Elastic IP

FAQs

Issue	**15**
Date	**2021-01-08**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Contents

1 Product Consultation

1.1 What Is a Quota?

What Is a Quota?

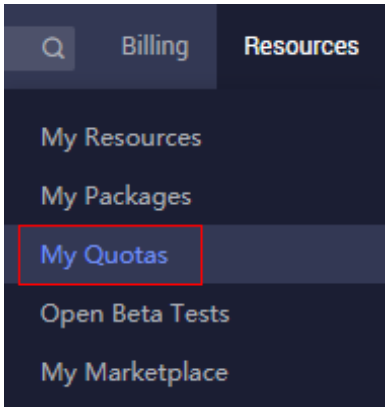
A quota limits the quantity of a resource available to users, thereby preventing spikes in the usage of the resource. For example, a VPC quota limits the number of VPCs that can be created.

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

How Do I View My Quotas?

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. In the upper right corner of the page, choose **Resources** > **My Quotas**.
   The **Service Quota** page is displayed.

   Figure 1-1 My Quotas

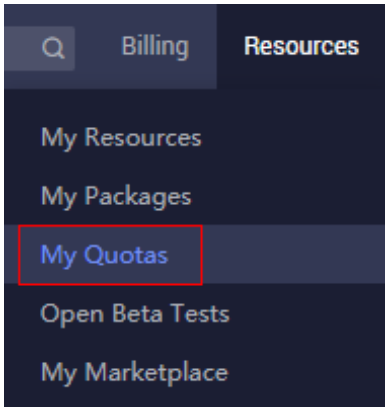
   

4. View the used and total quota of each type of resources on the displayed page.
   If a quota cannot meet service requirements, apply for a higher quota.

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.

   Figure 1-2 My Quotas



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**.

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. When assigning an EIP, set the value of **ip_address** to the IP address that you want to assign. For details, see 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.

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

An EIP is an IP address that can be accessed over the Internet. Each EIP can be used by only one ECS at a time. For details, see EIP Overview.

A private IP address is used by the internal network of the public cloud for internal communications. It cannot be accessed over the Internet.

A floating IP address is similar to an EIP. They are both public IP addresses that are used to connect to the Internet, but a floating IP address API cannot be used to configure bandwidth parameters. For details, see Floating IP Address.

A virtual IP address can be shared among multiple ECSs. A virtual IP address is used for active/standby switchover of ECSs for higher availability. If the active ECS becomes faulty and cannot provide services, the virtual IP address is dynamically re-assigned to the standby ECS so services can continue uninterrupted. For details, see Virtual IP Address Overview.

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

Yes. A pay-per-use EIP that uses the dedicated bandwidth can be changed to use the shared bandwidth. However, a yearly/monthly EIP that uses the dedicated bandwidth cannot be changed to use the shared bandwidth.

1.5 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.

1.6 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.

1.7 What Is the EIP Assignment Policy?

By default, an EIP is assigned randomly.

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

If you want an EIP that you released 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 an EIP first and then release the one that you do not require any more.

1.8 Can I Assign a Specific EIP?

By default, an EIP is assigned randomly. If you used to release EIPs, the system preferentially assigns an EIP from what you released.

To assign a specific EIP, you can call APIs. For details, see Assigning an EIP.

1.9 How Do I Query the Region of My EIPs?

You can visit https://en.ipip.net/?origin=CN to query the region of your EIPs.

- The region of an IP address you searched through a third-party website may be different from the actual region to which the IP address belongs.
- If the region searched through a third-party website is different from that searched on https://en.ipip.net/?origin=CN, use the region searched on https://en.ipip.net/?origin=CN.
- If the region searched on https://en.ipip.net/?origin=CN is different from the region you selected when purchasing the EIP, use the region you selected when purchasing the EIP.
- If your service is adversely affected due to the inconsistency between the region of the EIP you searched on the third-party database and the region of the EIP you selected when buying the EIP, submit a service ticket.

To know more about the region of EIPs, submit a service ticket.

1.10 Can a Bandwidth Be Used by Multiple Accounts?

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

1.11 What Are the Differences Between Shared Data Package and Shared Bandwidth?

Shared data package and shared bandwidth are two different products.

Table 1-1 Differences between shared data package and shared bandwidth

Aspect	Shared Data Package	Shared Bandwidth
Customer	All customers	Medium- and large-scale customers
Feature	After a shared data package takes effect, EIPs billed by traffic will use the shared data package first. After the shared data package is used up, the EIPs will be billed by traffic on a pay-per-use basis. A shared data package is more cost-effective than billing by traffic on	Multiple pay-per-use EIPs can be added to a shared bandwidth. Shared bandwidth can be billed by bandwidth or by 95th percentile bandwidth (enhanced).

Aspect	Shared Data Package	Shared Bandwidth
	the yearly/monthly basis.	
Usage method	A shared data package takes effect immediately after being purchased and you do not need to perform any configurations.	After purchasing a shared bandwidth, you need to add EIPs to the shared bandwidth.

1.12 Do I Need to Configure a Shared Data Package for Use After It Is Purchased?

No.

A shared data package takes effect immediately after being purchased and no additional operations are required. If you have subscribed to pay-per-use EIPs using bandwidth billed by traffic in a region and buy a shared data package in the same region, the EIPs will use the shared data package.

2 Billing and Payments

2.1 How Is an EIP Billed?

EIPs can be billed on a yearly/monthly or pay-per-use basis.

Table 2-1 EIP billing details

Billing Mode	Billed By	EIP Retention Fee	Bandwidth Price	Public Network Traffic Price
Yearly/Monthly	Bandwidth	-	Included	Not included
Pay-per-use	Bandwidth	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.
- For details about the EIP pricing, see Product Pricing Details.

2.2 How Do I Change the Billing Mode?

Changing the Billing Mode from Pay-per-Use to Yearly/Monthly

You can change the billing mode of pay-per-use EIPs and shared bandwidth billed by bandwidth to yearly/monthly. After the change is successful, the new billing mode will take effect immediately.

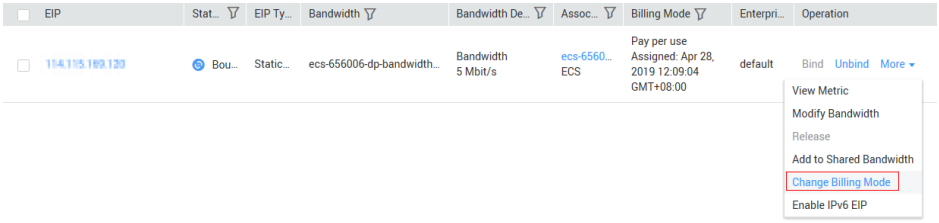
You can change the billing mode on the EIP console. Do as follows to change the billing mode of an EIP from pay-per-use to yearly/monthly.

NOTE

The billing mode of an EIP that is billed by traffic on a pay-per-use basis cannot be directly changed to yearly/monthly. Change the EIP to be billed by bandwidth and then change its billing mode to yearly/monthly.

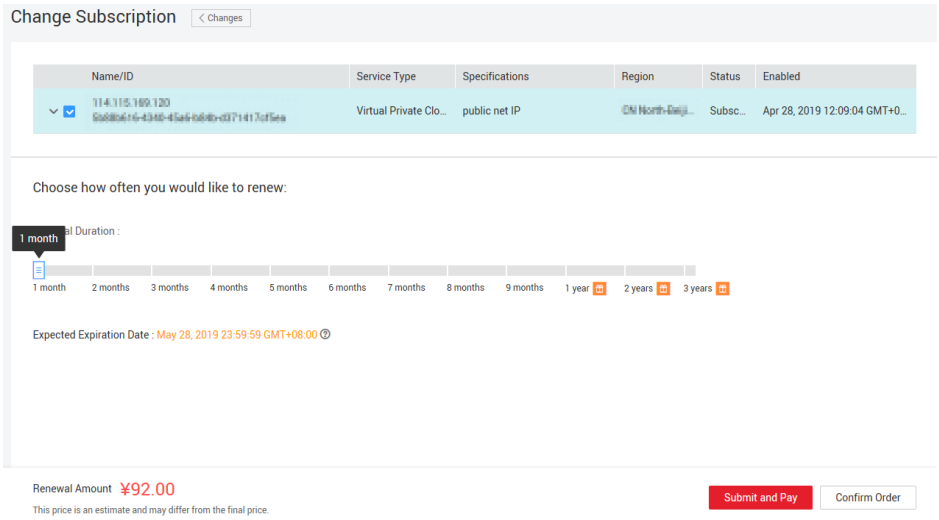
1. Log in to the management console.
2. Under **Network**, click **Elastic IP**.
3. On the displayed page, search for the pay-per-use EIP whose billing mode is to be changed.
4. Locate the row that contains the target EIP and click **Change Billing Mode** in the **Operation** column.

Figure 2-1 Changing the billing mode on the EIP console



5. Click **Yes**.
6. Set specifications.

Figure 2-2 Setting specifications



7. Click **Submit and Pay**.

You can also select multiple EIPs and click **Change Billing Mode** above the EIP list to change all the EIP billing modes at the same time.

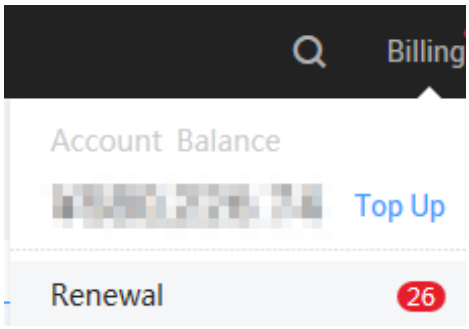
Changing the Billing Mode from Yearly/Monthly to Pay-per-Use

The billing mode of yearly/monthly EIPs and shared bandwidth can be changed to pay-per-use. The new billing mode takes effect only after the required duration of the yearly/monthly billing mode expires.

The billing mode of an EIP can be changed from yearly/monthly to pay-per-use in the billing center. Do as follows to change the billing mode of an EIP from yearly/monthly to pay-per-use:

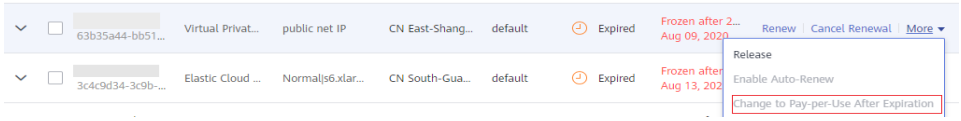
1. Log in to the management console.
2. Choose **Billing** > **Renewal**.

Figure 2-3 Renewal



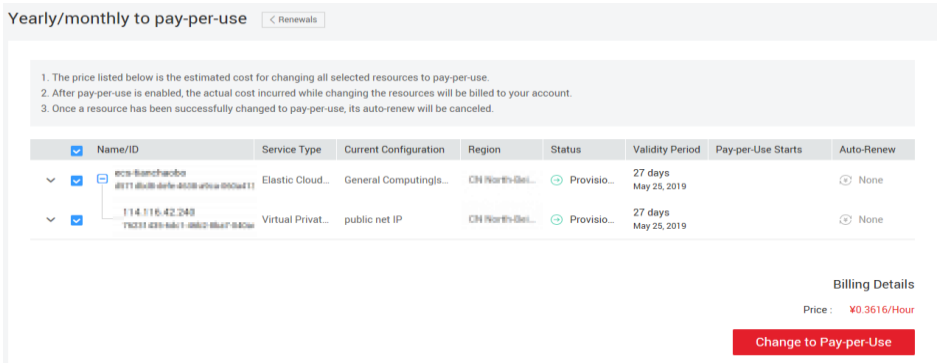
3. In the search box on the right, search for the EIP whose billing mode you want to change.
4. Locate the row that contains the target EIP and click **Change to Pay-per-Use After Expiration** in the **Operation** column.

Figure 2-4 Changing the billing mode to pay-per-use



5. In the page that is displayed, click the **Change to Pay-per-Use** button.

Figure 2-5 Confirming the change



The EIP billed by bandwidth on a yearly/monthly basis can only be changed to an EIP billed by bandwidth on a pay-per-use basis. After you change the billing mode of the EIP to pay-per-use, you can change the EIP billed by bandwidth to be billed by traffic. For details, see Changing Bandwidth Billing.

NOTE

The EIP remains the same after the billing mode is changed.

2.3 How Do I Change the Bandwidth Billing Option from Bandwidth to Traffic or from Traffic to Bandwidth?

- The billing option can be changed only when the billing mode is **Pay-per-use**. For details, see Changing Bandwidth Billing.
- A yearly/monthly resource can only be billed by bandwidth.

3 EIP Binding and Unbinding

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

Each ECS is automatically added to a security group after being created to ensure its security. The security group denies access traffic from the Internet by default (except TCP traffic from port 22 through SSH to the Linux OS and TCP traffic from port 3389 through RDP to the Windows OS). 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 **Port Range** to improve network security.
- Allocate ECSs that have different Internet access policies to different security groups.

NOTE

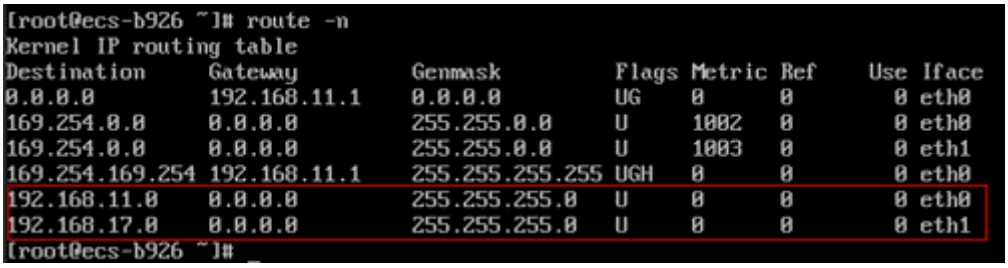
The default source IP address **0.0.0.0/0** indicates that all IP addresses can access ECSs in the security group.

3.2 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 run the **route** command to query the route.

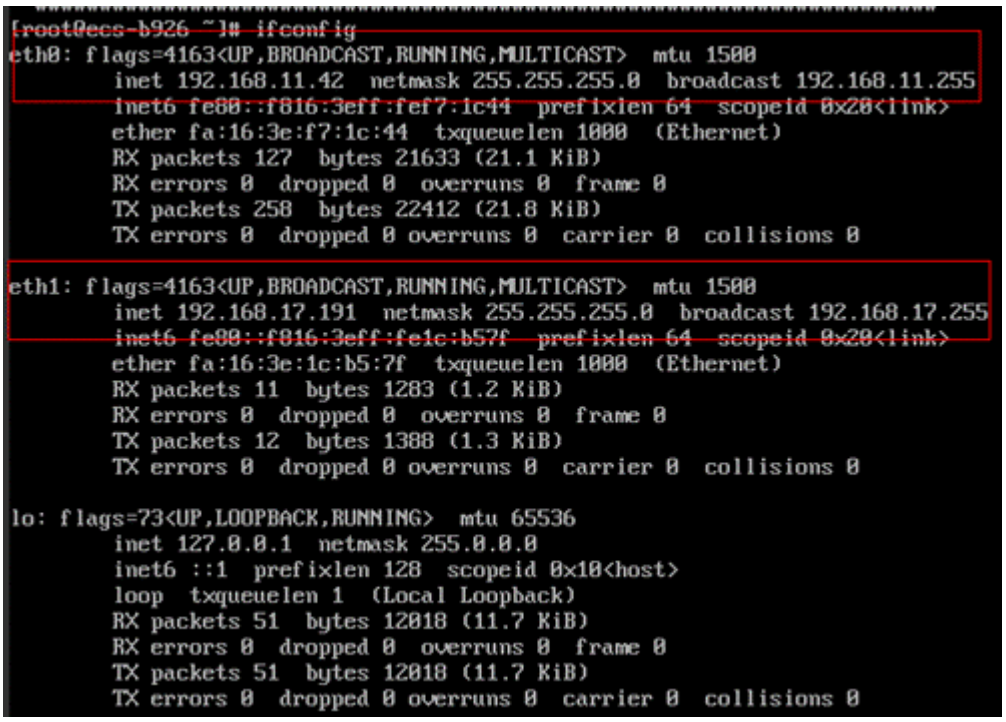
   You can run **route --help** to learn more about the **route** command.

Figure 3-1 Viewing route information



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

Figure 3-2 Viewing NIC information



3. Configure the extension NIC to 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 0.0.0.0 192.168.11.1 dev eth0

   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 network segment (for example, *xx.xx*.0.0/16) through the extension NIC:

You can configure the network segment as required.

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

3.3 Can I Bind an EIP to an ECS, to Another ECS?

Yes.

Unbind the EIP from the ECS. For details, see Unbinding or Releasing an EIP.

Then, bind the EIP to the target ECS. For details, see Binding an EIP to Cloud Resources.

Helpful Links

Change the EIP associated with an ECS. For details, see Changing an EIP.

3.4 Can Multiple EIPs Be Bound to an ECS?

Scenarios

An ECS can be bound with multiple EIPs, though this configuration is not recommended.

To bind multiple EIPs, you must manually configure routing policies. Exercise caution when you perform this operation.

Configuration Example

Table 3-1 lists ECS configurations.

Table 3-1 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 routing policy:

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

   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 routing policy:

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

   ip route delete default
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**.

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

No. EIPs can only be bound to cloud resources within the same region. For example, an EIP in the **CN North-Beijing1** region cannot be bound to a resource in the **CN North-Beijing4** region.

4 Bandwidth

4.1 What Is the Bandwidth Size Range?

The bandwidth ranges from 1 Mbit/s to 2000 Mbit/s.

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

Symptom

The EIP billed by traffic cannot be increased to be more than 300 Mbit/s.

Solution

Currently, the EIP billed by traffic can be increased to a maximum of 300 Mbit/s. 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 Changing Bandwidth Billing.

4.3 What Bandwidth Types Does the VPC Service Support?

The VPC service supports dedicated bandwidth and shared bandwidth. The dedicated bandwidth can only be used by one EIP, whereas the shared bandwidth can be used by multiple EIPs.

4.4 How Do I Buy a Shared Bandwidth?

1. Log in to the management console.

2. Click  in the upper left corner and select the desired region and project.
3. On the console homepage, under **Network**, click **Virtual Private Cloud**.
4. In the navigation pane on the left, choose **Elastic IP and Bandwidth** > **Shared Bandwidths**.
5. In the upper right corner, click **Buy Shared Bandwidth**. On the displayed page, configure parameters as prompted to buy a shared bandwidth.

4.5 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, submit a service ticket to request a quota increase.

4.6 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 and a NAT gateway.

Shared bandwidth: The bandwidth can be shared by multiple EIPs. You can add multiple pay-per-use EIPs to the bandwidth. Adding an EIP to or removing an EIP from a shared bandwidth does not affect running services.

A dedicated bandwidth cannot be changed to a shared bandwidth or the other way around. However, you can purchase shared bandwidth for pay-per-use EIPs.

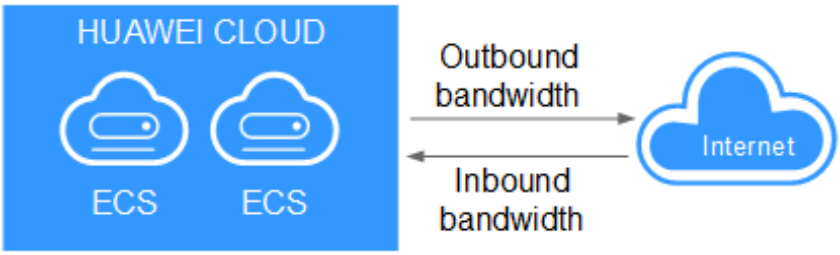
- After an EIP is added to a shared bandwidth, the EIP will use the shared bandwidth.
- After an EIP is removed from the shared bandwidth, the EIP will use the dedicated bandwidth.

4.7 What Are Inbound Bandwidth and Outbound Bandwidth?

Inbound bandwidth: refers to the bandwidth consumed when data is transferred from the Internet to HUAWEI CLOUD. For example, resources are downloaded from the Internet to ECSs in the cloud.

Outbound bandwidth: refers to the bandwidth consumed when data is transferred from HUAWEI CLOUD to the Internet. For example, the ECSs in the cloud provide services accessible from the Internet and external users download resources from the ECSs.

Figure 4-1 Inbound bandwidth and outbound bandwidth



HUAWEI CLOUD only bills for the outbound bandwidth.

NOTE

- If you have selected the enhanced 95th percentile bandwidth option, the total bandwidth billed will be the average of the bandwidths in inbound and outbound directions.
- Inbound and outbound bandwidths have been adjusted as follows since July 31, 2020 00:00:00 GMT+08:00:
- If your purchased or modified bandwidth is less than or equal to 10 Mbit/s, the inbound bandwidth will be 10 Mbit/s, and the outbound bandwidth will be the same as the purchased or modified bandwidth.
- If your purchased or modified bandwidth is greater than 10 Mbit/s, both the bandwidths in inbound and outbound directions will be the same as the purchased or modified bandwidth.

4.8 How Do I Know If My Used Bandwidth Exceeds the Limit?

Symptom

The bandwidth size configured when you buy a dedicated or shared bandwidth is the upper limit of the outbound bandwidth. If web applications that depend on the Internet freeze, check whether the dedicated bandwidth of the EIP bound to the ECS is greater than the configured bandwidth size.

NOTE

If the bandwidth exceeds the configured bandwidth size, packet loss may occur. To ensure normal service running, it is recommended that you monitor the bandwidth.

Troubleshooting

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 4-2 Troubleshooting

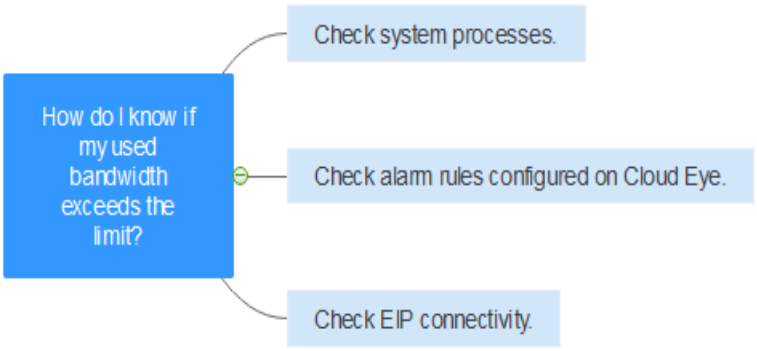


Table 4-1 Troubleshooting

Possible Cause	Solution
System processes leading to high bandwidth	See System Processes Leading to High Bandwidth
Improper Cloud Eye alarm rules	See Improper Cloud Eye Alarm Rules
EIP connection failure	See Why Does Internet Access Fail Even If My ECS Is Bound with an EIP?

System Processes Leading to High Bandwidth

If system processes leading to excessively high bandwidth or CPU usage, your ECS will run slowly or be inaccessible unexpectedly

You can visit the following links to locate the processes that lead to excessively high bandwidth or CPU usage, and optimize or stop the processes.

- Troubleshooting High Bandwidth or CPU Usage of a Windows ECS
- Troubleshooting High Bandwidth or CPU Usage of a Linux ECS

Improper Cloud Eye Alarm Rules

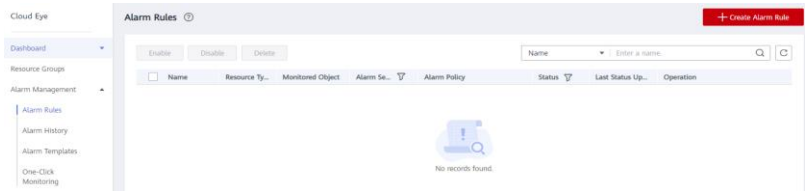
When you create alarm rules for bandwidths on the Cloud Eye console, if the maximum outbound bandwidth or the alarm period is set too small, the system will send alarms indicating that the bandwidth exceeds the threshold too frequently.

Solution 1: Create a proper bandwidth alarm rule.

You need to set an appropriate alarm rule based on your purchased 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 is greater than or equal to 4.8 Mbit/s in three consecutive periods. You can also increase your bandwidth.

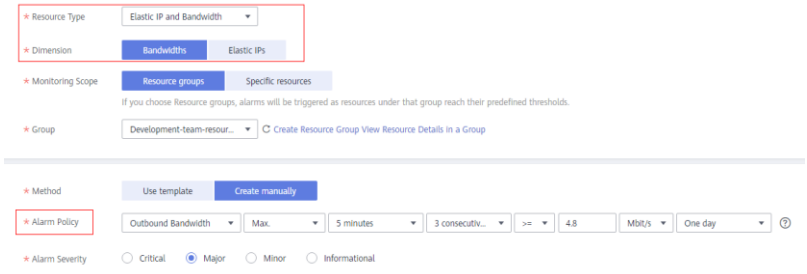
1. Log in to the management console, under **Management & Deployment**, click **Cloud Eye**. On the **Cloud Eye** console, choose **Alarm Management** > **Alarm Rules**.

   Figure 4-3 Alarm Rules

2. Click **Create Alarm Rule** and configure an alarm rule to generate alarms when the bandwidth exceeds the limit.

   Figure 4-4 Creating an alarm rule

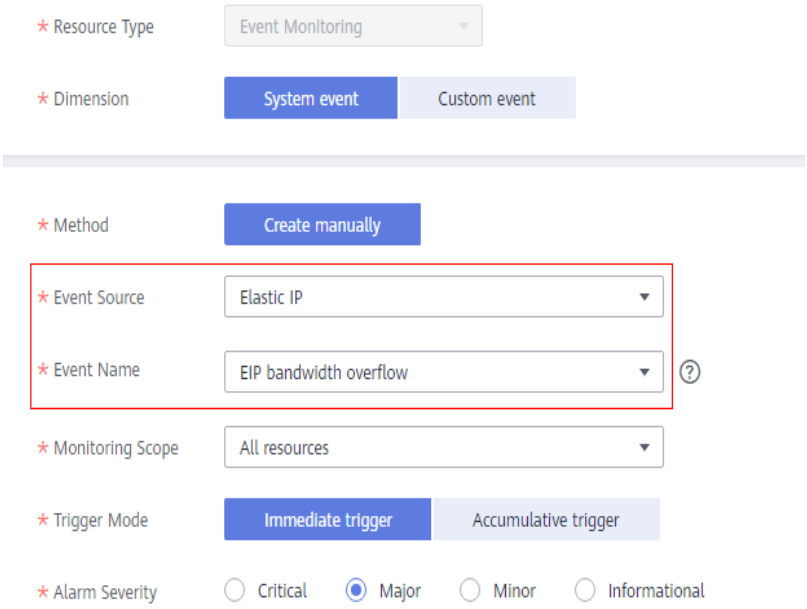
Solution 2: Configure the **EIP bandwidth overflow** event.

NOTE

- EIP bandwidth overflow is available only in regions **CN North-Beijing1**, **CN East-Shanghai2**, and **CN South-Guangzhou**.
- The **Event Monitoring** page only displays EIP status. For details, see Cloud Eye User Guide.

1. Configure EIP bandwidth overflow.
   a. Log in to the management console, under **Management & Deployment**, click **Cloud Eye**. On the **Cloud Eye** console, choose **Event Monitoring**.
   b. Click **Create Alarm Rule** and configure an alarm rule to generate alarms when the EIP bandwidth exceeds the limit.

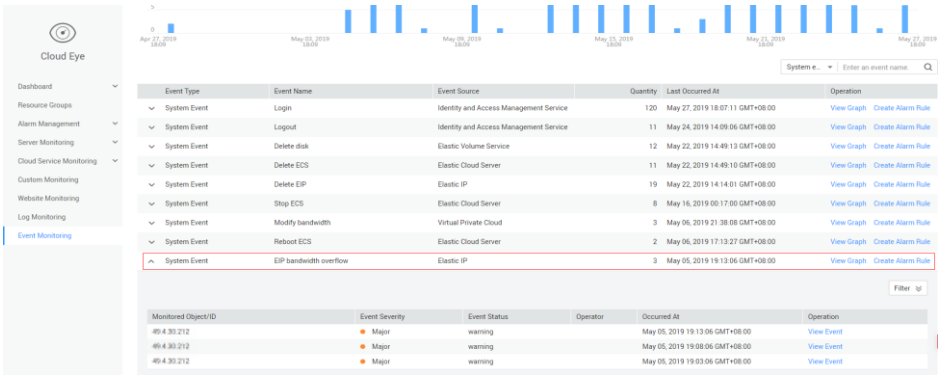
Figure 4-5 Creating an alarm rule



After the configuration, you can view the usage details of the EIP dedicated bandwidth on the **Event Monitoring** page when packet loss or shuttering occurs.

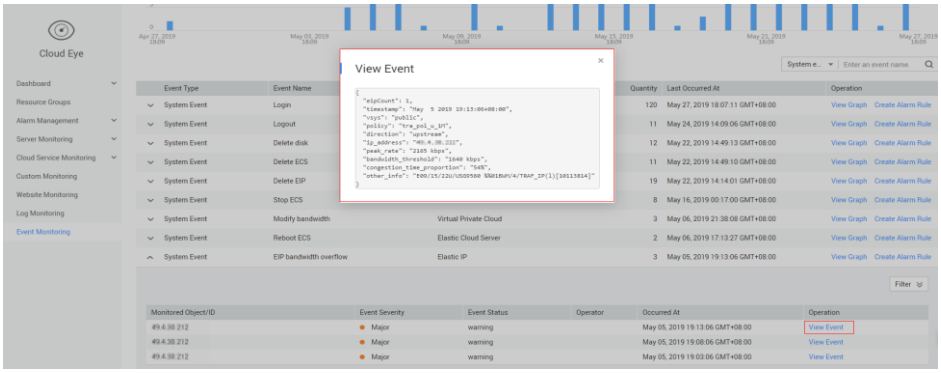
2. Query the historical dedicated bandwidth usage of an EIP.
   a. On the **Cloud Eye** console, click **Event Monitoring**.

Figure 4-6 Event Monitoring



   b. Click **View Event**.

Figure 4-7 View Event



If the event **EIP bandwidth overflow** is not displayed, the dedicated bandwidth of the EIP does not exceed the limit.

If the event **EIP bandwidth overflow** is displayed, the dedicated bandwidth of the EIP has exceeded the limit. To ensure stable service running, increase your bandwidth.

You will not be charged for the Cloud Eye alarm function. If you enable SMN to send alarm notifications, this will incur standard usage charges for the SMN service. For details, see Cloud Eye User Guide.

Submitting a Service Ticket

If the problem persists, submit a service ticket.

4.9 What Are the Differences Between EIP Bandwidth and Private Network Bandwidth?

The EIP bandwidth is used by ECSs to access the Internet through EIPs. The EIP bandwidth will be billed.

The private network bandwidth is used for communication between ECSs. The private network bandwidth and PPS of an ECS are determined based on ECS specifications. For details, see ECS Types.

4.10 Can I Increase My Bandwidth Billed on Yearly/Monthly Basis and Then Decrease It?

An increased bandwidth takes effect immediately. A decreased bandwidth will take effect in the first billing cycle after the EIP is renewed. For details, see Modifying EIP Bandwidth.

4.11 Can I Use Multiple Bandwidth Add-On Packages with Overlapping Validity Periods?

No.

A bandwidth add-on package is used to temporarily increase the maximum shared or dedicated bandwidth of a yearly/monthly EIP. You can buy multiple bandwidth add-on packages for the same bandwidth, but the validity periods of the packages cannot overlap. For details, see Bandwidth Add-On Package Overview and Buying a Bandwidth Add-On Package.

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

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

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

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) in consideration of losses, such as computer performance, network device quality, resource usage, and network peak hours.

4.13 What Are the Differences Between Static BGP and Dynamic BGP?

The differences between static BGP and dynamic BGP are as follows:

Table 4-2 Differences between static BGP and dynamic BGP

Aspect	Static BGP	Dynamic BGP
Definition	Static routes are manually configured and must be manually reconfigured any time the network topology or link status changes.	Dynamic BGP provides automatic failover and chooses the optimal path when a network connection fails.
Assurance	When changes occur on a network using static BGP, the manual configuration takes some time and high availability can't be guaranteed. **NOTE** If you select static BGP, your application system must have the disaster recovery capability.	When a fault occurs on a carrier's link, dynamic BGP will quickly select another optimal path to take over services, ensuring service availability. Currently, carriers in China that support dynamic BGP routing include China Telecom, China Mobile, China Unicom, China Education and Research Network (CERNET), National Radio and Television Administration, and Dr. Peng Group.

Aspect	Static BGP	Dynamic BGP
Service availability	99%	99.95%
Billing	Their price from least to most expensive: static BGP, dynamic BGP. For details, see EIP Pricing Details.	

NOTE

For more information about service availability, see Huawei Cloud Service Level Agreement.

4.14 What Is Enhanced 95th Percentile Bandwidth Billing?

The enhanced 95th percentile bandwidth billing mode allows you to use more bandwidth after you pay for the baseline bandwidth. You are billed based on the required duration and the average bandwidth size obtained after discarding some top bandwidth usages in a billing period.

Prerequisite

To use the enhanced 95th percentile billing mode, the following requirements must be met:

- Your level is greater than or equal to V4.
- You can select this billing mode when purchasing a shared bandwidth.
- The minimum bandwidth you can purchase is 300 Mbit/s.

Pricing Details

Billing formula: Monthly peak bandwidth x Monthly peak bandwidth price x Shared bandwidth in-use days/Calendar days of a month.

Billing cycle: Bills are generated for each calendar month.

NOTE

Billing mode: The enhanced 95th percentile bandwidth is billed on a pay-per-use basis, and does not require prepayment. The monthly fee is settled at the end of each calendar month.

Monthly peak bandwidth price: The price is preset and does not vary according to the number of days in a calendar month.

Shared bandwidth in-use days: Calculated based on the actual duration when the shared bandwidth is used. For example, if you apply for a shared bandwidth at 12: 00, the shared bandwidth use time is half a day.

NOTE

Shared bandwidth in-use days = Number of collected bandwidth values in a month/288.

Monthly peak bandwidth: The monthly peak bandwidth is calculated based on the enhanced 95 percentile billing mode in which some peak bandwidth values are discarded. It must be higher than the monthly baseline bandwidth.

Daily baseline bandwidth: Daily baseline bandwidth = Baseline percentage x Shared bandwidth. The baseline percentage is 20%.

In enhanced 95 percentile billing mode, the shared bandwidth can be adjusted in real time, and the adjustment takes effect immediately. After the shared bandwidth is adjusted, the baseline bandwidth changes accordingly. The daily baseline bandwidth is calculated based on the maximum baseline bandwidth set for a day. For example, if the bandwidth is adjusted from 100 Mbit/s to 300 Mbit/s and then to 200 Mbit/s during a day, the daily baseline bandwidth is 60 Mbit/s (300 x 20%).

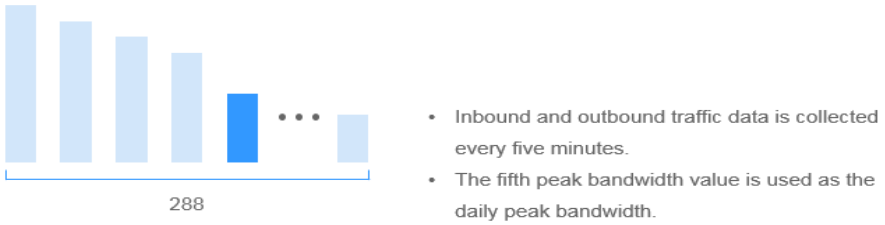
Monthly baseline bandwidth: The bandwidth can be adjusted frequently to suit the traffic requirements.

The monthly baseline bandwidth is calculated based on the following formula (only the integer is retained in the calculated result): Monthly baseline bandwidth = (Baseline bandwidth 1 x Number of days using baseline bandwidth 1 + Baseline bandwidth 2 x Number of days using baseline bandwidth 2 + ... + Baseline bandwidth n x Number of days using baseline bandwidth n)/Number of days using all baseline bandwidths in a month.

Monthly peak bandwidth calculation method

- Daily peak bandwidth
  - Inbound and outbound traffic data is collected every five minutes.
  - The averages of both inbound bandwidth and outbound bandwidth within five minutes are calculated, and the larger one is used as the bandwidth for that collection.
  - After all meter readings within a day are obtained, they are sequenced in descending order. The top four peak bandwidth values are discarded, and the fifth peak bandwidth value is used as the daily peak bandwidth.

  Figure 4-8 Daily peak bandwidth

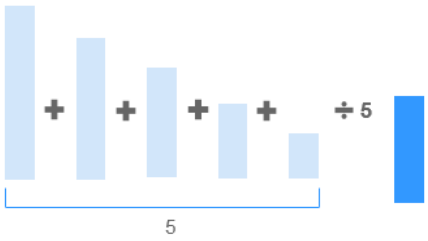
  NOTE

  If less than five peak bandwidth values are obtained in a day, the last value in the peak bandwidth sequence is used as the daily peak bandwidth. The daily peak bandwidth is an integer (any fractional parts are discarded).

- Monthly peak bandwidth

  At the end of each month, the daily peak bandwidth values are sequenced in descending order. The average of the top five daily peak bandwidth values is the monthly peak bandwidth (only the integer is retained and fractional parts are discarded).

Figure 4-9 Monthly peak bandwidth



- The daily peak bandwidth values of a month are sequenced in descending order.
- The average of the top five daily peak bandwidth values is the monthly peak bandwidth.

NOTE

If less than five daily peak bandwidth values are obtained, the average of all the daily peak bandwidth values in the month is the monthly peak bandwidth. The monthly peak bandwidth is an integer (any fractional parts are discarded).

The larger value between the baseline bandwidth of the month and the average of daily peak bandwidth values is used as the monthly peak bandwidth. If the baseline bandwidth of a month is greater than the average of the daily peak bandwidth values, the monthly peak bandwidth is equal to the baseline bandwidth of the month. Otherwise, the monthly peak bandwidth is equal to the average of daily peak bandwidth values.

5 Connectivity

5.1 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.

5.2 Why Does Internet Access Fail Even If My ECS Is Bound with an EIP?

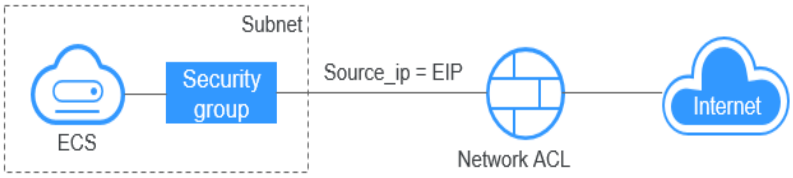
Symptom

You have an ECS that has an EIP bound, but the ECS cannot access the Internet.

Troubleshooting

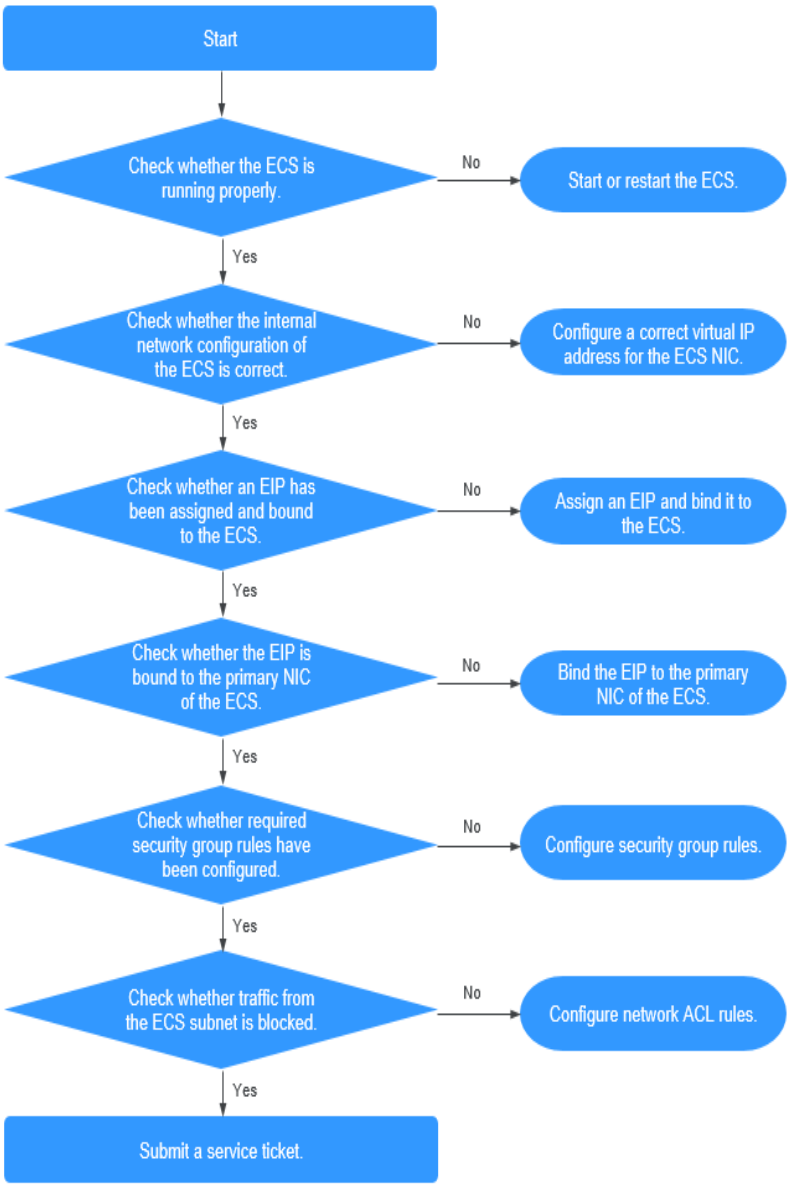
Figure 5-1 shows the process for an ECS to access the Internet using an EIP.

Figure 5-1 EIP network diagram



Locate the fault based on the following procedure.

Figure 5-2 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 the 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 whether the ECS is running properly.

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

Figure 5-3 ECS status

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

1. Check whether the ECS NIC has an IP address assigned.

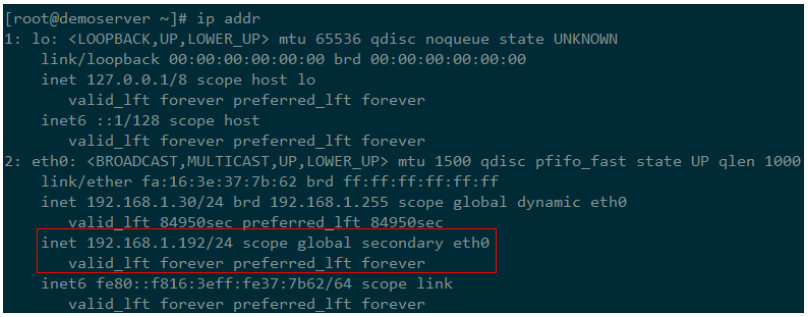
   Log in to the ECS, and run the **ifconfig** or **ip address** command to check the ECS NIC IP address.

   If an ECS runs the Window OS, run the **ipconfig** command.

2. Check whether the virtual IP address is correctly configured on the ECS NIC.

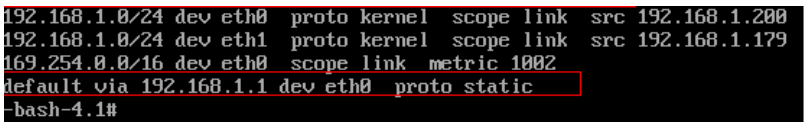
   Log in to the ECS, and run the **ifconfig** or **ip address** command to check the ECS NIC IP address. If the ECS NIC does not have an IP address configured, run a command to configure an IP address for the ECS NIC. For example, run the **ip addr add** *virtual IP address* **eth0** command to configure IP address **192.168.1.192/24** for the NIC.

   Figure 5-4 Virtual IP address of a NIC



   Check whether the default route exists. If no default route exists, run the **ip route add** command to add the default route.

   Figure 5-5 Default route

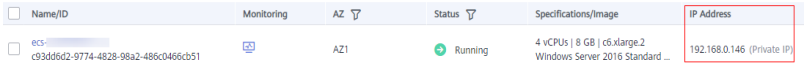


Step 3: Check Whether an EIP Has Been Assigned and Bound to the ECS

Check whether an EIP has been assigned and bound to the ECS. (If the EIP has not been assigned, assign an EIP and bind it to the ECS.)

The ECS shown in Figure 5-6 has no EIP bound and only has a private IP address bound.

Figure 5-6 EIP status

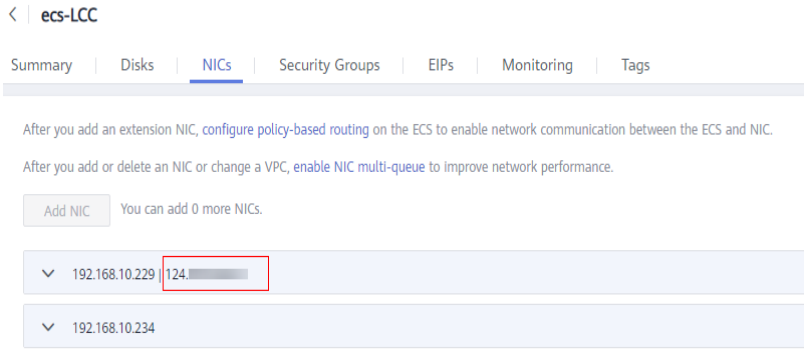


Step 4: Check Whether the EIP Is Bound to the Primary NIC of the ECS

Check whether the EIP is bound to the primary NIC of the ECS. If the EIP is not bound to the primary NIC of the ECS, bind it.

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 and the EIP is bound to the primary NIC as shown in the following figure.

Figure 5-7 Checking whether the EIP is bound to the primary NIC of the ECS



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 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 traffic filtering has been configured on the network ACL of the subnet used by the ECS NIC.

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

Submitting a Service Ticket

If the EIP still fails to communicate with the Internet after performing the preceding steps, submit a service ticket.

Provide the following information to the technical support engineer.

Item	Description	Example	Value
VPC CIDR block	Required for gateway configuration	Example: 10.0.0.0/16	N/A
VPC ID	N/A	Example: 120b71c7-94ac-45b8-8ed6-30aafc8fbdba	N/A
CIDR block of subnet 1 (can be the same as the VPC CIDR block)	N/A	Example: 10.0.1.0/24	N/A
ECS ID	N/A	N/A	N/A
ECS IP address	N/A	Example: 192.168.1.192/24	N/A
ECS route information	N/A	N/A	N/A
EIP	Required for the ECS to access the Internet	Example: 10.154.55.175	N/A
EIP bandwidth	Maximum bandwidth size used by the ECS to access the Internet	Example: 1 Mbit/s	N/A
EIP ID	N/A	Example: b556c80e-6345-4003-b512-4e6086abbd48	N/A

5.3 Why Cannot an EIP Be Pinged?

Symptom

After I purchased an EIP and bound it to an ECS, pinging the EIP failed, or the ECS failed to access the Internet.

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 5-8 Method of locating the failure to ping an EIP

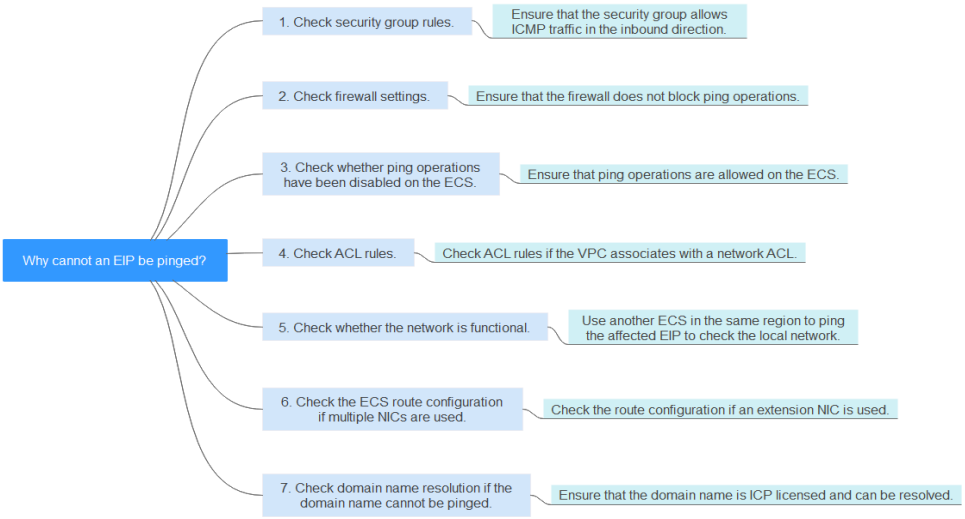


Table 5-1 Method of locating the failure to ping an EIP

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.
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 or cannot be resolved.	If the domain name cannot be pinged, the domain name is not ICP licensed or cannot be resolved. To resolve this issue, see Checking Domain Name Resolution If the Domain Name Cannot Be Pinged.

Checking Security Group Rules

The ping operations use the ICMP protocol. Check whether the security group accommodating the ECS allows ICMP traffic in the inbound direction.

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Under **Computing**, click **Elastic Cloud Server**.
4. On the **Elastic Cloud Server** page, click the name of the target ECS.

   The page providing details about the ECS is displayed.
5. Click the **Security Groups** tab, expand the information of the security group, and view security group rules.
6. Click the security group ID.

   The system automatically switches to the **Security Group** page.
7. On the **Inbound Rules** tab, click **Add Rule**. In the displayed dialog box, set required parameters to add an inbound rule.

   Figure 5-9 Setting an inbound rule

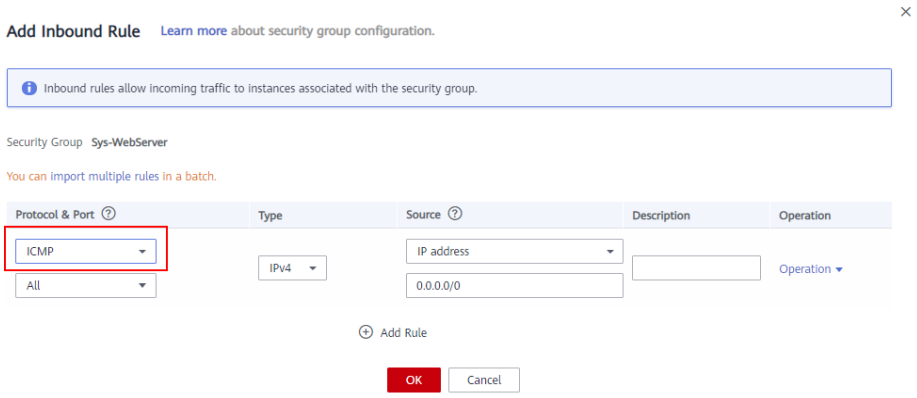


Table 5-2 Security group rules

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

8. 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

1. Run the following command to check the firewall status, taking CentOS 7 as an example:

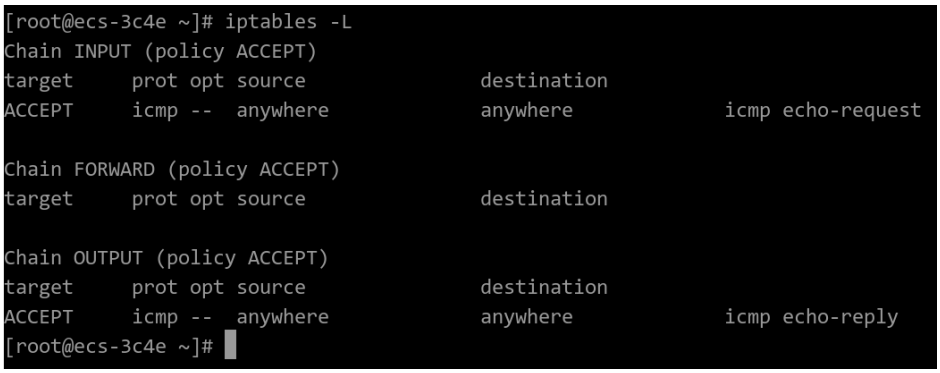
   firewall-cmd --state

   If **running** is displayed in the command output, the firewall has been enabled.
2. Check whether there is any ICMP rule blocking the ping operations.

   iptables -L

   If the command output shown in Figure 5-10 is displayed, there is no ICMP rule blocking the ping operations.

   Figure 5-10 Checking firewall rules



   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 5-11 Inbound Rules

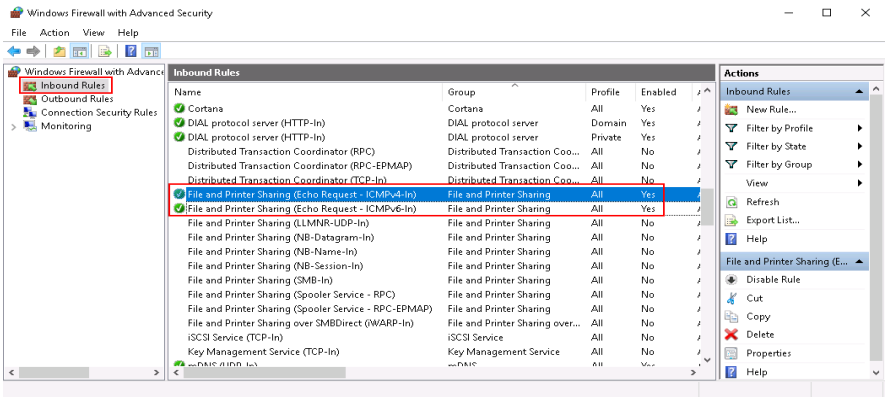
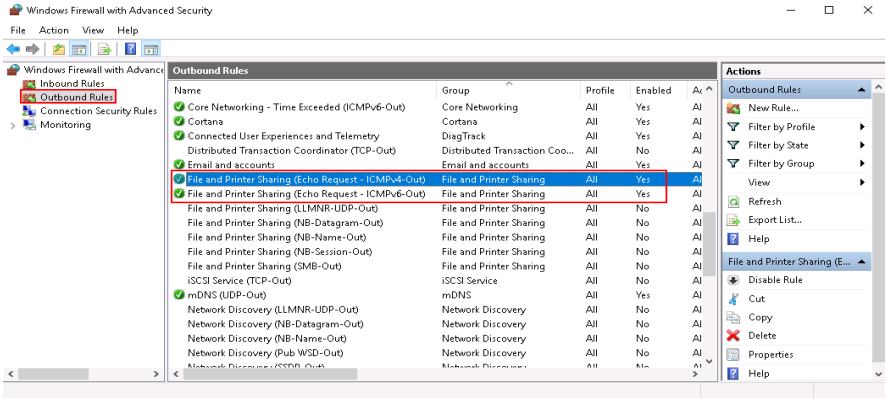


Figure 5-12 Outbound Rules



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:

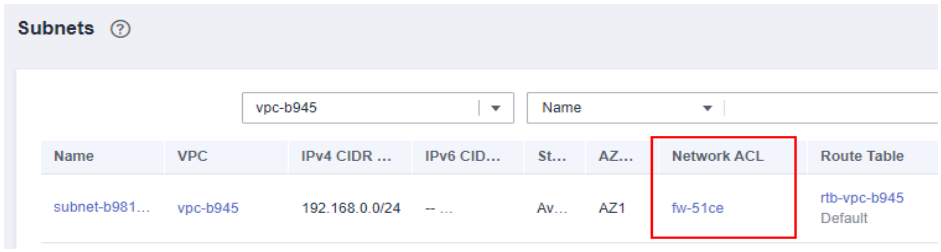
net.ipv4.icmp_echo_ignore_all=0

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.

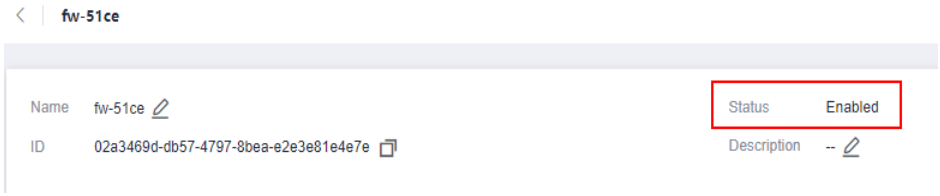
1. Check whether the subnet of the ECS has been associated with a network ACL.
   If an ACL name is displayed, the network ACL has been associated with the ECS.

   Figure 5-13 Network ACL



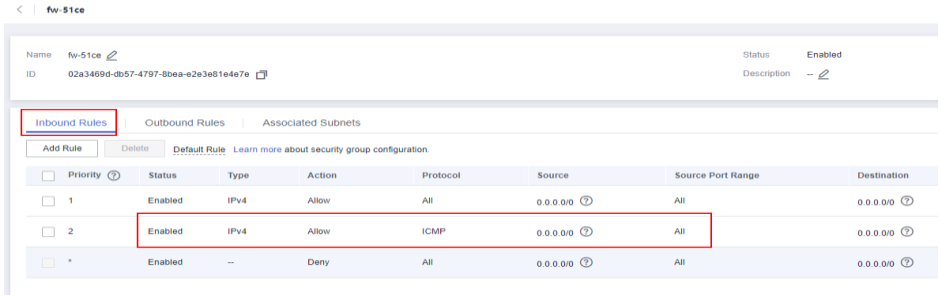
2. Click the ACL name to view its status.

   Figure 5-14 Enabled network ACL



3. If the network ACL is enabled, add an ICMP rule to allow traffic.

   Figure 5-15 Adding an ICMP rule



NOTE

The default network ACL rule denies all incoming and outgoing packets. After the network ACL is disabled, the default rule still takes effect.

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.

   For details, see Troubleshooting a Ping Failure or Packet Loss Using a Link Test.

Checking the ECS Route Configuration If Multiple NICs Are Used

The default route of an OS preferentially selects the primary NIC generally. If an extension NIC is selected in a route and the network malfunctions, this issue is generally caused by the 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 5-16 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.

  For details, see How Do I Configure Policy-Based Routing for ECSs with Multiple NICs?

Checking Domain Name Resolution If the Domain Name Cannot Be Pinged

If the EIP can be pinged but the domain name cannot be pinged, the possible cause is that the domain name has not obtained an ICP filing number or an error occurred in domain name.

1. Check the ICP filing of the domain name.

   According to the Regulation on Internet Information Service of the People's Republic of China released by the Ministry of Industry and Information Technology (MIIT), publicly accessed websites cannot be hosted on servers in the Chinese Mainland until an ICP filing number from the MIIT is obtained.

- If you want to use a server in the Chinese mainland to provide Internet services, you need to submit an ICP filing request to the server provider to obtain an ICP filing number for the domain name.
- If you use a server outside the Chinese mainland to provide Internet services, no ICP filing is required.

2. Check the domain name resolution.

   If your domain name has obtained an ICP filing number but the domain name resolution is not correctly configured, the domain name may fail to be pinged.

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

3. 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. In such a case, see Troubleshooting Slow Access of a Website Outside the Chinese Mainland over an ECS.

5.4 How Do I Unblock an EIP?

When the bandwidth of an EIP exceeds the threshold or an attack (usually a DDoS attack) occurs, the EIP will be blocked.

Blocked EIPs will be automatically unblocked 24 hours later if no attack occurs. It is recommended that you use Advanced Anti-DDoS to prevent attacks.