Elastic Network Interface

Product Documentation

Contents

Elastic Network Interface 3
- Product Introduction 3
  - Product Overview 3
  - Related Concepts 4
  - Limits 5
  - Related products 6
- Operation Guide 7
  - Create an Elastic Network Interface （ ENI) 7
  - Binding and Configuring CVMs 9
  - Unbind from the CVM 17
  - View Elastic Network Interface （ ENI) 18
  - Delete an Elastic Network Interface （ ENI) 19
  - Request for Secondary Private IP 20
  - Releasing Secondary Private IP Addresses 21
  - Bind an Elastic IP (EIP) 22
  - Unbind an Elastic IP (EIP) 23
  - Modify the primary private IP 24
  - Modify the subnet 25
  - Request for and Releasing IPv6 27
- FAQs 28
  - Concept category 28
  - Function category 29

Product Introduction
Product Overview

Introduction

An Elastic Network Interface (ENI) is bound to a CVM in a virtual private cloud (VPC) and can be freely migrated between multiple CVMs. ENIs are very helpful in configuring and managing networks and building highly reliable network solutions. You can bind multiple ENIs in the same availability zone to a CVM to implement a high-availability network solution. You can also bind multiple private IP addresses to an ENI to implement multi-IP deployment on a single host.

Product Features

Multiple Network Interfaces

In addition to the primary ENI that is automatically generated when a CVM is created, it supports binding with multiple secondary ENIs. ENIs can belong to different subnets in the same VPC and availability zone. Each network interface supports configuring an independent security group, and the subnet where the network interface is located can be configured with an independent routing and forwarding policy.

Flexible Migration

ENIs can be freely migrated between CVMs in the same VPC and availability zone. When an ENI is unbound from a CVM, the bound private IP, Elastic IP (EIP), and security group policy are retained. There is no need to reconfigure the association after migration.

Multiple IPs

Depending on the CVM configuration, the elastic network interface can support binding up to 30 private IP addresses, and each private IP can be bound to an independent EIP. A single CVM can open multiple identical ports through multiple elastic Ips. The binding relationship between the ENI and the private and public IP addresses does not change when the ENI is unbound from the CVM.

Independent Routing Forwarding

The CVM can be bound to ENIs located in different subnets in the same VPC and availability zone. Each subnet can independently set routing and forwarding policies to achieve network isolation. You can also set routing policies in the CVM to direct network traffic of a specific destination to different network interfaces.

Related Concepts

Before you use Elastic Network Interface (ENI), you need to understand the following concepts.

Primary or secondary network interfaces

- A network interface created when the CVM of VPC is created is a primary network interface. A network interface created by the user is a secondary network interface.
- The primary network interface cannot be bound or unbound, while the secondary network interface can.

Primary Private IP

- The primary private IP of the ENI can be randomly allocated by the system or set by the user when the ENI is created.
- The primary private IP of the primary network interface can be modified, but the primary private IP of the secondary network interface cannot.

Secondary Private IP

- The secondary private IP bound to the primary IP of the ENI is configured by the user when he creates or edits the ENI.
- A secondary private IP can be bound and unbound.

Elastic IP

Bind each of the private IP addresses on the ENI.

Security Group

An ENI can be bound to one or more security groups.

MAC address

The ENI has a globally unique MAC address.

Limits

Depending on the CPU and memory configuration, the number of Elastic Network Interface (ENI) that can be bound to a CVM and the number of private IPs that can be bound to a single network interface can vary greatly. The following table lists the private IP quotas for ENIs and single network interfaces.

> Note:
>
> - The number of private IPs bound to a single network interface only represents the upper limit of the quantity of private IPs that can be bound to the network interface, not the number of EIPs actually provided. The EIP quota of each account is provided according to the EIP usage limit.
> - Although the number of ENIs represents the quantity of network interfaces that can be bound to the corresponding configuration server, a CVM under the same VPC can be bound to a maximum of 1,000 ENIs.

Virtual Central Processing Core (vCPU)	Number of ENIs	IPv4 quota	IPv6 quota
1	2	6	6
[2,4]	4	10	10
[6,8]	6	20	20
12	8	30	30
[14,64)	8	40	40
≥64	16	40	40

> Note:
>
> - For details on CVM models, see Instance Specifications.
> - BMS supports 32 ENIs, each of which supports 20 secondary private IP addresses.

Related products

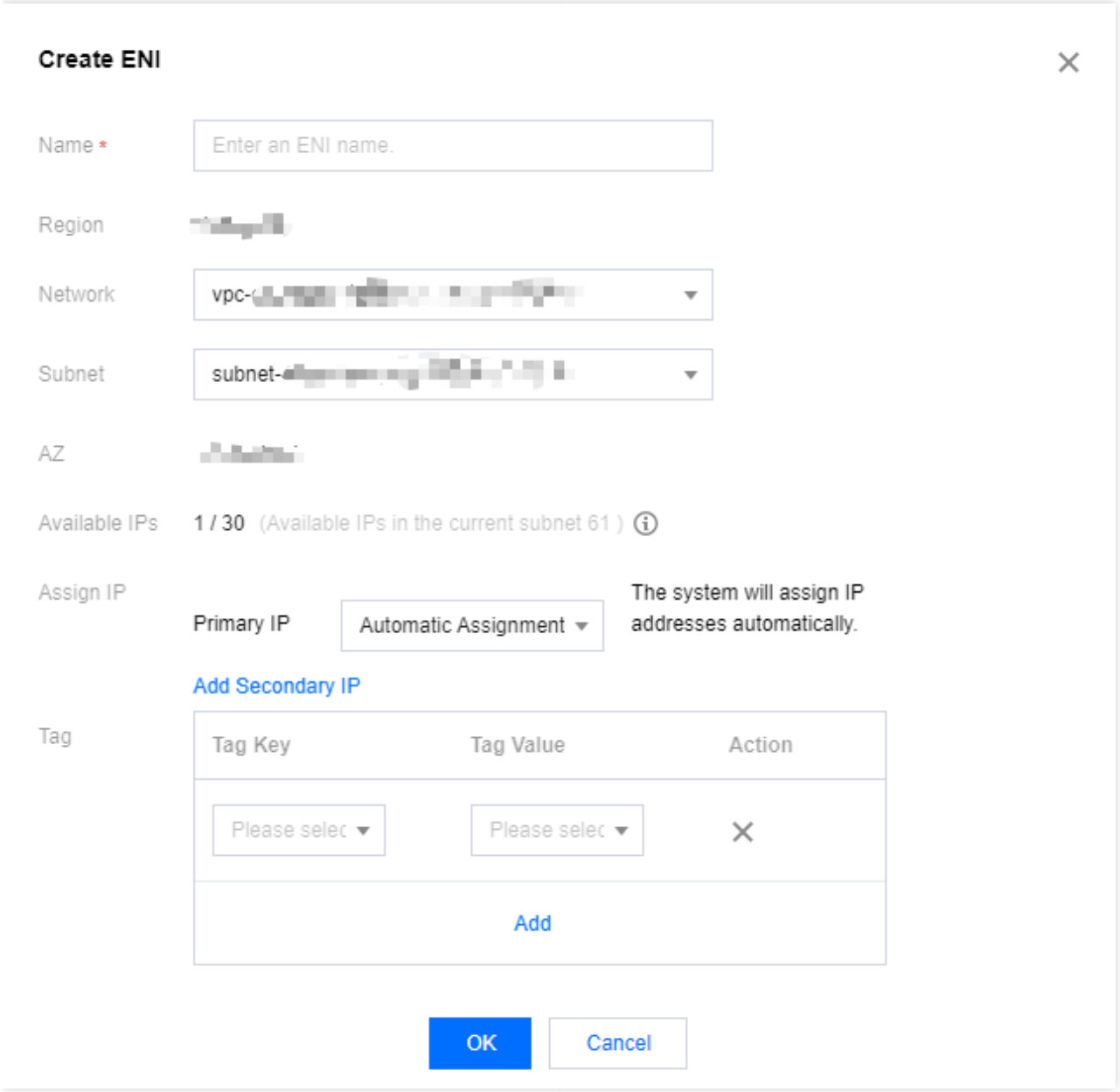
For information about Elastic Network Interface (ENI) products, see the following table:

Product Name	Relationship with ENI
CVM	You can bind the CVM with an ENI to connect to the network.
Virtual Private Cloud (VPC)	ENI has VPC attributes.
Elastic IP	Bind each of them to the private IP on the ENI.
Security Group	An ENI can be bound to one or more security groups.

Operation Guide
Create an Elastic Network Interface （ ENI)

1. Log in to the VPC console.
2. Click IP and Network Card > ENI to open the ENI list page.
3. Select the region and VPC and click Create.
4. In the pop-up, enter a name, select the VPC and subnet to which the secondary ENI belongs, allocate an IP to the NI, and add tags if necessary.

   > Note:
   >
   > - The security group of the secondary ENI needs to be configured separately. After the secondary ENI is created, determine the security policy of the ENI based on the business situation and bind it to a security group. For details, see Bind Security Group.
   > - IP allocation supports automatic allocation and manual filling:
   >   - Automatic Allocation: The system will automatically allocate an available private IP within the subnet CIDR range to the network interface.
   >   - Manual Entry: You need to fill in an available private IP within the subnet CIDR range.
   >   - The secondary ENI is configured with a primary IP by default. If you need multiple IPs, click Add a secondary IP to configure multiple secondary IPs.



5. In the pop-up, select the VPC and subnet where the ENI is located, select the allocated private IP (which can be automatically generated or manually filled in), and set the tag information.
6. After the parameter settings are completed, click OK.

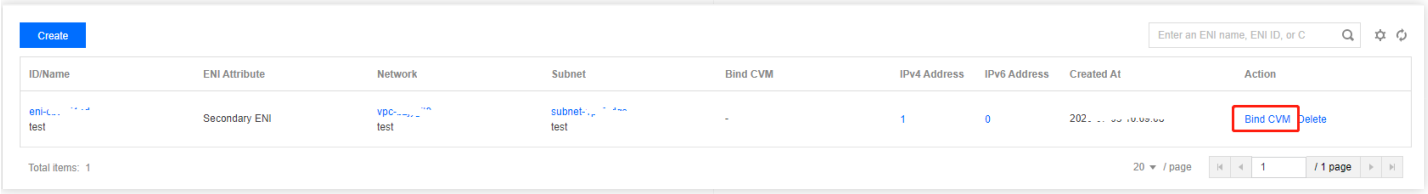
Binding and Configuring CVMs

I. Binding CVMs

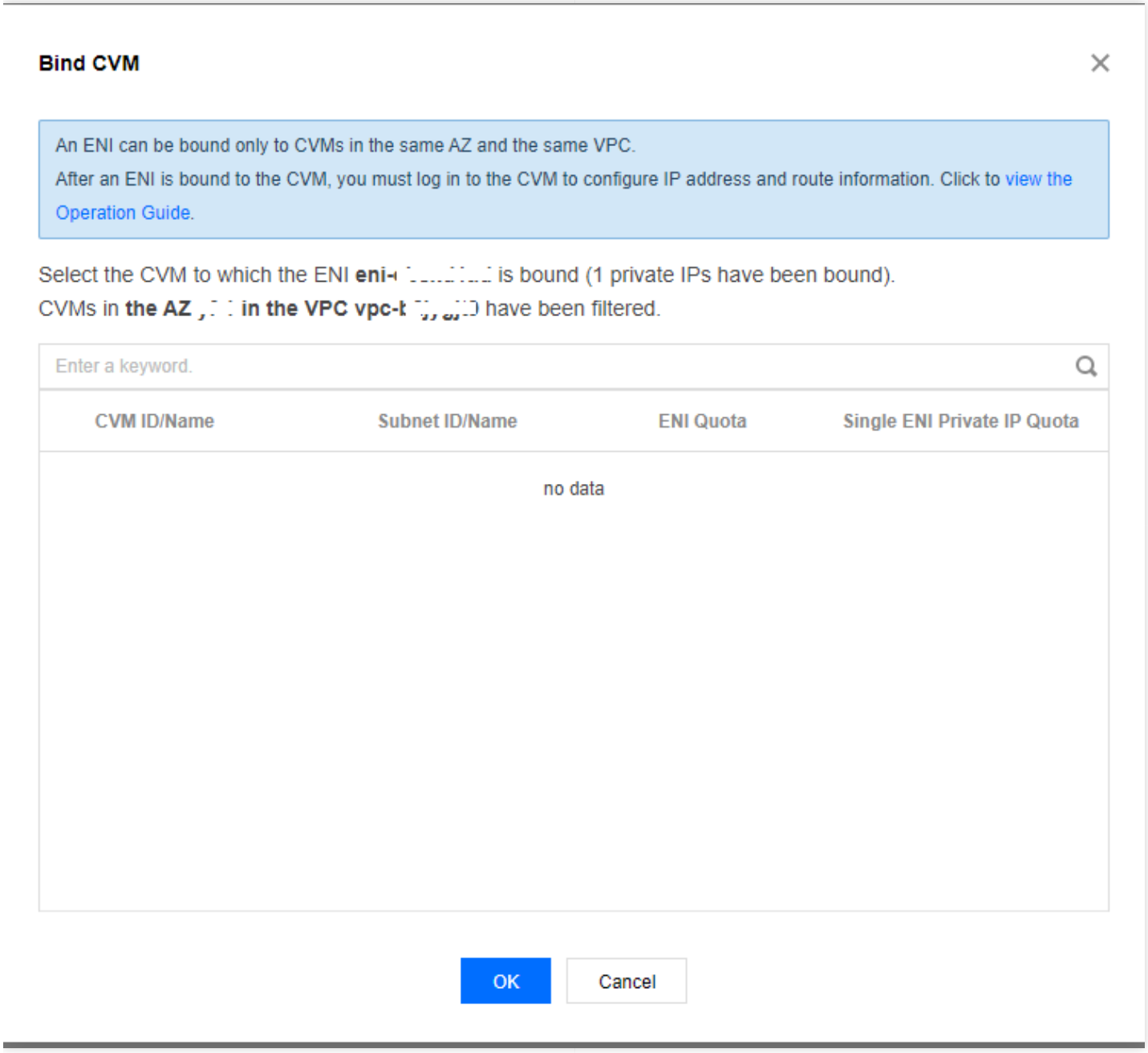
1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.

2. You can find the row of the Elastic Network Interface (ENI) that needs to be bound and configured and click Bind CVM in the operation column.

> Note:
>
> It only supports binding to CVMs in the same availability zone as the ENI.



3. In the pop-up box, you can select the CVMs you want to bind and click OK to bind.



II. Configuring CVMs

Configuration Steps Under Linux

> Note:
>
> The following steps take CentOS 7 and above as an example.

1. You can log in to the CVMs as an administrator and execute the following command:

   ```
   cd /etc/sysconfig/network-scripts/
   ```

2. You can create a NI configuration file ifcfg-eth1.

3. You can enter the following command:

   cp ifcfg-eth0 ifcfg-eth1

4. You can enter the command to modify the configuration file content.

   vim ifcfg-eth1

5. You can press i to switch to the edito mode and modify the configuration file content to:

   DEVICE='eth1'
   NM_CONTROLLED='yes'
   ONBOOT='yes'
   IPADDR='192.168.1.62' # Fill in the IP on the ENI according to the actual situation.
   NETMASK='255.255.255.192' # Fill in the subnet mask according to the actual situation.
   #GATEWAY='192.168.1.1' # Fill in according to the actual situation. Because the gateway is defin ed in the eth0 file, the gateway is not written here to avoid gateway conflicts.

   > Note:
   >
   > To view the IP and subnet mask of an ENI, please refer to the appendix below.

6. After modification, You can save the configuration file and exit (press Esc in vim's last line mode, enter wq! and press Enter).

7. You can enter the following command to restart the network service:

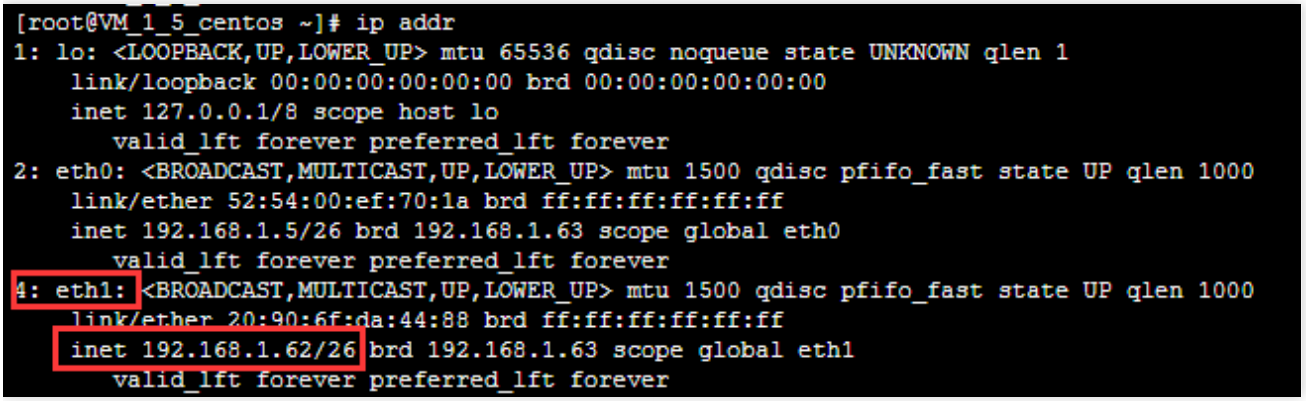
   systemctl restart network

8. You can check and confirm whether the IP is correctly configured.

9. You can enter the following command to view the IP:

   ip addr

10. You can confirm that the secondary NI and the IP on it are visible, as shown in the following figure.



11. You can configure routes based on actual service conditions.
After configuration according to the above steps, the Linux image still sends packets from the primary NI by default. You can determine which NI a message enters and returns from as per the policy routing.

12. You can create two route tables.

```
echo "10 t1" >> /etc/iproute2/rt_tables
echo "20 t2" >> /etc/iproute2/rt_tables
```

13. You can add a default route to both route tables.

```
ip route add default dev eth0 via 192.168.1.1 table 10
ip route add default dev eth1 via 192.168.1.1 table 20
```

> Note:
>
> In the above two commands,
>
> 192.168.1.1
>
> You need to replace them with the gateway of the subnet to which the primary NI belongs and that of the subnet to which the secondary NI belongs.

14. You can configure the policy route.

```
ip rule add from 192.168.1.5 table 10
ip rule add from 192.168.1.62 table 20
```

> Note:
>
> - In the above two commands, IP should be replaced with the IP on the primary network card, and the IP on the auxiliary network card, respectively.

- After restarting the network, you need to reconfigure the routes.

15. The configuration is now completed. You can use the CVMs in the same subnet to ping the private IP. If it works, it means that the private network address is successfully pinged. If there is no other CVMs, you can bind the public IP to the private IP of the secondary NI and ping the public IP to verify whether the private IP is bound.

Configuration Steps Under Windows

Situation I:
If DHCP is set in the Windows operating system, the secondary NI and the IP on it can be automatically recognized without configuration.

Situation II:
If DHCP is not set in the Windows operating system, the private IP shall be configured in the operating system. The directions are as follows:

1. You can log in to the cloud console and bind the ENI to the CVMs.

2. In the operating system, You can manually fill in the IP information (according to the actual situation).

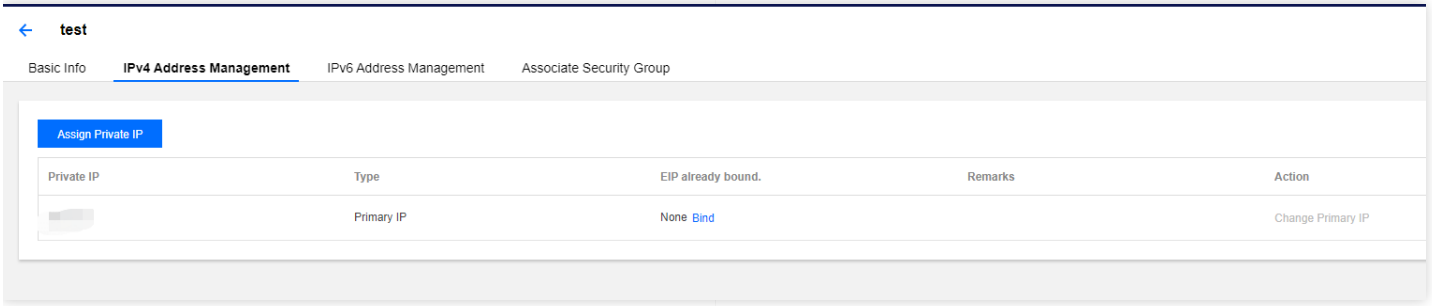
3. You can check the manually entered IP.

4. You can use the CVMs in the same subnet to ping the private IP. If it works, it means that the private network address is successfully pinged. If there is no other CVMs, you can bind the public IP to the private IP of the secondary NI and ping the public IP to verify whether the private IP is bound.

III. Appendix

Viewing the IP on the ENI

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
2. You can click the ENI ID to go to the details page.
3. You can select the IPv4 Address Management tab to view the IP on the ENI, that is, the private IP.

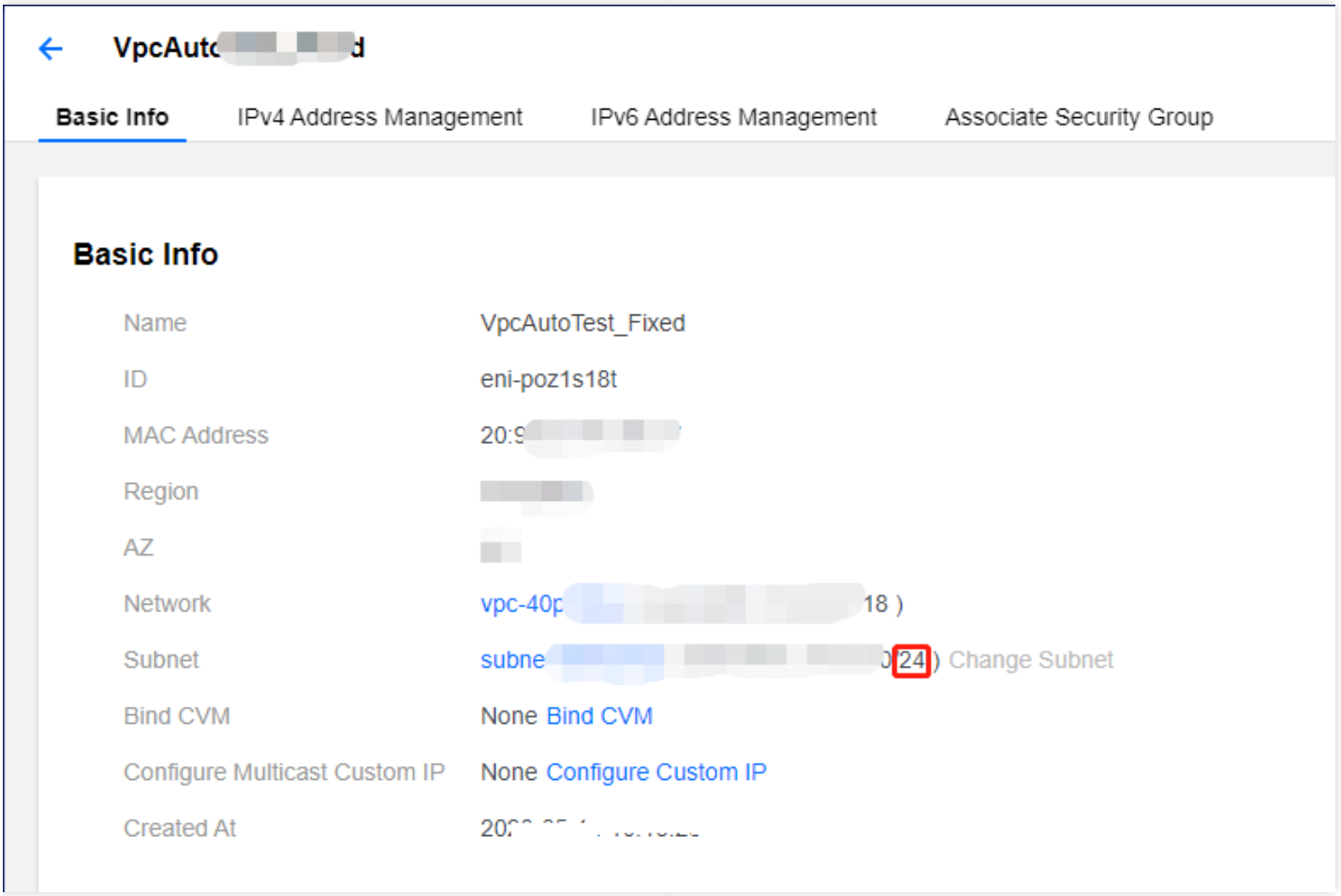


Viewing the Subnet Mask on the ENI

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
2. You can click the ENI ID to go to the details page and view the subnet mask on the ENI.

As shown in the figure below, the number of CIDR bits of the subnet is /24, that is, the subnet mask of the ENI is:

255.255.255.0



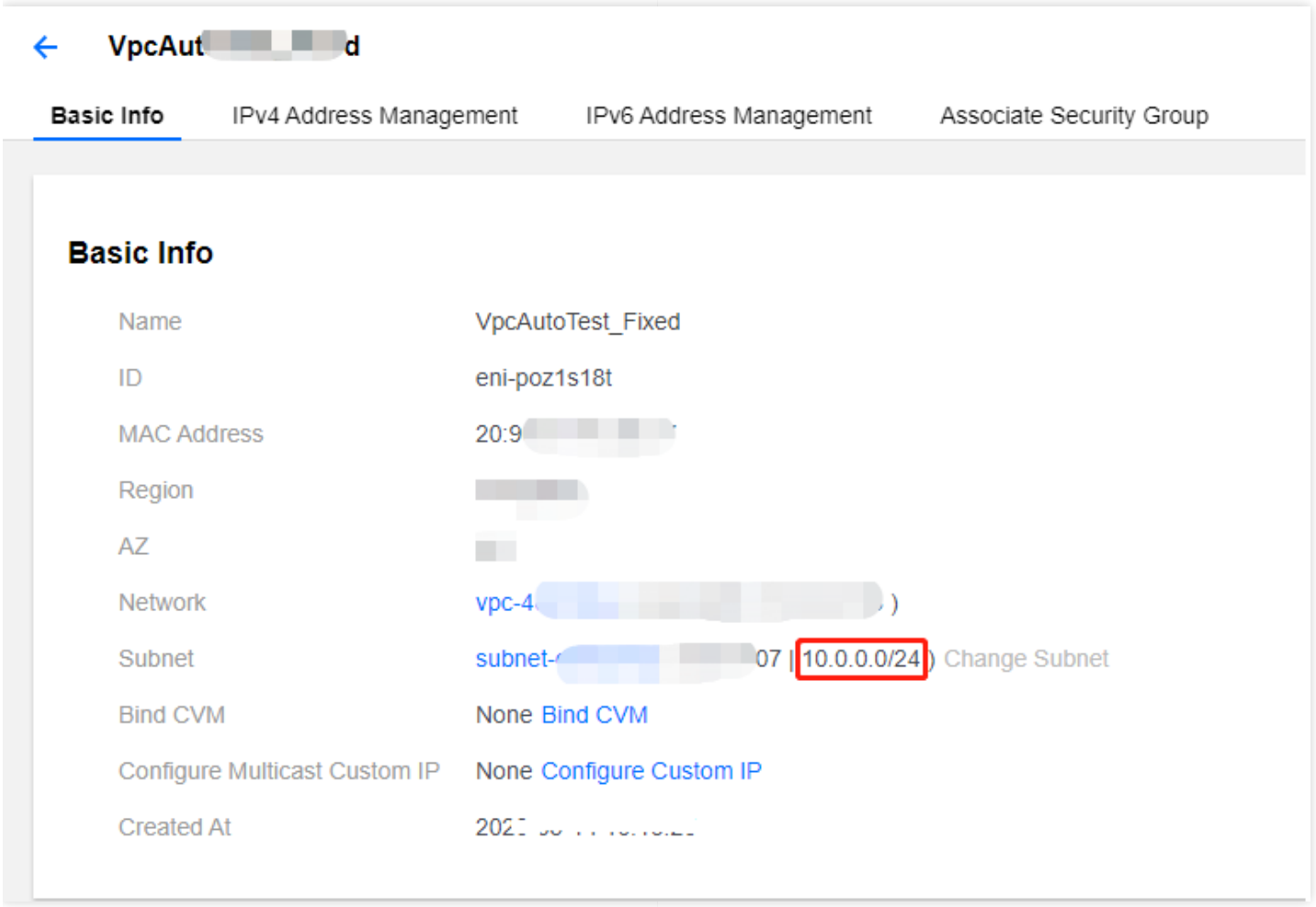
The correspondence between the number of CIDR bits and the subnet mask is shown in the following table.

Number of CIDR Bits	Subnet Mask
/28	255.255.255.240
/27	255.255.255.224
/26	255.255.255.192
/25	255.255.255.128
/24	255.255.255.0
/23	255.255.254.0
/22	255.255.252.0
/21	255.255.248.0
/20	255.255.240.0
/19	255.255.224.0
/18	255.255.192.0
/17	255.255.128.0
/16	255.255.0.0

Viewing Gateway

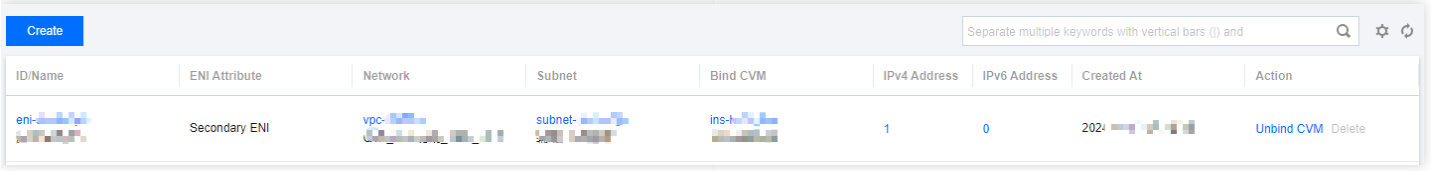
If you have not changed other settings, the gateway is the first IP of the subnet IP range. For example, the subnet IP range is 192.168.1.0/24 , and then the gateway is 192.168.1.1 . If you are not sure which subnet IP range the ENI belongs to, you can:

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
2. You can click the ENI ID to enter the details page and view the subnet IP range to which the ENI belongs, such as the first IP of the subnet IP range in the following figure.


VpcAut d
Basic Info
IPv4 Address Management
IPv6 Address Management
Associate Security Group
Basic Info
Name
VpcAutoTest_Fixed
ID
eni-poz1s18t
MAC Address
20:9
Region
AZ
Network
vpc-4)
Subnet
subnet- 07 | 10.0.0.0/24) Change Subnet
Bind CVM
None Bind CVM
Configure Multicast Custom IP
None Configure Custom IP
Created At

Unbind from the CVM

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
2. Find the row of the ENI that needs to be unbound and click Unbind CVM in the operation column.



3. Click OK in the pop-up window.

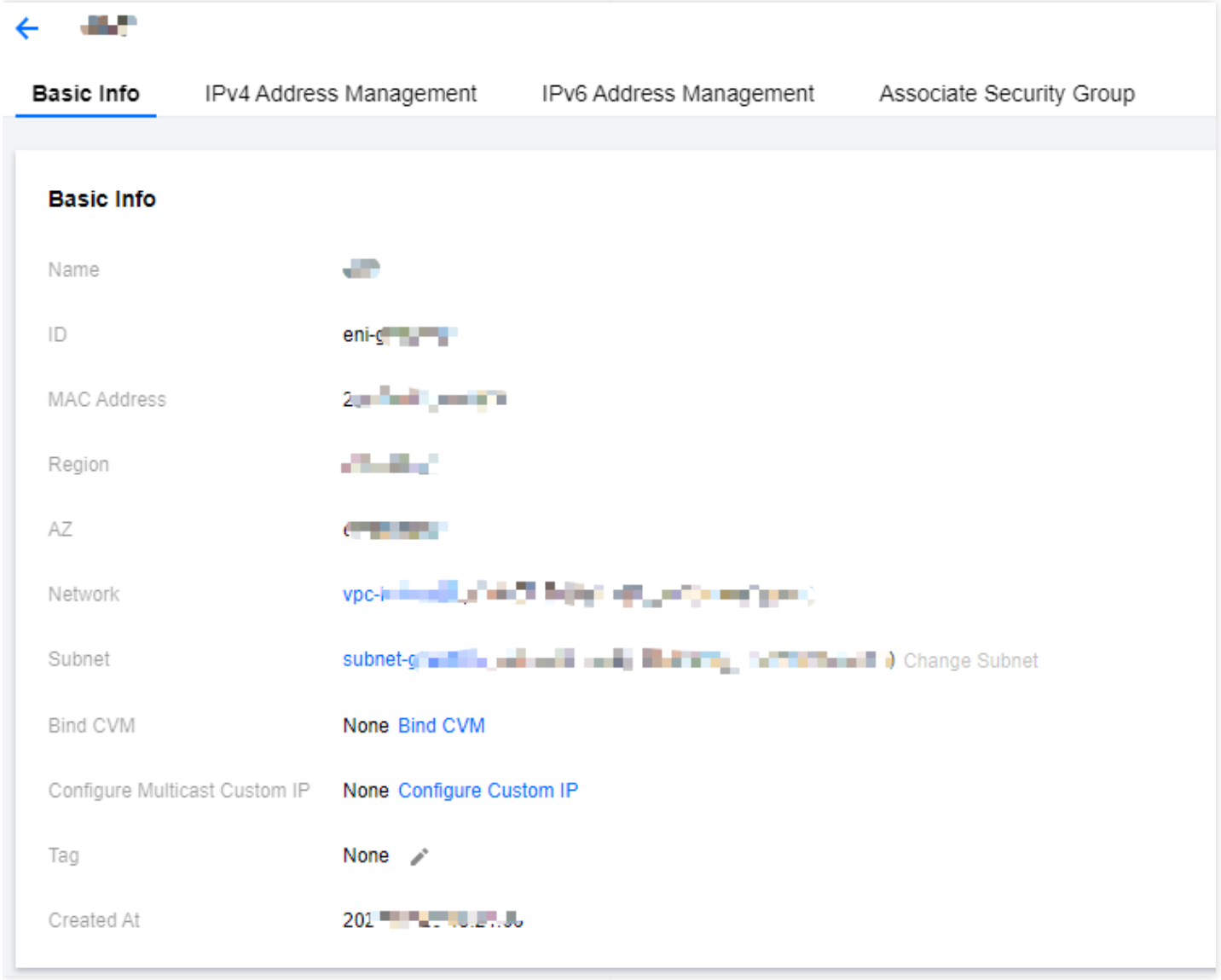
> Note:
> After the ENI is unbound, its associated private IP addresses, elastic IPs, security group and other information will be retained.

View Elastic Network Interface （ ENI)

1. Log in to the VPC console.

2. Click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.

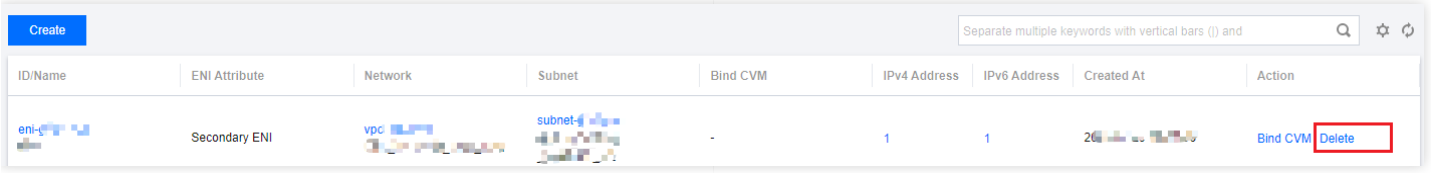
3. Click the instance ID you want to view to open the details page.



Delete an Elastic Network Interface （ ENI)

> Note:
>
> - After an ENI is deleted, the associated private IP, Elastic IP (EIP), and security group will be automatically unbound.
> - Only ENIs that are not associated with a CVM can be deleted.
> - The primary network interface will be deleted after the CVM is deleted.

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
2. Find the row of the ENI that you want to delete and click Delete in the Action column.



3. Click OK in the pop-up window.

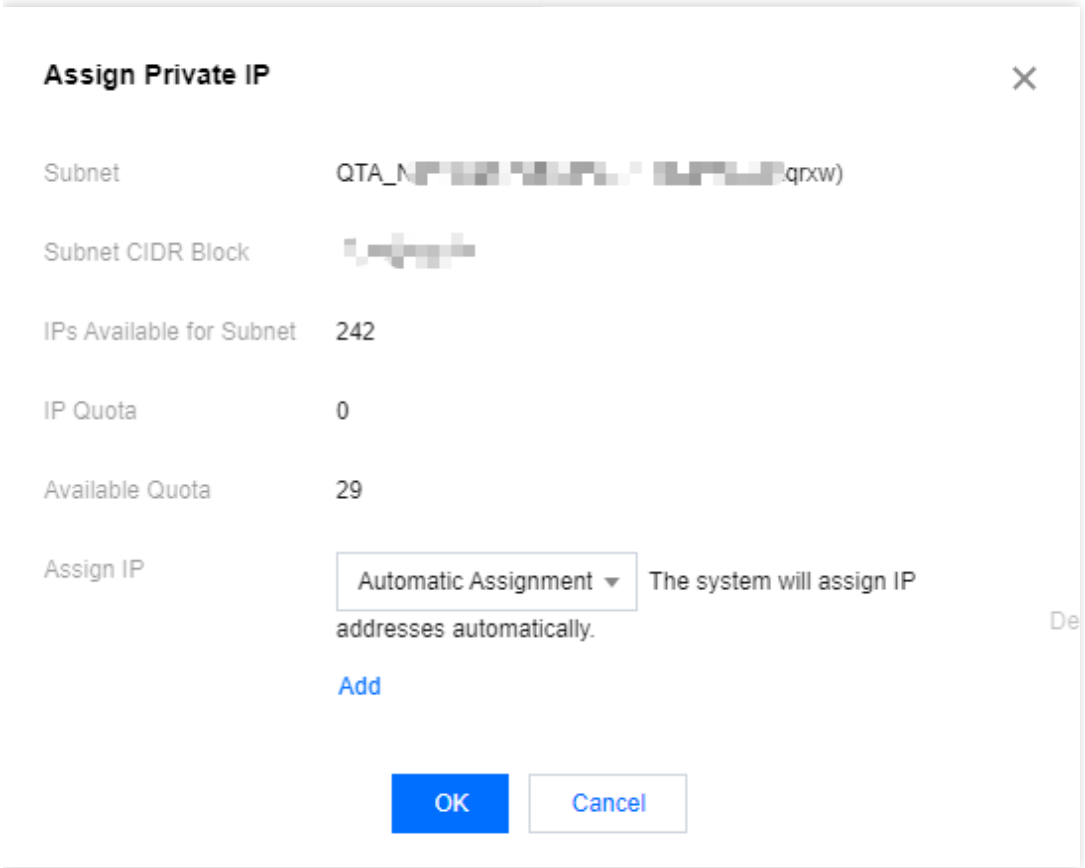
Request for Secondary Private IP

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.

2. Click the instance ID for which you want to request for a secondary private IP to open the details page.

3. Click the IPv4 Address Management tab, click Assign Private IP on the interface, select Automatically assign in the pop-up box, or manually fill in the private IP to be allocated.

> 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, the subnet IP range is: 10.0.0.0/24 , then the available private IP range is: 10.0.0.2 - 10.0.0.254 .

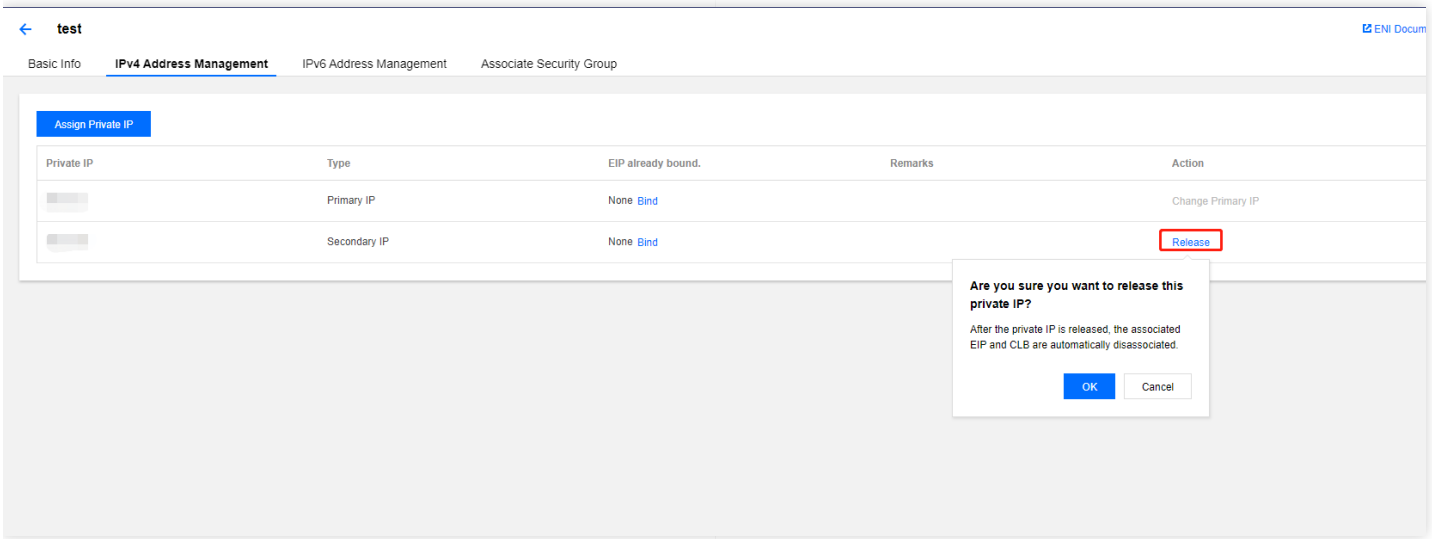


Releasing Secondary Private IP Addresses

> Note:
>
> - The Elastic Network Interface (ENI) only supports the release of secondary IP addresses, but not primary IP addresses.
> - After a private IP is unbound, its associated Elastic IP (EIP) will be automatically unbound.

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.

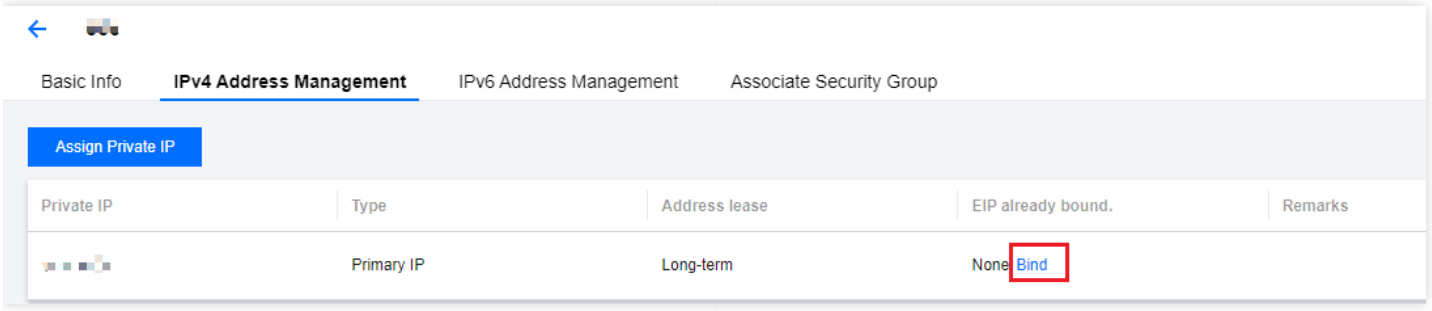
2. Click the instance ID you want to view to open the details page. Click IPv4 Address Management in the tab, find the row where the private IP to be released is located, and click Release in the Action column.



3. Click OK in the pop-up window to complete the operation.

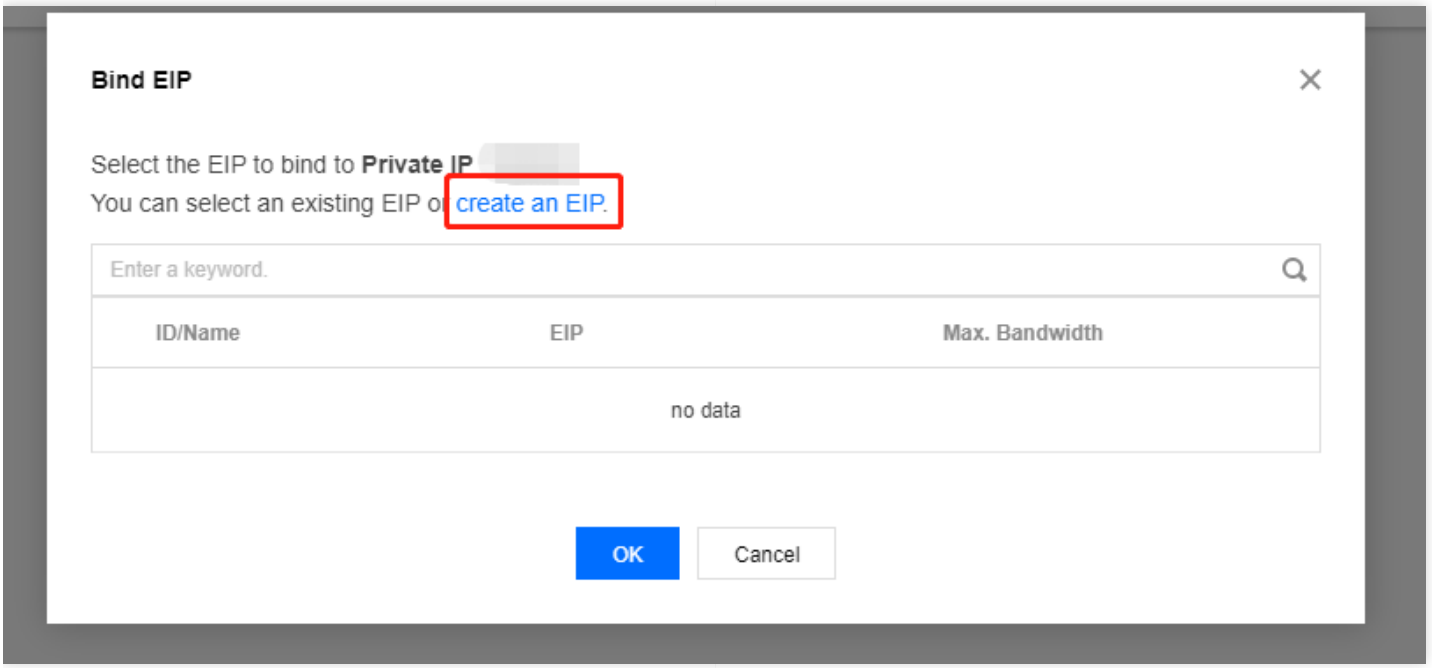
Bind an Elastic IP (EIP)

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
2. Click the instance ID to be bound to open the details page. Click IPv4 Address Management in the tab.
3. Click Bind in the EIP already bound column of the row containing the private IP to be bound.



4. In the Pop-up Box:

- If there is an optional EIP, select it and click OK.
- If there is no EIP available, you can click Create on the top of the pop-up window to request for it. After the request is successful, return to the pop-up window and click Refresh. You can see the EIP you requested for, select it and click OK.



Unbind an Elastic IP (EIP)

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.

2. Click the instance ID to be bound to open the details page. Click IPv4 Address Management in the tab, and click Unbind in the EIP already bound column of the row containing the private IP to be unbound.

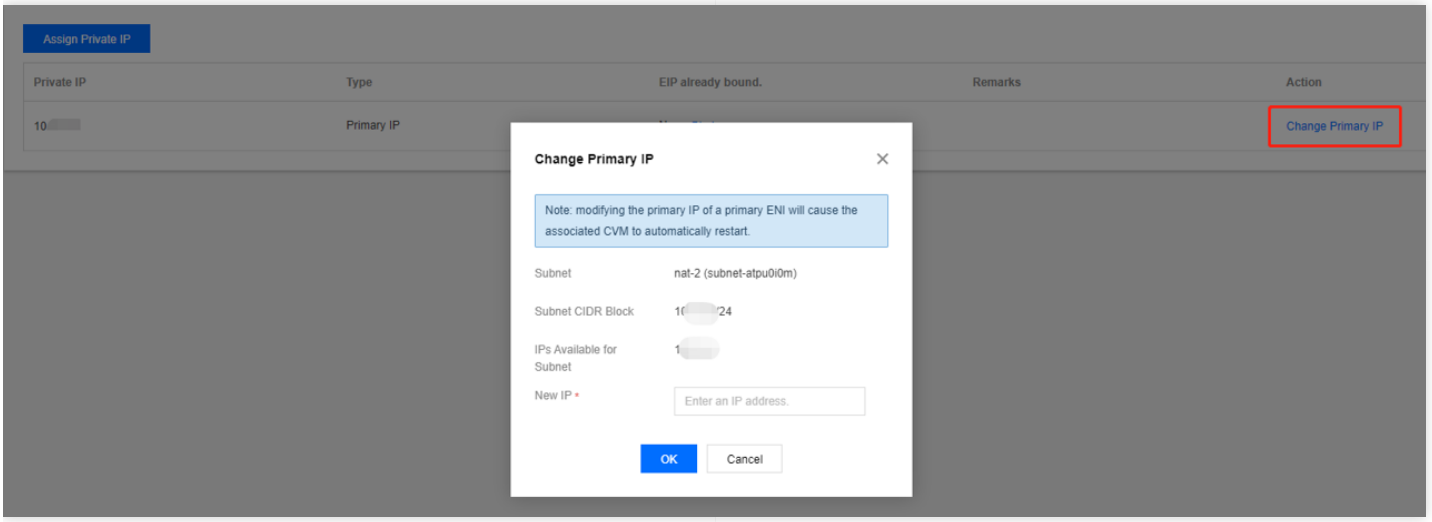
3. Click OK in the pop-up window.

Modify the primary private IP

> Note:
>
> Only the primary network interface supports modification of the private IP. IP addresses of manually created Elastic Network Interface (ENI) (secondary network interfaces) cannot be modified.

1. You can log in to the VPC console and click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.

2. Click the instance ID you want to view to open the details page. Click IPv4 Address Management in the tab, and click Modify Primary IP in the row where the primary private IP to be modified is located.



3. Click OK in the pop-up window to complete the operation.

Modify the subnet

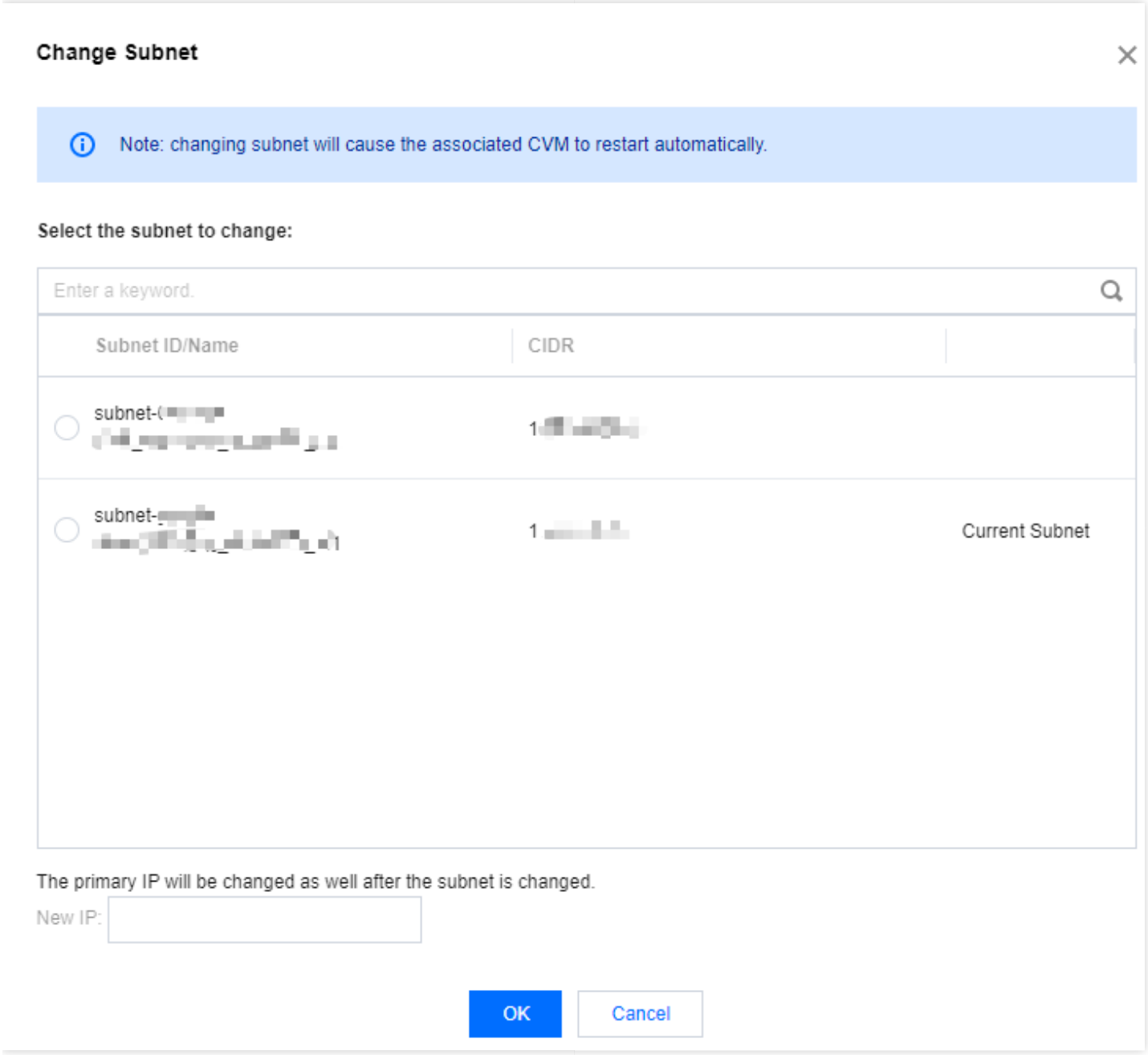
> Note:
>
> - Only the primary network interface can have its subnet modified.
> - Before you change the subnet, please unbind all secondary IPs.
> - The subnet can only be changed to another subnet in the same availability zone.

1. Log in to the VPC console and click ENI in the left directory to open the Elastic Network Interface list page.

2. Click the instance ID you want to view to open the details page. Click IP Management in the tab and click Change Subnet next to the corresponding subnet.



3. In the pop-up box, select the subnet that needs to be replaced and specify the new primary IP.


Change Subnet
Note: changing subnet will cause the associated CVM to restart automatically.
Select the subnet to change:
Enter a keyword.
Subnet ID/Name
CIDR
subnet-(
1
subnet-
1
Current Subnet
The primary IP will be changed as well after the subnet is changed.
New IP:
OK
Cancel

4. Click OK.

Request for and Releasing IPv6

1. Log in to VPC console.
2. Click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
3. Click the instance ID you want to view to open the details page.
4. Select the IPv6 Address Management tab and click Assign IP to request for an IPv6 address.

> Note:
>
> The standard quote of an ENI is one IPv6 address. If you need more IPv6 addresses, please contact the cloud platform administrator to modify the quota for you. A maximum of 10 IPv6 addresses can be allocated to one ENI.



5. Click OK in the pop-up.
6. In the IPv6 Address Management tab, you can see that the system has allocated an IPv6 address to the ENI.
7. You can release the IPv6 address by clicking Release under the operation column.

> Note:
>
> Before you release it, please disable the public network of the IPv6 address.

FAQs
Concept category

I. What is an Elastic Network Interface (ENI)?

- An ENI is a virtual network API. Users can bind with a CVM to an ENI to connect with the network. ENIs are very helpful in configuring and managing networks and building highly reliable network solutions.
- An ENI combines VPC, availability zone, and subnet attributes and can only be bound to CVMs in the same availability zone. A CVM can be bound to multiple ENIs, and the specific number of bindings will depend on the host specifications.

II. What is the difference between the primary network interface and the secondary network interface?

- The primary network interface is assigned to the user by the system and the information cannot be modified.
- The secondary network interface is created by the user and the information can be modified.

III. What are the restrictions on using ENIs?

Depending on the CPU and memory configuration, the number of ENIs that can be bound to a CVM and the number of private IPs that can be bound to a single network interface can vary greatly. For details, see the Usage Restrictions section.

IV. What should I do if the elastic IP is not accessible?

If the Elastic IP (EIP) is not accessible, consider the following reasons:

- EIP addresses are not bound to cloud services.
- The security policy is invalid. Users can check whether the security policy (security group or network ACL) is effective.
- Disable port access. Even if the bound cloud services instance has a security policy, if the port is prohibited from access, the port of the EIP is also inaccessible. For example, if access to port 8080 is prohibited, port 8080 of the EIP will also be inaccessible.

Function category

How to bind a CVM?

Users can enter the VPC console and bind the CVM.

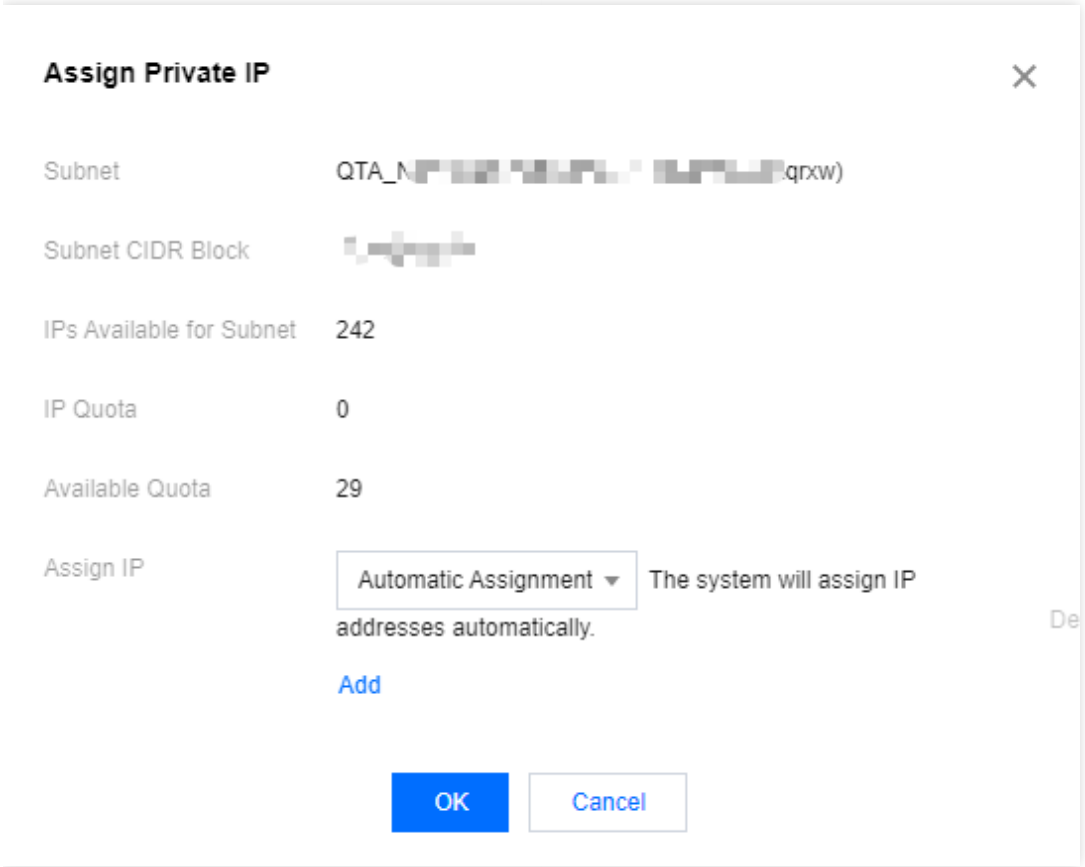
How to configure a CVM?

After the Elastic Network Interface (ENI) is bound in the console, it needs to be configured in the CVM before it can be used normally. For details, see Bind and Configure CVM.

How to allocate private IP addresses?

The steps to allocate an private IP address to a CVM ENI are as follows:

1. Open the VPC console.
2. Click IP And Network Card > ENI in the left-side directory to open the Elastic Network Interface list page.
3. Click the Instance ID of the ENI to open the ENI details page.
4. Click IPv4 Address Management to view the private IP and Elastic IP (EIP) bound to the ENI.
5. Click Assign Private IP and a pop-up window will appear to display the Assign Private IP window.
6. Select Automatically Assign or Manually Fill in the private IP.



7. Click Add and in the Allocate Private IP window, assign multiple IP addresses to the ENI.
8. Click OK to complete the console assignment of the private IP.

> Note:
>
> The private IP needs to be configured in the CVM before it can take effect.