

**Elastic IP**

# **User Guide**

**Issue**            01  
**Date**             2022-06-07



**Copyright © Huawei Technologies Co., Ltd. 2022. 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.

---

# Contents

---

<b>1 Service Overview</b>	<b>1</b>
1.1 What Is Elastic IP?	1
1.2 Region and AZ	2
<b>2 Quick Start</b>	<b>4</b>
2.1 Overview	4
2.2 Step 1: Create a VPC	5
2.3 Step 2: Create a Subnet for the VPC	10
2.4 Step 3: Assign an EIP and Bind It to an ECS	12
2.5 Step 4: Create a Security Group	14
2.6 Step 5: Add a Security Group Rule	15
<b>3 EIP</b>	<b>18</b>
3.1 Assigning an EIP and Binding It to an ECS	18
3.2 Unbinding an EIP from an ECS and Releasing the EIP	20
3.3 Modifying an EIP Bandwidth	21
<b>4 Shared Bandwidth</b>	<b>22</b>
4.1 Shared Bandwidth Overview	22
4.2 Assigning a Shared Bandwidth	22
4.3 Adding EIPs to a Shared Bandwidth	23
4.4 Removing EIPs from a Shared Bandwidth	24
4.5 Modifying a Shared Bandwidth	24
4.6 Deleting a Shared Bandwidth	25
<b>5 Monitoring</b>	<b>26</b>
5.1 Supported Metrics	26
5.2 Viewing Metrics	28
5.3 Creating an Alarm Rule	28
5.4 Exporting Monitoring Data	29
<b>6 FAQs</b>	<b>30</b>
6.1 Product Consultation	30
6.1.1 What Is a Quota?	30
6.1.2 Can I Bind an EIP to Multiple ECSs?	31
6.2 EIP Binding and Unbinding	31

6.2.1 How Do I Access an ECS with an EIP Bound from the Internet?.....	31
6.2.2 Can I Bind Multiple EIPs to an ECS?.....	31
6.3 Bandwidth.....	32
6.3.1 What Is the Bandwidth Size Range?.....	33
6.3.2 What Bandwidth Types Are Available?.....	33
6.3.3 Is There a Limit to the Number of EIPs That Can Be Added to Each Shared Bandwidth?.....	33
6.3.4 What Are the Differences Between a Dedicated Bandwidth and a Shared Bandwidth? Can a Dedicated Bandwidth Be Changed to a Shared Bandwidth or the Other Way Around?.....	33
6.4 Connectivity.....	33
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?.....	33
<b>A Change History.....</b>	<b>35</b>

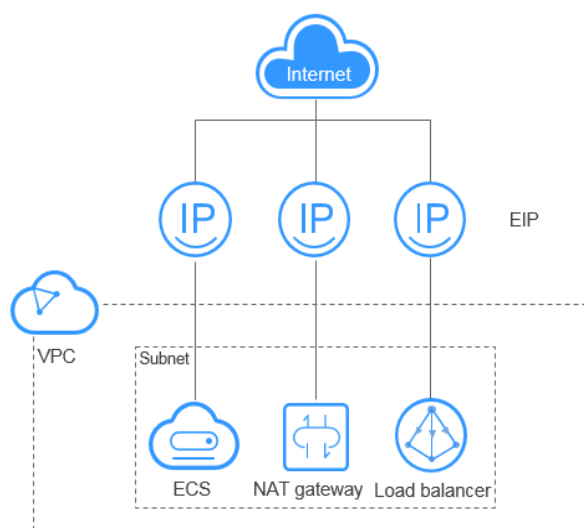
# 1 Service Overview

## 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. 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 Region and AZ

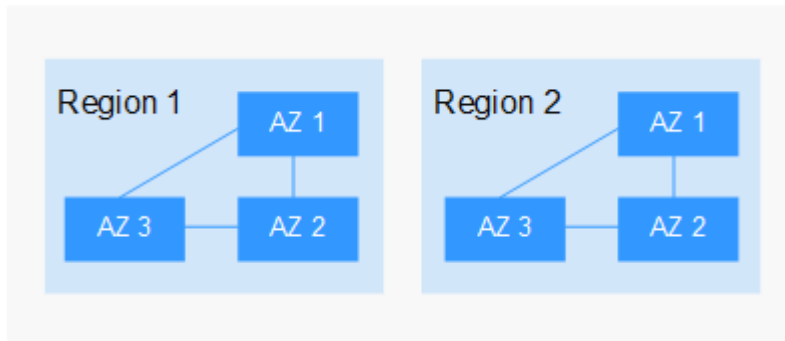
### Concept

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

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

[Figure 1-2](#) shows the relationship between regions and AZs.

**Figure 1-2** Regions and AZs



### Selecting a Region

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

### Selecting an AZ

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

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

## Regions and Endpoints

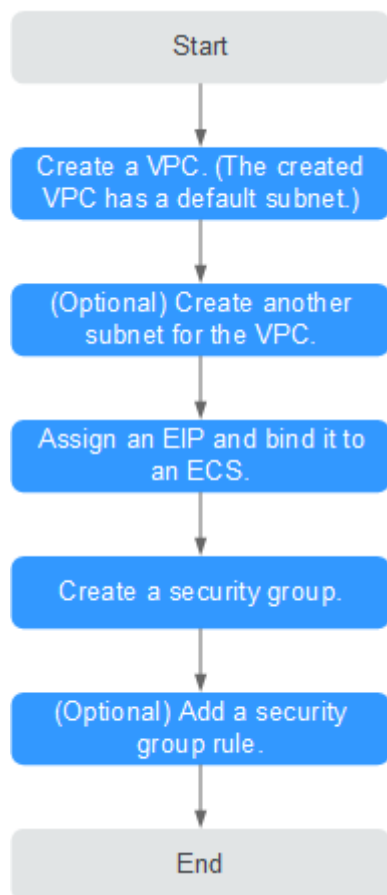
Before you use an API to call resources, specify its region and endpoint. For more details, see [Regions and Endpoints](#).

# 2 Quick Start

## 2.1 Overview

If your ECSs need to access the Internet (for example, the ECSs functioning as the service nodes for deploying a website), you can follow the procedure shown in [Figure 2-1](#) to bind EIPs to the ECSs.

**Figure 2-1** Configuring the network





**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 so that the ECS can access the Internet.
Create a security group.	This task is mandatory. You can create a security group and add ECSs in the VPC to the security group to improve ECS access security. After a security group is created, it has a default rule, which allows all outgoing data packets. ECSs in a security group can access each other without the need to add rules.
Add a security group rule.	This task is optional. If the default rule does not meet your service requirements, you can add security group rules.

## 2.2 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. On the console homepage, under **Network**, click **Virtual Private Cloud**.
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	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.	-
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"><li>• 10.0.0.0/8-24</li><li>• 172.16.0.0/12-24</li><li>• 192.168.0.0/16-24</li></ul>	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 <b>default</b>.</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.	Default
Tag	<p>The VPC tag, which consists of a key and value pair. You can add a maximum of 10 tags to each VPC.</p> <p>The tag key and value must meet the requirements listed in <a href="#">Table 2-4</a>.</p>	<ul style="list-style-type: none"><li>• Key: vpc_key1</li><li>• Value: vpc-01</li></ul>

**Table 2-3** Subnet parameter descriptions

Parameter	Description	Example Value
Name	<p>The subnet name.</p> <p>The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.</p>	subnet-01
IPv4 CIDR Block	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 <b>IPv6 CIDR Block</b> to <b>Enable</b>.</p> <p>After the IPv6 function is enabled, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.</p>	-
Associated Route Table	<p>The default route table to which the subnet will be associated. You can change the route table to a custom route table on the <b>Subnets</b> page.</p>	Default
Advanced Settings	<p>Click the drop-down arrow to set advanced settings for the subnet, including <b>Gateway</b> and <b>DNS Server Address</b>.</p>	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
Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet. The tag key and value must meet the requirements listed in <a href="#">Table 2-5</a> .	<ul style="list-style-type: none"><li>• Key: subnet_key1</li><li>• Value: subnet-01</li></ul>

**Table 2-4** VPC tag key and value requirements

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

**Table 2-5** Subnet tag key and value requirements

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

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

### Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, click **Subnets**.
4. Click **Create Subnet**.  
The **Create Subnet** page is displayed.
5. Set the parameters as prompted.

**Table 2-6** Parameter descriptions

Parameter	Description	Example Value
VPC	The VPC for which you want to create a subnet.	-
Name	The subnet name. The name can contain a maximum of 64 characters, which may consist of letters, digits, underscores (_), hyphens (-), and periods (.). The name cannot contain spaces.	Subnet
IPv4 CIDR Block	The CIDR block for the subnet. This value must be within the VPC CIDR block.	192.168.0.0/24
IPv6 CIDR Block	Specifies whether to set <b>IPv6 CIDR Block</b> to <b>Enable</b> . If you select this option, the system automatically assigns an IPv6 CIDR block to the created subnet. Currently, the IPv6 CIDR block cannot be customized. IPv6 cannot be disabled after the subnet is created.	-
Associated Route Table	The default route table to which the subnet will be associated. You can change the route table to a custom route table on the <b>Subnets</b> page.	Default

Parameter	Description	Example Value
Advanced Settings/Gateway	The gateway address of the subnet. This IP address is used to communicate with other subnets.	192.168.0.1
Advanced Settings/DNS Server Address	DNS server addresses allow ECSs in a VPC subnet to communicate with each other using private domain names. You can also directly access cloud services through private DNS servers.  If you want to use other public DNS servers for resolution, you can change the default DNS server addresses.  A maximum of two DNS server IP addresses can be configured. Multiple IP addresses must be separated using commas (,).	100.125.x.x
Advanced Settings/Tag	The subnet tag, which consists of a key and value pair. You can add a maximum of 10 tags to each subnet.  The tag key and value must meet the requirements listed in <a href="#">Table 2-7</a> .	<ul style="list-style-type: none"> <li>• Key: subnet_key1</li> <li>• Value: subnet-01</li> </ul>

**Table 2-7** Subnet tag key and value requirements

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

6. Click **OK**.

## Precautions

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

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

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

## 2.4 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. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, click **Assign EIP**.
4. 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.	N/A
EIP Type	<b>Dynamic BGP:</b> Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
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 <a href="#">Table 2-9</a> .	<ul style="list-style-type: none"><li>• Key: ipv4_key1</li><li>• Value: 192.168.12.10</li></ul>
Quantity	The number of EIPs you want to purchase.	1
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 <b>default</b> . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default

**Table 2-9** EIP tag requirements

Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none"><li>• Cannot be left blank.</li><li>• Must be unique for each EIP.</li><li>• Can contain a maximum of 36 characters.</li><li>• Can contain letters, digits, underscores (_), and hyphens (-).</li></ul>	ipv4_key1
Value	<ul style="list-style-type: none"><li>• Can contain a maximum of 43 characters.</li><li>• Can contain letters, digits, underscores (_), periods (.), and hyphens (-).</li></ul>	192.168.12.10

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

## Binding an EIP

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

## 2.5 Step 4: Create a Security Group

### Scenarios

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

### Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Virtual Private Cloud**.
3. In the navigation pane on the left, choose **Access Control** > **Security Groups**.
4. On the **Security Groups** page, click **Create Security Group**.
5. In the **Create Security Group** area, set the parameters as prompted. [Table 2-10](#) lists the parameters to be configured.

**Table 2-10** Parameter description

Parameter	Description	Example Value
Name	<p>The security group name. This parameter is mandatory.</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><b>NOTE</b></p> <p>You can change the security group name after a security group is created. It is recommended that you give each security group a different name.</p>	sg-318b

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

6. Click **OK**.

## 2.6 Step 5: Add a Security Group Rule

### Scenarios

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

- Inbound rules control incoming traffic to cloud resources in the security group.
- Outbound rules control outgoing traffic from cloud resources in the security group.

### Procedure

1. In the navigation pane on the left, choose **Access Control > Security Groups**.
2. On the **Security Groups** page, locate the target security group and click **Manage Rule** in the **Operation** column to switch to the page for managing inbound and outbound rules.
3. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters.

You can click + to add more inbound rules.

**Table 2-11** Inbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	<b>Protocol:</b> The network protocol. Currently, the value can be <b>All, TCP, UDP, ICMP, GRE</b> , or others.	Custom TC
	<b>Port:</b> The port or port range over which the traffic can reach your ECS. The value ranges from 1 to 65535.	22, or 22-30
Type	The IP address type. <ul style="list-style-type: none"> <li>IPv4</li> <li>IPv6</li> </ul>	IPv4
Source	The source of the security group rule. The value can be a single IP address or a security group to allow access from the IP address or instances in the security group. For example: <ul style="list-style-type: none"> <li>Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6)</li> <li>IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6)</li> <li>All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6)</li> <li>Security group: sg-abc</li> </ul>	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

- On the **Outbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters.

You can click + to add more outbound rules.

**Table 2-12** Outbound rule parameter description

Parameter	Description	Example Value
Protocol & Port	<b>Protocol:</b> The network protocol. Currently, the value can be <b>All, TCP, UDP, ICMP, GRE</b> , or others.	Custom TCP
	<b>Port:</b> The port or port range over which the traffic can leave your ECS. The value ranges from 1 to 65535.	22, or 22-30

Parameter	Description	Example Value
Type	The IP address type. <ul style="list-style-type: none"><li>• IPv4</li><li>• IPv6</li></ul>	IPv4
Destination	The destination of the security group rule. The value can be a single IP address or a security group to allow access to the IP address or instances in the security group. For example: <ul style="list-style-type: none"><li>• Single IP address: 192.168.10.10/32 (IPv4); 2002:50::44/127 (IPv6)</li><li>• IP address range: 192.168.1.0/24 (IPv4); 2407:c080:802:469::/64 (IPv6)</li><li>• All IP addresses: 0.0.0.0/0 (IPv4); ::/0 (IPv6)</li><li>• Security group: sg-abc</li></ul> For more information, see <i>Virtual Private Cloud User Guide</i> .	0.0.0.0/0
Description	Supplementary information about the security group rule. This parameter is optional. The security group rule description can contain a maximum of 255 characters and cannot contain angle brackets (< or >).	-

5. Click **OK**.

# 3 EIP

## 3.1 Assigning an EIP and Binding It to an ECS

### Scenarios

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

### Assigning an EIP

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, click **Assign EIP**.
4. Set the parameters as prompted.

**Table 3-1** Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	N/A
EIP Type	<b>Dynamic BGP:</b> Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.	Dynamic BGP
Bandwidth	The bandwidth size in Mbit/s.	100

Parameter	Description	Example Value
Bandwidth Name	The name of the bandwidth.	bandwidth
Tag	The EIP tags. Each tag contains a key and value pair. The tag key and value must meet the requirements listed in <a href="#">Table 3-2</a> .	<ul style="list-style-type: none"><li>• Key: ipv4_key1</li><li>• Value: 192.168.12.10</li></ul>
Quantity	The number of EIPs you want to purchase.	1
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 <b>default</b> . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default

**Table 3-2** EIP tag requirements

Parameter	Requirement	Example Value
Key	<ul style="list-style-type: none"><li>• Cannot be left blank.</li><li>• Must be unique for each EIP.</li><li>• Can contain a maximum of 36 characters.</li><li>• Can contain letters, digits, underscores (_), and hyphens (-).</li></ul>	ipv4_key1
Value	<ul style="list-style-type: none"><li>• Can contain a maximum of 43 characters.</li><li>• Can contain letters, digits, underscores (_), periods (.), and hyphens (-).</li></ul>	192.168.12.10

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

## Binding an EIP

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

3. Click **OK**.

## 3.2 Unbinding an EIP from an ECS and Releasing the EIP

### Scenarios

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

### Notes and Constraints

- You can only release EIPs that are not bound to any resources.
- 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. On the console homepage, under **Network**, click **Elastic IP**.
3. On the displayed page, locate the row that contains the target EIP, and click **Unbind**.
4. Click **Yes** in the displayed dialog box.

#### Releasing a single EIP

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

#### Unbinding multiple EIPs at once

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

#### Releasing multiple EIPs at once

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



## 3.3 Modifying an EIP Bandwidth

### Scenarios

Modify the EIP bandwidth name or size.

### Procedure

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

# 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, BMSs, and load balancers that have EIPs bound in the same region can share a bandwidth.

When you host a large number of applications on the cloud, if each EIP uses an independent bandwidth, a lot of bandwidths are required, increasing O&M workload. If all EIPs share the same bandwidth, VPCs and the region-level bandwidth can be managed in a unified manner, simplifying O&M statistics and network operations cost settlement.

- **Lowered Bandwidth Costs**  
Region-level bandwidth sharing and multiplexing reduce bandwidth usage and O&M costs.
- **Easy to Manage**  
Region-level bandwidth sharing and multiplexing simplify O&M statistics, management, and operations cost settlement.
- **Flexible Operations**  
You can add EIPs that are billed on a pay-per-use basis to a shared bandwidth or remove them from a shared bandwidth regardless of the instances to which they are bound.

## 4.2 Assigning a Shared Bandwidth

### Scenarios

Assign a shared bandwidth for use with EIPs.

### Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.

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

**Table 4-1** Parameter descriptions

Parameter	Description	Example Value
Region	Regions are geographic areas that are physically isolated from each other. The networks inside different regions are not connected to each other, so resources cannot be shared across different regions. For lower network latency and faster access to your resources, select the region nearest you.	N/A
Bandwidth	The bandwidth size in Mbit/s. The maximum bandwidth can be 300 Mbit/s.	10
Enterprise Project	The enterprise project to which the EIP belongs. An enterprise project facilitates project-level management and grouping of cloud resources and users. The name of the default project is <b>default</b> . For details about creating and managing enterprise projects, see the <i>Enterprise Management User Guide</i> .	default
Bandwidth Name	The name of the shared bandwidth.	Bandwidth-001

5. Click **Create Now**.

## 4.3 Adding EIPs to a Shared Bandwidth

### Scenarios

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

### Notes and Constraints

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

## Procedure

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

## 4.4 Removing EIPs from a Shared Bandwidth

### Scenarios

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

### Procedure

1. Log in to the management console.
2. On the console homepage, under **Network**, click **Elastic IP**.
3. In the navigation pane on the left, choose **Elastic IP and Bandwidth > Shared Bandwidths**.
4. In the shared bandwidth list, locate the row that contains the bandwidth from which EIPs are to be removed, choose **More > Remove EIP** in the **Operation** column, and select the EIPs to be removed in the displayed dialog box.
5. Click **OK**.

## 4.5 Modifying a Shared Bandwidth

### Scenarios

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

### Procedure

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

## 4.6 Deleting a Shared Bandwidth

### Scenarios

Delete a shared bandwidth when it is no longer required.

### Prerequisites

Before deleting a shared bandwidth, remove all the EIPs associated with it. For details, see [Removing EIPs from a Shared Bandwidth](#).

### Procedure

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

# 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	$\geq 0$ 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	$\geq 0$ bit/s	Bandwidth or EIP	1 minute
upstream_bandwidth_usage	Outbound Bandwidth Usage	Usage of outbound bandwidth in the unit of percent.	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	$\geq 0$ bytes	Bandwidth or EIP	1 minute
downstream	Inbound Traffic	Network traffic going into the cloud platform (Previously called "Downstream Traffic") Unit: byte	$\geq 0$ bytes	Bandwidth or EIP	1 minute

## Dimensions

Key	Value
publicip_id	EIP ID
bandwidth_id	Bandwidth ID

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

- Query a monitoring metric:

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

- Query monitoring metrics in batches:

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

## 5.2 Viewing Metrics

### Scenarios

View related metrics to see bandwidth and EIP usage information.

### 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. Click **Cloud Service Monitoring** on the left of the page, and choose **Elastic IP and Bandwidth**.
4. Locate the row that contains the target bandwidth or EIP and click **View Metric** in the **Operation** column to check the bandwidth or EIP monitoring information.

## 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. Hover on the upper left corner to display **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 the *Cloud Eye User Guide*.

## 5.4 Exporting Monitoring Data

### Scenarios

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

### Procedure

1. Log in to the management console.
2. Hover on the upper left corner to display **Service List** and choose **Management & Deployment > Cloud Eye**.
3. In the navigation pane on the left, choose **Cloud Service Monitoring > Elastic IP and Bandwidth**.
4. On the **Cloud Service Monitoring** page, click **Export Data**.
5. Configure the time range, resource type, dimension, monitored object, and metric.
6. Click **Export**.
  - The first row in the exported monitoring report 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**.
4. On the **Create Service Ticket** page, configure parameters as required.  
In **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 Tenant Authorization Letter and Privacy Statement** and click **Submit**.

## 6.1.2 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*.

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

#### NOTE

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

### 6.2.2 Can I Bind Multiple EIPs to an ECS?

#### Scenarios

You can bind multiple EIPs to an ECS. However, this configuration is not recommended.

To bind multiple EIPs to an ECS, you must manually configure routes.

## Configuration Example

**Table 6-1** lists ECS configurations.

**Table 6-1** ECS configurations

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

### Example 1:

If you are required 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 are required 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**.

## 6.3 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 What Bandwidth Types Are Available?

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

### 6.3.3 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?](#)

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

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

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

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

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

## 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.

---

# A Change History

---

Released On	Description
2022-06-07	This release incorporates the following changes: Added descriptions about IPv6 in the following sections: <ul style="list-style-type: none"><li>• <a href="#">Step 1: Create a VPC</a></li><li>• <a href="#">Step 2: Create a Subnet for the VPC</a></li><li>• <a href="#">Step 5: Add a Security Group Rule</a></li></ul>
2022-04-12	This issue is the first official release.