sysctl -p /etc/sysctl.conf
14. Configure SNAT.

    Run the following command to enable all ECSs on the network segment (for example, 192.168.1.0/24) to access the Internet using the SNAT function: Figure 7-1 shows the example command.

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

Figure 7-1 Configuring SNAT



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

NOTE

- To ensure that the rule will not be lost after the restart, write the rule into the **/etc/rc.local** file.
  1. Run the following command to switch to the **/etc/sysctl.conf** file:

     vi /etc/rc.local
  2. Perform **14** to configure SNAT.
  3. Run the following command to save the configuration and exit:

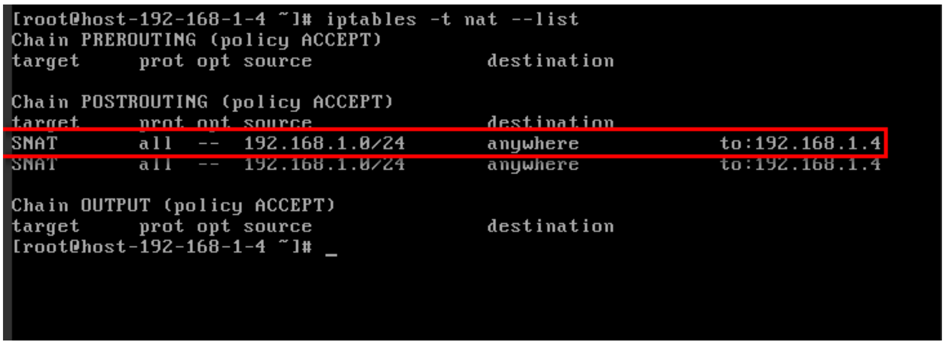
     :wq
  4. Run the following command to add the execute permission for the **rc.local** file:

     # chmod +x /etc/rc.local
- To ensure that the configuration takes effect, run the **iptables -L** command to check whether the configured rules conflict with each other.

15. Run the following command to check whether the operation is successful: If information similar to Figure 7-2 (for example, 192.168.1.0/24) is displayed, the operation was successful.

    iptables -t nat --list

Figure 7-2 Verifying configuration



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

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

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

16. Add a route. For details, see section **Adding a Custom Route**.

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

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

7.3 Adding a Custom Route

Scenarios

When ECSs in a VPC need to access the Internet, add a custom route to enable the ECSs to access the Internet through the ECS that has an EIP bound.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC to which a route is to be added and click the VPC name.
6. On the **Route Tables** tab, click **Add Route**.
7. Set route details on the displayed page.
   - **Destination** indicates the destination CIDR block. The default value is **0.0.0.0/0**. If the traffic originates from a VPC, the destination can be a subnet CIDR block in this VPC. If the traffic originates from outside the VPC, the destination CIDR block cannot conflict with any of the subnet CIDR blocks in this VPC. The destination of each route must be unique.
   - **Next Hop**: indicates the IP address of the next hop. Set it to a private IP address or a virtual IP address in a VPC.

   NOTE

   If the next hop is a virtual IP address, an EIP must be bound to the virtual IP address. Otherwise, access to the Internet through this virtual IP address is not possible. (A custom route is used to forward traffic from the virtual IP address to the Internet.)
8. Click **OK**.

7.4 Viewing a Route Table

Scenarios

You can view details about a route table.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC that is associated with the route table to be queried and click the VPC name.
6. View details about the route table.

7.5 Modifying a Route

Scenarios

Change the destination and next hop of the route.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC to which the route to be modified belongs and click the VPC name.
6. Click the **Route Tables** tab. On the displayed page, locate the row that contains the route to be modified, and click **Modify** in the **Operation** column. Modify the route information in the displayed dialog box.
7. Click **OK**.

7.6 Deleting a Route

Scenarios

Delete a route if it is no longer required.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC that the route to be deleted belongs to and click the VPC name.

6. Click the **Route Tables** tab. On the displayed page, locate the row that contains the route to be deleted, and click **Delete** in the **Operation** column.
7. Click **Yes** in the displayed dialog box.

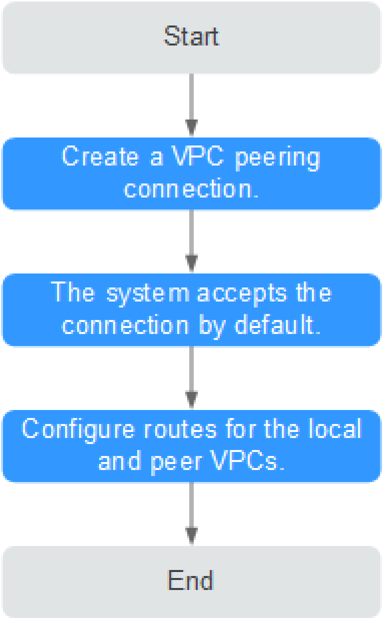
8 VPC Peering Connection

8.1 VPC Peering Connection Creation Procedure

A VPC peering connection is a network connection between two VPCs in one region that enables you to route traffic between them using private IP addresses. ECSs in either VPC can communicate with each other just as if they were in the same region. You can create a VPC peering connection between your own VPCs, or between your VPC and another account's VPC within the same region. However, you cannot create a VPC peering connection between VPCs in different regions.

- Creating a VPC peering connection between VPCs in your account

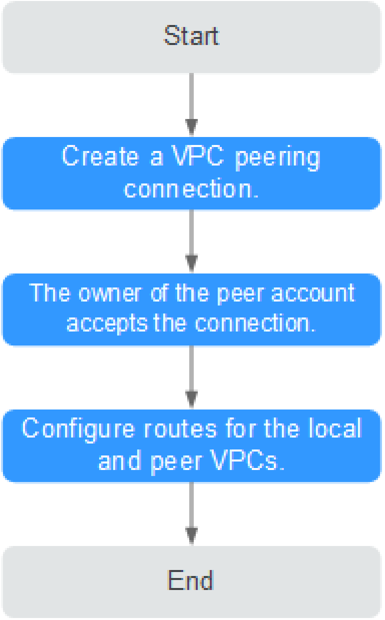
Figure 8-1 Creating a VPC peering connection between VPCs in your account


Start
Create a VPC peering connection.
The system accepts the connection by default.
Configure routes for the local and peer VPCs.
End

If you create a VPC peering connection between two VPCs in your account, the system accepts the connection by default. You need to add routes for the local and peer VPCs to enable communication between the two VPCs.

- Creating a VPC peering connection with a VPC in another account

Figure 8-2 Creating a VPC peering connection with a VPC in another account


Start
Create a VPC peering connection.
The owner of the peer account accepts the connection.
Configure routes for the local and peer VPCs.
End

If you create a VPC peering connection between your VPC and a VPC that is in another account, the VPC peering connection will be in the **Awaiting acceptance** state. After the owner of the peer account accepts the connection, the connection status changes to **Accepted**. The owners of both the local and peer accounts must configure the routes required by the VPC peering connection to enable communication between the two VPCs.

If the local and peer VPCs have overlapping CIDR blocks, the routes added for the VPC peering connection may become invalid. Before creating a VPC peering connection between two VPCs that have overlapping CIDR blocks, ensure that none of the subnets in the two VPCs overlap. If none of the subnets in the two VPCs overlap, the VPC peering connection you created enables communication between subnets in the two VPCs.

You can run the **ping** command to check whether the two VPCs can communicate with each other.

8.2 VPC Peering Connection Configuration Plans

To enable two VPCs to communicate with each other, you can create a VPC peering connection between them. As long as the two VPCs do not overlap, you can configure routes that point to entire VPCs for the VPC peering connection. If the two VPCs have overlapping CIDR blocks, you can only configure routes that point to specific subnets of the VPCs for the VPC peering connection.

- Configurations with Routes to Entire VPCs
  - There can be two or more VPCs peered together using VPC peering connections.
  - Regardless of how many VPCs are connected, if you need to configure routes that point to entire VPCs in a VPC peering connection, none of the

VPCs involved in the connection can have overlapping CIDR blocks. Otherwise, the VPC peering connection will be unable to take effect because the routes will be unreachable.

  – The destination of the route that points to an entire VPC is the CIDR block of the peer VPC, and the next hop is the VPC peering connection ID.

- Configurations with Routes to Specific Subnets

  If VPCs connected by a VPC peering connection have overlapping CIDR blocks, the connection can only enable communication between specific (non-overlapping) subnets in the VPCs. If subnets in the two VPCs of a VPC peering connection have overlapping CIDR blocks, the peering connection will not take effect. When you create a VPC peering connection, ensure that the VPCs involved do not contain overlapping subnets.

  For example, VPC 1 and VPC 2 have matching CIDR blocks, but the subnets in the two VPCs do not overlap. A VPC peering connection can be created between pairs of subnets that do not overlap with each other. The route table is used to control the specific subnets that the VPC peering connection is created for. **Figure 8-3** shows a VPC peering connection created between two subnets. Routes are required to enable communication between Subnet A in VPC 1 and Subnet X in VPC 2 in the figure.

Figure 8-3 VPC peering connection between Subnet A and Subnet X

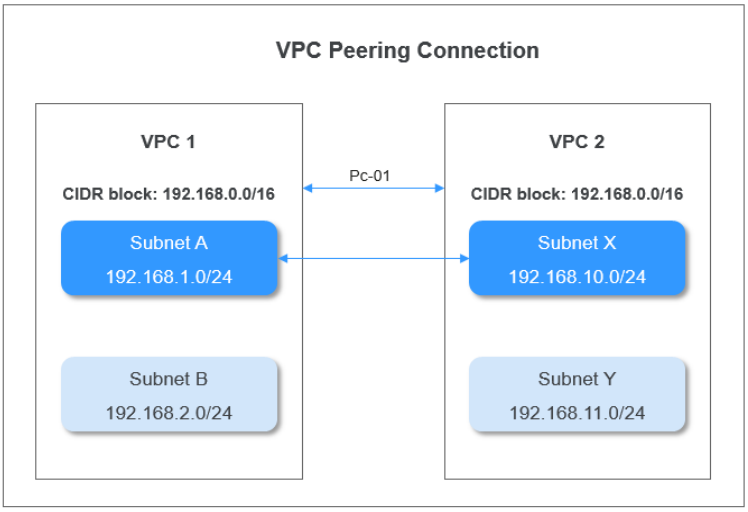
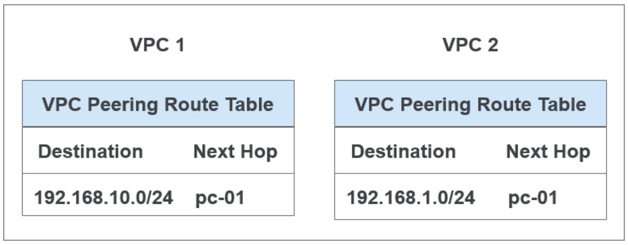


Figure 8-4 shows the routes configured for the VPC peering connection between Subnet A and Subnet X. After the routes are configured, Subnet A and Subnet X can communicate with each other.

Figure 8-4 Route table for the VPC peering connection between Subnet A and Subnet X



VPC 1

VPC Peering Route Table	
Destination	Next Hop
192.168.10.0/24	pc-01

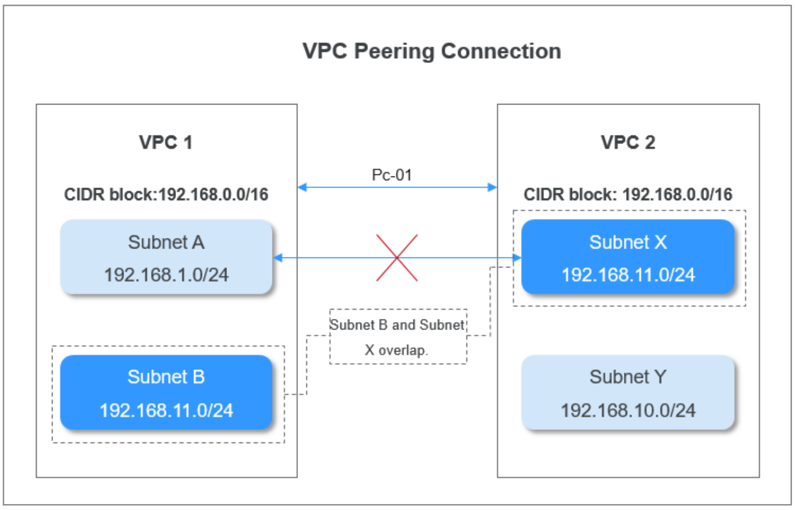
VPC 2

VPC Peering Route Table	
Destination	Next Hop
192.168.1.0/24	pc-01

If two VPCs have overlapping subnets, the VPC peering connection created between the two subnets does not take effect, and the subnets cannot communicate with each other.

As shown in **Figure 8-5**, Subnet B and Subnet X have matching CIDR blocks. Therefore, subnet A preferentially accesses subnet B that is in its same VPC and a VPC peering connection cannot be created between Subnet A and Subnet X.

Figure 8-5 Invalid VPC peering connection



If peering connections are used to link VPC 1 to multiple VPCs, for example, VPC 2, VPC 3, and VPC 4, the subnet CIDR blocks of VPC 1 cannot overlap with those of VPC 2, VPC 3, and VPC 4. If VPC 2, VPC 3, and VPC 4 have overlapping subnets, a VPC peering connection can be created between only one of these overlapping subnets and a subnet of VPC 1. If a VPC peering connection is created between a subnet and the other *N* subnets, none of the subnets can have overlapping CIDR blocks.

8.3 Creating a VPC Peering Connection with Another VPC in Your Account

Scenarios

To create a VPC peering connection, first create a request to peer with another VPC. You can request a VPC peering connection with another VPC in your account, but the two VPCs must be in the same region. The system automatically accepts the request.

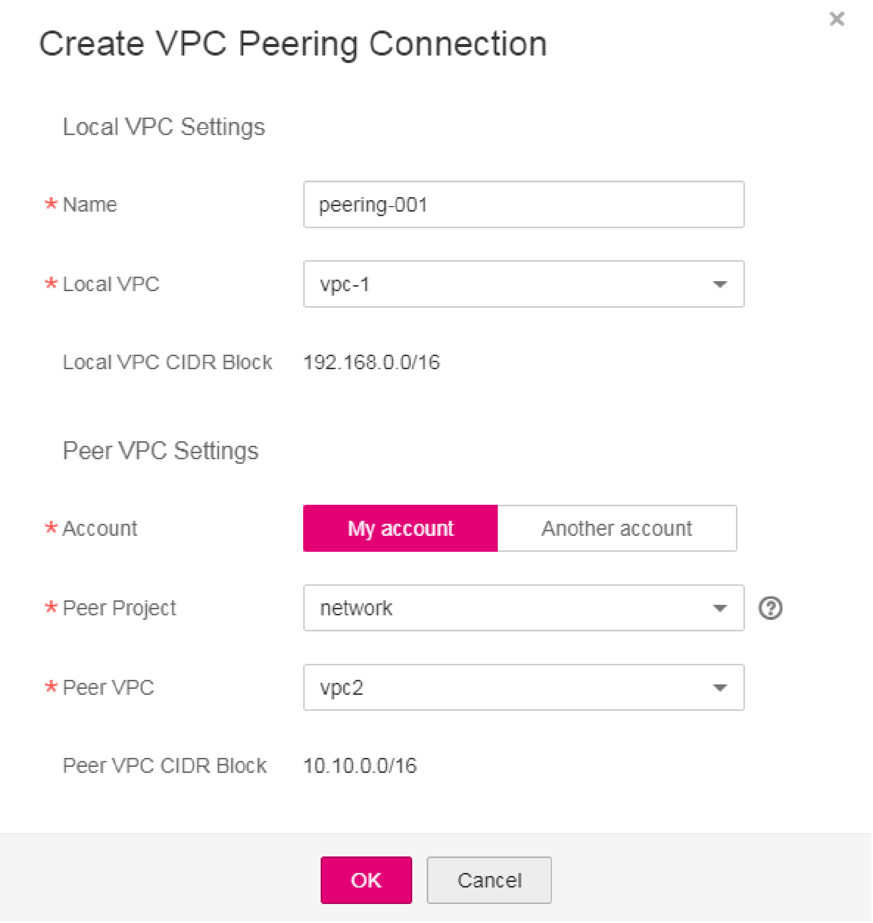
Prerequisites

Two VPCs in the same region have been created.

Creating a VPC Peering Connection

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **VPC Peering**.
5. In the right pane displayed, click **Create VPC Peering Connection**.
6. Configure parameters as prompted. You must select **My account** for **Account**. **Table 8-1** lists the parameters to be configured.

Figure 8-6 Create VPC Peering Connection



Create VPC Peering Connection

Local VPC Settings

* Name: peering-001

* Local VPC: vpc-1

Local VPC CIDR Block: 192.168.0.0/16

Peer VPC Settings

* Account: My account | Another account

* Peer Project: network

* Peer VPC: vpc2

Peer VPC CIDR Block: 10.10.0.0/16

Table 8-1 Parameter descriptions

Parameter	Description	Example Value
Name	The name of the VPC peering connection. The name contains a maximum of 64 characters, which consist of letters, digits, hyphens (-), and underscores (_).	peering-001
Local VPC	The local VPC. You can select one from the drop-down list.	vpc_002
Local VPC CIDR Block	The CIDR block for the local VPC.	192.168.10.0/24

Parameter	Description	Example Value
Account	The account to which the peer VPC belongs. ● **My account**: The VPC peering connection will be created between two VPCs, in the same region, in your account. ● **Another account**: The VPC peering connection will be created between your VPC and a VPC in another account, in the same region.	My account
Peer Project	The peer project name. The project name of the current project is used by default.	aaa
Peer VPC	The peer VPC. You can select one from the drop-down list if the VPC peering connection is created between two VPCs in your own account.	vpc_fab1
Peer VPC CIDR Block	The CIDR block for the peer VPC. The local and peer VPCs cannot have matching or overlapping CIDR blocks. Otherwise, the routes added for the VPC peering connection may not take effect.	192.168.2.0/24

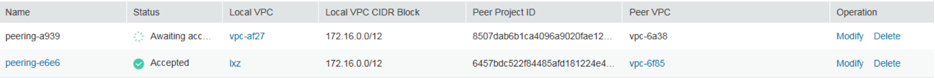
7. Click **OK**.

Adding Routes for a VPC Peering Connection

If you request a VPC peering connection with another VPC in your own account, the system automatically accepts the request. To enable communication between the two VPCs, you need to add local and peer routes for the VPC peering connection.

1. On the console homepage, under **Network**, click **Virtual Private Cloud**.
2. In the navigation pane on the left, click **VPC Peering**.
3. Locate the target VPC peering connection in the connection list.

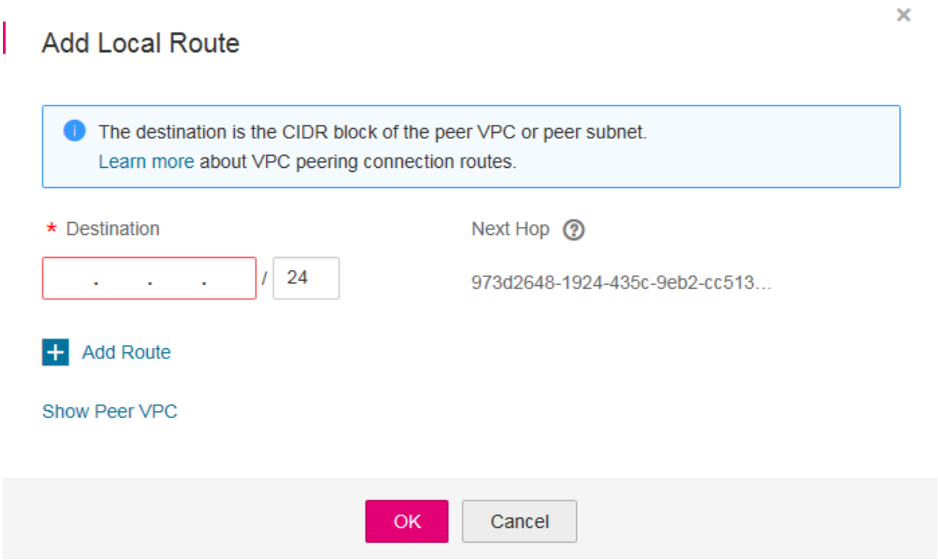
Figure 8-7 VPC peering connection list



Name	Status	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Operation
peering-a939	Awaiting acc...	vpc-af27	172.16.0.0/12	8507dab6b1ca4096a9020fae12...	vpc-6a38	Modify Delete
peering-e6e6	Accepted	lxz	172.16.0.0/12	6457bdc522f84485afd181224e4...	vpc-6f85	Modify Delete

4. Click the name of the VPC peering connection to switch to the page showing details about the connection.
5. On the displayed page, click the **Local Routes** tab.
6. In the displayed **Local Routes** area, click **Add Local Route**. In the displayed dialog box, add a local route. **Table 8-2** lists the parameters to be configured.

Figure 8-8 Add Local Route



Add Local Route

The destination is the CIDR block of the peer VPC or peer subnet.
Learn more about VPC peering connection routes.

* Destination: . . . / 24

Next Hop: 973d2648-1924-435c-9eb2-cc513...

Table 8-2 Route parameter description

Parameter	Description	Example Value
Destination	The destination address. Set it to the peer VPC or subnet CIDR block.	192.168.2.0/24
Next Hop	The next hop address. The default value is the VPC peering connection ID. Keep the default value.	d1a7863b-9d5e-4d27-8eaf-ab14d2a9148b

7. Click **OK** to switch to the page showing the VPC peering connection details.
8. On the displayed page, click the **Peer Routes** tab.
9. In the displayed **Peer Routes** area, click **Add Peer Route** and add a route.
10. Click **OK** to add the route.

After a VPC peering connection is created, the two VPCs can communicate with each other through private IP addresses. You can run the **ping** command to check whether the two VPCs can communicate with each other.

If two VPCs cannot communicate with each other, check the configuration by following the instructions provided in **Why Does Communication Fail Between VPCs That Are Connected by a VPC Peering Connection?**

8.4 Creating a VPC Peering Connection with a VPC in Another Account

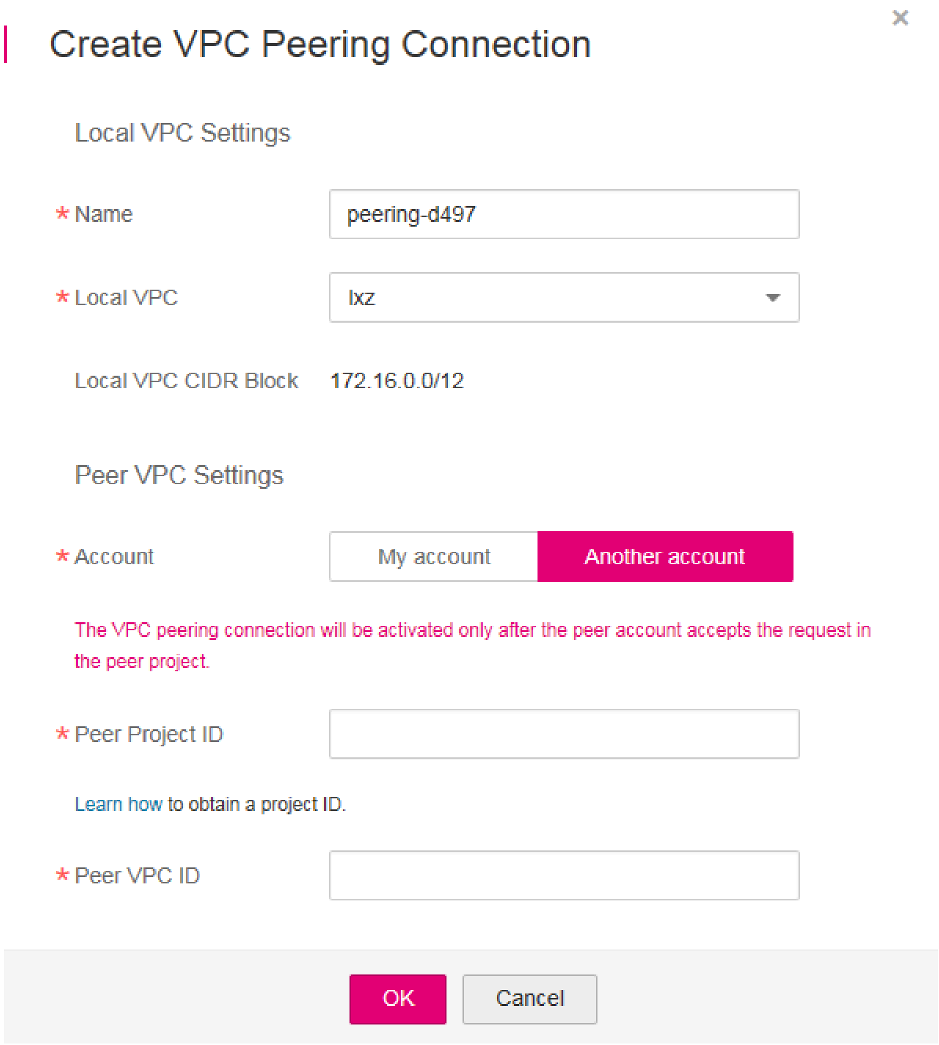
Scenarios

The VPC service also allows you to create a VPC peering connection with a VPC in another account. The two VPCs must be in the same region. If you request a VPC peering connection with a VPC in another account in the same region, the owner of the peer account must accept the request to activate the connection.

Creating a VPC Peering Connection

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **VPC Peering**.
5. In the right pane displayed, click **Create VPC Peering Connection**.
6. Configure parameters as prompted. You must select **Another account** for **Account**.

Figure 8-9 Create VPC Peering Connection



Create VPC Peering Connection

Local VPC Settings

* Name: peering-d497

* Local VPC: lxz

Local VPC CIDR Block: 172.16.0.0/12

Peer VPC Settings

* Account: My account | Another account

The VPC peering connection will be activated only after the peer account accepts the request in the peer project.

* Peer Project ID

Learn how to obtain a project ID.

* Peer VPC ID

Table 8-3 Parameter descriptions

Parameter	Description	Example Value
Name	The name of the VPC peering connection. The name contains a maximum of 64 characters, which consist of letters, digits, hyphens (-), and underscores (_).	peering-001
Local VPC	The local VPC. You can select one from the drop-down list.	vpc_002

Parameter	Description	Example Value
Account	The account to which the VPC to peer with belongs. ● **My account**: The VPC peering connection will be created between two VPCs, in the same region, in your account. ● **Another account**: The VPC peering connection will be created between your VPC and a VPC in another account, in the same region.	Another account
Peer Project ID	This parameter is available only when **Another account** is selected. For details about how to obtain the peer project ID, see **Obtaining the Peer Project ID**.	N/A
Peer VPC ID	This parameter is available only when **Another account** is selected. For details about how to obtain the peer VPC ID, see **Obtaining the Peer VPC ID**.	65d062b3-40fa-4204-8181-3538f527d2ab

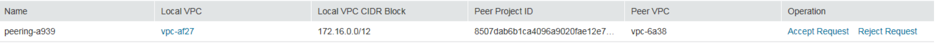
7. Click **OK**.

Accepting a VPC Peering Connection Request

To request a VPC peering connection with a VPC in another account, the owner of the peer account must accept the request to activate the connection.

1. The owner of the peer account logs in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the VPC peering connection list, locate the row that contains the target VPC peering connection and click **Accept Request** in the **Operation** column.

Figure 8-10 VPC peering connection list



Name	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Operation
peering-a939	vpc-af27	172.16.0.0/12	8507dab6b1ca4096a9020fae12e7...	vpc-6a38	Accept Request Reject Request

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

Refusing a VPC Peering Connection

The owner of the peer account can reject any VPC peering connection request that they receive. If a VPC peering connection request is rejected, the connection will not be established. You must delete the rejected VPC peering connection request before creating a VPC peering connection between the same VPCs as those in the rejected request.

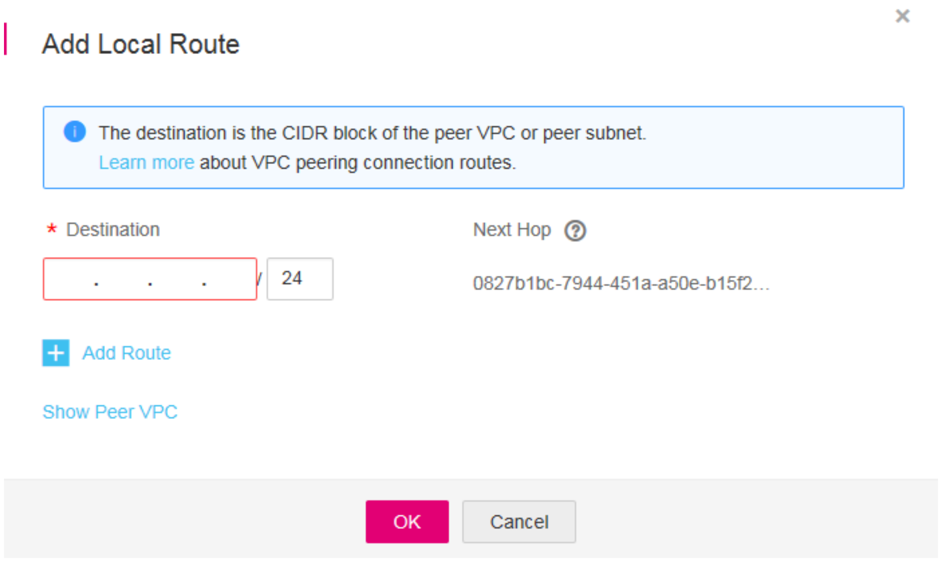
1. The owner of the peer account logs in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **VPC Peering**.
4. In the VPC peering connection list, locate the row that contains the target VPC peering connection and click **Reject Request** in the **Operation** column.
5. Click **Yes** in the displayed dialog box.

Adding Routes for a VPC Peering Connection

If you request a VPC peering connection with a VPC in another account, the owner of the peer account must accept the request. To enable communication between the two VPCs, you need to add routes for the VPC peering connection. The owner of the local account can add only the local route because the owner does not have the required permission to perform operations on the peer VPC. The owner of the peer account must add the peer route. The procedure for adding a local route and a peer route is the same.

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, click **VPC Peering**.
4. Locate the target VPC peering connection in the connection list.
5. Click the name of the VPC peering connection to switch to the page showing details about the connection.
6. On the displayed page, click the **Local Routes** tab.
7. In the displayed **Local Routes** area, click **Add Local Route**. In the displayed dialog box, add a local route.

Figure 8-11 Add Local Route



Add Local Route

The destination is the CIDR block of the peer VPC or peer subnet.
Learn more about VPC peering connection routes.

* Destination: . . . / 24

Next Hop: 0827b1bc-7944-451a-a50e-b15f2...

Table 8-4 Route parameter description

Parameter	Description	Example Value
Destination	The destination address. Set it to the peer VPC or subnet CIDR block.	192.168.2.0/24
Next Hop	The next hop address. The default value is the VPC peering connection ID. Keep the default value.	d1a7863b-9d5e-4d27-8eaf-ab14d2a9148b

8. Click **OK**.

   The routes are added for the VPC peering connection.

After a VPC peering connection is created, the two VPCs can communicate with each other through private IP addresses. You can run the **ping** command to check whether the two VPCs can communicate with each other.

If two VPCs cannot communicate with each other, check the configuration by following the instructions provided in **Why Does Communication Fail Between VPCs That Are Connected by a VPC Peering Connection?**

Obtaining the Peer Project ID

1. The owner of the peer account logs in to the management console.
2. Select **My Credentials** from the username drop-down list.
3. On the **Projects** tab, obtain the required project ID.

Obtaining the Peer VPC ID

1. The owner of the peer account logs in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Virtual Private Cloud**.
4. Click the target VPC name and view VPC ID on the VPC details page.

8.5 Viewing VPC Peering Connections

Scenarios

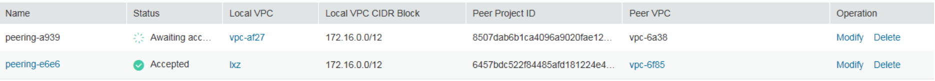
The owners of both the local and peer accounts can view information about the created VPC peering connections and those that are still waiting to be accepted.

Procedure

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

3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **VPC Peering**.
5. In the displayed pane on the right, view information about the VPC peering connections. You can search for specific VPC peering connections by connection status or by name.

Figure 8-12 VPC peering connection list



Name	Status	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Operation
peering-a939	Awaiting acc...	vpc-af27	172.16.0.0/12	8507dab6b1ca4096a9020fae12...	vpc-6a38	Modify Delete
peering-e6e6	✓ Accepted	lxz	172.16.0.0/12	6457bdc522f84485afd181224e4...	vpc-6f85	Modify Delete

6. Click the VPC peering connection name. On the displayed page, view detailed information about the VPC peering connection.

8.6 Modifying a VPC Peering Connection

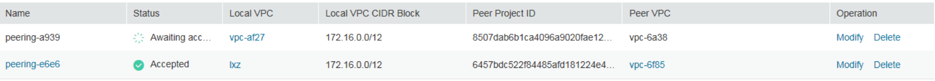
Scenarios

The owners of both the local and peer accounts can modify a VPC peering connection in any state. The VPC peering connection name can be changed.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **VPC Peering**.
5. In the displayed pane on the right, view information about the VPC peering connections. You can search for specific VPC peering connections by connection status or by name.

Figure 8-13 VPC peering connection list



Name	Status	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Operation
peering-a939	Awaiting acc...	vpc-af27	172.16.0.0/12	8507dab6b1ca4096a9020fae12...	vpc-6a38	Modify Delete
peering-e6e6	✓ Accepted	lxz	172.16.0.0/12	6457bdc522f84485afd181224e4...	vpc-6f85	Modify Delete

6. Locate the target VPC peering connection and click **Modify** in the **Operation** column. In the displayed dialog box, modify information about the VPC peering connection.
7. Click **OK**.

8.7 Deleting a VPC Peering Connection

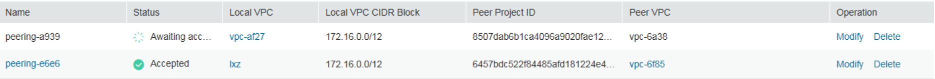
Scenarios

The owners of both the local and peer accounts can delete a VPC peering connection in any state. After a VPC peering connection is deleted, routes configured for the connection will be automatically deleted as well.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **VPC Peering**.
5. In the displayed pane on the right, view information about the VPC peering connections. You can search for specific VPC peering connections by connection status or by name.

Figure 8-14 VPC peering connection list



Name	Status	Local VPC	Local VPC CIDR Block	Peer Project ID	Peer VPC	Operation
peering-a939	Awaiting acc...	vpc-af27	172.16.0.0/12	8507dab6b1ca4096a9020fae12...	vpc-6a38	Modify Delete
peering-e6e6	✓ Accepted	lxz	172.16.0.0/12	6457bdc522f84485afd181224e4...	vpc-6f85	Modify Delete

6. Locate the target VPC peering connection and click **Delete** in the **Operation** column.
7. Click **Yes** in the displayed dialog box.

8.8 Viewing Routes Configured for a VPC Peering Connection

Scenarios

After routes are added for a VPC peering connection, the owners of both the local and peer accounts can view information about the routes on the page showing details about the VPC peering connection.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **VPC Peering**.
5. Locate the target VPC peering connection in the connection list.
6. Click the name of the VPC peering connection to switch to the page showing details about the connection.
7. On the displayed page, click the **Local Routes** tab and view information about the local route added for the VPC peering connection.
8. On the page showing details about the VPC peering connection, click the **Peer Routes** tab and view information about the peer route added for the VPC peering connection.

8.9 Deleting a VPC Peering Route

Scenarios

After routes are added for a VPC peering connection, the owners of both the local and peer accounts can delete the routes on the page showing details about the peering connection .

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **VPC Peering**.
5. Locate the target VPC peering connection in the connection list.
6. Click the name of the VPC peering connection to switch to the page showing details about the connection.
7. On the displayed page, click the **Local Routes** tab and view information about the local route added for the VPC peering connection.
8. On the **Local Routes** page, locate the target local route, and click **Delete** in the **Operation** column.
9. Click **Yes** in the displayed dialog box.
10. On the page showing details about the VPC peering connection, click the **Peer Routes** tab and view information about the peer route added for the VPC peering connection.
11. On the **Peer Routes** page, locate the target peer route, and click **Delete** in the **Operation** column.
12. Click **Yes** in the displayed dialog box.

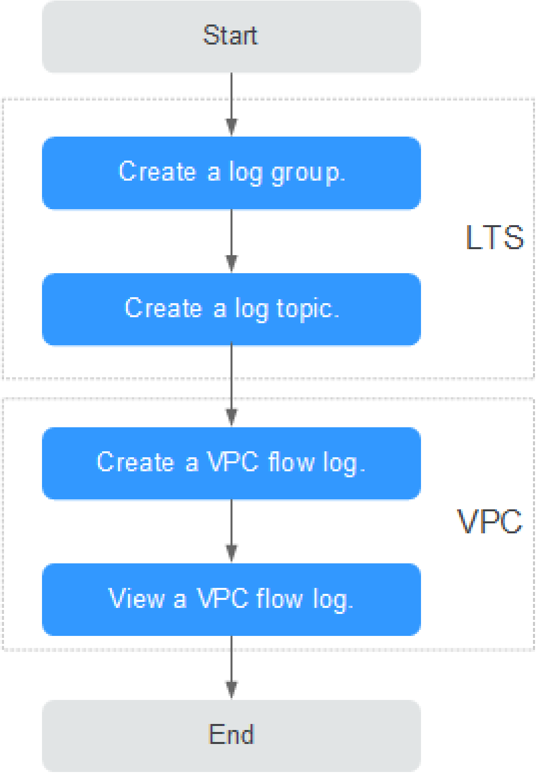
9 VPC Flow Log

9.1 VPC Flow Log Overview

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 firewall 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 topic in LTS. **Figure 9-1** shows the process for configuring the VPC flow log function.

Figure 9-1 Configuring the VPC flow log function



Notes and Constraints

- Currently, only C3, M3, and S2 ECSs support VPC flow logs.
- By default, you can create a maximum of 10 VPC flow logs.
- By default, a maximum of 400,000 flow log records are supported.

9.2 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:

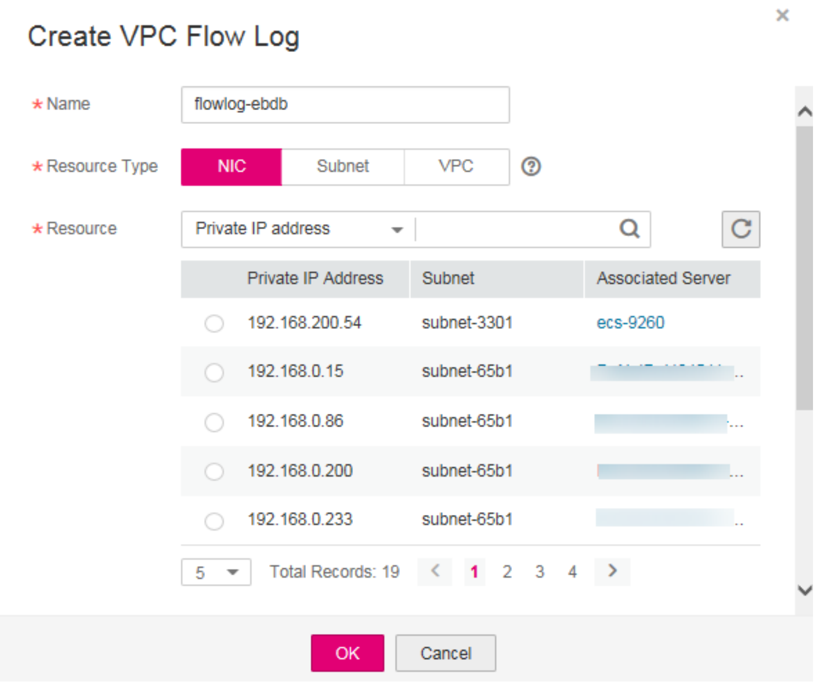
- Create a log group.
- Create a log topic.

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 select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **VPC Flow Logs**.
5. In the upper right corner, click **Create VPC Flow Log**. On the displayed page, configure parameters as prompted.

Figure 9-2 Create VPC Flow Log



Create VPC Flow Log

* Name: flowlog-ebdb

* Resource Type: NIC | Subnet | VPC

* Resource: Private IP address

	Private IP Address	Subnet	Associated Server
○	192.168.200.54	subnet-3301	ecs-9260
○	192.168.0.15	subnet-65b1	[redacted]...
○	192.168.0.86	subnet-65b1	[redacted]...
○	192.168.0.200	subnet-65b1	[redacted]...
○	192.168.0.233	subnet-65b1	[redacted]...

Table 9-1 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	● **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 firewall. ● **Rejected traffic**: specifies that only rejected traffic of the specified resource will be logged. Rejected traffic refers to the traffic denied by the firewall.	All
Log Group	The log group created in LTS.	lts-group-wule
Log Topic	The log topic created in LTS.	LogTopic1
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 topic. Each VPC flow log must be unique.

6. Click **OK**.

9.3 Viewing a VPC Flow Log

Scenarios

View information about your flow log record.

The capture window is approximately 10 minutes, which indicates that a flow log record will be generated every 10 minutes. After creating a VPC flow log, you need to wait about 10 minutes before you can view the flow log record.

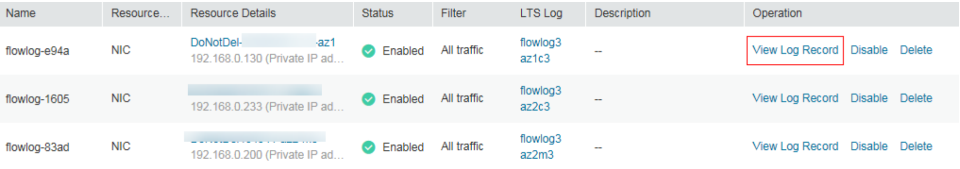
NOTE

If an ECS is in the stopped state, its flow log records will not be displayed.

Procedure

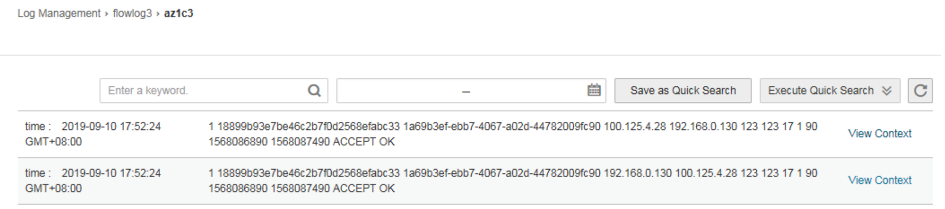
1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **VPC Flow Logs**.
5. Locate the target VPC flow log and click **View Log Record** in the **Operation** column to view information about the flow log record in LTS.

Figure 9-3 Viewing a log record



Name	Resource...	Resource Details	Status	Filter	LTS Log	Description	Operation
flowlog-e94a	NIC	DoNotDel-[redacted]-az1 192.168.0.130 (Private IP ad...	✓ Enabled	All traffic	flowlog3 az1c3	--	View Log Record Disable Delete
flowlog-1605	NIC	[redacted] 192.168.0.233 (Private IP ad...	✓ Enabled	All traffic	flowlog3 az2c3	--	View Log Record Disable Delete
flowlog-83ad	NIC	[redacted] 192.168.0.200 (Private IP ad...	✓ Enabled	All traffic	flowlog3 az2m3	--	View Log Record Disable Delete

Figure 9-4 Flow log record



```
time :   2019-09-10 17:52:24   1 18899b93e7be46c2b7f0d2568efabc33 1a69b3ef-ebb7-4067-a02d-44782009fc90 100.125.4.28 192.168.0.130 123 123 17 1 90
GMT+08:00                      1568086890 1568087490 ACCEPT OK
time :   2019-09-10 17:52:24   1 18899b93e7be46c2b7f0d2568efabc33 1a69b3ef-ebb7-4067-a02d-44782009fc90 192.168.0.130 100.125.4.28 123 123 17 1 90
GMT+08:00                      1568086890 1568087490 ACCEPT OK
```

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 9-2 describes the fields of a flow log record.

Table 9-2 Log field description

Field	Description	Example Value
version	Specifies the VPC flow log version.	1
project-id	Specifies the project ID.	5f67944957444bd6bb4fe3b367de8f3d
interface-id	Specifies the ID of the NIC for which the traffic is recorded.	1d515d18-1b36-47dc-a983-bd6512aed4bd
srcaddr	Specifies the source IP address.	192.168.0.154
dstaddr	Specifies the destination IP address.	192.168.3.25
srcport	Specifies the source port of the traffic.	38929
dstport	Specifies the destination port of the traffic.	53
protocol	Specifies the Internet Assigned Numbers Authority (IANA) protocol number of the traffic. For details, see **Assigned Internet Protocol Numbers**.	17
packets	Specifies the number of packets transferred during the capture window.	1
bytes	Specifies the number of bytes transferred during the capture window.	96

Field	Description	Example Value
start	Specifies the time, in Unix seconds, of the start of the capture window.	1548752136
end	Specifies the time, in Unix seconds, of the end of the capture window.	1548752736
action	Specifies the action associated with the traffic: ● **ACCEPT**: The recorded traffic was allowed by the security groups or firewalls. ● **REJECT**: The recorded traffic was denied by the firewalls.	ACCEPT
log-status	Specifies the logging status of the VPC flow log: ● **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. Example: When **Filter** is set to **Accepted traffic**, if there is accepted traffic, the value of **log-status** is **OK**. If there is no accepted traffic, the value of **log-status** is **NODATA** regardless of whether there is rejected traffic. If some accepted traffic is abnormally skipped, the value of **log-status** is **SKIPDATA**.	OK

You can enter a keyword on the log topic details page on the LTS console to search for flow log records.

9.4 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 traffic data, you can disable the corresponding VPC flow log. The disabled VPC flow log can be enabled again.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **VPC Flow Logs**.
5. Locate the VPC flow log to be enabled or disabled, and click **Enable** or **Disable** in the **Operation** column.
6. Click **Yes**.

9.5 Deleting a VPC Flow Log

Scenarios

Delete a VPC flow log that is not required. Deleting a VPC flow log will not delete the existing flow log records in LTS.

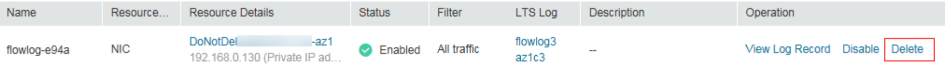
NOTE

If a NIC that uses a VPC flow log is deleted, the flow log will be automatically deleted. However, the flow log records are not deleted.

Procedure

1. Log in to the management console.
2. Click in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **VPC Flow Logs**.
5. Locate the row that contains the VPC flow log to be deleted and click **Delete** in the **Operation** column.

Figure 9-5 Deleting a VPC flow log



Name	Resource...	Resource Details	Status	Filter	LTS Log	Description	Operation
flowlog-e94a	NIC	DoNotDel[redacted]-az1 192.168.0.130 (Private IP ad...	✓ Enabled	All traffic	flowlog3 az1c3	--	View Log Record Disable Delete

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

10 Direct Connect

Direct Connect allows you to establish a dedicated network connection between your data center and the cloud platform. With Direct Connect, you can establish a private connection between the cloud platform and your data center, office, or collocation environment, which can reduce your network latency and provide a more consistent network experience than Internet-based connections.

For more information about Direct Connect, see the *Direct Connect User Guide*.

11 Virtual IP Address

11.1 Virtual IP Address Overview

What Is a Virtual IP Address?

A virtual IP address can be shared among multiple ECSs. An ECS can have both private and virtual IP addresses, and you can access the ECS through either IP address. A virtual IP address has the same network access capabilities as a private IP address, including layer 2 and layer 3 communication in VPCs, access between VPCs using VPC peering connections, as well as access through EIPs, VPN connections, and Direct Connect connections.

A virtual IP address can be bound to multiple ECSs deployed in active/standby mode. You can bind an EIP to the virtual IP address. When the EIP is accessed from the Internet, the virtual IP address has made it possible to either the active or standby ECS, making ECSs highly fault tolerant.

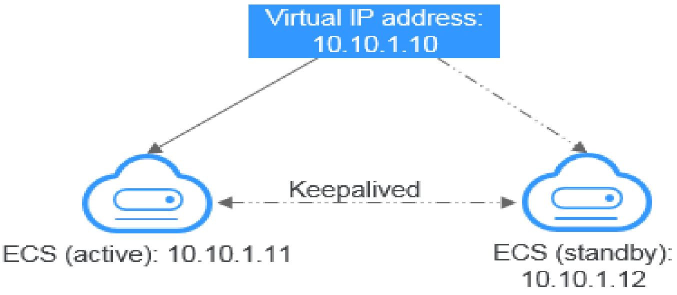
Networking

Virtual IP addresses are used for high availability as they 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

  If you want to improve service availability and avoid single points of failure, you can deploy ECSs in the active/standby mode or deploy one active ECS and multiple standby ECSs. In this arrangement, the ECSs all use the same virtual IP address. If the active ECS becomes faulty, a standby ECS takes over services from the active ECS and services continue uninterrupted.

Figure 11-1 Networking diagram of the HA mode

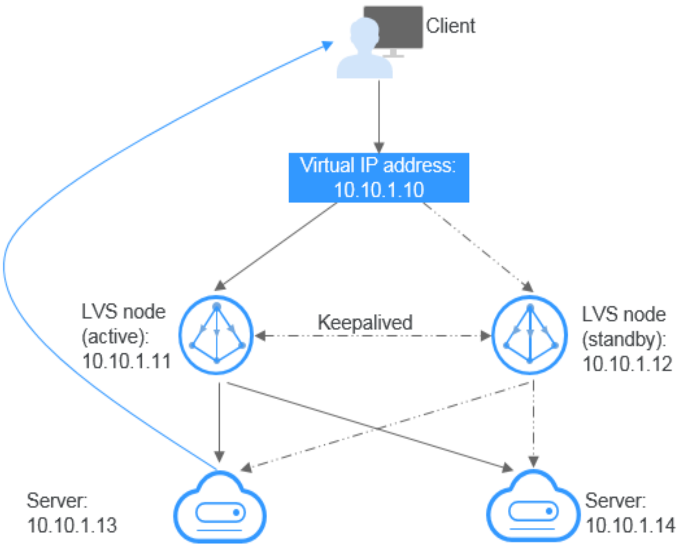


- In this configuration, a single virtual IP address is bound to two ECSs in the same subnet.
- Keepalived is then used to configure the two ECSs to work in the active/standby mode. Follow industry standards for configuring Keepalived. The details are not included here.

- **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 11-2 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 mode. 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 a VPN for security and Direct Connect for a stable connection. 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. It is too easy for there to be route conflicts on the ECS, which would cause communication failure using the virtual IP address.
- IP forwarding must be disabled on the standby ECS. Perform the following operations to confirm whether the IP forwarding is disabled on the standby ECS:

  a. Log in to standby ECS and run the following command to check whether the 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 the command output is **1**, perform **b** and **c** to disable the IP forwarding.
     - If the command output is **0**, no further action is required.

  b. 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. You can also use the **sed** command to modify the configuration. A command example is as follows:

     ```
     sed -i '/net.ipv4.ip_forward/s/1/0/g' /etc/sysctl.conf
     ```

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

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

- The virtual IP address can use only the default security group, which cannot be changed to a custom security group.
- It is recommended that no more than eight virtual IP addresses be bound to an ECS.
- It is recommended that no more than 10 ECSs be bound to a virtual IP address.

11.2 Assigning a Virtual IP Address

Scenarios

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC containing the subnet where a virtual IP address is to be assigned, and click the VPC name.
6. On the **Subnets** tab, click the name of the subnet where a virtual IP address is to be assigned.
7. Click the **Virtual IP Addresses** tab and click **Assign Virtual IP Address**.
8. Select a virtual IP address assignment mode.
   - **Automatic**: The system assigns an IP address automatically.
   - **Manual**: You can specify an IP address.
9. Select **Manual** and enter a virtual IP address.
10. Click **OK**.

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

11.3 Binding a Virtual IP Address to an EIP or ECS

Scenarios

You can bind a virtual IP address to an EIP so that you can access the ECSs can be deployed in active/standby mode for improve fault tolerance.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC containing the virtual IP address and click the VPC name.
6. On the **Subnets** tab, click the name of the subnet that the virtual IP address belongs to.

7. Click the **Virtual IP Addresses** tab, locate the row that contains the virtual IP address to be bound to an EIP or ECS, and choose **Bind to EIP** or **Bind to Server** in the **Operation** column.
8. Select the desired EIP, or ECS and its NIC.

   NOTE

   - If the ECS has multiple NICs, bind the virtual IP address to the primary NIC.
   - Multiple virtual IP addresses can be bound to an ECS NIC.
9. Click **OK**.
10. Manually configure a virtual IP address for an ECS that has been bound with the virtual IP address.

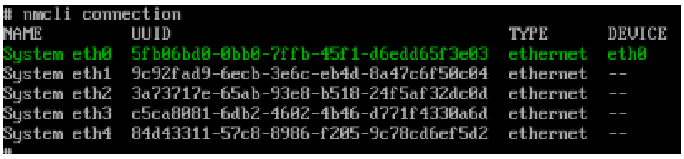
    After a virtual IP address is bound to an ECS NIC, you need to manually configure the virtual IP address on the ECS.

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

    a. Run the following command to check the NIC to which the virtual IP address is to be bound and the NIC connection:

       nmcli connection

       Figure 11-3 Checking the NIC and its connection

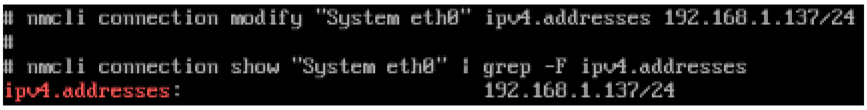
```
# nmcli connection
NAME         UUID                                  TYPE      DEVICE
System eth0  5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03  ethernet  eth0
System eth1  9c92fad9-6ecb-3e6c-eb4d-8a47c6f50c04  ethernet  --
System eth2  3a73717e-65ab-93e8-b518-24f5af32dc0d  ethernet  --
System eth3  c5ca8081-6db2-4602-4b46-d771f4330a6d  ethernet  --
System eth4  84d43311-57c8-8986-f205-9c78cd6ef5d2  ethernet  --
#
```

       In the preceding command output, **eth0** in the **DEVICE** column indicates the NIC to which the virtual IP address is bound, and **System eth0** in the **NAME** column indicates the corresponding connection.

    b. Run the following command to modify the corresponding connection and add the virtual IP address:

       nmcli connection modify "*CONNECTION***" ipv4.addresses** *VIP*

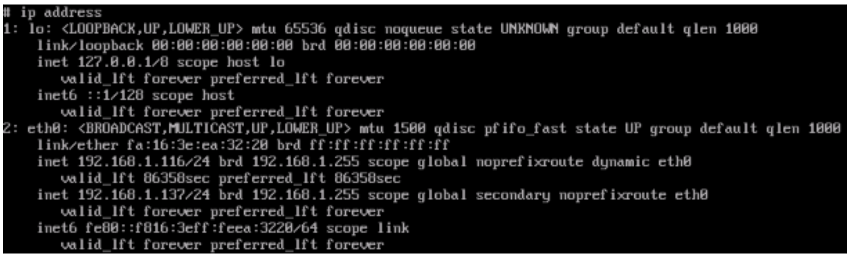
       Figure 11-4 Configuring virtual IP address

```
# nmcli connection modify "System eth0" ipv4.addresses 192.168.1.137/24
#
# nmcli connection show "System eth0" | grep -F ipv4.addresses
ipv4.addresses:                         192.168.1.137/24
```

    c. Restart the ECS and run the **ip address** command to check whether the virtual IP address has been configured.

       Figure 11-5 Checking whether the virtual IP address has been configured

```
# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether fa:16:3e:ea:32:20 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.116/24 brd 192.168.1.255 scope global noprefixroute dynamic eth0
       valid_lft 86358sec preferred_lft 86358sec
    inet 192.168.1.137/24 brd 192.168.1.255 scope global secondary noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:feea:3220/64 scope link
       valid_lft forever preferred_lft forever
```

In the preceding command output, **192.168.1.137** is the virtual IP address.

Windows ECS (Windows 7 is used as an example here.)

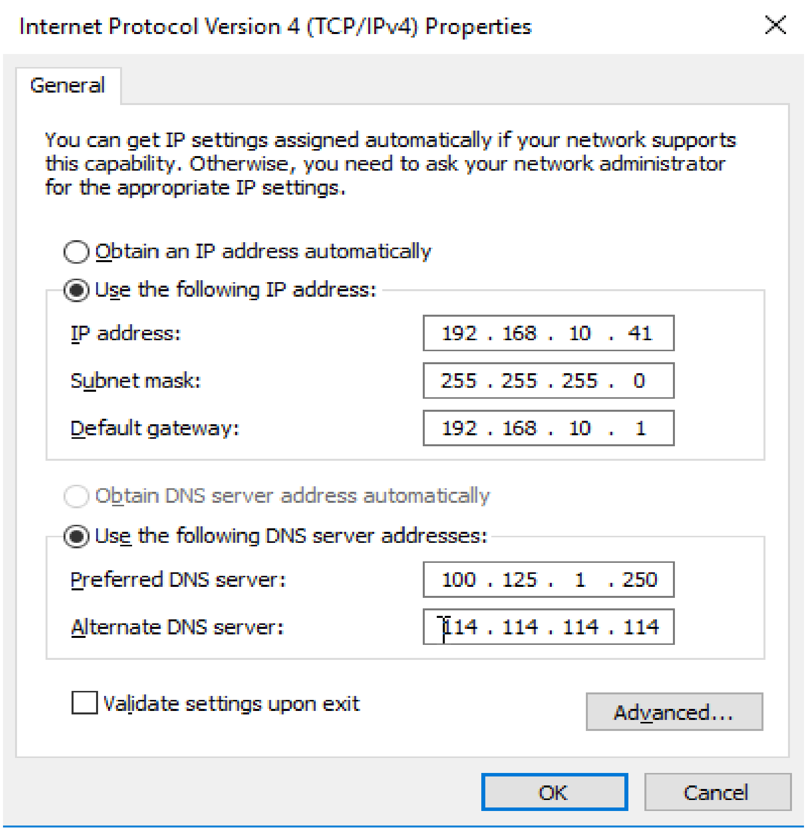
a. Choose **Control Panel** > **Network and Internet** > **Network Connections**. Right-click the corresponding local connection and then click **Properties**.

b. On the **Network** tab page, select **Internet Protocol Version 4 (TCP/IPv4)**.

c. Click **Properties**.

d. Select **Use the following IP address** and set **IP address** to the private IP address of the ECS, for example, 192.168.10.41.

Figure 11-6 Configuring private IP address



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 41

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 10 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 100 . 125 . 1 . 250

Alternate DNS server: 114 . 114 . 114 . 114

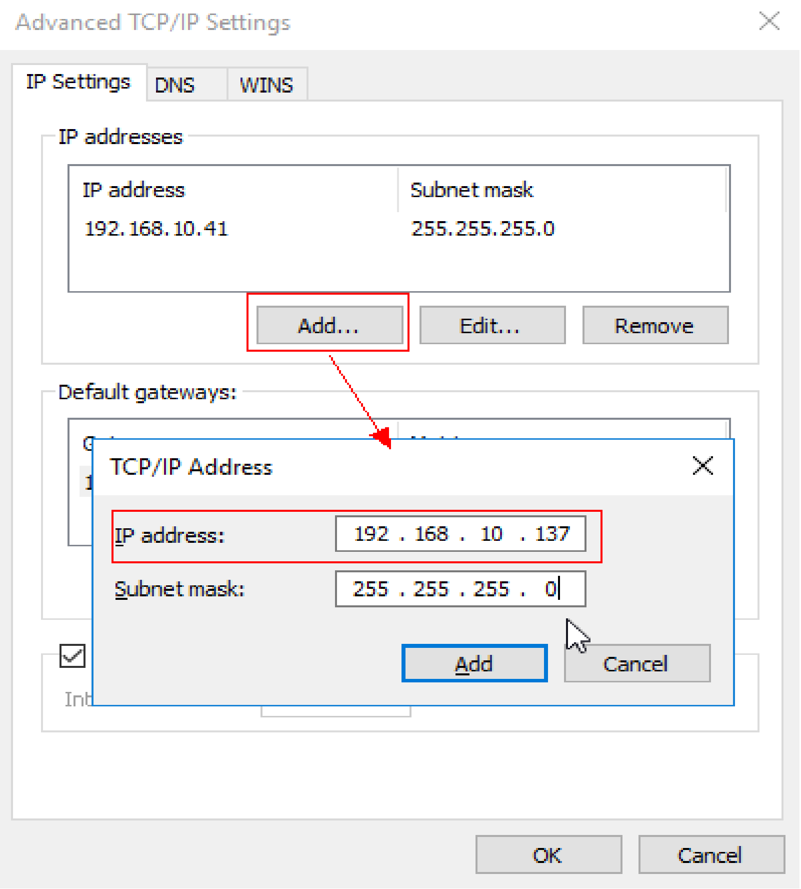
□ Validate settings upon exit

e. Click **Advanced**.

f. On the **IP Settings** tab, click **Add** in the **IP addresses** area.

Add the virtual IP address. For example, 192.168.10.137.

Figure 11-7 Configuring virtual IP address



Advanced TCP/IP Settings

IP addresses

IP address	Subnet mask
192.168.10.41	255.255.255.0

Default gateways:

TCP/IP Address

IP address: 192 . 168 . 10 . 137

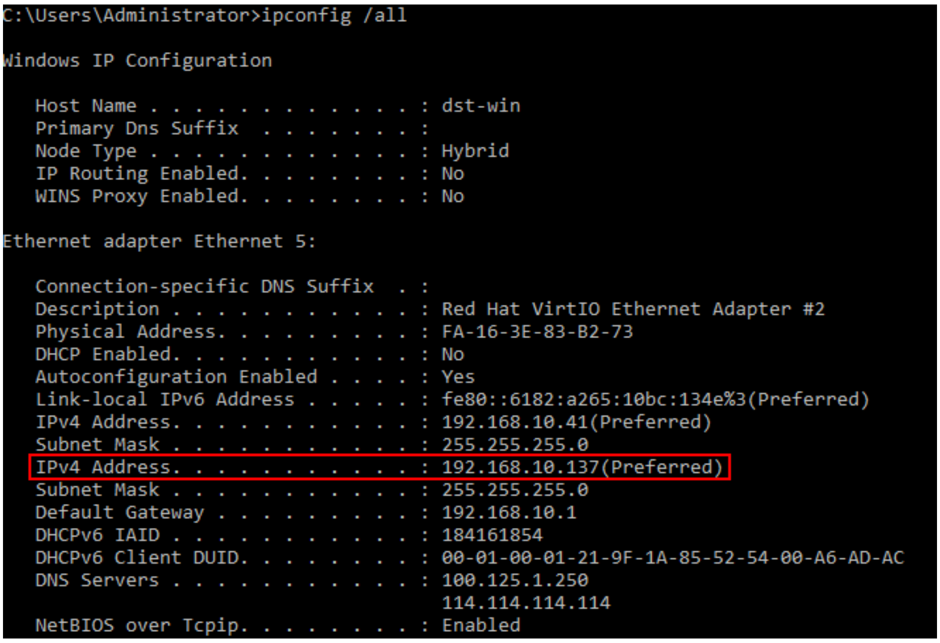
Subnet mask: 255 . 255 . 255 . 0

g. Click **OK**.

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

ipconfig /all

Figure 11-8 Checking whether the virtual IP address has been configured



```
C:\Users\Administrator>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : dst-win
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter Ethernet 5:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Red Hat VirtIO Ethernet Adapter #2
   Physical Address. . . . . . . . . : FA-16-3E-83-B2-73
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::6182:a265:10bc:134e%3(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.41(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   IPv4 Address. . . . . . . . . . . : 192.168.10.137(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.1
   DHCPv6 IAID . . . . . . . . . . . : 184161854
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-21-9F-1A-85-52-54-00-A6-AD-AC
   DNS Servers . . . . . . . . . . . : 100.125.1.250
                                       114.114.114.114
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

In the preceding command output, **IPv4 Address** is the virtual IP address 192.168.10.137, indicating that the virtual IP address of the ECS NIC has been correctly configured.

11.4 Using an EIP to Access a Virtual IP Address

Prerequisites

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

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Elastic IP**.
4. Locate the row that contains the EIP to be bound to the virtual IP address, and click **Bind** in the **Operation** column.
5. Select the target virtual IP address and click **OK**.

11.5 Using a VPN to Access a Virtual IP Address

Procedure

1. Configure the ECS networking based on **Networking**.

2. Create a VPN.

The VPN can be used to access the virtual IP address of the ECS.

11.6 Using a Direct Connect Connection to Access the Virtual IP Address

Procedure

1. Configure the ECS networking based on **Networking**.
2. Create a Direct Connect connection.

The created Direct Connect connection can be used to access the virtual IP address of the ECS.

11.7 Using a VPC Peering Connection to Access the Virtual IP Address

Procedure

1. Configure the ECS networking based on **Networking**.
2. Create a VPC peering connection.

The VPC peering connection can be used to access the virtual IP address of the ECS.

11.8 Disabling Source and Destination Check (HA Load Balancing Cluster Scenario)

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

11.9 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.

Prerequisites

Before deleting a virtual IP address, ensure that the virtual IP address has been unbound from the following resources:

- ECS
- EIP
- CCE cluster

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, click **Virtual Private Cloud**.
5. On the **Virtual Private Cloud** page, locate the VPC containing the subnet from which a virtual IP address is to be released, and click the VPC name.
6. On the **Subnets** tab, click the name of the subnet from which a virtual IP address is to be released.
7. Click the **Virtual IP Addresses** tab, locate the row that contains the virtual IP address to be released, click **More** in the **Operation** column, and select **Release**.
8. Click **Yes** in the displayed dialog box.

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

Metric	Metric Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic Unit: bit/s	≥ 0 bit/s	Object: Bandwidth or EIP Dimension[a]: bandwidth_id, publicip_id	1 minute

Metric	Metric Name	Description	Value Range	Measurement Object & Dimension	Monitoring Interval (Raw Data)
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic Unit: bit/s	≥ 0 bit/s	Object: Bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
up_stream	Outbound Traffic	Network traffic going out of the cloud platform Unit: byte	≥ 0 bytes	Object: Bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute
down_stream	Inbound Traffic	Network traffic going into the cloud platform Unit: byte	≥ 0 bytes	Object: Bandwidth or EIP Dimension: bandwidth_id, publicip_id	1 minute

a: If a service 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"

  }

  ],

Dimensions

Key	Value
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

12.2 Viewing Metrics

Scenarios

View related metrics to see bandwidth and EIP usage information.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Management & Deployment**, click **Cloud Eye**.
4. Click **Cloud Service Monitoring** on the left of the page, and choose **Elastic IP and Bandwidth**.
5. 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.

   You can view data during the last one, three, or twelve hours.

12.3 Creating an Alarm Rule

Scenarios

You can configure alarm rules to customize the monitored objects and notification policies. You can learn your resource statuses at any time.

Procedure

1. Log in to the management console.
2. Click 📍 in the upper left corner and select the desired region and project.
3. On the console homepage, under **Management & Deployment**, click **Cloud Eye**.
4. In the left navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
5. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters to create an alarm rule, or modify an existing alarm rule.

6. After the parameters are set, click **Create**.

   After the alarm rule is created, the system automatically notifies you if an alarm is triggered for the VPC service.

   NOTE

   For more information about VPC alarm rules, see the *Cloud Eye User Guide*.

13 FAQs

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 increase in quota if an 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?

The system does not support online quota adjustment. If you need to adjust a quota, call the hotline or send an email to the customer service mailbox. Customer service personnel will timely process your request for quota adjustment and inform you of the real-time progress by making a call or sending an email.

Before dialing the hotline number or sending an email, make sure that the following information has been obtained:

- Domain name, project name, and project ID, which can be obtained by performing the following operations:

  Log in to the management console using the cloud account, click the username in the upper right corner, select **My Credentials** from the drop-down list, and obtain the domain name, project name, and project ID on the **My Credentials** page.
- Quota information, which includes:
  - Service name
  - Quota type
  - Required quota

Learn how to obtain the service hotline and email address.

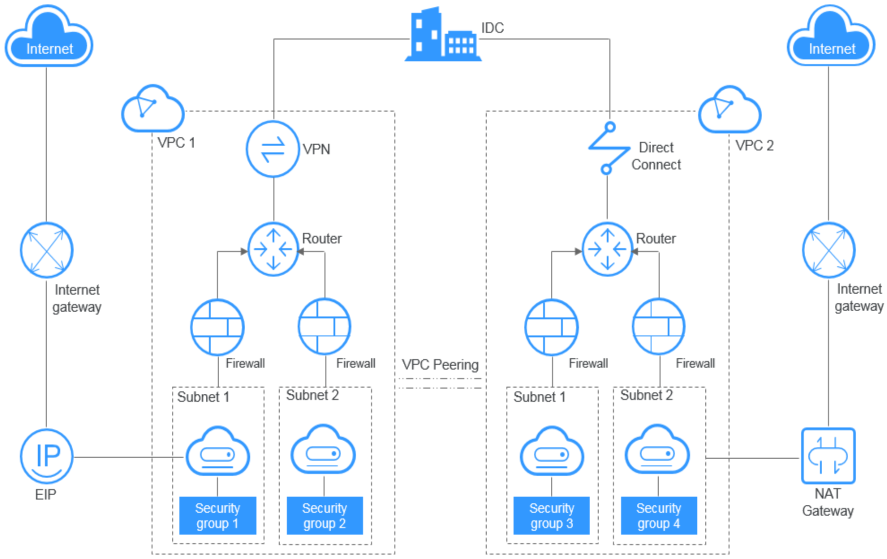
13.2 VPC and Subnet

13.2.1 What Is Virtual Private Cloud?

The Virtual Private Cloud (VPC) service enables you to provision logically isolated, configurable, and manageable virtual networks for Elastic Cloud Servers (ECSs), improving cloud resource security and simplifying network deployment.

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 for communication between ECSs in the same security group or in different security groups.

Figure 13-1 VPC components



13.2.2 Which CIDR Blocks Are Available for the VPC Service?

The VPC service supports the following CIDR blocks:

- 10.0.0.0/8-24
- 172.16.0.0/12-24
- 192.168.0.0/16-24

13.2.3 Can Subnets Communicate with Each Other?

Subnets in the same VPC can communicate with each other while subnets in different VPCs cannot communicate with each other by default. However, you can create VPC peering connections to enable subnets in different VPCs to communicate with each other.

NOTE

If a subnet is associated with a network ACL, configure network ACL rules to allow communication between subnets.

13.2.4 What Subnet CIDR Blocks Are Available?

A subnet CIDR block must be included in its VPC CIDR block. Supported VPC CIDR blocks are **10.0.0.0/8–24**, **172.16.0.0/12–24**, and **192.168.0.0/16–24**. The allowed block size of a subnet is between the netmask of its VPC CIDR block and the /29 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 How Can I Delete a Subnet That Is Being Used by Other Resources?

The VPC service allows you to create private, isolated virtual networks. In a VPC, you can manage private IP address ranges, subnets, route tables, and gateways. ECSs, BMSs, databases, and some other applications can use subnets created in VPCs.

A subnet cannot be deleted if it is being used by other resources. You must delete all resources in the subnet before you can delete the subnet.

You can view all resources of your account on the console homepage and check the resources that are in the subnet you want to delete.

The resources may include:

- ECS
- BMS
- CCE cluster
- RDS instance
- MRS cluster
- DCS instance
- Load balancer

- VPN
- Private IP address
- Custom route
- NAT gateway

13.2.7 What Are the Differences Between the Network ID and Subnet ID of a Subnet?

- The network ID of the subnet is the **neutron_network_id** in the **subnet** fields in **Subnet** > **Creating a Subnet** in the *Virtual Private Cloud API Reference*.

  Parameter **neutron_network_id** indicates the network ID (native OpenStack API). This uniquely identifies a subnet on the management console.
- The subnet ID of the subnet is the **neutron_subnet_id** in the **subnet** fields in **Subnet** > **Creating a Subnet** in the *Virtual Private Cloud API Reference*.

  Parameter **neutron_subnet_id** indicates the subnet ID (native OpenStack API).

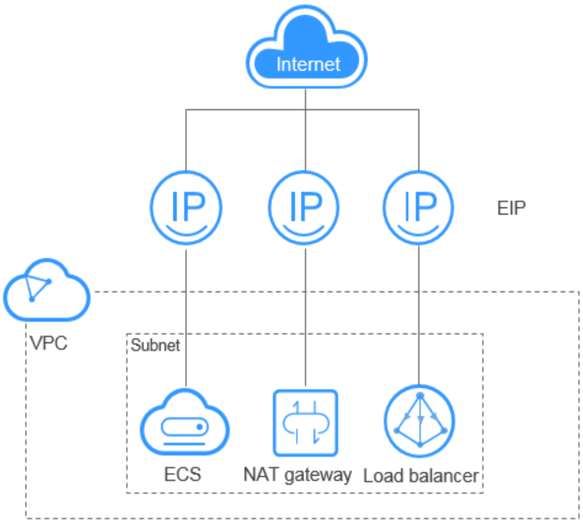
13.3 EIP

13.3.1 What Are EIPs?

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 13-2 Accessing the Internet using an EIP



13.3.2 Can I Bind an EIP to Multiple ECSs?

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

13.3.3 How Do I Access an ECS from the Internet After an EIP Is Bound to the ECS?

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. 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 the ECS needs to be accessible over the Internet and the IP address used to access the ECS over the Internet has been configured on the ECS, or the ECS does not need to be accessible over the Internet, set **Source** to the IP address range containing the IP address that is allowed to access the ECS over the Internet.
- If the ECS needs to be accessible over the Internet and the IP address used to access the ECS over the Internet has not been configured on the ECS, it is recommended that you retain the default setting **0.0.0.0/0** for **Source**, and then set allowed ports to improve network security.
- Allocate ECSs that have different Internet access policies to different security groups.

NOTE

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

13.4 Bandwidth

13.4.1 What Is the Bandwidth Size Range?

The bandwidth ranges from 1 Mbit/s to 1000 Mbit/s.

13.4.2 What Bandwidth Types Are Available?

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

13.4.3 What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth? Can a Dedicated Bandwidth Be Changed to a Shared Bandwidth or the Other Way Around?

Dedicated bandwidth: The bandwidth can only be used by one EIP and the EIP can only be used by one cloud resource, such as an ECS, a NAT gateway, or a load balancer.

Shared bandwidth: The bandwidth can be shared by multiple EIPs. Adding an EIP to or removing an EIP from a shared bandwidth does not affect your workloads.

A dedicated bandwidth cannot be changed to a shared bandwidth or the other way around. You can purchase a shared bandwidth for your EIPs.

- After you add an EIP to a shared bandwidth, the EIP will use the shared bandwidth.
- After you remove an EIP from a shared bandwidth, the EIP will use the dedicated bandwidth.

13.5 Connectivity

13.5.1 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.

13.5.2 Why Is 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 internal 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, click **Virtual Private Cloud**.
4. On the **Virtual Private Cloud** page, locate the VPC for which a subnet is to be modified and click the VPC name.

5. In the subnet list, locate the row that contains the subnet to be modified, click **Modify**. On the displayed page, change the DNS server address as prompted.
6. Click **OK**.

13.5.3 What Are the Constraints Related to VPC Peering?

- VPC peering connections created between VPCs that have overlapping subnet CIDR blocks may not take effect.
- You cannot have more than one VPC peering connection between any two VPCs at the same time.
- You cannot create a VPC peering connection between VPCs in different regions.
- You cannot use the EIPs in a VPC of a VPC peering connection to access resources in the other VPC. For example, VPC A is peered with VPC B, and VPC B has EIPs that can be used to access the Internet, you cannot use EIPs in VPC B to access the Internet from VPC A.
- If you request a VPC peering connection with a VPC of another account, the peer account must accept the request to activate the connection. If you request a VPC peering connection with a VPC of your own, the system automatically accepts the request and activates the connection.
- After a VPC peering connection is established, the local and peer tenants must add routes in the local and peer VPCs to enable communication between the two VPCs.
- VPC A is peered with both VPC B and VPC C. If VPC B and VPC C have overlapping CIDR blocks, you cannot configure routes with the same destinations for VPC A.
- To ensure security, do not accept VPC peering connections from unknown accounts.
- Either owner of a VPC in a peering connection can delete the VPC peering connection at any time. If a VPC peering connection is deleted by one of its owners, all information about this connection will also be deleted immediately, including routes added for the VPC peering connection.
- If VPCs connected by a VPC peering connection have overlapping CIDR blocks, the connection can only enable communication between specific (non-overlapping) subnets in the VPCs. If subnets in the two VPCs of a VPC peering connection have overlapping CIDR blocks, the peering connection will not take effect. When you create a VPC peering connection, ensure that the VPCs involved do not contain overlapping subnets.
- You cannot delete a VPC that has VPC peering connection routes configured.

13.5.4 Why Does Communication Fail Between VPCs That Are Connected by a VPC Peering Connection?

1. Check whether a VPC peering connection has been successfully created for the two VPCs, especially, whether the VPC IDs are correctly configured.
2. Check whether routes that point to the CIDR block (or portion of the CIDR block) of the other VPC have been configured.
3. Check whether routes configured for the VPC peering connection are correct. If VPCs in a VPC peering connections have overlapping CIDR blocks, you can

only add routes to enable communication between two subnets in the two VPCs.

4. Check whether the VPCs in the VPC peering connection contain overlapping subnets.
5. Check whether required security group rules have been configured for the ECSs that need to communicate with each other and whether restriction rules have been added to the iptables or firewall used by the ECSs.
6. If a message indicating that this route already exists is displayed when you add a route for a VPC peering connection, check whether the destination of a VPN, Direct Connect, or VPC peering connection route already exists.
7. If the route destination of the VPC peering connection overlaps with that of a Direct Connect or VPN connection, the route may be invalid.
8. If VPCs in a VPC peering connection cannot communicate with each other after all these possible faults have been rectified, contact customer service.

13.5.5 How Many VPC Peering Connections Can I Create?

You can create a maximum of 50 VPC peering connections in one region. Accepted VPC peering connections consume the quota of both the owners of a VPC peering connection. A VPC peering connection in the pending approval state consumes the quota of only the requester.

13.5.6 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. That is, if both are configured for an ECS to enable Internet access, the EIP will be used preferentially.

13.5.7 What Are the Priorities of the Shared SNAT and Custom Route If Both Are Configured for an ECS to Enable the ECS to Access the Internet?

The priority of a custom route is higher than that of shared SNAT.

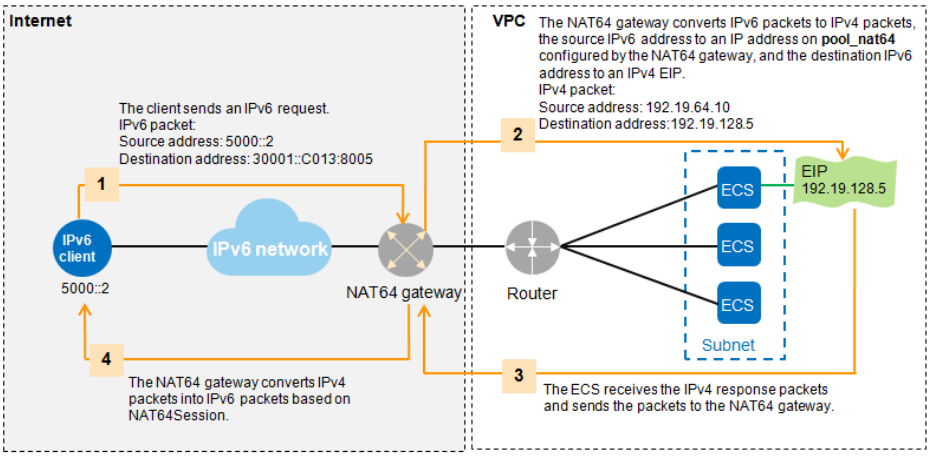
13.5.8 How Does an IPv6 Client on the Internet Access the ECS That Has an EIP Bound in a VPC?

Users with IPv6 clients can call APIs to assign IPv6 EIPs and bind the EIPs to ECSs. Then, the users can use the EIP to access the ECSs in the VPC over the Internet.

For details, see **Floating IP Address (IPv6)** > **Creating a Floating IP Address** in the ***Virtual Private Cloud API Reference***. The NAT64 gateway in the data center will convert the IPv6 EIP to the IPv4 address. (The last 32 bits of the obtained IPv6 EIP is the IPv4 EIP.)

After users who use IPv6 clients bind an IPv6 EIP to an ECS, the data flow is shown in **Figure 13-3**.

Figure 13-3 IPv6 data flow



The client sends an IPv6 request.
IPv6 packet:
Source address: 5000::2
Destination address: 30001::C013:8005

The NAT64 gateway converts IPv6 packets to IPv4 packets, the source IPv6 address to an IP address on **pool_nat64** configured by the NAT64 gateway, and the destination IPv6 address to an IPv4 EIP.
IPv4 packet:
Source address: 192.19.64.10
Destination address:192.19.128.5

The ECS receives the IPv4 response packets and sends the packets to the NAT64 gateway.

The NAT64 gateway converts IPv4 packets into IPv6 packets based on NAT64Session.

The IPv6 service has the following restrictions:

- ECSs use IPv4 addresses and cannot directly access public IPv6 addresses. Therefore, only public IPv6 addresses can access ECSs. That means ECSs cannot use IPv4 EIPs that are converted from IPv6 address to access the Internet. To enable the ECSs to access the Internet, you must bind IPv4 EIPs to them.
- Data packets from an IPv6 network on the Internet are converted to IPv4 packets on the NAT64 gateway. Both the source IP address and port number will be converted. (The source IP address is invisible.)
- The IPv6 client can access only the EIP and the ELB service.
- Only one EIP (IPv6 or IPv4) can be bound to each NIC.
- You can only make API calls to use an EIP to obtain the IPv6 address. The management console displays only IPv4 addresses.
- The security group function does not apply to IPv6 clients.
- Resources in internal networks of the public cloud can access IPv4 addresses converted by NAT64 gateway.
- The public cloud does not provide IP spoofing protection for IPv6 traffic from the Internet.
- Currently, the Anti-DDoS service does not protect IPv6 addresses.

13.6 Routing

13.6.1 How Many Routes Can a Route Table Contain?

Currently, a route table can contain 100 routes.

13.6.2 Are There Any Restrictions on Using a Route Table?

- The ECS providing SNAT must have the **Unbind IP from MAC** function 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.

13.6.3 Will a Route Table Be Billed?

The route table function itself is free of charge. However, you are charged for the ECSs and bandwidth that you use together with the route table function.

13.6.4 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. Therefore, there are different routing priorities for them.

13.6.5 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.

13.6.6 How Many Routes Can Be Added in a VPC?

By default, a maximum of 100 routes can be added for a VPC. The routes include those added for Direct Connect connections, custom routes, and VPC peering connections.

13.7 Security

13.7.1 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.

13.7.2 How Many Security Groups Can I Have?

Each account can have a maximum of 100 security groups and 5000 security group rules.

When you create an ECS, you can select multiple security groups. It is recommended that you select no more than five security groups.

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

ECS Configuration

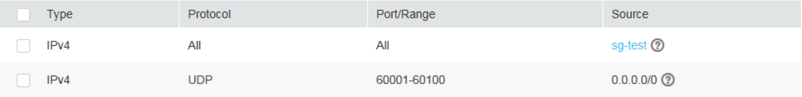
The TFTP daemon determines whether the configuration file specifies the port range. If you use the TFTP configuration file that allows the data channel ports to be configurable, it is a good practice to configure a small range of ports that are not listened on.

Security Group Configuration

You can configure port 69 and configure the 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. Therefore, you can configure a small range of ports for the TFTP daemon.

The following figure provides an example of the security group rule configuration if the ports used by data channels range from 60001 to 60100.

Figure 13-4 Security group rules



□ Type	Protocol	Port/Range	Source
□ IPv4	All	All	sg-test ⓘ
□ IPv4	UDP	60001-60100	0.0.0.0/0 ⓘ

13.7.4 How Many Firewalls Can I Create?

You can create a maximum of 200 firewalls. It is recommended that you configure a maximum of 20 inbound or outbound rules for each firewall. If you configure more than 20 inbound or outbound rules for a firewall, the forwarding performance will deteriorate.

13.7.5 Does a Security Group Rule or a Firewall Rule Immediately Take Effect for Its Original Traffic After It Is Modified?

- Security groups are stateful. Responses to outbound traffic are allowed to go in to the instance regardless of inbound security group rules, and vice versa. Security groups use connection tracking to track traffic information about traffic to and from instances. If a security group rule is added, deleted, or modified, or an instance in the security group is created or deleted, the connection tracking of all instances in the security group will be automatically cleared. In this case, the inbound or outbound traffic of the instance will be considered as new connections, which need to match the inbound or outbound security group rules to ensure that the rules take effect immediately and the security of incoming traffic.
- A modified firewall rule will not immediately take effect for its original traffic. It takes about 120 seconds for the new rule to take effect, and traffic will be interrupted during this period. To ensure that the traffic is immediately interrupted after the rule is changed, it is recommended that you configure security group rules.

13.7.6 Which Security Group Rule Has Priority When Multiple Security Group Rules Conflict?

Security group rules use the whitelist mechanism. If multiple security group rules conflict, the rules are aggregated to take effect.

A Change History

Release Date	What's New
2021-06-18	Modified the following content: - Updated screenshots and deleted the **Bandwidth Type** parameter in **Step 3: Assign an EIP and Bind It to an ECS** and **Assigning an EIP and Binding It to an ECS**. - Updated screenshots in **Assigning a Shared Bandwidth** and **Modifying a Shared Bandwidth**.
2021-05-10	Added the following content: - Added description about the default domain name of an EIP in section **Assigning an EIP and Binding It to an ECS**. - Added description about modifying a dedicated bandwidth or shared bandwidth in section **Modifying an EIP Bandwidth**.
2021-03-16	Added the following FAQs: - **What Bandwidth Types Are Available?** - **What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth? Can a Dedicated Bandwidth Be Changed to a Shared Bandwidth or the Other Way Around?**

Release Date	What's New
2020-12-16	Modified the following content: ● Modified the steps in section **Changing the Security Group of an ECS**. ● Added description about enabling ports 465 and 587 for Mail BGP EIPs in section **Assigning an EIP and Binding It to an ECS**. ● Deleted the restriction on the number of ECS NICs for SNAT in section **Are There Any Restrictions on Using a Route Table?** ● Added the procedure for binding a virtual IP address to an ECS in section **Binding a Virtual IP Address to an EIP or ECS**. ● Modified phrases to or added phrase **Notes and Constraints**. ● Changed the maximum number of tags that can be added to 20 in sections **Managing VPC Tags** and **Managing Subnet Tags**.
2020-06-30	Added the following content: Added basic information to **Security Group Overview** and **Firewall Overview**. Modified the following content: ● Added rules in **Denying Access from a Specific Port**. ● Modified **Does a Security Group Rule or a Firewall Rule Immediately Take Effect for Its Original Traffic After It Is Modified?** ● Modified **How Can I Delete a Subnet That Is Being Used by Other Resources?**
2020-03-20	This release incorporates the following changes: Added parameter **Type** in sections **Step 3: Assign an EIP and Bind It to an ECS** and **Assigning an EIP and Binding It to an ECS**.
2020-02-25	Added the following content: Added section **Shared Bandwidth**. Modified the following content: Modified the steps in section **EIP**.
2020-02-12	Added the following content: Added description that VPC flow logs support S2 ECSs in section **VPC Flow Log Overview**.

Release Date	What's New
2020-01-08	Added the following content: ● Added function and namespace description and optimized information in tables in **Supported Metrics**. ● Added section **Region and AZ**. ● Added the example of allowing external access to a specified port in the section **Security Group Configuration Examples**. Modified the following content: ● Added **Subnet** and **VPC** as the type of resources whose traffic is to be logged in **VPC Flow Log** . ● Updated screenshots in **Adding a Security Group Rule** and **Fast-Adding Security Group Rules**. ● Optimized figure examples in this document. ● Optimized descriptions in section **Firewall Configuration Examples**. ● Optimized descriptions in section **Default Firewall Rules**. ● Changed the position of section **Security**. ● Optimized **What Is a Quota?** Deleted the following content: ● Deleted section "Deleting a VPN".
2019-09-10	Added the following content: ● Added section **VPC Flow Log** . Deleted the following content: ● Deleted the concepts of VPN, IPsec VPN, remote gateway, remote subnet, region, and project in section **Basic Concepts**. ● Deleted the FAQs related to VPN in section **FAQs**. ● Deleted the content related to "Configuring a VPC for ECSs That Access the Internet Through a VPN" in section **Getting Started**. Modified the following content: ● Optimized section **Service Overview** and added the product advantage description to section **What Is Virtual Private Cloud?** ● Added section **Security Group Configuration Examples**. The security group configuration examples are integrated into one section and the original independent sections are deleted. ● Modified the description about how to switch to the **EIPs** page in section **EIP**.

Release Date	What's New
2019-02-23	Added the following content: ● Added the description about batch subnet creation in section **Creating a VPC**. ● Added precautions about disabling a firewall in section **Enabling or Disabling a Firewall**.
2019-02-22	Added the following content: ● Added the **Assign EIP** screenshot in section **Assigning an EIP and Binding It to an ECS**.
2019-02-15	Added the following content: ● Added the Anti-DDoS service restriction in section **How Does an IPv6 Client on the Internet Access the ECS That Has an EIP Bound in a VPC?** ● Added section **Modifying a Security Group**.
2019-02-11	Deleted the following content: ● Deleted the console screenshot from section **Assigning an EIP and Binding It to an ECS**.
2019-01-31	Accepted in OTC-4.0.

Release Date	What's New
2019-01-30	Modified the following content: ● Modified the table listing the parameters for creating a VPC in section **Creating a VPC**. ● Modified the table listing the parameters for modifying a security group rule section **Adding a Security Group Rule**. ● Added the link to the default security group rule introduction in section **Adding a Security Group Rule**. ● Modified the format of the exported file to Excel in sections **Exporting VPC Information** and **Importing and Exporting Security Group Rules**. ● Changed the number of characters allowed for the **Description** field to **255**. ● Modified the steps in section **Managing EIP Tags**. ● Added the **Monitoring Period** column to the table listing metrics in section **Supported Metrics**. ● Changed the maximum bandwidth size allowed to 1,000 Mbit/s in section **What Is the Bandwidth Size Range?** ● Modified the table listing subnet parameters in section **Modifying a Subnet**. ● Updated the security group description in section **Security Group**. ● Updated the VPC peering connection description in section **VPC Peering Connection**. ● Updated the firewall description in section **Firewall**. ● Updated the console screenshots in section **Adding a Firewall Rule**. ● Updated the console screenshots in section **Modifying a Firewall Rule**. Added the following content: ● Added section **Security Group Configuration Examples**. ● Added section **Route Table Overview**. ● Added section **Modifying an EIP Bandwidth**. ● Added description about disassociating and releasing multiple EIPs at a time in section **Unbinding an EIP from an ECS and Releasing the EIP**. Deleted the following content: ● Deleted description about the transitive peering relationships from section **What Are the Constraints Related to VPC Peering?** ● Deleted section "Viewing Routes Configured for a VPC Peering Connection in the VPC Peering Route Table".

Release Date	What's New
	- Deleted section "Deleting a Route from the VPC Peering Route Table". - Deleted description about the **Reject** action from section **Adding a Firewall Rule**.
2018-12-30	Modified the following content: - Modified the description about how to switch to the security group and firewall pages based on the changes made on the management console. Added the following content: - Added section "Firewall Overview". - Added section "Firewall Configuration Examples".
2018-11-30	Added the following content: - Added parameter **NTP Server Address** to the description about how to create a subnet. Modified the following content: - Updated the document based on changes made to the firewall console pages. – Added description about how to delete multiple firewall rules at a time and how to disassociate multiple subnets from a firewall at a time. – Changed parameter **Any** to **All**.
2018-09-18	Accepted in OTC-3.2/AGile-09.2018.
2018-09-06	Modified the following content: - Modified the content and changed some screenshots in the document based on the latest management console.
2018-08-30	This release incorporates the following change: - Added section "Adding Instances to and Removing Them from a Security Group".

Release Date	What's New
2018-07-30	This release incorporates the following changes: ● Optimized the sections related to security groups: – Added section "Replicating a Security Group Rule". – Added section "Modifying a Security Group Rule". – Modified section "Deleting a Security Group Rule" and added description about how to delete multiple security group rules at a time. – Added section "Importing and Exporting Security Group Rules". ● Modified the VPN sections. The details are as follows: – Modified the step for switching to the VPN console. – Deleted sections related to VPNs. An independent VPN user guide will be provided. – Deleted section **VPN Best Practice**.
2018-06-30	This release incorporates the following changes: ● Optimized sections under "Service Overview." ● Optimized sections under "Security Group". – Optimized section "Security Group Overview". – Optimized section "Default Security Groups and Security Group Rules". – Optimized section "Creating a Security Group". – Optimized section "Adding a Security Group Rule". – Optimized section "Fast-Adding Security Group Rules". – Added security group configuration examples. – Added section "Viewing the Security Group of an ECS". – Added section "Changing the Security Group of an ECS". ● Categorized FAQs.
2018-06-11	This release incorporates the following changes: ● Added section "Monitoring". ● Modified tag description.
2018-05-23	Accepted in OTC 3.1.
2018-04-28	This release incorporates the following changes: ● Added description about VPN tagging. ● Added the IPv6 address description. ● Added section "Exporting VPC Information". ● Modified the bandwidth range. ● Modified the VPN modification snapshot.

Release Date	What's New
2018-03-30	This release incorporates the following change: Deleted the IPv6 address description.
2018-02-28	This release incorporates the following change: Added the description that the security group description can contain a maximum of 128 characters.
2018-01-30	This release incorporates the following changes: ● Added description about the function of unbinding and releasing EIPs in batches. ● Added description about the function that the negotiation mode of the IKE policy in the VPN can be configured. ● Added the description that the security group description can contain a maximum of 64 characters.
2017-11-30	This release incorporates the following changes: ● Updated screenshots and steps based on the latest management console pages. ● Added description to indicate that subnets can be created without specifying the AZ.
2017-10-30	This release incorporates the following changes: ● Added description about the fast security group rule adding function. ● Added ECS security group configuration examples.
2017-09-30	This release incorporates the following changes: ● Added description to indicate that the peer project ID needs to be configured when a tenant creates a VPC peering connection with the VPC of another tenant. ● Modified description in sections "Adding a Security Group Rule" and "Deleting a Security Group Rule" based on changes made to the network console.
2017-08-30	This release incorporates the following changes: ● Added section "Managing Subnet Tags". ● Added description about the VPC, subnet, and EIP tags. ● Added section "Security Group Overview".

Release Date	What's New
2017-07-30	This release incorporates the following changes: ● Added description about how to enable shared SNAT on the management console. ● Added section "Managing VPC Tags". ● Added section "Managing EIP Tags". ● Changed the number of routes allowed in a route table by default to **100**. ● Updated procedures in sections "VPC and Subnet" and "Custom Route" based on changes made to the network console. ● Added description about the multi-project feature.
2017-06-30	This release incorporates the following change: ● Added description about the virtual IP address feature.
2017-05-30	This release incorporates the following change: ● Added FAQ "How Does an IPv6 Client on the Internet Access the ECS That Has an EIP Bound in a VPC?"
2017-04-28	This release incorporates the following change: ● Added description about how to add DNS server addresses during subnet information modification.
2017-03-30	This release incorporates the following changes: ● Added description about the firewall function. ● Added description about the shared SNAT function.
2017-02-28	This release incorporates the following change: ● Deleted description about the button for disabling the DHCP function.
2017-02-24	This release incorporates the following change: ● Added description about the VPC peering function.
2017-01-12	This release incorporates the following change: ● Added description about the custom route table function.
2016-10-19	This release incorporates the following change: ● Updated the Help Center URL of the VPN service.
2016-07-15	This release incorporates the following changes: ● Modified the VPN authentication algorithm. ● Optimized the traffic metering function.
2016-03-14	This issue is the first official release.

B Glossary

For details about the terms involved in this document, see **Glossary**.