

Elastic IP

User Guide(ME-Abu Dhabi Region)

Issue 01
Date 2024-04-01



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

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

Trademarks and Permissions



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

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

Notice

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

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

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
1.1 What Is Elastic IP?.....	1
1.2 Advantages.....	2
1.3 Application Scenarios.....	2
1.4 Functions.....	4
1.5 Notes and Constraints.....	5
1.6 Billing.....	5
1.7 EIP and Other Services.....	7
1.8 Region and AZ.....	8
2 Quick Start.....	10
2.1 Overview.....	10
2.2 Step 1: Create a VPC.....	11
2.3 Step 2: Create a Subnet for the VPC.....	17
2.4 Step 3: Assign an EIP and Bind It to an ECS.....	21
2.5 Step 4: Create a Security Group.....	24
2.6 Step 5: Add a Security Group Rule.....	28
3 Elastic IP.....	33
3.1 EIP Overview.....	33
3.2 Assigning an EIP and Binding It to an ECS.....	34
3.3 Assigning an EIP.....	37
3.4 Binding an EIP to an Instance.....	39
3.5 Unbinding an EIP from an Instance.....	40
3.6 Releasing an EIP.....	41
3.7 Changing Dedicated Bandwidth Size of an EIP.....	42
3.8 Unbinding an EIP from an ECS and Releasing the EIP.....	42
3.9 Modifying an EIP Bandwidth.....	43
3.10 Exporting EIP Information.....	44
3.11 Managing EIP Tags.....	44
4 Shared Bandwidth.....	47
4.1 Shared Bandwidth Overview.....	47
4.2 Assigning a Shared Bandwidth.....	47
4.3 Adding EIPs to a Shared Bandwidth.....	49

4.4 Removing EIPs from a Shared Bandwidth.....	49
4.5 Modifying a Shared Bandwidth.....	50
4.6 Deleting a Shared Bandwidth.....	50
5 Monitoring.....	52
5.1 Supported Metrics.....	52
5.2 Viewing Metrics.....	54
5.3 Creating an Alarm Rule.....	55
5.4 Exporting Monitoring Data.....	55
6 FAQs.....	57
6.1 Product Consultation.....	57
6.1.1 What Is a Quota?.....	57
6.1.2 How Do I Assign or Retrieve a Specific EIP?.....	58
6.1.3 Why Is an EIP Newly Assigned the Same as the One I Released?.....	58
6.1.4 What Are the Differences Between EIP, Private IP Address, and Virtual IP Address?.....	58
6.1.5 Can an EIP That Uses Dedicated Bandwidth Be Changed to Use Shared Bandwidth?.....	59
6.1.6 Can I Bind an EIP to Multiple ECSs?.....	59
6.1.7 What Are the Differences Between the Primary and Extension NICs of ECSs?.....	60
6.1.8 What Is the EIP Assignment Policy?.....	60
6.1.9 Can I Assign a Specific EIP?.....	60
6.1.10 Can a Bandwidth Be Used by Multiple Accounts?.....	60
6.1.11 How Do I Unbind an EIP from an Instance and Bind a New EIP to the Instance?.....	60
6.1.12 Why Can't I Find My Assigned EIP on the Management Console?.....	62
6.2 EIP Binding and Unbinding.....	63
6.2.1 How Do I Access an ECS with an EIP Bound from the Internet?.....	63
6.2.2 How Do I Access the Internet Using an EIP Bound to an Extension NIC?.....	63
6.2.3 Can I Bind an EIP of an ECS to Another ECS?.....	64
6.2.4 Can Multiple EIPs Be Bound to an ECS?.....	65
6.2.5 Can I Bind an EIP to a Cloud Resource in Another Region?.....	66
6.3 Bandwidth.....	66
6.3.1 What Is the Bandwidth Size Range?.....	66
6.3.2 How Do I Increase a Bandwidth to Be More Than 300 Mbit/s?.....	66
6.3.3 What Bandwidth Types Are Available?.....	66
6.3.4 Is There a Limit to the Number of EIPs That Can Be Added to Each Shared Bandwidth?.....	66
6.3.5 What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth?.....	67
6.3.6 What Are Inbound Bandwidth and Outbound Bandwidth?.....	67
6.3.7 How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?.....	68
6.3.8 What Are the Differences Between Public Bandwidth and Private Bandwidth?.....	70
6.3.9 What Is the Relationship Between Bandwidth and Upload/Download Rate?.....	70
6.4 Connectivity.....	71
6.4.1 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?.....	71
6.4.2 Why Can't My ECS Access the Internet Even After an EIP Is Bound?.....	71

6.4.3 What Should I Do If an EIP Cannot Be Pinged?.....	74
6.4.4 Why Does the Download Speed of My ECS Is Slow?.....	80
A Change History.....	81

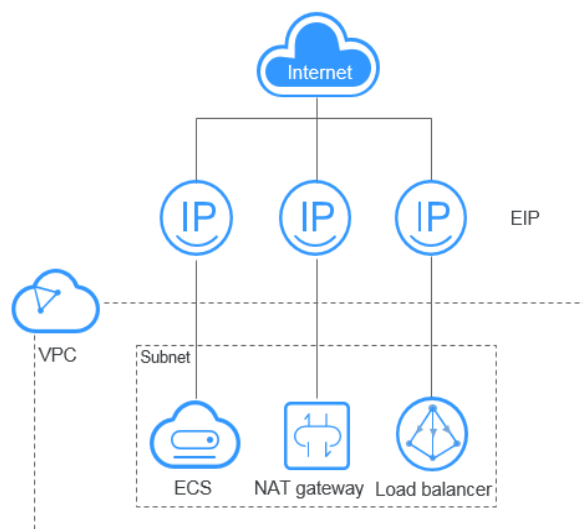
1 Service Overview

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, BMSs, virtual IP addresses, NAT gateways, 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



Accessing EIP

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

- Management console
Log in to the management console, select **Elastic IP** from the console homepage, and then perform operations on EIP resources.
- APIs
If you need to integrate the EIP service provided by the cloud system into a third-party system for secondary development, you can use an API to access the EIP service. For details, see the *Elastic IP API Reference*.

1.2 Advantages

An EIP has the following advantages:

- Flexibility
EIPs can be flexibly bound to or unbound from ECSs, BMSs, NAT gateways, load balancers, or virtual IP addresses. The bandwidth can be scaled according to service changes.
- Cost-effective
EIPs are available on a pay-per-use (billed by bandwidth or traffic) basis. You can use shared bandwidth to enjoy lower bandwidth costs.
- Ease of use
EIP binding, unbinding, and bandwidth adjustments take effect immediately.

1.3 Application Scenarios

Binding an EIP to an ECS

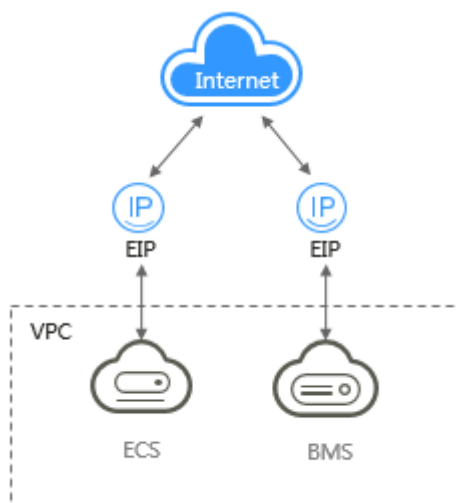
Scenario

You can bind an EIP to an ECS to enable the ECS to access the Internet.

Related Services

ECS, BMS, or VPC

Figure 1-2 Binding an EIP to a server



Binding an EIP to a NAT Gateway

Scenario

After an EIP is bound to a NAT gateway and SNAT and DNAT rules are added, multiple servers (such as ECSs and BMSs) can use the same EIP to access the Internet and provide services accessible from the Internet.

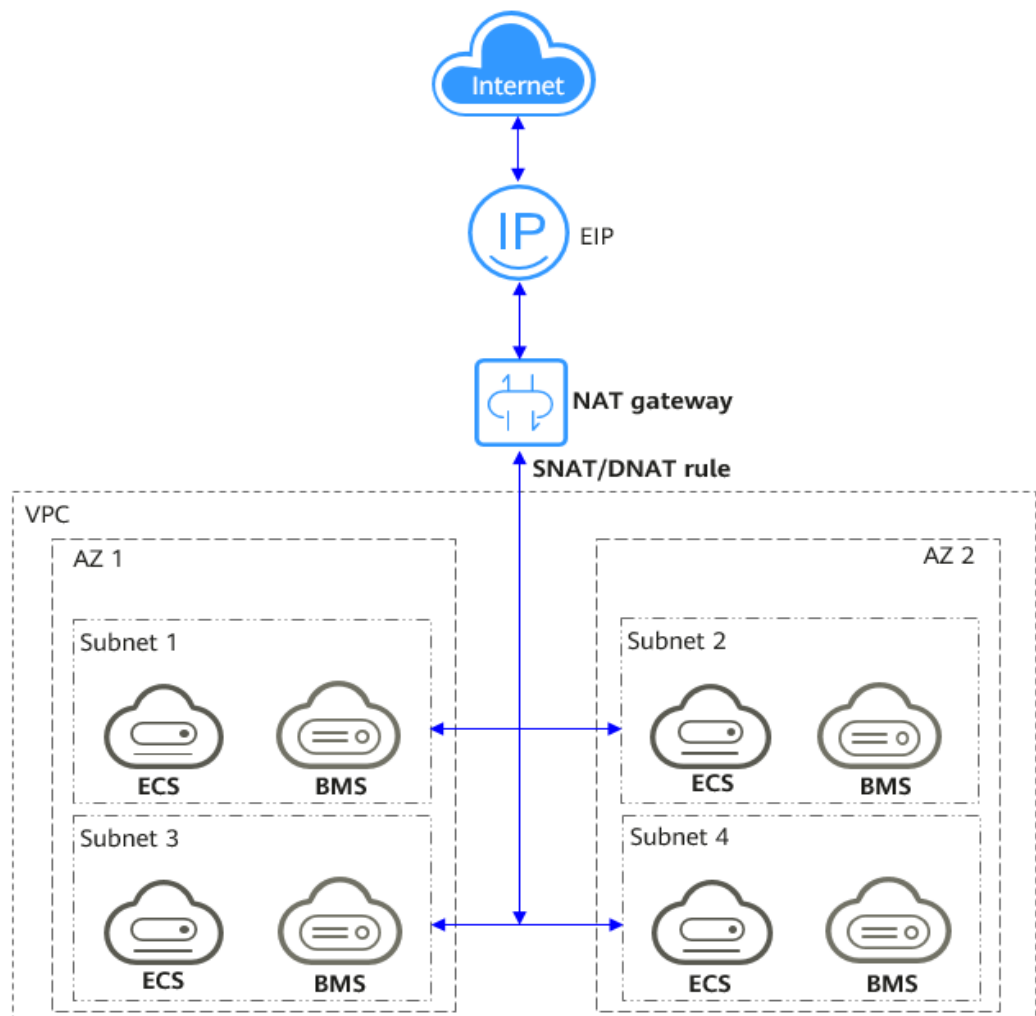
An SNAT rule allows servers in a specific VPC subnet to use the same EIP to access the Internet.

A DNAT rule enables servers in a VPC to provide services accessible from the Internet.

Related Services

NAT Gateway, cloud server (ECS and BMSs), and VPC

Figure 1-3 EIP used by a NAT gateway



Binding an EIP to a Load Balancer

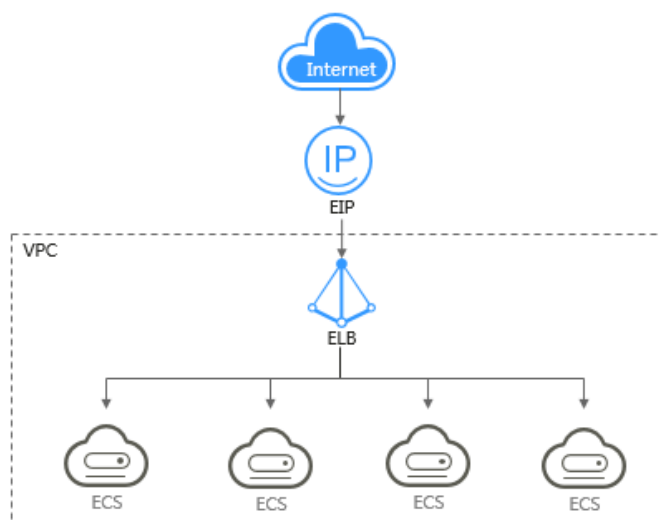
Scenario

After you attach an EIP to a load balancer, the load balancer can distribute requests from the Internet to backend servers.

Related Services

ELB, ECS, and VPC

Figure 1-4 EIP used by a load balancer



1.4 Functions

Table 1-1 lists the common functions of EIP.

Table 1-1 Common EIP functions

Category	Function	Description
EIP and Bandwidth	EIP	The EIP service enables your cloud resources to communicate with the Internet using static public IP addresses and scalable bandwidths. You can assign EIPs, bind them to or unbind them from cloud resources, release EIPs, and modify EIP bandwidth. For details, see section "EIP Overview" in the <i>Elastic IP User Guide</i> .
	Shared Bandwidth	All ECSs, BMSs, and load balancers can share the same bandwidth if they reside in the same region and have EIPs bound. You can assign, modify, delete a shared bandwidth, add EIPs to a shared bandwidth, and remove EIPs from a shared bandwidth. For details, see section "Shared Bandwidth Overview" in the <i>Elastic IP User Guide</i> .

Category	Function	Description
Monitoring	Viewing Metrics	<p>If you have subscribed to the VPC service, you can view bandwidth and EIP usage through Cloud Eye without adding plug-ins. On Cloud Eye, you can also create alarm rules, and customize monitored resources and notification policies.</p> <p>For details, see section "Supported Metrics" in the <i>Elastic IP User Guide</i>.</p>

1.5 Notes and Constraints

EIP

Note the following when using EIPs:

- Each EIP can only be bound to one cloud resource.
- An EIP that has already been bound to a cloud resource cannot be bound to another resource without first being unbound from the current resource.
- EIPs cannot be transferred across accounts.
- You can only release unbound EIPs.
- The system preferentially assigns EIPs to you from the ones you released, if any. However, if any of these EIPs is already assigned to another user, it cannot be re-assigned to you.

Bandwidth

- The smallest shared bandwidth that can be purchased is 5 Mbit/s. You can only add pay-per-use EIPs to a shared bandwidth.
- A shared bandwidth or dedicated bandwidth can only be used by resources owned by the same account.

NOTE

- Inbound bandwidth is the bandwidth consumed when data is transferred from the Internet to the cloud. Outbound bandwidth is the bandwidth consumed when data is transferred from the cloud to the Internet.

1.6 Billing

Billing Item

EIPs are billed on a pay-per-use basis. [Table 1-2](#) describes the EIP billing items.

Table 1-2 EIP billing

Billing Mode	Billing By	EIP Retention Fee	Bandwidth Price	Public Network Traffic Price
Pay-per-use	Bandwidth	<ul style="list-style-type: none"> EIP retention fee is not included if the EIP is bound to an ECS, BMS, or load balancer. EIP retention fee is included if the EIP is unbound but not released. 	Included	Not included
	Traffic		Not included	Included

 **NOTE**

- "Not included" indicates that the fee will not be included in the bill. "Included" indicates that the fee will be included in the bill.
- You can go to the product pricing details page to view details about the EIP pricing.

Billing Options

The public network bandwidth can be billed by fixed bandwidth or by traffic usage.

- By fixed bandwidth: You will be billed based on the bandwidth you specify. Your outbound bandwidth will not exceed the bandwidth specified.
- By traffic usage: You will be billed on a pay-per-use basis. Only traffic used in the outbound direction will be billed.

To prevent excessive fees due to sudden traffic spikes, you can set a peak value for the outbound bandwidth.

You can select the billing mode based on bandwidth usage.

EIPs are billed on a pay-per-use basis. For details, see [Table 1-3](#).

Table 1-3 EIP billing items

Billing Item	Description	Applicable Scenario
Bandwidth Price	The bandwidth is fixed and the traffic is not limited.	For heavy or stable traffic
Public network traffic	Specified maximum bandwidth, billed hourly by the amount of traffic used	For light or sharply fluctuating traffic

Billing Item	Description	Applicable Scenario
EIP retention fee	<ul style="list-style-type: none"> If an EIP is bound to an instance, the EIP is free. If an EIP is unbound from an instance but is not released, the EIP will be billed. 	-

Configuration Changes

For a pay-per-use EIP, you can change the bandwidth name, size, and specify whether it is to be billed by bandwidth or traffic.

Table 1-4 Impact on fees

Billing Mode	Change Scenario	Impact on Fees
Pay-per-use	Change the EIP to be billed by traffic or billed by bandwidth.	The change will take effect immediately.

1.7 EIP and Other Services

Table 1-5 Related services

Interactive Function	Service	Reference
Bind an EIP to a server to allow the server to access the Internet.	Elastic Cloud Server (ECS) BMS	Section "Binding an EIP" in the <i>Elastic Cloud Server User Guide</i> Section "Binding an EIP to a BMS" in <i>Bare Metal Server User Guide</i>
Bind a virtual IP address to an EIP so that you can access the ECSs deployed in active/standby mode through the virtual IP address.	Virtual Private Cloud (VPC)	Section "Binding a Virtual IP Address to an EIP or ECS" in the <i>Virtual Private Cloud User Guide</i>

Interactive Function	Service	Reference
Configure ECSs to share one or more EIPs through a NAT gateway to access the Internet.	NAT Gateway	Section "Using SNAT to Access the Internet" in the <i>NAT Gateway Quick Start</i>
Distribute incoming traffic to multiple ECSs in a VPC.	ELB	Section "Creating a Load Balancer" in the <i>Elastic Load Balance User Guide</i> .
Check the bandwidth and traffic usage.	Cloud Eye	Section "Viewing Metrics" in the <i>Elastic IP User Guide</i>

1.8 Region and AZ

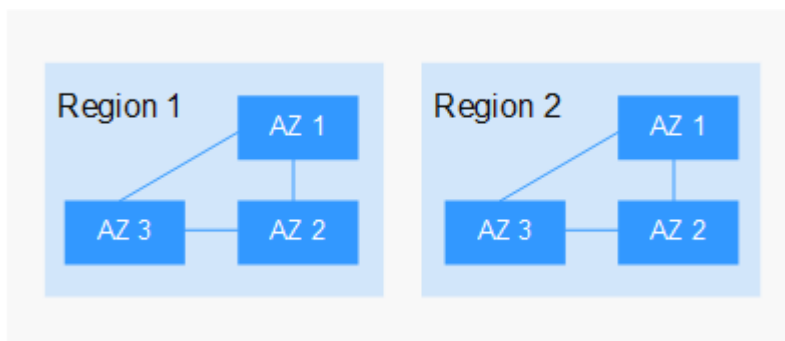
Concept

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

- A region is a physical data center, which is completely isolated to improve fault tolerance and stability. The region that is selected during resource creation cannot be changed after the resource is created.
- An AZ is a physical location where resources use independent power supplies and networks. A region contains one or more AZs that are physically isolated but interconnected through internal networks. Because AZs are isolated from each other, any fault that occurs in one AZ will not affect others.

Figure 1-5 shows the relationship between regions and AZs.

Figure 1-5 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

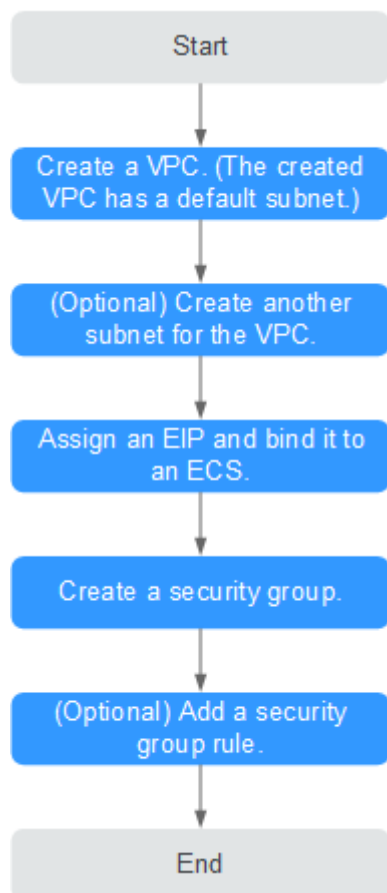


Table 2-1 describes the different tasks in the procedure for configuring the network.

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**.
The **Create VPC** page is displayed.
4. On the **Create VPC** page, set parameters as prompted.
A default subnet will be created together with a VPC and you can also click **Add Subnet** to create more subnets for the VPC.

Table 2-2 VPC parameter descriptions

Parameter	Description	Example Value
Region	Select the region nearest to you to ensure the lowest latency possible.	-
Name	The VPC name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	VPC-test
IPv4 CIDR Block	The CIDR block of the VPC. The CIDR block of a subnet can be the same as the CIDR block for the VPC (for a single subnet in the VPC) or a subset of the CIDR block for the VPC (for multiple subnets in the VPC). The following CIDR blocks are supported: <ul style="list-style-type: none"> ● 10.0.0.0/8-24 ● 172.16.0.0/12-24 ● 192.168.0.0/16-24 	192.168.0.0/16

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

Table 2-3 Subnet parameter descriptions

Parameter	Description	Example Value
AZ	<p>An AZ is a geographic location with independent power supply and network facilities in a region. AZs are physically isolated, and AZs in the same VPC are interconnected through an internal network.</p> <p>Note the following when you select an AZ:</p> <ul style="list-style-type: none"> • A VPC can have subnets that are in different AZs. For example, a VPC can have subnet A in AZ 1, and subnet B in AZ 3. • A cloud resource and its subnet can be in different AZs. For example, a cloud server in AZ 1 can use a subnet in AZ 3. 	AZ1

Parameter	Description	Example Value
Name	The subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	subnet-01
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set IPv6 CIDR Block to Enable . After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Associated Route Table	The default route table to which the subnet will be associated. You can change the route table to a custom route table on the Subnets page.	Default
Advanced Settings	Click the drop-down arrow to set advanced settings for the subnet, including Gateway and DNS Server Address .	Retain the default settings.
Gateway	The gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1

Parameter	Description	Example Value
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x
DHCP Lease Time	<p>The period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day or hour</p> <p>After you change the DHCP lease time on the console, the change is applied automatically when the DHCP lease of an instance (such as ECS) is renewed. You can wait for the system to renew the lease or manually renew the lease. Renewing lease will not change the IP address used by the instance. If you want the new lease time to take effect immediately, manually renew the lease or restart the ECS.</p>	-

Parameter	Description	Example Value
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses.</p> <p>If you do not specify this parameter, no additional NTP server IP addresses will be added.</p> <p>Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.</p>	192.168.2.1
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet.	<ul style="list-style-type: none"> ● Key: subnet_key1 ● Value: subnet-01
Description	<p>Supplementary information about the subnet. This parameter is optional.</p> <p>The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	N/A

Table 2-4 VPC tag key and value requirements

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

Table 2-5 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each subnet. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-). 	subnet_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	subnet-01

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

2.3 Step 2: Create a Subnet for the VPC

Scenarios

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

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

Procedure

1. Log in to the management console.



2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Network > Virtual Private Cloud**.
The **Virtual Private Cloud** page is displayed.
4. In the navigation pane on the left, choose **Virtual Private Cloud > Subnets**.
5. Click **Create Subnet**.
The **Create Subnet** page is displayed.
6. Set the parameters as prompted.

Table 2-6 Parameter descriptions

Parameter	Description	Example Value
VPC	The VPC for which you want to create a subnet.	-
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: <ul style="list-style-type: none"> • Subnets in a VPC can be in different AZs. For example, a VPC can have a subnet in AZ 1, and another subnet in AZ 3. • A cloud resource can be in a different AZ from its subnet. For example, a cloud server in AZ 1 can be in a subnet in AZ 3. 	AZ1
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

Parameter	Description	Example Value
IPv6 CIDR Block	<p>Specifies whether to set IPv6 CIDR Block to Enable.</p> <p>If you select this option, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.</p>	-
Associated Route Table	The default route table to which the subnet will be associated. You can change the route table to a custom route table on the Subnets page.	Default
Gateway	<p>The gateway address of the subnet.</p> <p>This IP address is used to communicate with other subnets.</p>	192.168.0.1
DNS Server Address	<p>DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.</p> <p>If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.</p> <p>A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).</p>	100.125.x.x

Parameter	Description	Example Value
NTP Server Address	<p>The IP address of the NTP server. This parameter is optional.</p> <p>You can configure the NTP server IP addresses to be added to the subnet as required. The IP addresses are added in addition to the default NTP server addresses. If you do not specify this parameter, no additional NTP server IP addresses will be added.</p> <p>Enter a maximum of four valid IP addresses, and separate multiple IP addresses with commas. Each IP address must be unique. If you add or change the NTP server addresses of a subnet, you need to renew the DHCP lease for or restart all the ECSs in the subnet to make the change take effect immediately. If the NTP server addresses have been cleared out, restarting the ECSs will not help. You must renew the DHCP lease for all ECSs to make the change take effect immediately.</p>	192.168.2.1
DHCP Lease Time	<p>The period during which a client can use an IP address automatically assigned by the DHCP server. After the lease time expires, a new IP address will be assigned to the client. Unit: Day or hour</p> <p>If the time period is changed, the new lease time takes effect when the instance (such as an ECS) in the subnet is renewed next time. You can wait for the instance to be renewed automatically or manually modify the lease time. If you want the new lease time to take effect immediately, manually renew the lease or restart the ECS.</p>	-
Tag	<p>The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet.</p> <p>The tag key and value must meet the requirements listed in Table 2-7.</p>	<ul style="list-style-type: none"> • Key: subnet_key1 • Value: subnet-01
Description	<p>Supplementary information about the subnet. This parameter is optional.</p> <p>The subnet description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-

Table 2-7 Subnet tag key and value requirements

Parameter	Requirements	Example Value
Key	<ul style="list-style-type: none">• Cannot be left blank.• Must be unique for each subnet.• Can contain a maximum of 36 characters.• Can contain letters, digits, underscores (_), and hyphens (-).	subnet_key1
Value	<ul style="list-style-type: none">• Can contain a maximum of 43 characters.• Can contain letters, digits, underscores (_), periods (.), and hyphens (-).	subnet-01

7. Click **OK**.

Precautions

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

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


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

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 select the desired region and project.


3. Click  in the upper left corner and choose **Network > Elastic IP**.
4. On the displayed page, click **Assign EIP**.
5. Set the parameters as prompted.

Table 2-8 Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you. The region selected for the EIP is its geographical location.	N/A
EIP Type	Dynamic BGP: Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
Billed By	The following bandwidth types are available: <ul style="list-style-type: none"> • Bandwidth: You specify a maximum bandwidth and pay for the amount of time you use the bandwidth. This is suitable for scenarios with heavy or stable traffic. • Traffic: You specify a maximum bandwidth and pay for the total traffic you use. This is suitable for scenarios with light or sharply fluctuating traffic. • Shared Bandwidth: The bandwidth can be shared by multiple EIPs and is suitable for scenarios with staggered traffic. 	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth

Parameter	Description	Example Value
Tag	The EIP tags. Each tag contains a key and value pair. The tag key and value must meet the requirements listed in Table 2-10 .	<ul style="list-style-type: none"> • Key: ipv4_key1 • Value: 3005eip
Quantity	The number of EIPs you want to purchase.	1
Enterprise Project	The enterprise project that the EIP belongs to. An enterprise project lets you manage cloud resources and personnel by enterprise project. The default project is default . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default

Table 2-9 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.	-
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth

Table 2-10 EIP tag requirements

Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each EIP. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-). 	Ipv4_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	3005eip

6. Click **Create 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 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.

When creating an instance (for example, an ECS), you must associate it with a security group. If no security group has been created yet, a default security group will be created and associated with the instance. You can also create a security group and add inbound and outbound rules to allow specific traffic.

Security Group Templates



Several security group templates are provided for you to create a security group. A security group template has preconfigured inbound and outbound rules. You can select a template based on your service requirements. [Table 2-11](#) describes the security group templates.

Table 2-11 Security group templates

Template	Direction	Protocol/Port/Type	Source/Destination	Description	Application Scenario
General - purpose web server	Inbound	TCP: 22 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 22 (SSH) for remotely logging in to Linux ECSs.	<ul style="list-style-type: none"> Remotely log in to ECSs. Use the ping command to test ECS connectivity. ECSs functioning as web servers provide website access services.
		TCP: 3389 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 3389 (RDP) for remotely logging in to Windows ECSs.	
		TCP: 80 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 80 (HTTP) for visiting websites.	
		TCP: 443 (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over port 443 (HTTPS) for visiting websites.	
		ICMP: All (IPv4)	0.0.0.0/0	Allows all IPv4 addresses to access ECSs in the security group over any port for using the ping command to test ECS connectivity.	
		All (IPv4) All (IPv6)	sg-xxx	Allows ECSs in the security group to communicate with each other.	
	Outbound	All (IPv4) All (IPv6)	0.0.0.0/0 ::/0	Allows access from ECSs in the security group to any IP address over any port.	

Template	Direction	Protocol/Port/Type	Source/Destination	Description	Application Scenario
All ports open	Inbound	All (IPv4) All (IPv6)	sg-xxx	Allows ECSs in the security group to communicate with each other.	Opening all ECS ports in a security group poses security risks.
		All (IPv4) All (IPv6)	0.0.0.0/0 ::/0	Allows all IP addresses to access ECSs in the security group over any port.	
	Outbound	All (IPv4) All (IPv6)	0.0.0.0/0 ::/0	Allows access from ECSs in the security group to any IP address over any port.	
Fast-add rule	Inbound	All (IPv4) All (IPv6)	sg-xxx	Allows ECSs in the security group to communicate with each other.	You can select protocols and ports that the inbound rule will apply to.
		Custom port and protocol	0.0.0.0/0	Allows all IP addresses to access ECSs in a security group over specified ports (TCP or ICMP) for different purposes.	
	Outbound	All (IPv4) All (IPv6)	0.0.0.0/0 ::/0	Allows access from ECSs in the security group to any IP address over any port.	

Procedure

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

- The **Create Security Group** page is displayed.
- Configure the parameters as prompted.

Figure 2-2 Create Security Group

Create Security Group ×

★ Name

★ Enterprise Project [Create Enterprise Project](#)

★ Template

Description

The security group is for general-purpose web servers and includes default rules that allow all inbound ICMP traffic and inbound traffic on ports 22, 80, 443, and 3389. The security group is used for remote login, ping, and hosting a website on ECSs.

0/255

[Hide Default Rule](#) ▲

Inbound Outbound

Prio...	Action	Type	Protocol & Port	Source
1	Allow	IPv4	TCP: 22	0.0.0.0/0
1	Allow	IPv4	TCP: 3389	0.0.0.0/0
1	Allow	IPv4	TCP: 80	0.0.0.0/0
1	Allow	IPv4	TCP: 443	0.0.0.0/0
1	Allow	IPv4	ICMP: All	0.0.0.0/0
1	Allow	IPv4	All	sg-AB

Table 2-12 Parameter description

Parameter	Description	Example Value
Name	<p>Mandatory</p> <p>Enter the security group name.</p> <p>The security group name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.</p> <p>NOTE You can change the security group name after a security group is created. It is recommended that you give each security group a different name.</p>	sg-AB
Enterprise Project	<p>Mandatory</p> <p>When creating a security group, you can add the security group to an enabled enterprise project. An enterprise project lets you manage cloud resources and personnel by enterprise project. The default project is default.</p> <p>For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i>.</p>	default
Template	<p>Mandatory</p> <p>Several security group templates are provided for you to create a security group. A security group template has preconfigured inbound and outbound rules. You can select a template based on your service requirements.</p>	General-purpose web server
Description	<p>Optional</p> <p>Supplementary information about the security group.</p> <p>The description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).</p>	-

7. 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 2-13 Inbound rule parameter description

Parameter	Description	Example Value
Type	Source IP address version. You can select: <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
Protocol & Port	The network protocol used to match traffic in a security group rule. The value can be All , TCP , UDP , GRE , and ICMP .	TCP
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Inbound rules control incoming traffic over specific ports to instances in the security group.	22, or 22-30
Source	Source of the security group rule. The value can be an IP address or a security group to allow access from IP addresses or instances in the security group. If you select IP address for Source , you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule. <ul style="list-style-type: none"> • IP address: <ul style="list-style-type: none"> - Single IP address: 192.168.10.10/32 - All IP addresses: 0.0.0.0/0 - IP address range: 192.168.1.0/24 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

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

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

Table 2-14 Outbound rule parameter description

Parameter	Description	Example Value
Type	Destination IP address version. You can select: <ul style="list-style-type: none"> • IPv4 • IPv6 	IPv4
Protocol & Port	The network protocol used to match traffic in a security group rule. The value can be All , TCP , UDP , GRE , and ICMP .	TCP
	Destination port used to match traffic in a security group rule. The value can be from 1 to 65535. Outbound rules control outgoing traffic over specific ports from instances in the security group.	22, or 22-30
Destination	Destination of the security group rule. The value can be an IP address or a security group to allow access to IP addresses or instances in the security group. For example: If you select IP address for Destination , you can enter multiple IP addresses in the same IP address box. Each IP address represents a different security group rule. <ul style="list-style-type: none"> • IP address: <ul style="list-style-type: none"> - Single IP address: 192.168.10.10/32 - All IP addresses: 0.0.0.0/0 - IP address range: 192.168.1.0/24 	0.0.0.0/0

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

10. Click **OK**.

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

Verifying Security Group Rules

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

For example, if you have deployed a website on an ECS and want users to access your website through HTTP (80), you need to add an inbound rule to the ECS security group to allow access over the port. [Table 2-15](#) shows the rule.

Table 2-15 Security group rule

Direction	Type	Protocol & Port	Source
Inbound	IPv4	TCP: 80	IP address: 0.0.0.0/0

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

1. Log in to the ECS and check whether the ECS port is opened.

– **Checking the port of a Linux server**

Run the following command to check whether TCP port 80 is being listened on:

netstat -an | grep 80

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

Figure 2-3 Command output for the Linux ECS

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

– **Checking the port of a Windows server**

i. Choose **Start > Run**. Type **cmd** to open the Command Prompt.

ii. Run the following command to check whether TCP port 80 is being listened on:

netstat -an | findstr 80

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

Figure 2-4 Command output for the Windows ECS

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

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

3 Elastic IP

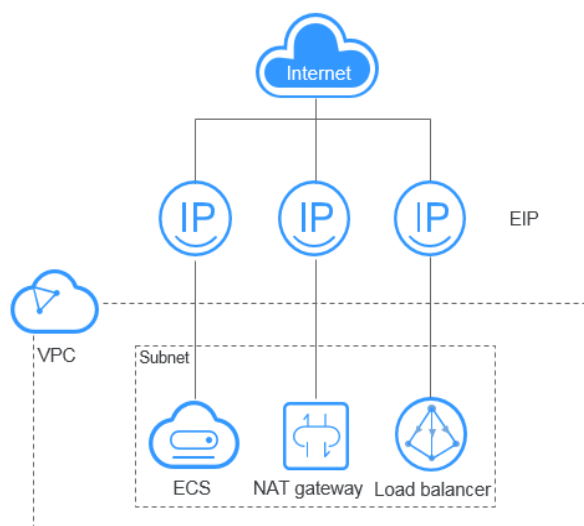
3.1 EIP Overview

EIP

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, BMSs, virtual IP addresses, NAT gateways, or load balancers.

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

Figure 3-1 Connecting to the Internet using an EIP



3.2 Assigning an EIP and Binding It to an ECS

Scenarios

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

Assigning an EIP



1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Network > Elastic IP**.
4. On the displayed page, click **Assign EIP**.
5. 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
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	<p>The following bandwidth types are available:</p> <ul style="list-style-type: none"> • Bandwidth: You specify a maximum bandwidth and pay for the amount of time you use the bandwidth. This is suitable for scenarios with heavy or stable traffic. • Traffic: You specify a maximum bandwidth and pay for the total traffic you use. This is suitable for scenarios with light or sharply fluctuating traffic. • Shared Bandwidth: The bandwidth can be shared by multiple EIPs and is suitable for scenarios with staggered traffic. 	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth
Tag	<p>The EIP tags. Each tag contains a key and value pair.</p> <p>The tag key and value must meet the requirements listed in Table 3-3.</p>	<ul style="list-style-type: none"> • Key: Ipv4_key1 • Value: 3005eip
Quantity	The number of EIPs you want to purchase.	1
Enterprise Project	<p>The enterprise project that the EIP belongs to.</p> <p>An enterprise project lets you manage cloud resources and personnel by enterprise project. The default project is default.</p> <p>For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i>.</p>	default

Table 3-2 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.	-
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth

Table 3-3 EIP tag requirements

Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each EIP. Can contain a maximum of 36 characters. Can contain letters, digits, underscores (_), and hyphens (-). 	Ipv4_key1
Value	<ul style="list-style-type: none"> Can contain a maximum of 43 characters. Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	3005eip

6. Click **Create 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 that you want to bind the EIP to.
3. Click **OK**.

3.3 Assigning an EIP

Scenarios

Assign an EIP for a cloud resource you want to make it accessible over the Internet.

NOTE

If you want to assign an EIP that you have released or assign a specific EIP, you can use APIs. When assigning an EIP, set the value of **ip_address** to the IP address that you want to assign. For details, see section "Assigning an EIP" in *Elastic IP API Reference*.

- If the EIP has been assigned to another user, you will fail to assign your required EIP.
- The management console does not support assigning a specific EIP.

Procedure



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

Table 3-4 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	<p>The following bandwidth types are available:</p> <ul style="list-style-type: none"> • Bandwidth: You specify a maximum bandwidth and pay for the amount of time you use the bandwidth. This is suitable for scenarios with heavy or stable traffic. • Traffic: You specify a maximum bandwidth and pay for the total traffic you use. This is suitable for scenarios with light or sharply fluctuating traffic. • Shared Bandwidth: The bandwidth can be shared by multiple EIPs and is suitable for scenarios with staggered traffic. 	Bandwidth
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth
Tag	<p>The EIP tags. Each tag contains a key and value pair.</p> <p>The tag key and value must meet the requirements listed in Table 3-6.</p>	<ul style="list-style-type: none"> • Key: lpv4_key1 • Value: 3005eip
Quantity	The number of EIPs you want to purchase.	1
Enterprise Project	<p>The enterprise project that the EIP belongs to.</p> <p>An enterprise project lets you manage cloud resources and personnel by enterprise project. The default project is default.</p> <p>For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i>.</p>	default

Table 3-5 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.	-
Bandwidth	The bandwidth size in Mbit/s.	100
Bandwidth Name	The name of the bandwidth.	bandwidth

Table 3-6 EIP tag requirements

Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none"> Cannot be left blank. Must be unique for each EIP. Can contain a maximum of 36 characters. Can contain letters, digits, underscores (_), and hyphens (-). 	Ipv4_key1
Value	<ul style="list-style-type: none"> Can contain a maximum of 43 characters. Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	3005eip

6. Click **Create Now**.
7. Click **Submit**.

3.4 Binding an EIP to an Instance

Procedure

Binding an EIP to an ECS or a virtual IP address

1. In the EIP list, locate the row that contains the EIP, and click **Bind**.
2. Select the instance.

3. Click **OK**.

NOTE

To bind an instance to an EIP:

- If the instance is an ECS:
 - The ECS must be in the running or stopped status.
 - The ECS must be in the same region as that of the EIP.
 - The ECS has no fixed public IP address or any other EIP.
- If the instance is a virtual IP address:
 - The virtual IP address must be in the same region as that of the EIP.
 - The virtual IP address must be in the available or assigned status.

Binding an EIP to a NAT gateway

If you want to bind a NAT gateway to an EIP, the NAT gateway must be in the same region as that of the EIP. After an EIP is bound to a NAT gateway, ECSs associated with this gateway can share the EIP to access the Internet or provide services accessible from the Internet.

You can bind an EIP to a NAT gateway by configuring SNAT and DNAT rules for the gateway. Sections "Allowing a Private Network to Access the Internet Using SNAT" and "Allowing Internet Users to Access a Service in a Private Network Using DNAT" in the *NAT Gateway User Guide*.

Binding an EIP to a load balancer

If you want to bind a load balancer to an EIP, the load balancer must be in the same region as that of the EIP. Then, the load balancer can receive requests over the Internet. For details, see "Binding or Unbinding an EIP" in *Elastic Load Balance User Guide*.

3.5 Unbinding an EIP from an Instance

Scenarios


Unbind an EIP from an instance, if:

- Your instance does not need to use an EIP.
- You want to bind the EIP to another instance.

Notes and Constraints

- EIPs assigned and bound to load balancers in the ELB service are displayed in the EIP list of the VPC service.


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 target EIP, and click **Unbind** in the **Operation** column.

A confirmation dialog box is displayed.

4. Click **Yes** in the displayed dialog box.
In the EIP list, the target EIP has no associated instance.

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. In the upper left corner of the EIP list, click **Unbind**.
A confirmation dialog box is displayed.
5. Click **Yes** in the displayed dialog box.
In the EIP list, the target EIPs have no associated instances.

3.6 Releasing an EIP


Scenarios

If an EIP is no longer required, you can unbind it from your instance and then release it.


Notes and Constraints

- Only EIPs that have no instances bound can be released. To release an EIP that has been bound to an instance, unbind it first. For details, see [Unbinding an EIP from an Instance](#).

Releasing a Single EIP

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Elastic IP**.
3. In the EIP list, locate the row that contains the EIP and choose **More > Release** in the **Operation** column.
A confirmation dialog box is displayed.
4. Click **Yes** in the displayed dialog box.
You can find that the EIP is not in the EIP list.

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. In the EIP list, select the EIPs to be released.
4. In the upper left corner of the list, choose **More > Release**.
A confirmation dialog box is displayed.
5. Click **Yes** in the displayed dialog box.
You can find that the EIPs are not in the EIP list.


3.7 Changing Dedicated Bandwidth Size of an EIP

Scenarios

No matter which billing mode is used, if your EIP is not added to a shared bandwidth, it uses a dedicated bandwidth. A dedicated bandwidth can control how much data can be transferred using a single EIP.

This section describes how to increase or decrease the bandwidth size. Changing bandwidth size does not change the EIPs.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Elastic IP**.
3. Locate the row that contains the target EIP in the EIP list, and click **More > Modify Bandwidth** in the **Operation** column.
 - If it is a pay-per-use EIP, the **Modify Bandwidth** page is displayed.
4. Change the bandwidth size as prompted.

 **NOTE**

5. Click **Next**.
6. Click **Submit**.

3.8 Unbinding an EIP from an ECS and Releasing the EIP

Scenarios


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


Notes and Constraints

- Only EIPs with no instance bound can be released. If you want to release an EIP with an instance bound, you need to unbind EIP from the instance first.
- You cannot buy an EIP that has been released if it is currently in use by another user.



Procedure

Unbinding a single EIP



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

3. Click  in the upper left corner and choose **Network > Elastic IP**.
4. On the displayed page, locate the row that contains the EIP, and click **Unbind**.
5. Click **Yes** in the displayed dialog box.



Releasing a single EIP

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

Unbinding multiple EIPs at once

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

Releasing multiple EIPs at once

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

3.9 Modifying an EIP Bandwidth



Scenarios

No matter which billing mode is used, if your EIP is not added to a shared bandwidth, it uses a dedicated bandwidth. A dedicated bandwidth can control how much data can be transferred using a single EIP.

This section describes how to increase or decrease the bandwidth size. Changing bandwidth size does not change the EIPs.

Procedure

1. Log in to the management console.


2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Network > 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**.

3.10 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.

3.11 Managing EIP Tags

Scenarios

Tags can be added to EIPs to facilitate EIP identification and administration. You can add a tag to an EIP when assigning the EIP. Alternatively, you can add a tag to an assigned EIP on the EIP details page. A maximum of 10 tags can be added to each EIP.


A tag consists of a key and value pair. [Table 3-7](#) lists the tag key and value requirements.

Table 3-7 EIP tag requirements


Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none"> • Cannot be left blank. • Must be unique for each EIP. • Can contain a maximum of 36 characters. • Can contain letters, digits, underscores (_), and hyphens (-). 	Ipv4_key1
Value	<ul style="list-style-type: none"> • Can contain a maximum of 43 characters. • Can contain letters, digits, underscores (_), periods (.), and hyphens (-). 	3005eip

Procedure

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

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Elastic IP**.
3. In the search box above the EIP list, click anywhere in the box to set filters.
Select the tag key and then the value as required. The system filters resources based on the tag you select.

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

1. Log in to the management console.
2. Click  in the upper left corner and choose **Network > Elastic IP**.
3. On the displayed page, locate the EIP whose tags you want to manage, and click the EIP name.
4. On the page showing EIP details, click the **Tags** tab and perform desired operations on tags.
 - View tags.
On the **Tags** tab, you can view details about tags added to the current EIP, including the number of tags and the key and value of each tag.
 - Add a tag.
Click **Add Tag** in the upper left corner. In the displayed **Add Tag** dialog box, enter the tag key and value, and click **OK**.
 - Edit a tag.
Locate the row that contains the tag you want to edit, and click **Edit** in the **Operation** column. Enter the new tag value, and click **OK**.
The tag key cannot be modified.
 - Delete a tag.

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

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.

- Lowered Bandwidth Costs
Region-level bandwidth sharing and multiplexing reduce bandwidth usage and O&M costs.
- Easy to Manage
Region-level bandwidth sharing and multiplexing simplify O&M statistics, management, and operations cost settlement.
- Flexible Operations
You can add pay-per-use EIPs (except for **5_gray** EIPs of dedicated load balancers) to or remove them from a shared bandwidth regardless of the type of instances that they are bound to.

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 select the desired region and project.
3. Click  in the upper left corner and choose **Network > 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.

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.	N/A
Billed By	The billing method for the shared bandwidth. You can specify a shared bandwidth to be billed by bandwidth.	Bandwidth
Bandwidth	The bandwidth size in Mbit/s. The maximum bandwidth can be 300 Mbit/s.	10
Name	The name of the shared bandwidth.	Bandwidth-001
Enterprise Project	The enterprise project that the EIP belongs to. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is default . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default

6. 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.
- If it is a standard shared bandwidth, you can add dynamic BGP EIPs and IPv6 NICs to it. If it is a premium shared bandwidth, you can add premium BGP EIPs and IPv6 NICs to it.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner and choose **Network > 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 target shared bandwidth that you want to add EIPs to. In the **Operation** column, choose **Add Public IP Address**, and select the EIPs to be added.

NOTE



- After an EIP is added to a shared bandwidth, the dedicated bandwidth used by the EIP will become invalid and the EIP will start to use the shared bandwidth. The EIP's dedicated bandwidth will be deleted and will no longer be billed.
6. 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 select the desired region and project.
3. Click  in the upper left corner and choose **Network > 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 target shared bandwidth from which EIPs are to be removed, choose **More > Remove Public IP Address** in the **Operation** column, and select the EIPs to be removed in the displayed dialog box.
6. 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 select the desired region and project.
3. Click  in the upper left corner and choose **Network > 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.
6. Click **Next**.
7. 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 select the desired region and project.
3. Click  in the upper left corner and choose **Network > 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 **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 (Previously called "Upstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute

ID	Name	Description	Value Range	Monitored Object	Monitoring Interval (Raw Data)
downstream_bandwidth	Inbound Bandwidth	Network rate of inbound traffic (Previously called "Downstream Bandwidth") Unit: bit/s	≥ 0 bit/s	Bandwidth or EIP	1 minute
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth in the unit of percent. Outbound bandwidth usage = Outbound bandwidth/ Purchased bandwidth	0% to 100%	Bandwidth or EIP	1 minute
upstream	Outbound Traffic	Network traffic going out of the cloud platform (Previously called "Upstream Traffic") Unit: byte	≥ 0 Bytes	Bandwidth or EIP	1 minute
downstream	Inbound Traffic	Network traffic going into the cloud platform (Previously called "Downstream Traffic") 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, period, resource type, dimension, monitored object, and metric.
6. Click **Export**.

NOTE

You can export data for multiple metrics at a time to a CSV file.

- 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:
$$\text{Target time} = [\text{Unix timestamp}/1000 + (\text{Target time zone}) \times 3600]/86400 + 70 \times 365 + 19$$
 - c. Set cell format to **Date**.

6 FAQs

6.1 Product Consultation



6.1.1 What Is a Quota?

What Is a Quota?

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

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

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, click  .
The **Service Quota** page is displayed.
4. View the used and total quota of each type of resources on the displayed page.
If a quota cannot meet service requirements, apply for a higher quota.

How Do I Apply for a Higher Quota?

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

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

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

6.1.2 How Do I Assign or Retrieve a Specific EIP?

If you want to retrieve an EIP that you have released or assign a specific EIP, you can use APIs by setting the value of **ip_address** to the one that you want to assign. For details, see section "Assigning an EIP" in *Elastic IP API Reference*.

NOTE

- If the EIP has been assigned to another user, you will fail to assign your required EIP.
- You cannot use the management console to assign a specific EIP.

6.1.3 Why Is an EIP Newly Assigned the Same as the One I Released?

If you have released EIPs in a region, the system preferentially assigns EIPs from the ones you released in the last 24 hours.

If you do not want an EIP that you have released, assign an EIP first and then release the one that you do not want.

You can assign a specific EIP by calling APIs. For details, see section "Assigning an EIP" in *Elastic IP API Reference*.

6.1.4 What Are the Differences Between EIP, Private IP Address, and Virtual IP Address?

Different types of IP addresses have different functions.

Figure 6-1 IP address architecture

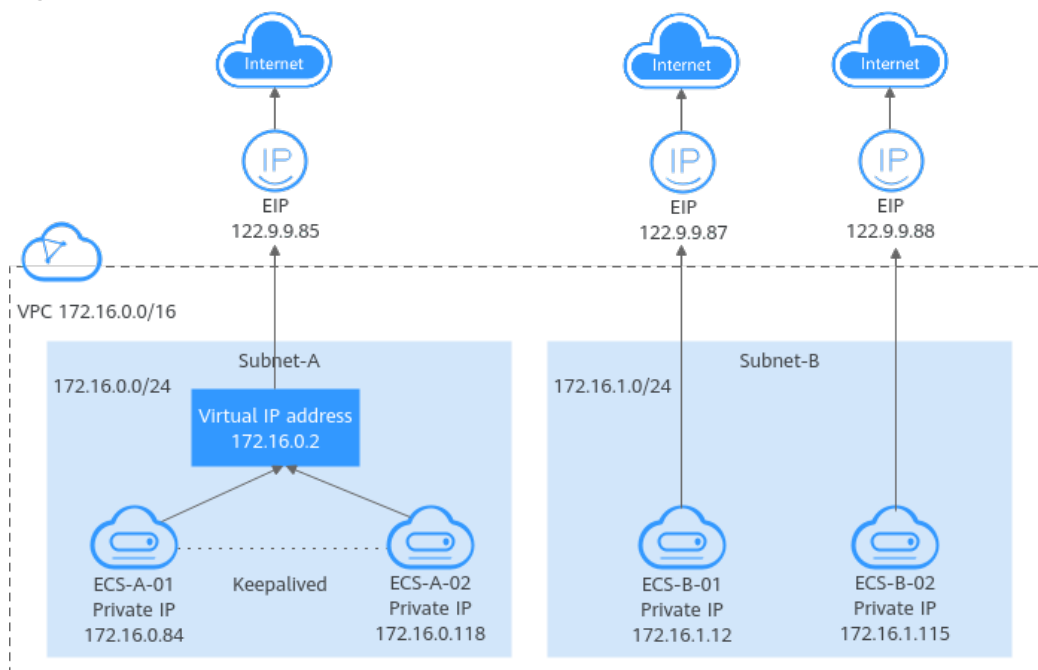


Table 6-1 Functions of different IP address types

IP Address Type	Description	Example Value
Private IP address	Private IP addresses come with your ECSs and belong to the VPC subnets of the ECSs. They are used for private communication on the cloud.	<ul style="list-style-type: none"> • Private IP address of ECS-A-01: 172.16.0.84 • Private IP address of ECS-B-01: 172.16.1.12
Virtual IP address	<p>A virtual IP address can be shared among multiple ECSs. Two ECSs can work as an active and standby pair to achieve high availability by using a virtual IP address and Keepalived. If the active ECS is faulty, the virtual IP address can be dynamically switched to the standby ECS to continue providing services.</p> <p>For more information about virtual IP addresses, see section "Virtual IP Address Overview" in the <i>Virtual Private Cloud User Guide</i>.</p>	Bind virtual IP address (172.16.0.2) both ECS-A-01 and ECS-A-02. The active/standby switchover of ECS-A-01 and ECS-A-02 can be implemented by using Keepalived.
EIP	<p>EIPs allow cloud resources to access the Internet. They can be flexibly bound to or unbound from instances.</p> <ul style="list-style-type: none"> • You can bind an EIP to a virtual IP address to enable the ECSs with the virtual IP address bound to access the Internet. • You can also bind an EIP to the ECSs to enable them to access the Internet. 	<ul style="list-style-type: none"> • Bind EIP (122.9.9.85) to virtual IP address (172.16.0.2) to enable ECS-A-01 and ECS-A-02 to access the Internet. • Bind EIP (122.9.9.87) to ECS-B-01 to enable ECS-B-01 to access the Internet.

6.1.5 Can an EIP That Uses Dedicated Bandwidth Be Changed to Use Shared Bandwidth?

Yes. An EIP that uses a dedicated bandwidth can be changed to use a shared bandwidth.

6.1.6 Can I Bind an EIP to Multiple ECSs?

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

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

6.1.7 What Are the Differences Between the Primary and Extension NICs of ECSs?

The differences are as follows:

- Generally, the OS default routes preferentially use the primary NICs. If the OS default routes use the extension NICs, network communication will be interrupted. Then, you can check the route configuration to rectify the network communication error.
- Primary NICs can communicate with the public service zone (zone where PaaS and DNS services are deployed). Extension NICs cannot communicate this zone.

6.1.8 What Is the EIP Assignment Policy?

By default, EIPs are assigned randomly.

If an EIP is released by mistake, the system will preferentially assign you an EIP that you have released in the last 24 hours.

If you want a specific EIP that you released more than 24 hours ago, see [How Do I Assign or Retrieve a Specific EIP?](#)

If you do not want an EIP that you have released, it is recommended that you buy another EIP first and then release the one that you do not need.

6.1.9 Can I Assign a Specific EIP?

By default, EIPs are assigned randomly. If you have released EIPs, the system preferentially assigns EIPs from the ones you released.


You can assign a specific EIP only by calling an API. For details, see section "Assigning an EIP" in the *Elastic IP API Reference*.


6.1.10 Can a Bandwidth Be Used by Multiple Accounts?



A bandwidth cannot be shared between different accounts. Each account can use and manage only its own EIP bandwidths.

6.1.11 How Do I Unbind an EIP from an Instance and Bind a New EIP to the Instance?

Scenario 1: Unbinding an EIP from an ECS and Binding a New EIP to the ECS


1. Unbind an EIP.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and choose **Network > Elastic IP**.
 - c. On the displayed page, locate the row that contains the target EIP, and click **Unbind**.

- d. Click **Yes**.
2. Assign an EIP.
 -  **NOTE**

If you already have an EIP that you require, skip this step.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and choose **Network > Elastic IP**.
 - c. On the displayed page, click **Assign EIP**.
 - d. Set the parameters as prompted.
 - e. Click **Next**.
3. Bind the new EIP to the ECS.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and choose **Network > Elastic IP**.
 - c. On the **EIPs** page, locate the row that contains the target EIP, and click **Bind**.
 - d. Select the desired ECS.
 - e. Click **OK**.
4. Release the EIP that is unbound.

 **NOTE**

If an unbound EIP is no longer required, you can release it.

- a. Log in to the management console.
- b. Click  in the upper left corner and choose **Network > Elastic IP**.
- c. In the EIP list, locate the row that contains the EIP, and choose **More > Release** in the **Operation** column.
- d. Click **Yes**.

Scenario 2: Unbinding an EIP from a Load Balancer and Binding a New EIP to the Load Balancer

1. Unbind an EIP.
 - a. Log in to the management console.
 - b. Click **Service List**. Under **Network**, click **Elastic Load Balance**.
 - c. In the load balancer list, locate the target load balancer and choose **More > Unbind EIP** in the **Operation** column.
 - d. Click **Yes**.
2. Assign an EIP by referring to [2](#).

 **NOTE**

If you already have an EIP that you require, skip this step.

3. Bind the new EIP to the load balancer.
 - a. Log in to the management console.

- b. Click **Service List**. Under **Network**, click **Elastic Load Balance**.
 - c. In the load balancer list, locate the target load balancer and choose **More > Bind EIP** in the **Operation** column.
 - d. In the **Bind EIP** dialog box, select the EIP to be bound and click **OK**.
4. Release the EIP that was replaced. For details, see [4](#).

 **NOTE**

If an unbound EIP is no longer required, you can release it.

Scenario 3: Unbinding an EIP from a NAT Gateway and Binding a New EIP to the NAT Gateway

1. Assign an EIP by referring to [2](#).

 **NOTE**

If you already have an EIP that you require, skip this step.

2. Modify an SNAT rule.

For details, see section "Modifying an SNAT Rule" of a public NAT gateway in *NAT Gateway User Guide*. In the EIP list, select the new EIP and deselect the existing EIP.

3. Modify a DNAT rule.

For details, see section "Modifying a DNAT Rule" of a public NAT gateway in the *NAT Gateway User Guide*.

4. Release the EIP that was replaced. For details, see [4](#).

 **NOTE**

If an unbound EIP is no longer required, you can release it.

6.1.12 Why Can't I Find My Assigned EIP on the Management Console?

Symptom

After I logged in to the management console, I could not find my assigned EIP.

Possible Cause

Your EIP is not in the current region. For details, see [EIP Not in the Current Region](#).

EIP Not in the Current Region

Step 1 Log in to the management console.

Step 2 Locate the EIP.

1. In the upper left corner of the console, select the region to which the EIP to be queried belongs.

2. In the EIP list, view the assigned EIP.

----End

6.2 EIP Binding and Unbinding

6.2.1 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 (except TCP traffic from port 22 through SSH to a Linux ECS and TCP traffic from port 3389 through RDP to a Windows ECS). To allow external access to ECSs in the security group, add an inbound rule to the security group.

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

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

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

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

6.2.2 How Do I Access the Internet Using an EIP Bound to an Extension NIC?

1. After an EIP is bound to an extension NIC, log in to the ECS and use the **route** command to query the routes.

You can run **route --help** to learn more about the **route** command.

Figure 6-2 Viewing route information

```
[root@ecs-b926 ~]# route -n
Kernel IP routing table
Destination      Gateway         Genmask        Flags Metric Ref    Use Iface
0.0.0.0          192.168.11.1   0.0.0.0        UG    0     0     0 eth0
169.254.0.0     0.0.0.0        255.255.0.0    U     1002  0     0 eth0
169.254.0.0     0.0.0.0        255.255.0.0    U     1003  0     0 eth1
169.254.169.254 192.168.11.1   255.255.255.255 UGH   0     0     0 eth0
192.168.11.0    0.0.0.0        255.255.255.0  U     0     0     0 eth0
192.168.17.0    0.0.0.0        255.255.255.0  U     0     0     0 eth1
[root@ecs-b926 ~]#
```

2. Run the **ifconfig** command to view NIC information.

Figure 6-3 Viewing NIC information

```
root@ecs-b926 ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.11.42 netmask 255.255.255.0 broadcast 192.168.11.255
    inet6 fe80::f816:3eff:fe17:1c44 prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:f7:1c:44 txqueuelen 1000 (Ethernet)
    RX packets 127 bytes 21633 (21.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 258 bytes 22412 (21.8 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.17.191 netmask 255.255.255.0 broadcast 192.168.17.255
    inet6 fe80::f816:3eff:fe1c:b57f prefixlen 64 scopeid 0x20<link>
    ether fa:16:3e:1c:b5:7f txqueuelen 1000 (Ethernet)
    RX packets 11 bytes 1283 (1.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1388 (1.3 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1 (Local Loopback)
    RX packets 51 bytes 12018 (11.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 51 bytes 12018 (11.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

3. Enable access to the Internet through the extension NIC by default.
 - a. Run the following command to delete the default route of the primary NIC:

```
route del -net 0.0.0.0 gw 192.168.11.1 dev eth0
```

192.168.11.1 is the gateway of the subnet that the NIC works. You can view the gateway on the **Summary** tab page of the subnet on the management console.

NOTE

This operation will interrupt ECS communication. It is recommended that you perform the configuration by following step 4.

- b. Run the following command to configure the default route for the extension NIC:

```
route add default gw 192.168.17.1
```

4. Configure Internet access from the extension NIC based on your destination address.

Run the following command to configure access to a specified CIDR block (for example, *xx.xx.0.0/16*) through the extension NIC:

You can configure the CIDR block as required.

```
route add -net xx.xx.0.0 netmask 255.255.0.0 gw 192.168.17.1
```

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

Yes.

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

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

6.2.4 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 6-2](#) lists ECS configurations.

Table 6-2 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**.

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

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

6.3 Bandwidth

6.3.1 What Is the Bandwidth Size Range?

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

6.3.2 How Do I Increase a Bandwidth to Be More Than 300 Mbit/s?

Symptom

The bandwidth of a pay-per-use EIP billed by traffic cannot be increased to be more than 300 Mbit/s.

Solution

If a higher bandwidth is required, you need to change the EIP to be billed by bandwidth. Then, your bandwidth can be increased to a maximum of 2000 Mbit/s.

If your bandwidth usage is high, billing by bandwidth is more cost-effective than billing by traffic. For details, see [Modifying an EIP Bandwidth](#).

6.3.3 What Bandwidth Types Are Available?

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

6.3.4 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?](#)

6.3.5 What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth?

A dedicated bandwidth can only be used by one EIP that is bound to one cloud resource, such as an ECS, a NAT gateway, or a load balancer.

A shared bandwidth can be shared by multiple EIPs. Adding an EIP to or removing an EIP from a shared bandwidth does not affect your services.

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.

6.3.6 What Are Inbound Bandwidth and Outbound Bandwidth?

Bandwidth refers to the maximum amount of data that can be transmitted in a given amount of time (generally one second). A larger bandwidth value indicates a stronger transmission capability. Bandwidth is classified into public bandwidth and private bandwidth.

Public bandwidth is the bandwidth consumed when data is transferred between cloud instances and the Internet. Public bandwidth is classified into inbound bandwidth and outbound bandwidth. For details the outbound bandwidth and inbound bandwidth, see [Table 6-3](#).

Figure 6-4 Inbound bandwidth and outbound bandwidth

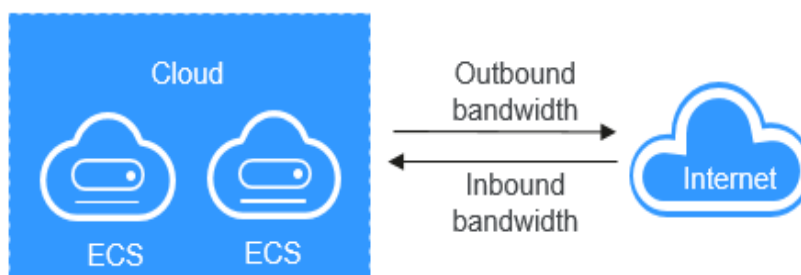


Table 6-3 Inbound bandwidth and outbound bandwidth

Type	Description
Outbound bandwidth	Bandwidth consumed when data is transferred from cloud to the Internet. For example, the outbound bandwidth is used when ECSs provide services accessible from the Internet and FTP clients download resources from the ECSs.

Type	Description
Inbound bandwidth	Bandwidth consumed when data is transferred from the Internet to cloud. For example, the inbound bandwidth is used when resources are downloaded from the Internet to ECSs and FTP clients upload resources to the ECSs.

6.3.7 How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?

Symptom

The bandwidth size configured when you assign a dedicated or shared bandwidth is the upper limit of the outbound bandwidth. If an ECS running your web applications cannot be accessed smoothly from the Internet, check whether the outbound bandwidth of the EIP bound to the ECS is greater than the configured bandwidth size.

 **NOTE**

If the outbound bandwidth exceeds the configured bandwidth size, there may be packet loss. To prevent data loss, it is recommended that you monitor the bandwidth.

Troubleshooting

The issues here are described in order of how likely they are to occur. Troubleshoot the issue by ruling out the causes described here, one by one.

Figure 6-5 Troubleshooting

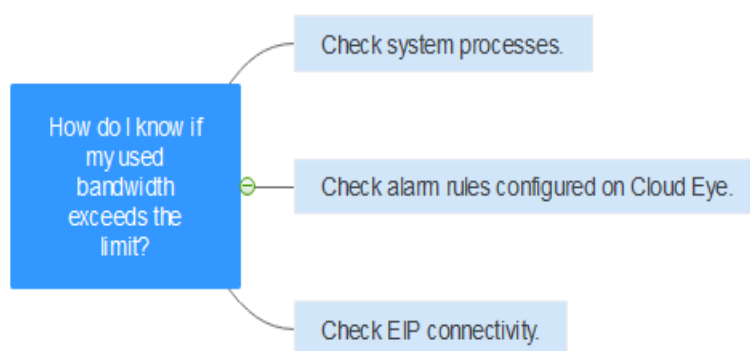


Table 6-4 Troubleshooting

Possible Cause	Description	Solution
System processes leading to high bandwidth	If some heavy-duty system processes or applications running on your ECS are causing the high bandwidth or CPU usage, your ECS will run slowly or may unexpectedly be inaccessible.	See System Processes Leading to High Bandwidth Usage
Improper Cloud Eye alarm rules	If you have created alarm rules for bandwidth usage on the Cloud Eye console, where the outbound bandwidth limit or the alarm period is set too small, the system may generate excessive alarms.	See Improper Cloud Eye Alarm Rules
EIP connection failure	An ECS with an EIP bound cannot access the Internet.	See section "Why Can't My ECS Access the Internet Even After an EIP Is Bound?" in the <i>Elastic IP User Guide</i> .

System Processes Leading to High Bandwidth Usage

If some heavy-duty system processes or applications running on your ECS are causing the high bandwidth or CPU usage, your ECS will run slowly or may unexpectedly be inaccessible.

You can refer to the following to locate the processes that have led to excessively high bandwidth or CPU usage, and optimize or stop the processes.

- Section "Why Is My Windows ECS Running Slowly?" in the "Elastic Cloud Server User Guide".
- Section "Why Is My Linux ECS Running Slowly?" in the "Elastic Cloud Server User Guide".

Improper Cloud Eye Alarm Rules

If you have created alarm rules for bandwidth usage on the Cloud Eye console, where the outbound bandwidth limit or the alarm period is set too small, the system may generate excessive alarms.

You need to set an appropriate alarm rule based on your assigned bandwidth. For example, if your purchased bandwidth is 5 Mbit/s, you can create an alarm rule to report an alarm when the maximum outbound bandwidth reaches 4.8 Mbit/s

three periods in a row. You can also increase your bandwidth. For details, see section "Modifying an EIP Bandwidth" in the *Elastic IP User Guide*.

1. Log in to the management console, under **Management & Deployment**, click **Cloud Eye**. On the **Cloud Eye** console, choose **Alarm Management > Alarm Rules**.
2. Click **Create Alarm Rule** and configure an alarm rule to generate alarms when the bandwidth exceeds the configured limit.

6.3.8 What Are the Differences Between Public Bandwidth and Private Bandwidth?

Public Bandwidth

Public bandwidth is the bandwidth consumed when data is transferred between cloud instances and the Internet. You can configure the public bandwidth when creating an ECS or bind an EIP to an ECS after the ECS is created.

Public bandwidth is classified into inbound bandwidth and outbound bandwidth.

Inbound bandwidth is the bandwidth consumed when data is transferred from the Internet to the cloud. For example, when resources are downloaded from the Internet to ECSs, that consumes inbound bandwidth.

Outbound bandwidth is the bandwidth consumed when data is transferred from the cloud to the Internet. For example, when ECSs provide services accessible from the Internet and external users download resources from the ECSs, that consumes outbound bandwidth.

Private Bandwidth

Private bandwidth is the bandwidth consumed when data is transferred between ECSs in the same region and on the same private network. ECSs can also be connected to cloud databases, load balancers, and OBS through private bandwidth. The private bandwidth size depends on the instance specifications.

For details, see section "ECS Types" in *Elastic Cloud Server Service Overview*.

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

The bandwidth is measured in bit/s, indicating the number of binary bits transmitted per second. The download rate is measured in byte/s, indicating the number of bytes transmitted per second.

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

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

6.4 Connectivity

6.4.1 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.

6.4.2 Why Can't My ECS Access the Internet Even After an EIP Is Bound?

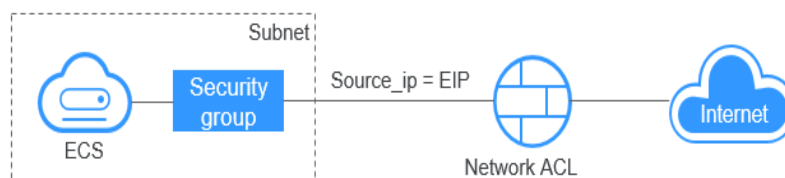
Symptom

An ECS with an EIP bound cannot access the Internet.

Troubleshooting

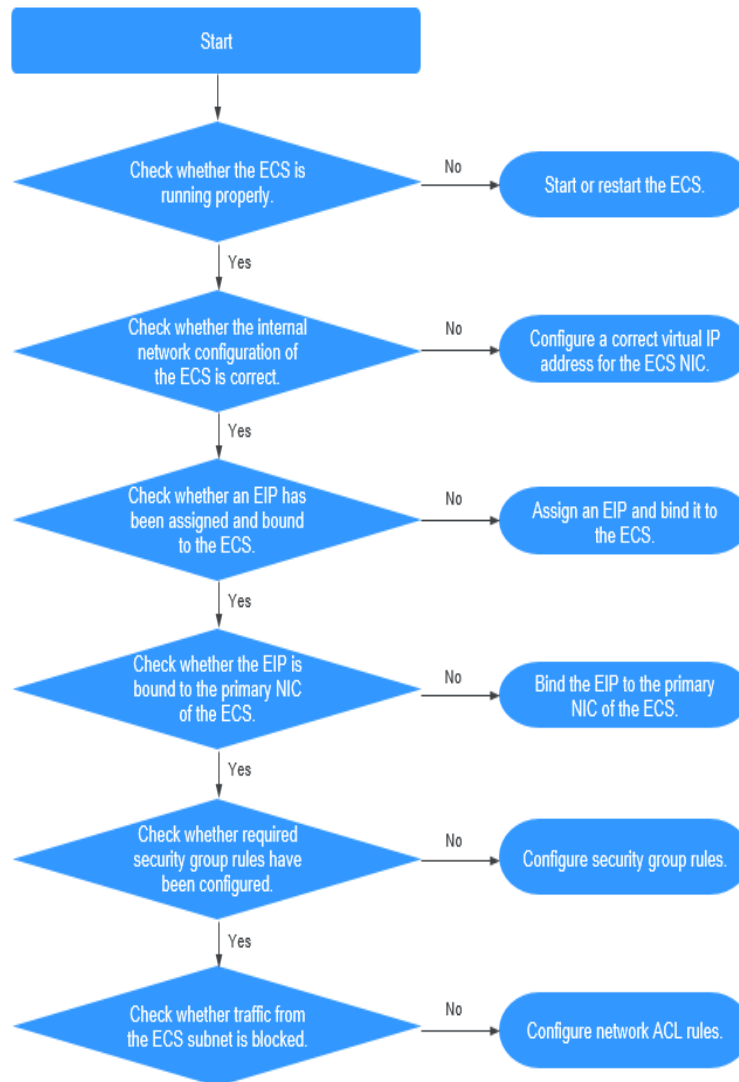
Figure 6-6 shows the networking diagram for an ECS to access the Internet using an EIP.

Figure 6-6 EIP network diagram



Locate the fault based on the following procedure.

Figure 6-7 Troubleshooting procedure



1. **Step 1: Check Whether the ECS Is Running Properly**
2. **Step 2: Check Whether the Network Configuration of the ECS Is Correct**
3. **Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECS**
4. **Step 4: Check Whether an EIP Is Bound to the Primary NIC of the ECS**
5. **Step 5: Check Whether Required Security Group Rules Have Been Configured.**
6. **Step 6: Check Whether Traffic from the ECS Subnet Is Blocked**

Step 1: Check Whether the ECS Is Running Properly

Check the ECS status.

If the ECS status is not **Running**, start or restart the ECS.

Step 2: Check Whether the Network Configuration of the ECS Is Correct

1. Check whether the ECS NIC has an IP address assigned.
Log in to the ECS, and run **ifconfig** or **ip address** to check the ECS NIC IP address.
If the ECS runs Windows, run **ipconfig**.
2. Check whether the ECS NIC has a virtual IP address.
Log in to the ECS, and run **ifconfig** or **ip address** to check whether the ECS NIC has a virtual IP address. If the ECS NIC has no virtual IP address, run the **ip addr add virtual IP address eth0** command to configure an IP address for the ECS NIC.

Figure 6-8 Virtual IP address of a NIC

```
[root@demoserver ~]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN
    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 qlen 1000
    link/ether fa:16:3e:37:7b:62 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.30/24 brd 192.168.1.255 scope global dynamic eth0
        valid_lft 84950sec preferred_lft 84950sec
    inet 192.168.1.192/24 scope global secondary eth0
        valid_lft forever preferred_lft forever
    inet6 fe80::f816:3eff:fe37:7b62/64 scope link
        valid_lft forever preferred_lft forever
```

Check whether the ECS NIC has a default route. If there is no default route, run **ip route add** to add one.

Figure 6-9 Default route

```
192.168.1.0/24 dev eth0 proto kernel scope link src 192.168.1.200
192.168.1.0/24 dev eth1 proto kernel scope link src 192.168.1.179
169.254.0.0/16 dev eth0 scope link metric 1002
default via 192.168.1.1 dev eth0 proto static
-bash-4.1#
```

Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECS

Check whether an EIP has been assigned and bound to the ECS. If no EIP has been assigned, assign an EIP and bind it to the ECS.

Step 4: Check Whether an EIP Is Bound to the Primary NIC of the ECS

Check whether an EIP is bound to the primary NIC of the ECS. If there is no EIP bound to the primary NIC of the ECS, bind one.

You can view the NIC details by clicking the **NICs** tab on the ECS details page. By default, the first record in the list is the primary NIC.

Step 5: Check Whether Required Security Group Rules Have Been Configured.

For details about how to add security group rules, see [Adding a Security Group Rule](#).

If security group rules have not been configured, configure them based on your service requirements. (The remote IP address indicates the allowed IP address, and **0.0.0.0/0** indicates that all IP addresses are allowed.)

Step 6: Check Whether Traffic from the ECS Subnet Is Blocked

Check whether the network ACL of the NIC subnet blocks certain traffic from the subnet.

You can configure the network ACL on the VPC console. Make sure that the network ACL rules allow the traffic from the ECS subnet.

6.4.3 What Should I Do If an EIP Cannot Be Pinged?

Symptom

After you purchase an EIP and bind it to an ECS, the local host or other cloud servers cannot ping the EIP of the ECS.

Fault Locating

The following fault causes are sequenced based on their occurrence probability.

If the fault persists after you have ruled out a cause, check other causes.

Figure 6-10 Method of locating the failure to ping an EIP

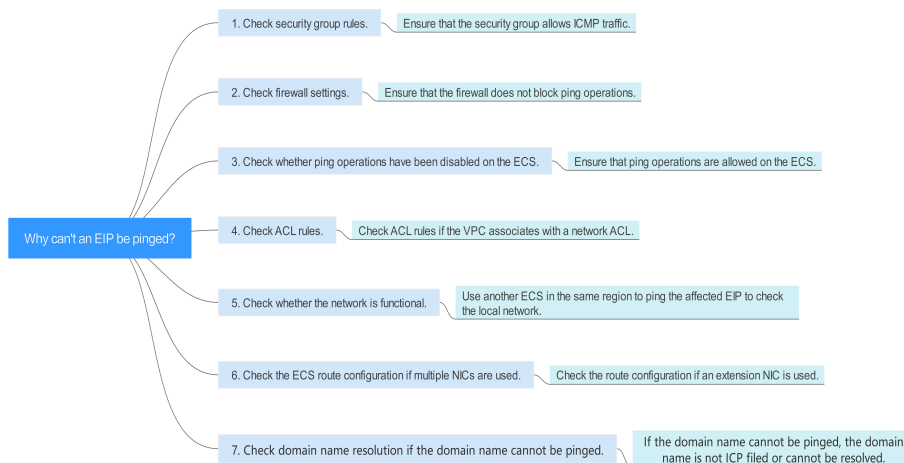


Table 6-5 Method of locating the failure to ping an EIP

Possible Cause	Solution
ICMP access rules are not added to the security group.	Add ICMP access rules to the security group. For details, see Checking Security Group Rules .
Ping operations are prohibited on the firewall.	Allow ping operations on the firewall. For details, see Checking Firewall Settings .

Possible Cause	Solution
Ping operations are prohibited on the ECS.	Allow ping operations on the ECS. For details, see Checking Whether Ping Operations Have Been Disabled on the ECS .
Network ACL is associated.	If the VPC is associated with a network ACL, check the network ACL rules. For details, see Checking ACL Rules .
A network exception occurred.	Use another ECS in the same region to check whether the local network is functional. For details, see Checking Whether the Network Is Functional .
Routes are incorrectly configured if multiple NICs are used.	If the network is inaccessible due to an extension NIC, the fault is generally caused by incorrect route configurations. To resolve this issue, see Checking the ECS Route Configuration If Multiple NICs Are Used .
The domain name is not ICP licensed.	If the domain name cannot be pinged or cannot be resolved, see Checking Domain Name Resolution If the Domain Name Cannot Be Pinged to resolve this issue.

Checking Security Group Rules

ICMP is used for the ping command. Check whether the security group accommodating the ECS allows ICMP traffic.

- Under **Computing**, click **Elastic Cloud Server**.
- On the **Elastic Cloud Server** page, click the name of the target ECS.
The page providing details about the ECS is displayed.
- Click the **Security Groups** tab, expand the information of the security group, and view security group rules.
- Click the security group ID.
The system automatically switches to the **Security Group** page.
- On the **Outbound Rules** page, click **Add Rule**. In the displayed dialog box, set required parameters to add an outbound rule.

Figure 6-11 Adding an outbound rule

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

Security Group: default
You can import multiple rules in a batch.

Priority	Action	Protocol & Port	Type	Destination	Description	Operation
1-100	Allow	Protocols/ICMP	IPv4	IP address		Replicate Delete
		All		0.0.0.0/0		

+ Add Rule

OK Cancel

Table 6-6 Security group rules

Transfer Direction	Type	Protocol/Port Range	Source
Outbound	IPv4	ICMP/Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.

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

Figure 6-12 Adding an inbound rule

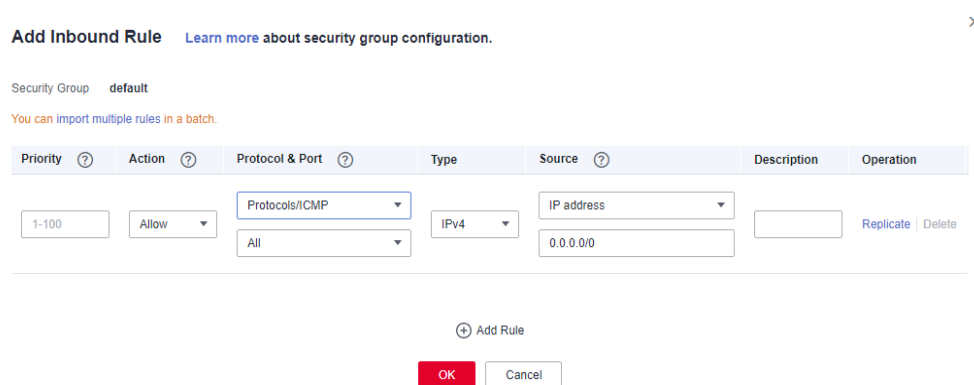


Table 6-7 Security group rules

Transfer Direction	Type	Protocol/Port Range	Source
Inbound	IPv4	ICMP/Any	0.0.0.0/0 0.0.0.0/0 indicates all IP addresses.

- Click **OK** to complete the security rule configuration.

Checking Firewall Settings

If a firewall is enabled on the ECS, check whether the firewall blocks the ping operations.

Linux

- Consider CentOS 7 as an example. Run the following command to check the firewall status:

firewall-cmd --state

If **running** is displayed in the command output, the firewall has been enabled.

- Check whether there is any ICMP rule blocking the ping operations.

iptables -L

If the command output shown in **Figure 6-13** is displayed, there is no ICMP rule blocking the ping operations.

Figure 6-13 Checking firewall rules

```
[root@ecs-3c4e ~]# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    icmp -- anywhere          anywhere          icmp echo-request

Chain FORWARD (policy ACCEPT)
target     prot opt source                destination

Chain OUTPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT    icmp -- anywhere          anywhere          icmp echo-reply
[root@ecs-3c4e ~]#
```

If the ping operations are blocked by an ICMP rule, run the following commands to modify the rule for unblocking:

```
iptables -A INPUT -p icmp --icmp-type echo-request -j ACCEPT
iptables -A OUTPUT -p icmp --icmp-type echo-reply -j ACCEPT
```

Windows

1. Log in to the Windows ECS, click the Windows icon in the lower left corner of the desktop, and choose **Control Panel > Windows Firewall**.
2. Click **Turn Windows Firewall on or off**.
View and set the firewall status.
3. If the firewall is **On**, go to **4**.
4. Check the ICMP rule statuses in the firewall.
 - a. In the navigation pane on the **Windows Firewall** page, click **Advanced settings**.
 - b. Enable the following rules:
Inbound Rules: File and Printer Sharing (Echo Request - ICMPv4-In)
Outbound Rules: File and Printer Sharing (Echo Request - ICMPv4-Out)
If IPv6 is enabled, enable the following rules:
Inbound Rules: File and Printer Sharing (Echo Request - ICMPv6-In)
Outbound Rules: File and Printer Sharing (Echo Request - ICMPv6-Out)

Figure 6-14 Inbound Rules

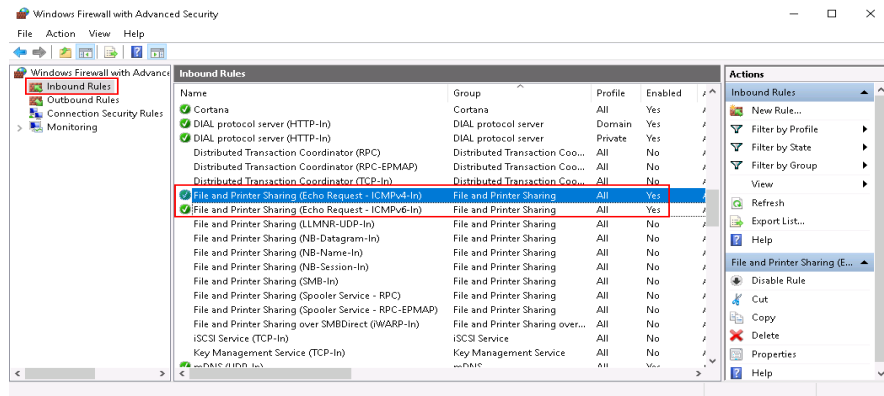
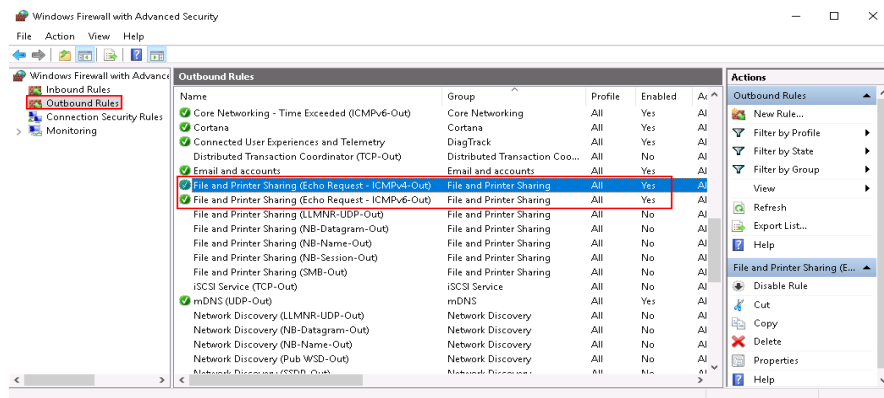


Figure 6-15 Outbound Rules



Checking Whether Ping Operations Have Been Disabled on the ECS

Windows

Enable ping operations using the CLI.

1. Start the **Run** dialog box. Enter **cmd** and press **Enter**.
2. Run the following command to enable ping operations:
netsh firewall set icmpsetting 8

Linux

Check the ECS kernel parameters.

1. Check the **net.ipv4.icmp_echo_ignore_all** value in the **/etc/sysctl.conf** file. Value **0** indicates that ping operations are allowed, and value **1** indicates that ping operations are prohibited.
2. Allow ping operations.
 - Run the following command to temporarily allow the ping operations:
#echo 0 >/proc/sys/net/ipv4/icmp_echo_ignore_all
 - Run the following command to permanently allow the ping operations:
net.ipv4.icmp_echo_ignore_all=0

Checking ACL Rules

By default, no ACL is configured for a VPC. If a network ACL is associated with a VPC, check the ACL rules.

1. Check whether the subnet of the ECS has been associated with a network ACL.
If an ACL name is displayed, the network ACL has been associated with the ECS.
2. Click the ACL name to view its status.
3. If the network ACL is enabled, add an ICMP rule to allow traffic.

NOTE

The default network ACL rule denies all incoming and outgoing packets. If a network ACL is disabled, the default rule is still effective.

Checking Whether the Network Is Functional

1. Use another ECS in the same region to check whether the local network is functional.
Use another ECS in the same region to ping the affected EIP. If the EIP can be pinged, the VPC is functional. In such a case, rectify the local network fault and ping the affected EIP again.
2. Check whether the link is accessible.
A ping failure is caused by packet loss or long delay, which may be caused by link congestion, link node faults, or heavy load on the ECS.

Checking the ECS Route Configuration If Multiple NICs Are Used

Generally, the default route of an OS will preferentially select the primary NIC. If an extension NIC is selected in a route and the network malfunctions, this issue is typically caused by incorrect route configuration.

- If the ECS has multiple NICs, check whether the default route is available.
 - a. Log in to the ECS and run the following command to check whether the default route is available:

ip route

Figure 6-16 Default route

```
[root@do-not-del-scy ~]# ip route
default via 192.168.2.1 dev eth0
169.254.0.0/16 dev eth0 scope link metric 1002
169.254.169.254 via 192.168.2.1 dev eth0 proto static
192.168.2.0/24 dev eth0 proto kernel scope link src 192.168.2.112
```

- b. If the route is unavailable, run the following command to add it:
ip route add default via XXXX dev eth0

NOTE

In the preceding command, *XXXX* specifies a gateway IP address.

- If the ECS has multiple NICs and the EIP is bound to an extension NIC, configure policy routing on the ECS for network communication with the extension NIC.

Checking Domain Name Resolution If the Domain Name Cannot Be Pinged

If you can ping the EIP but not the domain name, the possible cause is that an error occurred in domain name resolution.

1. Check the domain name resolution.

If the domain name records are incorrectly configured, the domain name may fail to be resolved.

Switch to the DNS management console to view details about the domain name resolution.

2. Check the DNS server configuration.

If the system shows no server found after you ping a domain name, this issue may be caused by slow response from the DNS server.

6.4.4 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
2024-04-01	This release incorporates the following changes: Updated the following content: Changed descriptions about parameter Name in Assigning a Shared Bandwidth .
2023-07-24	This release incorporates the following changes: Updated the following content: Added description of the billing mode parameter in Assigning a Shared Bandwidth .
2023-03-15	This release incorporates the following changes: Added the following content: <ul style="list-style-type: none">• Assigning an EIP• Binding an EIP to an Instance• Unbinding an EIP from an Instance• Releasing an EIP• Changing Dedicated Bandwidth Size of an EIP• Exporting EIP Information• Can an EIP That Uses Dedicated Bandwidth Be Changed to Use Shared Bandwidth?• What Are the Differences Between the Primary and Extension NICs of ECSs?

Released On	Description
2022-10-30	<p>This release incorporates the following changes: Added the following content:</p> <ul style="list-style-type: none"> • Advantages • Application Scenarios • Functions • Notes and Constraints • EIP and Other Services • EIP Overview • How Do I Assign or Retrieve a Specific EIP? • Why Is an EIP Newly Assigned the Same as the One I Released? • What Is the EIP Assignment Policy? • Can I Assign a Specific EIP? • Can a Bandwidth Be Used by Multiple Accounts? • How Do I Unbind an EIP from an Instance and Bind a New EIP to the Instance? • Why Can't I Find My Assigned EIP on the Management Console? • How Do I Access the Internet Using an EIP Bound to an Extension NIC? • Can I Bind an EIP of an ECS to Another ECS? • Can I Bind an EIP to a Cloud Resource in Another Region? • What Are Inbound Bandwidth and Outbound Bandwidth? • What Are the Differences Between Public Bandwidth and Private Bandwidth? • What Is the Relationship Between Bandwidth and Upload/Download Rate? • What Should I Do If an EIP Cannot Be Pinged? • Why Does the Download Speed of My ECS Is Slow?
2022-09-02	<p>This release incorporates the following changes: Added the following content:</p> <p>How Do I Know If My EIP Bandwidth Limit Has Been Exceeded?</p> <p>Why Can't My ECS Access the Internet Even After an EIP Is Bound?</p>
2021-11-30	<p>This release incorporates the following change: Added Billing.</p>
2020-11-05	<p>This issue is the first official release.</p>