Elastic IP

Product Documentation

Contents

Elastic IP 3
- Product Introduction 3
  - Elastic IP Overview 3
  - Use Cases 5
  - Use Limits 7
- Quick Start 9
- Operation Guide 13
  - Obtaining EIP 13
    - Converting Ordinary Public IP to EIP 13
    - Applying for EIP 15
  - Binding EIP 16
    - Binding EIP to Cloud Resources 16
    - CVM Primary Network Interface Binds Multiple IP 18
    - CVM Adds a Secondary Network Interface and Binds Multiple IP 25
  - Managing EIP 33
    - Adjusting Bandwidth 33
    - Viewing Monitoring Data 35
  - Unbinding/Releasing EIP 37
    - Unbind EIP 37
    - Release EIP 38
- Best Practice 39
  - Migrating Public IP 39
- FAQs

Product Introduction
Elastic IP Overview

Elastic IP (EIP) is a public IP address that is fixed in a certain region and can be purchased and owned independently. EIP can be bound to CVM, NAT gateway, ENI, and BMS, providing the ability to access and be accessed by the public network.

EIP can be decoupled from the lifecycle of cloud resources and operated independently. For example, if you need to keep a public IP address that is closely related to your business, you can convert the ordinary public IP address to an EIP and keep it in your account.

Difference Between EIP and Ordinary Public IP

A public IP address is a non-reserved address on the Internet. A cloud server with a public IP address can access other computers on the Internet.
Both ordinary public IP and EIP are public IP addresses, and both can provide CVM with the ability to access and be accessed by the public network.

- EIP: A public IP address resource that can be purchased and held independently and can be bound or unbound to CVM, NAT gateway, ENI, and BMS at any time.
- Ordinary Public IP: It can only be allocated when purchasing CVM and cannot be unbound from the cloud server. If it is not allocated when purchasing, it cannot be obtained.
  Compared with the ordinary public IP of CVM, EIP provides more flexible management methods, as shown in the following table. For details, see Public IPv4 Address.

Comparison Item	Ordinary Public IP	EIP
Accessing the Public Network/Being Accessed by the Public Network	✓	✓
Independent Purchase and Hold	×	✓
Free Binding and Unbinding	×	✓
Adjusting Bandwidth in Real Time	✓	✓

Strengths

Flexible

EIP is an independent public IP resource that belongs to your cloud platform account rather than any cloud resource. It can be bound and unbound to CVM, NAT gateway, ENI, BMS, etc., at any time and can be used flexibly and take effect in real time.

Easy to Operate

EIP supports on-demand purchases, configuration changes take effect in real time, and can be managed and operated through a variety of methods, such as the console and Cloud API.

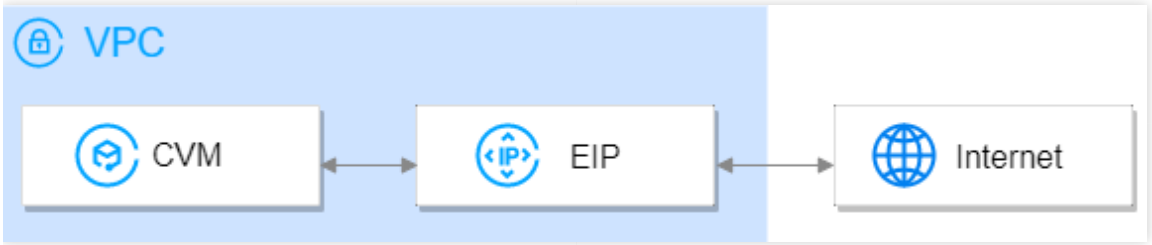
Use Cases

This document introduces the main use cases of EIP: Providing public network access capabilities and disaster recovery.

Providing Public Network Access Capabilities

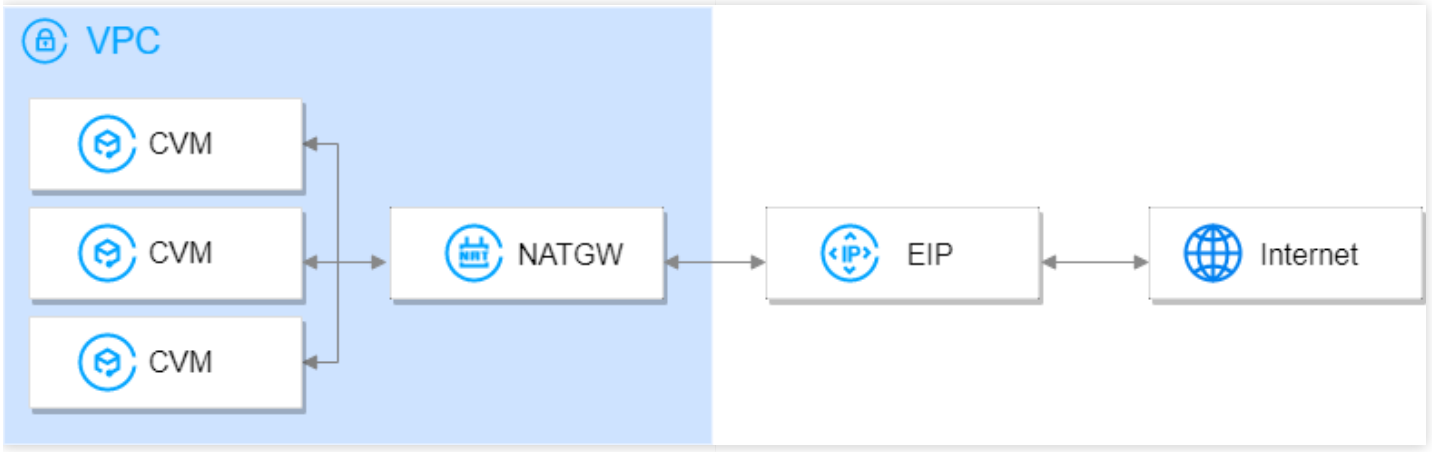
Binding CVM

EIP can be bound to a CVM, providing the CVM with the ability to access and be accessed by the public network.



Binding NAT Gateway

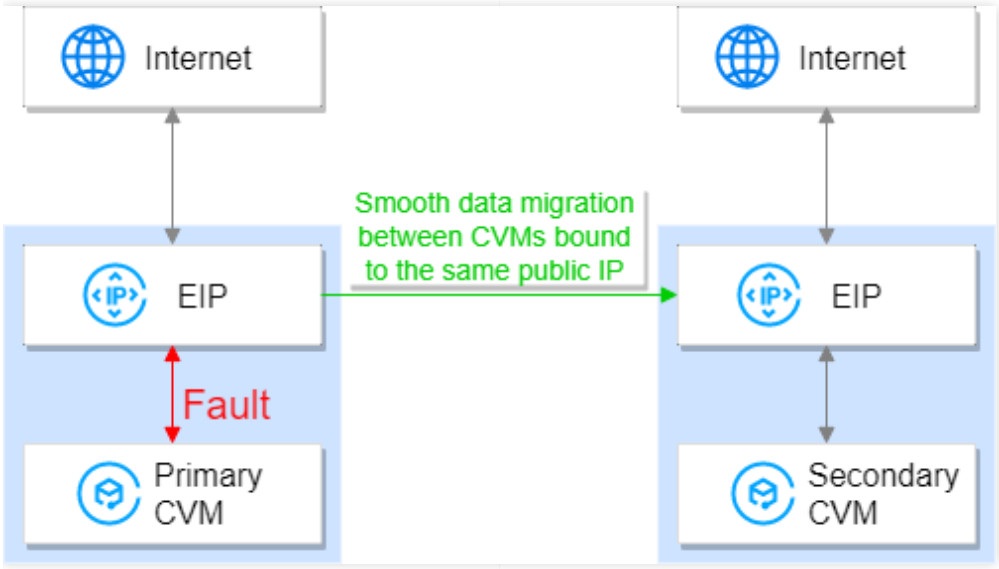
EIP can be bound to a NAT gateway. Through the SNAT and DNAT features of the NAT gateway, multiple CVMs without public IP addresses can access and be accessed by the public network.



Disaster Recovery

In an active-active disaster recovery scenario, applications and resources of the primary and backup CVM are synchronized in real time. The primary CVM is bound to the EIP. When the primary CVM fails, the EIP

can be unbound from the primary CVM and rebound to the backup CVM. The public IP used by the business can be smoothly migrated from the failed primary CVM to the backup CVM without modifying the DNS and other mapping relationships, ensuring service continuity.



Use Limits

Before you use the EIP, be aware of the following usage rules and quota limits.

Usage Rules

- EIP addresses can be bound to CVM, NAT gateway, ENI, and BMS.
- For EIP directions, see Operation Guide.

Quota Limit

EIP Quota Limit

Resources	Limit
EIP Quota for a Single Region per Account	20
Number of EIP Purchases per Account in a Single Region per Day	Number of quotas x 2
Number of Free Public IP Reallocations per Account Every Day When EIP Is Unbound	10

> Note:
>
> By default, EIP quotas cannot be adjusted. IP convergence can be performed through the NAT gateway and CLB.
>
> - If there are special circumstances that require adjustment, the account must have cloud service resources of the corresponding magnitude and use them reasonably.
> - If the required quota is higher, there may be a charge for exceeding the quota. Submit a ticket for details.
> - If there are frequent changes of IP and violations of applicable laws and regulations after the adjustment, the cloud platform has the right to recover the quota.

Limits on Binding CVM

Starting from September 18, 2019 (include), the maximum number of public IP addresses that can be

bound to a single CVM changes depending on the CPU configuration. The specific numbers are shown in the following table:

> Note:
>
> - CVM purchased before midnight on September 18, 2019, are not subject to the following limits.
> - If your CVM is purchased through a cloud platform activity, the number of public IP addresses that the CVM supports is subject to the activity rules.

Number of CPUs in the CVM	The maximum number of public IP addresses that can be bound (including ordinary public IP addresses and EIP addresses)
CPU: 1–5	2
CPU: 6–11	3
CPU: 12–17	4
CPU: 18–23	5
CPU: 24–29	6
CPU: 30–35	7
CPU: 36–41	8
CPU: 42–47	9
CPU: ≥ 48	10

Limits on Binding NAT Gateway

- Each NAT gateway needs to be bound to at least one EIP to have the ability to access the public network.
- Each NAT gateway supports a maximum of 10 EIP bindings.

Limits on Binding ENI

Each private IP on an ENI can be bound to a public IP (including ordinary public IP and EIP).

Quick Start

EIP is a public IP address resource that can be purchased and owned independently. After EIP is bound to cloud resources, cloud resources can communicate with the public network through EIP. This document uses EIP binding to CVM as an example to introduce the EIP usage lifecycle.

Background

The lifecycle of an EIP includes applying for an EIP, binding an EIP to a CVM, unbinding an EIP to a CVM, and releasing an EIP.



1. Apply for EIP: Apply for EIP resources based on actual usage needs.
2. Bind EIP to CVM: Bind EIP to the CVM instance and communicate with the public network through EIP.
3. Unbind EIP from CVM: After unbinding an EIP from a CVM instance, you can bind the EIP to other cloud resources. After you unbind an EIP from a CVM instance, the network of the corresponding CVM instance may be disconnected. Operate with caution.
4. Release EIP: If you no longer need to use the EIP, you can release it. No fees are incurred after release, but be aware that you may not be able to retrieve it after release.

Prerequisites

Ensure that the EIP and the bound CVM instance are in the same region. You can view the region of the corresponding EIP and CVM instance in the EIP or Instance interface of the CVM console.

Directions

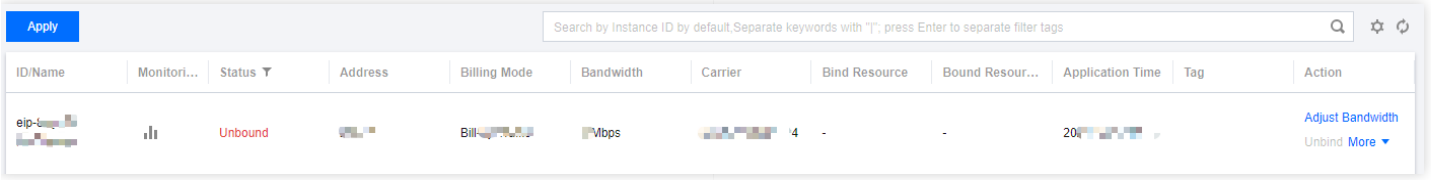
Step 1: Apply for EIP

1. Log in to the CVM console and choose EIP in the left sidebar to enter the EIP interface.
2. Select Region at the top of the EIP page and click Apply.
3. In the pop-up Apply for EIP dialog box, perform the following operations:

Parameter	Description
Selecting Region	Since EIP has a region attribute, select the region to which the EIP belongs.
Carrier	Specify the ISP attribute of the EIP. Currently, China Telecom, China Unicom, China Mobile, and the public network CAP are supported.
Billing Mode	Bill by traffic.
Max. Bandwidth	Set the bandwidth limit as needed and allocate bandwidth resources reasonably.
Quantity	Select the number of applications as needed and ensure that the total number of EIPs does not exceed the total product quota. For details, see Quota Limit.

4. Click Confirm to complete the EIP application.
5. In the list, you can view the applied EIP, which is currently unbound.

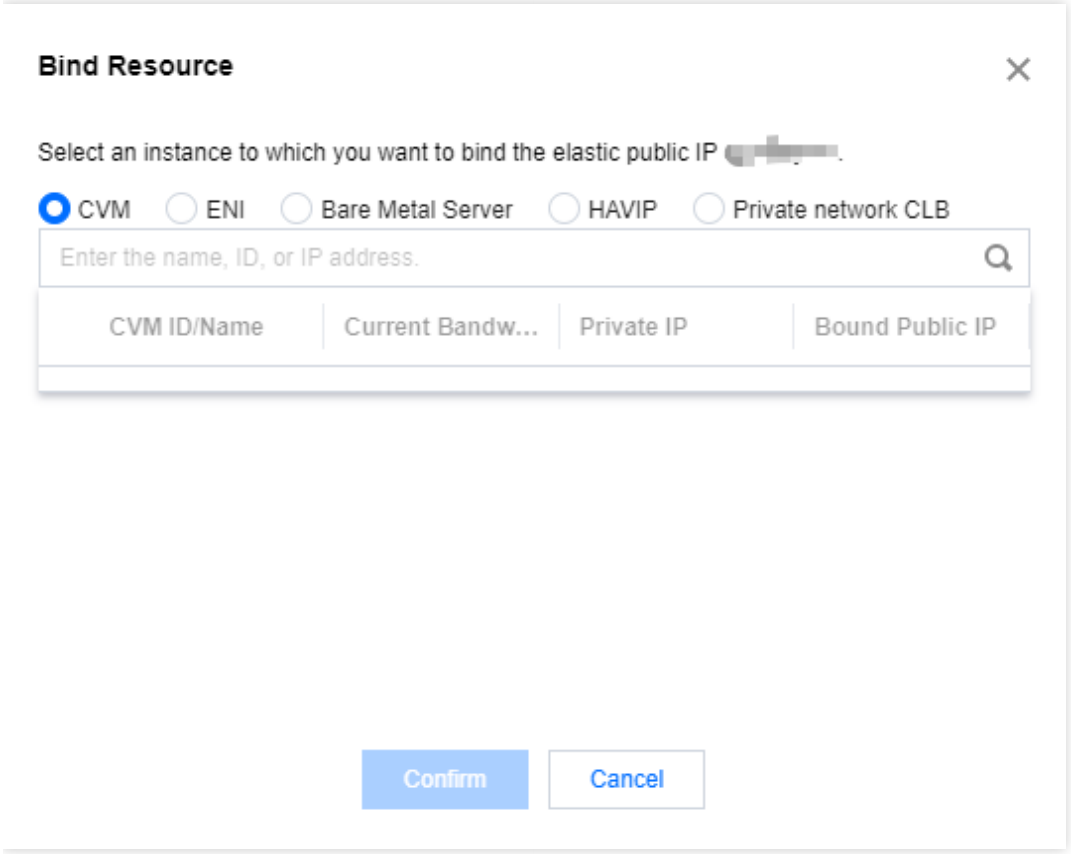
> Note:
>
> We recommend that you bind unbound EIP to cloud resources in a timely to save IP resources.



Step 2: Bind EIP to CVM

1. Log in to the CVM console, select EIP, and enter the EIP interface.
2. In the Action column to the right of the target EIP, select More > Bind.
3. In the Bind Resources window that pops up, click CVM, select the CVM instance to be bound, and then click Confirm.

> Note:
>
> If the CVM instance already has an ordinary public IP, you must release the ordinary public IP before you can bind the EIP.
> The number of CVM instances that can be bound to an EIP varies depending on the CPU configuration of the CVM instance. See Limits.



4. In the Confirm Binding dialog box that pops up, click OK to complete the binding with the cloud resources.

Step 3: Unbind EIP from CVM

1. Log in to the CVM console, select EIP, and enter the EIP interface.
2. In the Action column to the right of the target EIP, click Unbind.
3. In the Unbind EIP window that pops up, confirm the unbinding information and click Confirm.

Step 4: Release EIP

1. Log in to the CVM console, select EIP, and enter the EIP interface.
2. In the Action column to the right of the target EIP, select More > Release.
3. In the window confirming the release of the selected EIP that pops up, check Confirm to Release the Above IP and click Release.

Related Information

- If you need to convert the ordinary public IP of the CVM to EIP, see Converting Ordinary Public IP to EIP.
- If you need to bind other cloud resources, such as NAT gateways and ENI, see Binding EIP to Cloud Resources.
- If you need to adjust the peak bandwidth of the EIP, see Adjusting Bandwidth.

Operation Guide
Obtaining EIP
Converting Ordinary Public IP to EIP

You can convert the ordinary public IP of the CVM to an EIP. After the conversion is completed, the EIP has the ability to be unbound and bound to the CVM at any time, making it easier to achieve flexible management of the public IP.

Background

A public IP address is a non-reserved address on the Internet. A cloud server with a public IP address can access other computers on the Internet.
There are two types of public IP addresses: ordinary public IP and EIP. Both can provide CVM with the ability to access and be accessed by the public network.

- Ordinary Public IP: It can only be allocated when the CVM is purchased and cannot be unbound from the CVM. If it is not allocated when purchasing, it cannot be obtained.
- EIP: It is a public IP address resource that can be purchased and held independently and can be bound or unbound to cloud resources such as CVM and NAT gateways at any time.
  Compared with the ordinary public IP of the CVM, EIP provides more flexible management methods, as shown in the following table. For details, see public network IPv4 Address.

Comparison Item	Ordinary Public IP	EIP
Accessing the Public Network/Being Accessed by the Public Network	Supported	Supported
Independent Purchase and Hold	Not supported.	Supported
Free Binding and Unbinding	Not supported.	Supported
Adjusting Bandwidth in Real Time	Supported	Supported
IP Resource Usage Fees	Not supported.	Supported

Operation Instructions

- Before converting an ordinary public IP to an EIP, ensure that the total number of EIPs does not exceed the total product quota. For details, see Quota Limit.
- The conversion of an ordinary public IP to an EIP does not affect the CVM's ability to access or be accessed by the public network.
- After an ordinary public IP is converted to an EIP, the original address is not changed.
- After an ordinary public IP is converted to an EIP, it cannot be converted back to a public IP.

Directions

You can convert an ordinary public IP to an EIP by following the directions below:

1. Log in to the CVM console and click CVM in the left sidebar.
2. On the instance management page, select the region where the instance to be converted is located, and click  to the right of the ordinary public IP of the corresponding instance.
3. In the converting to EIP pop-up window that pops up, click OK.

Next Steps

If you need to adjust the peak bandwidth of the EIP, see Adjusting Bandwidth.

Applying for EIP

EIP is a public IP address resource that can be purchased and owned independently. You can apply for an EIP by following the steps below.

Directions

1. Log in to the CVM console and choose EIP in the left sidebar to enter the EIP interface.
2. Select Region at the top of the EIP page and click Apply.
3. In the pop-up Apply for EIP dialog box, perform the following operations:

Parameter	Description
Selecting Region	Since EIP has a region attribute, select the region to which the EIP belongs.
Carrier	Specify the ISP attribute of the EIP.
Billing Mode	Bill by traffic.
Bandwidth Cap	Set the bandwidth limit as needed and allocate bandwidth resources reasonably.
Quantity	Select the number of applications as needed and ensure that the total number of EIPs does not exceed the total product quota. For details, see Quota Limit.

4. Click Confirm to complete the EIP application.
5. In the list, you can view the applied EIP, which is currently unbound.

> Note:
>
> We recommend that you bind unbound EIP to cloud resources in a timely to save IP resources.

Next Steps

If you need to bind cloud resources to EIP, see Binding EIP to Cloud Resources.

Binding EIP
Binding EIP to Cloud Resources

You can bind an EIP to cloud resources such as CVM instances and NAT gateways and use EIP to flexibly provide disaster recovery and public network communication services.

Overview

- EIP is bound to the CVM instance. EIP is the public IP of the CVM instance. When a CVM instance fails, it can be unbound and rebound to a healthy CVM instance to help quickly restore services.
- EIP is bound to the NAT gateway, and port forwarding is configured using EIP so that resources on the CVM can be accessed from the public network.
- The EIP is bound to the private IP of the ENI, and the ENI is bound to the CVM instance to provide public network communication services for the CVM instance.
- The EIP is bound to the BMS and serves as the public IP of the BMS. When a BMS fails, it can be unbound and rebound to a healthy BMS to help quickly restore services.

Directions

1. Log in to the CVM console, select EIP, and enter the EIP interface.

2. On the EIP management page, select the region of the EIP to which you want to bind cloud resources, and click More > Bind in the operation column of the corresponding EIP.

   > Note:
   >
   > If the EIP has been bound to cloud resources, unbind it first. For example, you need to replace the EIP of a faulty CVM instance with a healthy CVM instance.

3. In the Bind Resource window that pops up, select the cloud resource to which the EIP is to be bound and click Confirm.

Bound Cloud Resources	Description
CVM Instance:	- The EIP is bound to the CVM instance. The CVM instance must not be bound to other EIPs and must not be allocated an ordinary public IP.

Bound Cloud Resources	Description
	- The EIP and CVM instances must be bound in the same region. - The number of CVM instances that can be bound to an EIP varies depending on the CPU configuration of the CVM instance. See Limits.
NAT Gateway	- The EIP and NAT gateway must be bound in the same region. - A NAT gateway can be bound to a maximum of 10 EIPs. - When a NAT gateway is bound to multiple EIPs, the system automatically performs a CLB.
Elastic Network Interface	- When an EIP is bound to the private IP of a primary network interface, the CVM instance bound to the primary network interface must not have an ordinary public IP allocated to it. - An EIP can only be bound to one private IP of the ENI. - When EIP is bound to the private IP of the secondary network interface, the secondary network interface has a public IP in addition to its private IP. You can bind multiple secondary network interfaces bound to EIP to the CVM instance and flexibly use multiple public IPs to provide public network communication services to the outside world, thus realizing a high-availability network solution.
BMS	EIP is bound to the BMS, providing the BMS with the ability to communicate with the public network.

4. In the pop-up confirmation dialog box, click OK to complete the binding with the cloud resources.

Next Steps

- If you need to unbind cloud resources from an EIP, see Unbinding Cloud Resources from EIP.
- If you need to adjust the peak bandwidth of the EIP, see Adjusting Bandwidth.

CVM Primary Network Interface Binds Multiple IP

A single CVM can be bound to a maximum number of public IP addresses (including ordinary public IP and EIP) to achieve traffic transfer and improve the CVM usage. This document introduces how to bind multiple EIPs to Linux and Windows CVM.

Prerequisites

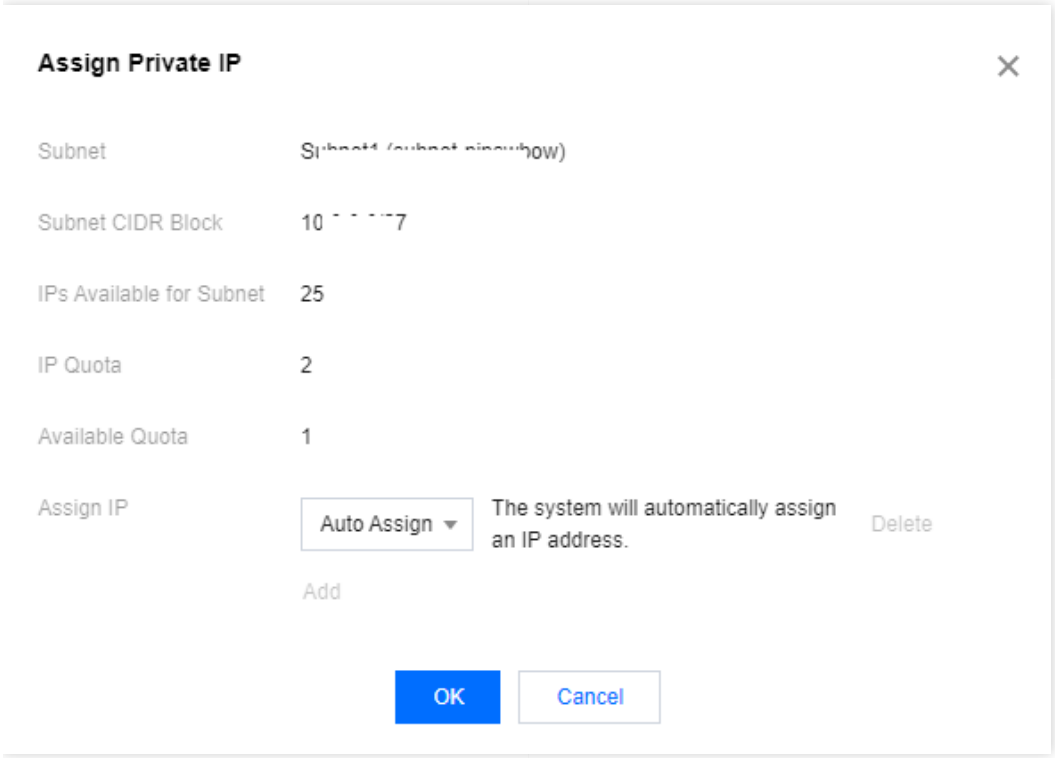
- You have purchased Linux CVM and Windows CVM, and the ICMP protocol is enabled in the security group.
- Ensure that your public IP is within the limit. For specific limits, see Limits.
- Ensure that the number of private IPs bound to a single network interface is within the limit.

Directions

Step 1: Allocate Private IP

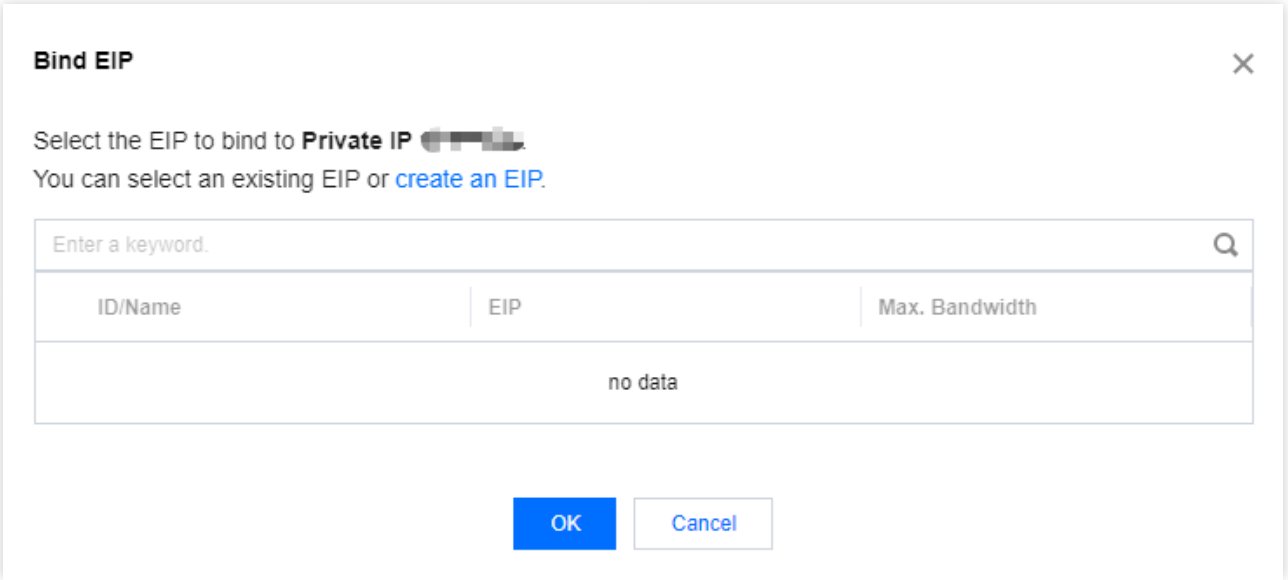
1. Log in to the CVM console.
2. In the instance list, click your CVM ID. On the details page, select ENI.
3. On the ENI page, click Assign Private IP on the right side of the primary network interface.
4. In the pop-up Assign Private IP dialog box, select automatic allocation or manually fill in the private IP to be allocated. If you need to allocate multiple private IPs, click Add and fill in the private IP to be allocated. After completion, click OK.

   > Note:
   >
   > If you choose to fill in manually, make sure that the private IP you fill in is within the subnet IP range and is not a system-reserved IP.
   >
   > For example, if the subnet segment is: 10.0.0.0/24 , then the available private IP range is : 10.0.0.2 - 10.0.0.254 . This operation takes manually filling in 10.0.0.3 as an example.

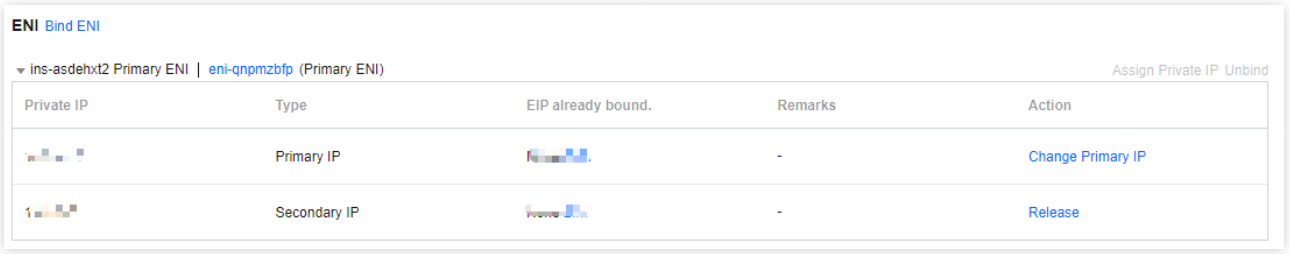


Step 2: Bind EIP

1. On the ENI page, click to expand the primary network interface information.
2. In the row of the private IP whose allocated type is secondary IP, click Bind under the Bound EIP column.
3. In the pop-up Bind EIP dialog box:
   - If there is an optional EIP, select it and click OK.
   - If there is no EIP available, click Create an EIP on the top of the pop-up window to apply for it. For details, see Applying for EIP. After the application is successful, return to the pop-up box and click Refresh to see the applied EIP, select it, and click OK.



4. In the list of primary network interfaces, you can view information about the binding of the private IP to the public IP.



Step 3: Configure the network interface

Select the corresponding network interface configuration operation according to the type of your CVM operating system:

- Linux CVM
- Windows CVM

Linux CVM

The following operations take CentOS 7 CVM as an example:

1. Log in to the CVM console.

2. In the instance list, click your CVM ID. On the details page, select ENI.

3. Click the primary network interface ID to enter the primary network interface details page and record the following information based on the subnet to which it belongs:
   - Subnet Mask: As shown in the figure below, the CIDR bit number of the subnet is /24; that is, the subnet mask is 255.255.255.0 .
   - Gateway: If you have not changed other settings, the gateway is the first IP of the subnet range. For example, the first IP of the subnet range in the figure below is 10.0.0.1 .

4. Log in to the CVM. For details, see Logging in to Linux Instance Using the Standard Log-in Method (Recommended).

5. Run the following command to back up the network interface information.

   ```
   cp /etc/sysconfig/network-scripts/ifcfg-eth0{,.bak}
   ```

6. Run the following command to open the network interface configuration file.

   ```
   vim /etc/sysconfig/network-scripts/ifcfg-eth0
   ```

7. You can press i to switch to the Edit mode and modify the configuration file content to:

```
# Created by cloud-init on instance boot automatically, do not edit.
#
# Change this to static
BOOTPROTO=static
DEVICE=eth0
#
# Comment this line
# HWADDR=52:54:00:8a:7a:64
#
# Add the following lines.
#
# Configure the primary IP.
IPADDR0=10.0.0.2 # Step 1: Bind the primary IP found in EIP. Fill in according to the actual situation.
NETMASK0=255.255.255.0 # The subnet mask recorded in step 3. Fill in according to the actual situation.
# Configure secondary IP 1.
IPADDR1=10.0.0.3 # Step 1: Bind the secondary IP manually filled in the EIP. Fill in according to the actual situ
ation.
NETMASK1=255.255.255.0
# If you have multiple secondary IPs, continue to configure secondary IP2, secondary IP3...
#IPADDR2=10.0.0.4
#NETMASK2=255.255.255.0
#IPADDR3=10.0.0.5
#NETMASK3=255.255.255.0
#.....
# Configure the gateway.
GATEWAY=10.0.0.1 # The gateway recorded in step 3. Fill in according to the actual situation.
#
NM_CONTROLLED=no
ONBOOT=yes
PERSISTENT_DHCLIENT=yes
TYPE=Ethernet
USERCTL=no
```

After it is modified, the example is as follows:

```
# Created by cloud-init on instance boot automatically, do not edit.
#
BOOTPROTO=static
DEVICE=eth0
#HWADDR=52:54:00:8a:7a:64
IPADDR0=10.0.0.2
NETMASK0=255.255.255.0
IPADDR1=10.0.0.3
NETMASK1=255.255.255.0
GATEWAY=10.0.0.1
NM_CONTROLLED=no
ONBOOT=yes
PERSISTENT_DHCLIENT=yes
TYPE=Ethernet
USERCTL=no

~
```

8. After completing the modification, press Esc, enter :wq! Press Enter to save the configuration and return.
9. Run the following command to restart the network service:

   systemctl restart network.service

   10. Run the following command to view the IP address:

   ip address

```
[root@VM_0_2_centos ~]# ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 52:54:00:59:de:bb brd ff:ff:ff:ff:ff:ff
    inet 10.0.0.2/24 brd 10.0.0.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet 10.0.0.3/24 brd 10.0.0.255 scope global secondary eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::5054:ff:fe59:debb/64 scope link
       valid_lft forever preferred_lft forever
```

Windows CVM

The following operations take Windows 2012 CVM as an example:

1. Log in to the CVM. For details, see Log in to Windows Instance Using RDP Files.

2. Follow the steps below to view the IP address, subnet mask, default gateway, and DNS server of the CVM:

3. On the operating system interface, select  in the lower left corner, click  , open the Windows PowerShell window and run the following command:

   ipconfig /all

4. Record the IPv4 address, subnet mask, default gateway, and DNS server values from the output of the network API information.

5. Go to the operating system's Control Panel > Network and Internet > Network and Sharing Center and click the network interface named Ethernet to edit it.

6. In the Ethernet Status pop-up window, click Attribute.

7. In the Ethernet Attributes pop-up window, select Internet Protocol Version 4 (TCP/IPv4) and click Attribute.

8. In the Internet Protocol Version 4 (TCP/IPv4) Attributes pop-up window, fill in the following information:

Parameter Name	Parameter Value
IP Address	The IPv4 address in the above Step 2.
Subnet Mask	The subnet mask in the above Step 2.
Default Gateway	The default gateway address in the above Step 2.
Preferred DNS Server	The DNS servers in the Above Step 2.
Backup DNS Server	The backup DNS Servers in the Above Step 2. If no backup DNS servers are listed, this parameter is not required.

9. Click Advanced and configure the secondary private IP.
10. Under the pop-up window Advanced TCP/IP Settings, in the IP Address module, click Add.
11. In the TCP/IP Address pop-up window, fill in the secondary private IP configured in Step 2: Bind EIP and subnet mask in the above Step 2, and click Add. If there are multiple secondary IPs, repeat the previous step and the current step.
12. In the Internet Protocol Version 4 (TCP/IPv4) Attribute pop-up window, click OK.
13. In the Ethernet Attribute pop-up window, click OK to complete the configuration.
14. In the "Ethernet Status" popup, click Details to view the configured IP information.

Step 4: Result verification

Log in to other CVM and execute ping <secondary IP public network address> command. If the following information is displayed, the binding is successful.

If the following results are not obtained after executing the command, check whether the ICMP protocol is enabled in the CVM security group configuration.

CVM Adds a Secondary Network Interface and Binds Multiple IP

If the limit of public IPs that can be bound to a single CVM does not meet your needs, you can add a secondary network interface to bind multiple public IPs to achieve traffic transfer and improve CVM usage. This document introduces how to add a secondary network interface to a Linux CVM and a Windows CVM and bind multiple EIPs.

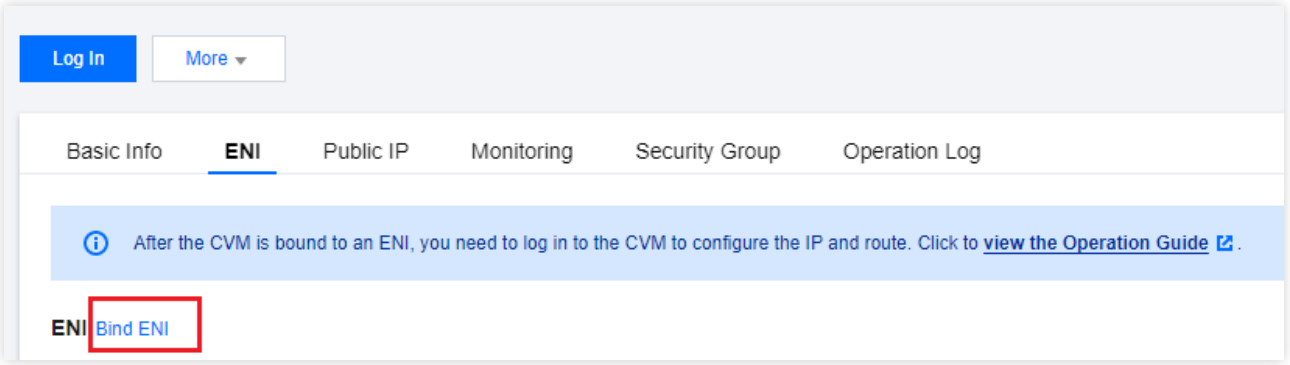
Prerequisites

- You have purchased Linux CVM and Windows CVM, and the ICMP protocol is enabled in the security group.
- Ensure that your public IP is within the limit. For specific limits, see Limits.
- Ensure that the number of private IPs bound to your secondary network interface is within the limit.

Directions

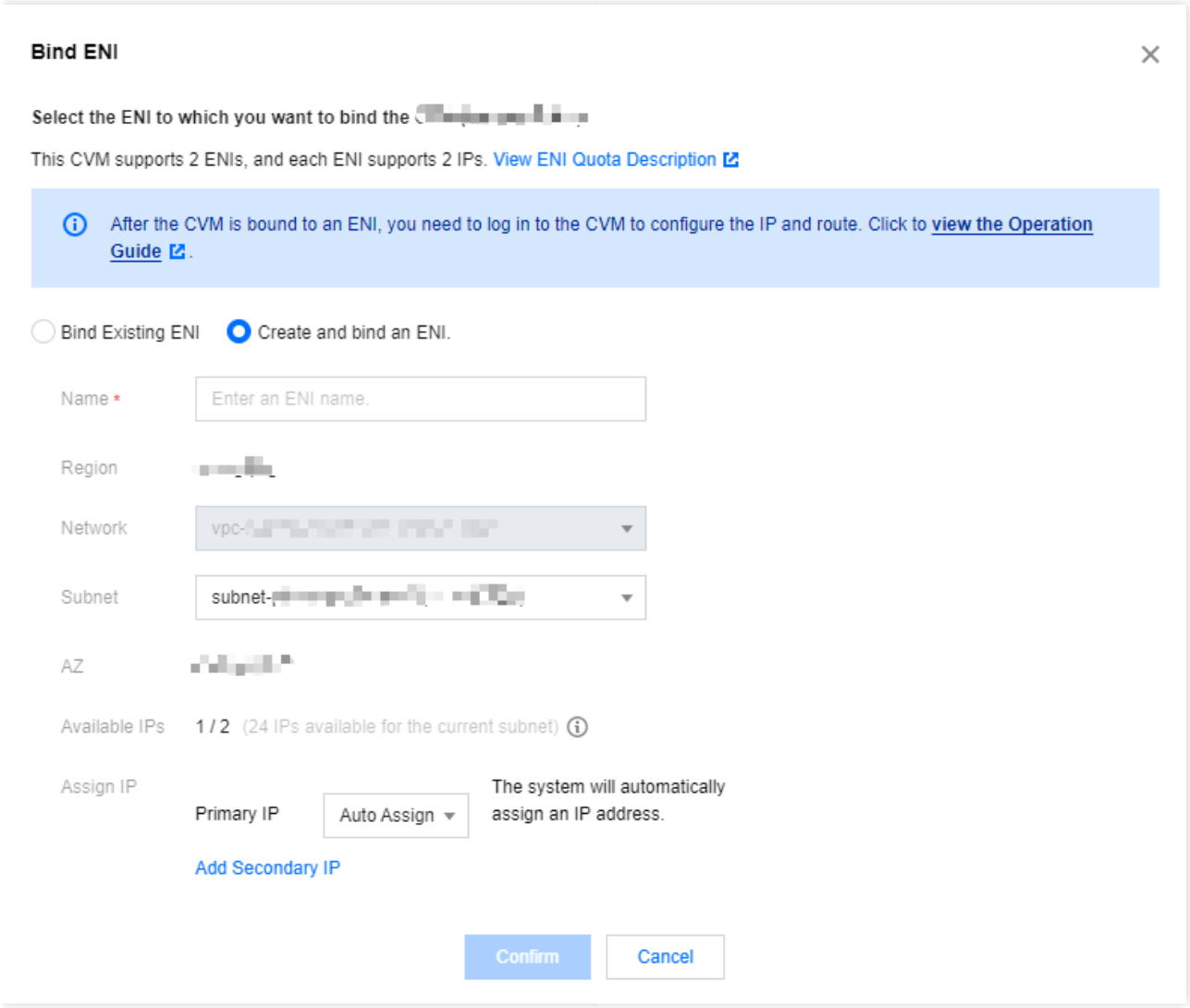
Step 1: Add secondary network interface

1. Log in to the CVM console and click CVM in the left sidebar.
2. In the CVM list, click your CVM ID and select ENI on the details page.



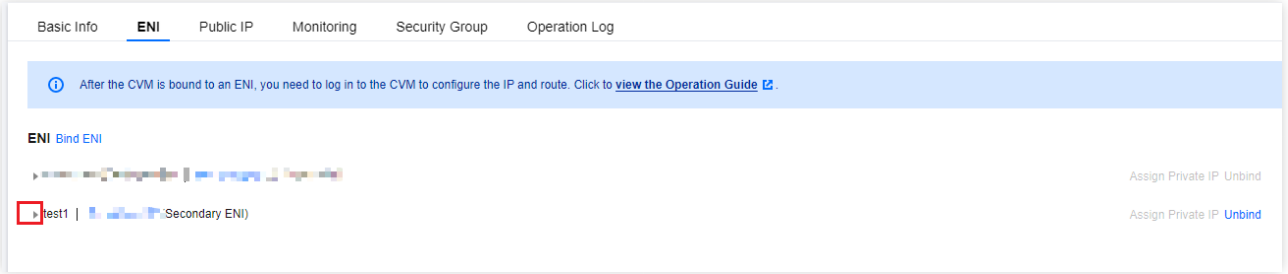
3. On the ENI page, click Bind ENI.
4. In the Bind ENI window that pops up, select the ENI to be bound. If you have not created an ENI, click Create and Bind an ENI, enter a name, select the subnet to which the ENI belongs, and select the allocated private IP (which can be automatically allocated or manually entered).

> Note:
>
> - If you need to allocate multiple IPs, click Add Secondary IP.
>
> If you choose to fill in manually, make sure that the private IP you fill in is within the subnet IP range and is not a system-reserved IP.
> For example, if the subnet segment is: 10.0.0.0/24 , the available private IP range is: 10.0.0.2 - 10.0.0.254 . This operation takes 10.0.0.7 as the primary IP and 10.0.0.8 as the secondary IP manually entered as an example.



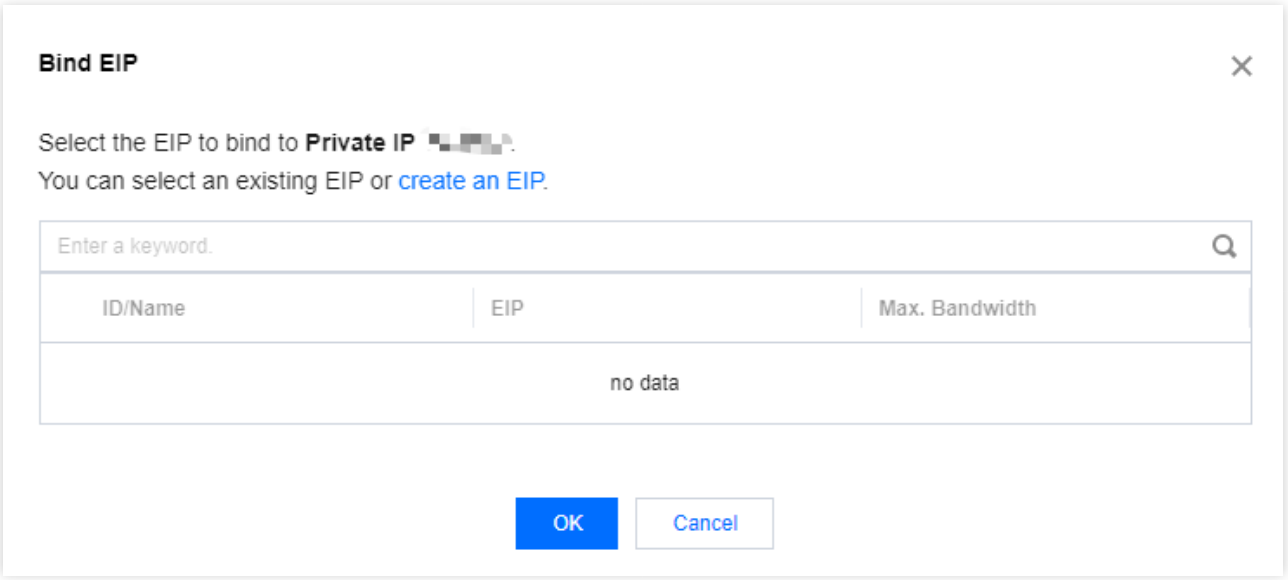
Step 2: Bind EIP

1. On the ENI page, click to expand the bound secondary network interface information.

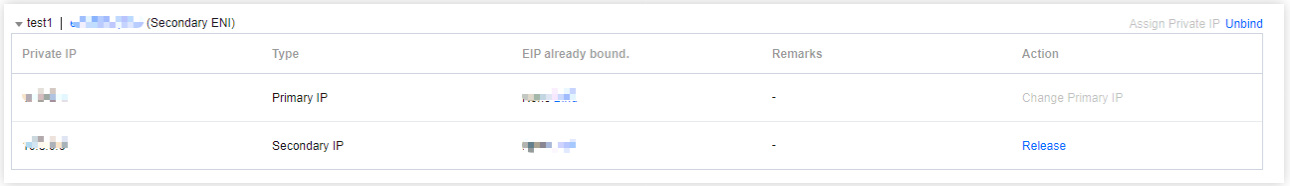


2. Under the Bound EIP column of the allocated IP, click Bind to bind an EIP to the allocated IP.
3. In the Bind EIP window that pops up:
   - If there is an optional EIP, select it and click OK.
   - If there is no EIP available, click Create an EIP on the top of the pop-up window to apply for it. For details, see Applying for EIP. After the application is successful, return to the pop-up box and click Refresh to see

the applied EIP, select it, and click OK.



4. In the list of secondary network interfaces, you can view information about the binding of the private IP to the public IP.



Step 3: Configure the network interface

Select the corresponding network interface configuration operation according to the type of your CVM operating system:

- Linux CVM
- Windows CVM

Linux CVM

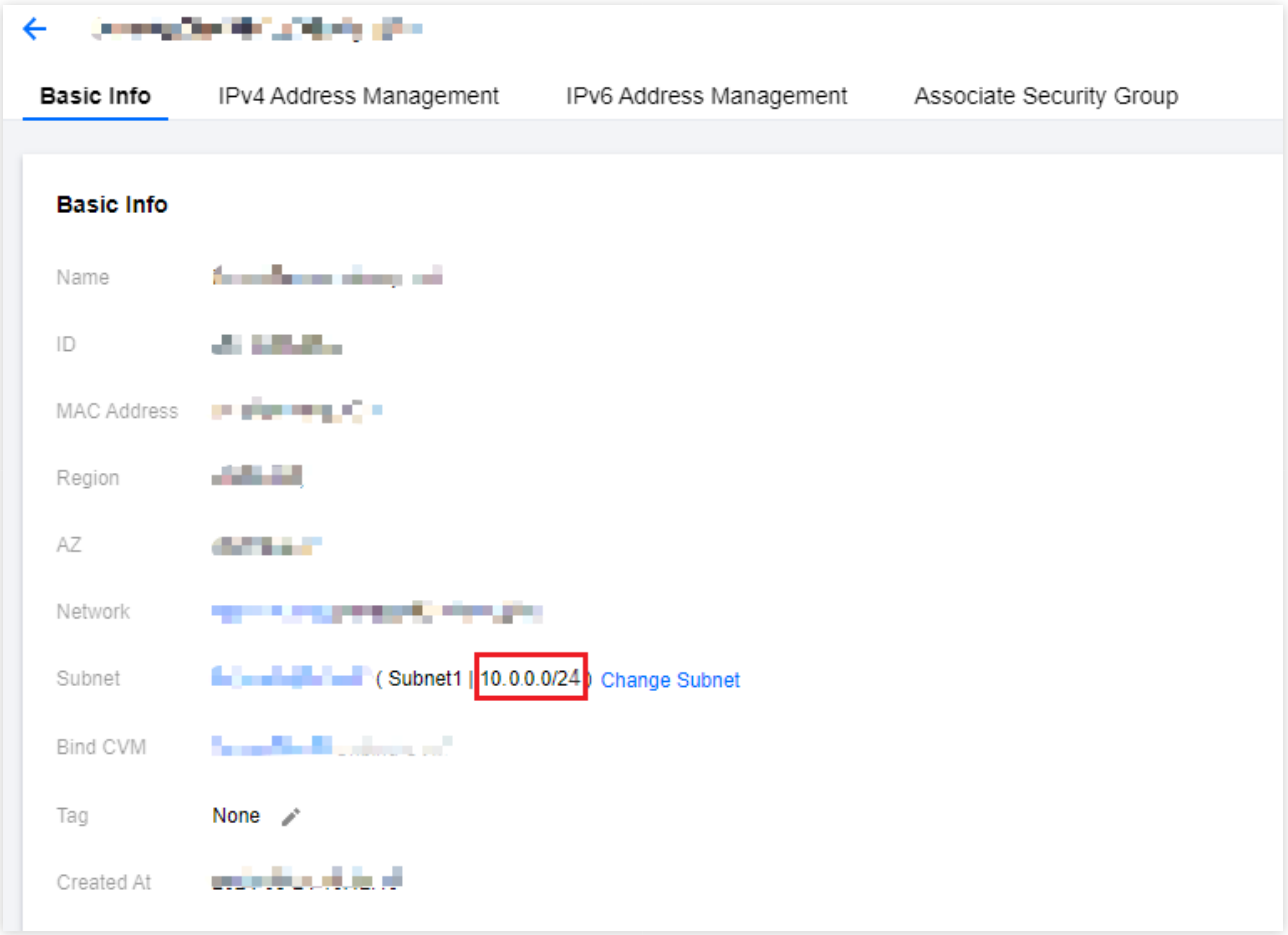
The following operations take CentOS 7 CVM as an example:

1. Log in to the CVM console and click CVM in the left sidebar.

2. In the instance list, click your CVM ID. On the details page, select ENI.

3. Click the secondary network interface ID to enter the auxiliary network interface details page, and record the following information based on the subnet to which it belongs:
   - Subnet Mask: As shown in the figure below, the CIDR bit number of the subnet is /24; that is, the subnet mask is 255.255.255.0 .
   - Gateway: If you have not changed other settings, the gateway is the first IP of the subnet range. For

example, the first IP of the subnet range in the figure below is 10.0.0.1 .



4. Log in to the CVM. For details, see Logging in to Linux Instance Using the Standard Log-in Method (Recommended).

5. Run the following command to copy the primary network interface file.

```
cp /etc/sysconfig/network-scripts/ifcfg-eth{0,1}
```

6. Run the following command to open the secondary network interface configuration file.

```
vim /etc/sysconfig/network-scripts/ifcfg-eth1
```

7. You can press i to switch to the Edit mode and modify the configuration file content to:

```
# Created by cloud-init on instance boot automatically, do not edit.
#
# Change this to static
BOOTPROTO=static
#
# Change this to eth1
```

DEVICE=eth1
Comment this line
HWADDR=52:54:00:8a:7a:64
Add the following lines.
#
Configure the primary IP.
IPADDR0=10.0.0.7 # Manually filled primary IP in Step 1: Add secondary network interface. Fill in according t o the actual situation.
NETMASK0=255.255.255.0 # The subnet mask recorded in step 3. Fill in according to the actual situation.
Configure secondary IP 1.
IPADDR1=10.0.0.8 # Step 1: Add the secondary IP manually filled in the secondary network interface accordi ng to the actual situation.
NETMASK1=255.255.255.0 # The subnet mask recorded in step 3. Fill in according to the actual situation.
#
Configure the gateway.
GATEWAY=10.0.0.1 # The gateway recorded in step 3. Fill in according to the actual situation.
#
NM_CONTROLLED=no
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PERSISTENT_DHCLIENT=yes

After it is modified, the example is as follows:

```
# Created by cloud-init on instance boot automatically, do not
BOOTPROTO=static
DEVICE=eth1
#HWADDR=52:54:00:8a:7a:64
IPADDR0=10.0.0.7
NETMASK0=255.255.255.0
IPADDR1=10.0.0.8
NETMASK1=255.255.255.0
GATEWAY=10.0.0.1
NM_CONTROLLED=no
ONBOOT=yes
TYPE=Ethernet
USERCTL=no
PERSISTENT_DHCLIENT=yes

~
```

8. After completing the modification, press Esc , enter :wq! Press Enter to save the configuration and return.
9. Run the following command to open /etc/sysctl.conf document.

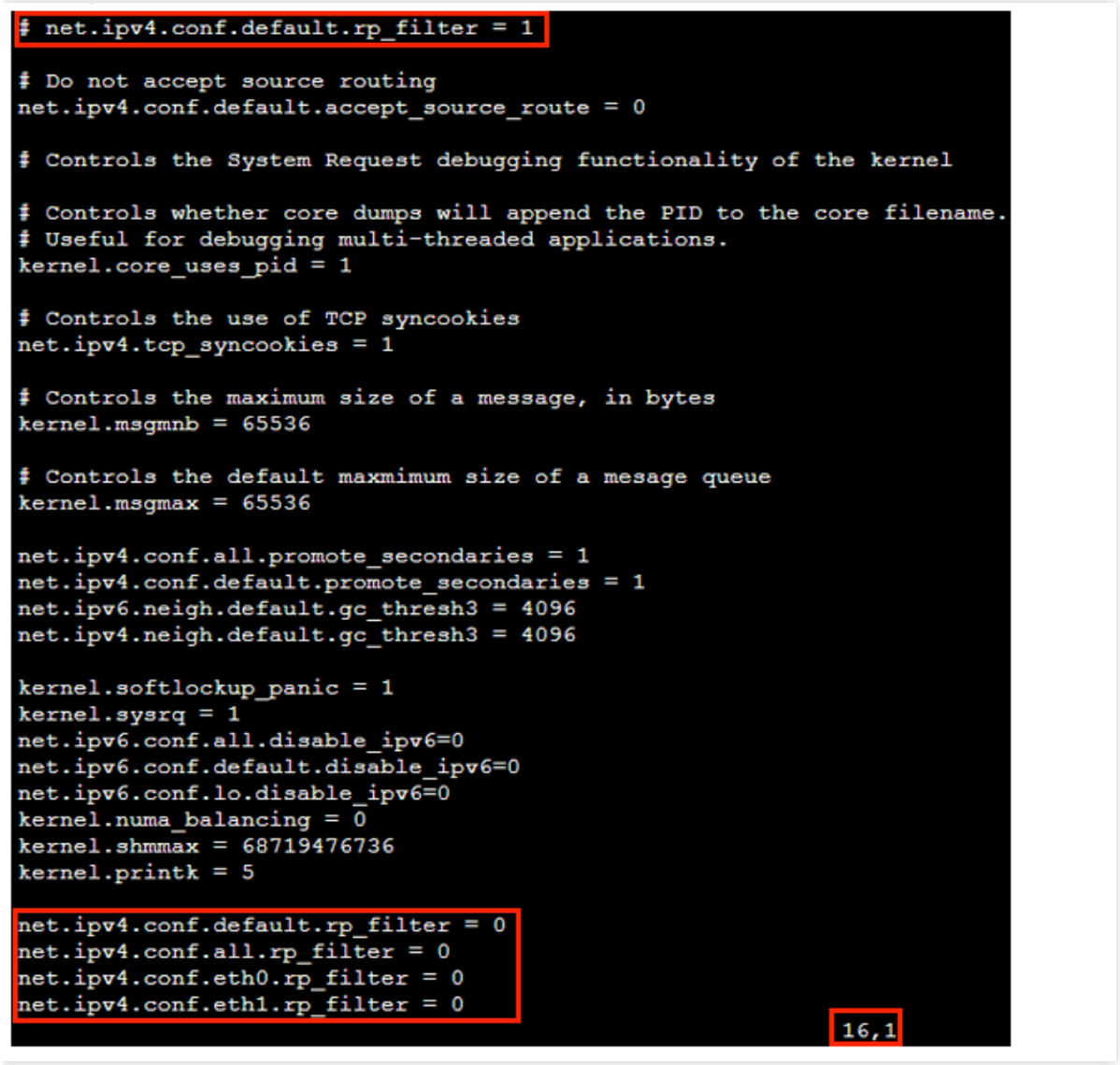
vim /etc/sysctl.conf

10. Press i to switch to edit mode, make the following changes, and close rp_filter for verification.

Find rp_filter on line 16 and comment on it.
net.ipv4.conf.default.rp_filter = 1 Comment if there is one.
Add the following 4 lines to the end of the file.

net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.conf.eth0.rp_filter = 0
net.ipv4.conf.eth1.rp_filter = 0

After it is modified, the example is as follows:



11. After completing the modification, press Esc , enter :wq! Press Enter to save the configuration and return.
12. Run the following command to make the configuration file take effect.

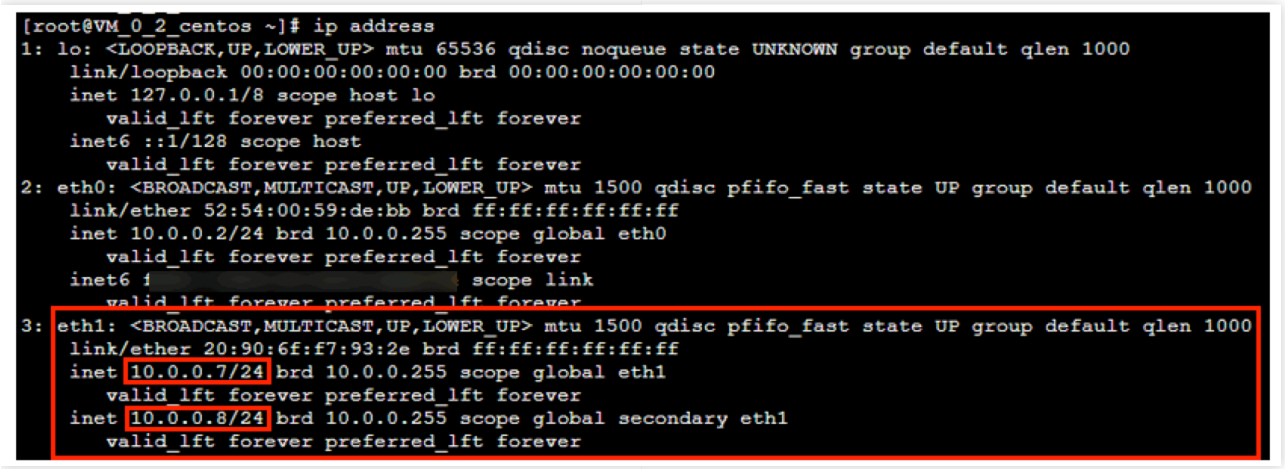
sysctl -p

13. Run the following command to restart the network service:

systemctl restart network.service

14. Run the following command to view the IP address:

ip address



Windows CVM

The following operations take Windows 2012 CVM as an example:

1. Log in to the CVM. For details, see Log in to Windows Instance Using RDP Files.

2. Follow the steps below to view the IP address, subnet mask, default gateway, and DNS server of the CVM's secondary network interface:

3. On the operating system interface, select in the lower left corner, click , open the Windows PowerShell window and run the following command:

   ipconfig /all

4. Record the IPv4 address, subnet mask, default gateway, and DNS server values from the Ethernet Adapter Ethernet 2 information output.

5. Go to the operating system's Control Panel > Network and Internet > Network and Sharing Center, and click the network interface named Ethernet 2 to edit it.

6. In the Ethernet 2 Status pop-up window, click Attributes.

7. In the Ethernet 2 Attribute pop-up window, double-click Internet Protocol Version 4 (TCP/IPv4).

8. In the Internet Protocol Version 4 (TCP/IPv4) Attributes pop-up window, fill in the following information:

Parameter Name	Parameter Value
IP Address	The IPv4 address in the above Step 2.
Subnet Mask	The subnet mask in the above Step 2.
Default Gateway	The default gateway address in the above Step 2.
Preferred DNS Server	The DNS servers in the Above Step 2.
Backup DNS Server	The backup DNS Servers in the Above Step 2. If no backup DNS servers are listed, this parameter is not required.

9. Click Advanced and configure the secondary private IP.
10. Under the pop-up window Advanced TCP/IP Settings, in the IP Address module, click Add.
11. In the TCP/IP Address pop-up window, fill in the secondary private IP address configured in Step 1: Add secondary network interface and the subnet mask in Step 2, and click Add. If there are multiple secondary IPs, repeat the previous step and the current step.
12. In the Internet Protocol Version 4 (TCP/IPv4) Attribute pop-up window, click OK.
13. In the Ethernet 2 Attribute pop-up window, click OK to complete the configuration.
14. In the Ethernet 2 Status pop-up window, click Details to view the configured IP information, as shown in the figure below.

Step 4: Result verification

Log in to another CVM and execute ping <secondary network interface public network address> command. If the following information is displayed, the binding is successful.

If the following results are not obtained after executing the command, check whether the ICMP protocol is enabled in the CVM security group configuration.

Managing EIP
Adjusting Bandwidth

EIP can adjust bandwidth timely according to your needs and take effect in real time.

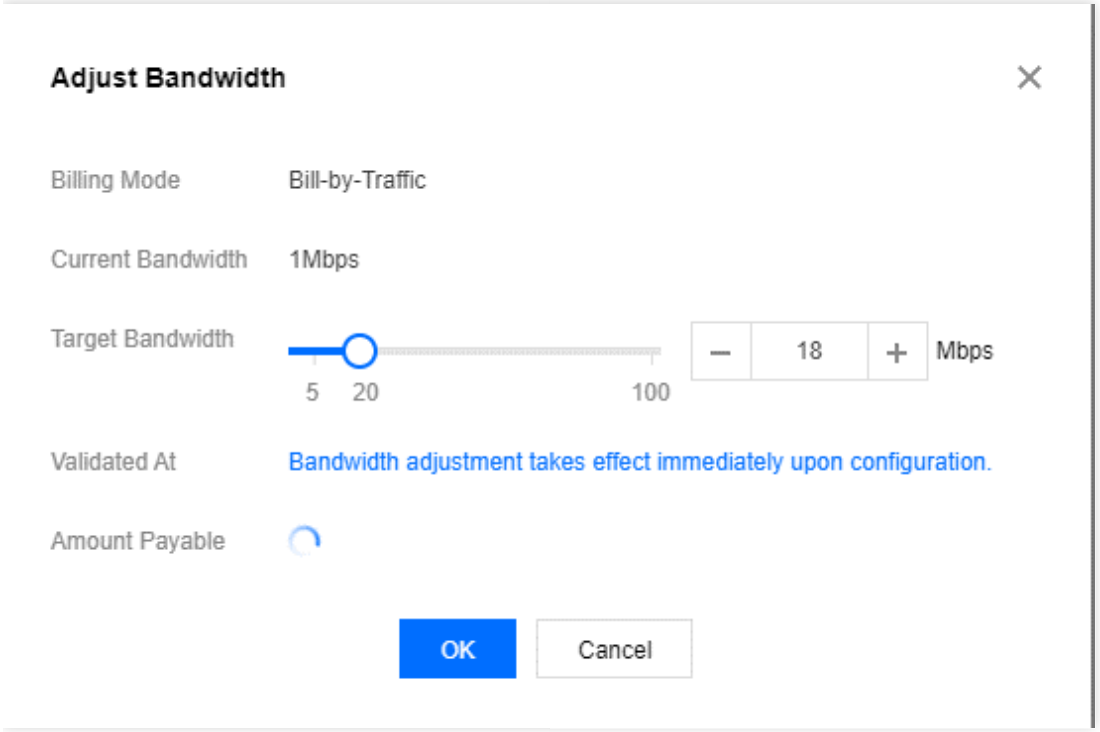
Overview

- When the service traffic is low, the bandwidth limit needs to be lowered to avoid increasing public network costs due to excessively high bandwidth limits.
- When the service traffic is large, the bandwidth limit needs to be increased to avoid access delays caused by bandwidth speed limits.

Directions

1. Log in to the CVM console and click EIP in the left sidebar to enter the EIP interface.
2. On the EIP management page, select the region of the EIP whose bandwidth you want to adjust, and click Adjust Bandwidth in the right operation column of the corresponding EIP.
3. In the pop-up Adjust Bandwidth dialog box, set the target bandwidth value and click OK to complete the bandwidth adjustment.

   > Note:
   >
   > If the cloud resource bound to the EIP is a NAT gateway, the bandwidth of the EIP cannot be less than the bandwidth of the NAT gateway. Otherwise, packet loss will occur. It is recommended that you log in to the NAT Gateway Console to view the bandwidth limit before adjusting the bandwidth.

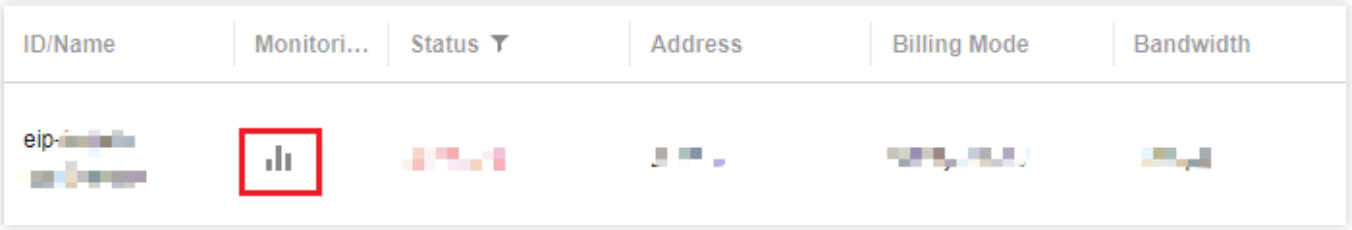

Adjust Bandwidth
Billing Mode
Bill-by-Traffic
Current Bandwidth
1Mbps
Target Bandwidth
5
20
100
18
Mbps
Validated At
Bandwidth adjustment takes effect immediately upon configuration.
Amount Payable
OK
Cancel

Viewing Monitoring Data

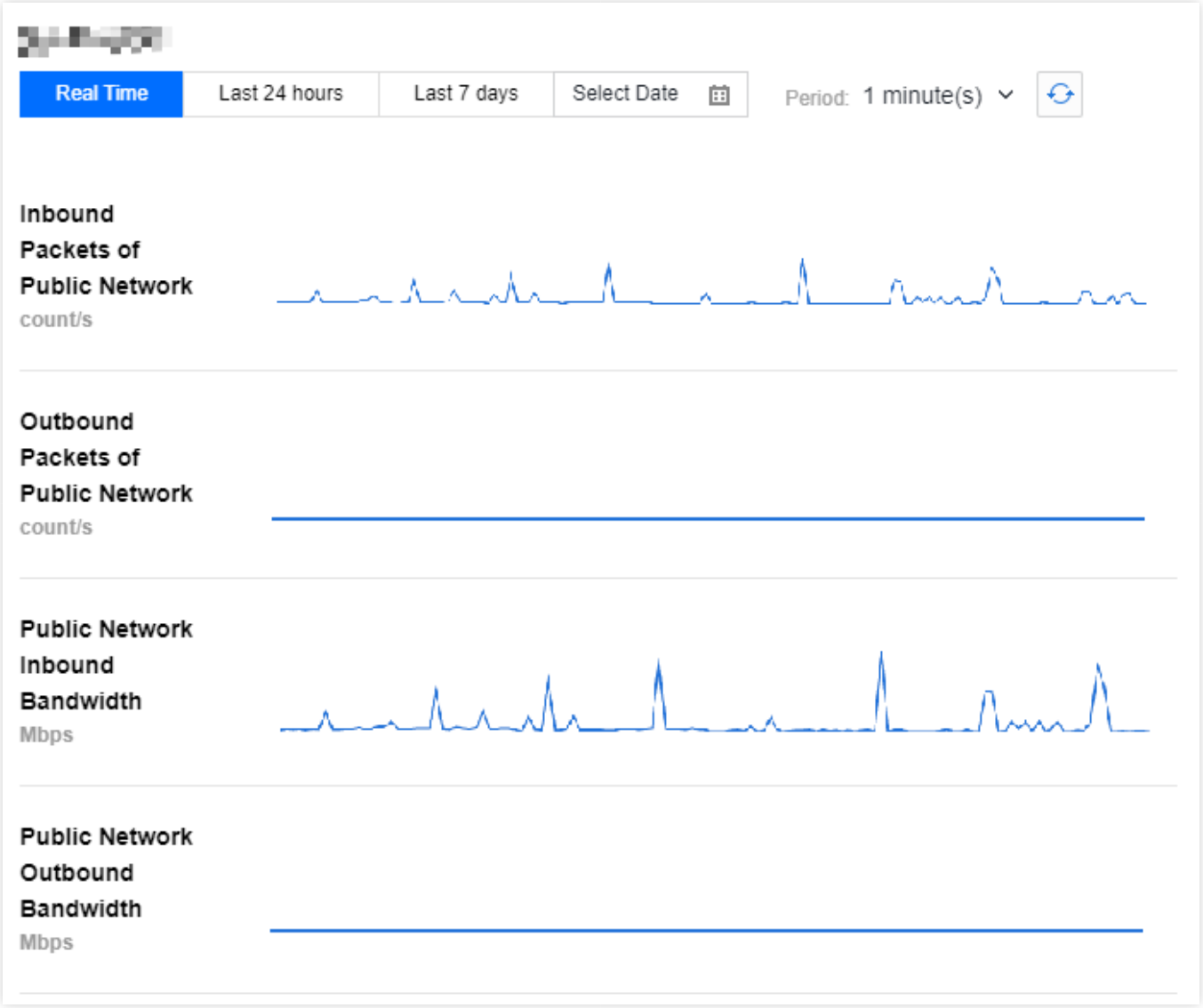
The monitoring feature of EIP can help you monitor traffic fluctuations in real time through relevant monitoring metrics, detect exceptional fluctuations in time, adjust the EIP bandwidth peak, and avoid access delays caused by bandwidth speed limits.

Directions

1. Log in to the CVM console and click EIP in the left sidebar to enter the EIP interface.
2. Click the Monitor icon to the right of the EIP instance.



3. On the right side of the page, you can view the monitoring data.


Real Time
Last 24 hours
Last 7 days
Select Date
Period: 1 minute(s)
Inbound Packets of Public Network
count/s
Outbound Packets of Public Network
count/s
Public Network Inbound Bandwidth
Mbps
Public Network Outbound Bandwidth
Mbps

Unbinding/Releasing EIP
Unbind EIP

You can unbind an EIP from a cloud resource anytime and then rebind it to other cloud resources. If you no longer need to use the EIP, release it in time to avoid wasting IP resources.

Overview

- If the CVM instance bound to the EIP fails and needs to be quickly restored, you can unbind it and then rebind it to a healthy CVM instance.
- If you no longer need EIP to provide public network communication services for cloud resources, you can unbind the cloud resources from EIP.

Directions

1. Log in to the CVM console, select EIP, and enter the EIP interface.

2. In the operation column to the right of the target EIP, click Unbind.

   > Note:
   >
   > A NAT gateway must be bound to at least one EIP. Therefore, if the cloud resource that is to be unbound from an EIP is a NAT gateway and the EIP is the only EIP bound to the NAT gateway, unbinding cannot be performed.

3. In the pop-up Unbind EIP window, confirm the unbinding information and click Confirm to complete the unbinding from the cloud resources.

Next Steps

- If you need to rebound an EIP that has been unbound from a cloud resource to another cloud resource, see Binding EIP to Cloud Resources.
- If you need to release an EIP that is in an idle (unbound) state, see Releasing EIP.

Release EIP

If you no longer use an EIP, you can release it in the console.

Directions

1. Log in to the CVM console, select EIP, and enter the EIP interface.
2. In the operation column to the right of the target EIP, select More > Release.
3. In the EIP window that pops up to confirm to release, check Confirm to Release the Above IP and click Release.

Best Practice
Migrating Public IP

This document describes how to migrate a public IP address from one CVM to another CVM.

Overview

If CVM A fails and cannot provide services normally, the public IP on CVM A needs to be migrated to the healthy CVM B to ensure normal service. Public IP for migration includes ordinary public IP and EIP.

Directions

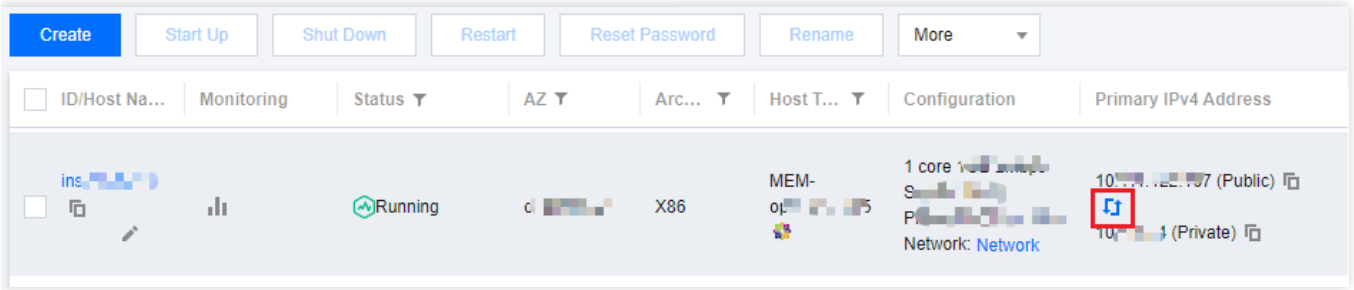
Step 1: Convert the ordinary public IP on CVM A to EIP

> Note:
>
> - If the public IP on CVM A is already an EIP, skip this step and proceed to Step 2: Unbind EIP from CVM A.
> - EIP has flexible binding and unbinding capabilities that ordinary public IPs do not have. If the public IP on CVM A is an ordinary public IP, it needs to be converted to EIP, and the public IP can be migrated using the capabilities of EIP.

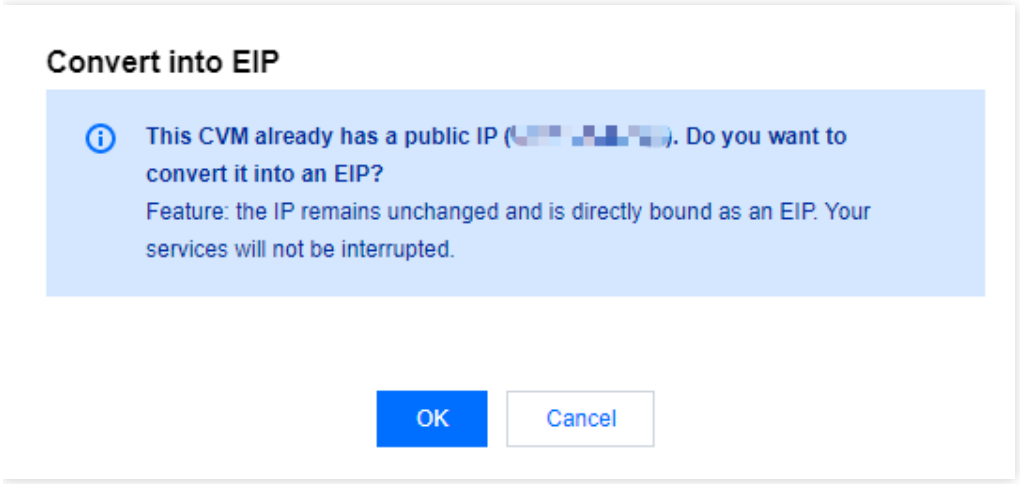
1. Log in to the CVM console and click CVM in the left sidebar.

2. On the CVM management page, select the region of CVM A and click .

> Note:
>
> When an ordinary public IP is converted to an EIP, the IP address remains unchanged, and your service is not interrupted. The EIP quota for each account in a single region is 20.



3. In the pop-up Convert to EIP window, click OK.



Step 2: Unbind EIP from CVM A

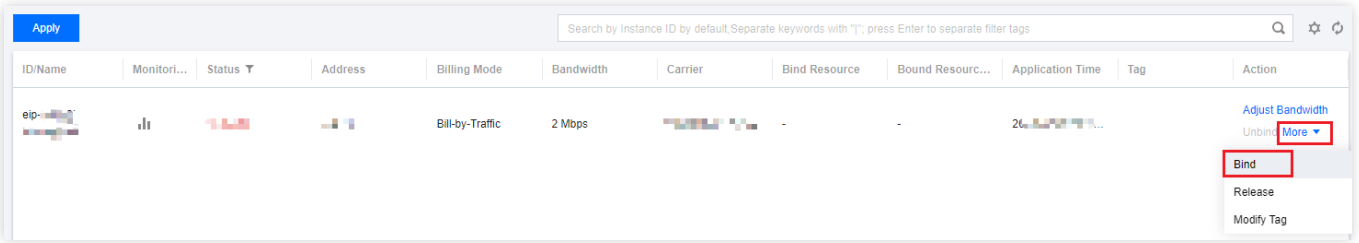
Unbind CVM A from the EIP. After it is unbound, CVM A cannot access the public network because it has no public IP.

1. Log in to the CVM console and click CVM in the left sidebar.
2. On the CVM management page, select the region of CVM A and click Operation > EIP > Unbind EIP in the operation column of the row.
3. In the pop-up Unbind EIP dialog box, click OK to complete the EIP unbinding.

Step 3: Bind EIP to CVM B

Bind the EIP unbound from CVM A to CVM B to complete the migration of the public IP.

1. Log in to the CVM console and click EIP in the left sidebar to enter the EIP interface.
2. Select the region where CVM A is located, find the row where the EIP to which CVM A is unbound is located in the list, and click More > Bind in the operation column.



3. In the Bind Resources window that pops up, select CVM Instance as the resource type, select the target CVM B to which the EIP needs to be migrated, and click OK.
4. In the pop-up dialog box, click OK.

Step 4: Verify the migration results

After the migration is completed, you can check on the CVM list page or EIP list page that the public IP has been bound to the target CVM B.

- Cloud Server List Page

  i. Log in to the CVM console and click CVM in the left sidebar.
  ii. On the CVM management page, select the region of CVM B and find the row of CVM B in the list to view that the public IP has been successfully migrated.

- EIP List Page

  i. Log in to the CVM console and click EIP in the left sidebar to enter the EIP interface.
  ii. Select the region where CVM B is located and find the row where the migrated EIP is located in the list. You can then check that the EIP has been successfully bound to CVM B.