Elastic IP

User Guide(Ankara Region)

Issue 01

Date 2024-04-15

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: https://www.huawei.com

Email: support@huawei.com

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:
https://www.huawei.com/en/psirt/vul-response-process
For vulnerability information, enterprise customers can visit the following web page:
https://securitybulletin.huawei.com/enterprise/en/security-advisory

Contents

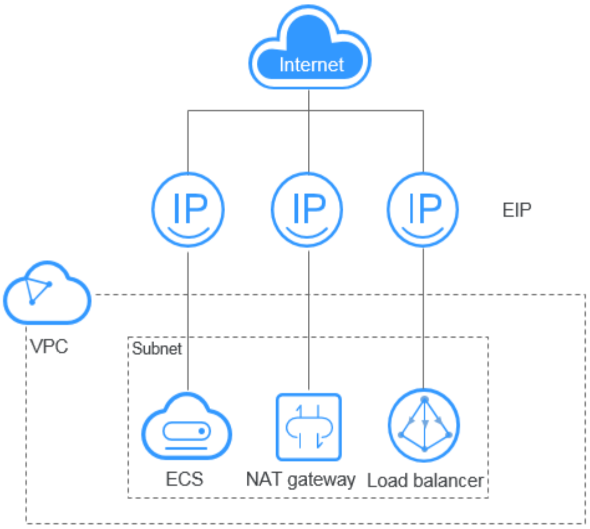
1 Service Overview

1.1 What Is Elastic IP?

The Elastic IP (EIP) service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. If a resource has an EIP bound, it can directly access the Internet. If a resource only has a private IP address, it cannot directly access the Internet. EIPs can be bound to or unbound from ECSs, virtual IP addresses, or load balancers.

Each EIP can be bound to only one cloud resource and they must be in the same region.

Figure 1-1 Connecting to the Internet using an EIP



1.2 Permissions

If you need to assign different permissions to employees in your enterprise to access your EIP resources, IAM is a good choice for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping you securely manage access to your cloud resources.

With IAM, you can use your cloud account to create IAM users, and assign permissions to the users to control their access to specific resources. For example, some software developers in your enterprise need to use EIP resources but should not be allowed to delete them or perform any high-risk operations. In this scenario, you can create IAM users for the software developers and grant them only the permissions required for using EIP resources.

If your cloud account does not need individual IAM users for permissions management, you may skip over this section.

IAM can be used free of charge. You pay only for the resources in your account. For more information, see section "IAM Service Overview" in the *Identity and Access Management Service User Guide*.

EIP Permissions

New IAM users do not have any permissions assigned by default. You need to first add them to one or more groups and attach policies or roles to these groups. The users then inherit permissions from the groups and can perform specified operations on cloud services based on the permissions they have been assigned.

Currently, EIP permissions are included in VPC permissions.

VPC is a project-level service deployed for specific regions. When you set **Scope** to **Region-specific projects** and select the specified projects in the specified regions, the users only have permissions for VPCs in the selected projects. If you set **Scope** to **All resources**, users have permissions for VPCs in all region-specific projects. When accessing VPCs, the users need to switch to the authorized region.

You can grant permissions by using roles and policies.

- Roles: A coarse-grained authorization strategy provided by IAM to assign permissions based on users' job responsibilities. Only a limited number of service-level roles are available for authorization. When you grant permissions using roles, you also need to attach dependent roles. Roles are not ideal for fine-grained authorization and least privilege access.
- Policies: A fine-grained authorization strategy that defines permissions required to perform operations on specific cloud resources under certain conditions. This type of authorization is more flexible and is ideal for least privilege access. For example, you can grant VPC users only the permissions for managing a certain type of resources. A majority of fine-grained policies contain permissions for specific APIs, and permissions are defined using API actions. For the API actions supported by VPC, see "Permissions Policies and Supported Actions" > "Introduction" in the *Virtual Private Cloud API Reference*.

Table 1-1 lists all the system-defined roles and policies supported by VPC.

Table 1-1 System-defined permissions for VPC

Policy Name	Description	Policy Type	Dependencies
VPC FullAccess	Full permissions for VPC	System-defined policy	To use the VPC flow log function, users must also have the **LTS ReadOnlyAccess** permission.
VPC ReadOnlyAccess	Read-only permissions on VPC.	System-defined policy	None
VPC Administrator	Most permissions on VPC, excluding creating, modifying, deleting, and viewing security groups and security group rules. To be granted this permission, users must also have the **Tenant Guest** and **Server Administrator** permission.	System-defined role	**Tenant Guest** and **Server Administrator** policies, which must be attached in the same project as **VPC Administrator**.

Table 1-2 lists the common operations supported by each system policy of VPC. Please choose proper system policies according to this table.

Table 1-2 Common operations supported by system-defined permissions

Operation	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Assigning an EIP	x	x	√
Viewing an EIP	√	x	√
Releasing an EIP	x	x	√
Binding or unbinding an EIP	x	x	√

Operation	VPC ReadOnlyAccess	VPC Administrator	VPC FullAccess
Adding an EIP to or removing an EIP from a shared bandwidth	x	x	√
Assigning a bandwidth	x	x	√
Viewing a bandwidth	√	x	√
Modifying a bandwidth	x	x	√
Deleting a bandwidth	x	x	√

1.3 Region and AZ

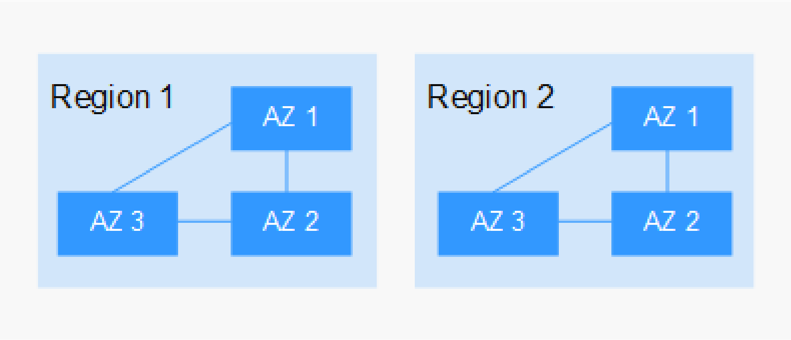
Concept

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 1-2 shows the relationship between regions and AZs.

Figure 1-2 Regions and AZs



Selecting a Region

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

Selecting an AZ

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

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

Regions and Endpoints

Before you use an API to call resources, specify its region and endpoint. For more details, see **Regions and Endpoints**.

2 Quick Start

2.1 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 2-1** to bind EIPs to the ECSs.

Figure 2-1 Configuring the network

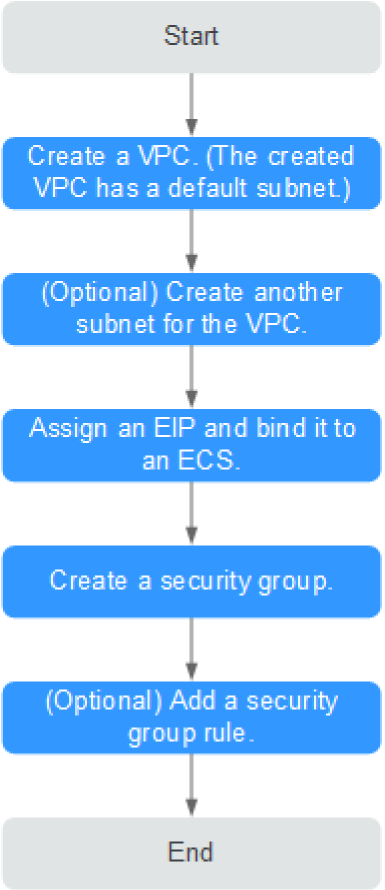

Start
Create a VPC. (The created VPC has a default subnet.)
(Optional) Create another subnet for the VPC.
Assign an EIP and bind it to an ECS.
Create a security group.
(Optional) Add a security group rule.
End

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. A created VPC comes with a default subnet you specified. After the VPC is created, you can create other required network resources in the VPC based on your service requirements.
Create another subnet for the VPC.	This task is optional. If the default subnet cannot meet your requirements, you can create one. The new subnet is used to assign IP addresses to NICs added to the ECS.
Assign an EIP and bind it to an ECS.	This task is mandatory. You can assign an EIP and bind it to an ECS for Internet access.
Create a security group.	This task is mandatory. You can create a security group and add ECSs in the VPC to the security group to improve ECS access security. After a security group is created, it has default rules, which allow all outgoing data packets. ECSs in a security group can access each other without the need to add rules.
Add a security group rule.	This task is optional. If the default rule does not meet your service requirements, you can add security group rules.

2.2 Step 1: Create a VPC

Scenarios

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

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

Procedure

1. Log in to the management console.

2. Click ☰ in the upper left corner and choose **Network** > **Virtual Private Cloud**.

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

3. Click **Create VPC**.

4. On the **Create VPC** page, set parameters as prompted.

   A default subnet will be created together with a VPC and you can also click **Add Subnet** to create more subnets for the VPC.

Table 2-2 Parameter descriptions

Category	Parameter	Description	Example Value
Basic Information	Region	Select the region nearest to you to ensure the lowest latency possible.	-
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	IPv4 CIDR Block	The CIDR block of the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets in the VPC). The following CIDR blocks are supported: ● 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	Advanced Settings	Click the drop-down arrow to set advanced VPC parameters.	Retain the default settings.
Basic Information	Description	Supplementary information about the VPC. This parameter is optional. The VPC description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	N/A

Category	Parameter	Description	Example Value
Default Subnet	AZ	The AZ of a VPC subnet.	sa-fb-1
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-001
Default Subnet	IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
Default Subnet	IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Default Subnet	Associated Route Table	The default route table to which the subnet will be associated. You can change the route table to a custom route table on the **Subnets** page.	Default
Default Subnet	Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including **Gateway** and **DNS Server Address**.	Retain the default settings.
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. Multiple IP addresses must be separated using commas (,).	100.125.x.x

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

5. Click **Create Now**.

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.

Procedure

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

   The **Virtual Private Cloud** page is displayed.
3. In the navigation pane on the left, choose **Virtual Private Cloud** > **Subnets**.
4. Click **Create Subnet**.

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

Table 2-3 Parameter descriptions

Parameter	Description	Example Value
VPC	The VPC for which you want to create a subnet.	-

Parameter	Description	Example Value
AZ	An AZ is a geographic location with independent power supply and network facilities in a region. AZs are physically isolated, and AZs in the same VPC are interconnected through an internal network. Note the following when you select an AZ: ● Subnets in a VPC can be in different AZs. For example, a VPC can have a subnet in AZ 1, and another subnet in AZ 3. ● A cloud resource can be in a different AZ from its subnet. For example, a cloud server in AZ 1 can be in a subnet in AZ 3.	sa-fb-1
Name	The subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set **IPv6 CIDR Block** to **Enable**. If you select this option, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
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. Multiple IP addresses must be separated using commas (,).	100.125.x.x

6. Click **OK**.

Precautions

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

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

2.4 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 choose **Network** > **Elastic IP**.
3. On the displayed page, click **Assign EIP**.
4. Set the parameters as prompted.

Table 2-4 Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you. The region selected for the EIP is its geographical location.	N/A
EIP Type	**Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP

Parameter	Description	Example Value
Billed By	The following bandwidth types are available: ● **Dedicated**: The bandwidth can be used by only one EIP and is suitable for scenarios with light or sharply fluctuating traffic. ● **Shared Bandwidth**: The bandwidth can be shared by multiple EIPs and is suitable for scenarios with staggered traffic.	Dedicated
Bandwidth	The bandwidth size in Mbit/s.	100
EIP Name	The name of the EIP.	eip-test
Bandwidth Name	The name of the bandwidth.	bandwidth
Type	The external network that the EIP connects to.	5_bgp
Quantity	The number of EIPs you want to purchase.	1

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

Binding an EIP

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

2.5 Step 4: Create a Security Group

Scenarios

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

Procedure

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

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

3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.

   The security group list is displayed.

4. In the upper right corner, click **Create Security Group**.

   The **Create Security Group** page is displayed.

5. Configure the parameters as prompted.

Table 2-5 Parameter description

Parameter	Description	Example Value
Name	Mandatory Enter the security group name. 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-AB
Template	Mandatory A template comes with default security group rules, helping you quickly create security groups. The following templates are provided: ● **Custom**: This template allows you to create security groups with custom security group rules. ● **General-purpose web server** (default value): The security group that you create using this template is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and allow inbound traffic on ports 22, 80, 443, and 3389. ● **All ports open**: The security group that you create using this template includes default rules that allow inbound traffic on any port. Note that allowing inbound traffic on any port poses security risks.	General-purpose web server
Description	Optional Supplementary information about the security group. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

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

2.6 Step 5: Add a Security Group Rule

Scenarios

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

Adding Rules to a Security Group

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

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

   The security group list is displayed.
4. Locate the row that contains the target security group, and click **Manage Rule** in the **Operation** column.

   The page for configuring security group rules is displayed.
5. On the **Inbound Rules** tab, click **Add Rule**.

   The **Add Inbound Rule** dialog box is displayed.
6. Configure required parameters.

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

Table 2-6 Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	The network protocol used to match traffic in a security group rule. The value can be **All**, **TCP**, **UDP**, **GRE**, and **ICMP**.	TCP
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Inbound rules control incoming traffic over specific ports to instances in the security group.	22, or 22-30

Parameter	Description	Example Value
Source	Source of the security group rule. The value can be an IP address or a security group to allow access from IP addresses or instances in the security group. ● IPv4 address: xxx.xxx.xxx.xxx/32 ● Subnet: xxx.xxx.xxx.0/24 ● Any IP address: 0.0.0.0/0 If the source is a security group, this rule will apply to all instances associated with the selected security group.	0.0.0.0/0
Description	(Optional) Supplementary information about the security group rule. The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

7. Click **OK**.

   The inbound rule list is displayed.

8. On the **Outbound Rules** tab, click **Add Rule**.

   The **Add Outbound Rule** dialog box is displayed.

9. Configure required parameters.

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

10. Click **OK**.

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

3 Elastic IP

3.1 Assigning an EIP and Binding It to an ECS

Scenarios

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

Assigning an EIP

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

Table 3-1 Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you. The region selected for the EIP is its geographical location.	N/A

Parameter	Description	Example Value
EIP Type	**Dynamic BGP**: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
Billed By	The following bandwidth types are available: ● **Dedicated**: The bandwidth can be used by only one EIP and is suitable for scenarios with light or sharply fluctuating traffic. ● **Shared Bandwidth**: The bandwidth can be shared by multiple EIPs and is suitable for scenarios with staggered traffic.	Dedicated
Bandwidth	The bandwidth size in Mbit/s.	100
EIP Name	The name of the EIP.	eip-test
Bandwidth Name	The name of the bandwidth.	bandwidth
Type	The external network that the EIP connects to.	5_bgp
Quantity	The number of EIPs you want to purchase.	1

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

Binding an EIP

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

3.2 Unbinding an EIP from an ECS and Releasing the EIP

Scenarios

If you no longer need an EIP, unbind it from the ECS and release the EIP to avoid wasting network resources.

Notes and Constraints

- Only EIPs with no instance bound can be released. If you want to release an EIP with an instance bound, you need to unbind EIP from the instance first.

Procedure

Unbinding a single EIP

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. On the displayed page, locate the row that contains the EIP, and click **Unbind**.
4. Click **Yes** in the displayed dialog box.

Releasing a single EIP

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. On the displayed page, locate the row that contains the target EIP, click **More** and then **Release** in the **Operation** column.
4. Click **Yes** in the displayed dialog box.

Unbinding multiple EIPs at once

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. On the displayed page, select the EIPs to be unbound.
4. Click the **Unbind** button located above the EIP list.
5. Click **Yes** in the displayed dialog box.

Releasing multiple EIPs at once

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. On the displayed page, select the EIPs to be released.
4. Click the **Release** button located above the EIP list.
5. Click **Yes** in the displayed dialog box.

3.3 Modifying an EIP Bandwidth

Scenarios

Modify the EIP bandwidth name or size.

Procedure

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

3. Locate the row that contains the target EIP in the EIP list, click **More** in the **Operation** column, and select **Modify Bandwidth**.
4. Modify the bandwidth parameters as prompted.
5. Click **Next**.
6. Click **Submit**.

3.4 Exporting EIP Information

Scenarios

The information of all EIPs under your account can be exported in an Excel file to a local directory. The file records the ID, status, type, bandwidth name, and bandwidth size of EIPs.

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. On the EIP list page, select one or more EIPs and click **Export** in the upper left corner.

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

3.5 IPv6 EIP

3.5.1 IPv6 EIP Overview

Overview

Both IPv4 and IPv6 EIPs are available. You can assign an IPv6 EIP or map an existing IPv4 EIP to an IPv6 EIP.

After the IPv6 EIP function is enabled, you will obtain both an IPv4 EIP and its corresponding IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

Application Scenarios of IPv4/IPv6 Dual Stack

If your ECS supports IPv6, you can use the IPv4/IPv6 dual stack. **Table 3-2** shows the example application scenarios.

Table 3-2 Application scenarios of IPv4/IPv6 dual stack

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Private IPv4 communication	Your applications on ECSs need to communicate with other systems (such as databases) through private networks using IPv4 addresses.	● No EIPs have been bound to the ECSs.	IPv4 CIDR Block	**Private IPv4 address**: used for private IPv4 communication.
Public IPv4 communication	Your applications on ECSs need to communicate with other systems (such as databases) through public IPv4 addresses.	● EIPs have been bound to the ECSs.	IPv4 CIDR Block	● **Private IPv4 address**: used for private IPv4 communication. ● **Public IPv4 address**: used for public IPv4 communication.

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Private IPv6 communication	Your applications on ECSs need to communicate with other systems (such as databases) through private IPv6 addresses.	● IPv6 has been enabled for the VPC subnet. ● The network has been configured for the ECSs as follows: – **VPC and Subnet**: IPv6-enabled subnet and VPC. – **Shared Bandwidth**: Selected **Do not configure**.	● IPv4 CIDR Block ● IPv6 CIDR block	● **Private IPv4 address + IPv4 EIP**: Bind an IPv4 EIP to the instance to allow public IPv4 communication. ● **Private IPv4 address**: Do not bind any IPv4 EIP to the instance and use only the private IPv4 address to allow private IPv4 communication. ● **IPv6 address**: Do not configure shared bandwidth for the IPv6 address to allow private IPv6 communication.

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv6 communication	An IPv6 network is required for the ECS to access the IPv6 service on the Internet.	- IPv6 has been enabled for the VPC subnet. - The network has been configured for the ECSs as follows: – **VPC and Subnet**: IPv6-enabled subnet and VPC. – **Shared Bandwidth**: Selected a shared bandwidth.	- IPv4 CIDR Block - IPv6 CIDR block	- **Private IPv4 address + IPv4 EIP**: Bind an IPv4 EIP to the instance to allow public IPv4 communication. - **Private IPv4 address**: Do not bind any IPv4 EIP to the instance and use only the private IPv4 address to allow private IPv4 communication. - **IPv6 address + shared bandwidth**: Allow both private IPv6 communication and public IPv6 communication.

For details, see section "IPv4 and IPv6 Dual-Stack Network" in *Virtual Private Cloud User Guide*.

Application Scenarios of IPv6 EIP

If you want an ECS to provide IPv6 services but the ECS does not support IPv6 networks or you do not want to build an IPv6 network, you can use IPv6 EIP to quickly address your requirements. For details about application scenarios and resource planning, see **Table 3-3**.

Table 3-3 Application scenarios and resource planning of an IPv6 EIP network (with IPv6 EIP enabled)

Application Scenario	Description	Requirement	IPv4 or IPv6 Subnet	ECS
Public IPv6 communication	You want to allow an ECS to provide IPv6 services for clients on the Internet without setting up an IPv6 network.	● An EIP has been bound to the ECS. ● IPv6 EIP has been enabled.	IPv4 CIDR Block	● **Private IPv4 address**: used for private IPv4 communication. ● **IPv4 EIP (with IPv6 EIP enabled)**: used for public network communication through IPv4 and IPv6 addresses.

3.5.2 Assigning or Releasing an IPv6 EIP

Scenarios

If you want an ECS to provide IPv6 services but the ECS does not support IPv6 networks or you do not want to build an IPv6 network, you can use an IPv6 EIP to quickly address your requirements.

Enabling IPv6 EIP

- Method 1:

  Apply for an EIP with **IPv6 EIP** enabled by referring to section **Assigning an EIP and Binding It to an ECS**.

  After the IPv6 EIP is enabled, you will obtain both an IPv4 EIP and an IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

- Method 2:

  If you want an IPv6 EIP in addition to an existing IPv4 EIP, locate the row that contains the target IPv4 EIP, click **More** in the **Operation** column, and select **Enable IPv6 EIP**. Then, a corresponding IPv6 EIP will be assigned.

  After the IPv6 EIP is enabled, you will obtain both an IPv4 EIP and an IPv6 EIP. External IPv6 addresses can access cloud resources through this IPv6 EIP.

Configuring Security Groups

After IPv6 EIP is enabled, add inbound and outbound security group rules to allow packets to and from the IP address range **198.19.0.0/16**. **Table 3-4** shows the security group rules. IPv6 EIP uses NAT64 to convert the source IP address in the inbound direction to an IPv4 address in the IP address range 198.19.0.0/16. The source port can be a random one, the destination IP address is the private IPv4 address of your local server, and the destination port remains unchanged.

For details, see section "Adding a Security Group Rule" in the *Virtual Private Cloud User Guide*.

Table 3-4 Security group rules

Direction	Protocol	Source or Destination
Inbound	All	Source: 198.19.0.0/16
Outbound	All	Destination: 198.19.0.0/16

Disabling IPv6 EIP

If you do not need the IPv6 EIP, locate the row that contains its corresponding IPv4 EIP, click **More** in the **Operation** column, and select **Disable IPv6 EIP**. Then, the IPv6 EIP will be released. You will only have the IPv4 EIP.

4 Shared Bandwidth

4.1 Shared Bandwidth Overview

A shared bandwidth can be shared by multiple EIPs and controls the data transfer rate on these EIPs in a centralized manner. All ECSs and load balancers that have EIPs bound in the same region can share a bandwidth.

NOTE

- A shared bandwidth cannot control how much data can be transferred using a single EIP. Data transfer rate on EIPs cannot be customized.

When you host a large number of applications on the cloud, if each EIP uses a bandwidth, a lot of bandwidths are required, 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 (except for **5_gray** EIPs of dedicated load balancers) to or remove them from a shared bandwidth regardless of the type of instances that they are bound to.

  NOTE

  Do not add EIPs of the dedicated load balancer type (**5_gray**) and other types to the same shared bandwidth. Otherwise, the bandwidth limit policy will not take effect.

4.2 Assigning a Shared Bandwidth

Scenarios

Assign a shared bandwidth for use with EIPs.

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the upper right corner, click **Assign Shared Bandwidth**. On the displayed page, configure parameters as prompted.

Table 4-1 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.	sa-fb-1
Bandwidth	The bandwidth size in Mbit/s. The maximum bandwidth can be 300 Mbit/s.	10
Name	The name of the shared bandwidth.	Bandwidth-001

5. Click **Create Now**.

4.3 Adding EIPs to a Shared Bandwidth

Scenarios

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

Notes and Constraints

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

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the target shared bandwidth that you want to add EIPs to. In the **Operation** column, choose **Add EIP**, and select the EIPs to be added.

NOTE

- After an EIP is added to a shared bandwidth, the dedicated bandwidth used by the EIP will become invalid and the EIP will start to use the shared bandwidth. The EIP's dedicated bandwidth will be deleted and will no longer be billed.

5. Click **OK**.

4.4 Removing EIPs from a Shared Bandwidth

Scenarios

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

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the target shared 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.
5. Click **OK**.

4.5 Modifying a Shared Bandwidth

Scenarios

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

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the shared bandwidth you want to modify, click **Modify Bandwidth** in the **Operation** column, and modify the bandwidth settings.
5. Click **Next**.
6. Click **Submit**.

4.6 Deleting a Shared Bandwidth

Scenarios

Delete a shared bandwidth when it is no longer required.

Prerequisites

Before deleting a shared bandwidth, remove all the EIPs associated with it. For details, see **Removing EIPs from a Shared Bandwidth**.

Procedure

1. Log in to the management console.
2. Click ☰ in the upper left corner and choose **Network** > **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the shared bandwidth you want to delete, click **More** in the **Operation** column, and then click **Delete**.
5. In the displayed dialog box, click **OK**.

5 Monitoring

5.1 Supported Metrics

Description

This section describes the namespace, list, and measurement dimensions of metrics of EIPs and bandwidths 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 generated alarms.

Namespace

Namespace of EIPs and bandwidths: SYS.VPC

Monitoring Metrics

Table 5-1 Metrics of EIPs and bandwidths

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth	Outbound Bandwidth	Network rate of outbound traffic Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth in the unit of percent. Outbound bandwidth usage = Outbound bandwidth/ Purchased bandwidth	0% to 100%	Bandwidth or EIP	1 minute
downstream_bandwidth_usage	Inbound Bandwidth Usage	Usage of inbound bandwidth in the unit of percent. Inbound bandwidth usage = Inbound bandwidth/ Purchased bandwidth	0-100%	Bandwidth or EIP	1 minute
up_stream	Outbound Traffic	Network traffic going out of the cloud platform Unit: byte	≥ 0 Bytes	Bandwidth or EIP	1 minute
down_stream	Inbound Traffic	Network traffic going into the cloud platform Unit: byte	≥ 0 Bytes	Bandwidth or EIP	1 minute

NOTE

If a bandwidth is increased or decreased, there is a delay of 5 to 10 minutes for the monitoring metrics to update for the new bandwidth.

Dimensions

Key	Value
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

If a monitored object has multiple dimensions, all dimensions are mandatory when you use APIs to query the metrics.

- Query a monitoring metric:

  ```
  dim.0=bandwidth_id,530cd6b0-86d7-4818-837f-935f6a27414d&dim.1=publicip_id,3773b058-5b4f-4366-9035-9bbd9964714a
  ```

- Query monitoring metrics in batches:

  ```
  "dimensions": [
  {
  "name": "bandwidth_id",
  "value": "530cd6b0-86d7-4818-837f-935f6a27414d"
  },
  {
  "name": "publicip_id",
  "value": "3773b058-5b4f-4366-9035-9bbd9964714a"
  }
  ],
  ```

5.2 Viewing Metrics

Scenarios

You can view the bandwidth and EIP usage.

You can view the inbound bandwidth, outbound bandwidth, inbound bandwidth usage, outbound bandwidth usage, inbound traffic, and outbound traffic in a specified period.

Procedure

1. Log in to the management console.
2. In the upper left corner of the page, click ☰ to open the service list and choose **Management & Deployment** > **Cloud Eye**.
3. Click **Cloud Service Monitoring** on the left of the page, and choose **Elastic IP and Bandwidth**.
4. Locate the target metric and click **View Metric** in the **Operation** column to check detailed information.

5.3 Creating an Alarm Rule

Scenarios

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

Procedure

1. Log in to the management console.
2. In the upper left corner of the page, click ≡ to open the service list and choose **Management & Deployment** > **Cloud Eye**.
3. In the left navigation pane on the left, choose **Alarm Management** > **Alarm Rules**.
4. On the **Alarm Rules** page, click **Create Alarm Rule** and set required parameters, or modify an existing alarm rule.
5. After the parameters are set, click **Create**.

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

   NOTE

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

5.4 Exporting Monitoring Data

Scenarios

If you want to analyze the bandwidth or traffic usage of EIPs to locate faults, you can export EIP monitoring data.

Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Management & Deployment** > **Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring** > **Elastic IP and Bandwidth**.
4. On the **Cloud Service Monitoring** page, click **Export Data**.
5. Configure the time range, resource type, dimension, monitored object, and metric.
6. Click **Export**.

- The first row in the exported CSV file displays the username, region, service, instance name, instance ID, metric name, metric data, time, and timestamp. You can view historical monitoring data.

- To convert the time using a Unix timestamp to the time of the target time zone, perform the following steps:
  a. Use Excel to open a .csv file.
  b. Use the following formula to convert the time:

     Target time = [Unix timestamp/1000 + (Target time zone) x 3600]/86400 + 70 x 365 + 19
  c. Set cell format to **Date**.

6 Permissions Management

6.1 Creating a User and Granting EIP Permissions

Currently, the EIP service permissions are included in the VPC permissions. For details, see **Permissions Management**.

This section describes how to use IAM to implement fine-grained permissions control for your VPC resources. With IAM, you can:

- Create IAM users for personnel based on your enterprise's organizational structure. Each IAM user has their own identity credentials for accessing VPC resources.
- Grant users only the permissions required to perform a given task based on their job responsibilities.
- Entrust a cloud account or cloud service to perform efficient O&M on your VPC resources.

If your cloud account meets your permissions requirements, you can skip this section.

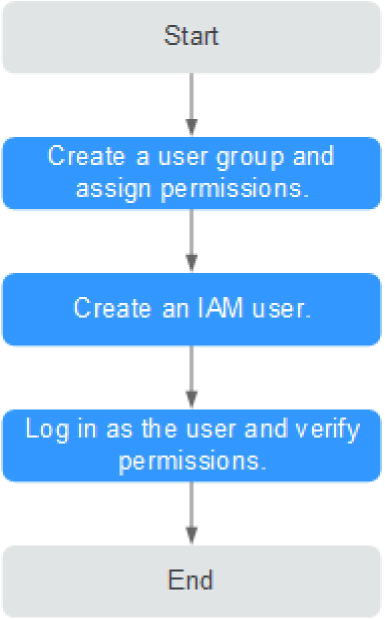
Figure 6-1 shows the process flow for granting permissions.

Prerequisites

Before granting permissions to user groups, learn about **EIP Permissions** for EIP.

Process Flow

Figure 6-1 Process for granting EIP permissions


Start
Create a user group and assign permissions.
Create an IAM user.
Log in as the user and verify permissions.
End

1. On the IAM console, create a user group and grant it permissions.

   Create a user group on the IAM console and click **Authorize** in the **Operation** column to assign the **EIP ReadOnlyAccess** permissions to the group.

2. Create an IAM user and add it to the created user group.

   Create a user on the IAM console and add it to the user group created in 1 by choosing **Authorize** in the **Operation** column.

3. Log in as the IAM user and verify permissions.

   In the authorized region, perform the following operations:

   – Choose **Service List** > **Elastic IP**. Then click **Assign EIP** on the EIP console. If a message appears indicating that you have insufficient permissions to perform the operation, the **EIP ReadOnlyAccess** policy is in effect.

   – Choose another service from **Service List**. If a message appears indicating that you have insufficient permissions to access the service, the **EIP ReadOnlyAccess** policy is in effect.

Example Custom Policies

- Example 1: Grant permissions to assign and view EIPs

```
{
   "Version": "1.1",
   "Statement": [
      {
         "Effect": "Allow",
         "Action": [
            "vpc:publicIps:create",
            "vpc:publicIps:list"
          ]
      }
```

```
    ]
}
```

- Example 2: Grant permission to deny EIP deletion.

  A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  Assume that you want to grant the permissions of the **EIP FullAccess** policy to a user but want to prevent them from releasing EIPs. You can create a custom policy for denying EIP release, and attach both policies to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on EIPs except releasing them. Example policy denying EIP release:

```
{
      "Version": "1.1",
      "Statement": [
            {
          "Effect": "Deny",
                  "Action": [
                        "vpc:publicIps:delete"
                  ]
            }
      ]
}
```

- Example 3: Create a custom policy containing multiple actions.

  A custom policy can contain the actions of one or multiple services that are of the same type (global or project-level). Example policy containing multiple actions:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpc:publicIps:update",
                "vpc:publicIps:create"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "vpc:publicIps:delete"
            ]
        }
    ]
}
```

6.2 EIP Custom Policies

Custom policies can be created as a supplement to the system policies of EIP. For the actions supported for custom policies, see "Permissions Policies and Supported Actions" > "Introduction" in the *Elastic IP API Reference.*

You can create custom policies in either of the following ways:

- Visual editor: Select cloud services, actions, resources, and request conditions. This does not require knowledge of policy syntax.
- JSON: Edit JSON policies from scratch or based on an existing policy.

For details, see "Creating a Custom Policy" in the *Identity and Access Management User Guide*. The following section contains examples of common EIP custom policies.

Example Custom Policies

- Example 1: Grant permissions to assign and view EIPs

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpc:publicIps:create",
                "vpc:publicIps:list"
             ]
        }
    ]
}
```

- Example 2: Grant permission to deny EIP deletion.

  A policy with only "Deny" permissions must be used together with other policies. If the permissions granted to an IAM user contain both "Allow" and "Deny", the "Deny" permissions take precedence over the "Allow" permissions.

  Assume that you want to grant the permissions of the **EIP FullAccess** policy to a user but want to prevent them from releasing EIPs. You can create a custom policy for denying EIP release, and attach both policies to the user. As an explicit deny in any policy overrides any allows, the user can perform all operations on EIPs except releasing them. Example policy denying EIP release:

```
{
      "Version": "1.1",
      "Statement": [
            {
          "Effect": "Deny",
                  "Action": [
                        "vpc:publicIps:delete"
                  ]
            }
      ]
}
```

- Example 3: Create a custom policy containing multiple actions.

  A custom policy can contain the actions of one or multiple services that are of the same type (global or project-level). Example policy containing multiple actions:

```
{
    "Version": "1.1",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "vpc:publicIps:update",
                "vpc:publicIps:create"
            ]
        },
        {
            "Effect": "Deny",
            "Action": [
                "vpc:publicIps:delete"
            ]
        }
```

```
  ]
}
```

7 FAQs

7.1 Product Consultation

7.1.1 What Is a Quota?

What Is a Quota?

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

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

How Do I View My Quotas?

1. Log in to the management console.
2. In the upper right corner of the page, click 📊 .

   The **Service Quota** page is displayed.
3. 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, contact the operations administrator.

Before contacting the operations administrator, make sure that the following information has been obtained:

- Account name, 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 account name on the **My Credentials** page.

- Quota information, which includes service name, quota type, and required quota

7.1.2 Can I Bind an EIP to Multiple ECSs?

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

7.2 EIP Binding and Unbinding

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

Each ECS is automatically added to a security group after being created to ensure its security. The security group denies access traffic from the Internet by default. To allow external access to ECSs in the security group, add an inbound rule to the security group.

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

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

  The default source **0.0.0.0/0** indicates that all IP addresses can access ECSs in the security group.
- Allocate ECSs that have different Internet access requirements to different security groups.

7.2.2 Can Multiple EIPs Be Bound to an ECS?

Scenarios

Multiple EIPs can be bound to an ECS, but this operation is not recommended.

If an ECS has multiple NICs attached and you want to bind multiple EIPs to this ECS, you need to configure policy-based routes for these NICs so that these extension NICs can communicate with external works. For details, see **Configuration Example**.

Configuration Example

Table 7-1 lists ECS configurations.

Table 7-1 ECS configurations

Parameter	Configuration
Name	ecs_test
Image	CentOS 6.5 64bit
EIP	2
Primary NIC	eth0
Secondary NIC	eth1

Example 1:

If you intend to access public network 11.11.11.0/24 through standby NIC **eth1**, perform the following operations to configure a route:

1. Log in to the ECS.
2. Run the following command to configure a route:

   ip route add 11.11.11.0/24 dev eth1 via 192.168.2.1

   In the preceding command, **192.168.2.1** is the gateway IP address of standby NIC **eth1**.

Example 2:

Based on example 1, if you intend to enable routing for default public network traffic through standby NIC **eth1**, perform the following operations to configure a route:

1. Log in to the ECS.
2. Run the following command to delete the default route:

   ip route delete default

   NOTICE

   Exercise caution when deleting the default route because this operation will interrupt the network and result in SSH login failures.

3. Run the following command to configure a new default route:

   ip route add 0.0.0.0/0 dev eth1 via 192.168.2.1

   In the preceding command, **192.168.2.1** is the gateway IP address of standby NIC **eth1**.

7.3 Bandwidth

7.3.1 What Is the Bandwidth Size Range?

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

7.3.2 Is There a Limit to the Number of EIPs That Can Be Added to Each Shared Bandwidth?

A maximum of 20 EIPs can be added to each shared bandwidth. If you want to add more EIPs to each shared bandwidth, request a quota increase. For details, see **What Is a Quota?**

7.4 Connectivity

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

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

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

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

7.4.2 Why Does the Download Speed of My ECS Is Slow?

If the download speed of an ECS is slow, check the following:

- Bandwidth limit exceeded: Your used bandwidth exceeds its limit and the limiting policy of the bandwidth takes effect, causing packet loss and slowing down the access. You can check the bandwidth usage or increase the bandwidth.

  If your service traffic continues to be high, you can increase the bandwidth by referring to **Modifying a Shared Bandwidth**.

- The memory usage of the ECS is higher than 80%.

  For details, see section "Why Is My Linux ECS Running Slowly?" or "Why Is My Windows ECS Running Slowly?" in the *Elastic Cloud Server User Guide*.

- Unstable carrier lines: The network between the local server and the cloud is unstable. Contact the carrier to check the network status.

A Change History

Released On	Description
2024-04-15	This issue is the first official release.